Generalized Humbert Schemes and Intersections of Humbert Surfaces

Ernst Kani

1 Introduction

In 1899 Humbert[Hu] attached to a principally polarized abelian surface (A, λ) which satisfies a certain "singular relation" an invariant Δ which is now called a *Humbert invariant* of (A, λ). This invariant gives rise to Humbert surfaces as follows.

Let A_2 denote the moduli space of principally polarized abelian surfaces (A, λ). For a positive integer $n > 0$, let $H_n \subset A_2$ denote the subset consisting of those surfaces $(A, \lambda) \in A_2$ which have a singular relation with Humbert invariant $\Delta = n$. It then follows from Humbert's work that H_n is a closed analytic surface in A_2, provided that $n \equiv 0, 1 \pmod 4$. The surfaces H_n are now called *Humbert surfaces*; cf. van der Geer[vdG], Ch. IX.

Here we want to study the components of the intersection $H_n \cap H_m$ of two Humbert surfaces. This problem was briefly addressed on p. 214 of [vdG], but the results obtained there (via analytic techniques) are somewhat incomplete; cf. Remark 11 below.

Here give a different approach to this problem by using the *refined Humbert invariant* which was introduced in [K1]. This approach is completely algebraic and hence has the advantage that it also works over an arbitrary algebraically closed field K instead of $\mathbb{C}$.

Using this invariant, we introduce in Section 2 (closed) subsets $H(q) \subset A_2(K)$ which are indexed by positive integral quadratic forms q in $r \geq 1$ variables. If $r = 1$, then these are precisely the Humbert surfaces, and so we will refer to the $H(q)$'s as *generalized Humbert schemes.*

From the definition of the $H(q)$'s it follows easily that if $m \neq n$, then

$$H_m \cap H_n = \bigcup_q H(q), \tag{1}$$

where the union runs over all equivalence classes of positive definite binary quadratic forms q which primitively represent both m and n; cf. Proposition 12.

However, if we want to make use of this formula in order to determine the irreducible components of the intersection $H_m \cap H_n$, then further work is necessary, for we need to know when $H(q)$ is non-empty and what are its irreducible components.

Here we will solve this problem only in the special case that $H(q) \subset H_{N^2}$, for some $N \geq 1$. In this case we can use the results from [K5] to prove in §2:

Theorem 1 *Let q be a positive integral binary quadratic form which primitively represents N^2, for some $N \geq 1$ with $\mathrm{char}(K) \nmid N$. Then $H(q) \neq \emptyset$ if and only if*

$(*)$ *every integer represented by q is congruent to 0 or 1 mod 4.*

By combining this theorem with formula (1), it is not difficult to show:

Corollary 2 *If $\mathrm{char}(K) \nmid N$, then $H_{N^2} \cap H_M$ is non-empty, for any $M \equiv 0, 1 \pmod 4$.*

Let $M_2(K) \subset A_2(K)$ denote the open subset consisting of the Jacobians of smooth genus 2 curves. Then $H_{N^2} \cap M_2$ classifies the genus 2 curves which have an elliptic subcover of degree N; cf. [Hu], [K1]. In their paper, Accola and Previato[AP] raised the question of whether Lange's moduli space[La] $M_2(n,1) = \cup_{N|n} H_{N^2} \cap M_2$ is connected. This follows from the following result which partially refines Corollary 2.

Corollary 3 *If $\mathrm{char}(K) \nmid N \geq 2$, then $H_{N^2} \cap H_m \cap M_2$ is non-empty, for any $m \equiv 0, 1 \pmod 4$, $m \geq 4$.*

Theorem 1 answers the question of when $H(q)$ is non-empty. To go further and to determine the irreducible components of $H(q)$ is a much more difficult task. To state the result, it is useful to introduce the following terminology.

Definition. Let $Q(N^2)$ denote the set of binary quadratic forms satisfying the conditions of Theorem 1. Thus, $q \in Q(N^2)$ if and only if q is a positive integral binary quadratic form which satisfies condition $(*)$ and which primitively represents N^2.

Moreover, if N, m, d are positive integers, then we say that q *is of type* (N, m, d) if $q \in Q(N^2)$, if $m|N$ and if

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

The following result gives a partial overview of the number of irreducible components of $H(q)$.

Theorem 4 *If $q \in Q(N^2)$, then q is of type (N, m, d), for unique integers $m|N$ and $d \geq 1$. Put $c_m(q) = \gcd(\mathrm{cont}(q), m)$, where $\mathrm{cont}(q)$ denotes the content of q, i.e., $\mathrm{cont}(q) = \gcd(a, b, c)$, where a, b, c are the coefficients of q. Moreover, assume that $\mathrm{char}(K) \nmid Nd$.*

(a) *$H(q)$ has at most $2^{\omega(c_m(q))}$ irreducible components, provided that $8 \nmid c_m(q)$. Here $\omega(n) = |\{p|n\}|$ denotes the number of distinct prime factors of n.*

(b) *If $d > N^4/(4m^2)$ and if N is odd, then $H(q)$ has precisely $2^{\omega(c_m(q))}$ irreducible components, except when q is equivalent to the binary quadratic form $N^2X^2 + 4dY^2$.*

The above theorem is a special case of more general results which also deal with the case that $8|c_m(q)$ and analyze the exceptional cases; cf. Theorems 49 and 55.

Note that Theorem 4(a) implies the following *irreducibility criterion*, which generalizes that of the case $m = 1$ studied in [K3].

Corollary 5 *If q has type (N, m, d) and if $c_m(q) = 1$, then $H(q)$ is irreducible, provided that* $\mathrm{char}(K) \nmid Nd$.

It is useful to observe that the above corollary and (1) imply the following result.

Corollary 6 *If* $\mathrm{char}(K) = 0$ *and if* $\gcd(N, M) = 1$, *then $H(q)$ is irreducible whenever $q \in Q(N^2)$ and $H(q) \subset H_{N^2} \cap H_M$. Thus every irreducible component of $H_{N^2} \cap H_M$ is of the form $H(q)$, for a suitable $q \in Q(N^2)$.*

Theorem 4 is a actually a consequence of several much finer results. The first of these identifies the irreducible components of $H(q)$. For this, we will generalize the method of [K3] and show that the components of $H(q)$ are the images $\overline{T}_\alpha^N \subset A_2$ of certain modular curves X_α^N. These are defined by primitive integral matrices $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$ and give rise to the modular correspondences T_α^N on $X(N) \times X(N)$; cf. Section 4. To state the result, it is useful to introduce the following notation.

Notation. Let $\mathcal{M}_d$ denote the set of primitive 2×2 matrices of determinant d. If $\alpha \in \mathcal{M}_d$ and if $N \geq 1$, then we define the binary quadratic form q_α^N by

$$q_\alpha^N(X, Y) \;=\; N^2X^2 + 2mtXY + \tfrac{m^2}{N^2}(t^2 + 4d)Y^2.$$

Here $t = \mathrm{trace}(\beta\alpha)$, where $\beta = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, and $\frac{N}{m} = \gcd(x - w, y, z, N)$, if $\beta\alpha = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$.

Theorem 7 *If q is a binary form of type (N, m, d), and if* $\mathrm{char}(K) \nmid Nd$, *then*

$$H(q) \;=\; \bigcup_\alpha \overline{T}_\alpha^N, \tag{3}$$

where the union is over all $\alpha \in \mathcal{M}_d$ such that q_α^N is equivalent to q. Thus $H(q)$ is an equidimensional curve which is a closed subscheme of A_2.

Note that if $m > 1$, then it can happen that $\gcd(N, d) > 1$, so in this case the above union (3) consists of the images $\overline{T}_\alpha^N$ of the "bad" modular correspondences T_α^N whose determinant $d = \det(\alpha)$ is not prime to the level N.

Theorem 7 has the following consequence.

Corollary 8 *Let $M \equiv 0, 1 \pmod 4$ be a positive integer. If* $\mathrm{char}(K) = 0$ *or if* $\mathrm{char}(K) > \frac{N^2M}{4}$, *then $H_{N^2} \cap H_M$ is an equidimensional curve, provided that $N^2 \neq M$.*

While Theorem 7 identifies the irreducible components of $H(q)$, further work is necessary in order to determine which of the components are actually *distinct*. For this, we show:

Theorem 9 *Let N, d be positive integers with $\mathrm{char}(K) \nmid Nd$. If $\alpha_1, \alpha_2 \in \mathcal{M}_d$, then*

$$g\beta\alpha_1 g^{-1} \equiv \pm\beta\alpha_2 \,(\mathrm{mod}\ N),\ \textit{for some}\ g \in \mathrm{SL}_2(\mathbb{Z}) \ \Rightarrow\ \overline{T}^N_{\alpha_1} = \overline{T}^N_{\alpha_2}. \tag{4}$$

Furthermore, the converse implication holds if $d > N^4/(4m^2)$, where m is determined by the (common) type (N, m, d) of $q^N_{\alpha_i}$, for $i = 1, 2$.

From this result, it is clear that the $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$-conjugacy classes of 2×2-matrices $\alpha \in M_2(\mathbb{Z}/N\mathbb{Z})$ play an important role in the determination of the irreducible components of $H(q)$. By extending the work of Nobs[No], it is possible to give a classification of these conjugacy classes; cf. §6.

It is much more difficult to analyze the precise number of components of $H(q)$ when $d \le N^4/(4m^2)$. Here we only do this in the cases that $N = 2$ and 4 (cf. Proposition 51 and Corollary 56), because already in the case of an odd prime N, the analysis is long and difficult and hence has been delegated to [K7]. There the following result is obtained. For this, recall from Gauss that a binary form q is called *ambiguous* if q is equivalent to $aX^2 + kaXY + cY^2$, for some $a, k, c \in \mathbb{Z}$.

Theorem 10 *Let $q \in Q(N^2)$, where N is a prime. If $N = 2$, then $H(q)$ is irreducible, and when $N > 2$, then $H(q)$ has at most 2 irreducible components. Furthermore, if $N \equiv 1 \,(\mathrm{mod}\ 4)$, then*

$$H(q)\ \textit{is irreducible} \quad\Leftrightarrow\quad q\ \textit{is primitive, i.e.,}\ \mathrm{cont}(q) = 1, \tag{5}$$

whereas if $N \equiv 3 \,(\mathrm{mod}\ 4)$, then

$$H(q)\ \textit{is irreducible} \quad\Leftrightarrow\quad q\ \textit{is primitive or ambiguous.} \tag{6}$$

By using these results and the reduction theory of binary quadratic forms, it is possible to work out the irreducible components of $H_{N^2} \cap H_M$ explicitly for small values of N and M; cf. §8.

Acknowledgment. This research was supported by a Discovery Grant from the Natural Sciences and Engineering Research Council of Canada (NSERC).

2 The refined Humbert invariant and generalized Humbert schemes

Let A be an abelian surface over an algebraically closed field K of arbitrary characteristic, and assume that A has a principal polarization $\lambda : A \xrightarrow{\sim} \hat{A}$. Thus, $\lambda = \phi_\theta$ for

unique class $\theta = \theta_\lambda$ in the Néron-Severi group $\mathrm{NS}(A) = \mathrm{Div}(A)/\equiv$, where $\equiv$ denotes numerical equivalence.

As in [K1], [K3] and [K5], the *refined Humbert invariant* $\tilde{q}_{(A,\lambda)}$ is defined by the formula

$$\tilde{q}_{(A,\lambda)}(D) = (D.\theta_\lambda)^2 - 2(D.D), \quad \text{for } D \in \mathrm{NS}(A), \tag{7}$$

where $(.)$ denotes the intersection number of divisors on A. From the Hodge index theorem it follows easily that $q_{(A,\lambda)}$ defines a positive definite quadratic form $q_{(A,\lambda)}$ on the quotient group $\mathrm{NS}(A,\lambda) = \mathrm{NS}(A)/\mathbb{Z}\theta_\lambda$; cf. [K1], §3. It is clear that the isomorphism class of the quadratic module $(\mathrm{NS}(A,\lambda), q_{(A,\lambda)})$ depends only the isomorphism class $\langle A,\lambda\rangle$ of the principally polarized abelian surface (A,λ).

As was explained in [K1], §5, $q_{(A,\lambda)}$ is closely related to the classical *Humbert invariant* attached to an abelian surface $A/\mathbb{C}$. More precisely, any primitive element $D \in \mathrm{NS}(A,\lambda)$ gives rise to a "singular relation" in the sense of Humbert[Hu] (and conversely), and $\Delta = q_{(A,\lambda)}(D)$ is the Humbert invariant attached to this "singular relation" of the principally polarized abelian surface (A,λ) as defined by Humbert[Hu]. It thus follows from this that the subset

$$H_\Delta \;=\; \{\langle A,\lambda\rangle \in A_2(K) : q_{(A,\lambda)} \text{ primitively represents } \Delta\} \tag{8}$$

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

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

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

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

Note that if q is a 1-variable quadratic form $q_\Delta(x) = \Delta x^2$, then (8) shows that $H(q_\Delta) = H_\Delta$ is the classical Humbert surface of discriminant Δ. Thus, the $H(q)$'s generalize Humbert surfaces and hence it is fitting to call them *generalized Humbert sets*. Below we will show (in certain cases) that they are closed subsets of A_2, so they inherit a scheme structure from A_2 and hence can be called *Humbert schemes.*

Remark 11 When $K = \mathbb{C}$ and q is a binary quadratic form, then $H(q)$ is closely related to the (analytic) curves C_U defined on p. 214 of [vdG]. These curves are defined by positive definite 2-dimensional quadratic subspaces (U,ϕ) of a certain 5-dimensional quadratic subspace $(V_\mathbb{Q},\Delta)$ of signature $(3,2)$. Unfortunately, van der Geer does not explain which (U,ϕ) can arise in this way, but only gives some necessary conditions. Moreover, he does not discuss the irreducible components of C_U.

As was mentioned in the introduction, the $H(q)$'s can be used to describe intersections of Humbert surfaces:

Proposition 12 *If m and n are distinct positive integers, then*

$$H_m \cap H_n = \bigcup_q H(q), \tag{9}$$

where the union runs over all equivalence classes of positive definite binary quadratic forms q which primitively represent both m and n.

Proof. Let q be such a form, and let $\langle A, \lambda\rangle \in H(q)$. Then $q_{(A,\lambda)}$ primitively represents q. Since m is primitively represented q, it follows that m also primitively represented by $q_{(A,\lambda)}$, so $\langle A, \lambda\rangle \in H_m$ by (8). Thus $H(q) \subset H_m$, and similarly, $H(q) \subset H_n$, so $H(q) \subset H_n \cap H_m$. This shows that the right side of (9) is contained in the left side.

Conversely, suppose that $\langle A, \lambda\rangle \in H_m \cap H_n$. Then there exist primitive vectors $v, w \in M := \mathrm{NS}(A, \lambda)$ such that $q_{(A,\lambda)}(v) = m$ and $q_{(A,\lambda)}(w) = n$. If v and w were linearly dependent, then $v = \pm w$ and hence $q_{(A,\lambda)}(v) = q_{(A,\lambda)}(w)$, contrary to the hypothesis. Thus, v and w are linearly independent and hence $M_0 := \mathbb{Z}v + \mathbb{Z}w$ has rank 2. Let M_1 be the saturation of M_0 in M. Then the restriction q of $q_{(A,\lambda)}$ to M_1 is a positive definite, binary quadratic form which is primitively represented by $q_{(A,\lambda)}$, and so $\langle A, \lambda\rangle \in H(q)$. Moreover, $m = q(v)$ is primitively represented by q (because v is primitive in M, hence also in M_1. Similarly, $n = q(w)$ is primitively represented by q. Thus q is one of the forms of the right side of (9), so $\langle A, \lambda\rangle \in \cup H(q)$.

