The moduli spaces of Jacobians isomorphic to a product of two elliptic curves

Ernst Kani

1 Introduction

In 1965 Hayashida and Nishi initiated the study of genus 2 curves C whose Jacobian J_C is isomorphic to a product $A = E_1 \times E_2$ of two elliptic curves. In their papers [15], [17] and [16], they determined the number of curves C with $J_C \simeq A$ for a fixed A in many cases, thereby exhibiting the existence of such curves. A similar count was done for supersingular curves by Ibukiyama, Katsura and Oort[19].

Recently there has been renewed interest in such curves, particularly in connection with moduli problems; cf. Earle[7], Lange[30], and McMullen[32], [33].

The purpose of this article is determine how such curves are distributed in the moduli space M_2 of genus 2 curves over an algebraically closed field K. By a result of Lange[29] it is known that these lie on countably many curves in M_2; see also [7]. Here we want to make the nature of these curves precise.

To this end, let us say that a curve C *has type* d if $J_C \simeq E_1 \times E_2$, where E_1 and E_2 are connected by a cyclic isogeny of degree d. (If E_1 has CM or is supersingular, then this definition has to slightly modified; see §4 below.) Since every curve C with $J_C \simeq E_1 \times E_2$ has some type $d \geq 1$ (cf. Proposition 26), the following result describes the set of all such curves in M_2:

Theorem 1 *The set $T(d) \subset M_2$ of curves of type d is a closed subset of M_2. If $T(d)$ is non-empty, then $T(d)$ is a finite union of irreducible curves. Moreover, if $\mathrm{char}(K) \nmid d$, then each such component is birationally isomorphic either to the modular curve $X_0(d)^+$ or to a degree 2 quotient thereof.*

Here $X_0(d)^+ = X_0(d)/\langle w_d \rangle$ is (as in Mazur[31], p. 145) the quotient of the usual modular curve $X_0(d)$ by the Fricke involution w_d.

The key tool for proving this and other related results is the concept of a "generalized Humbert variety" which is introduced here. This generalizes the *Humbert surfaces* of Humbert and is based on a *refinement* of the usual Humbert invariant (cf. [39]) that was suggested in [22]. There it was observed that each curve C comes equipped with a canonically defined positive definite quadratic form q_C which can be used to define the Humbert invariant (and hence Humbert surfaces).

It turns out that the curves C of type d can be characterized by a property of their associated *refined Humbert invariant* q_C as defined in §2. To formulate this property in a convenient manner, let us introduce the following terminology.

Definition. An integral binary quadratic form $q(x,y) = ax^2+bxy+cy^2$ is said to be *of type* $d \geq 1$ if (i) its discriminant $\mathrm{disc}(q) := b^2-4ac = -16d$; (ii) $q(x,y) \equiv 0, 1 \pmod 4$, for all $x, y \in \mathbb{Z}$ and (iii) there exists $x, y, N \in \mathbb{Z}$ with $(x,y) = (N,d) = 1$ such that $q(x,y) = N^2$.

The quadratic forms of type d are studied in detail in §5. The following result explains their connection with curves of type d.

Theorem 2 *If C is a curve of genus 2, then C has type d if and only if its refined Humbert invariant q_C primitively represents a form of type d.*

In view of this, we might expect the various forms q of type d to give us the components of the curve $T(d)$, and this is indeed the case. To make this precise, let $H'(q)$ denote the set of isomorphism classes of curves C in the moduli space M_2 such that q_C represents q primitively; we call $H'(q)$ the *generalized Humbert variety* associated to q; cf. §3. Thus, Theorem 2 can be restated in terms of the $H'(q)$'s; cf. Theorem 12 (which is a refinement of Theorem 2). Moreover, if $\bar{Q}(d)$ denotes the set of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of forms of type d, and if $\bar{Q}_d^* = \bar{Q}(d) \setminus \{1_{-16d}\}$, where 1_{-16d} denotes the class of the principal form $x^2 + 4dy^2$, then we prove in §8:

Theorem 3 *If $\mathrm{char}(K) \nmid d$, then the $H'(q)$, where $q \in \bar{Q}_d^*$, are precisely the irreducible components of $T(d)$. Thus $T(d)$ has exactly $t^*(d) := \#\bar{Q}_d^*$ irreducible components.*

Note that as a consequence of the Classification Theorem 13 for forms of type d, the number $t^*(d)$ can be expressed explicitly in terms of suitable class numbers $h(D)$ or, more correctly, in terms of the number $\bar{h}(D) = h(D)/g(D)$ of (proper) equivalence classes of forms in the principal genus of discriminant D; cf. Remark 15.

The precise birational structure of the curve $H'(q)$ depends on whether or not q is a so-called *ambiguous form*, i.e., on whether or not q has order 2 in the group $\bar{Q}_{-16d}$ of equivalence classes of primitive forms of discriminant $-16d$. (If q is not primitive, then this definition has to be suitably modified; cf. §10.)

Theorem 4 *Let $q \in \bar{Q}_d^*$. If q is not an ambiguous class, then $H'(q) \sim X_0(d)^+$; otherwise $H'(q) \sim X_0(d)^+/\langle\alpha_q\rangle$, where α_q is a suitable Atkin-Lehner involution.*

This result is made more precise in §10, where an explicit recipe for the Atkin-Lehner involution α_q is given; cf. Proposition 55 and Theorem 57. Note that it can happen in certain cases that α_q acts trivially on $X_0(d)^+$; these cases are analyzed there as well.

An interesting but difficult question is to characterize the $d's$ for which there is no curve of type d, i.e. to determine the d's for which $T(d)$ is empty or, equivalently, for which $t^*(d) = 0$. Now it turns out that this condition is essentially equivalent to

the condition that $\bar{h}(-16d) = 1$ (cf. Corollary 35), which in turn means that $4d$ is an *idoneal number* (or a *convenient number*) in the sense of Euler (1778); cf. Cox[4], p. 61. As a result, the precise determination of the exceptional d's hinges on the solution of a classical problem in number theory which was first raised by Euler and Gauss.

Indeed, first Euler (1778) and then Gauss (1801) (cf. [12], Article 303) conjectured that the largest idoneal number is $d = 1848$, i.e. that the list of 65 idoneal numbers found by Euler is complete. This conjecture has not yet been proven unconditionally. However, Chowla[3] proved in 1934 that there are only finitely many idoneal numbers and Weinberger[43] showed in 1973 that the Euler/Gauss Conjecture follows from the Generalized Riemann Hypothesis (GRH), and that unconditionally there is at most one more *squarefree* idoneal number. (A survey on results about idoneal numbers can be found in [24].) Using Weinberger's results, we thus prove in §7:

Theorem 5 *$T(d)$ is empty if and only if $d = 1$ or if d is an* even *idoneal number which is not divisible by* 8. *Thus, $T(d) = \emptyset$ 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 $d = d^* > 462$. Moreover, $d^* \equiv 2 (\mathrm{mod}\ 4)$ is squarefree, and $d^* > 10^{11}$. In addition, if the Euler/Gauss Conjecture (or if (GRH)) is true, then no such d^* exists, i.e. these 21 *values are all the d's for which $T(d) = \emptyset$.*

Note that the above result can also be viewed as an *existence theorem*, and hence as a refinement of the work of Hayashida[15]; cf. Remark 44.

Finally, it should be mentioned that there is a close connection between the results obtained here and the study of elliptic subcovers $f : C \to E$ of genus 2 curves, as is explained in [10], §6.

Acknowledgments. I would like to thank Gerd Frey for the many stimulating discussions which we had about this work. In addition, I would like to gratefully acknowledge receipt of funding from the from the Natural Sciences and Engineering Research Council of Canada (NSERC). Finally, I would like to thank the referees for their careful reading of my manuscript and their for their valuable comments and lists of corrections.

2 The refined Humbert invariant

Let A be an abelian surface over an algebraically closed field K of arbitrary characteristic, and assume that A has a principal polarization $\theta \in \mathrm{NS}(A) = \mathrm{Div}(A)/\equiv$, where $\equiv$ denotes numerical equivalence. Thus, $\theta = cl(\Theta)$ is the class defined by an ample divisor $\Theta \in \mathrm{Div}(A)$ with self-intersection number $(\Theta.\Theta) = 2$. Put

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

where (.) denotes the intersection number of divisors. From the Hodge index theorem it follows easily that $q_{(A,\theta)}$ defines a positive definite quadratic form on the quotient group $\mathrm{NS}(A,\theta) = \mathrm{NS}(A)/\mathbb{Z}\theta$ (cf. [22], §3), and so $(\mathrm{NS}(A,\theta), q_{(A,\theta)})$ is a quadratic $\mathbb{Z}$-module, which will be called the *refined Humbert invariant* of the principally polarized abelian variety (A,θ). Note that the choice of a basis of $\mathrm{NS}(A,\theta) \simeq \mathbb{Z}^{\rho-1}$, where $\rho = \mathrm{rk}(\mathrm{NS}(A))$ is the Picard number, gives rise to an integral, positive definite quadratic form in $\rho - 1$ variables, and so, by varying over all such choices, the refined Humbert invariant can also be viewed as a $\mathrm{GL}_{\rho-1}(\mathbb{Z})$-equivalence class of such forms.

As was explained in [22], §5, $q_{(A,\theta)}$ is closely related to the classical *Humbert invariant* attached to an abelian surface $A/\mathbb{C}$: indeed, any number Δ which is *primitively represented* by $q_{(A,\theta)}$ is a (classical) Humbert invariant of the principally polarized abelian surface (A,θ). It thus follows that the subset

$$H_\Delta = \{\langle A,\theta\rangle \in A_2(K) : q_{(A,\theta)} \text{ primitively represents } \Delta\}$$

of the moduli space A_2 (which classifies isomorphism classes $\langle A,\theta\rangle$ of principally polarized abelian surfaces) is precisely the *Humbert surface* of *discriminant* (or invariant) Δ as defined by Humbert[18]; cf. [39], §IX.2. By Humbert, this defines an irreducible surface in $A_2(\mathbb{C})$ whenever $\Delta \equiv 0, 1 \pmod 4$, and is empty otherwise.

As was indicated in the introduction, we are primarily interested in the principally polarized abelian varieties that arise as Jacobians of (irreducible) genus 2 curves. Now if M_2 denotes the moduli space of smooth, irreducible genus 2 curves, then we have Jacobi morphism $j_2 : M_2 \to A_2$ which takes a curve C to its principally polarized Jacobian (J_C, θ_C) in $A_2(K)$.

Over $\mathbb{C}$, it is a classical fact (cf. Humbert[18], §17, or Krazer[27], p. 485) that the complement $A_2 \setminus j_2(M_2)$ is the Humbert surface H_1 of invariant 1. By a result of Weil[41], this is also true over an arbitrary field, as we now show:

Proposition 6 *Let $\langle A,\theta\rangle \in A_2(K)$. Then $\langle A,\theta\rangle \notin j_2(M_2(K))$ if and only if $q_{(A,\theta)}$ represents 1, i.e. $q_{(A,\theta)}(D) = 1$, for some $D \in \mathrm{NS}(A)$. Thus*

$$A_2 \setminus j_2(M_2) = H_1.$$

Proof. By Weil[41], Satz 2, we have that $\langle A,\theta\rangle \notin j_2(M_2)$ if and only if $(A,\theta) \simeq (E_1 \times E_2, \theta_1 + \theta_2)$ is a product of two elliptic curves and $\theta = \theta_1 + \theta_2$ is the product polarization (where $\theta_i = cl(pr_i^*(0_{E_i}))$, for $i = 1, 2$).

Now if $(A,\theta) \simeq (E_1 \times E_2, \theta_1 + \theta_2)$, then $(\theta.\theta_i) = 1$, $(\theta_i.\theta_i) = 0$ and so $q_{(A,\theta)}(\theta_i) = 1$.

Conversely, suppose $q_{(A,\theta)}(D) = 1$ for some D. Then D is necessarily primitive, for if $D = mD'$ with $D' \in \mathrm{NS}(A)$, then $1 = q_\theta(D) = m^2 q_\theta(D')$, and so $m = \pm 1$, i.e. D is primitive. Thus, by [22], Theorem 3.1, there exists an elliptic curve E on A with $(E.\theta) = 1$. Put $\theta_1 = \theta - cl(E)$. Then $\theta_1^2 = \theta^2 - 2(\theta.E) + E^2 = 0$, and so $\theta_1 = cl(mE')$, for some elliptic curve E' on A and some $m \in \mathbb{Z}$; cf. [22], Prop. 2.3. But

since $\theta = cl(E + mE')$, we have $2 = \theta^2 = 2m(E.E')$, so $m = 1$. Thus $\theta = cl(E + E')$. By Weil[41], Satz 2, we have that $(A, \theta) \simeq (E_1 \times E_2, \theta_1 + \theta_2)$ with $\theta_i = pr_i^*(0_{E_i})$, $i = 1, 2$, and so the assertion follows.

Remark 7 The above shows that the rule $(E_1, E_2) \mapsto \langle E_1 \times E_2, pr_1^* 0_{E_1} + pr_2^* 0_{E_2} \rangle$ defines a surjection $A_1 \times A_1 \to H_1$, where A_1 denotes the moduli space of elliptic curves. It not difficult to see (by an argument similar to that of the proof of Proposition 45 below) that this map is a *proper* morphism, and so $j_2(A_2)$ is an open subset of A_2. Since j_2 is birational, it thus follows (by Zariski's Main Theorem) that j_2 is an open immersion. Note that by Oort/Steenbrink[38], the Torelli map $j_g : M_g \to A_g$ need not be an immersion if $g \geq 5$ and $\mathrm{char}(K) \neq 0$.

3 Generalized Humbert varieties

The definition of a Humbert surface can be generalized as follows. Given any integral positive definite quadratic form q in r variables, let

$$H(q) = \{\langle A, \theta \rangle \in A_2(K) : q_{(A,\theta)} \text{ primitively represents } q\}.$$

In other words, $\langle A, \theta \rangle \in H(q)$ if and only if there exists an injective homomorphism $f : \mathbb{Z}^r \hookrightarrow \mathrm{NS}(A, \theta)$ with $\mathrm{NS}(A, \theta)/f(\mathbb{Z}^r)$ torsionfree such that $q = q_{(A,\theta)} \circ f$. Clearly, $H(q)$ depends only on the $\mathrm{GL}_r(\mathbb{Z})$-equivalence class of q.

Note that if q is a 1-variable quadratic form $q_\Delta(x) = \Delta x^2$, then the discussion in §2 shows that $H(q_\Delta) = H_\Delta$ is the classical Humbert surface of discriminant Δ. Thus, the $H(q)$'s generalize Humbert surfaces and hence are called *generalized Humbert varieties*.

Remark 8 In [25] it is shown that $H(q)$ is always a closed algebraic subset of A_2, and that the $H(q)$'s can be used to describe the irreducible components of the intersection of two Humbert surfaces.

In order to determine some properties of $H(q)$, we shall need to work out the refined Humbert invariant $q_{(A,\theta)}$ in many cases, and for this it is useful to know its discriminant/determinant. (Here, as usual, the determinant $\det(M, \beta)$ of a bilinear module (M, β) is the determinant of any Gram matrix $(\beta(x_i, x_j))$ associated to a basis $\{x_i\}$ of M, and the determinant $\det(M, q)$ of a quadratic module (M, q) is the determinant of the associated bilinear module (M, β_q), where β_q is the bilinear form associated to q.) It turns out that $\det(q_{(A,\theta)})$ is closely related to the determinant of the Néron-Severi group, viewed as bilinear module via the intersection pairing:

Proposition 9 *Let $\rho = \mathrm{rank}(\mathrm{NS}(A))$. Then the determinant of the quadratic module $(\mathrm{NS}(A, \theta), q_{(A,\theta)})$ is related to that of the Néron-Severi group by the formula*

$$\det(\mathrm{NS}(A, \theta), q_{(A,\theta)}) = \tfrac{1}{2}(-4)^{\rho-1} \det(\mathrm{NS}(A), (.)).$$

Proof. Let $\beta = \beta_A$ denote the intersection pairing on $\mathrm{NS}(A)$, and let $M_0 = \{(x.\theta)\theta - 2x : x \in \mathrm{NS}(A)\}$. Clearly, $(y.\theta) = 0$, if $y \in M_0$, i.e. $M_0 \perp \mathbb{Z}\theta$. Thus, if we put $M = M_0 + \mathbb{Z}\theta$, then $\det(\beta_{|M}) = 2\det(\beta_{|M_0})$, where $\beta_{|M} = \beta_{|M\times M}$ (and $\beta_{|M_0} = \beta_{|M_0\times M_0}$). Moreover, since $M \supset 2\mathrm{NS}(A)$, we see that M has finite index in $\mathrm{NS}(A)$, and so $\det(\beta_{|M}) = n^2\det(\beta)$, where $n = [\mathrm{NS}(A) : M]$. Similarly, if we put $\bar{M} = M/\mathbb{Z}\theta$, then $[\mathrm{NS}(A,\theta) : \bar{M}] = [\mathrm{NS}(A) : M] = n$, and so $\det((\beta_{\bar{q}})_{|\bar{M}}) = n^2\det(\beta_{\bar{q}})$, where $\bar{q} = q_\theta$. Now for $y_i \in M_0$ we have $\beta_{\bar{q}}(y_1, y_1) = -4\beta(y_1, y_2)$, and hence $\det((\beta_{\bar{q}})_{|\bar{M}}) = (-4)^s\det(\beta_{|M_0})$, where $s = \mathrm{rank}(M_0)$. (Note that if the elements $x_1, \ldots, x_s$ form a basis of M_0, then their images in $\bar{M}$ form a basis of $\bar{M}$.) Since $s = \rho - 1$, we obtain

$$\det(\beta_{\bar{q}}) = \frac{1}{n^2}\det((\beta_{\bar{q}})_{|\bar{M}}) = \frac{(-4)^{\rho-1}}{n^2}\det(\beta_{|M_0}) = \frac{(-4)^{\rho-1}}{2n^2}\det(\beta_{|M}) = \frac{(-4)^{\rho-1}}{2}\det(\beta).$$

4 Curves of type d

We now focus our attention to those curves C of genus 2 whose Jacobian J_C is isomorphic to a product of two elliptic curves. As we shall see below (cf. Proposition 26), these can be classified by an integer d called its *type*, which is defined as follows.

Definition. Let $d \geq 1$ be an integer. A curve C is said to have *type* d if there exist two elliptic curves E_1, E_2, a cyclic isogeny $h : E_1 \to E_2$ of degree $d = \deg(h)$ and an isomorphism $\alpha : J_C \xrightarrow{\sim} E_1 \times E_2$ such that

$$\theta_C \equiv \alpha^*(a\theta_1 + b\theta_2 + c\Gamma_h), \quad \text{for some } a, b, c \in \mathbb{Z}, \tag{3}$$

where $\theta_i = pr_i^*(0_{E_i})$, for $i = 1, 2$, and $\Gamma_h \subset E_1 \times E_2$ denotes the graph of h. We denote the set of isomorphism classes $\langle C\rangle$ of curves C of type d by $T(d) \subset M_2(K)$.

Remark 10 Suppose that $J_C \simeq E_1 \times E_2$ with $E_1 \sim E_2$. If E_1 has no complex multiplication (i.e. if $\mathrm{End}(E_1) = \mathbb{Z}$), then its type d is uniquely determined by C by the formula $\det(\mathrm{NS}(J_C)) = 2d$, as we shall see below (cf. Corollary 27). In the other cases, however, C may have several types associated to it.

The first main result of this paper is that curves of type d can be characterized by a property of the refined Humbert invariant $q_C := q_{(J_C,\theta_C)}$ associated to C. As was mentioned in the introduction, this property involves the following concept.

Definition. Let $d \geq 1$ be an integer. An integral binary quadratic form q is said to be *of type* d if it satisfies the following properties.

(i) $\mathrm{disc}(q) = -16d$;

(ii) $q \equiv 0, 1 \pmod 4$, i.e., $q(x, y) \equiv 0$ or $1 \pmod 4$, for all $x, y \in \mathbb{Z}$;

(iii) q primitively represents a square prime to d, i.e., $\exists x, y, N \in \mathbb{Z}$ with $(x, y) = (N, d) = 1$ such that $q(x, y) = N^2$.

Notation. The set of quadratic forms of type d is denoted by $Q(d)$, and its set of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes by $\bar{Q}(d)$. Furthermore, we put $\bar{Q}_d^* = \bar{Q}(d) \setminus \{1_{-16d}\}$, where 1_{-16d} denotes the class of the principal form $x^2 + 4dy^2$ of discriminant $-16d$.

Remark 11 In the context of quadratic spaces (M, q) of rank n, it is natural to consider $\mathrm{GL}_n(\mathbb{Z})$-equivalence of the associated class of quadratic forms. However, when dealing with binary quadratic forms, it is often better to use *proper* (or $\mathrm{SL}_2(\mathbb{Z})$)-equivalence since the set $\bar{Q}_D = Q_D/\mathrm{SL}_2(\mathbb{Z})$ of proper equivalence classes of primitive forms of discriminant D form a group under the composition of forms; cf. [2], p. 61.

