Elliptic Subcovers of a Curve of Genus 2 II. The Refined Humbert Invariant

Ernst Kani

1 Introduction

This paper is a continuation of the article [6] whose aim is to study of the set $\mathcal{E}(C)$ of all equivalence classes of elliptic subcovers of a given smooth, projective, geometrically irreducible curve C/K of genus 2 over an arbitrary field K. By what was explained in [6], there is a natural bijection between the set $\mathcal{E}(C)$ and the set of primitive representations of squares by a certain quadratic form q_C called the *refined Humbert invariant*; cf. [6], Theorem 20.

The main objective of this paper is to present a method for computing q_C. As in [6], this method depends on the knowledge of a *presentation* (E, E', ψ) *of degree* N of C/K (which arises from a given elliptic subcover $f : C \to E$ of degree N). This triple consists of two elliptic curves E/K and E'/K and an isomorphism $\psi : E_1[N] \to E_2[N]$ which is an anti-isometry with respect to the e_N-pairings; cf. [6], Section 2.

As was shown [6], the discriminant of the quadratic form q_C can be determined from the N-presentation (E, E', ψ); cf. [6], Theorem 3. Moreover, in the case that $\operatorname{rank}(\operatorname{Hom}(E, E')) = 1$, then q_C has extra structure which is encapsulated in the following definition.

Definition. Let N, m, d be positive integers. An integral binary quadratic form q is said to be *of type* (N, m, d) if it is positive-definite and satisfies the following properties:

(i) $\operatorname{disc}(q_C) = -16m^2d$, and $m|N$ with $\gcd(N/m, d) = 1$.

(ii) q_C primitively represents N^2;

(iii) $q_C(X, Y) \equiv 0, 1 \pmod 4$, for all $X, Y \in \mathbb{Z}$.

Such quadratic forms are studied in some detail in Section 2. They are important in the study of q_C due to the following result which is Theorem 2 of [6].

Theorem 1 *Suppose that C/K is a curve which has a presentation (E, E', ψ) of degree N with $\operatorname{char}(K) \nmid N$. If $\operatorname{Hom}(E, E') = \mathbb{Z}h$, where $d := \deg(h) \geq 1$, then the refined Humbert invariant q_C is a binary quadratic form of type (N, m, d), where $m = m_\psi$ is the* isogeny defect *of ψ which is defined by*

$$m_\psi := \min\{m \geq 1 : m\psi = f_{|E[N]}, \ \text{for some } f \in \operatorname{Hom}(E, E')\}.$$

In addition, q_C satisfies the condition

(iv) $q_C(X, Y) \neq 1$, *for all $X, Y \in \mathbb{Z}$.*

Here we make this theorem more precise by giving an explicit formula for m_ψ and for q_C. More precisely, Proposition 28 and Remark 29 imply the following result.

Theorem 2 *In the situation of* Theorem 1*, there exists a primitive matrix M of determinant $-d$ such that $M \pmod N$ is the matrix of $\psi^{-1}h_{|E[N]} \in \mathrm{End}(E[N])$ with respect to some basis of $E[N](\overline{K})$. For any such matrix $M = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$ we have*

$$m_\psi \;=\; m := N/\bar{N}, \quad \textit{where} \quad \bar{N} := \gcd(x-w, y, z, N),$$

and the refined Humbert invariant q_C is equivalent to the integral binary quadratic form

$$q_{M,N}(X,Y) := N^2X^2 - 2m\,\mathrm{tr}(M)XY + \tfrac{m^2}{N^2}(\mathrm{tr}(M)^2 + 4d)Y^2.$$

Now it turns out that every binary form of type (N, m, d) is equivalent to a form $q_{M,N}$, for a suitable primitive matrix M of determinant $-d$; cf. Theorem 16. By combining this result with Theorem 2, we obtain as a consequence that every such form of type (N, m, d) satisfying property (iv) is (equivalent to) the refined Humbert invariant q_C of some curve C/K.

Theorem 3 *If K is an algebraically closed field of characteristic* 0*, then for each positive binary quadratic form q of type (N, m, d) which satisfies properties* (iv) *of* Theorem 1 *there exists a curve C/K such that its refined Humbert invariant q_C is equivalent to q.*

This theorem is actually a special case of the more general existence results of Section 5; cf. Theorem 32 and its corollaries.

In the last section we apply the above theory to study curves C/K of genus 2 which have an elliptic subcover of degree 2. This is equivalent to the condition that C has an *elliptic involution*; cf. Proposition 35. Using the above results, we prove the following characterization of curves whose automorphism group contains a certain dihedral group D_n of order $2n$.

Theorem 4 *Let C/K be a curve of genus* 2 *where* $\mathrm{char}(K) \neq 2, 3$*. Then:*

(a) $\mathrm{Aut}(C)$ *contains a subgroup isomorphic to the dihedral group D_4 (respectively, to D_6) if and only if the refined Humbert invariant q_C primitively represents the binary quadratic form $q_4(X,Y) = 4X^2 + 4Y^2$ (respectively, the form $q_6(X,Y) = 4X^2 + 4XY + 4Y^2$).*

(b) *If the conditions of part* (a) *hold, then C/K has an elliptic subcover of degree N whenever $N = 2N_1$, where $N_1 = 1$ or N_1 is a product of primes p_i with $p_i \equiv 1 \pmod 4$ (respectively, with $p_i \equiv 1 \pmod 3$).*

(c) *If the conditions of part* (a) *hold, and if also* $\mathrm{End}(E) = \mathbb{Z}$*, for some elliptic subcover $f : C \to E$, then q_C is equivalent to q_4 (respectively, to q_6). Then C/K has*

an elliptic subcover of degree N if and only if $N = 2N_1$, where $N_1 = 1$ or N_1 is a product of primes p_i with $p_i \equiv 1 \pmod 4$ (respectively, with $p_i \equiv 1 \pmod 3$).

Moreover, if N is of this form, then C/K has precisely $2^{\omega(N)+1}$ (respectively, $2^{\omega(N)+1} \cdot 3$) such subcovers of degree N, where $\omega(N)$ denotes the number of distinct prime factors of N.

Some examples of curves C/K which satisfy the hypotheses of Theorem 4(c) are the *Legendre curves*

$$y^2 \;=\; x(x^2 - a)(x^2 - a^{-1})$$

with $a \in \mathbb{Z}$, $a \neq 0 \pm 1, \pm 3$ and $K \supset \mathbb{Q}(i)$, as is explained in Example 46. Thus, for $N \leq 150$, these curves have an elliptic subcover of degree N if and only if $N =$ 2, 10, 26, 34, 50, 58, 74, 82, 106, 122, 130, or 146. We also investigate the case $a = 3$ in some detail; cf. Proposition 48.

This paper is organized as follows. In Section 2 we study the basic properties of binary quadratic forms of type (N, m, d). For convenience of the reader, we recall in Section 3 the basic notation and results of [6], which are then used in Section 4 to prove Theorem 2 and other results. In Section 5 we prove the existence theorems and in the last section we apply Theorem 2 to study elliptic involutions and to compute some explicit examples; cf. Theorem 4 and Example 46.

Acknowledgment. I would like to thank the referee for the useful comments. In addition, I gratefully acknowledge receipt of funding from the Natural Sciences and Engineering Research Council of Canada (NSERC).

2 Quadratic forms of type (N, m, d)

In this section we analyze the binary quadratic forms which occur in the statement of Theorem 1, i.e., those binary forms q which are positive-definite and satisfy properties (i), (ii) and (iii) of the Introduction. Here, as usual, we use the abbreviation $q = [a, b, c]$ to denote the binary quadratic form $q(X, Y) = aX^2 + bXY + cY^2$. We begin with the following simple observation.

Proposition 5 *Let $q = [a, b, c]$ be an integral binary quadratic form. Then q satisfies property* (iii) *if and only there exist $\bar{a}, \bar{c} \in \{0, 1\}$ such that*

$$q(X, Y) \;\equiv\; (\bar{a}X + \bar{c}Y)^2 \pmod 4, \quad \textit{for all } X, Y \in \mathbb{Z}. \tag{1}$$

Proof. If q satisfies (1), then clearly $q(X, Y) \equiv 0, 1 \pmod 4$, for all $X, Y \in \mathbb{Z}$, so condition (iii) holds.

Conversely, suppose that $q = [a, b, c]$ satisfies condition (iii). Then $a = q(1, 0) \equiv \bar{a} \equiv \bar{a}^2 \pmod 4$ with $\bar{a} \in \{0, 1\}$ and similarly $c = q(0, 1) \equiv \bar{c} \equiv \bar{c}^2$ with $\bar{c} \in \{0, 1\}$. Moreover, $a \pm b + c = q(1, \pm 1) \equiv 0, 1 \pmod 4$.

If $\bar{a} = \bar{c} = 0$, then the last two conditions imply that $b \equiv 0 \pmod 4$, so (1) holds in this case. If $\bar{a} = \bar{c} = 1$, then we must have $b \equiv 2 \pmod 4$, so again (1) holds. Finally, if $\bar{a} = 1$ and $\bar{c} = 0$ (or vice versa), then $b \equiv 0 \pmod 4$, and so (1) holds in all cases. $\square$

Corollary 6 *If q satisfies property* (iii)*, then* $16|\mathrm{disc}(q)$.

Proof. By the proposition, we have 4 cases to consider. If $\bar{a} = \bar{c} = 0$, then $q \equiv [0,0,0] \pmod 4$, so $q = [4a, 4b, 4c]$ with $a, b, c \in \mathbb{Z}$ and hence $\mathrm{disc}(q) = 16(b^2 - 4ac)$. Next, if $\bar{a} = 1$ and $\bar{c} = 0$, then $q = [1 + 4a, 4b, 4c]$ with $a, b, c \in \mathbb{Z}$ and so $\mathrm{disc}(q) = 16(b^2 - a - ac)$. Similarly, if $\bar{a} = 0$ and $\bar{c} = 1$, then $q = [4a, 4b, 1+4c]$ with $a, b, c \in \mathbb{Z}$ and so $\mathrm{disc}(q) = 16(b^2 - c - ac)$. Finally, if $\bar{a} = 1$ and $\bar{c} = 1$, then $q = [1+4a, 2+4b, 1+4c]$ with $a, b, c \in \mathbb{Z}$ and so $\mathrm{disc}(q) = (2+4b)^2 - 4(1+4a)(1+4c) = 16(b^2 + b - a - c - 4ac)$. $\square$

We next observe that property (i) is a consequence of properties (ii) and (iii). More precisely:

Proposition 7 *Let q be a positive binary quadratic form which primitively represents N^2 for some $N \geq 1$. If q satisfies property* (iii) *of* Theorem 1*, then there exist unique integers $m, d \geq 1$ with $m|N$ such that*

$$\mathrm{disc}(q) \;=\; -16m^2 d, \quad \textit{and} \quad \gcd(N/m, d) = 1. \tag{2}$$

Proof. We first observe that m and d are uniquely determined by the condition (2) (and by N) because (2) implies that $\gcd((N/m)^2, \mathrm{disc}(q)/(16m^2)) = 1$ and that hence $\gcd(N^2, \mathrm{disc}(q)/16) \;=\; m^2$.

To prove that there exist m and d satisfying (2), it suffices to verify that $M := \gcd(N^2, \mathrm{disc}(q)/16)$ is a square, for then $m = \sqrt{M}$ and $d = -\mathrm{disc}(q)/16m^2$ satisfy (2). (Note that $\mathrm{disc}(q)/16 \in \mathbb{Z}$ by Corollary 6 and that $\mathrm{disc}(q) < 0$ because q is positive-definite.)

For this, we observe that the first hypothesis implies that q is equivalent to the form $q' = [N^2, B, c]$, where $b, c \in \mathbb{Z}$. Since $16|\mathrm{disc}(q') = \mathrm{disc}(q)$ by Corollary 6, we see that $B = 2b$ is even. Thus, $M = \gcd(N^2, (b^2 - N^2 c)/4)$.

If N is odd, then $M = \gcd(N^2, b^2 - N^2 c) = \gcd(N, b)^2$ is a square. Thus, assume that N is even. Since q satisfies property (iii), we must have that $B = 4b_1$ by Proposition 5. If $2|c$, then $c = 4c_1$ by Proposition 5 and so $M = \gcd(N^2, b_1^2 - N^2 c_1) = \gcd(N, b_1)^2$. Thus, assume that c is odd, so $c \equiv 1 \pmod 4$ by (iii).

Write $N = 2^r N_0$ and $b = 2^s b_0$, where $N_0 b_0$ is odd. If $r = s$, then $2^{-2r}(b^2 - N^2 c) = b_0^2 - N_0^2 c \equiv 1 - 1 \cdot 1 \equiv 0 \pmod 4$. Thus $b^2 - N^2 c = 2^{2r+2} c_0$, where $c_0 \in \mathbb{Z}$, and so $M = 2^{2r} \gcd(N_0^2, c_0) = 2^{2r} \gcd(N_0, b_0^2 - N_0^2 c) = \gcd(N, b)^2$. If $r < s$, then $b^2 - N^2 c = 2^{2r} d_1$, where $d_1 = 2^{2s-2r} b_0^2 - N_0^2 c$ is odd, and so $M = 2^{2r-2} \gcd(4N_0^2, d_1) = 2^{2r-2} \gcd(N_0^2, b_0^2) = \frac{1}{4} \gcd(N, b)^2$. Finally, if $r > s$, then $b^2 - N^2 c = 2^{2s} d_2$, where $d_2 =$

$b_0^2 - 2^{2r-2s}N_0^2 c$ is odd, and so $M = 2^{2s-2}\gcd(2^{2r-2s-2}N_0^2, d_2) = 2^{2s-2}\gcd(N_0^2, b_0^2) = \frac{1}{4}\gcd(N,b)^2$. Thus, M is a square in all cases, as claimed. □

We next study the *existence* of binary forms of type (N,m,d). For this, let

$$Q(N,m,d) := \{[a,b,c] \in \mathbb{Z}^3 : q = [a,b,c] \text{ is a form of type } (N,m,d)\}.$$

Proposition 8 *If N, m, d are positive integers with $m|N$ and $\gcd(N/m, d) = 1$, then*

$$Q(N,m,d) \neq \emptyset \quad \Leftrightarrow \quad -d \equiv x^2 \pmod{N/m}, \text{ for some } x \in \mathbb{Z}. \tag{3}$$

As we shall see below, this result follows from the following more precise assertions.

Lemma 9 *If $q \in Q(N,m,d)$ is a quadratic form of type (N,m,d), then q is $\mathrm{SL}_2(\mathbb{Z})$-equivalent to $q' = [N^2, 2mb, c]$, for some $b, c \in \mathbb{Z}$ where $c = \frac{m^2}{N^2}(b^2+4d)$. Moreover, if $b_1 \equiv b \pmod{\frac{N^2}{m}}$, and $c_1 = \frac{m^2}{N^2}(b_1^2+4d)$, then $[N^2, 2mb_1, c_1]$ is $\mathrm{SL}_2(\mathbb{Z})$-equivalent to q'.*

Proof. It follows from condition (ii) that q is $\mathrm{SL}_2(\mathbb{Z})$-equivalent to $q' = [N^2, B, c]$, where $B, c \in \mathbb{Z}$. Put $\bar{N} = \frac{N}{m}$. Since $B^2 - 4m^2\bar{N}^2 c = \mathrm{disc}(q') = -16dm^2$ by condition (i), we see that $4m^2|B^2$, so $B = 2mb$, for some $b \in \mathbb{Z}$, and hence $q' = [N^2, 2mb, c]$. Moreover, from above we have that $c = \frac{B^2+16dm^2}{4N^2} = \frac{m^2}{N^2}(b^2+4d)$, as claimed. Finally, if $b' = b + s\frac{N^2}{m}$, then the matrix $M = \left(\begin{smallmatrix} 1 & s \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ transforms q' into $[N^2, 2mb_1, c_1]$. □

Lemma 10 *In the situation of* Proposition 8*, suppose that $k \in \mathbb{Z}$ satisfies $k^2 d \equiv -1 \pmod{\bar{N}}$, where $\bar{N} = \frac{N}{m}$. Then $n := (k^2d+1)/\bar{N} \in \mathbb{Z}$, and for any $r \in \mathbb{Z}$ the form*

$$q_{N,m,d,k,r} := [N^2, 2m(k(t-d) + r\bar{N}^2), n^2 t + 2k(t-d)r + r^2\bar{N}^2], \text{ where } t = d(\bar{N}n + 3),$$

is a binary form of type (N,m,d), i.e., $q_{N,m,d,k,r} \in Q(N,m,d)$.

Proof. It is clear from the hypothesis on k that $n \in \mathbb{Z}$. Put $q_{\bar{N},n,k} := [\bar{N}^2, 2k(t-d), n^2 t]$. Since $n\bar{N} - k^2 d = 1$, we have that $(\bar{N}, n, k) \in P(d)$ in the notation of [4], §5, so Theorem 13 of [4] shows that $q_{\bar{N},n,k}$ is a binary quadratic form of type d in the sense of [4]. This means in particular that property (iii) holds for $q_{\bar{N},n,k}$ and that $\mathrm{disc}(q_{\bar{N},n,k}) = -16d$. Now since

$$q_{N,m,d,k,r}(X,Y) \;=\; q_{\bar{N},n,k}(mX + rY, Y), \tag{4}$$

we thus see that property (iii) also holds for $q_{N,m,d,k,r}$. Moreover, property (ii) clearly holds because $q_{N,m,d,k,r}(1,0) = N^2$. Finally, since $\mathrm{disc}(q_{\bar{N},n,k}) = -16d$ and since $q := q_{N,m,d,k,r}$ is the transform of $q_{\bar{N},n,k}$ by the matrix $M = \left(\begin{smallmatrix} m & r \\ 0 & 1 \end{smallmatrix}\right)$, it follows that $\mathrm{disc}(q) = \mathrm{disc}(q_{\bar{N},n,k})\det(M)^2 = -16m^2 d$. Thus, property (i) holds for q, and so q has type (N,m,d). □

Proof of Proposition 8. If $-d \equiv x^2 \pmod{\bar{N}}$, where $\bar{N} = \frac{N}{m}$, then $\exists k \in \mathbb{Z}$ such that $kx \equiv 1 \pmod{\bar{N}}$ because $\gcd(d, \bar{N}) = 1$, and so $k^2 d \equiv -1 \pmod{\bar{N}}$. Thus $Q(N, m, d) \neq \emptyset$ by Lemma 10.