Remark 13 (a) Note that there are only finitely many equivalence classes of forms q satisfying the conditions of Proposition 12 because their discriminants are bounded. Indeed, it follows from the above proof that we have $|\mathrm{disc}(q)| \leq 4mn$ for any such q because $|\mathrm{disc}(q)| \leq |\mathrm{disc}(q_{|M_0|})| \leq 4mn$.

(b) The above proposition can be viewed as giving a partial answer to a question raised by McMullen[Mc], p. 96.

Proof of Theorem 1. Suppose first that $H(q) \neq \emptyset$, so there exists $\langle A, \lambda\rangle \in A_2(K)$ such that $q_{(A,\lambda)}$ primitively represents q. Now $q_{(A,\lambda)}$ satisfies condition $(*)$ because $(D.D) = 2\chi(\mathcal{L}(D)) \in 2\mathbb{Z}$ by the Riemann-Roch Theorem and so (7) shows that $q_{(A,\lambda)}(D) \equiv (D.\theta_\lambda)^2 \pmod 4$, for all $D \in \mathrm{Div}(A)$. Thus, q also satisfies condition $(*)$.

Conversely, suppose that q satisfies condition $(*)$ and primitively represents N^2. Then by Proposition 7 of [K5] we know that q has type (N, m, d) for a unique pair $m, d \geq 1$ with $m|N$ and $\gcd(N/m, d) = 1$. Since $\mathrm{char}(K) \nmid N$, we have by Corollary 33 of [K5] that there exists a principally polarized abelian surface (A, λ) such that $q_{(A,\lambda)}$ primitively represents q. Thus $\langle A, \lambda\rangle \in H(q)$, so $H(q) \neq \emptyset$.

Proof of Corollary 2. We may assume that $M \neq N^2$ and that $M > 1$. (If $M = 1$, then interchange M and N^2.) Put $\varepsilon = \mathrm{rem}(M, 4) \in \{0, 1\}$ and consider the binary quadratic form $q(X, Y) := N^2X^2 + 2\varepsilon NXY + MY^2$ which is positive definite because $\mathrm{disc}(q) = -4N^2(M - \varepsilon^2) < 0$. Since $q(1, 0) = N^2$ and $q(0, 1) = M$, we see that q primitively represents N^2 and M, so $H(q) \subset H_{N^2} \cap H_M$ by Proposition 12. Moreover, since $q(X, Y) \equiv (NX + \varepsilon Y)^2 \,(\mathrm{mod}\ 4)$, for all $X, Y \in \mathbb{Z}$, we see that property $(*)$ holds. Thus $H(q) \neq \emptyset$ by Theorem 1, and so $H_{N^2} \cap H_M \neq \emptyset$, as claimed.

Proof of Corollary 3. Let q be as in the proof of Corollary 2, so q is a positive form which primitively represents N^2 and M and satisfies (*). Thus, by Proposition 7 of [K5] there exists $m|N$ and $d \geq 1$ such that q has type (N, m, d). Moreover, since $q(x, y) = (Nx + \varepsilon y)^2 + (M - \varepsilon^2)y^2 \geq \min(N^2, M - \varepsilon^2) \geq 3$, if $(x, y) \neq (0, 0)$, we see that $q(x, y) \neq 1$, for all $x, y \in \mathbb{Z}$.

Suppose first that K is not the algebraic closure of a finite field. Then we are in the situation of Corollary 34 of [K5], so there is a curve C/K such that $q_C \sim q$, which means that $\langle J_C, \theta_C \rangle \in H(q) \cap M_2 \subset H_{N^2} \cap H_M \cap M_2$. This proves the assertion in this case.

Now suppose that $K = \overline{\mathbb{F}}_p$ is the algebraic closure of a finite field. Choose an algebraically closed overfield $K' \supset K$ which is transcendental over K. Since $H'(q) := H(q) \cap M_2$ is a closed algebraic subset of M_2 (cf. Theorem 7), and since $H'(q)(K') \neq \emptyset$ by what was proved before, it follows that also $H'(q)(K) \neq \emptyset$, and so the assertion also holds in this case.

Remark 14 It follows from Corollary 3 that in particular $H_{N^2} \cap H_{M^2} \cap M_2 \neq \emptyset$ whenever $N, M \geq 2$. This fact also follows from a result of [FPR]. Since H_{N^2} is irreducible by Humbert[Hu] and/or by Theorem 15 below, it thus follows that the moduli space

$$M_2(n, 1) \;=\; \bigcup_{N|n, N>1} H_{N^2} \,\cap\, M_2$$

consisting of all genus 2 curves admitting a surjective morphism of degree n to a curve of genus 1 is *connected* (provided that $\mathrm{char}(K) \nmid n$). This answers a question raised (implicitly) by Accola and Previato[AP], §1.7. Note that the moduli space $M_2(n, 1)$ was studied by Lange[La].

3 The morphism β_N

As a first step towards proving the main results of this paper, we recall from [K1], §3, and/or [FK], §4.4, that the Humbert surface H_{N^2} can be covered by the product surface $X(N) \times X(N)$, where $X(N)/K$ is the (affine) modular curve of level N. In other words, there exists a finite morphism

$$\beta_N : X(N) \times X(N) \;\to\; A_2$$

whose image is the Humbert surface H_{N^2}. This morphism is, in fact, a variant of the "basic construction" of [FK], §2.3.

For our purposes, however, we need not only the existence (and finiteness) of this morphism, but also its *modular description*, which is a modification of that of [FK].

For this, fix an integer $N \geq 1$ with $\mathrm{char}(K) \nmid N$, where (as before) K is an algebraically closed field. Moreover, fix a primitive N-th root of unity $\zeta_N \in K^\times$. Recall from [DR], [KM] and/or the discussion and references of [K6], §4, that the (affine) modular curve $X(N)/K$ (coarsely) represents the functor

$$\mathcal{X}(N) = \mathcal{X}(N)_{\zeta_N} : (\mathrm{Sch}/K) \ \to \ (\mathrm{Sets})$$

which is defined by $\mathcal{X}(N)(S) = \{\langle E/S, \phi\rangle\}$, where S is a K-scheme, E/S is an elliptic curve, $\phi : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E[N]$ is a level N-structure of fixed determinant $\zeta_N \in K^\times$, and $\langle E/S, \phi\rangle$ denotes the isomorphism class of the pair $(E/S, \phi)$.

Moreover, recall from [M1], Theorem 7.10, that the moduli space A_2/K coarsely represents the functor $\mathcal{A}_2 = \mathcal{A}_{2,1,1} : (\mathrm{Sch}/K) \to (\mathrm{Sets})$ which classifies principally polarized abelian surfaces, i.e., if S is a K-scheme, then $\mathcal{A}_2(S)$ is the set of isomorphism classes $\langle A, \lambda\rangle$ of pairs (A, λ) where A/S is an abelian scheme of relative dimension 2 and $\lambda : A \xrightarrow{\sim} \hat{A}$ is a principal polarization.

Modifying the construction of [FK] slightly, we will define the morphism (of functors)

$$\tilde{\beta}_N : \mathcal{X}(N) \times \mathcal{X}(N) \ \to \ \mathcal{A}_2$$

as follows. Let $\langle E_i/S, \phi_i\rangle \in \mathcal{X}(N)(S)$, where $i = 1, 2$, and put

$$\psi = \psi_{\phi_1,\phi_2} := \phi_2 \circ \left[\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)\right]_N \circ \phi_1^{-1} : E_1[N] \to E_2[N], \tag{10}$$

where, for an integral 2×2 matrix α, the symbol $[\alpha]_N$ denotes the endomorphism $[\alpha]_N \in \mathrm{End}((\mathbb{Z}/N\mathbb{Z})^2)$ whose matrix is $\alpha \pmod N$ with respect to the canonical basis $((1,0),(0,1))$ of $(\mathbb{Z}/N\mathbb{Z})^2$.

Let $\pi_\psi : E_1 \times E_2 \ \to \ A_\psi := (E_1 \times E_2)/G_\psi$ be the quotient map, where $G_\psi = \mathrm{Graph}(-\psi) \leq E_1[N] \times E_2[N] = (E_1 \times E_2)[N]$. Since $\psi : E_1[N] \to E_2[N]$ is an anti-isometry, there is a unique principal polarization $\lambda_\psi : A_\psi \to \hat{A}_\psi$ such that

$$\hat{\pi}_\psi \circ \lambda_\psi \circ \pi_\psi \ = \ N(\lambda_{E_1} \otimes \lambda_{E_2}), \tag{11}$$

where $\lambda_{E_1} \otimes \lambda_{E_2}$ is the product polarization on $E_1 \times E_2$; cf. [K2], Prop. 5.7. Thus $\langle A_\psi, \lambda_\psi\rangle \in \mathcal{A}_2(S)$, and so the rule $\langle E_1/S, \phi_1; E_2/S, \phi_2\rangle \mapsto \langle A_\psi, \lambda_\psi\rangle$ defines a map

$$\tilde{\beta}_{N,S} : (\mathcal{X}(N) \times \mathcal{X}(N))(S) \ \to \ \mathcal{A}_2(S).$$

Since the maps $\tilde{\beta}_{N,S}$ are compatible with base-change, they define a morphism of functors $\tilde{\beta}_N = \{\tilde{\beta}_{N,S}\}_S$. By the universal property of the (coarse) moduli scheme $X(N) \times X(N)$, we thus have an induced K-morphism

$$\beta_N : X(N) \times X(N) \ \to \ A_2.$$

Theorem 15 *The above morphism $\beta_N : X(N) \times X(N) \to A_2$ is* finite *and its image is the Humbert surface H_{N^2}. In particular, H_{N^2} is an affine closed irreducible subscheme of A_2 of dimension* 2.

Proof. Although this follows from Corollary 3.10 of [K1], no proof is given there, so it is useful to present one here. (See also [FK], Proposition 4.11).

We first show that $\mathrm{Im}(\beta_N) = H_{N^2}$. Indeed, if $x = (x_1, x_2) \in (X(N) \times X(N))(K)$, then each x_i corresponds to a tuple $\langle E_i/K, \phi_i\rangle \in \mathcal{X}(N)(K)$. By [K2], Corollary 5.9, the principally polarized surface (A_ψ, λ_ψ) contains an elliptic subgroup of degree N in the sense of [K1], and so by [K1], Corollary 3.9, we see that $\beta_N(x) = \langle A_\psi, \lambda_\psi\rangle \in H_{N^2}$. Thus $\mathrm{Im}(\beta_N) \subset H_{N^2}$. Conversely, if $y = \langle A, \lambda\rangle \in H_{N^2}$, then by [K1], Corollary 3.9 and Theorem 3.1, (A, λ) has an elliptic subgroup E of degree N, and so by [K2], Propositions 5.2 and 5.5, there is another elliptic curve E' and an anti-isometry $\psi : E[N] \to E'[N]$ such that $(A_\psi, \lambda_\psi) \simeq (A, \lambda)$. Since K is algebraically closed and $\mathrm{char}(K) \nmid N$, there exists a level N-structure ϕ such that $\langle E/K, \phi\rangle \in \mathcal{X}(N)(K)$. Since ψ is an anti-isometry, there is a unique level N-structure ϕ' such that $\langle E'/K, \phi'\rangle \in \mathcal{X}(N)(K)$ and $\psi_{\phi,\phi'} = \psi$. We then have that $\tilde{\beta}_{N,K}(\langle E/K, \phi; E'/K, \phi'\rangle) = \langle A, \lambda\rangle$, and so $\langle A, \lambda\rangle \in \mathrm{Im}(\beta_N)$. This proves that $\mathrm{Im}(\beta_N) = H_{N^2}$.

We next observe that β_N is quasi-finite. For this, let $x' \in \beta_N^{-1}(\beta_N(x))$, where $x = (x_1, x_2)$ is as above. Write $x' = (x_1', x_2')$, where $x_i' = \langle E_i'/K, \phi_i'\rangle \in \mathcal{X}(N)(K)$ and put $\psi' = \psi_{\phi_1',\phi_2'}$. To show that $\beta_N^{-1}(\beta_N(x'))$ is finite, it suffices to show that the E_i''s lie in finitely many K-isomorphism classes.

By hypothesis, $\langle A_\psi, \lambda_\psi\rangle = \langle A_{\psi'}, \lambda_{\psi'}\rangle$, where $\psi' = \psi_{\phi_1',\phi_2'}$, so there is an isomorphism $\alpha : A_\psi \xrightarrow{\sim} A_{\psi'}$ such that $\lambda_\psi = \hat{\alpha} \circ \lambda_{\psi'} \circ \alpha$. Thus, each elliptic subgroup of $A_{\psi'}$ of degree N is isomorphic to an elliptic subgroup of A_ψ of degree N. In particular, since $E_{\psi',1} := \pi_{\psi'}(E_1' \times \{0\}) \simeq E_1'$ and $E_{\psi',2} := \pi_{\psi'}(\{0\} \times E_2') \simeq E_2'$ are both elliptic subgroups of degree N on $A_{\psi'}$, we see that E_1' and E_2' are each isomorphic to an elliptic subgroup of degree N on A_ψ. Thus the finiteness of $\beta_N^{-1}(\beta_N(x'))$ follows because A_ψ has only finitely many elliptic subgroups $E \leq A_\psi$ of degree N. (Indeed, since $q_{(A,\lambda)}$ is positive-definite, there are only finitely many $\bar{D} \in \mathrm{NS}(A, \lambda)$ such that $q_{(A,\lambda)}(\bar{D}) = N^2$, and so the assertion follows from the bijection constructed in [K1], Theorem 3.1.)

This, therefore, shows that β_N is quasi-finite at closed points. Since the quasi-finite locus is open by [EGA], (IV, 13.1.4), it follows that β_N is quasi-finite because $X(N) \times X(N)$ is a Jacobson scheme.

To prove that β_N is actually finite, it suffices by [EGA], (III, 4.4.2) or (IV, 8.11.1), to verify that β_N is proper because β_N is quasi-finite. Moreover, since $X(N)$ and A_2 are separated K-schemes of finite type, it is enough to check that the functor $\tilde{\beta}_N$ satisfies the valuative criterion of properness. Thus, let $S = \mathrm{Spec}(R)$, where R is a discrete valuation ring with quotient field $F \supset K$ and let $y = \langle A, \lambda\rangle \in \mathcal{A}_2(S)$ be such that there exists $x_F = \langle E_1, \phi_1; E_2, \phi_2\rangle \in (\mathcal{X}(N) \times \mathcal{X}(N))(F)$ with $\tilde{\beta}_{N,F}(x_F) =$

$\langle A_F, \lambda_F \rangle$, where $A_F = A \otimes F$ and $\lambda_F = \lambda \otimes F$. We want to show that x_F extends to $x \in (\mathcal{X}(N) \times \mathcal{X}(N))(S)$ and that $\tilde{\beta}_{N,S}(x) = y$. For this we observe that since $A_F \simeq A_\psi$ is isogenous to $E_1 \times E_2$ and A_F has good reduction over R by hypothesis, it follows that the same is true for E_i (cf. [ST], Cor. 2 on p. 493). Thus, there exist elliptic curves $\tilde{E}_i/R$ with $\tilde{E}_i \otimes F = E_i$. By [KM], Th. 3.7.1, it follows that ϕ_i extends uniquely to an isomorphism $\tilde{\phi}_i : (\mathbb{Z}/N\mathbb{Z})^2 \tilde{\to} \tilde{E}_i[N]$ (of determinant ζ_N) and so $\tilde{x} := \langle \tilde{E}_1, \tilde{\phi}_1; \tilde{E}_2, \tilde{\phi}_2 \rangle$ lies in $(\mathcal{X}(N) \times \mathcal{X}(N))(S)$ and satisfies $\tilde{x}_F = x_F$. Thus $\tilde{y} = \tilde{\beta}_{N,S}(\tilde{x})$ satisfies $\tilde{y}_F = y_F$, and so $\beta_{N,S}(\tilde{x}) = y$ because A is the Neron model of A_F. Thus, $\tilde{\beta}_N$ satisfies the valuative criterion of properness, and so β_N is proper and hence finite.