We shall denote proper equivalence throughout by the symbol $\sim$, and use $\approx$ for $\mathrm{GL}_n(\mathbb{Z})$-equivalence. Note that for two primitive binary quadratic forms q_1, q_2 we have that

$$q_1 \approx q_2 \;\Leftrightarrow\; q_1 \sim q_2 \;\text{ or }\; q_1 \sim q_2^{-1}.$$

The following basic result is essentially a restatement of Theorem 2 of the introduction; it relates *curves* of type d to *forms* of type d.

Theorem 12 *A curve C has type d if and only if $\langle C \rangle \in H'(q) := j_2^{-1}(H(q))$, for some quadratic form q of type d. Thus*

$$T(d) = \bigcup_{q \in \bar{Q}_d^*} H'(q).$$

The proof of this theorem will be deferred until section 6 since it requires some basic facts about forms of type d which will be presented in the next section. In section 7 we shall also prove an *existence theorem* which shows that $H'(q)$ is non-empty whenever q is a non-principal form of type d; cf. Theorem 31.

5 Quadratic forms of type d

This section is devoted to a detailed study of the (binary) quadratic forms of type d which were introduced in the previous section. In particular, it will be shown that each proper equivalence class of such forms can be represented by a "standard prototype" q_s which is associated to a solution $s = (n_1, n_2, k)$ of the equation

$$n_1 n_2 \;-\; k^2 d = 1. \tag{4}$$

Notation. Fix an integer $d \geq 1$, and let

$$P(d) = \{(n_1, n_2, k) \in \mathbb{Z}^3 : n_1 > 0,\; n_2 > 0,\; n_1 n_2 - k^2 d = 1\}$$

denote the set of solutions of (4) with positive n_i's. For $s = (n_1, n_2, k) \in P(d)$, put

$$q_s(x, y) = n_1^2 x^2 + 2k(t - d)xy + n_2^2 t y^2, \quad \text{where } t = d(n_1 n_2 + 3). \tag{5}$$

Using (4) and the definition of t, we see that

$$k^2(t-d)^2 + 4d = n_1^2 n_2^2 t, \tag{6}$$

and so $\mathrm{disc}(q_s) = -16d$. It thus follows easily that q_s is always a form of type d. The main result of this section is the following.

Theorem 13 *Let $d \geq 1$ and let q be an integral binary quadratic form. Then the following conditions are equivalent:*

(i) *$q \in Q(d)$, i.e., q has type d;*

(ii) *either q is in the* principal genus *of forms of discriminant $-16d$ (i.e. $q \sim q_1^2$, for some primitive form q_1 of discriminant $-16d$) or $q = 4q_1$, for some primitive form q_1 of discriminant $-d \equiv 1 \pmod 4$ which is in the principal genus;*

(iii) *$q \sim q_s$, for some $s \in P(d)$.*

Proof. (iii) $\Rightarrow$ (ii): Let $s = (n_1, n_2, k) \in P(d)$. Since the conditions of (ii) are invariant under proper equivalence, its is enough to show that $q = q_s$ satisfies (ii). Note that $\mathrm{disc}(q_s) = -16d$ by (6).

Suppose first that n_1 is odd. Then $(n_1, \mathrm{disc}(q_s)) = (n_1, d) = 1$ by (4), so q_s primitively represents the square $n_1^2 = q_s(1,0)$ prime to $\mathrm{disc}(q_s)$, and hence by [8], Lemma 1, we know that q_s is primitive and $q_s \sim q_1^2$, for some form q_1. This means that q_s lies in the principal genus.

Next, suppose that n_2 is odd. Since $q_s(n_2^2, -k) = n_2^2(n_1^2 n_2^2 - (1 + n_1 n_2)k^2 d) = n_2^2$ and $(n_2^2, k) = 1$ by (4), we see that q_s primitively represents the square n_2^2 which is prime to $\mathrm{disc}(q_s)$, and so q_s is in the principal genus by the above argument.

Finally, suppose that n_1 and n_2 are both even. Then $q_s = 4q_1$ with $q_1 = a^2X^2 + bxy + c^2ty^2$, where $a = \frac{n_1}{2}$, $c = \frac{n_2}{2}$, and $b = k(t-d)/2 = kd(2ac+1) \in \mathbb{Z}$. Clearly $\mathrm{disc}(q_1) = \frac{1}{4^2}\mathrm{disc}(q_s) = -d$. Since q_1 primitively represents the square a^2 prime to d, it follows by the above argument that q_1 lies in the principal genus.

(ii) $\Rightarrow$ (i): If $q = 4q_1$, where $q_1 \sim q_2^2$ lies in the principal genus of discriminant $-d \equiv 1(4)$, then by Lemma 1 of [8] we see that q_1 primitively represents some square n^2 with $(n, d) = 1$ (because q_2 primitively represents some integer n with $(n, d) = 1$). Thus, q primitively represents $N^2 = (2n)^2$ and $(2n, d) = 1$. Since here $q \equiv 0 \pmod 4$, we see that $q \in Q(d)$.

Now suppose that q lies in the principal genus. Then by Lemma 1 of [8] again we see that q primitively represents some square N^2 with $(N, -16d) = 1$. Then $q \sim q' := N^2x^2 + bxy + cy^2$ with $b^2 - 4N^2c = -16d$. Thus $b = 2b_1$ is even and so $c \equiv N^2c \equiv b_1^2 \pmod 4$. Thus $q' \equiv N^2x^2 + 2b_1xy + b_1^2y^2 \equiv (Nx + b_1y)^2 \pmod 4$, and so $q' \equiv 0, 1 \pmod 4$. Thus also $q \equiv 0, 1 \pmod 4$, and so $q \in Q(d)$.

(i) $\Rightarrow$ (iii): Since $q \in Q(d)$ primitively represents N^2 with $(N^2, d) = 1$, we see that $q \sim q' := N^2x^2 + 2bxy + cy^2$ where $b, c \in \mathbb{Z}$ and $b^2 - N^2c = -4d$. To show that $q' \sim q_s$, for some $s \in P(d)$, it is enough to verify:

Claim: $\exists\, n_2, k$ such that $s = (N, n_2, k) \in P(d)$ and

$$kd(Nn_2 + 2) \equiv b \,(\mathrm{mod}\ N^2). \tag{7}$$

Indeed, if (7) holds, so $kd(Nn_2 + 2) = b + mN^2$, for some $m \in \mathbb{Z}$, and then the matrix $T = \left(\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right)$ transforms q' to q_s. Thus, $q \sim q' \sim q_s$, as desired.

To verify (7), suppose first that $N > 0$ is odd. Thus, $(N^2, 2d) = 1$ and so $\exists k \in \mathbb{Z}$ such that $2dk \equiv b \,(\mathrm{mod}\ N^2)$. Then $-4d \equiv b^2 \equiv 4d^2k^2 \,(\mathrm{mod}\ N^2)$, and so $k^2d \equiv -1 \,(\mathrm{mod}\ N^2)$. Put $n_2 := (k^2d+1)/N \in \mathbb{Z}$. Then $n_2 > 0$ and so $s := (N, n_2, k) \in P(d)$. Moreover, since $N|n_2$, we see that $kd(Nn_2+2) \equiv 2kd \equiv b \,(\mathrm{mod}\ N^2)$, and so (7) holds.

Next suppose that $N = 2N_1$ is even, so also $b = 2b_1$ is even. Since $q' \equiv 0, 1 \,(\mathrm{mod}\ 4)$ by hypothesis, we must have that $c \equiv \varepsilon \,(\mathrm{mod}\ 4)$, where $\varepsilon \in \{0, 1\}$. Thus

$$-d \;=\; b_1^2 - N_1^2 c \;\equiv\; b_1^2 - \varepsilon N_1^2 \ (\mathrm{mod}\ N^2).$$

Since $(d, N^2) = 1$, $\exists d^* \in \mathbb{Z}$ such that $d^*d \equiv 1 \,(\mathrm{mod}\ N^2)$. Put $k = d^*(b_1 + \varepsilon N_1)$. Then $kd = b_1 + \varepsilon N_1$, so $k^2d^2 \equiv d(\varepsilon Nk - 1) \,(\mathrm{mod}\ N^2)$, as a short computation shows. (This uses the fact that $\varepsilon^2 = \varepsilon$.) Multiplying by d^* yields $k^2d \equiv \varepsilon Nk - 1 \,(\mathrm{mod}\ N^2)$. Put $n_2 = (k^2d + 1)/N \equiv \varepsilon k \,(\mathrm{mod}\ N)$. Then $(N, n_2, k) \in P(d)$, and $kd(Nn_2 + 2) \equiv \varepsilon k^2 dN + 2dk \equiv \varepsilon N(Nn_2 - 1) + 2(b_1 + \varepsilon N_1) \equiv 2b_1 \,(\mathrm{mod}\ N^2)$, and so (7) holds.

Corollary 14 *The number of proper equivalence classes of forms of type d is*

$$t(d) \;:=\; |Q(d)/\mathrm{SL}_2(\mathbb{Z})| \;=\; \begin{cases} \bar{h}(-16d), & \text{if } d \not\equiv 3 \,(mod\ 4) \\ \bar{h}(-16d) + \bar{h}(-d), & \text{if } d \equiv 3 \,(mod\ 4), \end{cases} \tag{8}$$

where $\bar{h}(D) = |\bar{Q}_D^2|$ denotes the number of proper equivalence classes in the principal genus of discriminant D. Similarly, if $\bar{h}^*(D) = |\bar{Q}_D^2/\mathrm{GL}_2(\mathbb{Z})|$ denotes the number of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes in the principal genus of discriminant D, then

$$|\bar{Q}(d)| \;=\; |Q(d)/\mathrm{GL}_2(\mathbb{Z})| \;=\; \begin{cases} \bar{h}^*(-16d), & \text{if } d \not\equiv 3 \,(mod\ 4) \\ \bar{h}^*(-16d) + \bar{h}^*(-d), & \text{if } d \equiv 3 \,(mod\ 4). \end{cases} \tag{9}$$

Proof. This follows immediately from the equivalence of conditions (i) and (ii) of Theorem 13.

Remark 15 The number $\bar{h}(D)$ of classes in the principal genus can clearly be writen as

$$\bar{h}(D) \;=\; h(D)/g(D)$$

where $h(D) = |\bar{Q}_D|$ is the *class number* of forms of discriminant D and $g(D) = |\bar{Q}_D/\bar{Q}_D^2|$ denotes the *number of genera*. By Gauss's genus theory, the number $g(D)$ is explicitly known; cf. formula (18) below.

Moreover, by Remark 11 we see that $\bar{h}^*(D)$ is related to $\bar{h}(D)$ by the formula

$$\bar{h}^*(D) := \#(\bar{Q}_D^2/\mathrm{GL}_2(\mathbb{Z})) = \frac{1}{2}(\bar{h}(D) + \bar{s}(D)), \tag{10}$$

where $\bar{s}(D) = |\bar{Q}_D^2[2]|$ denotes the number of *ambiguous forms* in the principal genus. (Here and below, $\bar{Q}_D^2[2] = \{q \in \bar{Q}_D^2 : q^2 \sim 1_D\}$.) Note that this number is closely related to the number $s(D) = [\bar{Q}_D : \bar{Q}_D^4]$ of *spinor genera* of (primitive) forms of discriminant D as defined by Estes/Pall [8], for we have $\bar{s}(D) = s(D)/g(D)$. It is also interesting to observe that $\bar{h}^*(D) = c(1_D)$ is the *class number of the genus* of the principal form 1_D in the sense of Watson[40].

Although the above proof of Theorem 13 gives an explicit (computational) recipe for determining an $s \in P(d)$ such that $q_s \sim q$, we will require in the sequel more detailed information about this recipe. To this end we will give an *intrinsic* construction of s; cf. Proposition 18 below.

For this, we first note that the set $P(d)$ of solutions of (4) can be identified with a suitable set of quadratic forms of discriminant $-4d$. To define this set, it is useful to introduce the following notation. Given a discriminant $D \equiv 0, 1 \pmod 4$ and $n \in \mathbb{Z}$, let

$$Q_D^{(n)} = \{[a,b,c] \in \mathbb{Z}^3 : a > 0, b^2 - 4ac = D,\ \gcd(a,b,c)|n\}$$

denote the set of binary quadratic forms of discriminant D whose *content* $\gcd(a,b,c)$ divides n. Here, as usual, we identify $[a,b,c]$ with the quadratic form $ax^2+bxy+cy^2$.

Lemma 16 *The assignment $(n_1, n_2, k) \mapsto [n_1 d, 2kd, n_2]$ induces a bijection*

$$f_d : P(d) \xrightarrow{\sim} Q_{-4d}^{(2)}(d) := \{[a,b,c] \in Q_{-4d}^{(2)} : d|a,\ 2d|b\}.$$

Moreover, $f_d(n_1, n_2, k)$ is primitive if and only if $(n_1, n_2, k) \in P(d)^{odd}$, where $P(d)^{odd} = \{(n_1, n_2, k) \in P(d) : \gcd(n_1, n_2, 2) = 1\}$.

Proof. If $s = (n_1, n_2, k) \in P(d)$, then $\mathrm{disc}(f_d(s)) = (2dk)^2 - 4(n_1 d)n_2 = 4d(dk^2 - n_1 n_2) = -4d$. Furthermore, since $\gcd(n_1 n_2, k^2 d) = 1$ by (4), we have $\gcd(n_1 d, 2kd, n_2) = \gcd(n_1, n_2, 2)|2$, so $f_d(s) \in Q_{-4d}^{(2)}(d)$. (In particular, $f_d(s)$ is primitive if and only if $\gcd(n_1, n_2, 2) = 1$, i.e. if and only if $(n_1, n_2, k) \in P(d)^{odd}$.) Conversely, if $[n_1 d, 2dk, n_2]$ has discriminant $-4d$, then $n_1 n_2 - k^2 d = 1$, so $(n_1, n_2, k) \in P(d)$.

Next, we observe that the composition $\circ$ of binary quadratic forms (cf. [2]) gives the following relation between the quadratic forms $f_d(s)$ and q_s.

Lemma 17 *Let $s = (n_1, n_2, k) \in P(d)$ and put $t = d(n_1 n_2 + 3)$.*

(a) If n_1 is odd, then $\tilde{q}_s := [n_1, 2k(t-d), n_1 n_2^2 t] \in Q_{-16d}^{(1)}$ and

$$q_s \sim \tilde{q}_s \circ \tilde{q}_s \quad \textit{and} \quad \tilde{q}_s \circ 1_{-4d} \sim f_d(s), \tag{11}$$

where $1_{-4d} = [1, 0, d]$ *denotes the principal form of discriminant* $-4d$.

(b) If n_1 *and* n_2 *are even, then* $q_s = 4q'_s$ *with* $q'_s \in Q^{(1)}_{-d}$. *Moreover,* $f_d(s) = 2f'_d(s)$ *with* $f'_d(s) \in Q^{(1)}_{-d}$ *and we have*

$$q'_s \sim f'_d(s) \circ f'_d(s). \tag{12}$$

Proof. (a) Clearly, $\mathrm{disc}(\tilde{q}_s) = -16d$ by (6) and $\gcd(n_1, -16d) = \gcd(n_1, 2) = 1$ by (4), so $\tilde{q}_s \in Q^{(1)}_{-16d}$. Moreover, since $(n_1, \mathrm{disc}(\tilde{(q_s)}) = 1$, the the proof of [8], Lemma 1, shows that $\tilde{q}_s \circ \tilde{q}_s \sim q_s$. The second formula of (11) follows directly from the composition formula of Arndt applied to $\tilde{q}_s$ and $[d, 0, 1] \sim 1_{-4d}$; cf. [2], p. 129. (Note that $B = 2kd$ satisfies the required congruences.)

(b) In the proof of the implication $(iii) \Rightarrow (ii)$ of Theorem 13 we had seen that $q = 4q_1$ with $q_1 = [a^2, b, c^2 t]$, where $a = \frac{n_1}{2}$, $c = \frac{n_2}{2}$, and $b = k(t-d)/2 = kd(2ac+1)$, and that $q_1 \in Q^{(1)}_{-d}$. Thus, if we put $\tilde{q}'_s = [a, b, ac^2 t] \in Q^{(1)}_{-d}$, then we have again by [8], Lemma 1, that $\tilde{q}'_s \circ \tilde{q}'_s \sim q'_s$ because $\gcd(a, d) = 1$. Now $\tilde{q}'_s \sim f'_d(s) = [da, kd, c]$ because the matrix $g = \left(\begin{smallmatrix} 2c & -k \\ -kd & 2a \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & kdc \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ transforms $f'_d(s)$ into $\tilde{q}'_s$, as a computation shows. Thus, $f'_d(s) \circ f'_d(s) \sim \tilde{q}'_s \circ \tilde{q}'_s \sim q'_s$, which proves (12).

To obtain the desired intrinsic construction of s (or of $f_d(s)$), we shall interpret the relation (11) in terms of a natural homomorphism $\pi'_d : \bar{Q}_{-4d} \to \bar{Q}_{-16d}$. To construct this map, recall that for any discriminant D and integer $n \geq 1$ we have a natural homomorphism $\pi_{D,n} : \bar{Q}_{n^2 D} \to \bar{Q}_D$ given by $q \mapsto q \circ 1_D$; cf. [2], p. 132. We now prove:

Proposition 18 *For any* $d \geq 1$ *there is a unique homomorphism* $\pi'_d : \bar{Q}_{-4d} \to \bar{Q}_{-16d}$ *such that*

$$\pi'_d(\pi_{-4d,2}(q)) \sim q \circ q, \quad \textit{for all } q \in \bar{Q}_{-16d}. \tag{13}$$

Furthermore, the image of π'_d *is* $(\bar{Q}_{-16d})^2$, *the principal genus of discriminant* $-16d$.

Proof. First note that $\pi_{D,n}$ is always surjective. Indeed, by using Dedekind's identification of $\bar{Q}_D$ with $\mathrm{Pic}(\mathfrak{O}_D)$, where $\mathfrak{O}_D = \mathbb{Z} + \frac{1}{2}(1+\sqrt{D})\mathbb{Z}$, the map $\pi_{D,n}$ corresponds to the canonical map $\tilde{\pi}_{D,n} : \mathrm{Pic}(\mathfrak{O}_{n^2 D}) \to \mathrm{Pic}(\mathfrak{O}_D)$ induced by the inclusion $\mathfrak{O}_{n^2 D} \subset \mathfrak{O}_D$, and the map $\tilde{\pi}_{D,n}$ is known to be surjective; cf. Lang[28], p. 94.

From the explicit relation between $h(D) := |\bar{Q}_D| = |\mathrm{Pic}(\mathfrak{O}_D)|$ and $h(n^2 D)$ (cf. [28], p. 95), we see that $|\mathrm{Ker}(\pi_{D,2})| = 2$, if $D = -4d$ and $d > 1$; in fact, we have

$$\mathrm{Ker}(\pi_{-4d,2}) = \{1_{-16d}, q_d\}, \tag{14}$$

where $q_d = [4, 0, d]$, if $d \equiv 1\,(2)$, and $q_d = [4, 4, d+1]$, if $d \equiv 0\,(2)$, as is easy to verify. Thus, if $S(q) = q \circ q$ denotes the squaring homomorphism on $\bar{Q}_{4D}$, then $\mathrm{Ker}(\pi_{D,2}) \leq \mathrm{Ker}(S)$, and so by the universal property of quotients, there is a unique homomorphism $\pi'_d : \bar{Q}_D \to \bar{Q}_{4D}$ such that $S = \pi'_d \circ \pi_{D,2}$. This proves the first assertion (when $d > 1$), and the second follows because $(\bar{Q}_{4D})^2$ is the image of S and $\pi_{D,2}$ is surjective. On the other hand, if $d = 1$, then the unique isomorphism $\pi'_1 : \bar{Q}_{-4} \xrightarrow{\sim} \bar{Q}_{-16} = \{1\}$ trivially satisfies the assertions.

Corollary 19 *If $s = (n_1, n_2, k) \in P(d)^{odd}$, then $q_s \sim \pi'_d(f_d(s))$, and if $s \in P(d)^{even} := P(d) \setminus P(d)^{odd}$, then $q'_s \sim f'_d(s)^2$. In particular, if $s_1, s_2 \in P(d)$, then $q_{s_1} \sim q_{s_2}$ whenever $f_d(s_1) \sim f_d(s_2)$.*

Proof. The last assertion clearly follows from the first two because if $f_d(s_1) \sim f_d(s_2)$, then s_1, s_2 are either both odd or both even by Lemma 16.

If n_1 is odd, then the first assertion follows directly from (11) and (13), and if n_1 and n_2 are both even, then $q'_s \sim f'_d(s)^2$ by (12).

There remains the case that n_1 is even and n_2 is odd. Here we observe that

$$f_d(n_1, n_2, k) \sim f_d(n_2, n_1, -k), \quad \text{for all } s = (n_1, n_2, k) \in P(d),$$

because the matrix $g = \left(\begin{smallmatrix} n_2 & -k \\ -kd & n_1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ transforms $f_d(s)$ into $f_d(s')$, where $s' = (n_2, n_1, -k)$. Similarly, we have

$$q_s \sim q_{s'}, \tag{15}$$

because the matrix $g' = \left(\begin{smallmatrix} n_2^2 & -y \\ -k & n_1^2 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, where $y = (n_1 n_2 + 1)kd$, transforms q_s into $q_{s'}$, as a somewhat tedious computation using (4) shows. Thus, since n_2 is odd, we have by (11) and (13) that $q_{s'} \sim \pi'_d(f_d(s'))$, and so $q_s \sim q_{s'} \sim \pi'_d(f_d(s')) \sim \pi'_d(f_d(s))$, as claimed.