Conversely, suppose that $q \in Q(N, m, d)$. Since properties (i), (ii) and (iii) are stable under $\mathrm{GL}_2(\mathbb{Z})$-equivalence of forms, so is the set $Q(N, m, d)$. Thus, by Lemma 9 we may assume that $q = [N^2, 2mb, c] \in Q(N, m, d)$, for some $b, c \in \mathbb{Z}$ with $b^2 + 4d = c\bar{N}^2 \equiv 0 \pmod{\bar{N}^2}$, where $\bar{N} = \frac{N}{m}$. If $\bar{N}$ is odd, then there exists $y \in \mathbb{Z}$ such that $2y \equiv 1 \pmod{\bar{N}}$, and so $(by)^2 \equiv -d \pmod{\bar{N}}$. Thus, the right hand side of (3) holds with $x = by$. Next, suppose that $\bar{N}$ is even, so also $b = 2b_1$ is even. If c is even, then $b_1^2 + d = \frac{c\bar{N}}{4}\bar{N} \equiv 0 \pmod{\bar{N}}$, so we can take $x = b_1$. On the other hand, if c is odd, then $(c+1)\bar{N} \equiv 0 \pmod 4$ and then $(b_1 + \frac{\bar{N}}{2})^2 + d = b_1\bar{N} + \frac{(c+1)\bar{N}}{4}\bar{N} \equiv 0 \pmod{\bar{N}}$, so we can take $x = b_1 + \frac{\bar{N}}{2}$. □

The above Lemma 10 constitutes the first *construction principle* for forms of type (N, m, d). We now give another construction of such forms by using integral 2×2 matrices.

Proposition 11 *Let N and d be positive integers and let $M = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in M_2(\mathbb{Z})$ be an integral matrix such that $\det(M) \equiv -d \pmod{N}$. Assume that M is N-*primitive*, i.e., that $\gcd(x, y, z, w, N) = 1$. Put*

$$g \;=\; g_{M,N} := \gcd(x - w, y, z, N) \quad \textit{and} \quad m := N/g. \tag{5}$$

Then there is an integer k such that $kx \equiv 1 \pmod{g}$. Fix such a k and consider

$$q_{M,N,d,k} := [N^2, 2mT, (T^2 + 4d)/g^2], \quad \textit{where } T := -\mathrm{tr}(M) - dk^3(\det(M) + d). \tag{6}$$

Then $q_{M,N,d,k}$ is a form of type (N, m, d); in fact, we have that

$$q_{M,N,d,k} \;=\; q_{N,m,d,k,r}, \tag{7}$$

where r is determined as follows. Put $\bar{x} = (kx - 1)/g$ and $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, so

$$kM \;=\; I + gM_1, \quad \textit{where } M_1 := \bar{x}I + kM_0 \;\; \textit{and} \;\; M_0 := (M - xI)/g, \tag{8}$$

are integral matrices. Then $n := (k^2 d + 1)/g$ and $b := (x + kd)/g$ are integers, and (7) *holds with*

$$r := -kd\det(M_1) - n(2b + \mathrm{tr}(M_0)). \tag{9}$$

Proof. Since $\gcd(x, g) = \gcd(x, y, z, w, N) = 1$, there is a $k \in \mathbb{Z}$ such that $kx \equiv 1 \pmod{g}$. Thus $\bar{x} = (kx - 1)/g \in \mathbb{Z}$, and $kM = kxI + gkM_0 = I + g(\bar{x}I + kM_0)$, which proves (8). Note that $M_0 \in M_2(\mathbb{Z})$ by the definition of g.

To show that $q_{M,N,d,k} \in Q(N,m,d)$, it suffices in view of Lemma 10 to verify that $k^2 d \equiv -1 \pmod{g}$ and that (7) holds.

For this, put $\delta = \det(M)$, so $a := (\delta + d)/N \in \mathbb{Z}$ by our hypothesis on d. Moreover, put $n_1 := ak^2 m - \tau_1 - g\delta_1 \in \mathbb{Z}$, where $\tau_1 = \mathrm{tr}(M_1)$ and $\delta_1 = \det(M_1)$. Since $k^2\delta = \det(kM) = \det(I + gM_1) = 1 + \tau_1 g + \delta_1 g^2$, we have $gn_1 = k^2(\delta + d) - \tau_1 g - \delta_1 g^2 = k^2 d + 1 = gn$, and so $n = n_1 \in \mathbb{Z}$. Moreover, $b \in \mathbb{Z}$ because by the definition of $\bar{x}$ and n we have that $g(xn - \bar{x}kd) = xng - (kx-1)kd = x(ng - k^2 d) = kd = x + kd = bg$, so $b = xn - \bar{x}kd \in \mathbb{Z}$.

To prove (7), note first that $q_{N,m,d,k,r}$ is defined because $k^2 d = -1 + gn \equiv -1 \pmod{g}$. Thus, $q_{N,m,d,k,d} = [N^2, 2mT_1, T_2]$, where $T_1 = k(t-d) + rg^2$ and $T_2 = n^2 t + 2k(t-d)r + g^2 r^2$ and $t = d(ng+3)$. Note that since $q_{N,m,d,k,r}$ has type (N,m,d) by Lemma 10, we see that $T_2 = (T_1^2 + 4d)/g^2$; cf. Lemma 9. Thus, (7) follows once we have shown that $T = T_1$.

For this, put $\tau_0 := \mathrm{tr}(M_0)$. Then with r as in (9) we have

$$
\begin{aligned}
(10) \qquad rg^2 &= -g(-k^3 dam + kd(2\bar{x} - n) - 2nx - \tau_0) \\
&= -k^3 daN - kd(gn+2) - \mathrm{tr}(M).
\end{aligned}
$$

Indeed, the first equality can be derived from (9) by using the fact that $g\delta_1 = ak^2 m - \tau_1 - n = -(-ak^2 m + n + 2\bar{x} + k\tau_0)$, which is a variant of the definition of $n_1 = n$, together with the fact that $gn - k^2 d = 1$, and the second follows from the first by using that $g\bar{x} = kx - 1$ and $\mathrm{tr}(M) = 2x + g\tau_0$ and by using the identity $gn - k^2 d = 1$ again.

Since $k(t-d) = kd(gn+2)$, it is clear from the definition of T that (10) shows that $T_1 = T$. This proves (7). □

Corollary 12 *If $M \in M_2(\mathbb{Z})$ is an N-primitive matrix of determinant $-d$, and if $m = N/g$, where $g = g_{M,N}$, then $q_{M,N} := [N^2, -2m\mathrm{tr}(M), (\mathrm{tr}(M)^2 + 4d)/g^2]$ is a form of type (N,m,d).*

Proof. Clearly, M satisfies the hypotheses of Proposition 11. The extra hypothesis on M implies that $T = -\mathrm{tr}(M)$, so $q_{M,N} = q_{M,N,d,k}$, for any k as in Proposition 11. □

We note in passing that the quadratic form $q_{M,N}$ only depends on the $\mathrm{SL}_2(\mathbb{Z})$-conjugacy class of M.

Corollary 13 *If M is an integral matrix and if $M' = P^{-1}MP$, where $P \in \mathrm{SL}_2(\mathbb{Z})$, then for every $N \geq 1$ we have $g_{M',N} = g_{M,N}$. Thus, if M is N-primitive and if $\det(M) = -d$, then $q_{M',N} = q_{M,N}$.*

Proof. Write $M = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$, and put $g = g_{M,N}$. Then as above $M = xI + gM_0$, where $M_0 = \left(\begin{smallmatrix} 0 & \bar{y} \\ \bar{z} & \bar{w} \end{smallmatrix}\right)$. Write $M' = \left(\begin{smallmatrix} x' & y' \\ z' & w' \end{smallmatrix}\right)$. Then $M' = xI + gM_0'$, where $M_0' = P^{-1}M_0P =$

$\left(\begin{smallmatrix}\bar{x}' & \bar{y}'\\ \bar{z}' & \bar{w}'\end{smallmatrix}\right) \in M_2(\mathbb{Z})$. Thus $x' = x + g\bar{x}'$ and $w' = x + g\bar{w}'$, so $w' = x' + g\bar{w}''$ with $\bar{w}'' = \bar{w}' - \bar{x}'$. This means that $M' = x'I + g\left(\begin{smallmatrix}0 & \bar{y}'\\ \bar{z}' & \bar{w}''\end{smallmatrix}\right)$, and so $g|\gcd(x'-w', y', z', N) = g_{M',N}$. This shows that $g_{M,N}|g_{M',N}$. But since $M' = PMP^{-1}$, a similar argument shows that also $g_{M',N}|g_{M,N}$, so $g_{M,N} = g_{M',N}$. Moreover, if M is N-primitive, then so is M' and hence $q_{M',N} = q_{M,N}$ because $\mathrm{tr}(M') = \mathrm{tr}(M)$ and $\det(M') = \det(M)$. □

We next observe that the equivalence class of the quadratic form $q_{M,N,d,k}$ only depends on the congruence class mod N of the matrix M. More precisely:

Proposition 14 *If M' is an integral matrix with $M' \equiv M \pmod N$, where M is as in* Proposition 11, *and if $k' \equiv k \pmod g$, where $g = g_{M,N} = g_{M',N}$, then the form $q_{M,N,d,k}$ is $\mathrm{SL}_2(\mathbb{Z})$-equivalent to $q_{M',N,d,k'}$.*

Proof. First note that since $\det(M) + d \equiv 0 \pmod N$, and $k' \equiv k \pmod g$, it follows that $dk^3(\det(M) + d) + \mathrm{tr}(M) \equiv d(k')^3(\det(M) + d) + \mathrm{tr}(M) \pmod{gN}$, and so $q_{M,N,d,k} \sim q_{M,N,d,k'}$ by Lemma 9, where $\sim$ denotes $\mathrm{SL}_2(\mathbb{Z})$-equivalence.

Next, consider $M'\left(\begin{smallmatrix}x' & y'\\ z' & w'\end{smallmatrix}\right)$. Since $M' \equiv M \pmod N$, it is clear from (5) that $g_{M',N} = g_{M,N} = g$ and that $\det(M') \equiv \det(M) \equiv -d \pmod N$. Moreover, since $x' \equiv x \pmod N$, we see that $kx' \equiv kx \pmod N$, so $kx' \equiv 1 \pmod g$ and hence $q_{M',N,d,k}$ is defined.

Moreover, we observe that $M_0' := (M' - x'I)/g \equiv M_0 \pmod m$ and that $\bar{x}' := (kx' - 1)/g \equiv \bar{x} \pmod m$. Thus, $M_1' := \bar{x}'I + kM_0' \equiv M_1 \pmod m$. Since $b' := (x'+kd)/g \equiv b \pmod m$, we see that $r' := -kd\det(M_1') - n(2b' + \mathrm{tr}(M_0')) \equiv r \pmod m$, and so $T_1' := k(t-d) + r'g^2 \equiv T_1 \pmod{mg^2}$. Since $mg^2 = N^2/m$, this implies by Lemma 9 that $q_{N,m,d,k,r'} \sim q_{N,m,d,k,r}$, and so $q_{M',N,d,k} \sim q_{M,N,d,k}$ by (7). Moreover, by replacing k by k' in the above argument we see that $q_{M',N,d,k'} \sim q_{M,N,d,k'}$. Combining the above equivalences shows that $q_{M,N,d,k} \sim q_{M,N,d,k'} \sim q_{M',N,d,k'}$, as claimed. □

We next show that every form of type (N, m, d) is equivalent to a form $q_{M,N}$, for a suitable integral matrix M of determinant $-d$.

Proposition 15 *If $q = [N^2, 2mb, c]$ has type (N, m, d), then there is a primitive matrix M of discriminant $-d$ such that $q = q_{M,N}$.*

Proof. Put $\bar{N} = \frac{N}{m}$ and $g = \gcd(2, \bar{N})$. Since $-4d = b^2 - \bar{N}c$, we see that $b_1 := \frac{b}{g} \in \mathbb{Z}$. Moreover, since $\gcd(d, \bar{N}) = 1$ by property (i), we see that $\gcd(2d, \bar{N}^2) = \gcd(2, \bar{N}^2) = g$, so there exist integers α, β such that

$$2d\alpha \;-\; \beta\bar{N}^2 \;=\; g. \tag{11}$$

Note that $\gcd(\alpha d, g) = 1$ because $\alpha d(\frac{2}{g}) \;-\; g\beta(\frac{\bar{N}}{g})^2 = 1$, so $\alpha \equiv 1 \pmod 2$ if $g \neq 1$ and hence $\alpha^2 \equiv 1 \pmod{g^2}$ (for any g).

By property (iii) we know that $c = q(0,1) \equiv C \pmod 4$, for some $C \in \{0,1\}$, and so also $C = C^2 \equiv c \pmod{g^2}$. Since $\bar{N} \equiv 2 \equiv 0 \pmod g$, we see that $c_1 := \alpha\beta b_1^2 g^2 + 2g\beta + \beta^2\bar{N}^2 - \alpha^2 cd \equiv -cd \pmod{g^2}$ and $c_2 := Cgb_1\bar{N} + C^2 d \equiv cd \pmod{g^2}$. Thus the numbers

$$w_1 := \alpha b_1 + C\bar{N}/g, \quad \bar{w} = \beta b_1 \bar{N} + 2dC/g, \quad \text{and} \quad \bar{z} = (c_1 + c_2)/g^2$$

are all integers, as is $x := \bar{w}\bar{N} - w_1 d$. Put $P = \left(\begin{smallmatrix} x & \bar{N} \\ \bar{z}\bar{N} & w_1 \end{smallmatrix}\right)$. Then, after simplifying, $\det(P) = -(\alpha^2 b_1^2 dg^2 + \bar{N}^4\beta^2 - \bar{N}^2\alpha^2 cd + 2\bar{N}^2\beta g)/g^2$, and so, by using the relation (11) and the fact that $c = (g^2 b_1^2 + 4d)/\bar{N}^2$, it follows that $\det(P) = 1$. Thus $P \in \mathrm{SL}_2(\mathbb{Z})$, and hence $M := \left(\begin{smallmatrix} 1 & 0 \\ 0 & -d \end{smallmatrix}\right) P$ is a primitive matrix of discriminant $-d$.

We have $\mathrm{tr}(M) = x - w_1 d = b_1(\beta\bar{N}^2 - 2\alpha d) = -b_1 g = -b$ by (11). Furthermore, since $x + w_1 d = \bar{w}\bar{N}$, we see that $g_{M,N} = \gcd(\bar{w}\bar{N}, \bar{N}, -d\bar{z}\bar{N}, N) = \bar{N}$, and so $m = N/g_{M,N}$. This shows that $q = q_{M,N}$, as claimed. □

We can summarize the above results in the following way.

Theorem 16 *Let N, m, d be positive integers such that $m|N$ and $\gcd(\bar{N}, d) = 1$, where $\bar{N} = \frac{N}{m}$, and let q be a binary quadratic form. If $\sim$ denotes $\mathrm{SL}_2(\mathbb{Z})$-equivalence of binary quadratic forms, then the following conditions are equivalent.*

(i) *$q \in Q(N, m, d)$.*

(ii) *$q \sim q_{N,m,d,k,r}$, for some $k, r \in \mathbb{Z}$ with $k^2 d \equiv -1 \pmod{\bar{N}}$.*

(iii) *$q \sim q_{M,N,d,k}$, for some N-primitive matrix $M = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$ with $\det(M) \equiv -d \pmod N$ and $g_{M,N} = \bar{N}$ and some $k \in \mathbb{Z}$ such that $kx \equiv 1 \pmod{\bar{N}}$.*

(iv) *$q \sim q_{M,N}$, for some primitive matrix M with $g_{M,N} = \bar{N}$ and $\det(M) = -d$.*

Proof. (i) ⇒ (iv): Lemma 9 and Proposition 15.

(iv) ⇒ (iii): If $M = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$ is as in (iv), then M also satisfies condition (iii). Since $\gcd(x, \bar{N}) = \gcd(x, g_{M,N}) = \gcd(x, y, z, w, N) = 1$, there is a $k \in \mathbb{Z}$ such that $kx \equiv 1 \pmod{\bar{N}}$, and we have $q_{M,N,d,k} = q_{M,N}$. Thus (iii) holds.

(iii) ⇒ (ii): Proposition 11.

(ii) ⇒ (i): By Lemma 10, $q_{N,m,d,k,r} \in Q(N, m, d)$, and so $q \in Q(N, m, d)$ because $Q(N, m, d)$ is stable under $\mathrm{SL}_2(\mathbb{Z})$-equivalence; cf. the proof of Proposition 8. □

Remark 17 Note that Lemma 9 shows that $q_{N,m,d,k,r'} \sim q_{N,m,d,k,r}$, if $r' \equiv r \pmod m$. Thus, in property (ii) we can restrict to r's satisfying the extra condition $0 \le r < m$.

Corollary 18 *Let N and d be positive integers. Then a binary quadratic form q has type (N, N, d) if and only if q is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to $[N^2, 2Nr, r^2 + 4d]$, for some integer r with $0 \le r \le N/2$.*

Proof. Since here $\bar{N} = 1$, we see that $k = 0$ satisfies $k^2 d \equiv -1 \pmod{\bar{N}}$, and so by Theorem 16 we have that $[N^2, 2Nr, r^2 + 4d] = q_{N,N,d,0,r} \in Q(N, N, d)$, for all $r \in \mathbb{Z}$.

Conversely, if $q \in Q(N, N, d)$, then by Theorem 16 there is a matrix M such that $q \sim q_{M,N}$. Since $m = N$, we have that $q_{M,N} = [N^2, -2Nr, r^2 + 4d]$ with $r = \mathrm{tr}(M)$. Moreover, by Remark 17 we see that $q_{M,N} \sim [N^2, 2Nr_1, r_1^2+4d]$, where $r_1 \equiv r \pmod{N}$ and $|r_1| \leq N/2$. Since $[N^2, -2Nr_1, r_1^2+4d]$ is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to $[N^2, 2Nr_1, r_1^2+4d]$, we can replace r_1 by $-r_1$ if necessary to achieve that $r_1 \geq 0$. □

As an example, we can give a complete classification of the forms of type (N, m, d) in the case that $N = 2$.