Since β_N is a closed map, it follows that $H_{H^2} = \beta_N(X(N) \times X(N))$ is a closed subset of A_2. Moreover, since $X(N) \times X(N)$ is an affine and irreducible surface, it follows from Chevalley's Theorem ([EGA] (II, 6.7.1)) that the same is true for H_{N^2}.

4 The modular correspondence T_α^N

From Theorem 15 we see that every curve on the Humbert surface H_{N^2} is the image of a curve on the product surface $X(N) \times X(N)$, and so the irreducible curve components of the intersection $H_{N^2} \cap H_M$ can be obtained as images of curves lying on the product surface.

As is well-known (cf. [Sh]), the product surface $X(N) \times X(N)$ contains a multitude of interesting curves called *modular correspondences*. If $K = \mathbb{C}$, then each such curve is defined analytically as the image of the graph of a primitive integral matrix $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$ acting on the upper half plane $\mathfrak{H}$ and hence is denoted by T_α^N.

As we shall see (cf. Theorem 7), the irreducible components of $H_{N^2} \cap H_M$ are all of the form $\beta_N(T_\alpha^N)$, for suitable matrices α. To prove this, we require a *modular interpretation* of the modular correspondences T_α^N. Such an interpretation was given in [K6]. However, in place of working with T_α^N directly, it is more convenient to work with the normalization $\tau_\alpha^N : X_\alpha^N \to T_\alpha^N$ of T_α^N.

In order to give the modular interpretation of the modular curves X_α^N and T_α^N, it is useful to introduce the following terminology.

Definition. Let α be an integral 2×2 matrix. If $f : E \to E'$ is an S-isogeny of elliptic curves over a K-scheme S, and if ϕ and ϕ' are level N-structures of E/S and E'/S respectively, then we say that the tuple (ϕ, f, ϕ') is α-*compatible* if

$$f \circ \phi \;=\; \phi' \circ [\alpha]_N. \tag{12}$$

If $\alpha \in \mathcal{M}_d$ is a primitive matrix of determinant d, then let $\mathcal{X}_\alpha^N$ denote the moduli functor defined by the isomorphism classes of α-compatible tuples, i.e.,

$$\mathcal{X}_\alpha^N(S) \;=\; \{\langle E/S, \phi, E'/S, \phi', f\rangle : \langle E/S, \phi\rangle, \langle E'/S, \phi'\rangle \in \mathcal{X}(N)(S),\ f : E \to E' \text{ is a cyclic } S\text{-isogeny of degree } d \text{ such that } (\phi, f, \phi') \text{ is } \alpha\text{-compatible}\}.$$

Here, two such 5-tuples $(E_i/S, \phi_i, E_i'/S, \phi_i', f_i)$, for $i = 1, 2$, are *isomorphic* if there exist S-isomorphisms $g : E_1 \xrightarrow{\sim} E_2$ and $g' : E_1' \xrightarrow{\sim} E_2'$ with $f_2 \circ g = g' \circ f_1$, $\phi_2 = g \circ \phi_1$ and $\phi_2' = g' \circ \phi_1'$.

The following result follows from the more general results of [K6].

Theorem 16 *If* $\mathrm{char}(K) \nmid Nd$, *then the moduli functor* $\mathcal{X}_\alpha^N$ *is coarsely represented by a smooth, geometrically irreducible affine curve* X_α^N/K *which is a quotient of the modular curve* $X(Nd)$. *If, moreover,* $N \geq 3$, *then* $\mathcal{X}_\alpha^N$ *is finely represented by* X_α^N.

Proof. [K6], Theorems 2 and 3.

Remark 17 It was also shown in [K6] that the isomorphism class of the curves X_α^N only depends on $d = \det(\alpha)$ and on N, and that when $K = \mathbb{C}$, then X_α^N is analytically isomorphic to the open Riemann surface $\Gamma_0(N, d)\backslash\mathfrak{H}$, where $\mathfrak{H}$ is the upper half plane and $\Gamma_0(N, d) = \Gamma(N) \cap \Gamma_0(Nd)$.

As was mentioned above, the curve X_α^N is the normalization of the modular correspondence T_α^N on $X(N) \times X(N)$. More precisely, the normalization morphism $\tau_\alpha^N : X_A^N \to T_\alpha^N$ is induced by the forget morphism $\tilde{\tau}_\alpha^N = \{(\tau_\alpha^N)_S\}_S : \mathcal{X}_\alpha^N \to \mathcal{X}(N) \times \mathcal{X}(N)$, which is defined by the rule

$$(\tilde{\tau}_\alpha^N)_S(\langle E_1/S, \phi_1, E_2/S, \phi_2, f\rangle\}) = \langle E_1/S, \phi_1, E_2/S, \phi_2\rangle.$$

Thus, by the universal property of the coarse moduli scheme X_A^N, the morphism $\tilde{\tau}_A^N$ induces a morphism of K-schemes $\tau_\alpha^N : X_\alpha^N \to X(N) \times X(N)$ and we have

Proposition 18 *The morphism* τ_α^N *is finite and hence its image* T_α^N *is a closed irreducible curve on* $X(N) \times X(N)$. *Moreover,* τ_α^N *birational onto its image, and so* X_α^N *is the normalization of* T_α^N.

Proof. [K6], Proposition 30.

Remark 19 It follows from the above that if $x_i = \langle E_i/K, \phi_i\rangle \in X(N)(K)$, where $i = 1, 2$, then

$$(13)\quad (x_1, x_2) \in T_\alpha^N(K) \quad \Leftrightarrow \quad \begin{array}{l}\exists \text{ a cyclic isogeny } f : E_1 \to E_2 \text{ of degree } d = \det(\alpha)\\ \text{such that } (\phi_1, f, \phi_2) \text{ is } \alpha\text{-compatible.}\end{array}$$

Corollary 20 *If* $\mathrm{char}(K) \nmid Nd$, *then for every* $\alpha \in \mathcal{M}_d$ *there is a unique finite morphism*

$$\beta_\alpha^N : X_\alpha^N \to A_2$$

with the property that if $x \in X_\alpha^N(K)$ *is defined by* $\langle E_1/K, \phi_1, E_2/K, \phi_2, f\rangle \in \mathcal{X}_\alpha^N(K)$, *then* $y = \beta_\alpha^N(x)$ *is given by* $\langle A_\psi, \lambda_\psi\rangle \in \mathcal{A}_2(K)$, *where* $\psi = \psi_{\phi_1,\phi_2} : E_1[N] \to E_2[N]$ *is defined by* (10). *Moreover, we have the relation*

$$(14)\qquad \phi_1^{-1} \circ \psi^{-1} \circ f \circ \phi_1 = [\beta\alpha]_N, \quad \text{where } \beta = \left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right).$$

Proof. Consider the morphism $\beta_\alpha^N := \beta_N \circ \tau_\alpha^N : X_\alpha^N \to A_2$, where τ_α^N is as in Proposition 18 and β_N as in Theorem 15. Since both τ_α^N and β_N are finite morphisms, so is β_α^N. It is clear from the definitions that β_α^N satisfies the asserted property. Since K is algebraically closed, this property determines β_α^N at all closed points of X_α^N, and hence also the morphism β_α^N itself because X_α^N is reduced (and Jacobson). Finally, property (14) follows directly from (12) and (10).

Remark 21 It follows from Corollary 20 and Theorem 16 that if $\mathrm{char}(K) \nmid Nd$ and if $\alpha \in \mathcal{M}_d$, then

$$\overline{T}_\alpha^N \;:=\; \beta_\alpha^N(X_\alpha^N) \;=\; \beta_N(T_\alpha^N)$$

is an irreducible curve lying on the modular three-fold A_2. Note that since the definition of X_α^N depends only on N, d and $[\alpha]_N$, it follows that

$$\alpha_1 \equiv \alpha_2 \,(\mathrm{mod}\ N) \quad \Rightarrow \quad \overline{T}_{\alpha_1}^N \;=\; \overline{T}_{\alpha_2}^N, \quad \text{for all } \alpha_1, \alpha_2 \in \mathcal{M}_d. \tag{15}$$

5 The irreducible components of $H(q)$

By using the curves $\overline{T}_\alpha^N$ constructed in the previous section, we can now identify the irreducible components of the generalized Humbert schemes $H(q)$, where q is a form of type (N, m, d). These results depend heavily on the results of [K5].

As a first step, we show that the curve $\overline{T}_\alpha^N$ is contained in $H(q_\alpha^N)$, where q_α^N is the binary quadratic form defined in §1.

Proposition 22 *Let N and d be positive integers, and let $\alpha \in \mathcal{M}_d$ be a primitive matrix of determinant d. Write $\beta\alpha = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$, where $\beta = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, and put $g = \gcd(x - w, y, z, N)$, $m = \frac{N}{g}$, and $t = \mathrm{trace}(\beta\alpha) = x + w$. Then the binary quadratic form q_α^N defined by $q_\alpha^N = [N^2, 2mt, \frac{m^2}{N^2}(t^2 + 4d)]$, i.e., by*

$$q_\alpha^N(X, Y) \;=\; N^2X^2 + 2mtXY + \tfrac{m^2}{N^2}(t^2 + 4d)Y^2,$$

has type (N, m, d), and we have that $\overline{T}_\alpha^N \subset H(q_\alpha^N)$, provided that $\mathrm{char}(K) \nmid Nd$.

Proof. Since $\beta\alpha$ is primitive and $\det(\beta\alpha) = -d$, it follows from Corollary 12 of [K5] that q_α^N has type (N, m, d). (Note that there is a typo in this corollary: the hypothesis "N-primitive" has to be replaced by "primitive". Note also that the form given there is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to q_α^N.)

Assume now that $\mathrm{char}(K) \nmid Nd$. To show that $\overline{T}_\alpha^N \subset H(q_\alpha^N)$, let $y \in \overline{T}_\alpha^N(K)$. Since K is algebraically closed, there exists an $x \in X_\alpha^N(K)$ such that $\beta_\alpha^N(x) = y$, and x is given by a 5-tuple $\langle E/K, \phi, E'/K, \phi', f\rangle \in \mathcal{X}_\alpha^N(K)$. Then by Corollary 20

we have that y is given by $\langle A_\psi, \lambda_\psi \rangle \in \mathcal{A}_2(K)$, where $\psi = \psi_{\phi,\phi'}$ is as in (10). Thus, (E, E', ψ, π_ψ) is an *N-presentation* of (A_ψ, λ_ψ) in the sense of [K5], §3.

By (14) we see that $\alpha' := \beta\alpha$ is the matrix of $\psi^{-1} \circ f_{|E[N]}$ with respect to the basis (P, Q) of $E[N]$ defined by ϕ. Since α' is primitive of determinant $-d$ and f is cyclic of degree d, it follows from Proposition 28 and Remark 29 of [K5] that $q_{(A_\psi,\lambda_\psi)}$ primitively represents q_α^N, and so $y \in H(q_\alpha^N)$. Thus $\overline{T}_\alpha^N \subset H(q_\alpha^N)$, as claimed.

Proof of Theorem 7. By Proposition 22 we see that the right hand side of (3) is contained in the left hand side because $H(q) = H(q_\alpha^N)$, if $q \sim q_\alpha^N$.

To prove the opposite inclusion, let $y \in H(q)$ be given by $\langle J, \lambda \rangle \in \mathcal{A}_2(K)$. Then the definition of $H(q)$ implies that $q_{(J,\lambda)}$ primitively represents q, and so there exists a primitive submodule $\bar{\mathcal{G}}$ of $\mathrm{NS}(B, \lambda)$ such that the restriction of $q_{(J,\lambda)}$ to $\bar{\mathcal{G}}$ is equivalent to q. Since q has type (N, m, d) by hypothesis, it follows from Theorem 31 of [K5] that there exists an N-presentation (E, E', ψ, π) of (J, λ), and a cyclic isogeny $h : E \to E'$ of degree d and an integer k with $\gcd(k, N/m) = 1$ such that if M is any integral matrix with the property that $M \pmod N$ is the matrix of $\psi^{-1} \circ h_{|E[N]}$ (with respect to some basis of $E[N]$), then q is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to the form $q_{M,N,d,k} := [N^2, -2mT, \frac{m^2}{N^2}(T^2 + 4d)]$, where $T = -\mathrm{tr}(M) + dk^3(\det(M) + d)$.

Fix a level N-structure $\phi : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E[N]$ of E, and put $\phi' := \psi \circ \phi \circ [\beta]_N$. Note that ϕ' is a level N-structure of E', as is easy to check. Since $\phi^{-1} \circ \psi^{-1} \circ h \circ \phi \in \mathrm{End}((\mathbb{Z}/N\mathbb{Z})^2)$, it follows that there is an integral matrix $M \in M_2(\mathbb{Z})$ such that

$$\phi^{-1} \circ \psi^{-1} \circ h \circ \phi \;=\; [M]_N. \tag{16}$$

Note that this means that $M \pmod N$ is the matrix of $\psi^{-1} \circ h_{|E[N]}$ with respect to the basis $\mathcal{B} = (\phi(1,0), \phi(0,1))$ defined by ϕ, and so q is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to $q_{M,N,d,k}$.

Since h is a cyclic isogeny, it follows that M is N-primitive. Moreover, since ψ is an anti-isometry, we have that $\det(M) \equiv -\deg(h) \equiv -d \pmod N$. Thus, by [K5], Lemma 30, there exists a primitive matrix α' of determinant $-d$ such that $\alpha' \equiv M \pmod N$. Put $\alpha := \beta\alpha'$. Then $\alpha \in \mathcal{M}_d$, and $[\beta\alpha]_N = [M]_N$, so q is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to $q_{\beta\alpha,N,d,k} = q_\alpha^N$, and it follows from (16) and the definition of ϕ' that (ϕ, h, ϕ') is α-compatible. Thus $x = \langle E/K, \phi, E'/K, \phi', h \rangle \in X_\alpha^N$ and we have by Corollary 20 that $\beta_\alpha^N(x) = y$. This shows that $y \in \overline{T}_\alpha^N$, for suitable $\alpha \in \mathcal{M}_d$ with $q_\alpha^N \sim q$ (where $\sim$ denotes $\mathrm{GL}_2(\mathbb{Z})$-equivalence), and so (3) holds.

To prove the last assertion, note that it follows from (15) that the union on the right side of (3) consists of only finitely many distinct curves $\overline{T}_\alpha^N$. Since each of these is a closed subset of A_2 by Corollary 20, it follows that $H(q)$ is a closed subset of $A_2(K)$. Furthermore, since $H(q) \neq \emptyset$ by Theorem 1 and since the $\overline{T}_\alpha^N$'s are irreducible closed curves, it follows that $H(q)$ is an equidimensional curve.

Remark 23 As the above proof shows, there exists a closed subscheme $\mathbf{H}(q)_K$ of A_2/K such that its set of K-rational points equals $H(q) \subset A_2(K)$. We note that it

follows from Theorem 7 that the scheme $\mathbf{H}(q)_K$ is compatible with base-change: if K' is an algebraically closed extension field of K, then $\mathbf{H}(q)_K \otimes K' = \mathbf{H}(q)_{K'}$ because the $\overline{T}_\alpha^N$'s are compatible with base-change.

Proof of Corollary 8. From Corollary 2 it follows that $H_{N^2} \cap H_M \neq \emptyset$ and by Proposition 12 and Theorem 4 we know that $H_{N^2} \cap H_M$ is a union of $H(q)$'s, where q has type (N, m, d), for some $m|N$ and some $d \geq 1$. Since $\mathrm{disc}(q) = -16m^2d$, we see that $d \leq m^2d = \frac{|\mathrm{disc}(q)|}{16} \leq \frac{N^2M}{4}$ by Remark 13. Thus, by the given hypothesis we see that $\mathrm{char}(K) \nmid Nd$, and so by Theorem 7 we have that each such $H(q)$ is an equidimensional curve, and hence so is $H_{N^2} \cap H_N$.