Corollary 20 *For $d > 1$ we have*

$$|\mathrm{Ker}(\pi'_d)| \;=\; \tfrac{1}{2} g(-16d) \;=\; 2^{\omega(d)-1}, \tag{16}$$

where $\omega(d)$ denotes the number of distinct prime divisors of d. Thus

$$q \in \mathrm{Ker}(\pi'_d) \;\Leftrightarrow\; q \sim [d_1, 0, d_2], \text{ where } d_1 d_2 = d,\ d_1 \le d_2, \text{ and } \gcd(d_1, d_2) = 1. \tag{17}$$

Proof. Since $\pi'_d \circ \pi_{D,2} = S$ by (13), and $|\mathrm{Ker}(\pi_{D,2})| = 2$ by (14), we see that $|\mathrm{Ker}(\pi'_d)| = \frac{1}{2}|\mathrm{Ker}(S)| = \frac{1}{2}|\mathrm{Coker}(S)| = \frac{1}{2} g(4D)$. This proves the first equality of (16). To prove the second, recall that Gauss's genus theory yields

$$g(D) = 2^{\omega(D)-1+\varepsilon(D)}, \tag{18}$$

where $\varepsilon(D) = 1$ if $D \equiv 0 \pmod{32}$, $\varepsilon = -1$ if $D \equiv 4 \pmod{16}$ and $\varepsilon(D) = 0$ otherwise; cf. [21], p. 170. From this, the second part of formula (16) follows easily.

Let d_1, d_2 be as indicated. If d_1 is odd, then $[d_1, 0, 4d_2] \in \mathrm{Ker}(S)$ and so $[d_1, 0, d_2] \sim [d_1, 0, 4d_2] \circ 1_D \sim \pi_{D,2}([d_1, 0, 4d_2]) \in \mathrm{Ker}(\pi'_d)$. Similarly, if d_1 is even, then d_2 is odd, and then $[d_1, 0, d_2] \sim \pi_{D,2}([4d_1, 0, d_2]) \in \mathrm{Ker}(\pi'_d)$. Since the forms $[d_1, 0, d_2]$ are all reduced, they yield $2^{\omega(d)-1}$ distinct equivalence classes in $\mathrm{Ker}(\pi'_d)$. By (16) we have thus found all the classes in $\mathrm{Ker}(\pi'_d)$ and so (17) follows.

We conclude this section with the following two (technical) results which will be used in in the next section.

Lemma 21 *The inclusion $Q^{(2)}_{-4d}(d) \subset Q^{(2)}_{-4d}$ induces a bijection*

$$Q^{(2)}_{-4d}(d)/\Gamma_0(d) \xrightarrow{\sim} Q^{(2)}_{-4d}/\mathrm{SL}_2(\mathbb{Z}),$$

where $\Gamma_0(d) = \{g = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : d|z\}$.

Proof. Recall that the action of $g = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ on $Q^{(n)}_D$ is given by

$$[a,b,c]g = [ax^2 + bxz + cz^2, b(xw+yz) + 2(axy + czw), ay^2 + byw + cw^2]; \tag{19}$$

cf. [2], p. 4. In other words, we have $M(qg) = g^t M(q) q$, where $M(q) = \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$ denotes the matrix associated to $q = [a, 2b, c]$. From this we see easily that $\Gamma_0(d)$ acts on $Q^{(2)}_D(d)$, where $D = -4d$, and so we have a map $j : Q^{(2)}_D(d)/\Gamma_0(d) \to Q^{(2)}_D/\mathrm{SL}_2(\mathbb{Z})$.

To see that j is injective, suppose that $q_i = [a_i d, 2b_i d, c_i] \in Q^{(2)}_D(d)$, are such that $j(q_1) = j(q_2)$. Then there is a $g = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$ such that $m_2 = m_1[g] := g^t m_1 g$. Then $a_2 d = a_1 d x^2 + 2b_1 dxz + c_1 z^2$ and $b_2 d = b_1 d(xw + yz) + (a_1 dxy + c_1 zw)$, so $d|\gcd(c_1 z^2, c_1 zw) = c_1 z$, and hence $d|z$ because $\gcd(c_1, d) = 1$. (Recall that $(a_i, c_i, b_i) \in P(d)$; cf. Lemma 16.) Thus, $g \in \Gamma_0(d)$, and so j is injective.

We now prove that j is surjective. Let $q = [a, 2b, c] \in Q^{(2)}_{-4d}$. We first note that by replacing q by qg with a suitable $g \in \mathrm{SL}_2(\mathbb{Z})$ we may assume $\gcd(a, d) = 1$. Indeed, if $q \in Q^{(1)}_{-4d}$, then this is well-known; cf. [2], pp. 49-50. In the other case we have $q = 2q_1$, where $q_1 \in Q^{(1)}_{-d}$ and $-d \equiv 1 \pmod 4$, and so the assertion follows by the same argument applied to q_1. Thus, $\gcd(a, d) = 1$ and hence also $\gcd(a, b) = 1$ because $ac - b^2 = d$. Thus, there exist $x, y \in \mathbb{Z}$ such that $g = \left(\begin{smallmatrix} -b & x \\ a & y \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Then $qg = [ad, 2yd, *]$, and so we see that $q \in \mathrm{Im}(j)$. This proves that j is bijective.

Lemma 22 *Let (M, q) be a quadratic module of rank 2, and suppose that M has a basis $\{v_1, v_2\}$ such that for some $s = (n_1, n_2, k) \in P(d)$ we have*

$$q(xv_1 + yv_2) = q_s(x, y), \quad \textit{for all } x, y \in \mathbb{Z}.$$

Put $w_1 = v_1$ and $w_2 = -n_2^2 v_1 + k v_2$. Then

$$q(xw_1 + yw_2) = n_1^2 x^2 + 2(n_1 n_2 - 2)xy + n_2^2 y^2. \tag{20}$$

Moreover, for $w_3 = -n_2 k d v_1 + n_1 v_2$ we have that $q(w_3) = 4d n_1 n_2$.

Proof. The relation (20) is a straight-forward computation, using the transformation law (19) applied to $g = \left(\begin{smallmatrix} 1 & -n_2^2 \\ 0 & k \end{smallmatrix}\right)$ and the relation (4).

To compute $q(w_3)$, note first that by (4) we have $k w_3 = n_2 w_1 + n_1 w_2$. Thus, by (20) we obtain $k^2 q(w_3) = q(n_2 w_1 + n_1 w_2) = 4n_1 n_2(n_1 n_2 - 1) = 4n_1 n_2 k^2 d$, and so $q(w_3) = 4n_1 n_2 d$, provided that $k \neq 0$. Moreover, this relation also holds when $k = 0$ because in that case $n_1 = n_2 = 1$ by (4), so $q_s(x, y) = x^2 + 4dy^2$, and hence $q(w_3) = q_s(0, 1) = 4d = 4d n_1 n_2$.

6 The product surface $E_1 \times E_2$

The aim of this section is to prove the basic classification Theorem 12. For this, it is useful to use the following "presentation" of the Néron-Severi group $\mathrm{NS}(A)$ of a product surface $A = E_1 \times E_2$ of two elliptic curves E_1 and E_2.

Proposition 23 *For $a, b \in \mathbb{Z}$ and $h \in \mathrm{Hom}(E_1, E_2)$ put*

$$\mathbf{D}(a, b, h) = (a - \deg(h))\theta_1 + (b-1)\theta_2 + \Gamma_{-h} \in \mathrm{Div}(A), \tag{21}$$

where $\theta_i = p_i^*(0_{E_i})$, and $\Gamma_f \in \mathrm{Div}(A)$ is the graph of $f = -h$. Then the rule $(a, b, h) \mapsto cl(\mathbf{D}(a, b, h)) := \mathbf{D}(a, b, h) + \mathrm{Div}^0(A) \in \mathrm{NS}(A) = \mathrm{Div}(A)/\mathrm{Div}^0(A)$ defines a group isomorphism

$$\mathbf{D} = \mathbf{D}_{E_1, E_2} : \mathbb{Z} \oplus \mathbb{Z} \oplus \mathrm{Hom}(E_1, E_2) \xrightarrow{\sim} \mathrm{NS}(E_1 \times E_2),$$

and the intersection number of two such divisors is given by

$$(\mathbf{D}(a, b, f).\mathbf{D}(a', b', f')) \;=\; ab' + ba' - \beta_d(f, f'), \tag{22}$$

where β_d is the bilinear form associated to the degree quadratic form on $\mathrm{Hom}(E_1, E_2)$, i.e. $\beta_d(f, f') = \deg(f + f') - \deg(f) - \deg(f')$. In addition, the homomorphism $\phi_D : A \to \hat{A}$ associated to $D = \mathbf{D}(a, b, f)$ is given by

$$\phi_{\mathbf{D}(a,b,f)} = \lambda_1 \otimes \lambda_2 \circ \begin{pmatrix} [a]_{E_1} & f^t \\ f & [b]_{E_2} \end{pmatrix}, \tag{23}$$

where $\lambda_1 \otimes \lambda_2$ denotes the product polarization associated the canonical polarizations $\lambda_i : E_i \xrightarrow{\sim} \hat{E}_i$, for $i = 1, 2$, and $f^t = \lambda_1^{-1} \hat{f} \lambda_2$ is the dual map.

Proof. Most of this is well-known; for example, the fact that $\mathbf{D}$ is an isomorphism is a special case of the basic relation between correspondences of curves and homomorphisms of their Jacobians; cf. [35], p. 185. In the appendix below we derive this in Proposition 63 as a special case of a more general construction (based on (23)) which has the advantage of being more functorial.

Corollary 24 *The determinant of the Néron-Severi group of $E_1 \times E_2$ with respect to the intersection form is given by*

$$\det(\mathrm{NS}(E_1 \times E_2)) = (-1)^{\rho - 1} \det(\mathrm{Hom}(E_1, E_2), \beta_d), \tag{24}$$

where $\rho = \mathrm{rank}(\mathrm{NS}(E_1 \times E_2)) = \mathrm{rank}(\mathrm{Hom}(E_1, E_2)) + 2$ and β_d is as above.

Proof. Put $\Gamma_f^* = \mathbf{D}(0, 0, f)$. If $f_1, \ldots, f_r$ is a basis of $\mathrm{Hom}(E_1, E_2)$, then by Proposition 23 we have that $\theta_1, \theta_2, \Gamma_{f_1}^*, \ldots, \Gamma_{f_r}^*$ is a basis of $\mathrm{NS}(E_1 \times E_2)$ and so by (22) we see

that the Gram matrix $G(\theta_1, \theta_2, \Gamma_1^*, \ldots, \Gamma_{f_r}^*)$ of the intersection form with respect to this basis is given by the block diagonal matrix

$$G(\theta_1, \theta_2, \Gamma_{f_1}^*, \ldots, \Gamma_{f_r}^*) = \operatorname{diag}\left(\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), -G(f_1, \ldots, f_r)\right),$$

where $G(f_1, \ldots, f_r)$ is the Gram matrix of β_d with respect to the basis $f_1, \ldots, f_r$. From this, formula (24) follows by taking the determinant of both sides.

In the sequel we shall be particularly interested in the set $\mathcal{P}(A)$ consisting of those divisors $D \in \mathrm{NS}(A)$ which define principal polarizations on A. These can be characterized by using the set $P(d)$ introduced in the previous section.

Corollary 25 *Let $D = \mathbf{D}(a, b, h) \in \mathrm{NS}(A)$. Then D defines a principal polarization (i.e. $D \in \mathcal{P}(A)$) if and only if $a > 0$ and $ab - \deg(h) = 1$. Thus, every principal polarization of A has the form*

$$D_{s,h} = \mathbf{D}(n_1, n_2, kh) \quad \text{with } h \in \mathrm{Hom}(E_1, E_2) \text{ and } s = (n_1, n_2, k) \in P(\deg(h)). \tag{25}$$

Proof. By the Riemann-Roch Theorem (cf. [34], p. 127), $D \in \mathcal{P}(A)$ if and only if D is ample and $D^2 = 2$, and this holds if and only if $D^2 = 2$ and $(D.\theta_2) > 0$; cf. [22], Corollary 2.2b). Thus, the first assertion follows in view of (22). The second follows from this and the fact that $\deg(kh) = k^2 \deg(h)$.

We now turn to the study of curves C of type d. As promised, we first verify that every curve whose Jacobian is isomorphic to a product of two elliptic curves has a type d, for some $d \geq 1$.

Proposition 26 *Let C be a curve such that its Jacobian J_C has an isomorphism $\alpha : J_C \xrightarrow{\sim} E_1 \times E_2$ to a product of two elliptic curves. Then there exists a* cyclic *isogeny $h : E_1 \to E_2$ of some degree $d \geq 1$ such that*

$$\theta_C \equiv \alpha^*(D_{s,h}), \quad \text{for some } s = (n_1, n_2, k) \in P(d) \text{ with } k \neq 0. \tag{26}$$

In particular, E_1 is isogenous to E_2 and C has type d.

Proof. Put $D \equiv (\alpha^{-1})^*(\theta_C) \in \mathcal{P}(E_1 \times E_2)$. By Proposition 23 and Corollary 25, $D = \mathbf{D}(n_1, n_2, h_1)$, for some integers n_1, n_2 and homomorphism $h_1 \in \mathrm{Hom}(E_1, E_2)$ satisfying $n_1 n_2 - \deg(h_1) = 1$ and $n_1 > 0$. Note that $h_1 \neq 0$, for otherwise $n_1 = n_2 = 1$ which means $D \equiv \theta_1 + \theta_2$. But then $q_C(\alpha^* \theta_1) = 1$, which contradicts Proposition 6.

Thus, we can write $h_1 = kh$, where h is a cyclic isogeny and $k \neq 0$, and so we see that (26) holds with $s = (n_1, n_2, k) \in P(d)$. Note that this means that C has type d because $D \equiv k\mathbf{D}(n_1, n_2, h) = k(n_1 - d)\theta_1 + k(n_2 - 1)\theta_2 + k\Gamma_{-h}$.

Corollary 27 *If $J_C \simeq E_1 \times E_2$, where $\mathrm{End}(E_1) = \mathbb{Z}$, then C is a curve of unique type $d = \frac{1}{2}\det(\mathrm{NS}(J_C))$.*

Proof. Since $E_1 \sim E_2$ by Proposition 26, it follows that $\mathrm{Hom}(E_1, E_2) = \mathbb{Z}h$, for some isogeny h, and so by (24) we have $\det(\mathrm{NS}(J_C)) = (-1)^2 \det(\mathrm{NS}(E_1 \times E_2)) = \beta_d(h,h) = 2d$, where $d = \deg(h)$.

Note that h is necessarily cyclic, and that the only cyclic isogenies in $\mathrm{Hom}(E_1, E_2)$ are $\pm h$. Thus, if $\alpha : J_C \xrightarrow{\sim} E_1 \times E_2$ is any isomorphism, then $\theta_C \equiv \alpha^*(D_{s,h})$, for some $s \in P(d)$, and so C has (unique) type $d = \frac{1}{2}\det(\mathrm{NS}(J_C))$.

Remark 28 (a) Although the type d is uniquely determined by the curve C in the above situation, the (isomorphism classes of the) elliptic curves E_1 and E_2 are not unique. Indeed, if d has more than one prime factor, then we can have an isomorphism $E_1 \times E_2 \simeq E_1' \times E_2'$ with $E_1' \not\simeq E_1, E_2$; cf. Proposition 51 below.

(b) If C is any curve of type d satisfying (26) with $(n_1, n_2, k) \in P(d)$, then $\langle C \rangle \in H_{n_1^2} \cap H_{n_2^2}$. because $q_C(\alpha^*(\theta_1)) = n_2^2$ and $q_C(\alpha^*(\theta_1)) = n_1^2$ by (22) (and (2)), and because the image of the elliptic curve $\alpha^*(\theta_i)$ in $\mathrm{NS}(J_C, \theta_C)$ is primitive by [22], Theorem 2.8.

We now turn to the proof of Theorem 12. One direction is contained in the following more precise result.

Proposition 29 *Let $A = E_1 \times E_2$ and $\theta = D_{s,h} \in \mathcal{P}(A)$, where h is a cyclic isogeny of degree d and $s = (n_1, n_2, k) \in P(d)$. Let $\bar\theta_1$, $\bar\theta_2$ and $\bar\Gamma_h^*$ denote the images of θ_1, θ_2, and $\Gamma_h^* = \mathbf{D}(0,0,h)$ in $\mathrm{NS}(A,\theta)$, respectively.*

(a) $\bar M := \langle \bar\theta_1, \bar\theta_2, \bar\Gamma_h^* \rangle$ is a primitive submodule of $\mathrm{NS}(A,\theta)$, and so $\langle A, \theta\rangle \in H(q_{\bar M})$, where $q_{|M}$ denotes the restriction of $q_\theta = q_{(A,\theta)}$ to $\bar M$.

(b) Let $\bar D = -kd\bar\theta_1 - n_2\bar\Gamma_h^*$. Then $\{\bar\theta_2, \bar D\}$ is a basis of $\bar M$, and we have

$$q_\theta(x\bar\theta_2 + y\bar D) \;=\; q_s(x,y) \quad \forall x, y, \in \mathbb{Z}, \quad \textit{where } q_s \textit{ is defined by } (5). \tag{27}$$

Proof. (a) Since h is a cyclic isogeny, it is a primitive element in $\mathrm{Hom}(E_1, E_2)$, and so we can extend h to a basis $h_1 = h, h_2, \ldots, h_r$ of $\mathrm{Hom}(E_1, E_2)$. Then $\{cl(\theta_1), cl(\theta_2), cl(\Gamma_{h_1}^*), \ldots, cl(\Gamma_{h_r}^*)\}$ is a basis of $\mathrm{NS}(E_1 \times E_2)$; cf. Corollary 24. Thus, $M := \langle cl(\theta_1), cl(\theta_2), cl(\Gamma_h^*)\rangle$ is a primitive submodule of $\mathrm{NS}(E_1 \times E_2)$, and so we see that $\bar M = M/(\mathbb{Z}\theta)$ is a primitive submodule of $\mathrm{NS}(A,\theta)$. This means that q_θ primitively represents $q_{\bar M}$, and so $\langle A, \theta\rangle \in H(q_{\bar M})$.

(b) Put $D = \mathbf{D}(-kd, 0, -n_2 h) \in \mathrm{NS}(A)$; thus, the image of D in $\mathrm{NS}(A,\theta)$ is $\bar D$. Using (4), we see that $cl(\theta_1) = n_2\theta - n_2^2 cl(\theta_2) + kD$, and $cl(\Gamma_h^*) = -kd\theta + n_2 kd cl(\theta_2) - n_1 D$, so $\{\theta, cl(\theta_2), D\}$ is a basis of M, and hence $\{\bar\theta_2, \bar D\}$ is a basis of $\bar M$.

Put $D_1 = x\theta_2 + yD$. Then by computing intersection numbers we find that $(\theta.D_1) = n_1 x + n_2 kdy$ and $D_1^2 = 2(-kdxy - n_2^2 dy^2)$, and so $q_\theta(D_1) = (\theta.D_1)^2 - 2D_1^2 = n_1^2x^2 + 2kd(n_1n_2 + 2)xy + n_2^2 d(k^2 d + 4)y^2 = q_s(x,y)$; here we used the fact that $k^2 d + 4 = n_1 n_2 + 3$ by (4).

For the other direction we shall use the following elementary fact.

Lemma 30 *Let* $\overline{cl} : \mathrm{NS}(A) \to \mathrm{NS}(A,\theta) = \mathrm{NS}(A)/\mathbb{Z}\theta$ *denote the quotient map, and let* $\bar{D} \in \mathrm{NS}(A,\theta)$. *If* $n \in \mathbb{Z}$, *then*

$$(28)\quad \exists D \in \mathrm{NS}(A) \text{ with } (D.\theta) = n \text{ and } \overline{cl}(D) = \bar{D} \;\Leftrightarrow\; n \equiv q_{(A,\theta)}(\bar{D}) \pmod 2.$$

Proof. If D exists, then $q_\theta(\bar{D}) = q_\theta(D) = n^2 - 2D^2 \equiv n^2 \equiv n \pmod 2$. Conversely, suppose that $n \equiv q_C(\bar{D}) \pmod 2$, and let $D_0 \in \mathrm{NS}(A)$ be any class with $\overline{cl}(D_0) = \bar{D}$. Put $n_0 = (D.\theta)$. Then, by what was just shown, $n_0 \equiv q_C(\bar{D}) \equiv n \pmod 2$, and so $D = \frac{1}{2}(n - n_0)\theta + D_0$ satisfies (28).

Proof of Theorem 12. If C is a curve of type d, then by definition and the proof of Proposition 26 we see that (26) holds for some $s = (n_1, n_2, k) \in P(d)$. Then Proposition 29 shows that q_C primitively represents the form q_s, which is a form of type d by Theorem 13.