Proposition 19 *Let q be a binary quadratic form and let $d \geq 1$. Then q has type $(2, 2, d)$ if and only if q is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to one of the forms*

$$[4, 0, 4d] \quad \text{or} \quad [4, 4, 4d + 1], \tag{12}$$

and q has type $(2, 1, d)$ if and only if q is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to one of the forms

$$[4, 4s, d + s], \quad \text{where } d \equiv 1 + 2s \pmod{4} \text{ and } s = 0 \text{ or } 1. \tag{13}$$

Proof. The first assertion follows directly from Corollary 18 because here $\frac{N}{2} = 1$, so $r = 0$ or 1. Thus, assume now that $m = 1$.

It is clear that the forms (13) have discriminant $-16d$ with $\gcd(2, d) = 1$, so property (i) holds for them. Moreover, they satisfy property (ii) since $q(1, 0) = 2^2$ when $q = [4, *, *]$. Finally, since all the forms are congruent to $[0, 0, 1]$ or $[0, 0, 0]]$ (mod 4), it is clear that they all satisfy property (iii). Thus, each is of type $(2, 1, d)$.

Conversely, suppose that $q \in Q(2, 1, d)$. By reduction theory, q is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to $q' = [a, b, c]$ with $0 \leq b \leq a \leq c$. If $a < 4$, then necessarily $a = 1$ because $a \equiv 0, 1 \pmod{4}$ by property (iii). Thus q' is the principal form of discriminant $-16d$, so $q' = [1, 0, 4d]$. But of these, the only form that primitively represents 4 is $q' = [1, 0, 4]$, which is equivalent to $[4, 0, 1]$. Thus we get the case $d = 1$ of (13).

Now suppose that $a \geq 4$. Since a is the smallest value represented by q, we must have $a = 4$ by property (ii). Thus, $16|(\mathrm{disc}(q)+16c) = b^2$, so $b = 0$ or 4. If $b = 0$, then $c = d \geq 4$. But since $\gcd(2, d) = 1$ and $c \equiv 0, 1 \pmod{4}$, it follows that $d \equiv 1 \pmod{4}$. This gives a form of (13) with $s = 0$.

Now suppose that $b = 4$, so $c = \frac{4^2+16d}{16} = d + 1$ and $\gcd(d, 2) = 1$. Thus $c \equiv 0 \pmod{4}$ by property (iii), and so $d \equiv 3 \pmod{4}$. This gives us the cases of (13) with $s = 1$. □

3 Basic definitions and previous results

In this section we review some of the notations, definitions and results which were presented in the first part[6]. As in [6], we refer to Milne[9], [10] for basic facts about Jacobians and abelian varieties.

Throughout, let K be an arbitrary field, and let (J, λ) be a principally polarized abelian surface over K. Thus, J/K is an abelian variety of dimension 2 and $\lambda : J \xrightarrow{\sim} \hat{J}$ is an isomorphism such that its base change $\lambda_{\overline{K}} : J_{\overline{K}} \to \hat{J}_{\overline{K}}$ to an algebraic closure $\overline{K}$ of K is given by a theta-divisor $\theta \in \mathrm{NS}(J_{\overline{K}})$, i.e., $\lambda_{\overline{K}} = \phi_\theta$ in the notation of [11].

Definition. If $N \geq 2$, then an *N-presentation over K* is a triple (E, E', ψ) where E/K and E'/K are elliptic curves and $\psi : E[N] \to E'[N]$ is a K-isomorphism of finite group schemes which is an anti-isometry with respect to the e_N-pairings.

If (J, λ) is a principally polarized abelian surface over K, then an *N-presentation of (J, λ) over K* is a 4-tuple (E, E', ψ, π) such that (E, E', ψ) is an N-presentation over K and $\pi : E \times E' \to J$ is an isogeny such that

$$\mathrm{Ker}(\pi) \;=\; \mathrm{Graph}(-\psi) \quad \text{and} \quad \hat{\pi} \circ \lambda \circ \pi \;=\; N(\lambda_E \otimes \lambda_{E'}), \tag{14}$$

where $\lambda_E : E \to \hat{E}$ is the canonical principal polarization of E/K and $\lambda_E \otimes \lambda_{E'}$ denotes the product polarization on $E \times E'$, i.e., $\lambda_E \otimes \lambda_{E'} = \phi_{\theta_E + \theta_{E'}}$, where $\theta_E = \mathrm{pr}_E^*(0_E)$ and $\theta_{E'} = \mathrm{pr}_{E'}^*(0_{E'})$, and $\mathrm{pr}_E : E \times E' \to E$ and $\mathrm{pr}_{E'} : E \times E' \to E'$ are the projections.

Remark 20 (a) If (E, E', ψ) is an N-presentation, and if $\pi_\psi : A := E \times E' \to A_\psi := A/\mathrm{Graph}(-\psi)$ is the quotient map, then A_ψ has a unique principal polarization λ_ψ such that (E, E', ψ, π_ψ) is an N-presentation of (A_ψ, λ_ψ); cf. [6], Proposition 10(b). We then say that $(\pi_\psi, A_\psi, \lambda_\psi)$ is the *quotient data* associated to (E, E', ψ).

(b) If (J, λ) is principally polarized abelian surface over K with an elliptic subgroup $E \leq J$ of λ-degree N, then (J, λ) has an N-presentation (E, E', ψ, π), for some elliptic curve E'/K and anti-isometry ψ and isogeny $\pi : E \times E' \to J$; cf. [6], Proposition 10(a). Note that $E' = E_\lambda^\perp$ in the notation of [6], Proposition 10(a).

Moreover, if $f : C \to E$ is an elliptic subcover of degree N of a curve C/K of genus 2, then $E = f^* J_E$ is an elliptic subgroup of the Jacobian J_C/K of C/K, and E has λ_C-degree N, where λ_C denotes the canonical polarization of J_C, so f induces an N-presentation (E, E', ψ_f, π_f) of (J_C, λ_C); cf. [6], Corollary 12.

We next recall the definition of the *refined Humbert invariant* $q_{(J,\lambda)}$ of a principally polarized abelian surface (J, λ) over K. If K is algebraically closed, then we can use the Néron-Severi group $\mathrm{NS}(J) = \mathrm{Div}(J)/\equiv$ to define $q_{(J,\lambda)}$, but for a general base field K this group is no longer suitable, as was explained in [6], Section 3. Instead, one has to work with a slightly larger group $\mathrm{NS}'(J)$ which is defined as the *saturation* (or *primitive hull*) of $\mathrm{NS}(J)$ in the group $\mathrm{NS}(J_{\overline{K}})$, i.e.,

$$\mathrm{NS}'(J) \;=\; \{D \in \mathrm{NS}(J_{\overline{K}}) : nD \in \mathrm{NS}(J), \;\; \text{for some } n \geq 1\}.$$

Note that the theta-divisor $\theta \in \mathrm{NS}(J_{\overline{K}})$ of $\lambda_{\overline{K}}$ lies in $\mathrm{NS}'(J)$ (cf. proof of [6], Proposition 14), so the quotient group

$$\mathrm{NS}(J, \lambda) \;:=\; \mathrm{NS}'(J)/\mathbb{Z}\theta$$

is defined. Then the *refined Humbert invariant* is the positive-definite quadratic form $q_{(J,\lambda)} : \mathrm{NS}(J,\lambda) \to \mathbb{Z}$ defined by the formula

$$(15) \qquad q_{(J,\lambda)}(D + \mathbb{Z}\theta) \;=\; \tilde{q}_{(J,\lambda)}(D) \;:=\; (D.\theta)^2 - 2(D.D), \quad \text{for } D \in \mathrm{NS}'(J),$$

where $(\,\cdot\,)$ denotes the intersection pairing on the surface $J_{\overline{K}}$.

In the case of a product surface $A = E \times E'$, the group $\mathrm{NS}'(A)$ is just the usual Néron-Severi group $\mathrm{NS}(A)$. Moreover, if $\lambda_A = \lambda_E \otimes \lambda_{E'}$ is the product polarization on A, then $q_{(A,\lambda_A)}$ is given by formula (16) below.

Lemma 21 *Let E/K and E'/K be elliptic curves over an arbitrary field K, and let $A = E \times E'$ be the product surface. For $a, b \in \mathbb{Z}$ and $h \in \mathrm{End}(E, E')$ put*

$$\tilde{\mathbf{D}}'(a,b,h) := (a - \deg(h))\theta_E + (b-1)\theta_{E'} + \Gamma_{-h} \;\in\; \mathrm{Div}(A),$$

where Γ_{-h} denotes the graph of $-h$, and let $\mathbf{D}'(a,b,h) = \mathrm{cl}(\tilde{\mathbf{D}}'(a,b,h))$ denote its class in $\mathrm{NS}(A)$. Then the rule $(a,b,h) \mapsto \mathbf{D}'(a,b,h) \in \mathrm{NS}(A)$ defines an isomorphism

$$\mathbf{D}'_{E,E'} : \tilde{\mathcal{H}}_{E,E'} := \mathbb{Z} \times \mathbb{Z} \times \mathrm{Hom}(E,E') \;\xrightarrow{\sim}\; \mathrm{NS}'(A) = \mathrm{NS}(A),$$

and if $\lambda_A = \lambda_E \otimes \lambda_{E'}$ denotes the product polarization, then

$$(16) \qquad q_{(A,\lambda_A)}(\mathbf{D}'(a,b,h) + \mathbb{Z}\theta_A) \;=\; (a-b)^2 + 4\deg(h) \;=\; (a-b)^2 + 4q_{E,E'}(h),$$

where $q_{E,E'}$ denotes the degree form *on* $\mathrm{Hom}(E,E')$.

Proof. [6], Lemma 28. □

It is much more difficult to determine the refined Humbert invariant for an arbitrary principally polarized abelian surface (J,λ); indeed, this is precisely the aim of the present paper. A first step towards this was done in [6], which determined the discriminant (or determinant) of the quadratic form $q_{(J,\lambda)}$ in terms of a presentation data (E, E', ψ, π). This result depends on the *isogeny defect* m_ψ of ψ with respect to the group $\mathrm{Hom}(E,E')$. For applications, it is useful to generalize this concept as follows; cf. [6], Section 4.

Definition. Let E/K and E'/K be elliptic curves, and let $\psi \in \mathrm{Hom}(E[N], E'[N])$. Moreover, let $\mathcal{H} \leq \mathcal{H}_{E,E'} := \mathrm{Hom}(E,E')$ be a *primitive subgroup* of $\mathcal{H}_{E,E'}$, i.e., $\mathcal{H}$ is a subgroup of $\mathcal{H}_{E,E'}$ such that $\mathcal{H}_{E,E'}/\mathcal{H}$ is torsionfree. Then the *isogeny defect of ψ with respect to $\mathcal{H}$* is

$$m_\psi(\mathcal{H}) \;:=\; \min\{m \geq 1 : m\psi = h_{|E[N]}, \text{ for some } h \in \mathcal{H}\}.$$

As is mentioned in [6], Remark 21(b), $m_\psi(\mathcal{H})$ can be expressed as an index of groups. Indeed, let

$$\rho_N : \mathrm{Hom}(E,E') \;\to\; \mathrm{Hom}(E[N], E'[N])$$

be the restriction map $h \mapsto h_{|E[N]}$, and put $\mathcal{H}_N = \rho_N(\mathcal{H})$, which is a subgroup of $\mathrm{Hom}(E[N], E'[N])$. Then by elementary group theory we have that

$$m_\psi(\mathcal{H}) \;=\; [\langle\psi\rangle + \mathcal{H}_N : \mathcal{H}_N] \;=\; [\langle\psi\rangle : \langle\psi\rangle \cap \mathcal{H}_N]. \tag{17}$$

In particular, we see that $m_\psi(\mathcal{H}) \mid \mathrm{ord}(\psi) \mid N$, and that

$$k\psi = \rho_N(h), \text{ for some } k \in \mathbb{Z}, h \in \mathcal{H} \quad \Rightarrow \quad m_\psi(\mathcal{H}) \mid k. \tag{18}$$

The main result which was used in the calculation of the discriminant of $q_{(J,\lambda)}$ is the following *index formula*, which is Theorem 31 of [6].

Theorem 22 *Let E/K and E'/K be elliptic curves and let $\psi \in \mathrm{Hom}(E[N], E'[N])$. Moreover, let $G_\psi = \mathrm{Graph}(-\psi)$ be the graph of $-\psi$ and let*

$$\pi = \pi_\psi : A := E \times E' \to A_\psi := (E \times E')/G_\psi,$$

be the associated quotient isogeny. Assume that A_ψ has a principal polarization λ_ψ. In addition, let $\mathcal{H} \leq \mathrm{Hom}(E, E')$ be a primitive subgroup, and put

$$\tilde{\mathcal{H}} \;:=\; \{\mathbf{D}'(a, b, h)) : a, b \in \mathbb{Z},\, h \in \mathcal{H}\} \;\leq\; \mathrm{NS}'(A).$$

If $r_{\mathcal{H}} := \mathrm{rank}(\mathcal{H})$ and if $\mathrm{char}(K) \nmid m_\psi(\mathcal{H})$, then

$$[\tilde{\mathcal{H}} : \pi_\psi^*(\mathrm{NS}'(A_\psi)) \cap \tilde{\mathcal{H}}] \;=\; m_\psi(\mathcal{H}) N^{r_{\mathcal{H}}+2}. \tag{19}$$

Note that ψ does not have to be an anti-isometry in Theorem 22; indeed, if this is the case, then the existence of the principal polarization λ_ψ is automatic; cf. Remark 20(a). The generality of Theorem 22 is necessary to be able to apply it to the map $\bar{\psi}$ of the following *factorization lemma*, which is Proposition 39 of [6].

Proposition 23 *In the situation of* Theorem 22, *put $m = m_\psi(\mathcal{H})$. Then there exists an $h \in \mathcal{H}$ such that $m\psi = m\rho_N(h)$ and we have*

$$\varepsilon_{N,m}^{E'} \circ \bar{\psi} \circ \pi_{N,m}^{E} \;=\; \psi - \rho_N(h), \tag{20}$$

for a unique $\bar{\psi} \in \mathrm{Hom}(E[m], E'[m])$, where $\varepsilon_{N,m}^{E'} : E'[m] \hookrightarrow E'[N]$ denotes the canonical inclusion and $\pi_{N,m}^{E} : E[N] \to E[m]$ denotes the map which is given by multiplication by $\bar{N} = \frac{N}{m}$.

Moreover, if $\nu = v_{\bar{N},h} := \begin{pmatrix} [\bar{N}]_E & 0 \\ h & [1]_{E'} \end{pmatrix} \in \mathrm{End}(A)$, then $\nu^{-1} G_{\bar{\psi}} = G_\psi$, and hence there is a unique isomorphism $\alpha_\psi : A_\psi \xrightarrow{\sim} A_{\bar{\psi}}$ such that

$$\alpha_\psi \circ \pi_\psi = \pi_{\bar{\psi}} \circ \nu. \tag{21}$$

In addition, $m_{\bar{\psi}}(\mathcal{H}) = m_\psi(\mathcal{H})$.

Another concept which was used in the calculation of the discriminant of q_C in [6] (and which is required here) was the notion of the *trace* $\mathrm{tr}(g)$ of an element $g \in \mathrm{End}(E[N])$. Since $\mathrm{tr}(g)$ is closely linked to the *transpose* g^t of g, we first recall the definition of g^t and some of its properties. For this, *assume henceforth in this section* that $\mathrm{char}(K) \nmid N$.

If $g \in \mathrm{Hom}(E[N], E'[N])$, then by [6], Proposition 23, there exists a unique homomorphism $g^t \in \mathrm{Hom}(E'[N], E[N])$ such that

$$e_N^{E'}(g(P), Q) \;=\; e_N^E(P, g^t(Q)), \quad \forall P \in E[N](\overline{K}),\, Q \in E'[N](\overline{K}), \tag{22}$$

where $e_N^E : E[N] \times E[N] \to \mu_N$ is the usual e_N-pairing on E. Moreover, we have

$$(g^t)^t \;=\; g \quad \text{and} \quad g^t g \;=\; [\det(g)]_{E[N]}, \tag{23}$$

for all $g \in \mathrm{Hom}(E[N], E'[N])$, where $\det(g) \in \mathbb{Z}/N\mathbb{Z}$ is the unique number such that

$$e_N^{E'}(g(P), g(Q)) \;=\; e_N^E(P, Q)^{\det(g)}, \quad \text{for all } P, Q \in E[N](\overline{K}). \tag{24}$$

From this it follows (cf. [6], Corollary 24) that if we put $\mathrm{tr}(g) := \det(1+g) - \det(d) - 1$ for $g \in \mathrm{End}(E[N])$, then

$$g^t + g \;=\; [\mathrm{tr}(g)]_{E[N]}. \tag{25}$$

Note that if $h \in \mathrm{Hom}(E, E')$ is a homomorphism of elliptic curves, then its transpose is defined as $h^t := \lambda_{E'}^{-1} \circ \hat{h} \circ \lambda_E \in \mathrm{End}(E', E)$, where (as before) $\lambda_E = \phi_{0_E} : E \xrightarrow{\sim} \hat{E}$ is the canonical principal polarization of E. This transpose is compatible with the above transpose in the sense that

$$(h_{|E[N]})^t \;=\; (h^t)_{|E'[N]}, \quad \text{and hence} \quad \det(h_{|E[N]}) \equiv \deg(h) \,(\mathrm{mod}\ N); \tag{26}$$

cf. [6], Remark 25(a). In addition, the transpose is compatible with restriction to the subgroup $E[M]$ for $M|N$. More precisely, if $g_M \in \mathrm{Hom}(E[M], E'[M])$ is the unique map such that

$$\pi_{N,M}^{E'} \circ g \;=\; g_M \circ \pi_{N,M}^E, \tag{27}$$

then by [6], Section 4, we have that

$$(g^t)_M \;=\; (g_M)^t, \quad \text{for all } g \in \mathrm{Hom}(E[N], E'[N]), \tag{28}$$

and from (23) it follows that

$$\det(g_M) \;\equiv\; \det(g) \,(\mathrm{mod}\ M), \quad \text{for all } g \in \mathrm{Hom}(E[N], E'[N]). \tag{29}$$

Finally, we recall the following technical result which was used in the derivation of Theorem 22 and which is required in the proof of Theorem 25 below.