For later use, we note the following partial refinement of Theorem 7.

Proposition 24 *Let q be a form of type (N, m, d) and let $\alpha \in \mathcal{M}_{d_1}$. If $\mathrm{char}(K) \nmid Ndd_1$, then $\overline{T}_\alpha^N \subset H(q)$ if and only if q is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to q_α^N, i.e., $q \sim q_\alpha^N$. If this is the case, then $d_1 = d$.*

The proof uses the following technical fact about *non-CM points* in $\mathcal{X}_\alpha^N$ which will be used several times below. A point $x = \langle E/K, \phi, E'/K, \phi', h\rangle \in \mathcal{X}_\alpha^N(K)$ is called a *non-CM point* if $\mathrm{End}(E) = \mathbb{Z}$.

Lemma 25 *Let $\alpha \in \mathcal{M}_d$ and $N \geq 1$, and suppose that $\mathrm{char}(K) \nmid Nd$ and that K is not the algebraic closure of a finite field.*

(a) *There exist infinitely many non-CM points in $\mathcal{X}_\alpha^N(K)$.*

(b) *If $x \in \mathcal{X}_\alpha^N(K)$ is a non-CM point, and if $\beta_\alpha^N(x) = \langle J, \lambda\rangle$, then $q_{(J,\lambda)} \sim q_\alpha^N$.*

Proof. (a) The hypothesis on K implies that there exist infinitely many non-isomorphic elliptic curves E_i/K such that $\mathrm{End}(E_i) = \mathbb{Z}$. Fix a level N-structure ϕ_i on E_i, and choose a cyclic subgroup $C_i \leq E_i$ of order Nd such that $C_i[N]$ is generated by $P_i = \phi_{i1}(1, 0)$. Let $h_i : E_i \to E_i' := E_i/C_i[d]$ be the quotient isogeny. Then by [K6], Proposition 24, there exists a level N-structure ϕ_{i1}' on E_i' such that $(\phi_{i1}, h_i, \phi_{i1}')$ is α_d-compatible, where $\alpha_d = \left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Now $\alpha = g_1\alpha_d g_2$, for some $g_1, g_2 \in \mathrm{SL}_2(\mathbb{Z})$, so if we put $\phi_i = \phi_{i1} \circ [g_2]_N$ and $\phi_i' = \phi_{i1}' \circ [g_1^{-1}]_N$, then (ϕ_i, h_i, ϕ_i') is α-compatible, as is easy to check. Thus, $x_i = \langle E_i/K, \phi_i, E_i'/K, \phi_i', h_i\rangle \in \mathcal{X}_\alpha^N(K)$ is a non-CM point. Moreover, $x_i \neq x_j$, if $i \neq j$ (because $E_i \not\simeq E_j$), and so we obtain infinitely many non-CM points.

(b) By Proposition 22 we know that $q_{(J,\lambda)}$ primitively represents q_α^N. But since $\mathrm{Hom}(E, E') \simeq \mathbb{Z}$, we see that $\mathrm{rank}(q_{(J,\lambda)}) = 2$, and so it follows that $q_{(J,\lambda)} \sim q_\alpha^N$.

Proof of Proposition 24. If $q \sim q_\alpha^N$, then by definition $H(q) = H(q_\alpha^N)$, and so $\overline{T}_\alpha^N \subset H(q_\alpha^N) = H(q)$ by Proposition 22.

Now suppose conversely that $\overline{T}_\alpha^N \subset H(q)$. Then this also holds after a base-change of K (cf. Remark 23), so we may assume that K is not the algebraic closure of a

finite field. Then by Lemma 25 there exists $\langle J, \lambda \rangle \in \overline{T}_\alpha^N(K)$ such that $q_{(J,\lambda)} \sim q_\alpha^N$. On the other hand, since $\langle J, \lambda \rangle \in H(q)$, we have that $q_{(J,\lambda)}$ primitively represents q, so $q_{(J,\lambda)} \sim q$, and hence $q_\alpha^N \sim q$, as claimed.

To prove the last assertion, recall from [K5], Proposition 11, that q_α^N has type (N, m_1, d_1) for some unique $m_1 | N$ with $\gcd(d_1, \frac{N}{m_1}) = 1$. Now if $q_\alpha^N \sim q$, then q_α^N also has type (N, m, d), and so we have that $m_1 = m$ and $d_1 = d$ by [K5], Proposition 7.

We observe that the above Proposition 24 has the following interesting application.

Corollary 26 *Let $q_i \in Q(N, m_i, d_i)$, where $i = 1, 2$, be two binary forms which are not equivalent. If $\mathrm{char}(K) \nmid N d_1 d_2$, then $H(q_1) \cap H(q_2)$ consists of finitely many CM-points.*

Proof. If $H(q_1) \cap H(q_2)$ were infinite, then from Theorem 7 it follows that $H(q_1)$ and $H(q_2)$ would contain a common irreducible curve component T_α^N, where $\alpha \in \mathcal{M}_{d_1}$. By Proposition 24 we then have that $q_\alpha^N \sim q_i$, for $i = 1, 2$, and so $q_1 \sim q_2$, contrary to our hypothesis. Thus $H(q_1) \cap H(q_2)$ is a finite set. Furthermore, if any of these intersection points $\langle J, \lambda \rangle$ were images of non-CM points, then by the proof of Proposition 24 we see that $q_{(J,\lambda)} \sim q_i$, for $i = 1, 2$, so again we obtain the contradiction that $q_1 \sim q_2$.

We now turn to the proof of Theorem 9 of the introduction. The first assertion follows easily from the following lemma.

Lemma 27 *Let $\alpha_1, \alpha_2 \in \mathcal{M}_d$, and suppose that*

$$\beta \alpha_2 \equiv \varepsilon g^{-1} \beta \alpha_1 g \pmod{N}, \quad \text{for some } g \in \mathrm{SL}_2(\mathbb{Z}) \text{ and } \varepsilon \in \{1, -1\}.$$

If $x_1 := \langle E/K, \phi; E'/K, \phi'; h \rangle \in \mathcal{X}_{\alpha_1}^N(K)$, then $x_2 := \langle E/K, \phi \circ [g]_N; E'/K, \phi' \circ [g']_N; \varepsilon h \rangle \in \mathcal{X}_{\alpha_2}^N(K)$, where $g' = \beta^{-1} g \beta$, and we have that $\beta_{\alpha_1}^N(x_1) = \beta_{\alpha_2}^N(x_2)$.

Proof. Since g, $g' = \beta^{-1} g \beta \in \mathrm{SL}_2(\mathbb{Z})$, it is clear that $\phi \circ [g]_N$ and $\phi' \circ [g']_N$ are level N-structures of E/K and E'/K, respectively. Now since (ϕ, h, ϕ') is α_1-compatible, it follows that $(\phi \circ [g]_N, \varepsilon h, \phi \circ [g']_N)$ is α_2-compatible because $\varepsilon h \circ \phi \circ [g]_N = \varepsilon \phi' \circ [\alpha_1 g]_N = \phi' \circ [g' \alpha_2]_N = \phi' \circ [g'] \circ [\alpha_2]_N$. This proves the first assertion.

To prove the second assertion, let $\psi = \psi_{\phi, \phi'} : E[N] \to E'[N]$ be defined as in (10), so $\beta_{\alpha_1}^N(x_1) = \langle A_\psi, \pi_\psi \rangle$, where $A = E \times E'$. Similarly, $\beta_{\alpha_2}^N(x_2) = \langle A_{\psi'}, \pi_{\psi'} \rangle$, where $\psi' = \psi_{\phi \circ [g]_N, \phi' \circ [g']_N}$. Now since $g \beta (g')^{-1} = \beta$, we see that

$$\psi' = \phi' \circ [g]_N \circ [\beta]_N \circ (\phi \circ [g']_N)^{-1} = \phi' \circ [g \beta (g')^{-1}]_N \circ \phi^{-1} = \phi' \circ [\beta]_N \circ \phi^{-1} = \psi,$$

and so it is clear that $\beta_{\alpha_1}^N(x_1) = \beta_{\alpha_2}^N(x_2)$.

It is more difficult to prove the second assertion of Theorem 9. For this, we will prove the following more general assertion.

Theorem 28 *Let q be a form of type (N, m, d) which satisfies the condition*

$$|\{(X,Y) \in \mathbb{Z}^2 : \gcd(X,Y) = 1 \text{ and } q(X,Y) = N^2\}| \;=\; 2. \tag{17}$$

If $\mathrm{char}(K) \nmid Nd$ *and if* $\alpha_1, \alpha_2 \in \mathcal{M}_d$ *satisfy* $q_{\alpha_i} \sim q$, *for* $i = 1, 2$, *then*

$$g\beta\alpha_1 g^{-1} \equiv \pm\beta\alpha_2 \,(\mathrm{mod}\ N), \text{ for some } g \in \mathrm{SL}_2(\mathbb{Z}) \;\Leftrightarrow\; \overline{T}^N_{\alpha_1} = \overline{T}^N_{\alpha_2}. \tag{18}$$

We observe that the hypothesis (17) follows from the hypothesis on d and N which was made in Theorems 4 and 9.

Lemma 29 *If q is a form of type (N, m, d) with $d > N^4/(4m^2)$, then q satisfies condition* (17).

Proof. Suppose first that $q = [N^2, 2mt, m^2(t^2 + 4d)/N^2]$, for some $t \in \mathbb{Z}$, and assume that $(X, Y) \in \mathbb{Z}^2$ satisfies $q(X, Y) = N^2$. If $Y \neq 0$, then $N^2 = q(X, Y) = (NX + \frac{m}{N}tY)^2 + \frac{4m^2 d}{N^2}Y^2 \geq \frac{4m^2 d}{N^2}$, which contradicts the hypothesis that $N^4/(4m^2) < d$. Thus $Y = 0$, and hence $X = \pm 1$ because $\gcd(X, Y) = 1$. Thus q satisfies (17).

If q is any form of type (N, m, d), then $q \sim q' := [N^2, 2mt, m^2(t^2 + 4d)/N^2]$, for some $t \in \mathbb{Z}$. By what was just proved, condition (17) holds for q' and hence also for q because the left hand side of (17) is the same for all $q \sim q'$.

Before proving Theorem 28, we observe that it and Lemma 27 imply Theorem 9.

Proof of Theorem 9 (using Theorem 28). The first assertion clearly follows from Lemma 27.

To prove the second assertion, suppose that $\overline{T}^N_{\alpha_1} = \overline{T}^N_{\alpha_2}$. Then $\overline{T}^N_{\alpha_1} \subset H(q^N_{\alpha_2})$ by Proposition 22, so $q^N_{\alpha_1} \sim q^N_{\alpha_2}$ by Proposition 24. (Recall that $q^N_{\alpha_2}$ has type (N, m_2, d), for some $m_i | N$, by [K5], Proposition 11.) Thus, $q^N_{\alpha_1} \sim q^N_{\alpha_2}$, and so both have the same type (N, m, d).

By Lemma 29 we know that the hypothesis $d > N^4/(4m^2)$ implies that $q^N_{\alpha_i}$ satisfies (17), and so the converse implication of (4) follows from (18).

To prove Theorem 28, we will use the following fact which will be proved in §6; cf. Corollary 37.

Lemma 30 *Let $\alpha \in \mathcal{M}_d$, where $d \neq 0$, and let $\alpha^* = dA^{-1}$ be its adjoint. Then for any $N \geq 1$, there exists a $g \in \mathrm{SL}_2(\mathbb{Z})$ such that $\beta\alpha^*\beta^{-1} \equiv g\alpha g^{-1} \,(\mathrm{mod}\ N)$.*

The following is the key result used in the proof of Theorem 28.

Proposition 31 *Let α_1, $\alpha_2 \in \mathcal{M}_d$ and suppose that $\mathrm{char}(K) \nmid Nd$. For $i = 1, 2$, let $x_i = \langle E_i, \phi_i, E_i', \phi', h_i\rangle \in \mathcal{X}^N_{\alpha_i}(K)$ be two non-CM points such that $\beta^N_{\alpha_1}(x_1) = \beta^N_{\alpha_2}(x_2)$,*

so there exists an isomorphism $\varphi : (A_{\psi_2}, \lambda_{\psi_2}) \xrightarrow{\sim} (A_{\psi_1}, \lambda_{\psi_1})$*, where* $\psi_i = \psi_{\phi_i, \phi_i'}$*, for* $i = 1, 2$*. If*

$$\varphi\pi_2(E_2 \times \{0\}) = \pi_1(E_1 \times \{0\}) \quad \textit{or} \quad \varphi\pi_2(\{0\} \times E_2') = \pi_1(E_1 \times \{0\}), \tag{19}$$

where $\pi_i = \pi_{\psi_i} : E_i \times E_i' \to A_{\psi_i}$ *is the quotient isogeny, for* $i = 1, 2$*, then there exists* $g \in \mathrm{SL}_2(\mathbb{Z})$ *such that* $g\beta\alpha_1 g^{-1} \equiv \pm\beta\alpha_2 \pmod N$*, and hence* $\overline{T}_{\alpha_1}^N = \overline{T}_{\alpha_2}^N$*.*

Proof. Note first that $(E_i, E_i', \psi_i, \pi_i)$ is an N-presentation of $(A_{\psi_i}, \lambda_{\psi_i})$ in the sense of [K4], §2. Put $(J, \lambda) := (A_{\psi_1}, \lambda_{\psi_1})$; then $(E_2, E_2', \psi_2, \varphi\pi_2)$ is also an N-presentation of (J, λ). Put $\overline{E} := \pi_1(E_1 \times \{0\})$. We have to consider the following two cases:

Case 1: $\overline{E} = \varphi\pi_2(E_2 \times \{0\})$.

Here it follows from Proposition 10(e) of [K4] that there exist isomorphisms $f : E_1 \xrightarrow{\sim} E_2$ and $f' : E_1' \xrightarrow{\sim} E_2'$ such that $\pi_1 = \varphi \circ \pi_2 \circ (f \times f')$. Put $h_1' = (f')^{-1} \circ h_2 \circ f \in \mathrm{Hom}(E_1, E_1')$. Since x_1 is a non-CM point, we have that $\mathrm{Hom}(E_1, E_1') = \mathbb{Z}h_1$, and so $h_1' = \varepsilon h_1$ with $\varepsilon \in \{1, -1\}$ because h_1' is cyclic. Moreover, since $\mathrm{Graph}(-\psi_1) = \mathrm{Ker}(\pi_1) = \mathrm{Ker}(\pi_2 \circ (f \times f')) = (f \times f')^{-1}(\mathrm{Graph}(-\psi_2))$, we see that $f' \circ \psi_1 = \psi_2 \circ f_{|E_1[N]}$.

Recall from (14) that $[\beta\alpha_i]_N = \phi_i^{-1} \circ \psi_i^{-1} \circ h_i \circ \phi_i$, for $i = 1, 2$. Substituting $h_2 = f' \circ (\varepsilon h_1) \circ f^{-1}$ and $\psi_2^{-1} = f \circ \psi^{-1} (f'_{E_1'[N]})^{-1}$ shows that $[\varepsilon\beta\alpha_2]_N = \bar{g} \circ [\beta\alpha_1]_N \circ \bar{g}^{-1}$, where $\bar{g} := \phi_2^{-1} \circ f \circ \phi_1 \in \mathrm{Aut}(E[N])$. Since f is an isomorphism of elliptic curves and the ϕ_i are level N-structures (of the same determinant), we see that $\det(\bar{g}) = 1$. Thus, there exists $g \in \mathrm{SL}_2(\mathbb{Z})$ such that $[g]_N = \bar{g}$, and so $\varepsilon\beta\alpha_2 \equiv g\beta\alpha_1 g^{-1} \pmod N$. Thus $\overline{T}_{\alpha_1}^N = \overline{T}_{\alpha_2}^N$ by Lemma 27.