Conversely, suppose that $\langle C\rangle \in H(q)$, where q is a form of type d. Then by Theorem 26 we know that $q \sim q_s$ for some $s = (n_1, n_2, k) \in P(d)$. (Note that $k \neq 0$ for otherwise q_s represents $1 = n_2^2$, which contradicts Proposition 6.) Since q_C represents $q \sim q_s$ primitively, there exists a primitive submodule $\bar{M}$ of $\mathrm{NS}(J_C, \theta_C)$ and a basis $\{\bar{D}'_1, \bar{D}'_2\}$ of $\bar{M}$ such that

$$q_C(x\bar{D}'_1 + y\bar{D}'_2) = q_s(x,y), \quad \text{for all } x, y \in \mathbb{Z}.$$

Put $\bar{D}_1 = \bar{D}'_1$ and $\bar{D}_2 = -n_2^2\bar{D}'_1 + k\bar{D}'_2$; note that $\bar{D}_1$ and $\bar{D}_2$ are primitive elements of $\bar{M}$ and hence also of $\mathrm{NS}(J_C, \theta_C)$ because $\gcd(-n_2^2, k) = 1$. Applying Lemma 22 to $M = \bar{M}$ and $v_i = \bar{D}'_i$, we see from (20) that $q_C(\bar{D}_1) = n_1^2$ and $q_C(\bar{D}_2) = n_2^2$. Thus, by Theorem 3.2 of [22] we know that there are unique elliptic subgroups $E_i \leq J_C$ such that $\overline{cl}(E_i) = \bar{D}_i$, for $i = 1, 2$, and that we have $(E_i.\theta_C) = n_i$. Furthermore, since $E_i^2 = 0$, we have $4(E_1.E_2) = 2(E_1 + E_2)^2 = ((E_1 + E_2).\theta_C)^2 - q_C(E_1 + E_2) = (n_1+n_2)^2 - q_C(\bar{D}_1+\bar{D}_2)$. By (20) we know that $q_C(\bar{D}_1+\bar{D}_2) = n_2^2+2(n_1n_2-2)+n_1^2$, and so $(E_1.E_2) = 1$. Thus, by Weil[41], Satz 2, there is an isomorphism $\alpha : J_C \xrightarrow{\sim} E_1 \times E_2$ such that $\alpha^*\theta_1 = E_2$ and $\alpha^*\theta_2 = E_1$.

It remains to show that C has type $d = -\frac{1}{16}\mathrm{disc}(q)$. For this, put $D = \alpha_*\theta_C \in \mathcal{P}(E_1 \times E_2)$, and write $D = \mathbf{D}(a, b, ch)$, where $a, b, c \in \mathbb{Z}$ and $h \in \mathrm{Hom}(E_1, E_2)$ is cyclic. Then $n_1 = (\theta_C.E_1) = (D.\theta_2) = a$, so $a = n_1$ and similarly $b = n_2$.

To prove that $d = \deg(h)$, consider $\bar{D}_3 := -n_2kd\bar{D}'_1 + n_1\bar{D}'_2$. Since $q_C(\bar{D}_3) = 4dn_1n_2$ by Lemma 22, we know by Lemma 30 that there exists $D_3 \in \mathrm{NS}(J_C)$ such that $(D_3.\theta_C) = -2kd$ and $\overline{cl}(D_3) = \bar{D}_3$. We now observe that

$$(29)\qquad \theta_C \equiv n_2E_1 + n_1E_2 - kD_3.$$

Indeed, since $k\bar{D}_3 = n_2\bar{D}_1 + n_1\bar{D}_2$ (cf. the proof of Lemma 22), it follows that $\theta' := n_2E_1 + n_1E_2 - kD_3 = m\theta_C$, for some $m \in \mathbb{Z}$. But then $2m = m\theta_C^2 = (\theta'.\theta_C) = n_2n_1 + n_1n_2 + k(-2kd) = 2$ by (4), so $m = 1$. Thus (29) holds, and so we obtain that

$-k\alpha_* D_3 = c\Gamma_h^*$ because $\mathbf{D}(n_1, n_2, ch) = \alpha_*\theta_C = n_2 cl(\theta_2) + n_1 cl(\theta_1) - k\alpha_* D_3$. Since Γ_h^* is primitive in $\mathrm{NS}(E_1 \times E_2)$, it follows that $\alpha_* D_3 = c'\Gamma_h^*$, where $c' = -\frac{c}{k} \in \mathbb{Z}$. Thus, $D_3 = c' D_3'$, where $D_3' := \alpha^*(\Gamma_h^*)$, and so $\bar{D}_3' = \overline{cl}(D_3') \in \bar{M} = \mathbb{Z}D_1' + \mathbb{Z}D_2'$ because $\bar{M}$ is a primitive submodule of $\mathrm{NS}(J_C, \theta_C)$. Now $c'\bar{D}_3' = \bar{D}_3 = -n_2 kd\bar{D}_1' + n_1\bar{D}_2'$, so $c' | \gcd(n_2 kd, n_1, c) = \gcd(n_1, n_2, c) = 1$, the latter because $n_1 n_2 - c^2 \deg(h) = 1$ (since $D \in \mathcal{P}(E_1 \times E_2)$). Thus, $c' = \pm 1$ and $\deg(h) = d$, so C has type d.

7 The existence theorem

We now show that $H'(q)$ is non-empty, whenever q is a form of type d which is not in the principal class, i.e., one which satisfies $q \not\sim 1_{-16d}$. This follows from the following more precise assertion:

Theorem 31 *Suppose that q is a binary quadratic form of type d. Let E_1 be any elliptic curve with $\mathrm{End}(E_1) = \mathbb{Z}$, and let $E_2 = E_1/H$, where $H \leq E_1$ is any cyclic subgroup (scheme) of degree d. Then there exists a principal polarization θ on $A = E_1 \times E_2$ such that $q_{(A,\theta)} \approx q$. Moreover, if $q \not\sim 1_{-16d}$, then there exists a curve C with $J_C \simeq E_1 \times E_2$ such that $q_C \approx q$; in particular, $\langle C \rangle \in H'(q)$.*

To prove this, we shall use the following refinement of Corollary 25.

Proposition 32 *Suppose that $\mathrm{Hom}(E_1, E_2) = \mathbb{Z}h$ where $d := \deg(h) \geq 1$. Then the map $s \mapsto D_{s,h}$ defines a bijection between the set $P(d)$ and the set $\mathcal{P}(A)$ of principal polarizations on $A := E_1 \times E_2$. Furthermore, $\theta \in \mathcal{P}(A)$ is represented by a smooth curve C of genus 2 if and only if $q_{(A,\theta)}$ is not in the principal class.*

Proof. The first assertion follows immediately from Corollary 25 since here every $D \in \mathrm{NS}(E_1 \times E_2)$ has the (unique) form $\mathbf{D}(a, b, ch)$, and since $\deg(ch) = c^2 \deg(h)$. The second assertion follows from Proposition 6 because here $q_{(A,\theta)}$ is a binary quadratic form, and such a form represents 1 if and only if it is in the principal class.

Proof of Theorem 31. By Theorem 13 there exists $s \in P(d)$ such that $q \sim q_s$. Put $\theta = D_{s,h} \in \mathrm{NS}(E_1 \times E_2)$, where $h : E_1 \to E_2 = E_1/H_1$ denotes the quotient map. (Note that h is cyclic, and so $\mathrm{Hom}(E_1, E_2) = \mathbb{Z}h$.) By Proposition 32 we see that $\theta \in \mathcal{P}(A)$, and Proposition 29 shows that $q_{(A,\theta)} \approx q_s \sim q$. (Here $\bar{M} = \mathrm{NS}(A, \theta)$ because $\bar{M}$ is primitive in $\mathrm{NS}(A, \theta)$ and $\mathrm{rk}(\mathrm{NS}(A, \theta)) = 2$.) Moreover, if $q \not\sim 1_{-16d}$, then Proposition 32 shows that $(A, \theta) \simeq (J_C, \theta_C)$, for some curve C of genus 2.

We now consider some applications of the Existence Theorem 31. The first is the following useful fact.

Corollary 33 *If q_i is a quadratic form of type d_i, for $i = 1, 2$, then $H(q_1) = H(q_2)$ if and only if $q_1 \approx q_2$. Moreover, if $q_1 \not\sim 1_{-16d_1}$, then also $H'(q_1) = H'(q_2) \Leftrightarrow q_1 \approx q_2$.*

Proof. If $q_1 \approx q_2$, then $H(q_1) = H(q_2)$ and $H'(q_1) = H'(q_2)$ by definition. Conversely, suppose that $H'(q_1) = H'(q_2)$. If $q \not\sim 1_{-16}$, then by Theorem 31 there exists $\langle C\rangle \in H(q_1)$ such that $q_C \approx q_1$. Since $\langle C\rangle \in H(q_2)$, this means that q_C primitively represents q_2, and so $q_2 \approx q_C$ because both are binary forms. Thus $q_1 \approx q_2$, as asserted. By a similar argument one shows that $H(q_1) = H(q_2) \Rightarrow q_1 \approx q_2$.

Remark 34 The above proof also shows that if $q_1 \not\approx q_2$, then $H(q_1) \cap H(q_2)$ consists only of *CM-points*, i.e. of points $\langle A, \theta\rangle$ such that $A \simeq E_1 \times E_2$, where $E_1 \sim E_2$ are elliptic curves which have complex multiplication (or are supersingular).

Corollary 35 *If $d \geq 1$, then $T(d) = \emptyset \;\Leftrightarrow\; \bar{Q}_d^* = \emptyset$, and hence*

$$\begin{aligned} (30)\quad T(d) = \emptyset \;&\Leftrightarrow\; \bar{h}(-16d) = 1 \text{ and } d \not\equiv 3\,(4) \;\Leftrightarrow\; \bar{h}(-16d) = 1 \text{ and } d \neq 3, 7, 15 \\ &\Leftrightarrow\; d = 1, \quad \text{or: } \bar{h}(-4d) = 1 \text{ and } d \equiv 2, 4, 6 \,(\mathrm{mod}\, 8), \end{aligned}$$

where, as before, $\bar{h}(D) = \frac{h(D)}{g(D)}$ denotes the number of forms in the principal genus.

Proof. The first assertion follows directly from Theorems 12 and 31. To prove the first equivalence of (30), recall that $\bar{Q}_d^* = \bar{Q}(d) \setminus \{1_{-16d}\}$, so $\bar{Q}_d^* = \emptyset \Leftrightarrow \bar{Q}(d) = \{1_{-16d}\} \Leftrightarrow Q(d)/\mathrm{SL}_2(\mathbb{Z}) = \{1_{-16d}\}$, the latter by Remark 11. Thus, $T(d) = \emptyset \Leftrightarrow t(d) = |Q(d)/\mathrm{SL}_2(\mathbb{Z})| = 1$. Now by (8) we see that $t(d) = 1 \Leftrightarrow \bar{h}(-16d) = 1$ and $d \not\equiv 3 \,(\mathrm{mod}\, 4)$, and so the first equivalence of (30) follows.

The second equivalence is equivalent to the assertion that for $d \equiv 3(4)$ we have $\bar{h}(-16d) > 1$ when $d \neq 3, 7, 15$, and this was proved by Grube[13], §7; cf. [24], Corollary 8. (To apply this result, we also need the fact that $\bar{h}(-16d) = \bar{h}(-4d)$, when $d \equiv 3\,(4)$; cf. (31) below.)

To prove the last equivalence, note first that (18) implies that $g(-16d) = 2g(-4d)$, if $d \not\equiv 0, 1, 5$ (8) and that $g(-16d) = g(-4d)$ otherwise. Thus, since $h(-16d) = 2h(-4d)$, if $d > 1$ (cf. (14)), we see that for $d > 1$ we have

$$(31)\qquad \bar{h}(-16d) \;=\; \begin{cases} 2\bar{h}(-4d), & \text{if } d \equiv 1 \,(\mathrm{mod}\, 4) \text{ or } d \equiv 0 \,(\mathrm{mod}\, 8), \\ \bar{h}(-4d), & \text{otherwise.} \end{cases}$$

From this we see in particular that $h(-16) \geq 2$ if $d \equiv 1\,(4)$, $d \neq 1$, or if $d \equiv 0\,(8)$, and so the last equivalence follows since the case $d \equiv 3\,(4)$ has already been excluded.

Remark 36 As was already mentioned in the introduction, a number $d \geq 1$ is called *idoneal* (or *convenient* or *suitable*) if $\bar{h}(-4d) = 1$. Such numbers (but under a different definition) were introduced by Euler in 1778; cf. Weil[42], pp. 188, 223ff and [24]. The fact that an idoneal number (in the sense of Euler) agrees with the above definition was first proved by Grube[13]; cf. Cox[4], p. 61, for a simpler proof.

Proof of Theorem 5. The first assertion follows directly from (30). From Euler and/or Gauss[12], Art. 303, we know that if $d = 1$ or if $d \not\equiv 0\,(8)$ is even and $d < 10^5$, then $\bar{h}(-4d) = 1$ if and only if d is one of the values of (1); cf. also Dickson[6], p. 89. In particular, we see that if the Euler/Gauss Conjecture is true (i.e. if $\bar{h}(-4d) > 1$ for all $d > 1848$), then d is of the form (1). Note also that the fact that (GRH) implies Gauss's Conjecture was proved by Weinberger[43].

Now assume that $\bar{h}(-4d^*) = 1$ where $d^* > 462$ and $d \equiv 0\,(2)$ but $d^* \not\equiv 0\,(8)$ (so d^* is a counterexample to the Euler/Gauss Conjecture). Then in fact $d^* \not\equiv 0\,(4)$ because we have

$$\bar{h}(-4d^*) > 1 \quad \text{if } d^* \equiv 4\,(\mathrm{mod}\ 8),\ \text{and } d^* > 60. \tag{32}$$

Indeed, suppose $d^* = 4d$, where d is odd. If $d \equiv 1\,(4)$, then $\bar{h}(-4d^*) = \bar{h}(-16d) = 2h(-4d) \geq 2$ by (31), and if $d \equiv 3\,(4)$, then we have $h(-4d^*) = h(-16d) = h(-4d) > 1$ when $d > 15$, the latter by Hall's Theorem I. This proves (32).

We are thus left with the case that $d^* \equiv 2\,(4)$. Since $\bar{h}(-4d^*) = 1$, then by a theorem of Grube[13], p. 515 (cf. also Hall[14], Theorem II), d^* cannot have any odd square factor (since $d^* > 72$) and so $-4d^*$ is a *fundamental* discriminant. Now by Weinberger[43], Theorem 1, there is at most one fundamental discriminant $D < -10^5$ with $\bar{h}(D) = 1$, so there is at most one of the form $D = -4d^*$ satisfying in addition $d \equiv 2\,(4)$. Note also that $4d^* > 10^{12}$ (this was established by explicit computations and was used in Weinberger[43]'s proof), and so $d^* > \frac{5}{2} \times 10^{11} > 10^{11}$. This proves Theorem 5.

Remark 37 It is perhaps useful to point out that Weinberger's "one more" theorem applies only to fundamental discriminants, and so his theorem proves that there is at most one *squarefree* idoneal number $d > 1848$. It is not true that it follows from Weinberger's result that "Euler's list is complete except possibly for one exception", an assertion that is often found in the literature; cf. e.g. [9]. Indeed, if the squarefree exception satisfies $d \equiv 2\,(4)$, then by (31) we see that $4d$ is also an exceptional idoneal number, and hence there are then two exceptional idoneal numbers; cf. also [24].

For later applications it is useful to refine the above existence theorem by determining the number of isomorphism classes of curves C on $E_1 \times E_2$ such that $q_C \approx q$.

Theorem 38 *Let $A = E_1 \times E_2$, where $\mathrm{Hom}(E_1, E_2) = \mathbb{Z}h$, and let $q \not\sim 1_{-16d}$ be a quadratic form of type $d := \deg(h)$. Then the number $N_A(q)$ of isomorphism classes of smooth genus 2 curves C on A with $q_C \approx q$ is given by:*

$$N_A(q) = \begin{cases} 2^{\omega(d)-2} & \text{if } q \in \bar{Q}^2_{-16d}[2] \setminus \{q_d\} \text{ or if } \frac{1}{4}q \in \bar{Q}^2_{-d}[2] \setminus \{1_{-d}\}, \\ 2^{\omega(d)-1} & \text{otherwise,} \end{cases} \tag{33}$$

where, as in (14), $q_d = 4x^2 + dy^2$, *if* $d \equiv 1(2)$, *and* $q_d = 4x^2 + 4xy + (d+1)y^2$, *if* $d \equiv 0(2)$.

Remark 39 Note that q_d is not necessarily in $\bar{Q}^2_{-16d}[2]$. In fact, this is the case if and only if $d \equiv 0, 1, 5\,(8)$, as can be verified by checking the generic characters of q_d.

As we shall see presently, the above theorem follows easily from the following fact which is interesting in itself.

Proposition 40 *Let $A = E_1 \times E_2$, where $\mathrm{Hom}(E_1, E_2) = \mathbb{Z}h$, and let $d = \deg(h)$. If C is a smooth genus 2 curve on A, then $C \equiv D_{s,h}$, for a unique $s \in P(d)$ with $q_s \approx q_C$, and the rule $C \mapsto f_d(s)$ induces an isomorphism*

$$\bar{f}'_A : \mathcal{C}_2(A)/\simeq \quad \tilde{\to} \quad Q^{(2)}_{-4d}/\mathrm{GL}_2(\mathbb{Z}) \ \setminus \ \mathrm{Ker}(\pi'_d)$$

between the set of isomorphism classes of smooth genus 2 curves on A and the above set of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of binary quadratic forms of discriminant $-4d$.

Before proving this, let us see how Theorem 38 follows from it.

Proof of Theorem 38. Suppose first that q is primitive. If $C \in \mathcal{C}_2(A)$ is a curve with $q_C \approx q$, and if $C \equiv D_{s,h}$ with $s \in P(d)$ (cf. Proposition 40), then by Corollary 19 and Lemma 16 we have that $\pi'_d(f_d(s)) \sim q$. We thus obtain from Proposition 40 that

$$N_A(q) = \#({\pi'_d}^{-1}(q) \ \cup \ {\pi'_d}^{-1}(q^{-1}))/\mathrm{GL}_2(\mathbb{Z}).$$

Now if $q \not\sim q^{-1}$, then the sets ${\pi'_d}^{-1}(q)$ and ${\pi'_d}^{-1}(q^{-1})$ are interchanged under the $\mathrm{GL}_2(\mathbb{Z})$-action, and so $N_A(q) = \#({\pi'_d}^{-1}(q)) = |\mathrm{Ker}(\pi'_d)| = 2^{\omega(d)-1}$ by Corollary 20. (Note that $d > 1$ because $q \not\sim 1_{-16d}$.) This proves (33) in this case.

Next, suppose $q \sim q^{-1}$, i.e. $q \in \bar{Q}^2_{-16d}[2]$. Now if $q \in \mathrm{Ker}(\pi_{-4d,2})$, i.e. if $q \sim q_d$ by (14), then ${\pi'_d}^{-1}(q) \subset \bar{Q}_{-4d}[2]$ (cf. Proposition 18), and so $N_A(q) = \#({\pi'_d}^{-1}(q)) = |\mathrm{Ker}(\pi'_d)| = 2^{\omega(d)-1}$ again. On the other hand, if $q \in \bar{Q}^2_{-16d}[2] \setminus \{q_d\}$, then ${\pi'_d}^{-1}(q) \cap \bar{Q}_{-4d}[2] = \emptyset$, and so the $\mathrm{GL}_2(\mathbb{Z})$-action has no fixed points on ${\pi'_d}^{-1}(q)$, and hence $N_A(q) = \frac{1}{2}\#({\pi'_d}^{-1}(q)) = \frac{1}{2}|\mathrm{Ker}(\pi'_d)| = 2^{\omega(d)-2}$ by Corollary 20.

Finally, suppose that q is not primitive. Then $q \approx 4q_1$ with $q_1 \in \bar{Q}^2_{-d}$ and $d \equiv 3\,(\mathrm{mod}\ 4)$. In this case we have by the same reasoning as above that

$$N_A(q) = \#({S_d}^{-1}(q_1) \ \cup \ {S_d}^{-1}(q_1^{-1}))/\mathrm{GL}_2(\mathbb{Z}),$$

where $S_d : \bar{Q}_{-d} \to \bar{Q}^2_{-d}$ is the squaring map. Since $|\mathrm{Ker}(S_d)| = g(-d) = 2^{\omega(d)-1}$ (cf. (18)), a similar analysis as above yields (33).

We now turn to the proof of Proposition 40. For this, we require the following information about the functorial behaviour of the divisor $D_{s,f}$.

Proposition 41 *If* $g = \left(\begin{smallmatrix} a & b \\ cd & e \end{smallmatrix}\right) \in \Gamma_0^{\pm}(d) := \Gamma_0(d) \dot\cup \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\Gamma_0(d)$, *and if* $f \in \mathrm{Hom}(E_1, E_2)$ *has degree* $d \geq 1$, *then*

$$\alpha_{g,f} = \begin{pmatrix} [a]_{E_1} & bf^t \\ cf & [e]_{E_2} \end{pmatrix} \in \mathrm{Aut}(E_1 \times E_2),$$

and we have

$$\alpha_{g,f}^*(D_{s,f}) := D_{sg,f}, \quad \textit{for all } s \in P(d), \tag{34}$$

where $sg \in P(d)$ *is defined by the rule* $f_d(sg) = f_d(s)g$.