Proposition 24 *In the situation of* Theorem 22*, assume also that* $\mathrm{char}(K) \nmid N$*. If* $D = \mathbf{D}'(a, b, f) \in \mathrm{NS}'(A)$*, then*

$$ND \in \pi_\psi^* \mathrm{NS}'(A_\psi) \quad \Leftrightarrow \quad p_\psi(D) := a + b\det(\psi) - \mathrm{tr}(f^t\psi) \equiv 0 \,(\mathrm{mod}\ N). \tag{30}$$

Proof. [6], Proposition 37.

4 The computation of q_C

The purpose of this section is to compute the refined Humbert invariant q_C of C/K explicitly from the data given by a presentation (E, E', ψ) of degree N in the case that rank $\mathrm{Hom}(E, E') = 1$.

Since essentially the same computation can also be done in a much more general context, we shall do it first in the general situation of a principal polarized abelian surface with an N-presentation $(E, E'\psi, \pi)$, and then explain how to deduce the above case from it; cf. Corollary 27. Thus, we shall prove:

Theorem 25 *Let (E, E', ψ) be an N-presentation over K with associated quotient data $(\pi_\psi, A_\psi, \lambda_\psi)$, and let $d \geq 1$ be an integer. Then:*

(a) *There exists a cyclic isogeny $h \in \mathrm{Hom}(E, E')$ such that $d = \deg(h)$ if and only if d is primitively represented by the degree form $q_{E,E'}$. If this is the case, put $m = m_\psi(\mathbb{Z}h)$ and $\bar{N} = \frac{N}{m}$. Then there is an integer $k \in \mathbb{Z}$ such that the restriction $\psi_{\bar{N}}$ of ψ to $E[\bar{N}]$ equals the restriction of kh to $E[\bar{N}]$, i.e.,*

$$\psi_{\bar{N}} \;=\; \rho_{\bar{N}}(kh). \tag{31}$$

(b) *In the situation of part* (a)*, fix a cyclic isogeny h with $\deg(h) = d$ and an integer $k \in \mathbb{Z}$ such that* (31) *holds, and put $n := (k^2 d + 1)/\bar{N}$. Then $n \in \mathbb{Z}$ and so the binary quadratic from $q_{\bar{N},n,k}$ is defined as in the proof of* Lemma 10*. Moreover,*

$$\tilde{q}_{(A,\lambda)}(XD_1 + YD_2) \;=\; \bar{N}^2 q_{\bar{N},n,k}(X, Y), \quad \textit{for all } X, Y \in \mathbb{Z}, \tag{32}$$

where $A = E \times E'$, λ is the product polarization on A, and $D_1 := \mathbf{D}'(\bar{N}^2, 0, 0)$ and $D_2 := \mathbf{D}'(k(t-2d), -kd, h) \in \mathrm{NS}'(A)$ with $t = d(k^2 d + 4) = d(\bar{N}n + 3)$.

(c) *Assume henceforth that $\mathrm{char}(K) \nmid m$. Then there is an integer r such that $m(rD_1 + D_2) \in \pi_\psi^*(A_\psi)$, and $r \pmod m$ is uniquely determined by this property. Moreover, if $\mathcal{H} = \mathbb{Z}h$ and $\theta = \mathbf{D}'(1, 1, 0)$, then*

$$\tilde{\mathcal{H}} \cap \pi_\psi^* \mathrm{NS}'(A_\psi) \;=\; \mathbb{Z}N\theta + \mathbb{Z}m^2 D_1 + \mathbb{Z}m(rD_1 + D_2). \tag{33}$$

(d) *There is a unique $\bar{\psi} \in \mathrm{Hom}(E[m], E'[m])$ such that*

$$\varepsilon_{N,m} \circ \bar{\psi} \circ \pi_{N,m} \;=\; \psi - \rho_N(kh), \tag{34}$$

and then the integer r of part (c) *is given by the formula*

$$r \;\equiv\; kd \det(\bar{\psi}) + n\mathrm{tr}(h^t \bar{\psi}) \pmod m. \tag{35}$$

(e) *Fix r as in part* (c)*. Then there exist $\bar{D}_1, \bar{D}_2 \in \mathrm{NS}(A_\psi, \lambda_\psi)$ such that $\mathbb{Z}\bar{D}_1 + \mathbb{Z}\bar{D}_2$ is a primitive submodule of $\mathrm{NS}(A_\psi, \lambda_\psi)$ of rank 2 and such that*

$$q_{(A_\psi,\lambda_\psi)}(X\bar{D}_1 + Y\bar{D}_2) \;=\; q_{N,m,d,k,r}(X, Y), \quad \textit{for all } X, Y \in \mathbb{Z}, \tag{36}$$

where $q_{N,m,d,k,r}$ is as in Lemma 10*. In particular, $q_{(A_\psi,\lambda_\psi)}$ primitively represents the binary quadratic form $q_{N,m,d,k,r}$.*

Proof. (a) The first assertion is clear because $h \in \mathrm{Hom}(E, E')$ is primitive if and only if h is a cyclic isogeny.

Now by the definition of m there exists a $k' \in \mathbb{Z}$ such that $m\psi = \rho_N(k'h)$. Since $m|N$, we see that $E[m] \leq \mathrm{Ker}(k'h)$, and so $m|k'$ because $\mathrm{Ker}(h)$ is cyclic. Thus $k' = mk$, for some $k \in \mathbb{Z}$, so $m(\psi - \rho_N(kh)) = 0$ and hence (31) holds by (27).

(b) Since $\deg(kh) = k^2 d$, we have by (31), (26) and (29) that $k^2 d \equiv \det(\rho_{\bar{N}}(kh)) \equiv \det(\psi_{\bar{N}}) \equiv -1 \,(\mathrm{mod}\, \bar{N})$, the latter because ψ (and hence also $\psi_{\bar{N}}$) is an anti-isometry. Thus $\bar{N}|(k^2 d + 1)$, i.e., $n \in \mathbb{Z}$.

To prove (32), write $\tilde{q} = \tilde{q}_{(A,\lambda)}$. Then by (16) we see that $\tilde{q}(D_1) = \bar{N}^4$ and $\tilde{q}(D_2) = k^2(t-d)^2 + 4d = \bar{N}^2 n^2 t$, where the last equality follows by using the identity (6) of [4]. Similarly, since $\tilde{q}(D_1 + D_2) = (\bar{N}^2 + k(t-d))^2 + 4d = 2k(t-d)\bar{N}^2 + \bar{N}^4 + \bar{N}^2 n^2 t$ by the same identity (6) again, it follows that (32) holds.

(c) To show that such an r exists, we shall use the results which were summarized in the previous section (and prove part (d) along the way).

First of all, since $m\psi = m\rho_N(kh)$ (cf. the proof of part (a)), we have by Proposition 23 that (34) holds for a unique $\bar{\psi}$. Let $r \in \mathbb{Z}$ be such that (35) holds. We now claim that $m(rD_1 + D_2) \in \mathcal{N}_\psi := (\pi_\psi)^* \mathrm{NS}'(A_\psi)$.

For this, recall from Proposition 23 that we have the isomorphism $\alpha : A_\psi \xrightarrow{\sim} A_{\bar{\psi}}$ such that (21) holds, where $\nu = \nu_{\bar{N},kh}$. Since λ_ψ is a principal polarization on A_ψ (cf. Remark 20(a)), there is a unique principal polarization $\lambda_{\bar{\psi}}$ on $A_{\bar{\psi}}$ such that $\hat{\alpha} \circ \lambda_{\bar{\psi}} \circ \alpha = \lambda_\psi$, so $\bar{\psi}$ satisfies the hypothesis of Theorem 22, and hence we can apply Proposition 24 to $\bar{\psi}$. Let $p_{\bar{\psi}}$ be as in Proposition 24.

Put $D_1' = \mathbf{D}'(1,0,0)$ and $D_2' = \mathbf{D}'(0,-kd,nh)$, so $rD_1' + D_2' = \mathbf{D}'(r,-kd,nh)$. Then $p_{\bar{\psi}}(rD_1' + D_2') \equiv r - (kd)\det(\bar{\psi}) - n\mathrm{tr}(h^t\psi) \equiv 0 \,(\mathrm{mod}\, m)$ by (35), so by Proposition 24 we have that $m(rD_1' + D_2') \in \mathcal{N}_{\bar{\psi}} := (\pi_{\bar{\psi}})^* \mathrm{NS}'(A_{\bar{\psi}})$. Thus, since

$$\nu^*(D_1') = D_1 \quad \text{and} \quad \nu^*(D_2') = D_2 \tag{37}$$

by [6], formula (42), and the fact that $\bar{N}n - k^2 d = 1$, it follows that $m(rD_1 + D_2) \in \nu^* \mathcal{N}_{\bar{\psi}} = \mathcal{N}_\psi$, where the latter equality follows from (21). This proves the existence of $r \in \mathbb{Z}$ such that $m(rD_1 + D_2) \in \mathcal{N}_\psi$.

We next show that (33) holds. To see this, note first that if $\tilde{\mathcal{H}}_1$ denotes the module on the right hand side of (33), then clearly $\tilde{\mathcal{H}}_1 \subset \tilde{\mathcal{H}}$. Next we verify that $\tilde{\mathcal{H}}_1 \subset \mathcal{N}_\psi$.

For this, recall from above that $m(rD_1 + D_2) \in \mathcal{N}_\psi$. Moreover, since clearly $p_{\bar{\psi}}(mD_1') \equiv 0 \,(\mathrm{mod}\, m)$, we see that $m^2 D_1' \in \mathcal{N}_{\bar{\psi}}$ and so $m^2 D_1 = \nu^*(m^2 D_1') \in \mathcal{N}_\psi$. Finally, we observe that $N\theta \in \mathcal{N}_\psi$. Indeed, if $\theta_\psi \in \mathrm{NS}'(A_\psi)$ is such that $\phi_{\theta_\psi} = \lambda_\psi$, then $\phi_{\pi_\psi^* \theta_\psi} = \phi_{N\theta}$ because $\hat{\pi}_\psi \lambda_\psi \pi_\psi = N\lambda = N\phi_\theta$ by (14), so we have

$$N\theta \;=\; \pi_\psi^* \theta_\psi \;\in\; \mathcal{N}_\psi. \tag{38}$$

This shows the desired inclusion $\tilde{\mathcal{H}}_1 \subset \tilde{\mathcal{H}} \cap \mathcal{N}_\psi$.

Now since θ, D_1', and $D := \mathbf{D}'(0,0,h)$ form a basis of $\tilde{\mathcal{H}}$, and since $m^2 D_1 = N^2 D_1'$ and $m(rD_1 + D_2) = a\theta + bD_1 + mD$, for some $a, b \in \mathbb{Z}$, we see that $[\tilde{\mathcal{H}} : \tilde{\mathcal{H}}_1] = N \cdot N^2 \cdot m = mN^3$. On the other hand, since $\mathcal{H} = \mathbb{Z}h$ is primitive in $\mathrm{Hom}(E, E')$ because h is cyclic, it follows from Theorem 22 that $[\tilde{\mathcal{H}} : \tilde{\mathcal{H}} \cap \mathcal{N}_\psi] = mN^3$, and so we have that $\tilde{\mathcal{H}}_1 = \tilde{\mathcal{H}} \cap \mathcal{N}_\psi$. This proves (33).

We now show that r is uniquely determined by the given condition. Indeed, suppose that we have $m(r'D_1 + D_2) \in \mathcal{N}_\psi$, for some $r' \in \mathbb{Z}$. Then by (33) there exist $a, b, c \in \mathbb{Z}$ such that $m(r'D_1 + D_2) = aN\theta + bm^2 D_1 + cm(rD_1 + D_2)$. Since θ, D_1 and D_2 are linearly independent, it follows that $c = 1$ and $a = 0$, so $mr' = bm^2 + mr$, or $r' \equiv r \,(\mathrm{mod}\, m)$, as claimed. Note also that the converse holds: if $r' = r + bm$, $b \in \mathbb{Z}$, then $m(r'D_1 + D_2) = m(rD_1 + D_2) + m^2 bD_1 \in \mathcal{N}_\psi$ by (33).

(d) This was established in the course of proving part (c).

(e) From (33) we see that there exist $D_1'', D_2'' \in \mathrm{NS}'(A_\psi)$ such that

$$\pi_\psi^*(D_1'') \;=\; m^2 D_1 \quad \text{and} \quad \pi_\psi^*(D_2'') \;=\; m(rD_1 + D_2). \tag{39}$$

Thus, if we put $\tilde{\mathcal{H}}_2 := \mathbb{Z}\theta_\psi + \mathbb{Z}D_1'' + \mathbb{Z}D_2''$, then $\pi_\psi^*(\tilde{\mathcal{H}}_2) = \tilde{\mathcal{H}} \cap \mathcal{N}_\psi$ by (38), (39) and (33), and so $\tilde{\mathcal{H}}_2$ is a primitive submodule of $\mathrm{NS}'(A_\psi)$ because $\tilde{\mathcal{H}} \cap \mathcal{N}_\psi$ is primitive in $\mathcal{N}_\psi$. Thus, if $\bar{D}_i$ denotes the image of D_i'' in $\mathrm{NS}(A_\psi, \lambda_\psi) = \mathrm{NS}'(A_\psi)/\mathbb{Z}\theta_\psi$, then $\mathbb{Z}\bar{D}_1 + \mathbb{Z}\bar{D}_2 = \tilde{\mathcal{H}}_2/\mathbb{Z}\theta_\psi$ is a primitive submodule of $\mathrm{NS}(A_\psi, \lambda_\psi)$.

Finally, to prove (36), we use (39), the projection formula (cf. [6], formula (14)) together with (32) and (4) to obtain that

$$\begin{aligned} N^2 \tilde{q}_{(A_\psi,\lambda_\psi)}(XD_1'' + YD_2'') &= \tilde{q}_{(A,\lambda)}(X(m^2 D_1) + Ym(rD_1 + D_2)) \\ &= m^2 \tilde{q}_{(A,\lambda)}((mX + rY)D_1 + YD_2) \\ &= m^2 \bar{N}^2 q_{\bar{N},n,k}(mX + rY, Y) \;=\; N^2 q_{N,m,d,k,r}(X, Y), \end{aligned}$$

and so (36) follows because $q_{(A_\psi,\lambda_\psi)}(x\bar{D}_1 + y\bar{D}_2) = \tilde{q}_{(A_\psi,\lambda_\psi)}(xD_1'' + yD_2'')$ by definition. □

We observe that the above theorem yields the following result which generalizes Theorem 1.

Corollary 26 *In the situation of* Theorem 25 *assume in addition that* $\mathrm{char}(K) \nmid N$.

(a) *If $d \geq 1$ is an integer which is primitively represented by $q_{E,E'}$, then $q_{(A_\psi,\lambda_\psi)}$ primitively represents a binary quadratic form of type (N, m, d), where m is some integer with $m_\psi | m | N$, where m_ψ is defined as in the* Introduction.

(b) *If* $\mathrm{Hom}(E, E') \neq 0$, *then there exists an integer $d \geq 1$ which is primitively represented by $q_{E,E'}$ such that $q_{(A_\psi,\lambda_\psi)}$ primitively represents a binary quadratic form of type (N, m_ψ, d).*

Proof. (a) This clearly follows from Theorem 25 by taking $m = m_\psi(\mathbb{Z}h)$ as in the theorem. Note that $m | N$ by (17) and also that $m_\psi = m_\psi(\mathrm{Hom}(E, E'))| m$ by (17) because $\mathbb{Z}h \leq \mathrm{Hom}(E, E')$.

(b) By definition there exists $h' \in \mathrm{Hom}(E, E')$ such that $m_\psi \psi = \rho_N(h')$. We can write $h' = kh$, where h is a cyclic isogeny. (If $h' = 0$, then $m_\psi = N$ and then we can take $k = 0$ and h any cyclic isogeny which exists because $\mathrm{Hom}(E, E') \neq 0$.) Thus $d = \deg(h)$ is primitively represented by $q_{E,E'}$ and $m_\psi = m_\psi(\mathbb{Z}h)$. Thus, applying Theorem 25 to this d, h and k, we see that the last assertion follows. □

Corollary 27 *Suppose that C/K has a presentation (E, E', ψ) of degree N such that $\mathrm{Hom}(E, E') = \mathbb{Z}h$, where $d = \deg(h) \geq 1$. Put $m = m_\psi$ and $\bar{N} = \frac{N}{m}$, and assume that $\mathrm{char}(K) \nmid m$. Then there is an integer k such that (31) holds. Thus, if we choose the integer r according to the recipe of* Theorem 25(d)*, then q_C is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to the binary quadratic form $q_{N,m,d,k,r}$.*

Proof. The hypothesis implies that h is cyclic of degree d, so by Theorem 25(a) there is an integer k such that (31) holds. Since $(J_C, \lambda_C) \simeq (A_\psi, \lambda_\psi)$, and since $\mathrm{rank}(\mathrm{NS}'(J_C)) = 3$ by our hypothesis, it follows that the elements $\bar{D}_1$, $\bar{D}_2$ of Theorem 25(e) form a basis of $\mathrm{NS}(A_\psi, \lambda_\psi) \simeq \mathrm{NS}(J_C, \lambda_C)$, and so the last assertion of Theorem 25(e) shows that q_C and $q_{(A_\psi, \lambda_\psi)}$ are both $\mathrm{GL}_2(\mathbb{Z})$-equivalent to $q_{N,m,d,k,r}$. □

We next observe that the basic integers m, k, r which determine the quadratic form $q_{N,m,d,k,r}$ can be computed directly from the matrix $[\psi^{-1} h_{|E[N]}]_{\mathcal{B}}$ of the endomorphism $\psi^{-1} h_{|E[N]} \in \mathrm{End}(E[N])$ with respect to some basis $\mathcal{B}$ of $E[N](\overline{K})$.

More precisely, assume that $\mathrm{char}(K) \nmid N$ and that $\mathcal{B} = (P_1, P_2)$ is a basis of $E[N](\overline{K})$. Then there exist $x, y, z, w \in \mathbb{Z}$ such that

$$\psi^{-1} h(P_1) \;=\; xP_1 + zP_2 \quad \text{and} \quad \psi^{-1} h(P_2) \;=\; yP_1 + wP_2, \tag{40}$$

and so $[\psi^{-1} \rho_N(h)]_{\mathcal{B}} \equiv \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \pmod N$ is the matrix of $\psi^{-1} \rho_N(h)$ with respect to the basis $\mathcal{B} = (P_1, P_2)$ of $E[N]$. Note that x, y, z, w are uniquely determined $\pmod N$ by h and ψ (and by the basis $\mathcal{B}$).