Case 2: $\overline{E} = \varphi\pi_2(\{0\} \times E_2')$.

Since (ϕ_2, h_2, ϕ_2') is α_2-compatible, it follows that (ϕ_2', h_2^t, ϕ_2) is α_2^*-compatible, and so $x_2^* := \langle E_2', \phi_2', E_2, \phi_2, h_2^t \rangle \in \mathcal{X}_{\alpha_2^*}^N(K)$. Since $\beta^{-1} = \beta$, we see that $\psi_{\phi_2', \phi_2} = \phi_2 \circ [\beta]_N \circ (\phi_2')^{-1} = (\phi_2' \circ [\beta]_N \circ (\phi_2)^{-1})^{-1} = \psi_2^{-1}$. Let $\eta : E_2' \times E_2 \to E_2 \times E_2'$ be defined by $\eta(x', x) = (x, x')$, and put $\pi_2' = \varphi \circ \pi_2 \circ \eta : E_2' \times E_2 \to J$. Then $(E_2', E_2, \psi_2^{-1}, \pi_2')$ is an N-presentation of (J, λ), so $\beta_{\alpha_2^*}^N(x_2^*) = \langle J, \lambda \rangle$.

Since $\pi_2'(E_2' \times \{0\}) = \varphi\pi_2(\{0\} \times E_2') = \overline{E}$, we see that x_1 and x_2^* satisfy the hypotheses of the proposition and also the condition of Case 1. Thus, by what was proven above, it follows that there exists $g_1 \in \mathrm{SL}_2(\mathbb{Z})$ and $\varepsilon \in \{\pm 1\}$ such that $[\varepsilon\beta\alpha_2^*]_N = [g_1\beta\alpha_1 g_1^{-1}]_N$. On the other hand, by Lemma 30 there exists $g_2 \in \mathrm{SL}_2(\mathbb{Z})$ such that $[\beta\alpha_2]_N = [g_2(\beta(\beta\alpha_2)^*\beta^{-1})g_2^{-1}]_N = [g_2\beta\alpha_2^* g_2^{-1}]_N$, where the latter equality follows because $(\beta\alpha_2)^* = \alpha_2^*\beta^* = \alpha_2^*\beta$. Thus, putting $g = g_2 g_1$ shows that $[\varepsilon\beta\alpha_2]_N = [g\beta\alpha_1 g^{-1}]_N$, and so $\overline{T}_{\alpha_1}^N = \overline{T}_{\alpha_2}^N$ as before.

Corollary 32 *Let* α_1*,* $\alpha_2 \in \mathcal{M}_d$ *and suppose that* $\mathrm{char}(K) \nmid Nd$ *and that* $q = q_{\alpha_1}^N$ *satisfies condition* (17)*. If there exists a non-CM point* $x_1 \in \mathcal{X}_{\alpha_1}^N(K)$ *and a point* $x_2 \in \mathcal{X}_{\alpha_2}^N(K)$ *such that* $\beta_{\alpha_1}^N(x_1) = \beta_{\alpha_2}^N(x_2)$*, then there exists* $g \in \mathrm{SL}_2(\mathbb{Z})$ *such that* $g\beta\alpha_1 g^{-1} \equiv \pm\beta\alpha_2 \pmod N$*, and hence* $\overline{T}_{\alpha_1}^N = \overline{T}_{\alpha_2}^N$*.*

Proof. Write $x_i = \langle E_i/K, \phi_i, E_i'/K, \phi_i', h_i\rangle$, and let ψ_i, π_i, φ and (J,λ) be as in the proof of Proposition 31. By Lemma 25 we know that $q_{(J,\lambda)} \sim q_{\alpha_1}^N = q$, so by Theorem 18 of [K4] we see that the condition (17) is equivalent to the condition $|\mathcal{S}_N(J,\lambda)| = 2$, where $\mathcal{S}_N(J,\lambda)$ denotes the set of elliptic subgroups of J of λ-degree N.

By Proposition 10(d) of [K4] we know that $\overline{E} := \pi_1(E_1 \times \{0\}) \in \mathcal{S}_N(J,\lambda)$, and so $\mathcal{S}_N(J,\lambda) = \{\overline{E}, \overline{E}^\perp\}$ by Proposition 10(a) of [K4] and the fact that $|\mathcal{S}_N(J,\lambda)| = 2$. Since also $\overline{E}_2 := \varphi\pi_2(E_2 \times \{0\}) \in \mathcal{S}_N(J,\lambda)$ and $\overline{E}_2' := \varphi\pi_2(\{0\} \times E_2') \in \mathcal{S}_N(J,\lambda) = (\overline{E}_2)^\perp \neq \overline{E}_2$, we thus have that either $\overline{E} = \overline{E}_2$ or $\overline{E} = \overline{E}_2'$. This means that condition (19) holds and so the assertion follows from Proposition 31.

Proof of Theorem 28. The one implication of (18) follows from Lemma 27. To prove the converse implication, suppose that $\overline{T}_{\alpha_1}^N = \overline{T}_{\alpha_2}^N$. Then this equality of subschemes of A_2/K also holds over any extension field, and so we may assume that K is not the algebraic closure of a finite field. Then by Lemma 25 there is a non-CM point $x_1 \in \mathcal{X}_{\alpha_1}^N(K)$, and so there exists $x_2 \in \mathcal{X}_{\alpha_2}^N(K)$ such that $\beta_{\alpha_1}^N(x_1) = \beta_{\alpha_2}^N(x_2)$ because $\overline{T}_{\alpha_1}^N = \overline{T}_{\alpha_2}^N$. We thus are in the situation of Corollary 32, and so (18) follows.

6 Conjugacy classes of matrices

In view of Theorems 9 and 28, it is important to understand the $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$-conjugacy classes of matrices mod N. If $N = p^r$ is a power of prime, then the conjugacy classes of matrices in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ were determined by Nobs[No]. His method can be generalized to obtain similar results for an arbitrary integer N and arbitrary matrices α mod N. For our purposes, however, it is more convenient to express this in terms of $\mathrm{SL}_2(\mathbb{Z})$-conjugacy, using the fact that $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is surjective.

The first step is to find a normal form for a representative of the conjugacy class of such matrices.

Notation. Let $\alpha = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in M_2(\mathbb{Z})$ be an integral matrix, and let $N \geq 1$ be an integer. Put

$$g_{\alpha,N} := \gcd(x-w, y, z, N), \quad \text{and} \quad \bar{x}_{\alpha,N} := \mathrm{rem}(x, g_{\alpha,N}).$$

Thus, if $g = g_{\alpha,N}$, and $\bar{x} = \bar{x}_{\alpha,N}$, then $0 \leq \bar{x} < g$ and $\bar{x} \equiv x \,(\mathrm{mod}\, g)$. In addition, put

$$\begin{aligned} (20) \qquad \tau_{\alpha,N} &:= (\mathrm{tr}(\alpha) - 2\bar{x})/g \quad \text{and} \\ \delta_{\alpha,N} &:= (\det(\alpha) + \bar{x}^2 - \mathrm{tr}(\alpha)\bar{x})/g^2 = (\det(\alpha) - \bar{x}^2 - \bar{x}g\tau_{\alpha,N})/g^2. \end{aligned}$$

Lemma 33 *If $\alpha \in M_2(\mathbb{Z})$ and $N \geq 1$, then $\tau_{\alpha,N}$ and $\delta_{\alpha,N}$ are integers which satisfy the relation*

$$(21) \qquad \mathrm{tr}(\alpha)^2 - 4\det(\alpha) = (\tau_{\alpha,N}^2 - 4\delta_{\alpha,N})g_{\alpha,N}^2.$$

Proof. Put $\alpha' = (\alpha - \bar{x}I)/g$. From definitions of $g = g_{\alpha,N}$ and $\bar{x} = \bar{x}_{\alpha,N}$ we see that $\alpha' \in M_2(\mathbb{Z})$. We have that $\mathrm{tr}(\alpha') = (\mathrm{tr}(\alpha) - 2\bar{x})/g = \tau_{\alpha,N}$, so $\tau_{\alpha,N} = \mathrm{tr}(\alpha') \in \mathbb{Z}$. Moreover, $\det(\alpha) = \det(\bar{x}I + g\alpha') = \bar{x}^2 + \bar{x}g\mathrm{tr}(\alpha') + g^2\det(\alpha')$, so we also have that $\delta_{\alpha,N} = \det(\alpha') \in \mathbb{Z}$.

Put $\tau = \tau_{\alpha,N}$ and $\delta = \delta_{\alpha,N}$. From (20) we have that $\mathrm{tr}(\alpha)^2 - 4\det(\alpha) = (2\bar{x} + g\tau)^2 - 4(\bar{x}^2 + \bar{x}g\tau + g^2\delta) = g^2(\tau^2 - 4\delta)$, as claimed.

The above quantities are invariants of the conjugacy class of $\alpha \pmod N$, as the following result shows.

Proposition 34 *Let $N \geq 1$, and let $\alpha_i \in M_2(\mathbb{Z})$, $i = 1, 2$ be two matrices such that*

$$\alpha_1 \equiv \gamma\alpha_2\gamma^{-1} \pmod N.$$

Then $g_{\alpha_1,N} = g_{\alpha_2,N}$ and $\bar{x}_{\alpha_1,N} = \bar{x}_{\alpha_2,N}$. Moreover, if $m := \frac{N}{g_{\alpha_1,N}}$, then

$$\tau_{\alpha_1,N} \equiv \tau_{\alpha_2,N} \pmod m \quad \textit{and} \quad \delta_{\alpha_1,N} \equiv \delta_{\alpha_2,N} \pmod m. \tag{22}$$

Proof. Put $\alpha_3 = \gamma\alpha_2\gamma^{-1}$. Then $g_{\alpha_1,N} = g_{\alpha_3,N}$ because $g_{\alpha,N}$ depends only on $\alpha \pmod N$. Moreover, since $g_{\alpha,N}$ is invariant under conjugation by [K5], Corollary 13 , it follows that $g_{\alpha_3,N} = g_{\alpha_2,N}$, and hence $g_{\alpha_2,N} = g$.

Put $\alpha_i' = (\alpha_i - \bar{x}_i I)/g$, where $\bar{x}_i = x_{\alpha_i,N}$. Then $\alpha_i' \in M_2(\mathbb{Z})$, and $\tau_i := \tau_{\alpha_i,N} = \mathrm{tr}(\alpha_i')$ and $\delta_i := \delta_{\alpha_i,N} = \det(\alpha_i')$, as we saw in the proof of Lemma 33. Now $\bar{x}_1 I + g\alpha_2' = \alpha_1 \equiv \gamma\alpha_2\gamma^{-1} \equiv \bar{x}_2 I + g\gamma\alpha_2'\gamma^{-1} \pmod N$, so $\bar{x}_1 I \equiv \bar{x}_2 I \pmod g$, and hence $\bar{x}_1 \equiv \bar{x}_2 \pmod g$, so $\bar{x}_1 = \bar{x}_2$ since $0 \leq \bar{x}_i < g$. From this we see that the hypothesis implies that $\alpha_1' \equiv \gamma\alpha_2'\gamma^{-1} \pmod m$, so $\mathrm{tr}(\alpha_1') \equiv \mathrm{tr}(\alpha_2') \pmod m$ and $\det(\alpha_1') \equiv \det(\alpha_2') \pmod m$, and hence (22) follows.

We next observe that we can find a representative of the conjugacy class of $\alpha \pmod N$ of a special type.

Proposition 35 *Let $N \geq 1$ and $\alpha \in M_2(\mathbb{Z})$ and put $g = g_{\alpha,N}$, $m = N/g$, $\bar{x} = \bar{x}_{\alpha,N}$, $\tau = \tau_{\alpha,N}$ and $\delta = \delta_{\alpha,N}$. Then there exist $z, z' \in \mathbb{Z}$ with $zz' \equiv 1 \pmod m$ such that*

$$\gamma\alpha\gamma^{-1} \equiv \bar{x}I + g\left(\begin{smallmatrix} 0 & -\delta z' \\ z & \tau \end{smallmatrix}\right) \pmod N, \quad \textit{for some } \gamma \in \mathrm{SL}_2(\mathbb{Z}). \tag{23}$$

Proof. Put $\alpha' = (\alpha - \bar{x}I)/g \in M_2(\mathbb{Z})$. By construction, $g_{\alpha',m} = 1$. Suppose first that $m = p^r$ is a prime power. Then by Nobs[No], Lemma 4, there exists $\gamma_1 \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma_1\alpha'\gamma_1^{-1} \equiv \alpha_1 \pmod m$, where $\alpha_1 = \left(\begin{smallmatrix} * & * \\ z & * \end{smallmatrix}\right)$, with $\gcd(z, m) = 1$. Choose z' such that $zz' \equiv 1 \pmod m$, and put $\alpha_2 = \left(\begin{smallmatrix} 0 & -\delta z' \\ z & \tau \end{smallmatrix}\right)$. Then $\det(\alpha_2) \equiv \delta = \det(\alpha') \equiv \det(\alpha_1) \pmod m$ and $\mathrm{tr}(\alpha_2) = \tau = \mathrm{tr}(\alpha') \equiv \mathrm{tr}(\alpha_1) \pmod m$, so by Nobs[No], Lemma 5, there exists $\gamma_2 \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma_2\alpha_1\gamma_2^{-1} \equiv \alpha_2 \pmod m$. Put $\gamma = \gamma_2\gamma_1$. Then $\gamma\alpha'\gamma^{-1} \equiv \alpha_2 \pmod m$, so $\gamma\alpha\gamma^{-1} = \bar{x}I + g\gamma\alpha'\gamma^{-1} \equiv \bar{x}I + g\alpha_2 \pmod{gm}$, and hence

(23) holds when $m = p^r$. If m is a product of prime powers, then the same result follows from the prime power cases by using the Chinese remainder theorem.

The above elements $z, z' \in \mathbb{Z}$ are not uniquely determined mod m by the mod N conjugacy class of α. In order to classify the conjugacy classes we follow (and generalize) Nobs[No] and introduce the following set:

$$S_N(\tau, \delta) := \{a \in (\mathbb{Z}/N\mathbb{Z})^\times : \exists (\xi, \eta) \in \mathbb{Z}^2 \text{ with } \xi^2 + \tau\xi\eta + \delta\eta^2 \equiv a \,(\mathrm{mod}\ N)\}$$

It is easy to see (as in Nobs[No]) that $S_N(t, d)$ is a subgroup of $R_N^\times := (\mathbb{Z}/N\mathbb{Z})^\times$.

Proposition 36 *Suppose that $\alpha_1, \alpha_2 \in M_2(\mathbb{Z})$ and N satisfy $g_{\alpha_1,N} = g_{\alpha_2,N} = g$, and that $\alpha_i = xI + g\alpha_i'$, $i = 1, 2$, where $\alpha_i' = \left(\begin{smallmatrix} * & * \\ z_i & * \end{smallmatrix}\right)$ with $\gcd(z_i, m) = 1$, for $i = 1, 2$, where $m = N/g$. Put $\tau = \mathrm{tr}(\alpha_1')$ and $\delta = \det(\alpha_1')$, and let $\bar{z}_i$ denote the image of z_i in $R_m^\times = (\mathbb{Z}/m\mathbb{Z})^\times$. Then the following conditions are equivalent:*

(i) *There exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma\alpha_1\gamma^{-1} \equiv \alpha_2 \,(\mathrm{mod}\ N)$.*

(ii) $\mathrm{tr}(\alpha_2') \equiv \tau \,(\mathrm{mod}\ m)$, $\det(\alpha_2') \equiv \delta \,(\mathrm{mod}\ m)$ *and $\bar{z}_1\bar{z}_2^{-1} \in S_m(\tau, \delta)$.*

Proof. It is clear that condition (i) is equivalent to the condition

$$\text{There exists } \gamma \in \mathrm{SL}_2(\mathbb{Z}) \text{ such that } \gamma\alpha_1'\gamma^{-1} \equiv \alpha_2' \,(\mathrm{mod}\ m). \tag{24}$$

If $m = p^r$ is a prime power, then the equivalence of (24) and (ii) follows from Nobs[No], Lemma 5, and hence the general case follows from this by using the Chinese remainder theorem.