Proof. We first observe that if $[g]_{E_2} \in \mathrm{End}(E_2 \times E_2)$ denotes the endomorphism induced by the matrix $g \in M_2(\mathbb{Z})$, then in $\mathrm{End}^0(E_1 \times E_2)$ we have the relation

$$\alpha_{g,f} = (f^t \times 1_{E_2})^{-1} \circ [g]_{E_2} \circ (f^t \times 1_{E_2}), \tag{35}$$

and so $\alpha_{g,f} \in \mathrm{Aut}(A)$ as $\deg(\alpha_{g,f}) = \deg([g]_{E_2}) = (\det(g))^2 = 1$; cf. Corollary 65.

Although we could deduce (34) directly from the pullback formula (76) by a tedious calculation, it is easier to apply formula (66) to the map $\Psi_f := \Phi_{\lambda_1 \otimes \lambda_2, f^t \times 1} : \mathrm{NS}(A) \to \mathrm{End}(E_2 \times E_2)$ which is introduced in Proposition 58 of the appendix. In our situation (66) becomes

$$\Psi_f(\alpha_{g,f}^* D) = [g^t]_{E_2} \Psi_f(D) [g]_{E_2}, \quad \text{for all } D \in \mathrm{NS}(A), \tag{36}$$

because by (35) and (69) we have

$$c_{f^t \times 1}(\alpha_{g,f}) = [g]_{E_2} \quad \text{and} \quad r_{\lambda_2 \otimes \lambda_2}(c_h(\alpha_{g,f})) = [g^t]_{E_2}. \tag{37}$$

Next we observe that by (23) we have

$$\Psi_f(\mathbf{D}(a,b,cf)) = \begin{pmatrix} f & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} [a] & cf^t \\ cf & [b] \end{pmatrix} \begin{pmatrix} f^t & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} [ad] & [cd] \\ [cd] & [b] \end{pmatrix}, \ \forall a,b,c \in \mathbb{Z}, \tag{38}$$

and so $\Psi_f(D_{s,f}) = [M(f_d(s))]_{E_2}$, where (as before) $M(q) = \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right) \in M_2(\mathbb{Z})$ denotes the matrix associated to the quadratic form $q = [a, 2b, c]$.

Since the action of g on quadratic forms is given by the formula $M(f_d(sg)) := M(f_d(s)g) = g^t M(f_d(s)) g$, we thus obtain from (36) that

$$\Psi_f(\alpha_{g,f}^* D_{s,f}) = [g^t]_{E_2} \Psi_f(D_{s,f}) [g]_{E_2} = [g^t M(f_d(s)) g]_{E_2} = [M(f_d(sg))]_{E_2} = \Psi_f(D_{sg,f}),$$

and so (34) follows because Ψ_f is injective (cf. Corollary 60).

Corollary 42 *If* $A = E_1 \times E_2$ *and* $\mathrm{Hom}(E_1, E_2) = \mathbb{Z}h$, *where* $\deg(h) = d \geq 1$, *then the map* $g \mapsto \alpha_{g,h}$ *defines a group isomorphism* $\Gamma_0^{\pm}(d) \xrightarrow{\sim} \mathrm{Aut}(A)$. *Moreover, the rule* $D_{s,f} \mapsto f_d(s)$ *defines a bijection* $f_A : \mathcal{P}(A) \xrightarrow{\sim} Q_{-4d}^{(2)}(d)$ *which induces bijections*

$$\bar f_A : \mathcal{P}(A)/\mathrm{Aut}(A) \xrightarrow{\sim} Q_{-4d}^{(2)}(d)/\Gamma_0^{\pm}(d) \xrightarrow{\sim} Q_{-4d}^{(2)}/\mathrm{GL}_2(\mathbb{Z}). \tag{39}$$

Proof. By Proposition 41 we know that $g \mapsto \alpha_{g,h}$ defines an (injective) map $\Gamma_0^{\pm}(d) \to \mathrm{Aut}(A)$. Now since $\mathrm{Hom}(E_1, E_2) = \mathbb{Z}h$ and hence $\mathrm{Hom}(E_2, E_1) = \mathbb{Z}h^t$, we see that every $\alpha \in \mathrm{Aut}(A)$ has the form $\alpha = \left(\begin{smallmatrix} a & bh^t \\ ch & e \end{smallmatrix}\right)$, for some $a, b, c, e \in \mathbb{Z}$. But since $1 = \deg(\alpha) = (ae - bcd)^2$ by (75) (cf. proof of Proposition 41), we see that $g := \left(\begin{smallmatrix} a & b \\ cd & e \end{smallmatrix}\right) \in \Gamma_0^{\pm}(d)$ and so $\alpha = \alpha_{g,h}$. Thus, the map $g \mapsto \alpha_{g,h}$ is bijective. Moreover, since $c_{h^t \times 1}$ is a ring homomorphism, it follows from (37) that this bijection is an isomorphism of groups.

By combining Proposition 32 with Lemma 16 we see that the map $D_{s,h} \mapsto s \mapsto f_d(s)$ defines a bijection $f_A : \mathcal{P}(A) \xrightarrow{\sim} Q_{-4d}^{(2)}(d)$. By (34) this is $\Gamma_0^{\pm}(d)$-equivariant, and so the first bijection of (39) follows. The second follows from Lemma 21.

Proof of Proposition 40. If $C \in \mathcal{C}_2(A)$ is a smooth curve of genus 2 on A, then $cl(C)$ is a principal polarization on A and $(A, cl(C)) \simeq (J_C, \theta_C)$; cf. Weil[41] or [22]. Thus, the first assertion follows from the bijection $f_d^{-1} \circ f_A : \mathcal{P}(A) \to Q_{-4d}^{(2)}(d) \to P(d)$ of Corollary 42 and Lemma 16.

Moreover, the rule $C \mapsto cl(C)$ defines a map $\mathcal{C}_2(A) \to \mathcal{P}(A)$ which, by Torelli's Theorem, induces an injection $\bar{c}_A : \mathcal{C}_2(A)/\!\simeq \ \hookrightarrow P(A)/\mathrm{Aut}(A)$, and so by (39) we have an injection $\bar{f}'_A = \bar{f}_A \circ \bar{c}_A : \mathcal{C}_2(A)/\!\simeq \ \hookrightarrow Q_{-4d}^{(2)}/\mathrm{GL}_2(\mathbb{Z})$. Now by (39) and Proposition 6 we see that $q \approx f_d(s)$ is in $\mathrm{Im}(\bar{f}'_A) \Leftrightarrow q_s \not\sim 1_{-16d} \Leftrightarrow q \notin \mathrm{Ker}(\pi'_d)$, the latter by Corollary 19. This proves that $\bar{f}'_A$ yields the given bijection. Note that since $\mathrm{Ker}(\pi'_d) \subset \bar{Q}_{-4d}[2]$, its SL_2 and GL_2-equivalence classes are the same.

Corollary 43 *Let $A = E_1 \times E_2$, where $\mathrm{Hom}(E_1, E_2) = \mathbb{Z}h$ and $d = \deg(h) \geq 1$. Then the number N_A of isomorphism classes of smooth genus 2 curves on A is*

$$N_A = \#(Q_{-4d}^{(2)}/\mathrm{GL}_2(\mathbb{Z})) - 2^{\omega(d)-1} = \begin{cases} \frac{1}{2}h(-4d) & \text{if } d \equiv 0, 1, 5 \pmod 8 \\ \frac{1}{2}(h(-4d) - 2^{\omega(d)-1}) & \text{if } d \equiv 2, 4, 6 \pmod 8 \\ \frac{1}{2}(h(-4d) + h(-d)) & \text{if } d \equiv 3, 7 \pmod 8 \end{cases},$$

except when $d = 1$; in that case $N_A = 0$.

Proof. By Corollary 42 the total number of isomorphism classes of principal polarizations on A is $\#(Q_{-4d}^{(2)}/\mathrm{GL}_2(\mathbb{Z}))$. By Proposition 40 we know that $f_d(s) \in Q_{-4d}^{(2)}$ corresponds to a smooth curve if and only if $f_d(s) \notin \mathrm{Ker}(\pi'_d)$, and so the first formula for N_A follows from (16). The second formula follows from this and (18) because $\#(Q_D^{(1)}/\mathrm{GL}_2(\mathbb{Z})) = \frac{1}{2}(h(D) + g(D))$.

Remark 44 The number N_A was also determined by Hayashida [15], §7-8, but his formula for N_A is much more complicated than the one above since he gives the result in terms of the class number h_K of the associated imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$. However, by using the well-known relation between $h(-16d)$ and h_K (cf. Lang[28], p. 95), a somewhat tedious calculation shows that the two formulae give the same result.

8 The irreducibility of $H(q)$

The next task is to show that the generalized Humbert variety $H(q)$ is a closed and irreducible subset of A_2 when q is quadratic form of type d. This will be done by exhibiting $H(q)$ as the image of the modular curve $X_0(d)$ by a suitable morphism μ_s.

To define this morphism, recall that $X_0(d)$ classifies *cyclic* isogenies of degree d of elliptic curves, i.e. $X_0(d)(K)$ can be identified with the set of isomorphism classes $\langle f : E \to E' \rangle$, where f is a cyclic isogeny of degree d; cf. [5], p. 283, or [26], p. 100.

Proposition 45 *For $s \in P(d)$, the rule $\langle f : E \to E' \rangle \mapsto \langle E \times E', D_{s,f} \rangle$ defines a* proper *morphism*

$$\mu_s : X_0(d) \quad \to \quad A_2$$

with image $\mu_s(X_0(d)) = H(q_s)$, where q_s is the quadratic form defined by (5).

Proof. Recall from Corollary 25 that $D_{s,f} \in \mathcal{P}(E \times E')$, so $\mu_s(f) \in A_2(K)$, i.e. $\mu_s(f)$ is a principally polarized abelian variety. Since this formation is compatible with isomorphisms, we thus see that this rule defines a map $\mu_s : X_0(d)(K) \to A_2(K)$.

To show that μ_s comes from a morphism of varieties, we shall use the fact that both $X_0(d)$ and A_2 are the coarse moduli spaces of functors $\mathcal{X}_0(d)$ and $\mathcal{A}_2 = \mathcal{A}_{2,1,1}$ on $\underline{Sch}_{/K}$, respectively. It is thus enough to construct a morphism of functors $\tilde{\mu}_s = \{\tilde{\mu}_{s,S}\}_S : \mathcal{X}_0(d) \to \mathcal{A}_2$ which extends μ_s (i.e. $\tilde{\mu}_{s,S} = \mu_s$ for $S = \mathrm{Spec}(K)$).

To construct $\tilde{\mu}_s$, we can use almost the same definition as for μ_s. Indeed, given a K-scheme S, then $\mathcal{X}_0(d)(S)$ consists of isomorphism classes $\langle f : E \to E' \rangle$ in which $f : E \to E'$ is an isogeny of elliptic curves $/S$ which is cyclic in the sense of [26], p. 100. Moreover, $\mathcal{A}_2(S)$ consists of isomorphism classes $\langle A, \lambda \rangle$ of principally polarized abelian schemes A/S of dimension 2; cf. [36], p. 129. We now define

$$\tilde{\mu}_{s,S}(\langle f : E \to E' \rangle) = \langle E \times_S E', \lambda_{s,f} \rangle,$$

where $\lambda_{s,f} : A := E \times_S E' \xrightarrow{\sim} \hat{A}$ is the principal polarization defined in Lemma 46 below.

It is clear that this definition is compatible with isomorphisms, and so we obtain a map $\tilde{\mu}_{s,S} : \mathcal{X}_0(d) \to \mathcal{A}_2(S)$. Note that for $S = \mathrm{Spec}(K)$ we have $\lambda_{s,f} = \phi_{D_{s,f}}$ (cf. proof of Lemma 46 below) and so $\tilde{\mu}_{s,S} = \mu_s$ agrees with the map μ_s as defined above. (Here we use the fact that we can identify $D \in P(A)$ with the associated isomorphism $\phi_D : A \xrightarrow{\sim} \hat{A}$.) Moreover, since this construction is compatible with base change, the collection $\tilde{\mu}_s = \{\tilde{\mu}_{s,S}\}_S$ defines a morphism of functors, which therefore induces a morphism $\mu_s : X_0(d) \to A_2$ between the coarse moduli schemes.

By Proposition 29 we know that $\mu_s(X_0(d)) \subset H(q_s)$. On the other hand, the proof of Theorem 12 in §6 shows that if $\langle A, \theta \rangle \in H(q_s)$, then $(A, \theta) \simeq (E \times E', D_{s,f})$ for some cyclic isogeny $f : E \to E'$ of degree d, and so $\langle A, \theta \rangle = \mu_s(\langle f \rangle)$. Thus $\mu_s(X_0(d)) = H(q_s)$, as claimed.

It remains to show that μ_s is proper. Since $X_0(d)$ and A_2 are of finite type over K, it is enough to check that the functor $\tilde{\mu}_s$ satisfies the valuative criterion of properness. Thus, let $S = \mathrm{Spec}(R)$ be a discrete valuation ring with quotient field $F \supset K$ and let $y = \langle A, \lambda \rangle \in \mathcal{A}_2(S)$ be such that there exists $x_F = \langle E_1 \xrightarrow{h} E_2 \rangle \in \mathcal{X}_0(d)(F)$ with $\tilde{\mu}_{s,F}(x_F) = \langle A_F, \lambda_F \rangle$, where $A_F = A \otimes F$ and $\lambda_F = \lambda \otimes F$. We want to show that x_F extends to $x \in \mathcal{X}_0(d)(S)$ and that $\tilde{\mu}_{s,S}(x) = y$. For this we observe that since $A_F \simeq E_1 \times E_2$, and A_F has good reduction over R by hypothesis, it follows that the same is true for E_i, and so there exist elliptic curves $\tilde{E}_i/R$ with $\tilde{E}_i \otimes F = E_i$. By the Néron property we know that $A \simeq \tilde{E}_1 \times_S \tilde{E}_2$ and that h extends to $\tilde{h} : \tilde{E}_1 \to \tilde{E}_2$. From [26], p. 162, it follows that $\tilde{h}$ is again cyclic, so $x = \langle \tilde{h} \rangle \in \mathcal{X}_0(d)(S)$. We then have $\tilde{\mu}_s(x) = y$ because $\lambda_{s,\tilde{h}}$ and λ agree on the generic fibre, and so $\tilde{\mu}_s$ is proper.

Lemma 46 *Let $f : E_1 \to E_2$ be an isogeny of degree d between two elliptic curves over a scheme S, and let $s = (n_1, n_2, k) \in P(d)$. If $\lambda_i : E_i \xrightarrow{\sim} \hat{E}_i$ denotes the canonical polarization of E_i, and $\lambda_1 \otimes \lambda_2$ the product polarization, then*

$$\lambda_{s,f} = \lambda_1 \otimes \lambda_2 \circ \begin{pmatrix} [n_1]_{E_1} & kf^t \\ kf & [n_2]_{E_2} \end{pmatrix}$$

is a principal polarization on $E_1 \times_S E_2$.

Proof. First note that if $S = \mathrm{Spec}(K)$, then $\lambda_{s,f} = \phi_{D_{s,f}}$ by (23). Thus, since the formation of $\lambda_{s,f}$ clearly commutes with base-change, it follows that $\lambda_{s,f}$ is a principal polarization (in the sense of [36], p. 120) once we have shown that $\lambda_{s,f}$ is an isomorphism. Now since $f^t f = [d]_{E_1}$ and $f f^t = [d]_{E_2}$ (cf. [26], p. 81), it follows from (4) that

$$\begin{pmatrix} [n_1]_{E_1} & kf^t \\ kf & [n_2]_{E_2} \end{pmatrix} \begin{pmatrix} [n_2]_{E_1} & -kf^t \\ -kf & [n_1]_{E_2} \end{pmatrix} = \begin{pmatrix} 1_{E_1} & 0 \\ 0 & 1_{E_2} \end{pmatrix}.$$

Thus, since the product polarization $\lambda_1 \otimes \lambda_2$ (which is defined as in §11) is an isomorphism, we see that $\lambda_{s,f}$ is an isomorphism.

Corollary 47 *If q is a quadratic form of type d, then $H(q)$ is a closed subvariety of A_2 of dimension 1. Moreover, if $\mathrm{char}(K) \nmid d$, then $H(q)$ is an irreducible curve. Thus, $H'(d) = H(d) \cap M_2$ is a closed subvariety of M_2, and $H'(d)$ is open in $H(d)$.*

Proof. By Theorem 13 and 45 we have $H(q) = \mu_s(X_0(d))$, for some $s \in P(d)$, and so $H(q)$ is a closed subset since μ_s is proper. Moreover, $\dim H(q) = \dim X_0(d) = 1$ because $H(q)$ is infinite by Theorem 31. Finally, if $\mathrm{char}(K) \nmid d$, then $X_0(d)$ is irreducible (by Igusa), and hence so is its image $H(q)$. The last assertion follows from the first together with Remark 7.

Proof of Theorem 3. By Corollary 47 and Theorem 12 we see that the $H'(q)$ for $q \in \bar{Q}_d^*$ are the irreducible components of $T(d)$. Since $H'(q_1) \neq H'(q_2)$ if $q_1 \not\approx q_2$ (cf. Corollary 33), we see that the number of such components is precisely $\#\bar{Q}_d^*$.

9 The action of Atkin-Lehner involutions

As is well-known, the curve $X_0(d)$ comes equipped with a group of automorphisms called *Atkin-Lehner involutions*. In order to understand the birational structure of $H(q)$, it is important to determine how these involutions act on the maps μ_s which were constructed in the previous section. Before stating the result, we first observe:

Proposition 48 *Let $s, s' \in P(d)$. Then $\mu_s = \mu_{s'}$ if and only if $f_d(s) \approx f_d(s')$.*

Proof. Suppose first that $f_d(s) = f_d(s')g$ with $g \in \mathrm{GL}_2(\mathbb{Z})$. Then by the proof of Lemma 21 we know that $g \in \Gamma_0^{\pm}(d)$, and so $f_d(s) = f_d(s'g)$ in the notation of (34). Thus, if $x = \langle f : E \to E' \rangle \in X_0(d)(K)$, then $\alpha_{g,f}$ defines by Proposition 41 an isomorphism $(E \times E', D_{s',f}) \simeq (E \times E', D_{s,f})$, and so $\mu_{s'}(x) = \mu_s(x)$. This proves that $\mu_s = \mu_{s'}$ provided that $X_0(d)$ is reduced. In the general case (i.e. when $\mathrm{char}(K)|d$), essentially the same argument (by replacing $D_{s,f}$ by $\lambda_{s,f}$ as in the proof of Proposition 45) shows that we actually have an equality $\tilde{\mu}_{s'} = \tilde{\mu}_s$ of morphisms of functors, and so the induced morphisms μ_s and $\mu_{s'}$ on the coarse moduli spaces are equal.

Conversely, suppose $\mu_s = \mu_{s'}$. Then in particular $\mu_s(x) = \mu_{s'}(x)$ for any point $x = \langle E \xrightarrow{f} E' \rangle \in X_0(d)(K)$ which we can take to be a non-CM point, i.e. we have $\mathrm{Hom}(E, E') = \mathbb{Z}f$. Then the equality $\mu_s(x) = \mu_{s'}(x)$ means that there is an $\alpha \in \mathrm{Aut}(E \times E')$ such that $\alpha^* D_{s,f} = D_{s',f}$. Now by Corollary 42 we know that $\alpha = \alpha_{g,f}$ for some $g \in \Gamma_0^{\pm}(d)$ and that $f_d(s)g = f_d(s')$. Thus, $f_d(s) \approx f_d(s')$, as asserted.

We now come to the action on the Atkin-Lehner involutions on the maps μ_s. For this, recall that each Atkin-Lehner involution α on $X_0(d)$ is uniquely defined by a divisor $d_1||d$ of d, i.e. by a divisor $d_1|d$ with the property that $\gcd(d_1, d/d_1) = 1$. We can thus write $\alpha = \alpha_{d_1}$; this will be explained in more detail below.

Theorem 49 *For each $d_1||d$, the Atkin-Lehner involution α_{d_1} permutes the μ_s's. More precisely, if $s \in P(d)$, then*

$$\mu_s \circ \alpha_{d_1} = \mu_{s'}, \quad \text{where } f_d(s') \approx f_d(s) \circ a_{d_1}. \tag{40}$$

Here $a_{d_1} = [d_1, 0, d/d_1]$ if $s \in P(d)^{odd}$ and $a_{d_1} = [d_1, d_1, (d_1^2+d)/(4d_1)]$, if $s \in P(d)^{even}$. Moreover, the orbits of the group of Atkin-Lehner automorphisms on $\{\mu_s\}$ are in one-to-one correspondence with the images $H(q_s) = \mathrm{Im}(\mu_s)$; i.e. we have

$$\mathrm{Im}(\mu_{s_1}) = \mathrm{Im}(\mu_{s_2}) \quad \Leftrightarrow \quad \exists d_1||d \text{ such that } \mu_{s_1} = \mu_{s_2} \circ \alpha_{d_1}. \tag{41}$$

In order to prove this theorem, we need some auxiliary results concerning Atkin-Lehner involutions. We begin with their (functorial) definition, i.e. with their action on the functor $\mathcal{X}_0(d)$ which was discussed in the previous section.