Proposition 28 *In the situation of* Theorem 25*, assume that $\mathrm{char}(K) \nmid N$, and let $h \in \mathrm{Hom}(E, E')$ be a cyclic isogeny of degree d. Let $M = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in M_2(\mathbb{Z})$ be an integral matrix such that $M \pmod N$ is the matrix of $\psi^{-1} \rho_N(h)$ with respect to some basis $\mathcal{B} = (P_1, P_2)$ of $E[N]$. Then M is N-primitive and $\det(M) \equiv -d \pmod N$, and*

$$m := m_\psi(\mathbb{Z}h) \;=\; N/g_{M,N} \quad \textit{where } g_{M,N} = \gcd(x - w, y, z, N). \tag{41}$$

Moreover, there exists an integer k such that $kx \equiv 1 \pmod{\frac{N}{m}}$, and then (31) holds for this k. In addition, the quadratic form $q_{N,m,d,k,r}$ of Theorem 25(e) *is equivalent to the form $q_{M,N,d,k}$ of* Proposition 11*, i.e., $q_{N,m,d,k,r} \sim q_{M,N,d,k}$.*

Proof. Write $g := \psi^{-1} \rho_N(h) \in \mathrm{End}(E[N])$. Then $\det(g) = \det(\psi)^{-1} \det(\rho_N(h)) \equiv -d \pmod N$ by (26), and so $\det(M) \equiv \det(g) \equiv -d \pmod N$. Moreover, we have

that $\gcd(x,y,z,w,N)=1$ because $E[n] \not\leq \mathrm{Ker}(h)$, $\forall n>1$, since h is a cyclic isogeny. Thus, M is N-primitive.

To prove the other assertions, we first observe that it follows from the definitions that if $n|N$ is any divisor, and if $\bar{n}=\frac{N}{n}$, then $\bar{n}\mathcal{B}=(\bar{n}P_1,\bar{n}P_2)$ is a basis of $E[n]$, and hence $M \pmod n$ is the matrix of $g_n \in \mathrm{End}(E[n])$ with respect to this basis.

Applying this to our situation, we thus see from Theorem 25(a) that $\exists k' \in \mathbb{Z}$ such that $k'M \equiv \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) \pmod{\bar{N}}$, so $k'x \equiv 1 \equiv k'w \pmod{\bar{N}}$ and $k'y \equiv k'z \equiv 0 \pmod{\bar{N}}$. Since $\gcd(k',\bar{N})=1$ by Theorem 25(b), it follows that $x \equiv w \pmod{\bar{N}}$ and $y \equiv z \equiv 0 \pmod{\bar{N}}$, which implies that $\bar{N}|N' := g_{M,N}$.

In order to show that $N'=\bar{N}$, note first that by the definition of N' we have that $\gcd(x,N') = \gcd(x,y,z,w,N) = 1$ and that $M = \left(\begin{smallmatrix}x&0\\0&x\end{smallmatrix}\right) + N'M_0$, for some integral matrix M_0. Thus, there exists $x' \in \mathbb{Z}$ such that $x'x \equiv 1 \pmod{N'}$, and so $m'x'M \equiv \left(\begin{smallmatrix}m'&0\\0&m'\end{smallmatrix}\right) \pmod N$, where $m'=N/N'$. This means that $m'x'g = [m']_{E[N]}$, or that $\rho_N(m'x'h) = m'\psi$. By (18) we thus have that $m_\psi := m_\psi(\mathbb{Z}h)|m'$, and so $N' = \frac{N}{m'}|\frac{N}{m_\psi} = \bar{N}$. This proves that $\bar{N}=N'$ and so (41) follows.

Since M is N-primitive and $g_{M,N} = \bar{N} = \frac{N}{m}$, there exists $k \in \mathbb{Z}$ such that $kx \equiv 1 \pmod{\bar{N}}$; cf. Proposition 11. Thus, by (8) we have that $kM \equiv I \pmod{\bar{N}}$, which is equivalent to (31).

To verify the last assertion, it suffices in view of Proposition 11, Remark 17 and (35) to verify that

$$\det(\bar{\psi}) \equiv -\det(M_1) \pmod m \quad \text{and} \quad \mathrm{tr}(h^t\bar{\psi}) \equiv -2b - \mathrm{tr}(M_0) \pmod m, \tag{42}$$

where $\bar{\psi}$ is as in Theorem 25(d), M_1 and M_0 are as in (8) and b is as in (9).

Since by definition $\bar{\psi}(\bar{N}P) = \psi(P) - h(P)$, for all $P \in E[N]$, it follows immediately that $\psi_m^{-1}\bar{\psi}(\bar{N}P) = P - \psi^{-1}h(P)$, and so we see that $M_1 \pmod m$ is the matrix of $\psi_m^{-1}\bar{\psi}$ with respect to the basis $\bar{N}\mathcal{B} = (\bar{N}P_1, \bar{N}P_2)$. Thus $\det(\psi_m^{-1}\bar{\psi}) \equiv \det(M_1) \pmod m$, and so $\det(\bar{\psi}) \equiv \det(M_1)\det(\psi_m) \equiv -\det(M_1) \pmod m$ by (29).

This proves the first formula of (42). To prove the second formula, it suffices to show that the matrix of $\rho_m(h)^t\bar{\psi}$ with respect to the basis $\bar{N}\mathcal{B}$ is given by the formula

$$[\rho_m(h)^t\bar{\psi}]_{\bar{N}\mathcal{B}} \;\equiv\; -bI - M_0^* \pmod m, \tag{43}$$

where M_0^* is the (classical) adjoint of M_0, because then the second formula of (42) follows by taking traces of both sides and observing that $\mathrm{tr}(M_0^*) = \mathrm{tr}(M_0)$.

In order to derive (43), we apply h^t to (34) to obtain that $h^t\bar{\psi}(\bar{N}P) = h^t\psi(P) - kh^th(P) = h^t\psi(P) - kdP$, for all $P \in E[N]$. Thus $\varepsilon_{N,\varepsilon} \circ \rho_m(h)^t\bar{\psi} \circ \pi_{N,m} = h^t\psi - [kd]_{E[N]}$. Now by (23) and by [6], formula (27), we have

$$\rho_N(h)^t\psi = \rho_N(h)^t\psi^{tt} = (\psi^t\rho_N(h))^t = -(\psi^{-1}\rho_N(h))^t,$$

the latter because $\psi^t = -\psi^{-1}$ by (23). Since $[g^t]_{\mathcal{B}} = ([g]_{\mathcal{B}})^*$, for any $g \in \mathrm{End}(E[N])$, we see that the matrix of $-\rho_N(h)^t\psi$ is the adjoint M^* of $M = [\psi^{-1}\rho_N(h)]_{\mathcal{B}}$. Since

$M^* = xI + \bar{N}(M_0)^*$, it follows that the matrix of $\varepsilon_{N,m} \circ \rho_m(h)^t \psi \circ \pi_{N,m} = h^t\psi - [kd]_{E[N]}$ is $-xI - \bar{N}(M_0)^* - kdI = -\bar{N}(bI + M_0^*)$, and so (43) follows. This proves (42). $\square$

Remark 29 It is useful to observe that we can choose the matrix M of Proposition 28 in such way that M is primitive and of determinant $-d$; cf. Lemma 30 below. If we do this, then the above quadratic form $q_{M,N,d,k}$ equals the form $q_{M,N}$ of Corollary 12, i.e., $q_{M,N,d,k} = q_{M,N}$.

Lemma 30 *Let* $M' = \left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right)$ *be an integral matrix and let* N *and* d *be positive integers. If* M' *is* N*-primitive, i.e., if* $\gcd(a_1, a_2, a_3, a_4, N) = 1$*, and if* $\det(M') \equiv -d \pmod{N}$*, then there exists a primitive integral matrix* M *of determinant* $-d$ *such that* $M \equiv M' \pmod{N}$*.*

Proof. Put $g_i = \gcd(a_i, N)$, so $\gcd(g_1, \ldots, g_4) = 1$. Then by Dirichlet's theorem on primes in arithmetic progressions, there are distinct primes $p_i \equiv \frac{a_i}{g_i} \pmod{\frac{N}{g_i}}$ with $p_i \nmid g_1 \cdots g_4$. Put $b_i := p_i g_i$ and $\tilde{M} := \left(\begin{smallmatrix} b_1 & b_2 \\ b_3 & b_4 \end{smallmatrix}\right)$. Then $\tilde{M} \equiv M' \pmod{N}$ and $\tilde{M}$ is primitive, i.e., $\gcd(b_1, \ldots, b_4) = 1$.

Note that $\delta := \det(\tilde{M}) \equiv \det(M') \equiv -d \pmod{N}$. Thus, since $\tilde{M}$ is primitive, there is a matrix $P \in \mathrm{SL}_2(\mathbb{Z})$ such that $\tilde{M} = P\left(\begin{smallmatrix} 1 & b \\ 0 & \delta \end{smallmatrix}\right)$, for some $b \in \mathbb{Z}$, and so $M := P\left(\begin{smallmatrix} 1 & b \\ 0 & -d \end{smallmatrix}\right)$ is primitive with $\det(M) = -d$ and $M \equiv \tilde{M} \equiv M' \pmod{N}$. $\square$

The following result can be viewed as a partial converse of Theorem 25.

Theorem 31 *Let* (J, λ) *be a principally polarized abelian surface over* K *and let* $N \geq 2$ *be an integer. Suppose that* $\mathrm{NS}(J, \lambda)$ *contains a primitive submodule* $\bar{\mathcal{G}}$ *of rank* 2 *such that the restriction* $q_{\bar{\mathcal{G}}}$ *of* $q_{(J,\lambda)}$ *to* $\bar{\mathcal{G}}$ *primitively represents* N^2*. Then there exist unique positive integers* m, d *with* $m|N$ *and* $\gcd(N/m, d) = 1$ *such that* $q_{\bar{\mathcal{G}}}$ *has type* (N, m, d)*, and hence there exist integers* k, r *with* $k^2 d \equiv -1 \pmod{\frac{N}{m}}$ *such that* $q_{\bar{\mathcal{G}}} \sim q_{N,m,d,k,r}$*. Moreover, if* $\mathrm{char}(K) \nmid m$*, then the following properties hold.*

(a) *There is an* N*-presentation* (E, E', ψ, π) *of* (J, λ) *and a cyclic isogeny* $h \in \mathrm{Hom}(E, E')$ *of degree* d *such that* (31) *holds. Thus* $m = m_\psi(\mathcal{H})$*, where* $\mathcal{H} = \mathbb{Z}h$*.*

(b) *If* $A = E \times E'$ *and* $\theta = \mathbf{D}'(1, 1, 0)$*,* $D_1 = \mathbf{D}'(\bar{N}^2, 0, 0)$*, and* $D_2 = \mathbf{D}'(k(t - 2d), -kd, h) \in \mathrm{NS}'(A)$*, where* $t = d(k^2 d + 4)$*, then the analogue of* (33) *holds, i.e.,*

$$\tilde{\mathcal{H}} \cap \pi^* \mathrm{NS}'(J) \;=\; \mathbb{Z}N\theta + \mathbb{Z}m^2 D_1 + \mathbb{Z}m(rD_1 + D_2). \tag{44}$$

In particular, the given r *satisfies the condition of* Theorem 25(c)*, and hence satisfies the congruence* (35)*.*

(c) *If* $\mathrm{char}(K) \nmid N$*, and if* M *is an integral matrix such that* $M \pmod{N}$ *is the matrix of* $\psi^{-1} \circ \rho_N(h)$ *with respect to some basis* $\mathcal{B} = (P_1, P_2)$ *of* $E[N](\overline{K})$*, then* $q_{\bar{\mathcal{G}}} \sim q_{M,N,d,k}$*.*

Proof. Recall that $q_{(J,\lambda)}$ and also hence $q_{\bar{\mathcal{G}}}$ is positive definite. Since $q_{(J,\lambda)}(D) \equiv (D.\theta)^2 \,(\mathrm{mod}\ 4)$, $\forall D \in \mathrm{NS}(J,\lambda)$ (cf. the proof of Theorem 3 of [6]), we see that $q_{\bar{\mathcal{G}}}$ satisfies property (iii) of Theorem 1. Thus, since $q_{\bar{\mathcal{G}}}$ primitively represents N^2 by hypothesis, the first assertion follows from Proposition 7, and the second follows from Theorem 16. To prove the other assertions, assume henceforth that $\mathrm{char}(K) \nmid m$.

(a) Since $q_{\bar{\mathcal{G}}} \sim q_{N,m,d,k,r}$, there exists a basis $(\bar{D}_1, \bar{D}_2)$ of $\bar{\mathcal{G}}$ such that

$$q_{(J,\lambda)}(X\bar{D}_1 + Y\bar{D}_2) \;=\; q_{N,m,d,k,r}(X,Y), \quad \text{for all } X, Y \in \mathbb{Z}. \tag{45}$$

Thus, $\bar{D}_1$ is a primitive element of $\mathrm{NS}(J,\lambda)$ and $q_{(J,\lambda)}(\bar{D}_1) = q_{N,d,m,k,r}(1,0) = N^2$, so by [6], Theorem 18, there is an elliptic subgroup $E' \leq J$ such that $\bar{D}_1 = \mathrm{cl}'(E') + \langle\bar{\theta}\rangle$ and $(E'.\bar{\theta}) = N$, where $\bar{\theta} \in \mathrm{NS}'(J)$ is such that $\lambda_{\bar{K}} = \phi_{\bar{\theta}}$.

Let $E = (E')^{\perp}$, where $(E')^{\perp}$ is as in [6], Proposition 10(a). Applying the latter to $E \leq J$, and noting that $E^{\perp} = E'$, we have that (E, E', ψ, π) is an N-presentation of (J,λ), for some $\psi : E[N] \to E'[N]$ and isogeny $\pi : A := E \times E' \to J$. Furthermore, by [6], equation (6), we have that

$$\pi^*E \;\equiv\; N^2\theta_{E'} \quad \text{and} \quad \pi^*E' \;\equiv\; N^2\theta_E, \tag{46}$$

where $\theta_E = \mathrm{pr}_E^*0_E = \mathbf{D}'(1,0,0)$ and $\theta_{E'} = \mathrm{pr}_{E'}^*0_{E'} = \mathbf{D}'(0,1,0)$.

We next observe that there exists a $\tilde{D}_2 \in \mathrm{NS}'(J)$ such that

$$\bar{D}_2 \;\equiv\; \tilde{D}_2 + \langle\bar{\theta}\rangle \quad \text{and} \quad (\tilde{D}_2.\bar{\theta}) \;=\; T_3 \;:=\; r\bar{N} + knd. \tag{47}$$

Indeed, by [4], Lemma 30, such a divisor class $\tilde{D}_2$ exists if and only if $T_3 \equiv T_2 \,(\mathrm{mod}\ 2)$, where $T_2 := q_{(J,\lambda)}(\bar{D}_2)$. To verify this congruence, note that by (45) and the definition of $q_{N,m,d,k,r}$ we have that $T_2 = q_{(J,\lambda)}(\bar{D}_2) = q_{N,m,d,k,r}(0,1) = n^2t + 2k(t-d)r + \bar{N}^2r^2$, where $n = (k^2d+1)/\bar{N}$. Now since $t = d(k^2d+4) \equiv (kd)^2 \equiv kd \,(\mathrm{mod}\ 2)$, we see that $nt - kd \equiv (n-1)kd \,(\mathrm{mod}\ 2)$, and hence $n(nt-kd) \equiv 0 \,(\mathrm{mod}\ 2)$. Thus $T_2 - T_3 = \bar{N}^2r^2 + 2k(t-d)r + n^2t - (r\bar{N} + knd) \equiv r\bar{N}(r\bar{N}-1) + n(nt-kd) \equiv 0 \,(\mathrm{mod}\ 2)$, and so there exists $\tilde{D}_2 \in \mathrm{NS}'(J)$ satisfying (47).

Put $\mathcal{G} = \mathbb{Z}\bar{\theta} + \mathbb{Z}\tilde{D}_1 + \mathbb{Z}\tilde{D}_2$, where $\tilde{D}_1 = E'$, and let $\tilde{\mathcal{H}}'$ be the primitive hull of $\pi^*\mathcal{G}$ in $\mathrm{NS}'(A)$. Since $\bar{\mathcal{G}} = \mathcal{G}/\langle\bar{\theta}\rangle$ is primitive in $\mathrm{NS}'(J,\lambda) = \mathrm{NS}'(J)/\langle\bar{\theta}\rangle)$, we see that $\mathcal{G}$ is primitive in $\mathrm{NS}'(J)$. Thus $\pi^*\mathcal{G}$ is primitive in $\pi^*\mathrm{NS}'(J)$, and so it follows that $\tilde{\mathcal{H}}' \cap \pi^*\mathrm{NS}'(J) = \pi^*\mathcal{G}$.

By (46) we see that $\theta_E, \theta_{E'} \in \tilde{\mathcal{H}}'$. Since $\mathrm{rank}(\tilde{\mathcal{H}}') = \mathrm{rank}(\pi^*\mathcal{G}) = \mathrm{rank}(\mathcal{G}) = 3$, it follows that $\tilde{\mathcal{H}}' = \mathbb{Z}\theta_E + \mathbb{Z}\theta_{E'} + \mathbb{Z}\mathbf{D}'(0,0,h)$, for some $h \in \mathrm{End}(E,E')$. Note that h is necessarily cyclic because $\mathbb{Z}h = \mathbf{D}_{E,E'}^{-1}(\tilde{\mathcal{H}}')/\mathbf{D}_{E,E'}^{-1}(\langle\theta_E, \theta_{E'}\rangle)$ is primitive in $\mathrm{Hom}(E,E')$. Thus $\tilde{\mathcal{H}}' = \tilde{\mathcal{H}}$, where $\mathcal{H} = \mathbb{Z}h$.

Put $d' = \deg(h)$ and $m' = m_\psi(\mathcal{H})$. Then the proof of Theorem 25(e) (applied to (E,E',ψ)) shows that the restriction of $q_{(J,\lambda)}$ to $\bar{\mathcal{G}}$ has type (N,m',d') because $\bar{\mathcal{G}} = \mathcal{G}/\langle\bar{\theta}\rangle$ and $\tilde{\mathcal{H}} \cap \pi^*\mathrm{NS}'(J) = \pi^*\mathcal{G}$. Thus, this restriction has discriminant $-16d'(m')^2$.