Corollary 37 *If $\alpha \in M_2(\mathbb{Z})$ and $N \geq 1$, then there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that*

$$\beta\alpha^*\beta \equiv \gamma\alpha\gamma^{-1} \,(\mathrm{mod}\ N). \tag{25}$$

Proof. Note first that if $\alpha = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$, then $\beta\alpha^*\beta = \left(\begin{smallmatrix} w & y \\ z & x \end{smallmatrix}\right)$. Thus, if $\alpha \equiv \alpha_1 \,(\mathrm{mod}\ N)$, then $\beta\alpha^*\beta \equiv \beta\alpha_1^*\beta \,(\mathrm{mod}\ N)$.

Put $g = g_{\alpha,N}$, $m = \frac{N}{g}$, and let $\bar{x}$, $\tau = \tau(\alpha)$, $\delta = \delta(\alpha)$ be defined as in (20). By Proposition 35 there exists $\alpha_1 = \left(\begin{smallmatrix} 0 & \delta z' \\ z & \tau \end{smallmatrix}\right)$ with $zz' \equiv 1 \,(\mathrm{mod}\ m)$ such that if $\alpha' = \bar{x}I + g\alpha_1$, then $\alpha' \equiv \gamma_1\alpha\gamma_1^{-1} \,(\mathrm{mod}\ N)$, for some $\gamma_1 \in \mathrm{SL}_2(\mathbb{Z})$. Then $\beta(\alpha')^*\beta = \bar{x}I + g\beta(\alpha_1)^*\beta$. Since $\beta(\alpha_1)^*\beta = \left(\begin{smallmatrix} \tau & \delta z' \\ z & 0 \end{smallmatrix}\right)$, it follows from Proposition 36 that there exists $\gamma_2 \in \mathrm{SL}_2(\mathbb{Z})$ such that $\beta(\alpha')^*\beta \equiv \gamma_2\alpha'\gamma_2^{-1} \,(\mathrm{mod}\ N)$. Now since $\alpha \equiv \gamma_1^{-1}\alpha'\gamma_1 \,(\mathrm{mod}\ N)$, we have that $\beta\alpha^*\beta \equiv \beta(\gamma_1^{-1}\alpha'\gamma_1)^*\beta \,(\mathrm{mod}\ N)$. Since $\gamma_1^* = \gamma_1^{-1}$, we see that $(\gamma_1^{-1}\alpha'\gamma_1)^* = \gamma_1^*(\alpha')^*(\gamma_1^{-1})^* = \gamma_1^{-1}(\alpha')^*\beta\gamma_1$. Thus, since $\beta^2 = 1$, it follows that $\beta(\gamma_1^{-1}\alpha'\gamma_1)^*\beta = \gamma_3\beta(\alpha')^*\beta\gamma_3^{-1}$, where $\gamma_3 = \beta(\gamma_1^{-1})\beta \in \mathrm{SL}_2(\mathbb{Z})$, and so $\beta\alpha^*\beta \equiv \gamma_3\beta(\alpha')^*\beta\gamma_3^{-1} \equiv \gamma_3\gamma_2\alpha'\gamma_2^{-1}\gamma_3^{-1} \equiv \gamma_3\gamma_2\gamma_1\alpha\gamma_1^{-1}\gamma_2^{-1}\gamma_3^{-1} \,(\mathrm{mod}\ N)$, which shows that (25) holds with $\gamma = \gamma_3\gamma_2\gamma_1$.

In view of Proposition 36, it is of interest to determine the subgroup $S_m(t, \delta)$ in $R_m^\times$. Nobs[No] computed $S_m(t, d)$ for prime powers $m = p^r$ and listed the result in Tabelle 1 of [No]. Using this, we see easily:

Proposition 38 *Let $\tau, \delta \in \mathbb{Z}$ and $N \geq 1$ be integers and put $\Delta_N = \Delta_N(\tau,\delta) := \gcd(\tau^2 - 4\delta, N)$. Then*

$$i_N(\tau,\delta) := [R_N^\times : S_N(\tau,\delta)] \ \leq \ 2^{\omega(\Delta_N)}, \tag{26}$$

except when $8|\Delta_N$, in which case $i_N(t,d) \leq 2^{\omega(\Delta_N)+1}$. Moreover, if $4 \nmid \Delta_N$ and if $\omega'(\Delta_N) := |\{p|\Delta_N : p \text{ is an odd prime}\}|$, then

$$i_N(\tau,\delta) \ = \ 2^{\omega'(\Delta_N)}. \tag{27}$$

Proof. If $N = p_1^{e_1} \cdots p_r^{e_r}$, where the p_i's are distinct primes, then by using the Chinese Remainder Theorem we see that

$$i_N(\tau,\delta) \ = \ \prod_{k=1}^{r} i_{p_k^{e_k}}(\tau,\delta). \tag{28}$$

From Tabelle 1 of Nobs[No] it follows that if $p_k \nmid \Delta_N$, then $i_{p_k^{e_k}}(\tau,\delta) = 1$, and that if $p_k|\Delta_N$, then

$$S_{p_k^{e_k}}(\tau,\delta) \ = \ (R^\times_{p_k^{e_k}})^2 \quad \text{and} \quad i_{p_k^{e_k}}(\tau,\delta) = 2, \quad \text{provided that } p_k \neq 2. \tag{29}$$

Moreover, by Nobs[No], loc. cit., we also have that $i_2(\tau,\delta) = 1$, that $i_4(\tau,\delta)|2$ and that $i_{2^e}(\tau,\delta)|4$, if $e \geq 3$, and so the assertions follow.

If $4|\Delta_N(\tau,\delta)$, then the exact formula for $i_N(\tau,\delta)$ is much more complicated. To write it in a convenient form, we first introduce the the following notation.

Notation. If $a \in \mathbb{Z}$, put

$$w_4(a) \ = \ \begin{cases} 1 & \text{if } a \equiv 1,2 \,(\text{mod } 4) \\ 2 & \text{if } a \equiv 0,3 \,(\text{mod } 4) \end{cases} \quad \text{and} \quad w_8(a) \ = \ \begin{cases} 1 & \text{if } a \equiv 1,5 \,(\text{mod } 8) \\ 2 & \text{if } a \equiv 2,3,4,6,7 \,(\text{mod } 8) \\ 4 & \text{if } a \equiv 0 \,(\text{mod } 8) \end{cases}$$

From the table in Nobs[No] and (28) we deduce:

Proposition 39 *Let $\tau, \delta \in \mathbb{Z}$ and suppose that $4|\Delta_N = \Delta_N(\tau,\delta)$, so $\tilde{\Delta} := \Delta/4 \in \mathbb{Z}$, where $\Delta = \tau^2 - 4\delta$. Then:*

$$i_N(\tau,\delta) \ = \ \begin{cases} 2^{\omega'(\Delta_N)} w_4(\tilde{\Delta}) & \text{if } 4||N, \\ 2^{\omega'(\Delta_N)} w_8(\tilde{\Delta}) & \text{if } 8|N, \end{cases} \tag{30}$$

7 The number of components of $H(q)$

We now apply the above results on conjugacy classes to refine Theorem 7 as follows.

Theorem 40 *Let q be a binary form of type (N, m, d), and put $g = \frac{N}{m}$. Then there exists a primitive matrix $\alpha \in \mathcal{M}_d$ such that $q \sim q_\alpha^N$. Fix such a matrix α, and let $z_1, \dots, z_s$ be integers such that their residues mod m is a system of representatives of $R_m^\times / S_m(\tau, \delta)$, where $\tau = \tau_{\beta\alpha,N}$ and $\delta = \delta_{\beta\alpha,N}$ are as in (20), and let $z_i' \in \mathbb{Z}$ be such that $z_i z_i' \equiv 1 \,(\mathrm{mod}\ m)$, for $1 \le i \le s$. Then there exist primitive matrices $\alpha_1, \dots, \alpha_s \in \mathcal{M}_d$ such that*

$$\beta\alpha_i \ \equiv\ \bar{x} I + g \left(\begin{smallmatrix} 0 & -\delta z_i' \\ z_i & \tau \end{smallmatrix} \right) \ (\mathrm{mod}\ N), \quad \textit{for } 1 \le i \le s,$$

where $\bar{x} = \bar{x}_{\beta\alpha,N}$. Moreover, if $\mathrm{char}(K) \nmid Nd$, then

$$H(q) \ =\ \bigcup_{i=1}^{s} \overline{T}_{\alpha_i}^N. \tag{31}$$

In particular, the number of irreducible components of $H(q)$ satisfies the estimate

$$|\mathrm{Irr}(H(q))| \ \le\ i_m(\tau, \delta) \ =\ [R_m^\times : S_m(\tau, \delta)]. \tag{32}$$

The key result for proving this is the following variant of Theorem 31 of [K5].

Proposition 41 *Suppose that $\mathrm{char}(K) \nmid N$ and that $\langle J, \lambda \rangle \in H(q_\alpha^N)$, where $\alpha \in \mathcal{M}_d$. Then there exists 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 if $\alpha' \in \mathcal{M}_d$ satisfies the relation*

$$(\psi^{-1} h)_{|E[N]} \ =\ \phi \circ [\beta\alpha']_N \circ \phi^{-1}, \tag{33}$$

for some level N-structure ϕ of E/K, then $g_{\beta\alpha',N} = g_{\beta\alpha,N}$ and $\bar{x}_{\beta\alpha',N} = \bar{x}_{\beta\alpha,N}$, and

$$\mathrm{tr}(\beta\alpha') \ \equiv\ \mathrm{tr}(\beta\alpha) \ (\mathrm{mod}\ Ng), \tag{34}$$

where $g = g_{\beta\alpha,N}$. Thus, if $m = \frac{N}{g}$, then

$$\tau_{\beta\alpha',N} \ \equiv\ \tau_{\beta\alpha,N} \ (\mathrm{mod}\ m) \quad \textit{and} \quad \delta_{\beta\alpha',N} \ \equiv\ \beta_{\beta\alpha,N} \ (\mathrm{mod}\ m). \tag{35}$$

In order to deduce this from the results of [K5], we need to recall some basic results which were (implicitly) proven there.

Lemma 42 *Let N and d be positive integers and let $\alpha \in \mathcal{M}_d$. If $g = g_{\beta\alpha,N}$, then there exists $k \in \mathbb{Z}$ such that $k\bar{x}_{\beta\alpha,N} \equiv 1 \,(\mathrm{mod}\ N)$, and for any such k we have that*

$$r_{\beta\alpha,k,N} := -(\mathrm{tr}(\beta\alpha) + kd(k^2 d + 3))/g^2 \in \mathbb{Z}. \tag{36}$$

Proof. Since $\beta\alpha = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$ is primitive, and $\bar{x} := \bar{x}_{\beta\alpha,N} \equiv x \pmod{g}$, we see that $\gcd(\bar{x}, g) = \gcd(x, g) = \gcd(x, y, z, w, N) = 1$, and so there exists a $k \in \mathbb{Z}$ such that $k\bar{x} \equiv 1 \pmod{g}$. This proves the first assertion.

We observe that $M = \beta\alpha$ and k satisfy the hypotheses of Proposition 11 of [K5], so if $r \in \mathbb{Z}$ is defined by equation (9) of [K5], then $q_{\beta\alpha,N,d,k} = q_{N,m,d,k,r}$ by [K5], equation (7). This means that $-2m\mathrm{tr}(\beta\alpha) = 2mT = 2m(kd(k^2d + 3) + rg^2)$, so $r_{\beta\alpha,,k,N} = r \in \mathbb{Z}$.

For the next result, recall from Lemma 21 of [K5] that if E/K and E'/K are elliptic curves, then every $D \in \mathrm{NS}(E \times E')$ has the unique representation $D = \mathbf{D}(a, b, h)$, where $a, b \in \mathbb{Z}$ and $h \in \mathrm{Hom}(E, E')$.

Proposition 43 *Let (E, E', ψ, π) be an N-presentation of $\langle J, \lambda\rangle \in \mathcal{A}_2(K)$, and let $h \in \mathrm{Hom}(E, E')$ be a cyclic isogeny of degree $d \geq 1$. Assume that $\mathrm{char}(K) \nmid N$. Then there exists $\alpha \in \mathcal{M}_d$ such that*

$$(\psi^{-1}h)_{|E[N]} \;=\; \phi \circ [\beta\alpha]_N \circ \phi^{-1}, \tag{37}$$

holds for some level N-structure ϕ of E. Fix k such that $k\bar{x}_{\beta\alpha,N} \equiv 1 \pmod{g}$, where $g = g_{\beta\alpha,N}$, and put $D_1 = \mathbf{D}(g^2, 0, 0)$ and $D_2 = \mathbf{D}(kd(k^2d + 2), -kd, h)$. Then

$$m(rD_1 + D_2) \;\in\; \pi^* NS(J), \tag{38}$$

where $m = \frac{n}{g}$ and $r = r_{\beta\alpha,k,N}$. Moreover, $r \pmod{m}$ is uniquely determined by (38).

Proof. Fix a level N-structure ϕ. As in the proof of Proposition 28 of [K5], we see that $\phi^{-1} \circ \psi^{-1} \circ h_{|E[N]} \circ \phi \in \mathrm{End}(E[N])$ is N-primitive and has determinant $\equiv -d \pmod{N}$, so by Remark 29 of [K5] there exists $\alpha \in \mathcal{M}_d$ such that (37) holds. Note that by Lemma 42 there exists a k such that $k\bar{x}_{\beta\alpha,N} \equiv 1 \pmod{g}$.

By [K5], Propositions 28 and 25(c), we know that (38) holds for some $r \in \mathbb{Z}$ which is uniquely determined mod m by (38). Moreover, by equations (35), (42) and (9) of [K5] we have that $r \equiv r_{\beta\alpha,b,N} \pmod{m}$, and so the assertions follow.

Proof of Proposition 41. Put $g = g_{\beta\alpha,N}$ and $m = \frac{N}{g}$. Fix $k \in \mathbb{Z}$ such that $k\bar{x}_{\beta\alpha,N} \equiv 1 \pmod{N}$ and put $r := r_{\beta\alpha,k,N}$ as in Lemma 42. Since $q^N_{-\alpha} = q_{\beta\alpha,N,d,k}$ in the notation of Proposition 11 of [K5], we have by equation (7) of [K5] that $q^N_{-\alpha} = q_{N,n,d,k,r}$. Thus $q^N_\alpha \sim q^N_{-\alpha} = q_{N,n,d,k,r}$.

Since $\langle J, \lambda\rangle \in H(q^N_\alpha)$, we are thus in the situation of Theorem 31 of [K5], and so we obtain an N-presentation (E, E', ψ, π) of (J, λ) and a cyclic isogeny $h : E \to E'$ of degree d such that if $D_1 = \mathbf{D}(g^2, 0, 0)$ and $D_2 = \mathbf{D}(kd(k^2d + 2), -kd, h)$, then (38) holds; cf. equation (44) of [K5].

Moreover, by Theorem 31(a) and Proposition 28 of [K5] we then have that $g_{\beta\alpha',N} = g$ and that $kx' \equiv 1 \pmod{g}$, where $\beta\alpha' = \left(\begin{smallmatrix} x' & y' \\ z' & w' \end{smallmatrix}\right)$, so $\bar{x}_{\beta\alpha,N} = \bar{x}_{\beta\alpha',N}$ because they are

uniquely determined by k and g. Furthermore, both r and $r_{\beta\alpha',k,N}$ satisfy (38), so by the uniqueness assertion of Proposition 43 we see that

$$r \;=\; r_{\beta\alpha,k,N} \;\equiv\; r_{\beta\alpha',k,N} \,(\mathrm{mod}\ m).$$

Thus $g^2 r_{\beta,k,N} \equiv g^2 r_{\beta\alpha',k,N} \,(\mathrm{mod}\ Ng)$, and so (34) follows. In view of Lemma 44 below, this implies that (35) also holds.