Fix $d_1||d$ and put $d_2 = d/d_1$. Let $h : E_1 \to E_2$ be a *cyclic* isogeny of degree d and for $i = 1, 2$, consider the quotient maps

$$h_{i1} = h_{i1}^{(h)} : E_1 \to E_i' := E_1/\mathrm{Ker}(h)[d_i], \quad \text{where } \mathrm{Ker}(h)[d_i] = \mathrm{Ker}(h) \cap E_1[d_i].$$

Note that h_{i1} is a cyclic isogeny of degree $\deg(h_{i1}) = d_i$, for $i = 1, 2$. By the universal property of quotients, there is a unique morphism $h_{i2}' = (h_{i2}')^{(h)} : E_i' \to E_2$ such that

$$h = h_{i2}' \circ h_{i1}, \quad \text{for } i = 1, 2. \tag{42}$$

Note that h_{i2}' is cyclic of degree d/d_i, for $i = 1, 2$. Put $h_{i2} = (h_{i2}')^t : E_2 \to E_i'$; thus, $h_{i2}^t = ((h_{i2}')^t)^t = h_{i2}'$. Finally, put

$$h' = (h')^{(h)} := h_{21} \circ h_{11}^t = (h_{11} \circ h_{21}^t)^t : E_1' \to E_2'.$$

Note that h' is a cyclic isogeny of degree $d = d_1 d_2$ because h_{21} and h_{11}^t are cyclic of degree d_2 and degree d_1, respectively, and because $\gcd(d_1, d_2) = 1$. We observe that

$$h' = h_{21} \circ h_{11}^t = h_{22} \circ h_{12}^t. \tag{43}$$

(Indeed, the first equality is just the definition, whereas the second follows from the fact that $h_{21} h_{11}^t h_{11} = h_{21}[d_1] = [d_1] h_{21} = h_{22} h_{22}^t h_{21} \overset{(42)}{=} h_{22} h_{12}^t h_{11}$ and from the fact that h_{11} is an isogeny.) We now put

$$\alpha_{d_1}(\langle E_1 \xrightarrow{h} E_2 \rangle) = \langle E_1' \xrightarrow{h'} E_2' \rangle.$$

Note that the above construction works for elliptic curves over an arbitrary base scheme, and that it is compatible with base change. Thus, α_{d_1} defines a morphism of functors $\alpha_{d_1} : \mathcal{X}_0(d) \to \mathcal{X}_0(d)$. In fact, α_{d_1} is an automorphism (and even an involution, i.e. $\alpha_{d_1} \circ \alpha_{d_1} = 1_{\mathcal{X}_0(d)}$) because with the above notation we have

$$\alpha_{d_1}(\langle E_1' \xrightarrow{h'} E_2' \rangle) = \langle E_1 \xrightarrow{h} E_2 \rangle.$$

(To see this, note first that by (43) we have $\mathrm{Ker}(h')[d_i] = \mathrm{Ker}(h_{1i}^t)$, and so $h_{i1}^{(h')} = h_{1i}^t : E_i' \to E_i$ and $(h_{i2}')^{(h')} = h_{2i}$. Thus $(h')^{(h')} = (h_{11}^{(h')}(h_{21}')^{(h')})^t = (h_{11}^t h_{21})^t = h_{21}^t h_{11} = h$, and the assertion follows.)

Over $\mathbb{C}$, the Atkin-Lehner involutions on $X_0(d)_{\mathbb{C}} = \Gamma_0(d) \backslash \mathfrak{H}$ can be defined by the Atkin-Lehner matrices of [1]. Although we don't need this here, we do need these matrices in order to construct isomorphisms between $E_1 \times E_2$ and $E_1' \times E_2'$.

Notation. Put $\Gamma_0^{\pm}(d_2)_{d_1} = \{g \in \Gamma_0^{\pm}(d_2) : g \equiv \left(\begin{smallmatrix} 0 & * \\ * & * \end{smallmatrix}\right) \pmod{d_1}\}$. Thus, $g \in \Gamma_0^{\pm}(d_2)_{d_1} \Leftrightarrow$

$$g = \begin{pmatrix} a_{11} d_1 & a_{12} \\ a_{21} d_2 & a_{22} \end{pmatrix} \quad \text{where } a_{ij} \in \mathbb{Z} \text{ and } a_{11} a_{22} d_1 - a_{12} a_{21} d_2 = \pm 1. \tag{44}$$

If $g \in \Gamma_0^{\pm}(d_2)_{d_1}$, then the *associated Atkin-Lehner matrix* is

$$\tilde{g} := \begin{pmatrix} 1 & 0 \\ 0 & d_1 \end{pmatrix} g = \begin{pmatrix} a_{11} d_1 & a_{12} \\ a_{21} d & a_{22} d_1 \end{pmatrix}. \tag{45}$$

Proposition 50 *Let* $\alpha_{d_1}(E_1 \xrightarrow{h} E_2) = (E_1' \xrightarrow{h'} E_2')$ *and let* $g \in \Gamma_0^{\pm}(d_2)_{d_1}$. *Put*

$$\alpha_g := \begin{pmatrix} a_{11}h_{11} & a_{12}h_{12} \\ a_{21}h_{21} & a_{22}h_{22} \end{pmatrix}, \quad \textit{where} \quad g = \begin{pmatrix} a_{11}d_1 & a_{12} \\ a_{21}d_2 & a_{22} \end{pmatrix}$$

and where the $h_{ij} = h_{ij}^{(h)}$ *are as defined above. Then*

$$(h_{12} \times h_{22}) \circ [g]_{E_2} = \alpha_g \circ (h^t \times 1), \tag{46}$$

and so $\alpha_g : E_1 \times E_2 \xrightarrow{\sim} E_1' \times E_2'$ *is an isomorphism. Moreover,*

$$((h')^t \times 1) \circ [\tilde{g}]_{E_2'} = \alpha_g \circ (h^t \times 1) \circ (h_{22}^t \times h_{22}^t). \tag{47}$$

Proof. By (42) we have $h_{i1}h^t = h_{i1}(h_{i2}^t h_{i1})^t = h_{i1}h_{i1}^t h_{i2} = d_i h_{i2}$, and from this (46) follows immediately. Since $\det(g) = \pm 1$, we see that $\deg([g]_{E_2}) = (\pm 1)^2 = 1$; cf. Corollary 65. Thus, since $\deg(h_{12} \times h_{22}) = d_1 d_2 = d = \deg(h^t \times 1)$, it follows from (46) that $\deg(\alpha_g) = 1$, i.e. that α_g is an isomorphism.

To prove (47), note first that (43) shows that $(h_{12} \times h_{22}) \circ (h_{22}^t \times h_{22}^t) = (h')^t \times [d_1]$ (because $\deg(h_{22}) = d/d_2 = d_1$), and so by (46) we obtain $\alpha_g \circ (h^t \times 1) \circ (h_{22}^t \times h_{22}^t) = (h_{12} \times h_{22}) \circ [g]_{E_2} \circ (h_{22}^t \times h_{22}^t) = (h_{12} \times h_{22}) \circ (h_{22}^t \times h_{22}^t) \circ [g]_{E_2'} = ((h')^t \times [d_1]) \circ [g]_{E_2'} = ((h')^t \times 1) \circ [\tilde{g}]_{E_2'}$, which is (47).

In passing, we observe the following interesting fact concerning isomorphisms of product surfaces in the non-CM case; this will be used in the next section.

Proposition 51 *Let* (E_1, E_2) *and* (E_1', E_2') *be two pairs of elliptic curves, and assume that* $\mathrm{Hom}(E_1, E_2) = \mathbb{Z}h$ *and* $\mathrm{Hom}(E_1', E_2') = \mathbb{Z}h'$. *If* $d = \deg(h)$, *then*

$$E_1 \times E_2 \simeq E_1' \times E_2' \Leftrightarrow \exists\, d_1 || d \text{ such that } \langle E_1' \xrightarrow{h'} E_2' \rangle = \alpha_{d_1}(\langle E_1 \xrightarrow{h} E_2 \rangle). \tag{48}$$

Proof. The one direction follows from Proposition 50. Conversely, suppose that there exists an isomorphism $f : E_1 \times E_2 \xrightarrow{\sim} E_1' \times E_2'$. Then $E_i' \sim E_1 \sim E_2$, and so $\mathrm{Hom}(E_i, E_j') = \mathbb{Z}h_{ji}$, for some (cyclic) $h_{ji} \in \mathrm{Hom}(E_i, E_j')$, for all $i, j = 1, 2$. We can thus write $f = (a_{ij}h_{ij})$ with $a_{ij} \in \mathbb{Z}$. Similarly, since $\mathrm{Hom}(E_j', E_i) = \mathbb{Z}h_{ji}^t$, we can write $g := f^{-1} = (b_{ij}h_{ji}^t)$ with $b_{ij} \in \mathbb{Z}$. Since $1_{E_1' \times E_2'} = fg = \left(\begin{smallmatrix} [c_{11}] & * \\ * & [c_{22}] \end{smallmatrix}\right)$, we obtain the relations

$$c_{11} = a_{11}b_{11}d_{11} + a_{12}b_{21}d_{12} = 1 \quad \text{and} \quad c_{22} = a_{21}b_{12}d_{21} + a_{22}b_{22}d_{22} = 1,$$

where $d_{ij} = \deg(h_{ij})$. From these we see that $\gcd(d_{11}, d_{12}) = 1 = \gcd(d_{21}, d_{22})$. Thus, $h_{12}^t h_{11} \in \mathrm{Hom}(E_1, E_2)$ is a composition of isogenies with cyclic kernels of relatively prime order, and hence also has cyclic kernel. This means that $h_{12}^t h_{11}$ is a generator of $\mathrm{Hom}(E_1, E_2)$ and hence $h_{12}^t h_{11} = \pm h$. By replacing h_{11} by $-h_{11}$ if necessary, we

thus have $h = h_{12}^t h_{11}$. Similarly, $h_{22}^t h_{21} = h$, (replacing h_{21} by $-h_{21}$, if necessary). Thus (42) holds with $h'_{i2} = h_{i2}^t$.

Next, using the fact that $gf = 1_{E_1 \times E_2}$, we obtain in a similar way the relations

$$a_{11}b_{11}d_{11} + a_{21}b_{12}d_{21} = 1 \quad \text{and} \quad a_{12}b_{21}d_{12} + a_{22}b_{22}d_{22} = 1,$$

and hence $\gcd(d_{11}, d_{21}) = 1 = \gcd(d_{12}, d_{22})$. Thus, since by (42) we have $d_{12}d_{11} = d_{22}d_{21}$, we see that $d_{11}|d_{22}$ and $d_{22}|d_{11}$, and hence $d_{11} = d_{22}$ and also $d_{12} = d_{21}$. Thus, if we put $d_i = d_{i1}$, then $d = d_1 d_2$ and $(d_1, d_2) = 1$, so $d_1||d$ and $\mathrm{Ker}(h_{i1}) = \mathrm{Ker}(h)[d_i]$, for $i = 1, 2$. Now $h'^{(h)} = h_{21} \circ h_{11}^t \in \mathrm{Hom}(E'_1, E'_2)$ has cyclic kernel because $h_{12} = (h'_{12})^t$ and h_{11}^t both have cyclic kernels of orders $d_{12} = d_2$, and $d_{11} = d_1$, respectively, and $(d_1, d_2) = 1$. Thus, $h'^{(h)} = \pm h'$, and so $\alpha_{d_1}(\langle E_1 \xrightarrow{h} E_2 \rangle) = \langle E'_1 \xrightarrow{h'} E'_2 \rangle$, as claimed.

Remark 52 In terms of the terminology of [23], p. 99, condition (42) means that $(h, h_{11}, h'_{12}, h_{21}, h'_{22})$ is an *isogeny factor set* representing the *diamond configuration* $(h, \mathrm{Ker}(h)[d_1], \mathrm{Ker}(h)[d_2])$. Thus, Proposition 51 gives a (partial) explanation of why such factor sets arise in the study of product surfaces.

We now want to compute the pullback of divisors with respect the isomorphism α_g defined in Proposition 50. For this, we shall use the embedding $\Psi_h = \Phi_{\lambda_1 \otimes \lambda_2, h^t \times 1}$ which was defined in the proof of Proposition 41.

Proposition 53 *In the situation of* Proposition 50 *we have*

$$(49) \quad (h_{22} \times h_{22}) \Psi_h(\alpha_g^* D')(h_{22}^t \times h_{22}^t) = [\tilde{g}^t]_{E'_2} \Psi_{h'}(D')[\tilde{g}]_{E'_2}, \quad \forall D' \in \mathrm{NS}(E'_1 \times E'_2).$$

In particular, if $a', b', c' \in \mathbb{Z}$, *then*

$$(50) \qquad \alpha_g^* \mathbf{D}(a', b', c'h') = \mathbf{D}(a, b, ch),$$

where $a, b, c \in \mathbb{Z}$ *are given by the matrix equation*

$$(51) \qquad \begin{pmatrix} ad & cd \\ cd & b \end{pmatrix} = g^t \begin{pmatrix} a'd_2 & c'd \\ c'd & b'd_1 \end{pmatrix} g = \frac{1}{d_1} \tilde{g}^t \begin{pmatrix} a'd & c'd \\ c'd & b' \end{pmatrix} \tilde{g}.$$

Thus, if $s' \in P(d)$, *then we have an isomorphism of principally polarized abelian surfaces*

$$(52) \qquad \alpha_g : (E_1 \times E_2, D_{s'\tilde{g},h}) \xrightarrow{\sim} (E'_1 \times E'_2, D_{s',h'}),$$

where $s'\tilde{g} \in P(d)$ *is defined by the rule* $M(f_d(s'\tilde{g})) = \frac{1}{d_1} \tilde{g}^t M(f_d(s')) \tilde{g}$.

Proof. Since $r_{\lambda'_2 \otimes \lambda'_2, \lambda_2 \otimes \lambda_2}(h_{22}^t \times h_{22}^t) = h_{22} \times h_{22}$ (cf. (69)), it follows from the definitions and formula (61) of the appendix that the left hand side of (49) equals $(h_{22}^t \times h_{22}^t)^\flat (h^t \times 1)^\flat \Phi_{\lambda_1 \otimes \lambda_2}(\alpha_g^* D') = (h_{22}^t \times h_{22}^t)^\flat (h^t \times 1)^\flat (\alpha_g)^\flat \Phi_{\lambda'_1 \otimes \lambda'_2}(D') = (\alpha_g (h^t \times$

$1)(h_{22}^t \times h_{22}^t))^\flat \Phi_{\lambda_1' \otimes \lambda_2'}(D') = (((h')^t \times 1)[\tilde{g}]_{E_2'})^\flat \Phi_{\lambda_1' \otimes \lambda_2'}(D') = ([\tilde{g}]_{E_2'})^\flat \Psi_{h'}(D')$, where we have used (63) and (47) in the last three equalities. Since $r_{\lambda_2 \otimes \lambda_2'}([\tilde{g}]_{E_2'}) = [\tilde{g}^t]_{E_2'}$ by (69), we obtain $([\tilde{g}]_{E_2'})^\flat \Psi_{h'}(D') = [\tilde{g}^t]_{E_2'} \Psi_{h'}(D')[\tilde{g}]_{E_2'}$, which proves (49).

We next note that the second equality of (51) follows immediately from the fact that $\tilde{g} = \mathrm{diag}(1, d_1)g$. Furthermore, by multiplying out the right hand side of (51), we see that if g has the form (44), then the first equality of (51) holds with $a = a'd_1a_{11}^2 + 2dc'a_{11}a_{21} + b'd_2a_{21}^2, b = a'd_2a_{12}^2 + 2c'da_{12}a_{22} + b'd_1a_{22}^2, c = a'a_{11}a_{12} + c'(d_2a_{12}a_{21} + d_1a_{11}a_{22}) + b'a_{21}a_{22}$, and so in particular $a, b, c \in \mathbb{Z}$. This proves (51).

To prove (50), note first that by (38) we have $\Psi_h(\mathbf{D}(a, b, ch)) = [g_1]_{E_2}$, where $g_1 = \left(\begin{smallmatrix} ad & cd \\ cd & b \end{smallmatrix}\right)$, and similarly $\Psi_{h'}(\mathbf{D}(a', b', c'h')) = [g_1']_{E_2'}$ with $g_1' = \left(\begin{smallmatrix} a'd & c'd \\ c'd & b' \end{smallmatrix}\right)$. Thus, if $D' = \mathbf{D}(a', b', c'h')$, then by (51) the right hand side of (49) equals $[d_1g_1]_{E_2'} = (h_{22} \times h_{22})(h_{22}^t \times h_{22}^t)[g_1]_{E_2'} = (h_{22} \times h_{22})[g_1]_{E_2}(h_{22}^t \times h_{22}^t) = (h_{22} \times h_{22})\Psi_h(D)(h_{22}^t \times h_{22}^t)$, where $D = \mathbf{D}(a, b, ch)$. Comparing this to the left hand side of (49) yields $\Psi_h(\alpha_g^*(D')) = \Psi_h(D)$ (because $h_{22} \times h_{22}$ and $h_{22}^t \times h_{22}^t$ are isogenies), and so (50) follows because Ψ_h is injective; cf. Corollary 60 of the appendix.

Finally, to prove (52), recall from Proposition 50 that $\alpha_g : E_1 \times E_2 \xrightarrow{\sim} E_1' \times E_2'$ is an isomorphism. Now by (50) we have $\alpha_g^* D_{s',h'} = D_{s'\tilde{g},h}$, and so (52) follows.

Proof of Theorem 49. Fix $s = (n_1, n_2, k) \in P(d)$ and let $g \in \Gamma_0^\pm(d_2)_{d_1}$. If $\tilde{g}$ is defined by (45), then a short computation shows that $\frac{1}{d_1}\tilde{g}^t M(f_d(s))\tilde{g} = M(f_d(s'))$, for some $s' \in P(d)$ and that $M(f_d(s')) = g^t M(q)g$, where $q = [n_1d_2, 2kd, n_2d_1]$. Since $g \in \mathrm{GL}_2(\mathbb{Z})$, this implies that $f_d(s') \approx q$, and so Lemma 54 below shows that $f_d(s') \approx q \sim f_d(s) \circ a_{d_1}$. Thus, (40) follows once we have shown that $\mu_s \circ \alpha_{d_1} = \mu_{s'}$.

For this, let $x = \langle E_1 \xrightarrow{h} E_2 \rangle \in \mathcal{X}_0(d)$ and put $x' = \alpha_{d_1}(x) = \langle E_1' \xrightarrow{h'} E_2' \rangle$. Then $\mu_s(\alpha_{d_1}(x)) = \mu_s(x') = \langle E_1' \times E_2', D_{s,h'} \rangle$. Now by (52) we have $\alpha_g : (E_1 \times E_2, D_{s',h}) \xrightarrow{\sim} (E_1' \times E_2', D_{s,h})$, and so $\mu_s(\alpha_{d_1}(x)) = \mu_{s'}(x)$. This proves that $\mu_s \circ \alpha_{d_1} = \mu_{s'}$ when $X_0(d)$ is reduced. In the general case a similar argument (generalized to elliptic curves over K-schemes) shows that we have an equality $\tilde{\mu}_s \circ \alpha_{d_1} = \tilde{\mu}_{s'}$ of morphisms of functors, and so (40) holds in general.

It remains to prove (41). For this, let $s_1, s_2 \in P(d)$ be such that $\mathrm{Im}(\mu_{s_1}) = \mathrm{Im}(\mu_{s_2})$. Then Proposition 45 shows that $H(q_{s_1}) = H(q_{s_2})$ and so by Corollary 33 we have that $q_{s_1} \approx q_{s_2}$. We now distinguish two cases.

If $s_1 \in P(d)^{odd}$, then q_{s_1} is primitive by Lemma 17 and hence so is q_{s_2}. Thus, also $s_2 \in P(d)^{odd}$. By Corollary 19 (and Remark 11) we thus have that $f_d(s_1) \sim f_d(s_1) \circ a$, where $a \in \mathrm{Ker}(\pi_d')$. By Corollary 20 we have $a \sim a_{d_1}$, for some $d_1 || d$, and so (40) shows that $\mu_{s_1} \circ \alpha_{d_1} = \mu_{s_2}$, as desired.

Now suppose that $s_1 \in P(d)^{even}$; then also $s_2 \in P(d)^{even}$. Here $f_d(s_i) = 2f_d'(s_i)$, where $f_d'(s_i) \in Q_{-d}^{(1)}$, and by Corollary 19 we thus have $f_d'(s_1) \sim f_d'(s_2) \circ a$ with $a \in \bar{Q}_{-d}[2]$. Now $a \sim a_{d_1} := [d_1, d_1, \frac{d_1+d_2}{4}]$, for some $d_1 || d$, because the set $\{a_{d_1} : d_1 || d,\ d_1 \leq d_2\}$ represents the classes in $\bar{Q}_{-d}[2]$, and so (40) shows again that $\mu_{s_1} \circ \alpha_{d_1} = \mu_{s_2}$. This proves one direction of (41), and so (41) follows since the other direction is trivial.