On the other hand, by (45) this restriction has discriminant $-16dm^2 = \mathrm{disc}(q_{N,m,d,k,r})$, so $d'(m')^2 = dm^2$. Now since $\gcd(\bar{N}, d) = 1$ by (31), we see that $\gcd(dm^2, N^2) = m^2$ and similarly $\gcd(d'(m')^2, N^2) = (m')^2$. Thus $m' = m$ and $d' = d$.

We next determine $\pi^*\tilde{D}_2$. Since $\pi^*\tilde{D}_2 \in \tilde{\mathcal{H}}$, we have $\pi^*\tilde{D}_2 = \mathbf{D}'(a, b, ch)$, for some $a, b, c \in \mathbb{Z}$. Put $\Gamma_h^* := \mathbf{D}'(0, 0, h)$. Then we have

$$\pi^*\bar{\theta} \;=\; N\theta, \quad \pi^*\tilde{D}_1 \;=\; N^2\theta_E \quad \text{and} \quad \pi^*\tilde{D}_2 \;=\; b\theta + (a-b)\theta_E + c\Gamma_h^*. \tag{48}$$

Since $(\theta, \theta_E, \Gamma_h^*)$ is a basis of $\mathcal{H}$ and $(\pi^*\bar{\theta}, \pi^*\tilde{D}_1, \pi^*\tilde{D}_2)$ is one of $\pi^*\mathcal{G}$, we see from (48) that $[\tilde{\mathcal{H}} : \pi^*\mathcal{G}] = |N \cdot N^2 \cdot c|$. On the other hand, since $\tilde{\mathcal{H}} \cap \pi^*\mathrm{NS}'(J) = \pi^*\mathcal{G}$, we have by Theorem 22 that $[\tilde{\mathcal{H}} : \pi^*\mathcal{G}] = mN^3$, and so we see that $|c| = m$. Thus, by replacing h by $-h$ if $c < 0$, we may assume that $m = c$. We now show:

$$a \;=\; m(k(t-2d) + \bar{N}^2 r), \quad b \;=\; -mkd \quad \text{and so} \quad \pi^*(\tilde{D}_2) \;=\; m(rD_1 + D_2). \tag{49}$$

To prove this, write $q = \tilde{q}_{(J,\lambda)}$. Then by (15) we have that

$$q(D + D') - q(D) - q(D') \;=\; 2(D.\bar{\theta})(D'.\bar{\theta}) - 4(D.D'), \quad \forall D, D' \in \mathrm{NS}'(J). \tag{50}$$

We apply this to $D = \tilde{D}_1$ and $D' = \tilde{D}_2$. Since $(\tilde{D}_1.\bar{\theta}) = (E'.\bar{\theta}) = m\bar{N}$ and $(\tilde{D}_2.\bar{\theta}) = T_3$ by (47) and since $q(\tilde{D}_1 + \tilde{D}_2) - q(\tilde{D}_1) - q(\tilde{D}_2) = 2mT_1$ by (45), we see that

$$4(\tilde{D}_1.\tilde{D}_2) \;=\; 2m\bar{N}T_3 - 2mT_1 \;=\; -4mkd, \tag{51}$$

where the second equality holds because $T_1 = \bar{N}^2 r + k(t-d) = \bar{N}^2 r + kd(\bar{N}n + 2) = \bar{N}T_3 + 2kd$. From this and (47) we see that $N^2 b = N^2(\theta_E.\pi^*\tilde{D}_2) = (\pi^*\tilde{D}_1.\pi^*\tilde{D}_2) = N^2(\tilde{D}_1.\tilde{D}_2) = -N^2 mkd$, which proves the second equality of (49). Moreover, since $N(a+b) = N(\theta.\pi^*\tilde{D}_2) = (\pi^*\bar{\theta}.\pi^*\tilde{D}_2) = N^2(\bar{\theta}.\tilde{D}_2) = N^2 T_3$ by (47), we see that $a = NT_3 - b = m(\bar{N}T_3 + kd) = m(T_1 - kd) = m(k(t-2d) + \bar{N}^2 r)$. This proves the first equality of (49), and it is clear that the third equality follows from the first two.

Since $m = m_\psi(\mathbb{Z}h)$, we have by Theorem 25(a) that $\psi_{\bar{N}} = \rho_{\bar{N}}(k'h)$ for some $k' \in \mathbb{Z}$, and then $m\psi = mk'h$. Thus, applying [6], Corollary 40, to $D = \pi^*\tilde{D}_2 = m\mathbf{D}(a', b', h)$, where $a' = k(t-2d) + \bar{N}^2 r$ and $b' = -kd$, we see that $\rho_{\bar{N}}(h) = \rho_{\bar{N}}(b'k'h) = \rho_{\bar{N}}(-kdk'h)$. Since $-k^2 d \equiv 1 \,(\mathrm{mod}\ \bar{N})$, we have that $\rho_{\bar{N}}(-k^2 dh) = \rho_{\bar{N}}(h) = \rho_{\bar{N}}(-kdk'h)$, and so $\rho_{\bar{N}}(kh) = \rho_{\bar{N}}(k'h)$ because $\gcd(kd, \bar{N}) = 1$. Thus $\psi_{\bar{N}} = \rho_{\bar{N}}(k'h) = \rho_{\bar{N}}(kh)$, and hence (31) holds.

(b) From part (a) we know that $\tilde{\mathcal{H}} \cap \pi^*\mathrm{NS}'(J) = \pi^*\mathcal{G}$, and that $(\pi^*\theta, \pi^*\tilde{D}_1, \pi^*\tilde{D}_2)$ is a basis of $\pi^*\mathcal{G}$. Thus, (44) follows from (46) and (49). The last assertion follows from Theorem 25(c), (d) because $m(rD_1 + D_2) \in \pi^*\mathrm{NS}'(J)$ by (49).

(c) In view of part (b) we are in the situation of Theorem 25 and so $q_{\tilde{\mathcal{G}}} \sim q_{N,m,d,k,r} \sim q_{M,N,d,k}$ by Proposition 28. $\square$

5 The existence theorem

We now prove that for every binary quadratic form q of type (N, m, d) there exists a principally polarized abelian surface (A, λ) such that its refined Humbert invariant $q_{(A,\lambda)}$ is equivalent to q. As a first step for this, we prove:

Theorem 32 (Existence Theorem) *Let E/K and E'/K be two elliptic curves over an algebraically closed field $K = \overline{K}$ with the property that the degree form $q_{E,E'}$ primitively represents $d \geq 1$. Then for any binary quadratic form q of type (N, m, d) with $\mathrm{char}(K) \nmid N$ there exists an anti-isometry $\psi : E[N] \to E'[N]$ such that the refined Humbert invariant $q_{(A_\psi,\lambda_\psi)}$ of the abelian variety $A_\psi = A/\mathrm{Graph}(-\psi)$ primitively represents q.*

Proof. By hypothesis, there is a cyclic isogeny $h \in \mathrm{Hom}(E, E')$ with $\deg(h) = d$, and by Theorem 16 there is a primitive matrix M of discriminant $-d$ such that q is equivalent to $q_{M,N}$.

To find the desired anti-isometry ψ, fix an anti-isometry $\psi' : E[N] \to E'[N]$ and a basis $\mathcal{B} = (P_1, P_2)$ of $E[N](K)$. Then by Remark 29 there is primitive matrix M' of discriminant $-d$ such that $[(\psi')^{-1}\rho_N(h)]_{\mathcal{B}} \equiv M' \pmod N$.

Since M and M' are both primitive of discriminant $-d$, there are matrices $M_1, M_2 \in \mathrm{SL}_2(\mathbb{Z})$ such that $M_1 M M_2 = M'$. Put $P = (M_1 M_2)^{-1} \in \mathrm{SL}_2(\mathbb{Z})$ and let $g \in \mathrm{End}(E[N])$ be such that $[g]_{\mathcal{B}} \equiv P \pmod N$. Then $\psi := \psi' \circ g$ is an anti-isometry and $[\psi^{-1}\rho_N(h)]_{\mathcal{B}} = [g^{-1}(\psi')^{-1}\rho_N(h)]_{\mathcal{B}} \equiv PM' \equiv M_2^{-1} M M_2 \pmod N$. By Proposition 28 (and Remark 29) we see that $q_{(A_\psi,\lambda_\psi)}$ primitively represents $q_{M_2^{-1}MM_2,N}$. But $q_{M_2^{-1}MM_2,N} = q_{M,N}$ by Corollary 13 and so the assertion follows. □

Corollary 33 *Let E be an elliptic curve over an algebraically closed field K, and let q be a binary quadratic form of type (N, m, d) with $\mathrm{char}(K) \nmid N$. Then there exists a principally polarized abelian surface (A, λ) with A isogenous to $E \times E$ such that $q_{(A,\lambda)}$ primitively represents q. In particular, if $\mathrm{End}(E) = \mathbb{Z}$, then $q_{(A,\lambda)}$ is equivalent to q.*

Moreover, if $q(X, Y) \neq 1$, for all $X, Y \in \mathbb{Z}$, and if $\mathrm{End}(E) = \mathbb{Z}$, then there is a curve C/K such that q_C is equivalent to q.

Proof. It is well-known that there exists a cyclic subgroup scheme $H \leq E$ of order d. (Indeed, if $\mathrm{char}(K) \nmid d$, then we can take $H = \langle P \rangle$, where $P \in E(K)$ is a point of order d. On the other hand, if $d = p^r d_0$, where $p = \mathrm{char}(K) > 0$ and $p \nmid d_0$, then we can take $H = F_{p^r}^{-1}(\langle P_0 \rangle)$, where $F_{p^r} : E \to E^{(p^r)}$ denotes the Frobenius morphism and $P_0 \in E^{(p^r)}(K)$ has order d_0.) Let $h : E \to E' := E/H$ be the associated cyclic isogeny. Then $q_{E,E'}$ primitively represents d, and so the first assertion follows directly from Theorem 32 because $A_\psi \sim E \times E' \sim E \times E$.

Moreover, if $\mathrm{End}(A) = \mathbb{Z}$, then $\mathrm{rank}(\mathrm{NS}(A_\psi)) = \mathrm{rank}(\mathrm{NS}(E \times E)) = 3$, so $q_{(A_\psi,\lambda_\psi)}$ is also a binary quadratic form and hence it follows that $q_{(A_\psi,\lambda_\psi)}$ is equivalent to q.

The last assertion follows immediately from Proposition 6 of [4], which states that the given condition on $q \sim q_{(A_\psi,\lambda_\psi)}$ is equivalent to the condition that $(A_\psi, \lambda_\psi) \simeq (J_C, \lambda_C)$ for some curve C/K of genus 2. □

Corollary 34 *Let K be an algebraically closed field which is not the algebraic closure of a finite field, and let q be a binary quadratic form of type (N, m, d) with $\mathrm{char}(K) \nmid N$. Then there exists a principally polarized abelian surface (A, λ) over K such that $q_{(A,\lambda)}$ is equivalent to q. Moreover, if $q(X, Y) \neq 1$, for all $X, Y \in \mathbb{Z}$, then there is a curve C/K such that q_C is equivalent to q.*

Proof. Since K is not the algebraic closure of a finite field, there exists an elliptic curve E/K with $\mathrm{End}(E) = \mathbb{Z}$. Thus the assertions follow from Corollary 33. □

6 Application to elliptic involutions

We now consider the special case that C/K is a curve of genus 2 which has a presentation (E, E', ψ) of degree 2. As we shall see presently, this is equivalent to assumption that C/K has an *elliptic involution*, i.e., an automorphism $\sigma \in \mathrm{Aut}(C)$ of order 2 such that $\sigma \neq \sigma_C$, where σ_C denotes the hyperelliptic involution of C. Let $I(C)$ denote the set of elliptic involutions, and for $\sigma \in \mathrm{Aut}(C)$ let $f_\sigma : C \to C_\sigma := C/\langle\sigma\rangle$ denote the quotient cover.

Proposition 35 *The rule $\sigma \mapsto f_\sigma$ defines a bijection between the set $I(C)$ of elliptic involutions and the set $\mathcal{E}_2(C)$ of equivalence classes of elliptic subcovers of C/K, and hence the rule $\sigma \mapsto E_\sigma := f_\sigma^* J_{C_\sigma}$ defines a bijection between $I(C)$ and the set $\mathcal{S}_2(J_C, \lambda_C)$ of elliptic subgroups of J_C of λ_C-degree 2.*

Proof. Let $\sigma \in I(C)$. Since $\deg(f_\sigma) = \mathrm{ord}(\sigma) = 2$, the uniqueness of the hyperelliptic cover implies that $g_{C_\sigma} > 0$, and hence $g_{C_\sigma} = 1$ by Riemann-Hurwitz. By [5], Corollary 1.4, C_σ has a K-rational point and hence f_σ is an elliptic subcover of degree 2. Note that f_σ is uniquely defined by σ up to equivalence of covers. We thus obtain a map $f_C : I(C) \to \mathcal{E}_2(C)$. This map is injective because if f_σ is equivalent to $f_{\sigma'}$, then $\langle\sigma\rangle = \mathrm{Gal}(f_\sigma) = \mathrm{Gal}(f_{\sigma'}) = \langle\sigma'\rangle$, and hence $\sigma = \sigma'$. Moreover, this map is surjective because if $f : C \to E$ is an elliptic subcover of degree 2, then it is separable and hence Galois, so $\mathrm{Gal}(f) = \langle\sigma\rangle$ with $\sigma \in I(C)$, and then f_σ is equivalent to f. This proves the first statement, and the second statement follows from [6], Theorems 20 and 18. □

Proposition 36 *Let $\sigma \in I(C)$, and put $\sigma' = \sigma\sigma_C$. Then $\sigma' \in I(C)$ and there exists an isomorphism $\psi_\sigma : E_\sigma[2] \to E_{\sigma'}[2]$ and an isogeny $\pi_\sigma : E_\sigma \times E_{\sigma'} \to J_C$ such that $(E_\sigma, E_{\sigma'}, \psi_\sigma, \pi_\sigma)$ is a 2-presentation of C/K. Moreover, every 2-presentation of C/K is of this form.*

Proof. Since σ_C lies in the centre of $\mathrm{Aut}(C)$, we see that σ and σ_C commute, and so it follows that $\sigma' \neq \sigma_C$ has order 2, so $\sigma' \in I(C)$. We next show that $(E_\sigma)^\perp = E_{\sigma'}$ in the notation of [6], Proposition 10.

For this, consider $f_G : C \to C/G$, where $G := \langle \sigma, \sigma_C \rangle$, and let $\bar{f}_\sigma : C_\sigma \to C/G$ and $\bar{f}_{\sigma'} : C_{\sigma'} \to C/G$ be the unique maps such that $\bar{f}_\sigma \circ f_\sigma = f_G$ and $\bar{f}_{\sigma'} \circ f_{\sigma'} = f_G$. Note that G is a Klein 4-group, so $\bar{f}_\sigma$ and $\bar{f}_{\sigma'}$ also have degree 2. It thus follows (cf. [5], Lemma 3.3) that $(f_\sigma)_*(f_{\sigma'})^*(D) = (\bar{f}_\sigma)^*(\bar{f}_{\sigma'})_*(D)$, for all $D \in \mathrm{Div}(C_{\sigma'})$, and so $(f_\sigma)_*(f_\sigma)^*(D) \sim 0$, for all $D \in \mathrm{Div}^0(C_{\sigma'})$ because $(\bar{f}_{\sigma'})_*(D) \sim 0$ as $g_{\bar{C}} = 0$. From [6], Remark 13, we thus see that $E_{\sigma'} = f^*_{\sigma'} J_{C_{\sigma'}} = (f^*_\sigma J_{C_\sigma})^\perp = (E_\sigma)^\perp$, as claimed.

Now since $E_{\sigma'} = (E_\sigma)^\perp$, we have $f_{\sigma'} = (f_\sigma)^\perp$ in the notation of [6], Corollary 12, and so by that corollary there exists an isomorphism $\psi_\sigma : E_\sigma[2] \to E_{\sigma'}[2]$ and an isogeny $\pi_\sigma : E_\sigma \times E_{\sigma'} \to J_C$ such that $(E_\sigma, E_{\sigma'}, \psi_\sigma, \pi_\sigma)$ is a 2-presentation of C/K.

Moreover, if (E, E', σ, π) is a 2-presentation of C/K, then by Proposition 10(b) of [6] we know that E and E' are isomorphic to elliptic subgroups $\bar{E}, \bar{E}' \in \mathcal{S}_2(J_C, \lambda_C)$ with $\bar{E}' = \bar{E}^\perp$, and so $\bar{E} = E_\sigma$ and $\bar{E}' = E_{\sigma\sigma_C}$ for some $\sigma \in I(C)$ by Proposition 35 and by what was proved above. □

Corollary 37 *Let C/K be curve of genus 2, where $\mathrm{char}(K) \neq 2$, and let $d \geq 1$. Then the following conditions are equivalent.*

(i) *There exists $\sigma \in I(C)$ and a cyclic isogeny $h : E_\sigma \to E_{\sigma\sigma_C}$ of degree d.*

(ii) *q_C primitively represents a binary form of type $(2, m, d)$, with $m = 1$ or $m = 2$.*

Proof. (i) ⇒ (ii): By Proposition 36, there exist ψ and π such that $(E_\sigma, E_{\sigma\sigma_C}, \psi, \pi)$ is a 2-presentation of C/K. Since $h \in \mathrm{Hom}(E_\sigma, E_{\sigma\sigma_C})$ is cyclic of degree d, Theorem 25 shows that q_C primitively represents a binary form of type $(2, m, d)$ with $m|2$.

(ii) ⇒ (i): By Theorem 16 we may assume that the binary form q represented by q_C is $q = q_{2,m,d,k,r}$, for some suitable $k, r \in \mathbb{Z}$ with $k^2 d \equiv -1 \,(\mathrm{mod}\, \frac{2}{m})$. Applying Theorem 31 shows that there exists an 2-presentation (E, E', ψ, π) of C/K and a cyclic isogeny $h \in \mathrm{Hom}(E, E')$ of degree d. By Proposition 36 we have that there exists an elliptic involution σ on C such E and E' are as in (i), and so the assertion follows. □

Remark 38 In their paper, Accola and Previato[1] mention on p. 141-142 that "a condition for [two degree-2 elliptic subcovers] being isogenous to any degree does not appear to be known". The above result can be viewed as a contribution towards filling in this knowledge gap. In particular, we can use it to prove the following result.