Lemma 44 *Let $\alpha_1, \alpha_2 \in M_2(\mathbb{Z})$ be two integral matrices and let $N \geq 1$ be an integer. Suppose that $g_{\alpha_1,N} = g_{\alpha_2,N}$ and that $\bar{x}_{\alpha_1,N} = \bar{x}_{\alpha_2,N}$. If*

$$\mathrm{tr}(\alpha_1) \equiv \mathrm{tr}(\alpha_2) \,(\mathrm{mod}\ Ng), \quad \textit{and} \quad \det(\alpha_1) \equiv \det(\alpha_2) \,(\mathrm{mod}\ Ng), \tag{39}$$

where $g = g_{\alpha_1,N}$, then for $m = \frac{N}{g}$ we have that

$$\tau_{\alpha_1,N} \;\equiv\; \tau_{\alpha_2,N} \,(\mathrm{mod}\ N) \quad \textit{and} \quad \delta_{\alpha_1,N} \;\equiv\; \delta_{\alpha_2,N} \,(\mathrm{mod}\ m). \tag{40}$$

Proof. Put $\bar{x} = \bar{x}_{\alpha_i,N}$, $\tau_i = \tau_{\alpha_i,N}$ and $\delta_i = \delta_{\alpha_i,N}$, for $i = 1, 2$. Then $g(\tau_1 - \tau_2) = \mathrm{tr}(\alpha_1) - \mathrm{tr}(\alpha_2) \equiv 0 \,(\mathrm{mod}\ Ng)$, so $\tau_1 \equiv \tau_2 \,(\mathrm{mod}\ N)$. Moreover, since $g^2(\delta_1 - \delta_2) = (\det(\alpha_1) - \det(\alpha_2)) - \bar{x}(\tau_1 - \tau_2)g \equiv 0 \,(\mathrm{mod}\ g^2 m)$, we see that $\delta_1 \equiv \delta_2 \,(\mathrm{mod}\ m)$.

Proof of Theorem 40. The existence of $\alpha \in \mathcal{M}_d$ with $q_\alpha^N \sim q$ follows from Theorem 16 of [K5]. Thus $g_{\beta\alpha,N} = g$ and $\gcd(\bar{x}_{\beta\alpha,N}, g) = 1$; cf. the proof of Lemma 42.

Put $\bar{\alpha}_i := \bar{x}I + g \left(\begin{smallmatrix} 0 & -\delta z_i' \\ z_i & \tau \end{smallmatrix}\right)$. Then $g_{\bar{\alpha}_i,N} = g$ because $\gcd(z_i, m) = 1$, and so $\bar{\alpha}_i$ is N-primitive because $\gcd(\bar{x}, g) = 1$.

We next observe that if $t := \mathrm{tr}(\alpha)$, then

$$\mathrm{tr}(\bar{\alpha}_i) = t \quad \text{and} \quad \det(\bar{\alpha}_i) \equiv -d \ (\mathrm{mod}\ Ng), \quad \text{for } 1 \leq i \leq s. \tag{41}$$

Indeed, $\mathrm{tr}(\bar{\alpha}_i) = 2\bar{x} + g\tau = t$, and $\det(\bar{\alpha}_i) = \bar{x}^2 + \bar{g}\tau + g^2\delta z_i z_i^* \equiv \bar{x}^2 + \bar{g}\tau + g^2\delta \,(\mathrm{mod}\ g^2 m)$, so $\det(\bar{\alpha}_i) \equiv -d \,(\mathrm{mod}\ g^2 m)$ by the definition of δ. This proves (41).

It follows from (41) that $\det(\bar{\alpha}_i) \equiv -d \,(\mathrm{mod}\ N)$, so by Lemma 30 of [K5] there exists a primitive matrix α_i' of determinant $-d$ such that $\alpha_i' \equiv \bar{\alpha}_i \,(\mathrm{mod}\ N)$. Put $\alpha_i := \beta\alpha_i'$. Then $\alpha_i \in \mathcal{M}_d$, and $\beta\alpha_i = \alpha_i' \equiv \bar{\alpha}_i \,(\mathrm{mod}\ N)$. This proves the existence of the matrices $\alpha_1, \ldots, \alpha_s$.

To prove (31), let $k \in \mathbb{Z}$ be such that $k\bar{x} \equiv 1 \,(\mathrm{mod}\ g)$, and put $t_i := -\mathrm{tr}(\alpha_i) - dk^3(\det(\bar{\alpha}_i) + d)$. Then by (41) we see that $t_i \equiv -t \,(\mathrm{mod}\ Ng)$, for $1 \leq i \leq s$. Thus, if we put $q_i = [N^2, 2mt_i, (t_i^2 + 4d)/g^2]$, then $q_i \sim q_{-\alpha}^N = [N^2, -2mt, (t^2 + 4d)/g^2]$; cf. [K5], Lemma 9. Since $q_i = q_{\bar{\alpha}_i,N,d,k}$ in the notation of Proposition 11 of [K5], and since by construction $\beta\alpha_i \equiv \bar{\alpha}_i \,(\mathrm{mod}\ N)$, it follows from Proposition 14 of [K5] that $q_{-\alpha_i}^N \sim q_{-\alpha}^N$, for $1 \leq i \leq s$. Thus $q_{\alpha_i}^N \sim q$ because $q_{-\alpha}^N \sim q_\alpha^N \sim q$, and so it follows from Theorem 7 that $\overline{T}_{\alpha_i}^N \subset H(q)$. This proves that the right hand side of (31) is contained in $H(q)$.

To prove the opposite inclusion, let $\langle J,\lambda\rangle \in H(q) = H(q_\alpha^N)$. Then by Proposition 41 (and by Proposition 43) there exists an N-presentation (E,E',ψ,π) of (J,λ), a cyclic isogeny $h : E \to E'$ of degree d and a matrix $\alpha' \in \mathcal{M}_d$ such that (33) holds for some level N-structure ϕ of E/K. Then $\phi' := \psi\circ\phi\circ[\beta]_N$ is a level N-structure on E'/K and (33) shows that (ϕ,h,ϕ') is α'-compatible in the sense of (12), and so $x := \langle E,\phi,E',\phi',h\rangle \in \mathcal{X}_{\alpha'}^N(K)$. Since $\langle J,\lambda\rangle = \langle A_\psi,\lambda_\psi\rangle$ because (E,E',ψ,π) is an N-presentation of (J,λ) and since $\psi_{\phi,\phi'} = \psi$, it follows from Corollary 20 that

$$\langle J,\lambda\rangle \;=\; \beta_{\alpha'}^N(x) \;\in\; \beta_{\alpha'}^N(X_{\alpha'}^N) \;=\; \overline{T}_{\alpha'}^N. \tag{42}$$

By the second part of Proposition 41 we know that $\beta\alpha'$ has the same invariants g, $\bar{x}$, τ, δ as $\beta\alpha$. Thus, by Proposition 35 there exists $z \in R_m^\times$ and $\gamma_1 \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma_1\beta\alpha'\gamma_1^{-1} \equiv \alpha'' := \bar{x}I + g\left(\begin{smallmatrix} 0 & -\delta z' \\ z & \tau\end{smallmatrix}\right) \pmod N$, where $z'z \equiv 1 \pmod m$. Then $z \equiv z_k\sigma \pmod m$, for some k with $1 \le k \le s$ and $\sigma \in S_m(\tau,\delta)$ by our hypothesis on the z_i's. Then by Lemma 33 and Proposition 36 there exists $\gamma_2 \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma_2\alpha''\gamma_2^{-1} \equiv \bar{\alpha}_k \equiv \beta\alpha_k \pmod N$, so if we put $\gamma = \gamma_2\gamma_1$, then $\gamma\beta\alpha'\gamma^{-1} \equiv \beta\alpha_k \pmod N$. Then by (4) we see that $\overline{T}_{\alpha'}^N = \overline{T}_{\alpha_k}^N$, and so $\langle J,\lambda\rangle \in \overline{T}_{\alpha_k}^N$ by (42). This shows that opposite inclusion of (31) holds, and so concludes the proof of (31). From this (32) follows immediately since the $\overline{T}_{\alpha_i}^N$'s are irreducible (but not necessarily distinct) components of $H(q)$; cf. Remark 21.

Theorem 40 provides us with an upper bound for the number of irreducible components of $H(q)$; cf. (32). To go further and to compute the number of components *precisely* in the situation of Theorem 4(b) (or of Theorem 28) requires further work.

Indeed, although the previous section analyzed the SL_2-conjugacy classes of matrices mod N, the conditions (4) and (18) involve SL_2-conjugacy classes up to to sign. Now in many cases this does not make a difference, but it does in some cases, which leads to certain exceptional forms. More precisely, we have:

Proposition 45 *Let q be binary form of type (N,m,d) which satisfies the condition* (17) *of* Theorem 28*, and let τ,δ be as in* Theorem 40*. If $\mathrm{char}(K) \nmid Nd$, then the number of irreducible components of $H(q)$ is given by the formula*

$$|\mathrm{Irr}(H(q))| \;=\; i_m(\tau,\delta) \;=\; [R_m^\times : S_m(\tau,\delta)], \tag{43}$$

except when $-1 \notin S_m(\tau,\delta)$ and q is equivalent to one of the following forms:

$$[N^2,0,4d], \quad [N^2,N^2,(N^2+16d)/4], \quad [N^2,\varepsilon N^2,(\varepsilon^2N^2+4d)/4], \tag{44}$$

where $2|N$, $\varepsilon \in \{0,1\}$ and $d \equiv 1+\varepsilon N \pmod 4$ in the last case. For the exceptional cases we have

$$|\mathrm{Irr}(H(q))| \;=\; i_m(t,\delta)/2. \tag{45}$$

Proof. Suppose that the $\overline{T}^N_{\alpha_i}$ constructed in Theorem 40 are not all distinct. Then there exists i and j with $1 \le i < j \le s$ such that $\overline{T}^N_{\alpha_i} = \overline{T}^N_{\alpha_j}$, so by Theorem 18 we have that $\gamma\beta\alpha_i\gamma^{-1} \equiv \pm\beta\alpha_j \pmod N$, for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. We thus have that

$$\gamma\beta\alpha_i\gamma^{-1} \equiv -\beta\alpha_j \pmod N, \tag{46}$$

because the other case is ruled out by our choice of the α_k's; cf. Proposition 36. Thus, since $\beta\alpha_k$ has the invariants $\bar{x}$, $\tau \pmod m$ and $\delta \pmod m$, for all k, it follows from (46) and Proposition 34 that we have $\bar{x}_{-\beta\alpha_j,N} = \bar{x}$, $\tau_{-\beta\alpha_j} \equiv \tau \pmod m$ and $\delta_{-\beta\alpha_j} \equiv \delta \pmod m$. Moreover, if these conditions hold, then

$$-\beta\alpha_j \equiv -\bar{x}I + g\begin{pmatrix} 0 & -\delta(-z_j) \\ -z_j & -\tau \end{pmatrix} \equiv \bar{x}I + g\begin{pmatrix} * & \delta z_j \\ -z_j & * \end{pmatrix} \pmod N,$$

so by (46) and Proposition 36 we see that the residues of z_i and $-z_j \bmod m$ lie in the same $S_m(\tau,\delta)$-coset of $R_m^\times$. But this is only possible if $-1 \notin S_m(\tau,\delta)$.

We now analyze the above conditions on $\bar{x}$, etc. Since $\bar{x} = \bar{x}_{\beta\alpha_i} = \bar{x}_{-\beta\alpha_j,N} \equiv -\bar{x} \pmod g$, we see that $2\bar{x} \equiv 0 \pmod g$. But since $\gcd(\bar{x}, g) = 1$, this implies that $2 \equiv 0 \pmod g$, which is only possible if $g = 1$ or $g = 2$.

Case 1: $g = 1$.

Here $m = N$ and $\bar{x} = 0$, so it follows that $\mathrm{tr}(\beta\alpha_k) = \tau_{\beta\alpha_k,N} \equiv \tau \pmod N$, for all k. But then $\tau \equiv \mathrm{tr}(\beta\alpha_i) \equiv -\mathrm{tr}(\beta\alpha_j) \equiv -\tau \pmod N$, so $2\tau \equiv 0 \pmod N$. Thus, either $\tau \equiv 0 \pmod N$ or $2|N$ and $\tau \equiv \frac{N}{2} \pmod N$. But since $\tau = \mathrm{tr}(\beta\alpha)$, this implies that $q \sim q^N_\alpha \sim [N^2, 0, 4d]$ or $2|N$ and $q \sim [N^2, N^2, (N/2)^2 + 4d]$; cf. [K5], Lemma 9. This gives us the first two cases of (44).

Case 2: $g = 2$.

Here $m = \frac{N}{2}$ and $\bar{x} = 1$, so $\bar{\alpha}_k = I + 2\left(\begin{smallmatrix} 0 & -\delta z'_k \\ z_k & \tau \end{smallmatrix}\right)$, for all k, where $\bar{\alpha}_k$ is as in the proof of Theorem 40. (Thus, $\beta\alpha_k \equiv \bar{\alpha}_k \pmod N$, for all k.) We have $\bar{x}_{-\bar{\alpha}_j,N} = \bar{x} = 1$, so $2\tau_{-\bar{\alpha}_j,N} = \mathrm{tr}(-\bar{\alpha}_j) - 2 = -\mathrm{tr}(\bar{\alpha}_j) - 2 = -(2\tau+2) - 2 = -2\tau - 4$, i.e., $\tau_{-\bar{\alpha}_j,N} = -(\tau+2)$. Thus $4\delta_{-\bar{\alpha}_j,N} = \det(-\bar{\alpha}_j) - 1^2 - 2(-\tau-2) = \det(\bar{\alpha}_j) - 1^2 - 2\tau + 4\tau + 4 = 4\delta_{\bar{\alpha}_j} + 4\tau + 4$, and hence $\delta_{-\bar{\alpha}_j,N} = \delta_{\bar{\alpha}_j,N} + \tau + 1 \equiv \delta + \tau + 1 \pmod m$. Since $\delta_{\beta\alpha_k,N} \equiv \delta \pmod m$, for all k, it follows from (46) and Proposition 34 that

$$\delta \equiv \delta_{\beta\alpha_i,N} \equiv \delta_{-\delta\alpha_j,N} \equiv \delta + \tau + 1 \pmod m,$$

so $\tau \equiv -1 \mod m$, and hence $t := \mathrm{tr}(\beta\alpha) = 2\tau + 2 \equiv 0 \pmod{2m}$. Since $2m = N$, we thus see that $t \equiv \varepsilon N \pmod{2N}$, where $\varepsilon \in \{0, 1\}$, and so $q^N_\alpha = [N^2, Nt, (t^2+4d)/4] \sim q' := [N^2, \varepsilon N^2, (\varepsilon^2 N^2 + 4d)/4]$; cf. [K5], Lemma 9. Moreover, since $-d + 1^2 - 1 \cdot t = 4\delta$, we see that $d \equiv 1 - t \equiv 1 - \varepsilon N \equiv 1 + \varepsilon N \pmod 4$ because $2|N$. We thus obtain the last case of (44).