Lemma 54 *Let $s = [n_1, n_2, k] \in P(d)$, and put $q = [d_2 n_1, 2kd, d_1 n_2]$, where $d = d_1 d_2$ with $\gcd(d_1, d_2) = 1$. Then $f_d(s) \circ a_{d_1} \sim q$, where $a_{d_1} = [d_1, 0, d_2]$ if $s \in P(d)^{odd}$, and $a_{d_1} = [d_1, d_1, (d_1 + d_2)/4]$ if $s \in P(d)^{even}$.*

Proof. If $s \in P(d)^{odd}$, then $f_d(s) = [dn_1, 2kd, n_2]$ is primitive of discriminant $-4d$, and the composition algorithm of Arndt (cf. [2], p. 129) shows that $a_{d_1} \circ f_d(s) \sim q$. Indeed, apply [2], Theorem 7.8, to $f_1 = [d_1, 0, d_2] \in Q^{(1)}_{-4d}$ and $f_2 = f_d(s)$. Then (with the notation there) $n = d_1$, and so we can take $t = 1, u = v = 0$, and so $f_1 \circ f_2 \sim [d_1 n_1 d/d_1^2, d_1(2kd)/d_1, *] = q$.

Now suppose $s \in P(d)^{even}$. Then $f_d(s) = 2f'_d(s)$ where $f'_d(s) = [n'_1 d, kd, n'_2]$ is primitive of discriminant $-d$. Thus, applying Arndt's algorithm ([2], Theorem 7.8) to $f_1 = [d_1, d_1, (d_1 + d_2)/4] \in Q^{(1)}_{-d}$ (cf. proof of Theorem 49) and $f_2 = f'_d(s)$ shows that $f_1 \circ f_2 \sim [n'_1 d_2, kd, n'_2 d_1]$ because here again $n = d_1$, and so we can take $t = 1$, $u = v = 0$. Thus $f_d(s) \circ a_{d_1} := 2(f'_d(s) \circ a_{d_1}) \sim 2[n'_1 d_2, kd, n'_2 d_1] = q$.

10 The birational structure of $H(q)$

In order to determine the birational structure of $H(q)$, we shall first calculate the automorphism group $\mathrm{Aut}(\mu_s)$ of the morphism $\mu_s : X_0(d) \to H(q_s)$. As we shall see, the *Fricke involution* $w_d = \alpha_d$ on $X_0(d)$ always lies in $\mathrm{Aut}(\mu_s)$. However, if q_s is an ambiguous form, then there is another Atkin-Lehner involution α_s in $\mathrm{Aut}(\mu_s)$, as the following result shows.

Proposition 55 *(a) If $s \in P(d)^{odd}$, then $q_s \in \bar{Q}^2_{-16d}[2]$ (i.e., q_s is ambiguous) if and only if $f_d(s)^2 \in \mathrm{Ker}(\pi'_d)$. If this is the case, then there is a unique $d_1 || d$ with $d_1 \le d_2 := d/d_1$ such that $[d_1, 0, d_2] \sim \pi_{-4d,2}(q_s) \sim f_d^2(s)$.*

(b) If $s \in P(d)^{even}$, then $q'_s := \frac{1}{4} q_s \in \bar{Q}^2_{-d}[2]$ (i.e., q_s is ambiguous) if and only if $f'_d(s)^2 \in \bar{Q}^2_{-d}[2]$. If this is the case, then there is a unique $d_1 || d$ with $d_1 \le d_2 := d/d_1$ such that $[d_1, d_1, (d_1 + d_2)/4] \sim q'_s \sim f'_d(s)^2$.

(c) Let $s \in P(d)$ and put $\alpha_s = \alpha_{d_1}$, where d_1 is as above, if q_s is ambiguous, and $d_1 = 1$ otherwise. Then the stabilizer of μ_s under the group of Atkin-Lehner involutions is given by

$$G(\mu_s) := \{\alpha_k : k || d \text{ and } \mu_s \circ \alpha_k = \mu_s\} \;=\; \langle w_d, \alpha_s \rangle. \tag{53}$$

(d) We have $G(\mu_s) = \langle w_d \rangle$ if and only if either q_s is not ambiguous or if $q_s \sim q$ with $q \in \{1_{-16d}, 4(1_{-d}), q_d\}$, where q_d is as in Theorem 38 *(or as in* (14)*).*

Proof. (a) By (11) we have $f_d(s)^2 \sim \pi_{-4d,2}(q_s)$ and by (13) we have $\pi'_d(\pi_{-4d,2}(q_s)) \sim q_s^2$. Thus, $f_d(s)^2 \in \mathrm{Ker}(\pi'_d) \Leftrightarrow q_s^2 \sim 1 \Leftrightarrow q_s \in \bar{Q}^2_{-16d}[2]$. This proves the first assertion, and the second follows from (17).

(b) By (12) we have $f'_d(s)^2 \sim q'_s$, so the first assertion is trivial. The second follows immediately from the fact that the forms $[d_1, d_1, (d_1+d_2)/2]$ represent all of the ambiguous classes in $\bar{Q}_{-d}$; cf. proof of Theorem 49.

(c) Let $k||d$. From (40) we see that $a_k \in G(\mu_s) \Leftrightarrow f_d(s) \approx f_d(s) \circ a_k$, and so (53) is equivalent to the assertion

$$f_d(s) \approx f_d(s) \circ a_k \quad \Leftrightarrow \quad k \in \{1, d, d_1, d/d_1\}. \tag{54}$$

because $\alpha_1 = 1$, $\alpha_d = w_d$, $\alpha_{d_1} = \alpha_s$ and $\alpha_{d/d_1} = w_d\alpha_s$.

To verify (54), assume first that $f_d(s)$ is primitive, i.e. that $s \in P(d)^{odd}$. Then we have

$$f_d(s) \approx f_d(s) \circ a_k \quad \Leftrightarrow \quad a_k \sim 1 \text{ or } a_k \sim f_d(s)^2. \tag{55}$$

Indeed, by Remark 11 we see that the left condition holds if and only if either $f_d(s) \sim f_d(s) \circ a_k$ or $f_d(s)^{-1} \sim f_d(s) \circ a_k$. In the first case this means that a_k is principal, and in the second case that $a_k^{-1} \sim f_d(s)^2$. This proves (55) because $a_k \sim a_k^{-1}$.

Thus, if $q_s \notin \bar{Q}^2_{-16d}[2]$, then $d_1 = 1$ by definition. Moreover, the second condition of the right hand side of (55) is impossible because $a_k \in \mathrm{Ker}(\pi'_d)$ (cf. (17)) and so this condition yields the contradiction $1 \sim \pi'_d(a_k) \sim \pi'_d(f_d(s)^2) \sim q_s^2$. Thus, the right hand side of (55) reduces to the condition that $a_k \sim 1$, and by reduction theory we see that this is the case if and only $k = 1$ or $k = d$. This proves (54) in this case.

Next, suppose that $q_s \in \bar{Q}^2_{-16d}[2]$. Then by part (a) we have that $f_d(s)^2 \sim a_{d_1}$. Thus, the right hand side of (55) is equivalent to $a_k \sim 1$ or $a_k \sim a_{d_1}$, which, by reduction theory, is equivalent to $k \in \{1, d, d_1, d/d_1\}$. This proves (54) for $s \in P(d)^{odd}$.

Now suppose that $f_d(s)$ is not primitive, i.e. $s \in P(d)^{even}$. Then $f_d(s) = 2f'_d(s)$ with $f'_d(s) \in Q^{(1)}_{-d}$ and $q_s = 4q'$ with $q' \sim f'_d(s)^2$; cf. Lemma 17(b). In this case a similar argument to the one above shows that

$$f_d(s) \approx f_d(s) \circ a_k \quad \Leftrightarrow \quad a_k \sim 1 \text{ or } a_k \sim f'_d(s)^2. \tag{56}$$

Thus, if $q' \notin \bar{Q}_{-d}[2]$ then $d_1 = 1$ by definition. Here the second condition of the right side of (56) is impossible (because it implies that $q' \sim f'_d(s)^2 \sim a_k \in Q_{-d}[2]$), so the right side of (56) reduces to the condition $a_k \sim 1$, i.e., $k = 1$ or d. This proves (54) in this case. On the other hand, if $q' \in \bar{Q}_{-d}[2]$, then $f'_d(s)^2 \sim a_{d_1}$ and one concludes by a similar argument as above that (54) holds.

(d) Since $\langle w_d \rangle = \{\alpha_1, \alpha_d\}$, we see by part (c) that $G(\mu_s) = \langle w_d \rangle \Leftrightarrow \alpha_{d_1} \in \langle w_d \rangle \Leftrightarrow d_1 = 1$ (because $d_1 \leq d/d_1$). Thus, if q_s is not ambiguous, then the assertion is clear by part (c), so assume q_s is ambiguous.

If q_s is not primitive, then by part (b) we see that $d_1 = 1 \Leftrightarrow a_{d_1} \sim 1_{-d} \Leftrightarrow q'_s \sim 1_{-d}$, and if q_s is primitive, then by part (a) we have $d_1 = 1 \Leftrightarrow a_{d_1} \sim 1_{-4d} \Leftrightarrow q_s \in \mathrm{Ker}(\pi_{-4d,2}) \Leftrightarrow q_s \sim 1_{-16d}$ or q_d, the latter by (14).

We now show that $\mathrm{Aut}(\mu_s) = G(\mu_s)$ by examining the fibres of μ_s at non-CM points.

Proposition 56 *Let $s \in P(d)$ and let $x \in X_0(d)(K)$ be a non-CM point. Then*

$$\mu_s^{-1}(\mu_s(x)) = G(\mu_s)x = \{x, w_d(x), \alpha_s(x), w_d\alpha_s(x)\}, \tag{57}$$

and so $\mathrm{Aut}(\mu_s) = G(\mu_s)$*, provided that* $\mathrm{char}(K) \nmid d$.

Proof. The second equality of (57) follows from (53). To prove the first, write $x = \langle E_1 \xrightarrow{h} E_2 \rangle$ and let $y = \langle E_1' \xrightarrow{h'} E_2' \rangle \in X_0(d)(K)$. Then by (40) and the definition of $G(\mu_s)$, it is clear that the first equality of (57) follows from:

$$\mu_s(x) = \mu_s(y) \;\Leftrightarrow\; y = \alpha_k(x), \text{ for some } k||d \text{ with } f_d(s) \approx f_d(s) \circ a_k. \tag{58}$$

To verify (58), note first that if $y = \alpha_k(x)$ and $f_d(s) \approx f_d(s) \circ a_k$, then $\mu_s(y) = \mu_s(\alpha_k(x)) = \mu_s(x)$ by (40). Conversely, if $\mu_s(x) = \mu_s(y)$, then $\exists \alpha : E_1 \times E_2 \xrightarrow{\sim} E_2' \times E_2'$ such that $\alpha^* D_{s,h'} = D_{s,h}$. Then by (48) we know that $\exists k||d = \deg(h)$ such that $y = \alpha_k(x)$, and so by (40) we have $\mu_s(y) = \mu_{s'}(x)$, where $s' \in P(d)$ is such that $f_d(s') \approx f_d(s) \circ a_k$. Thus, $\mu_s(x) = \mu_{s'}(x)$, which means that $(E_1 \times E_2, D_{s,h}) \simeq (E_1 \times E_2, D_{s',h})$. Then (39) shows that $f_d(s) \approx f_d(s') \approx f_d(s) \circ a_k$, and so (58) holds.

To verify the last assertion, assume that $\mathrm{char}(K) \nmid d$. Then $\mu_s : X_0(d) \to H(q_s)$ is finite because by Proposition 45 (and Corollary 47) it is a proper, surjective morphism between irreducible curves; cf. EGA (II, 7.4.4) and EGA (III, 4.4.2). Thus, from (57) we see that the separable degree $\deg_s(\mu_s)$ of μ_s equals $|G(q_s)|$ because (after enlarging K, if necessary) there are infinitely many non-CM points on $X_0(d)(K)$. We thus have $|G(\mu_s)| \leq |\mathrm{Aut}(\mu_s)| \leq \deg_s(\mu_s) = |G(\mu_s)|$, and so we have equality throughout. In particular, $G(\mu_s) = \mathrm{Aut}(\mu_s)$, as claimed.

Theorem 57 *Let $s \in \bar{P}(d)$, and suppose that* $\mathrm{char}(K) \nmid d$*. Then*

$$\deg(\mu_s) \;=\; |G(\mu_s)| \;=\; \begin{cases} 2 & \text{if } q_s \sim 1_{-16d}, 4(1_{-d}) \text{ or } q_d \text{ or } q_s \text{ is not ambiguous} \\ 4 & \text{otherwise} \end{cases} \tag{59}$$

and so the curve $X_0(d)_s^+ = X_0(d)/G(\mu_s)$ is the normalization of $H(q_s)$. In particular, $X_0(d)^+ = X_0(d)/\langle w_d \rangle$ is the normalization of $H(q)$ if $|G(\mu_s)| = 2$.

Proof. The second equality of (59) follows from Proposition 55(d). Moreover, since the proof of Proposition 56 shows that $\deg_s(\mu) = |G(\mu_s)|$, the first equality follows once we have shown that μ_s is separable. This will also yield the second assertion. Indeed, if $\pi_{G(\mu_s)} : X_0(d) \to X_0(d)_s^+/G(\mu_s)$ denotes the quotient map, then $\mu_s = \bar{\mu}_s \circ \pi_{G(\mu_s)}$, for some morphism $\bar{\mu}_s : X_0(d)_s^+ \to H(q_s)$. Note that $X_0(d)_s^+$ is affine and that hence $\bar{\mu}_s$ is again finite (use EGA (II, 5.4.3)). Since $X_0(d)$ and hence also $X_0(d)_s^+$ is normal, we see that $\bar{\mu}_s = \nu \circ \tilde{\mu}_s$ factors over the normalization $\nu : \tilde{H}(q_s) \to H(q_s)$. By the above, $\deg_s(\tilde{\mu}_s) = 1$, so if μ_s is separable, then $\bar{\mu}_s$ is birational.

Since separability is automatic if $p = \mathrm{char}(K) = 0$, it remains to verify it if $p \neq 0$.

For this, we shall use a specialization argument. Let $R = \mathbb{Z}_{(p)} \subset \mathbb{Q}$ denote the discrete valuation ring with residue field $\mathbb{F}_p$, and let $X_0(d)/R$ and A_2/R be the coarse moduli schemes of the functors $\mathcal{X}_0(d)$ and $\mathcal{A}_2$ on $\underline{Sch}_{/R}$, respectively. Since $p \nmid d$, we know that $X_0(d)/R$ is smooth and that hence its fibres are the coarse moduli schemes of the corresponding fibre functors; cf. [26], p. 510. In addition, one has that the fibres of A_2 are the coarse moduli schemes of its fibre functors; cf. Igusa[20], for M_2 in place of A_2 (which suffices for our purposes). Now the method of proof of Proposition 45 extends to construct an R-morphism $\mu_s : X_0(d) \to A_2$, and the same proof shows that μ_s is again proper. Thus, by Fulton [11], Proposition 20.3(a), we have $\deg(\mu_s^\circ) = \deg(\mu_s^s)$, where μ_s° and μ_s^s are the restrictions of μ_s to the generic and special fibres of $X_0(d)$, respectively. Since these can be identified with the previously constructed morphisms μ_s (over $K = \mathbb{Q}$ and over $K = \mathbb{F}_p$, respectively), we have by (the proof of) Proposition 56 that $\deg_s(\mu_s^\circ) = |G(q_s)| = \deg_s(\mu_s^s)$. But since $\deg_s(\mu_s^\circ) = \deg(\mu_s^\circ)$, it follows that also $\deg_s(\mu_s^s) = \deg(\mu_s^s)$, and so μ_s^s is separable.

Proof of Theorem 1 *and* Theorem 4. Theorem 12 and Corollary 47 show that $T(d)$ is a closed subset which is a finite union of curves $H'(q)$ with $q \in \bar{Q}_d^*$. From this and Theorem 13 it is clear that Theorem 4 and the last part of Theorem 1 are special cases of Theorem 57.

11 Appendix: The Néron-Severi group

The purpose of this appendix is to present some basic facts about the Néron-Severi groups of abelian varieties which were used throughout the paper.

Let A be an abelian variety over an algebraically closed field K, and let $\mathrm{NS}(A) = \mathrm{Pic}(A)/\mathrm{Pic}^0(A)$ denote the Néron-Severi group of A. If A has a principal polarization $\lambda = \phi_\theta : A \xrightarrow{\sim} \hat{A}$ (cf. Milne[34], p. 126), then $\mathrm{NS}(A)$ can be interpreted as a subgroup of $\mathrm{End}(A)$. More precisely, if r_λ denotes the Rosati involution on $\mathrm{End}(A)$ (which is defined by the rule $r_\lambda(\alpha) = \lambda^{-1}\hat{\alpha}\lambda$), then by Mumford[37], p. 190, 189, the map $D \mapsto \lambda^{-1}\phi_D$ defines an isomorphism

$$\Phi_\lambda : \mathrm{NS}(A) \xrightarrow{\sim} \mathrm{End}_\lambda(A) := \{\alpha \in \mathrm{End}(A) : r_\lambda(\alpha) = \alpha\}. \tag{60}$$

The isomorphism Φ_λ satisfies the following functorial property.

Proposition 58 *If (A_i, λ_i), $i = 1, 2$, are two principally polarized abelian varieties, and $h \in \mathrm{Hom}(A_1, A_2)$,*

$$\Phi_{\lambda_1}(h^* D) \;=\; r_{\lambda_1,\lambda_2}(h)\Phi_{\lambda_2}(D)h, \quad \forall D \in \mathrm{NS}(A_2), \tag{61}$$

where $r_{\lambda_1,\lambda_2}(h) = \lambda_1^{-1}\hat{h}\lambda_2 \in \mathrm{Hom}(A_2, A_1)$. In other words, $\Phi_{\lambda_1} \circ h^* = h^\flat \circ \Phi_{\lambda_2}$, where $h^\flat : \mathrm{End}(A_2) \to \mathrm{End}(A_1)$ is defined by $h^\flat(\alpha) = r_{\lambda_1,\lambda_2}(h)\alpha h$. Moreover,

$$r_{\lambda_1} \circ h^\flat = h^\flat \circ r_{\lambda_2}, \tag{62}$$

and hence $\Phi_{\lambda_1} \circ h^*$ *defines a homomorphism* $\Phi_{\lambda_1,h} : \mathrm{NS}(A_2) \to \mathrm{End}_{\lambda_1}(A_1)$.

Proof. The first formula follows immediately from the definitions and the fact that $\phi_{h^*D} = \hat{h} \circ \phi_D \circ h$, for $D \in \mathrm{Pic}(A)$. Similarly, (62) follows from the definitions together with the fact that $r_{\lambda_1,\lambda_2}(h)\hat{} \circ \lambda_1 = \lambda_2 \circ h$.

Remark 59 For later reference, let us observe here that the assignment $h \mapsto h^\flat = h^\flat_{\lambda_1,\lambda_2}$ is functorial: if (A_i, λ_i), $i = 1, 2, 3$, are three principally polarized abelian varieties, and $h_i \in \mathrm{Hom}(A_i, A_{i+1})$ for $i = 1, 2$, then

$$(h_2 \circ h_1)^\flat_{\lambda_1,\lambda_2} = (h_1)^\flat_{\lambda_1,\lambda_2} \circ (h_2)^\flat_{\lambda_2,\lambda_3}. \tag{63}$$

This follows easily from the definitions and the fact that $r_{\lambda_1,\lambda_3}(h_1 \circ h_2) = r_{\lambda_1,\lambda_2}(h_1) \circ r_{\lambda_2,\lambda_3}(h_2)$.

In the case that h is an isogeny, we can define $h^\flat$ in another way.

Corollary 60 *If* $h : A_1 \to A_2$ *is an isogeny, then the rule* $c_h(\alpha) = h^{-1}\alpha h$ *defines a ring isomorphism* $c_h : \mathrm{End}^0(A_2) \xrightarrow{\sim} \mathrm{End}^0(A_1)$ *which is related to* $h^\flat$ *by the formula*

$$h^\flat(\alpha) = \beta c_h(\alpha), \quad \textit{where } \beta = h^\flat(1) = r_{\lambda_1,\lambda_2}(h)h, \tag{64}$$

and we have

$$r_{\lambda_1}(c_h(\alpha)) = \beta c_h(r_{\lambda_2}(\alpha))\beta^{-1}, \quad \forall \alpha \in \mathrm{End}^0(A_2). \tag{65}$$

Thus $\Phi_{\lambda_1,h} := \Phi_{\lambda_1} \circ h^* = h^\flat \circ \Phi_{\lambda_2} = \beta(c_h \circ \Phi_{\lambda_2}) : \mathrm{NS}(A_2) \to \mathrm{End}_{\lambda_1}(A_1)$ *is an injective group homomorphism which satisfies*

$$\Phi_{\lambda_1,h}(\alpha^* D) = r_{\lambda_1}(c_h(\alpha))\Phi_{\lambda_1,h}(D)c_h(\alpha), \quad \forall D \in \mathrm{NS}(A_2),\ \alpha \in \mathrm{End}(A_2). \tag{66}$$

Proof. It is clear that c_h is a ring isomorphism and that (64) holds. Thus, since $r_{\lambda_1}(\beta) = r_{\lambda_1}(h^\flat(1)) = h^\flat(1) = \beta$ by (62), we see that $r_{\lambda_1}(c_h(\alpha))\beta = r_{\lambda_1}(c_h(\alpha))r_{\lambda_1}(\beta) = r_{\lambda_1}(\beta c_h(\alpha)) \overset{(64)}{=} r_{\lambda_1}(h^\flat(\alpha)) \overset{(62)}{=} h^\flat(r_{\lambda_2}(\alpha)) \overset{(64)}{=} \beta c_h(r_{\lambda_2}(\alpha)$, and so (65) follows.