Corollary 39 *Let E/K be an elliptic curve with $\mathrm{End}(E) = \mathbb{Z}$, where K is an algebraically closed field of $\mathrm{char}(K) \neq 2$, and let $d \geq 1$ be an integer. Then there exists a curve C/K with two elliptic subcovers $f : C \to E_i$ of degree 2 and a cyclic isogeny $h : E_1 \to E_2$ of degree d such that $E_1 \simeq E$.*

Proof. Let q be a binary form of type $(2, m, d)$, where $m|2$. Then q is equivalent to one of the forms listed in Proposition 19. Now all the forms listed there with the exception of the form $[4, 0, 1]$, which has type $(2, 1, 1)$, are reduced, so have 4 as their minimum, and hence satisfy condition (iv) of Theorem 1. (Thus, for $d = 1$ take $m = 2$.) By Corollary 33 we thus see that there exists a curve C/K with q_C equivalent to q, so C satisfies condition (ii) of Corollary 37, and hence the assertion follows from condition (i) of the corollary. □

We now study the case that C/K has several elliptic involutions in some detail. We first observe:

Proposition 40 *Let $\sigma_1, \sigma_2 \in I(C)$ and put $\bar{E}_{\sigma_1} = E_\sigma + \mathbb{Z}\theta_C \in \mathrm{NS}(J_C, \lambda)$ and $\bar{M} = \bar{M}(\sigma_1, \sigma_2) = \mathbb{Z}\bar{E}_{\sigma_1} + \mathbb{Z}\bar{E}_{\sigma_2}$. If $\sigma_2 \neq \sigma_1, \sigma_1\sigma_C$, then $\mathrm{rank}\bar{M} = 2$ and*

$$q_C(X\bar{E}_{\sigma_1} + Y\bar{E}_{\sigma_2}) \;=\; 4X^2 + 4rXY + 4Y^2, \quad \textit{for all } X, Y \in \mathbb{Z}, \tag{52}$$

where $r = 2 - (E_{\sigma_1}.E_{\sigma_2})$. Furthermore, $|r| \leq 1$.

Proof. In view of (the proof of) Proposition 36, the hypothesis implies that $E_{\sigma_2} \neq E_{\sigma_1}, (E_{\sigma_1})^\perp$, so $\bar{E}_{\sigma_2} \neq \pm\bar{E}_{\sigma_1}$. Thus, since $\bar{E}_{\sigma_i}$ is primitive in $\mathrm{NS}(J_C, \lambda_C)$ (cf. [6], Theorem 18), it follows that $\bar{E}_{\sigma_1}$ and $\bar{E}_{\sigma_2}$ are linearly independent, so $\mathrm{rank}(\bar{M}) = 2$.

Since $q_C(\bar{E}_{\sigma_i}) = 4$ (cf. [6], Theorem 18) and since $q_C(\bar{E}_{\sigma_1} + \bar{E}_{\sigma_2}) = 4^2 - 2(E_{\sigma_1} + E_{\sigma_2})^2 = 16 - 4(E_{\sigma_1}.E_{\sigma_2}) = 8 + 4r$, we see that (52) holds.

Moreover, since $E_{\sigma_2} \neq E_{\sigma_1}^\perp = E_{\sigma_1\sigma_C}$, we have that $(E_{\sigma_2}.E_{\sigma_1}^\perp) \geq 1$. Thus, since $E_{\sigma_1} + E_{\sigma_1}^\perp = 2\theta_C$, we have that $1 \leq (E_{\sigma_2}.E_{\sigma_1}) = 4 - (E_{\sigma_2}.E_{\sigma_1}^\perp) \leq 3$, and so we see that $|r| \leq 1$. □

Corollary 41 *In the situation of* Proposition 40 *we have that $\bar{M}(\sigma_1, \sigma_2)$ is a primitive submodule of $\mathrm{NS}(J_C, \lambda_C)$. Thus, q_C primitively represents the form q, where $q = [4, 0, 4]$, if $r = 0$, and $q = [4, 4, 4]$, if $r = \pm 1$.*

Proof. Let $\bar{M}'$ be the primitive hull of $\bar{M} = \bar{M}(\sigma_1, \sigma_2)$ in $\mathrm{NS}(J_C, \lambda_C)$, and put $c = [\bar{M}' : \bar{M}]$. Let q' and q be the restriction of q_C to $\bar{M}'$ and to $\bar{M}$, respectively. By Theorem 31 we know that q' has type $(2, m, d)$, for some (unique) integers m, d, so $\mathrm{disc}(q') = -16m^2d$ and hence $\mathrm{disc}(q) = -16m^2c^2d$.

Now if $r = \pm 1$, then $q \sim [4, \pm 4, 4]$ by the proposition, so $\mathrm{disc}(q) = -16 \cdot 3$, and hence $m^2c^2d = 3$, which shows that $m = c = 1$ and $d = 3$. Thus, $\bar{M} = \bar{M}'$ is primitive, and $q \sim [4, 4, 4]$. On the other hand, if $r \neq \pm 1$, then $q \sim [4, 0, 4]$ by the proposition, so $\mathrm{disc}(q) = -16 \cdot 4$, and hence $m^2c^2d = 4$. If $c \neq 1$, then $c = 2$, $m = 1$ and $d = 1$, so q' has type $(2, 1, 1)$. Thus $q \sim [4, 0, 1]$ (cf. Proposition 19), which represents 1 and hence does not satisfy property (iv) of Theorem 1, contradiction. Thus, $c = 1$ and hence $\bar{M} = \bar{M}'$ is primitive and $q \sim [4, 0, 4]$. □

Note that the above results are valid for an arbitrary ground field K. In order to analyze the above situation further, it is useful to impose some mild restrictions on the characteristic of K.

Proposition 42 *Let $\sigma_1, \sigma_2 \in I(C)$ be such that $\sigma_2 \neq \sigma_1, \sigma_1\sigma_C$, and put $\sigma = \sigma_1\sigma_2$ and $n := \mathrm{ord}(\sigma)$. Then $G := \langle \sigma_1, \sigma_2 \rangle \simeq D_n$ is a dihedral group of order $2n$. Moreover, if $\mathrm{char}(K) \neq 2$, then $n = 3$, 4, or 6, and if n is even, then $\sigma^{n/2} = \sigma_C$.*

Proof. The first assertion is clear by elementary group theory. To prove the other assertions, assume that $\mathrm{char}(K) \neq 2$. Moreover, we may assume without loss of generality that K is algebraically closed. Then the set $W_C = \mathrm{Fix}(\sigma_C)$ of Weierstrass points of C consists of 6 distinct points. Since each $\tau \in \mathrm{Aut}(C)$ commutes with σ_C, we see that τ permutes the elements of W_C. We first show:

Claim: $\tau \in \mathrm{Aut}(C)$ acts trivially on $W_C \Leftrightarrow \tau = 1$ or $\tau = \sigma_C$.

Indeed, if $\tau \neq 1$ acts trivially, then τ has at least 6 fixed points, so the different divisor $\mathrm{Diff}(f_\tau)$ of $f_\tau : C \to C_\tau = C/\langle\tau\rangle$ has degree at least $6(m-1)$, where $m = \mathrm{ord}(\tau)$. Thus, by Riemann-Hurwitz we have $m(-2) + 6(m-1) \leq 2$, so $m \leq 2$. If $m = 2$ and $\tau \neq \sigma_C$, then τ has no fixed points on W_C because $\langle \tau, \sigma_C \rangle$ is a Klein 4-group, so f_σ and f_{σ_C} have disjoint ramification. Since this is a contradiction, we must have $\tau = \sigma_C$. This proves the claim because the other implication is trivial.

Let $\bar{\sigma}_i \in \mathrm{Sym}(W_C) \simeq S_6$ be the permutation induced by σ_i, for $i = 1, 2$. By the claim and our hypotheses have that $\bar{\sigma}_1 \neq \bar{\sigma}_2$. Moreover, since σ_i does not have any fixed points on W_C, we see that $\bar{\sigma}_i$ is a $(2,2,2)$-cycle. Then $\bar{\sigma} = \bar{\sigma}_1\bar{\sigma}_2$ is either a $(2,2)$-cycle (if $\bar{\sigma}_1$, $\bar{\sigma}_2$ have a common transposition) or a $(3,3)$-cycle, as is easy to check. Thus $\mathrm{ord}(\bar{\sigma}) = 2$ or 3, and so σ has order $2, 3, 4$ or 6. Now $\mathrm{ord}(\sigma) \neq 2$ because in that case $\sigma \in I(C)$ and so $\bar{\sigma}$ is a $(2,2,2)$-cycle and not a $(2,2)$-cycle as above. This proves that $n = 3, 4$ or 6.

To prove the last assertion, note that if n is even, then the above shows that $\bar{\sigma}$ is an $(\frac{n}{2}, \frac{n}{2})$-cycle, so $\bar{\sigma}^{n/2} = (1)$, and hence $\sigma^{n/2} = \sigma_C$ by the claim. □

Proposition 43 *Let $\sigma_1, \sigma_2, \sigma$ be as in* Proposition 42*, and assume that* $\mathrm{char}(K) \neq 2$.

(a) *If* $\mathrm{ord}(\sigma) = 4$*, then* $(E_{\sigma_1}.E_{\sigma_2}) = 2$.

(b) *If* $3|n := \mathrm{ord}(\sigma)$ *and if* $\mathrm{char}(K) \neq 3$*, then* $(E_{\sigma_1}.E_{\sigma_2}) = \begin{cases} 3 & \text{if } n = 3, \\ 1 & \text{if } n = 6. \end{cases}$

Proof. Again, we may assume without loss of generality that K is algebraically closed. Fix $P_0 \in C(K)$ and consider the map $\varphi_i = \varphi_{\sigma_i, P_0} : C(K) \to J_C(K)$ defined by

$$\varphi_i(P) \;=\; \mathrm{cl}(f_{\sigma_i}^*(f_{\sigma_i})_*(P - P_0)) \;=\; \mathrm{cl}(P - P_0 + \sigma_i(P) - \sigma_i(P_0)), \quad \text{for } P \in C(K).$$

To analyze this map we first observe that if $P \in C(K)$ and if $\sigma_i' := \sigma_C\sigma_i$, then

$$h^0(P + \sigma_i(P)) > 1 \;\Leftrightarrow\; \exists P' : P + \sigma_i(P) = P' + \sigma_C(P') \;\Leftrightarrow\; P \in \mathrm{Fix}(\sigma_i'). \tag{53}$$

Indeed, $h^0(P+\sigma_i(P)) > 1$ if and only if $P+\sigma_i(P)$ is a canonical divisor of C. Now every effective canonical divisor on C is of the form $P+\sigma_C(P')$, for $P' \in C(K)$, and so the first equivalence follows. To verify the second, note that if $P+\sigma_i(P) = P'+\sigma_C(P')$, then either $P = P'$ and $\sigma_i(P) = \sigma_C(P')$, so $P = \sigma_C\sigma_i(P) \in \mathrm{Fix}(\sigma_i')$ or $P = \sigma_C(P')$ and $\sigma_i(P) = P'$, so $P = \sigma_i\sigma_C(P) \in \mathrm{Fix}(\sigma_i')$. Conversely, if $P \in \mathrm{Fix}(\sigma_i')$, then $\sigma_i(P) = \sigma_C(P)$, so $P+\sigma_i(P) = P+\sigma_C(P)$. This proves (53).

Using (53), we see easily that

$$\varphi_i(P_1) \,=\, \varphi_i(P_2) \quad \Leftrightarrow \quad P_2 \,=\, P_1 \text{ or } P_2 \,=\, \sigma_i(P_1). \tag{54}$$

Indeed, clearly $\varphi_i(P_1) = \varphi_i(P_2) \Leftrightarrow \mathrm{cl}(P_1+\sigma_i(P_1)) = \mathrm{cl}(P_2+\sigma_i(P_2))$. If $h^0(P_1+\sigma_i(P_1)) = 1$, then this latter condition is equivalent to the equality $P_1+\sigma_i(P_1) = P_2+\sigma_i(P_2)$, and so (54) follows in this case. If $h^0(P_1+\sigma_i(P_1)) > 1$, then by (53) we see that the latter condition is equivalent to $P_1, P_2 \in \mathrm{Fix}(\sigma_i')$. Now if $P \in \mathrm{Fix}(\sigma_i')$, then $\mathrm{Fix}(\sigma_i') = \{P, \sigma_i(P)\}$ because $|\mathrm{Fix}(\sigma_i')| = 2$ and σ_i and σ_i' commute and have disjoint fixed points. This proves (54) in this case as well.

Now suppose that $P_0 \in \mathrm{Fix}(\sigma)$, i.e., that $\sigma_1(P_0) = \sigma_2(P_0)$. Then we have:

$$\varphi_1(P) \,\in\, E_{\sigma_1}(K) \cap E_{\sigma_2}(K) \quad \Leftrightarrow \quad P \,\in\, \mathrm{Fix}(\sigma) \cup \mathrm{Fix}(\sigma_1'). \tag{55}$$

Indeed, since $\varphi_i(C(K)) = E_{\sigma_i}(K)$, for $i = 1, 2$, we see that the condition of the left side of (55) is equivalent to the condition that $\varphi_1(P) = \varphi_2(P')$, for some $P' \in C(K)$. This in turn is equivalent to $\mathrm{cl}(P+\sigma_1(P)) = \mathrm{cl}(P'+\sigma_2(P'))$ because $\sigma_1(P_0) = \sigma_2(P_0)$. If $h^0(P+\sigma_1(P)) = 1$, then this is equivalent to $P+\sigma_1(P) = P'+\sigma_2(P')$, for some $P' \in C(K)$, which in turn is equivalent to $P \in \mathrm{Fix}(\sigma)$. On the other hand, if $h^0(P+\sigma_1(P)) > 1$, then by (53) we have that $P \in \mathrm{Fix}(\sigma_1')$. Conversely, if $P \in \mathrm{Fix}(\sigma_1')$ then $\mathrm{cl}(P+\sigma_1(P)) = \mathrm{cl}(P'+\sigma_C(P')) = \mathrm{cl}(P'+\sigma_2(P')$ for $P' \in \mathrm{Fix}(\sigma_2')$, and so (55) follows.

(a) If $\mathrm{ord}(\sigma) = 4$, then $|\mathrm{Fix}(\sigma)| = 2$ (because $\mathrm{Fix}(\sigma) \subset \mathrm{Fix}(\sigma^2) = W_C$ and $\bar{\sigma}$ is a $(2,2)$-cycle), so $P_0 \in \mathrm{Fix}(\sigma)$ exists. Since $\mathrm{Fix}(\sigma) \subset W_C$ and $\mathrm{Fix}(\sigma_1')$ are disjoint, we see that $|\varphi_1(\mathrm{Fix}(\sigma) \cup \mathrm{Fix}(\sigma_1'))| \geq 2$. Thus, (54) and (55) show that $(E_{\sigma_1}.E_{\sigma_2}) \geq 2$. Moreover, since $\sigma_1\sigma_2' = \sigma\sigma_C$ also has order 4, we have by the same argument that $(E_{\sigma_1}.E_{\sigma_2'}) \geq 2$. But since $(E_{\sigma_1}.E_{\sigma_2}) + (E_{\sigma_1}.E_{\sigma_2'}) = 4$ (cf. the proof of Proposition 40), the assertion follows.

(b) Now assume that $\mathrm{char}(K) \neq 3$ and that $\mathrm{ord}(\sigma) = 3$. Since f_σ is tamely ramified, it follows from Riemann-Hurwitz that $|\mathrm{Fix}(\sigma)| = 1$ or 4. Since $\mathrm{Fix}(\sigma)$ is σ_C-stable, the first case implies that $\mathrm{Fix}(\sigma)$ has a fixed point under σ_C, which contradicts the fact that $\bar{\sigma}$ is a $(3,3)$-cycle. Thus $|\mathrm{Fix}(\sigma)| = 4$ (and $g_{C_\sigma} = 0$), so there exists $P_0 \in \mathrm{Fix}(\sigma)$. Now $\mathrm{Fix}(\sigma) \cap \mathrm{Fix}(\sigma_1') = \emptyset$ because $\langle\sigma_1'\rangle$ is a maximal cyclic subgroup of $\langle\sigma, \sigma_1'\rangle \simeq D_6$, so we obtain from (54) and (55) that $(E_{\sigma_1}.E_{\sigma_2}) \geq 3$. Since $(E_{\sigma_1}.E_{\sigma_2}) \leq 3$ by the proof of Proposition 40, this proves the assertion in this case.

Now suppose that $\mathrm{ord}(\sigma) = 6$. Since $\sigma^3 = \sigma_C$ by Proposition 42, we see that $\sigma_1\sigma_2' = \sigma\sigma_C = \sigma^4$ has order 3, so by the above (applied to σ_1, σ_2') we see that $(E_{\sigma_1}.E_{\sigma_2'}) = 3$, and hence $(E_{\sigma_1}.E_{\sigma_2}) = 4 - (E_{\sigma_1}.E_{\sigma_2'}) = 1$, as claimed. □

Remark 44 If K is algebraically closed and if $\mathrm{char}(K) \neq 2, 3$, then the above proof shows that

$$(E_{\sigma_1}.E_{\sigma_2}) = \tfrac{1}{2}|\mathrm{Fix}(\sigma_1\sigma_2)| + 1. \tag{56}$$

Indeed, if $\sigma := \sigma_1\sigma_2$ has order 4 or 3, then this was implicitly shown in the above proof. If $\mathrm{ord}(\sigma) = 6$, then $(E_{\sigma_1}.E_{\sigma_2}) = 1$ by Proposition 43(b), and we have $\mathrm{Fix}(\sigma) = \emptyset$ (because $\mathrm{Fix}(\sigma) \subset \mathrm{Fix}(\sigma^3) = W_C$ but $\bar{\sigma}$ has type $(3,3)$ and hence has no fixed points on W_C), so (56) holds in this case as well. Thus (56) holds because there are no other cases by Proposition 42.