Write $\Phi = \Phi_{\lambda_1,h}$. Then $\Phi = h^\flat \circ \Phi_{\lambda_2}$ by (61) and hence $\Phi = \beta(c_h \circ \Phi_{\lambda_2})$ by (64). From the latter expression it is clear that Φ is an injective group homomorphism. Moreover, since c_h is multiplicative, we have $\Phi(\alpha^* D) = \beta c_h(\Phi_{\lambda_2}(\alpha^* D)) \overset{(61)}{=} \beta c_h(r_{\lambda_2}(\alpha)\Phi_{\lambda_2}(D)\alpha) \overset{(65)}{=} r_{\lambda_1}(c_h(\alpha))\beta c_h(\Phi_{\lambda_2}(D))c_h(\alpha)$, which proves (66).

Let (A_i, λ_i) be two principally polarized abelian varieties, and $A = A_1 \times A_2$ be the product variety with projections $p_i : A \to A_i$ and inclusions $e_i : A_i \to A$. Then $p := \hat{p}_1 + \hat{p}_2 : \hat{A}_1 \times \hat{A}_2 \xrightarrow{\sim} \hat{A}$ is an isomorphism, and $\lambda_1 \times \lambda_2 := p \circ \lambda_1 \times \lambda_2 : A \xrightarrow{\sim} \hat{A}$ is a principal polarization of A, called the product polarization. (Note that if $\lambda_i = \phi_{\theta_i}$, then $\lambda_1 \otimes \lambda_2 = \phi_\theta$, where $\theta = p_1^*\theta_1 + p_2^*\theta_2$.)

If $\alpha \in \mathrm{End}(A_1 \times A_2)$, then we can identify α with the 2×2 matrix (α_{ij}) by putting $\alpha_{ij} = p_i \alpha e_j \in \mathrm{Hom}(A_j, A_i)$. Thus

$$\mathrm{End}(A_1 \times A_2) = \left\{ \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix} : \alpha_{ij} \in \mathrm{Hom}(A_j, A_i) \right\}.$$

Proposition 61 *In the above situation we have*

$$(67)\, \mathrm{End}_{\lambda_1 \otimes \lambda_2}(A_1 \times A_2) = \left\{ \begin{pmatrix} \alpha_{11} & \alpha'_{21} \\ \alpha_{21} & \alpha_{22} \end{pmatrix} : \alpha_{ii} \in \mathrm{End}_{\lambda_i}(A_i), \alpha_{21} \in \mathrm{Hom}(A_1, A_2) \right\},$$

where $\alpha'_{21} = r_{\lambda_1, \lambda_2}(\alpha_{21})$. *Thus, the rule* $(\alpha_1, \alpha_2, \beta) \mapsto \left(\begin{smallmatrix} \alpha_1 & \beta' \\ \beta & \alpha_2 \end{smallmatrix}\right)$ *defines an isomorphism*

$$\mu = \mu_{\lambda_1, \lambda_2} : \mathrm{End}_{\lambda_1}(A_1) \oplus \mathrm{End}_{\lambda_2}(A_2) \oplus \mathrm{Hom}(A_1, A_2) \xrightarrow{\sim} \mathrm{End}_{\lambda_1 \otimes \lambda_2}(A_1 \times A_2)$$

which induces an isomorphism

$$\mathbf{D} = \mathbf{D}_{\lambda_1, \lambda_2} : \mathrm{NS}(A_1) \oplus \mathrm{NS}(A_2) \oplus \mathrm{Hom}(A_1, A_2) \xrightarrow{\sim} \mathrm{NS}(A_1 \times A_2).$$

Moreover, we have

$$(68) \qquad \mathbf{D}(D_1, D_2, 0) = p_1^* D_1 + p_2^* D_2, \quad \forall D_i \in \mathrm{NS}(A_i).$$

Proof. Since $\hat{e}_i(\lambda_1 \otimes \lambda_2) = \lambda_i p_i$ and $(\lambda_1 \otimes \lambda_2) e_j = \hat{p}_j \lambda_j$, we see that $p_i r_{\lambda_1 \otimes \lambda_2}(\alpha) e_j = r_{\lambda_i, \lambda_j}(p_j \alpha e_i) = r_{\lambda_i, \lambda_j}(\alpha_{ji})$. Thus

$$(69) \qquad r_{\lambda_1 \otimes \lambda_2} \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix} = \begin{pmatrix} \alpha'_{11} & \alpha'_{21} \\ \alpha'_{12} & \alpha'_{22} \end{pmatrix},$$

where $\alpha'_{ji} = r_{\lambda_i, \lambda_j}(\alpha_{ji}) = \lambda_i^{-1} \hat{\alpha}_{ji} \lambda_j$. From (69) we therefore see that $\alpha = (\alpha_{ij}) \in \mathrm{End}_{\lambda_1 \otimes \lambda_2}(A) \Leftrightarrow \alpha_{ij} = \alpha'_{ji}, \forall i, j = 1, 2 \Leftrightarrow \alpha_{12} = \alpha'_{21}, \alpha_{ii} \in \mathrm{End}_{\lambda_i}(A_i), i = 1, 2$, the latter because the hypothesis $\alpha_{12} = \alpha'_{21}$ implies that $\alpha'_{12} = (\alpha'_{21})' = \alpha_{12}$. This proves (67), and from this the assertion about μ follows immediately. Finally, if we put $\mathbf{D}_{\lambda_1, \lambda_2} = \Phi^{-1}_{\lambda_1 \otimes \lambda_2} \circ \mu_{\lambda_1, \lambda_2} \circ (\Phi_{\lambda_1} \oplus \Phi_{\lambda_2} \oplus id)$, then it is clear by (60) that $\mathbf{D} = \mathbf{D}_{\lambda_1, \lambda_2}$ yields the desired isomorphism.

To prove (68), we first note that since $\hat{e}_i(\lambda_1 \otimes \lambda_2) = \lambda_i p_i$, we have $r_{\lambda_1 \otimes \lambda_2, \lambda_i}(p_i) = e_i$ and hence $\Phi_{\lambda_1 \otimes \lambda_2}(p_i^* D_i) = e_i \Phi_{\lambda_i}(D_i) p_i$ by (61). Thus $\Phi_{\lambda_1 \otimes \lambda_2}(p_1^* D_1 + p_2^* D_2) = \mu(\Phi_{\lambda_1}(D_1), \Phi_{\lambda_2}(D_2), 0)$, and so (68) follows.

Another useful formula is the following.

Proposition 62 *Let* (A, λ) *be a principally polarized abelian variety. If* $m_A : A \times A \to A$ *denotes the addition map and* $\delta_A : A \to A \times A$ *the diagonal map, then* $r_{\lambda \otimes \lambda, \lambda}(m_A) = \delta_A$ *and hence*

$$(70) \qquad \Phi_{\lambda \otimes \lambda}(m_A^* D) = \delta_A \Phi_\lambda(D) m_A, \quad \forall D \in \mathrm{NS}(A).$$

Proof. Since $\hat{e}_i(\lambda \otimes \lambda) = \lambda p_i$ and $\hat{e}_i \hat{m}_A = id_{\hat{A}}$, we have $p_i r_{\lambda\otimes\lambda,\lambda}(m_A) = p_i(\lambda \otimes \lambda)^{-1}\hat{m}_A\lambda = \lambda^{-1}\hat{e}_i\hat{m}_A\lambda = 1_A$, and so $r_{\lambda\otimes\lambda,\lambda}(m_A) = \delta_A$. Thus (70) follows from (61).

We now specialize the above results to the case of products of two elliptic curves.

Proposition 63 *Let $A = E_1 \times E_2$ be a product of two elliptic curves, and let $\lambda_i = \phi_{0_{E_i}}$. Then the isomorphism*

$$\mathbf{D} = \mathbf{D}_{\lambda_1,\lambda_2} : \mathbb{Z} \oplus \mathbb{Z} \oplus \mathrm{Hom}(E_1, E_2) \xrightarrow{\sim} \mathrm{NS}(A)$$

is given by the formula

$$\mathbf{D}(a, b, f) = cl((a - \deg(f))\theta_1 + (b - 1)\theta_2 + \Gamma_{-f}). \tag{71}$$

Here $\theta_i = p_i^*(0_{E_i})$, $\Gamma_f \in \mathrm{Div}(A)$ is the graph of f, and $cl(D) \in \mathrm{NS}(A)$ denotes the class of a divisor $D \in \mathrm{Div}(A)$. Thus

$$(\mathbf{D}(a, b, f).\mathbf{D}(a, b, f)) = 2(ab - \deg(f)), \tag{72}$$

$$(\mathbf{D}(a, b, f).(x\theta_1 + y\theta_2)) = bx + ay. \tag{73}$$

Proof. First note that since $\mathrm{NS}(E_i) = \mathbb{Z}cl(0_{E_i}) \simeq \mathbb{Z}$, the map $\mathbf{D}$ yields the indicated isomorphism. To prove (71), it is in view of (68) enough to verify that

$$\Phi_{\lambda_1\otimes\lambda_2}(\Gamma_{-f}) = \mu([\deg(f)]_{E_1}, 1_{E_2}, f) \tag{74}$$

and this follows from the identities $\Gamma_{-f} = (f \times 1)^* m_{E_2}^*(0_{E_2})$, $r_{\lambda_1\otimes\lambda_2,\lambda_2\otimes\lambda_2}(f \times 1_{E_2}) = f' \times 1_{E_2}$ and $\Phi_{\lambda_2}(0_{E_2}) = 1_{E_2}$ because by (61) and (70) we obtain $\Phi_{\lambda_1\otimes\lambda_2}(\Gamma_{-f}) = (f' \times 1_{E_2})\Phi_{\lambda_2\otimes\lambda_2}(m_{E_2}^* 0_{E_2})(f \times 1_{E_2}) = (f' \times 1_{E_2})\delta_{E_2}\Phi_{\lambda_2}(0_{E_2})m_{E_2}(f \times 1_{E_2}) = (f' \times 1_{E_2})\delta_{E_2}m_{E_2})(f \times 1_{E_2}) = \left(\begin{smallmatrix} f' & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} f & 0 \\ 0 & 1 \end{smallmatrix}\right) = \mu(f'f, 1, f) = \mu([\deg(f)], 1, f)$.

From (71), the formulae (72) and (73) follow immediately because $(\theta_1.\theta_2) = (\Gamma_{-f}.\theta_1) = 1$, $(\Gamma_{-f}.\theta_2) = \deg(-f) = \deg(f)$ and $\theta_1^2 = \theta_2^2 = \Gamma_{-f}^2 = 0$, the latter because $\theta_1 = \{0\} \times E_2 \simeq E_2$ and $\theta_2 \simeq \Gamma_{-f} \simeq E_1$ are elliptic curves.

Corollary 64 *Let $A' = E_1' \times E_2'$ be another product surface and let $\alpha = (\alpha_{ij}) \in \mathrm{Hom}(A', A))$, where $\alpha_{ij} \in \mathrm{Hom}(E_j', E_i)$. Then*

$$\deg(\alpha) = \left|(d_{11} + d_{21})(d_{12} + d_{22}) - \deg(f_\alpha)\right|, \tag{75}$$

where $d_{ij} = \deg(\alpha_{ij})$ and $f_\alpha = \alpha_{12}^t\alpha_{11} + \alpha_{22}^t\alpha_{21}$. Moreover, for $f \in \mathrm{Hom}(E_1, E_2)$ we have

$$\alpha^*\mathbf{D}(n_1, n_2, f) = \mathbf{D}(n_1', n_2', f') \tag{76}$$

where n_1', n_2', and f' are determined by the matrix equation

$$\begin{pmatrix} [n_1']_{E_1'} & (f')^t \\ f' & [n_2']_{E_2'} \end{pmatrix} = \begin{pmatrix} \alpha_{11}^t & \alpha_{21}^t \\ \alpha_{12}^t & \alpha_{22}^t \end{pmatrix} \begin{pmatrix} [n_1]_{E_1} & f^t \\ f & [n_2]_{E_2} \end{pmatrix} \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix}. \tag{77}$$

In other words, we have explicitly

$$\begin{aligned} n_1' &= n_1 d_{11} + n_2 d_{21} + \mathrm{tr}(\alpha_{21}^t f \alpha_{11}) \\ n_2' &= n_1 d_{12} + n_2 d_{22} + \mathrm{tr}(\alpha_{12}^t f \alpha_{22}) \\ f' &= n_1 \alpha_{12}^t \alpha_{11} + n_2 \alpha_{22}^t \alpha_{21} + \alpha_{12}^t f^t \alpha_{21} + \alpha_{22}^t f \alpha_{11} \end{aligned}$$

where $\mathrm{tr}(h) \in \mathbb{Z}$ *is defined by* $[\mathrm{tr}(h)] = h + h^t$*, for* $h \in \mathrm{End}(E_i')$*.*

Proof. To prove (75), consider $\tilde{\alpha} := r_{\lambda_1 \otimes \lambda_2}(\alpha)\alpha$. Since $\deg(r_{\lambda_1 \otimes \lambda_2}(\alpha)) = \deg(\hat{\alpha}) = \deg(\alpha)$, we have $\deg(\alpha)^2 = \deg(\tilde{\alpha})$. Now by (69) we have $\tilde{\alpha} = \left(\begin{smallmatrix} \alpha_{11}' & \alpha_{21}' \\ \alpha_{12}' & \alpha_{22}' \end{smallmatrix}\right)\left(\begin{smallmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{smallmatrix}\right) = \mu([d_1], [d_2], f_\alpha)$, where $d_1 = d_{11} + d_{21}$ and $d_2 = d_{12} + d_{22}$, and so $4\deg(\alpha)^2 = 4\deg(\mu([d_1], [d_2], f_\alpha) = (\mathbf{D}(d_1, d_2, f_\alpha)^2)^2$, where the latter equality follows from the Riemann-Roch Theorem (cf. [37], p. 150) because $\mu([a], [b], f) = \Phi_{\lambda_1 \otimes \lambda_1}(\mathbf{D}(a, b, f))$. From this (75) follows immediately by using (72).

To prove (76) and (77), note first that there exist unique n_1', n_2' and f' such that (76) holds. Then $\Phi_{\lambda_1' \otimes \lambda_2'}(\mathbf{D}(n_1', n_2', f'))$ equals the left hand side of (77), where λ_i' denotes the canonical polarization of E_i'. On the other hand, by (a slight generalization of) formula (69), the right hand side of (77) equals $r_{\lambda_1' \otimes \lambda_2', \lambda_1 \otimes \lambda_2}(\alpha)\Phi_{\lambda_1 \otimes \lambda_2}(\mathbf{D}(n_1, n_2, f))\alpha$. Since this equals $\Phi_{\lambda_1' \otimes \lambda_2'}(\alpha^* \mathbf{D}(n_1, n_2, f))$ by (61), we see that (77) holds. The last assertion follows from this by multiplying out the right side of (77).

Corollary 65 *Let* $g \in M_2(\mathbb{Z})$ *be a* 2×2 *matrix and let* $[g]_E \in \mathrm{End}(E \times E)$ *be the endomorphism induced by* g*. Then* $\deg([g]_E) = \det(g)^2$*.*

Proof. Write $g = (a_{ij})$, and apply (75) to $\alpha = [g]_E = ([a_{ij}]_E)$. Here $d_{ij} = \deg([a_{ij}]_E) = a_{ij}^2$, and $\deg(f_\alpha) = \deg([a_{12}a_{11} + a_{22}a_{21}]) = (a_{12}a_{11} + a_{22}a_{21})^2$. Thus $\deg(\alpha) = |(a_{11}^2 + a_{21}^2)(a_{12}^2 + a_{22}^2) - (a_{12}a_{11} + a_{22}a_{21})^2| = |(a_{11}a_{22} - a_{12}a_{21})^2| = \det(g)^2$.

References

[1] A. Atkin, J. Lehner, Hecke operators on $\Gamma_0(m)$. *Math. Ann.* **185** (1970), 134-160.

[2] D. Buell, *Binary Quadratic Forms.* Springer-Verlag, New York, 1989.

[3] S. Chowla, An extension of Heilbronn's class-number theorem. *Quart. J. Math.* **5** (1934), 304–307.

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

[5] P. Deligne, M. Rapoport, Les schémas de modules de courbes elliptiques. In: *Modular functions of one variable II*, Lecture Notes in Math. 349, Springer-Verlag, Berlin, 1973, pp. 143–316.

[6] L. Dickson, *Introduction to the Theory of Numbers.* U of Chicago Press, Chicago, 1929.

[7] C. Earle, The genus two Jacobians that are isomorphic to a product of elliptic curves. In: *The Geometry of Riemann Surfaces and Abelian Varieties*. Contemp. Math. 397, AMS, Providence, RI, 2006, pp. 27–36.

[8] D. Estes, G. Pall, Spinor genera of binary quadratic forms. *J. Number Theory* **5** (1973), 421–432.

[9] G. Frei, Euler's convenient numbers. *Math. Intell.* **7** No. 3 (1985), 55–58 and 64.

[10] G. Frey, E. Kani, Curves of genus 2 with elliptic differentials and associated Hurwitz spaces. In: *Arithmetic, Geometry, Cryptography and Coding Theory* (G. Lachaud, C. Ritzenthaler, M. Tsfasman, eds.) *Contemp. Math.* **487** (2009), 33–81.

[11] W. Fulton, *Intersection Theory*. Springer-Verlag, Berlin, 1984.

[12] C.F. Gauss, *Untersuchungen über die höhere Arithmetik.* (Translation of *Disquisitiones Arithmeticae*). Chelsea Reprint, New York, 1981.

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

[14] N. Hall, Binary quadratic discriminants with a single class in each genus. *Math. Z.* **44** (1938), 85–90.

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

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

[17] 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.

[18] G. Humbert, Sur les fonctions abéliennes singulières. I. *J. de Math.* (ser. 5) **5** (1899), 233–350 = Œuvres, Gauthier-Villars et Cie., Paris, 1929, pp. 297–401.

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

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

[21] B. Jones, *The Arithmetic Theory of Quadratic Forms*. Carus Monographs No. 10, MAA, 1967.

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

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

[24] E. Kani, Idoneal numbers and some generalizations. *Ann. Sci. Math. Québec* **35** (2011), 197-227.

[25] E. Kani, Generalized Humbert Varieties and intersections of Humbert surfaces. In preparation.

[26] N. Katz, B. Mazur, *Arithmetic Moduli of Elliptic Curves*. Princeton University Press, Princeton, NJ, 1985.

[27] A. Krazer, *Lehrbuch der Thetafunktionen*. Leipzig, 1903; Chelsea Reprint, New York, 1970.

[28] S. Lang, *Elliptic Functions*. Addison-Wesley, Reading, MA, 1972.

[29] H. Lange, Produkte elliptischer Kurven. *Nachr. Akad. Wiss. Göttingen* Math.-Phys. Kl. II 1975, no. 8, 95–108.

[30] H. Lange, Principal polarizations on products of elliptic curves. In: *The Geometry of Riemann Surfaces and Abelian Varieties*. Contemp. Math. 397, AMS, Providence, RI, 2006, pp. 153–162.

[31] B. Mazur, Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.* **47** (1977), 33 – 186.

[32] C. McMullen, Teichmüller curves in genus 2: discriminant and spin. *Math. Ann.* **333** (2005), 87–130.

[33] C. McMullen, Dynamics of $\mathrm{SL}_2(\mathbb{R})$ over moduli space in genus two. *Ann. Math.* **165** (2007), 397–456.

[34] J.S. Milne, Abelian varieties. In: *Arithmetic Geometry.* (G. Cornell, J. Silverman, eds.), Springer-Verlag, New York, 1986; pp. 103–150.

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

[36] D. Mumford, *Geometric Invariant Theory.* Springer-Verlag, Berlin, 1965.

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

[38] F. Oort, J. Steenbrink, The local Torelli problem for algebraic curves. *Journées de Géometrie Algébrique d'Angers, Juillet 1979/Algebraic Geometry, Angers, 1979*, Sijthoff & Noordhoff, Alphen aan den Rijn—Germantown, Md., 1980; pp. 157–204.

[39] G. van der Geer, *Hilbert Modular Surfaces*. Springer-Verlag, Berlin, 1988.

[40] G.L. Watson, One-class genera of positive quadratic forms in seven variables. *Proc. London Math. Soc.* (3) **48** (1984), 175–192.

[41] A. Weil, Zum Beweis des Torellischen Satzes. *Nachr. Ges. Wiss. Göttingen, Math.-Phys. Klasse* 1957, = Œuvres II, pp. 307–327.

[42] A. Weil, *Number Theory: An Approach through History. From Hammurapi to Legendre*. Birkhäuser, Boston, 1983.

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