Proof of Theorem 4. (a) Suppose first that we have a subgroup $G \leq \mathrm{Aut}(C)$ with $G \simeq D_n$, where $n = 4$ (respectively, $n = 6$). Then $G = \langle \sigma_1, \rho \rangle$, where $\mathrm{ord}(\rho) = n$ and $\mathrm{ord}(\sigma_1) = 2$. Put $\sigma_2 := \sigma_1\rho$. Then $\rho = \sigma_1\sigma_2$ and $\mathrm{ord}(\sigma_2) = 2$, so σ_1 and σ_2 do not commute and hence $\sigma_2 \neq \sigma_1, \sigma_1\sigma_C$. Thus, σ_1 and σ_2 satisfy the conditions of Corollary 41, and so q_C primitively represents $q = [4, 4r, 4]$ with $r = 2 - (E_{\sigma_1}, E_{\sigma_2})$. By Proposition 43 we see that $r = 0$ if $n = 4$ and $r = 1$ if $n = 6$. This proves one direction of the assertion.

Conversely, suppose that q_C primitively represents q_n, where $n = 4$ (respectively, $n = 6$). This means that there exist $\bar{D}_1, \bar{D}_2 \in \mathrm{NS}(J_C, \lambda_C)$ such that $q_C(X\bar{D}_1 + Y\bar{D}_2) = q_n(X, Y), \forall X, Y \in \mathbb{Z}$. Thus $q_C(\bar{D}_i) = 4$, for $i = 1, 2$, and so by [6], Theorem 18, there exist elliptic subgroups $E_i \leq J_C$ of degree 2 such that $E_i + \mathbb{Z}\theta_C = \bar{D}_i$, for $i = 1, 2$. By Proposition 35 we see that $E_i = E_{\sigma_i}$ with $\sigma_i \in I(C)$. Moreover, since $\bar{D}_2 \neq \pm\bar{D}_1$, it follows that σ_1 and σ_2 satisfy the hypotheses of Proposition 40, and so $(E_{\sigma_1}.E_{\sigma_2}) = 2 - r$, where $r = 0$ because $q_4 = [4, 0, 4]$ (respectively, $r = 1$ because $q_6 = [4, 4, 4]$). By Propositions 43 and 42 we thus have that $\mathrm{ord}(\sigma_1\sigma_2) = n$ and that $G := \langle \sigma_1, \sigma_2 \rangle \simeq D_n$, as desired.

(b) Note first that if N^2 is primitively represented by q_n, then it is also primitively represented by q_C, and so by [6], Theorem 20, each such representation gives rise to an elliptic subcover $f : C \to E$ of degree N.

Now N^2 is primitively represented by $q_4 = [4, 0, 4]$ (respectively, by $q_6 = [4, 4, 4]$) if and only if $2|N$ and N_1^2 is primitively represented by $[1, 0, 1]$, (respectively, by $[1, 1, 1]$), where $N_1 = \frac{N}{2}$. But it is well-known that N_1^2 is primitively represented by $[1, 0, 1]$ (respectively, by $[1, 1, 1]$) if and only if N_1^2 (and hence N_1) is a product of primes $p_i \equiv 1 \pmod 4$ (respectively, $p_i \equiv 1 \pmod 3$); cf. Satz 161 of Landau[8].

(c) Since q_C represents q_n, which has type $(2, m, d)$, for $(m, d) = (2, 1)$ (respectively, for $(m, d) = (1, 3)$), we see by Proposition 36 and Corollary 37 that $J_C \sim E_\sigma \times E_{\sigma'} \sim E_\sigma^2$. Thus, if $f : C \to E$ is any elliptic subcover, then E is an isogeny

factor of J_C and so $E \sim E_\sigma$. Thus, the hypothesis implies that $\mathrm{rank}(\mathrm{NS}(J_C, \lambda_C)) = 2$, and hence it follows that q_C is equivalent to q_n. Thus, by [6], Theorem 20, there is a bijection between the set $\mathcal{E}_N$ of equivalence classes of elliptic subcovers of degree N and the set of primitive representations of N^2 by q_n. Thus, the statement about the existence of subcovers follows from what was said in the proof of part (b). The last assertion about the number of subcovers follows from the corresponding assertion about representations of q_n; cf. Satz 161 of Landau[8]. □

It is interesting to note the following alternate characterization of curves whose automorphism groups contain D_4 as a subgroup.

Proposition 45 *Let C/K be a genus 2 curve, where $\mathrm{char}(K) \neq 2, 3$. Then there exists $G \leq \mathrm{Aut}(C)$ with $G \simeq D_4$ if and only if there is an elliptic curve E/K and a K-rational $\psi \in \mathrm{Aut}(E[2])$ of order 2 such that $J_C \simeq (E \times E)/\mathrm{Graph}(\psi)$.*

Proof. By the proof of Theorem 4(a), the first condition is equivalent to the existence of a 2-presentation $(E_\sigma, E_{\sigma'}, \psi, \pi)$ of J_C/K and a primitive submodule $\bar{M} = \bar{M}(\sigma, \sigma'')$ of $\mathrm{NS}(J_C, \lambda_C)$ such that the restriction of q_C is equivalent to $[4, 0, 4]$. Since the latter has type $(2, 2, 1)$, this implies by Corollary 37 that there is an isomorphism $h : E_\sigma \xrightarrow{\sim} E_{\sigma'}$. We can thus replace $E_{\sigma'}$ by $E := E_\sigma$ and adjust ψ and π accordingly to obtain a 2-presentation of the form (E, E, ψ, π) of J_C/K with $\psi \in \mathrm{Aut}(E[2]) \simeq \mathrm{GL}_2(2) \simeq S_3$. Now since $[4, 0, 4] = q_{2,2,1,0,0}$, it follows from Theorem 25(d) that $\mathrm{tr}(\psi) = \mathrm{tr}(1^t\psi) \equiv r \equiv 0 \pmod 2$. Now the elements of order 2 in $\mathrm{GL}_2(2)$ are conjugate to $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and hence have trace 0, whereas the two elements of order 3 have trace 1. Now $\psi \neq 1$ because otherwise $m_\psi = 1$, so we must have that ψ has order 2. This proves the one direction of the assertion, and the converse follows by reversing the steps. □

We now show that the classical Legendre curve family which was studied by Legendre in 1832 (cf. Krazer[7], p. 477) gives many examples of curves which satisfy the hypotheses of Proposition 45 and/or of Theorem 4(c).

Example 46 Let K be a field with $\mathrm{char}(K) \neq 2$ and let $a \in K^\times$, $a \neq \pm 1$. Then the plane curve

$$C_a : \qquad y^2 \;=\; x(x^2 - a)(x^2 - a^{-1})$$

is a curve of genus 2 which is a twist of the classical Legendre curve

$$L_\kappa : \qquad y^2 \;=\; x(1 - x^2)(1 - \kappa^2 x^2)$$

because if $a = b^2$, then the transformation $x = bX$, $y = Y$ transforms C_a to the curve $Y^2 = b(1 - X^2)(1 - a^2X^2)$, which is a quadratic twist of L_a.

It is immediate that the rule $\sigma : (x, y) \mapsto (\frac{1}{x}, \frac{y}{x^3})$ defines an involution of C_a/K. Since $\sigma \neq \sigma_C : (x, y) \mapsto (x, -y)$, it follows that σ is an elliptic involution.

Let $F = K(x,y)$ denote the function field of C_a. Then the fixed field of F with respect to σ is $K(u,v)$, where $u = x + \frac{1}{x}$ and $v = y(x+1)/x^2$. These are related by the cubic equation

$$E_a : \qquad v^2 = (u+2)\left(u^2 - \tfrac{(a+1)^2}{a}\right),$$

which defines an elliptic curve. Thus, the rule $(x,y) \mapsto (u,v)$ defines an elliptic subcover $f : C_a \to E_a$ of degree 2.

Now suppose that $-1 = i^2$ is a square in K. Then the rule $\rho : (x,y) \mapsto (-x, iy)$ defines an automorphism of order 4 on C_a, and we have $\sigma\rho\sigma = \rho^3$ and $\rho^2 = \sigma_C$. Thus, $G = \langle \sigma, \rho \rangle \simeq D_4$ is a dihedral subgroup of $\mathrm{Aut}(C_a)$, and so C_a/K satisfies the hypotheses of Theorem 4(a).

To find examples satisfying the hypotheses of Theorem 4(c), we need to impose further restrictions on a. For this, note that (by MAPLE) the j-invariant of E_a is

$$j(E_a) = \frac{64(a+3)^3(3a+1)^3}{(a+1)^2(a-1)^4}. \tag{57}$$

It is immediate that $j(E_a) \notin \mathbb{Z}$, if $a \in \mathbb{Z}$ ($a \neq 0, \pm 1$), except for $a = \pm 3$. Indeed, if p is an odd prime which divides the denominator $(a+1)^2(a-1)^4$ of $j(E_a)$, then $a \equiv \pm 1 \,(\mathrm{mod}\, p)$ and then the numerator is not divisible by p because it is congruent to a power of 2 mod p. Thus, if $j(E_a)$ is integral, then $(a-1)(a+1)$ is (up to sign) a power if 2, and this can happen only for $a = \pm 3$. Thus, if $a \neq \pm 3$, then $\mathrm{End}(E_a \otimes K) = \mathbb{Z}$, for every extension field K of $\mathbb{Q}(i)$, and so these examples satisfy the hypotheses of Theorem 4(c).

Remark 47 Let C'_a/K denote the curve defined by $y^2 = (x^3 - a)(x^3 - a^{-1})$, where $a \in K^\times$, $a \neq \pm 1$. If $\mathrm{char}(K) \neq 2, 3$, then C'_a/K is curve of genus 2 which has an elliptic involution defined by $(x,y) \mapsto (\frac{1}{x}, \frac{y}{x^3})$. Moreover, if K contains a primitive third root of unity ζ_3, then $\mathrm{Aut}(C'_a)$ contains a subgroup isomorphic to D_6, as is easy to see. Thus, a similar discussion as in Example 46 gives us examples for the D_6 case of Theorem 4.

Finally, we consider the following example of a curve C/K for which the refined Humbert invariant is a ternary form.

Proposition 48 *Let $C/\mathbb{Q}$ be the curve defined by $y^2 = x(x^2-3)(x^2-\frac{1}{3})$, and let K be any subfield of $\mathbb{C}$. Then:*

$$q_{C_K} \sim \begin{cases} 4X^2 & \text{if } \mathbb{Q}(i) \not\subset K, \\ 4X^2 + 4Y^2 & \text{if } \mathbb{Q}(i) \subset K \text{ and } \mathbb{Q}(\sqrt{-3}) \not\subset K, \\ 4X^2 + 4Y^2 + 4YZ + 4Z^2 & \text{if } \mathbb{Q}(i, \sqrt{-3}) \subset K. \end{cases} \tag{58}$$

Thus, if $K \not\supset \mathbb{Q}(i)$, then C_K/K has precisely 2 elliptic subcovers, both of degree 2, and if $\mathbb{Q}(i) \subset K$ but $\mathbb{Q}(\sqrt{-3}) \not\subset K$, then C_K/K has an elliptic subcover of degree

N if and only if $N = 2N_1$, where $N_1 = 1$ or N_1 is a product of primes p_i with $p_i \equiv 1 \pmod 4$. On the other hand, if $\mathbb{Q}(i, \sqrt{-3}) \subset K$, then C_K/K has in addition an elliptic subcover of degree N whenever $N = 2N_2$, where N_2 is a product of primes p_i with $p_i \equiv 1 \pmod 3$.

Proof. By Example 46 we know that $C/\mathbb{Q}$ has an elliptic involution $\sigma \in I(C)$, so by Proposition 36 we know that $C/\mathbb{Q}$ has a 2-presentation $(E_\sigma, E_{\sigma'}, \psi, \pi)$. Thus, $J_C \sim E_\sigma \times E_{\sigma'}$, so by Lemma 21 we see that q_{C_K} is a quadratic form in $1 + r_K$ variables, where $r_K = \operatorname{rank}(\operatorname{Hom}(E_\sigma \otimes K, E_{\sigma'} \otimes K))$. Moreover, since $\operatorname{Aut}(C \otimes \mathbb{Q}(i))$ contains a subgroup isomorphic to D_4, we see that $E_\sigma \otimes \mathbb{Q}(i) \simeq E_{\sigma'} \otimes \mathbb{Q}(i)$; cf. Proposition 45. Since $j(E_\sigma) = 0$ by (57), we see that $r_K = 1$ in the second case of formula (58) and $r_K = 2$ in the third case. Moreover, $r_K = 0$ in the first case. (This can be verified either by verifying by a direct computation that $E_{\sigma'}$ is a nontrivial quadratic twist of E_σ or by observing that the D_4-subgroup cannot be K-rational except when $\mathbb{Q}(i) \subset K$ and using Proposition 45.)

In the first case we have $q_{C_K} \sim nX^2$, for some $n \geq 1$. Since C_K has an elliptic subcover of degree 2, we know that 4 is primitively represented by q_{C_K} (cf. [6], Theorem 20), and so $n = 4$ because n the only value which is primitively represented by nX^2. This proves (58) in the first case. Moreover, in the second case we are in the situation of Theorem 4(c), so (58) holds in this case as well.

Now suppose that $\mathbb{Q}(i, \sqrt{-3}) \subset K$, so q_{C_K} is a ternary form. We first prove that $m_{\psi_K} = 2$. If not, then $m_{\psi_K} = 1$ because $m_{\psi_K} | 2$, and then by Diem-Frey (cf. [6], Theorem 4) $J_{C_K} \simeq (E_\sigma \times E_{\sigma'})_K \simeq E^2$, where $j(E) = 0$. But this is impossible because this product surface cannot be a Jacobian by Hayashida-Nishi[2]; cf. [3], Remark 60. Thus, $m_\psi = 2$.

By Theorem 4(a) and Corollary 41 we know that $\mathrm{NS}(J_C, \lambda_C)$ has a primitive submodule $\bar{M}$ such that the restriction of q_{C_K} to $\bar{M}$ primitively represents $[4, 0, 4] = q_{2,2,1,0,0}$. Thus, by Theorem 31 we see that $\pi^* \mathrm{NS}'(J_{C_K})$ contains $M := \mathbb{Z}(2\theta) + \mathbb{Z}(4D_1) + \mathbb{Z}(2D_2)$ as a primitive submodule, where $D_1 = \mathbf{D}'(1, 0, 0)$ and $D_2 = \mathbf{D}'(0, 0, 1_E)$. Thus, there exists $D_3' \in \mathrm{NS}(E^2)$ such that $(2\theta, 4D_1, 2D_2, D_3')$ is a basis of $\pi^* \mathrm{NS}'(J_{C_K})$. Since $m_\psi = 2$, we have by [6], Corollary 38, that $D_3' = 2D_3$, for some $D_3 = \mathbf{D}'(a, b, h)$. By replacing D_3' by $D_2' - b(2\theta)$, we may assume without loss of generality that $b = 0$. Moreover, since $\mathrm{End}(E) \simeq \mathbb{Z}[\zeta_3]$, there exists $\alpha \in \mathrm{End}(E)$ of order 3 such that $(1_E, \alpha)$ is a basis of $\mathrm{End}(E)$. Thus, we can write $h = c_1 \cdot 1_E + c_2\alpha$, and so, by replacing D_3' by $D_3' - c_1(2D_2)$, we may assume that $D_3' = 2D_3$, where $D_3 = \mathbf{D}'(a, 0, c\alpha)$. It then follows from Proposition 24 that $a \equiv c\mathrm{tr}(\alpha^t\psi) \pmod 2$. Now since the restriction of α to $E[2]$ has order 3, and ψ has order 2, it follows that $\alpha^t\psi$ has order 2 and so $\mathrm{tr}(\alpha^t\psi) = 0$; cf. the proof of Proposition 45. Thus, $a \equiv 0 \pmod 2$, and so by replacing D_3' by $D_3' - 4\frac{a}{2}D_1$ we may assume that $D_3' = 2cD_3$, where $D_3 = \mathbf{D}'(0, 0, \alpha)$. Since θ, D_1, D_2, D_3 is a basis of $\mathrm{NS}'(E^2)$, we see that $[\mathrm{NS}'(E^2) : \pi^* \mathrm{NS}'(J_{C_K})] = |2 \cdot 4 \cdot 2 \cdot 2c| = 32|c|$. But by Theorem 22 we know that

this index equals $m_\psi 2^{2+2} = 2^5$, so $c = \pm 1$, so we may take $c = 1$. Thus,

$$\pi^*\mathrm{NS}'(J_C) \;=\; \mathbb{Z}(2\theta) + \mathbb{Z}(4D_1) + \mathbb{Z}(2D_2) + \mathbb{Z}(2D_3) \tag{59}$$

where $D_3 = \mathbf{D}'(0,0,\alpha)$, and so $\mathrm{NS}'(J_C)$ has a basis $(\theta_C, \tilde{D}_1, \tilde{D}_2, \tilde{D}_3)$ where $\pi^*\tilde{D}_1 = 4D_1$, $\pi^*\tilde{D}_2 = 2D_2$, and $\pi^*\tilde{D}_3 = 2D_3$.

Using the projection formula (cf. [6], Proposition 17) and (16), we thus obtain

$$\begin{aligned} q_C(X\tilde{D}_1 + Y\tilde{D}_2 + Z\tilde{D}_3) &= \tfrac{1}{4} q_{(E^2,\theta)}(X(4D_1) + Y(2D_2) + Z(2D_3)) \\ &= \tfrac{1}{4}(16X^2 + 4\deg(2(Y\cdot 1_E + Z\cdot\alpha))), \end{aligned}$$

where $X, Y, Z \in \mathbb{Z}$. Since $\deg(Y\cdot 1_E + Z\cdot\alpha) = Y^2 + YZ + Z^2$, we thus see that $q_C \sim X^2 + Y^2 + XY + Z^2$, which proves the third case of (58).

The last assertion follows immediately from Theorem 4(a),(b) because the form $4Y^2 + 4YZ + 4Z^2$ is primitively represented by q_C. □

References

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

[2] 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.

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

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

[5] E. Kani, Elliptic subcovers of hyperelliptic curves. *Math. Nachr.* **290** (1917), 2890–2900.

[6] E. Kani, Elliptic subcovers of a curve of genus 2. I. The isogeny defect. To appear in *Ann. Math. Québec.*

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

[8] E. Landau, *Vorlesungen über Zahlentheorie.* Chelsea Reprint, New York, 1950.

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

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

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