Now suppose that we are in the exceptional cases. Then $-1 \notin S_m(\tau,\delta)$, so $2|s = i_m(\tau,\delta)$. Choose $z_1, \ldots, z_{\frac{s}{2}}$ in such a way that their residues mod m are a system of

representatives of $R_m^\times/\langle -1, S_m(\tau,\delta)\rangle$ and put $z_k = -z_{k-\frac{s}{2}}$ for $k = \frac{s}{2}+1, \ldots, s$. Then $z_1, \ldots, z_s$ satisfy the conditions of Theorem 40. Moreover, since $\bar{x}$, g, τ and δ satisfy the above conditions, we see that $\beta\alpha_k \equiv -\beta\alpha_{k+\frac{s}{2}} \pmod N$, for $1 \le k \le \frac{s}{2}$. Thus, $\overline{T}^N_{\alpha_k} = \overline{T}^N_{\alpha_{k+\frac{s}{2}}}$, for these k's. On the other hand, by construction (and by Proposition 36) we have that $\gamma\beta\alpha_i\gamma^{-1} \not\equiv \pm\beta\alpha_j$, for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and $1 \le i < j \le \frac{s}{2}$, so by Theorem 28 it follows that $\overline{T}^N_{\alpha_i} \ne \overline{T}^N_{\alpha_j}$, for $1 \le i < j \le \frac{s}{2}$, and so (45) follows.

Remark 46 As the above proof shows, even if the hypothesis (17) does not hold for q, but if $-1 \notin S_m(\tau,\delta)$ and q is equivalent to one of the forms of (44), then we still have the estimate

$$|\mathrm{Irr}(H(q))| \;\le\; i_m(\tau,\delta)/2. \tag{47}$$

To analyze the above results further, we first make the following observations.

Lemma 47 *If q has type (N,m,d) and if α, τ, and δ are as* Theorem 40, *then $q^N_\alpha = [N^2, 2mt, \Delta]$, where $t = \mathrm{tr}(\beta\alpha)$ and $\Delta = \Delta(\tau,\delta) = \tau^2 - 4\delta$. Thus, if $\mathrm{cont}(q) = \gcd(a,b,c)$ denotes the content of $q = [a,b,c]$, then we have*

$$\Delta_m(\tau,\delta) \;:=\; \gcd(\Delta, m) \;=\; \gcd(\mathrm{cont}(q), m) \;=:\; c_m(q).$$

Proof. By definition, $q^N_\alpha = [N^2, 2mt, (t^2+4d)/g^2]$, so the first assertion follows from (21) because $\det(\beta\alpha) = -d$. Thus $\gcd(m, \mathrm{cont}(q^N_\alpha)) = \gcd(m, N, 2mt, \Delta) = \gcd(m, \Delta)$. Since $q \sim q^N_\alpha$, we have that $\mathrm{cont}(q) = \mathrm{cont}(q^N_\alpha)$, and so the assertion follows.

Lemma 48 *Let $\tau, \delta \in \mathbb{Z}$ and let $m \ge 1$. If $4 \nmid \Delta_m(\tau,\delta)$, then $-1 \notin S_m(\tau,\delta)$ if and only if there exist a prime $p \equiv 3 \pmod 4$ with $p | \Delta_m(\tau,\delta)$.*

Proof. Write $m = \prod_{i=1}^r p_i^{e_i}$, where the p_i's are distinct primes. Then the Chinese Remainder Theorem induces an isomorphism

$$S_m(\tau,\delta) \;\simeq\; \prod_{i=1}^r S_{p_i^{e_i}}(\tau,\delta), \tag{48}$$

so $-1 \in S_m(\tau,\delta) \Leftrightarrow -1 \in S_{p_i^{e_i}}(\tau,\delta)$, for $1 \le i \le r$. Since $-1 \in S_2(\tau,\delta) = R_2^\times = \{1\}$ and since for an odd prime p we have by (29) that $-1 \notin S_{p^e}(\tau,\delta) \Leftrightarrow p | \Delta_{p^e}(\tau,\delta)$ and $(\frac{-1}{p}) = -1 \Leftrightarrow p | \Delta_{p^e}(\tau,\delta)$ and $p \equiv 3 \pmod 4$, we see that the assertion follows.

We are now ready to prove the following refinement of Theorem 4.

Theorem 49 *Let q be a binary form of type (N, m, d) and assume that $4 \nmid c_m = \gcd(\mathrm{cont}(q), m)$ and that $\mathrm{char}(K) \nmid Nd$. Let $\omega' = \omega'(c_m) = |\{p | c_m : p \text{ is an odd prime}\}|$.*

(a) *We always have that $|\mathrm{Irr}(H(q))| \leq 2^{\omega'}$.*

(b) *If there exists a prime $p | \gcd(N, d)$ with $p \equiv 3 \pmod 4$ and if q is equivalent to one of the forms of (44), then then $|\mathrm{Irr}(H(q))| \leq 2^{\omega'-1}$.*

(c) *Suppose that q satisfies condition (17). If q satisfies the conditions of part (b), then equality holds in part (b), otherwise equality holds in part (a).*

Proof. By Lemma 47 we have that $c_m = \Delta_m(\tau, \delta)$, where τ and δ are as in Theorem 40, and so by (27) we have that $i_m(\tau, \delta) = 2^{\omega'}$ since $4 \nmid c_m$. Thus, part (a) follows from (32). Moreover, in the situation of part (b) we have that $-1 \notin S_m(\tau, \delta)$ by Lemma 48 and the fact that $p | c_m \Leftrightarrow p | \gcd(N, d)$ for the forms of (44), so part (b) follows from Remark 46. Finally, part (c) follows from Proposition 45.

Corollary 50 *If q is a binary form of type (N, m, d) with $c_m(q) \mid 2$, then $H(q)$ is irreducible, provided that $\mathrm{char}(K) \nmid Nd$.*

Proof. Since $4 \nmid c_m = c_m(q)$ and $\omega'(c_m) = 0$, it follows from Theorem 49(a) that $|\mathrm{Irr}(H(q)| \leq 2^0 = 1$, so $H(q)$ is irreducible.

We observe that the above corollary implies the following result for the case $N = 2$.

Proposition 51 *If q has type $(2, m, d)$, and if $\mathrm{char}(K) \nmid 2d$, then $H(q)$ is irreducible. Moreover, $H(q)$ is uniquely determined by d if $m = 1$, whereas there are precisely two distinct $H(q)$'s for each d when $m = 2$.*

Proof. Since $c_m(q) | m | N = 2$, it follows from Corollary 50 that $H(q)$ is irreducible.

If $m = 1$, then $\gcd(d, 2/1) = 1$, so $d \equiv 1 \pmod 2$. Thus, it follows from [K5], Proposition 19, that $q \sim [4, 0, d]$, if $d \equiv 1 \pmod 4$, whereas $q \sim [4, 4, d + 1]$, if $d \equiv 3 \pmod 4$. Thus $H(q)$ is uniquely determined by d in this case.

If $m = 2$, then by [K5], loc. cit., we know that either $q \sim q_1 := [4, 0, 4d]$ or $q \sim q_2 := [4, 4, 4d + 1]$. Since q_1 and q_2 are distinct reduced forms, it follows that $q_1 \not\sim q_2$, and hence $H(q_1) \neq H(q_2)$ by Corollary 26.

If $4 | c_m$, then the situation is much more complicated because the formula for $i_m(\tau, \delta)$ is more involved since it does not depend on $\gcd(m, \tau^2 - 4\delta)$ alone, but involves the quantities $w_4(\tilde{\Delta})$ and $w_8(\tilde{\Delta})$, as we saw in Proposition 39. For this reason we introduce the following value $w(q)$ for (special) binary quadratic forms q.

Notation. Let $q = [N^2, 2mt, c]$ be a binary form of type (N, m, d) and suppose that $4 | c_m(q) = \gcd(m, \mathrm{cont}(q)) = \gcd(m, c)$. Put

$$w(q) = \begin{cases} w_4\left(\frac{c}{4}\right) & \text{if } 4 || m, \\ w_8\left(\frac{c}{4}\right) & \text{if } 8 | m \end{cases} \tag{49}$$

We then have the following connection between $w(q)$ and $i_m(\tau,\delta)$.

Lemma 52 *Let $\alpha \in \mathcal{M}_d$ and $N \geq 1$ and put $g = g_{\beta\alpha,N}$, $m = \frac{N}{g}$, $\tau = \tau_{\beta\alpha,N}$, and $\delta = \delta_{\beta\alpha,N}$. Moreover, let q_α^N be the quadratic form associated to α. If $4|c_m = \gcd(m, \mathrm{cont}(q_\alpha^N)) = \gcd(m, \tau^2 - 4\delta)$, then*

$$i_m(\tau,\delta) \;=\; 2^{\omega'(c_m)} w(q_\alpha^N). \tag{50}$$

Proof. By definition and (21) we have $q_\alpha^N = [N^2, 2mt, \Delta]$, where $t = \mathrm{tr}(\beta\alpha)$ and $\Delta = \tau^2 - 4\delta$, and so $c_m = \gcd(m, \mathrm{cont}(q_\alpha^N)) = \gcd(m, \Delta)$. Thus, if $4|c_m$, then $w(q_\alpha^N) = w_4(\Delta/4)$, when $4||m$, and $w(q_\alpha^N) = w_8(\Delta/4)$ otherwise, and so (50) is just a restatement of formula (30).

It is useful to observe that the value of $w(q)$ only depends on the equivalence class of q and not on the particular form q of the form $[N^2, 2mt, c]$. Thus, we can extend the symbol $w(q)$ to any form q of type (N, m, d) by setting $w(q) = w([N^2, 2mt, c])$, if $q \sim [N^2, 2mt, c]$. This is justified by the following result.

Lemma 53 *Let $q_i := [N^2, 2mt_i, c_i]$, where $i = 1, 2$, be two forms of type (N, m, d). Suppose that $q_1 \sim q_2$ and that $4|c_m(q_i)$. Then*

$$\frac{c_1}{4} \;\equiv\; \frac{c_2}{4} \pmod{2^r}, \tag{51}$$

where $r = \min(3, v_2(m))$. In particular, we have that $w(q_1) = w(q_2)$,

Proof. Since $4|c_m(q_i) = \gcd(m, c_i)$ we see that $4|m$ and hence $4m|m^2|N^2$. Moreover, we have that $2|t_i$ because $t_i^2 + 4d = c_i g^2 \equiv 0 \pmod 4$. By hypothesis, there exists $\gamma = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$ such that $\gamma^t M(q_1)\gamma = M(q_2)$, where $M(q_i) = \left(\begin{smallmatrix} N^2 & mt_i \\ mt_i & c_i \end{smallmatrix}\right)$, for $i = 1, 2$. Thus

$$\begin{pmatrix} N^2 & mt_2 \\ mt_2 & c_2 \end{pmatrix} = \begin{pmatrix} N^2x^2 + 2mt_1xz + c_1z^2 & N^2xy + mt_1(wx + yz) + c_1wz \\ N^2xy + mt_1(wx + yz) + c_1wz & N^2y^2 + 2mt_1wy + c_1w^2 \end{pmatrix}$$

Since $N^2 \equiv 0 \pmod{4m}$ and $2t_1 \equiv 0 \pmod 4$, it follows by comparing the $(1,1)$-entries and the $(2,2)$-entries of this matrix identity that

$$c_1z^2 \equiv 0 \pmod{4m} \quad \text{and} \quad c_1w^2 \equiv c_2 \pmod{4m}. \tag{52}$$

Suppose first that $2 \nmid w$, so $w^2 \equiv 1 \pmod 8$. Since $\frac{c_1}{4}w^2 \equiv \frac{c_2}{4} \pmod m$ by (52), it follows that $\frac{c_1}{4} \equiv \frac{c_1}{4}w^2 \equiv \frac{c_2}{4} \pmod{2^r}$. Thus, (51) holds in this case.

Now suppose that $2|w$. Then $2 \nmid z$ because $\gcd(z, w) = 1$, so by the first equation of (52) we obtain that $c_1 \equiv c_1z^2 \equiv 0 \pmod{2^{s+2}}$, where $s = v_2(m)$. Thus $\frac{c_1}{4} \equiv 0 \pmod{2^s}$, so by the second equation of (52) we obtain that $\frac{c_2}{4} \equiv \frac{c_1}{4}w^2 \equiv 0 \pmod{2^s}$. This implies that $\frac{c_1}{4} \equiv \frac{c_2}{4} \equiv 0 \pmod{2^r}$, so (51) holds in all cases.

To prove the last assertion, suppose first that $4||m$, so $r = 2$. Since the value of $w_4(c_i/4)$ only depends on the residue class of $c_i/4$ mod 4, we have $w_4(c_1/4) = w_4(c_2/4)$ by (51) and so $w(q_1) = w(q_2)$. If $8|m$, then $r = 3$, so $w_8(c_1/4) = w_8(c_2/4)$ and $w(q_1) = w(q_2)$.

We also require the following result from Nobs[No].

Lemma 54 *Suppose that* $4|\gcd(m, \Delta)$*, where* $\Delta = \tau^2 - 4\delta$*, and put* $\tilde{\Delta} = \frac{\Delta}{4}$*.*

(a) *If* $4||m$*, then* $-1 \notin S_4(\tau, \delta)$ *if and only if* $\tilde{\Delta} \not\equiv 1, 2 \pmod 4$*.*

(b) *If* $8|2^r||m$*, then* $-1 \notin S_{2^r}(\tau, \delta)$ *if and only if* $\tilde{\Delta} \not\equiv 1, 2, 5 \pmod 8$*.*

Proof. This follows immediately from Tabelle 1 of Nobs[No].

We are now ready to study the number of irreducible components of $H(q)$ in the case that $4|c_m(q)$. Here we have:

Theorem 55 *Let* q *be a binary form of type* (N, m, d) *and assume that* $4|c_m$ *and that* $\mathrm{char}(K) \nmid Nd$*.*

(a) *We always have that* $|\mathrm{Irr}(H(q))| \le 2^{\omega'(c_m)} w(q)$*.*

(b) *Suppose that* q *is equivalent to either* $[N^2, 0, 4d]$ *or to* $[N^2, N^2, \frac{N^2}{4} + 4d]$*, where* $4|N$*. Put* $\tilde{\Delta} = d$ *in the first case and* $\tilde{\Delta} = \frac{N^2}{16} + d$ *in the second case. If either* $\gcd(N, d) \equiv 0 \pmod p$ *for some prime* $p \equiv 3 \pmod 4$ *or if* $\tilde{\Delta} \not\equiv 1, 2 \pmod 4$ *when* $4||N$ *or if* $\tilde{\Delta} \not\equiv 1, 2, 5 \pmod 8$ *when* $8|N$*, then* $|\mathrm{Irr}(H(q))| \le 2^{\omega'(c_m)-1} w(q)$*.*

(c) *Suppose that* q *satisfies condition* (17)*. If* q *satisfies the conditions of part* (b)*, then equality holds in part* (b)*, otherwise equality holds in part* (a)*.*

Proof. (a) Let $\alpha \in \mathcal{M}_d$ be such that $q \sim q_\alpha^N$, and let τ, δ be as in Theorem 40. Then the assertion follows directly from (32) and Lemma 52.

(b) Suppose first $q \sim q_1 := [N^2, 0, 4d]$, so $\mathrm{disc}(q) = -16N^2 d$ and hence $m = N$. Note that $4|c_m = (N, 4d) \Leftrightarrow 4|N$. By Proposition 15 of [K5] we can choose $\alpha \in \mathcal{M}_d$ such that $q_\alpha^N = q_1$, and then $\tau^2 - 4\delta = 4d$ by (21). Thus by the proof of Lemma 48 we see that $-1 \notin S_N(\tau, \delta)$ if and only if either there exists $p \equiv 3 \pmod 4$ with $p|c_m = \gcd(N, 4d)$ or if $-1 \notin S_4(\tau, \delta)$, when $4||m = N$, or if $-1 \notin S_{2^r}(\tau, \delta)$, when $8|2^r||N$. By Lemma 54, the latter two possibilities are equivalent to $d = \tilde{\Delta} \not\equiv 1, 2 \pmod 4$, when $4||N$, and to $d = \tilde{\Delta} \not\equiv 1, 2, 5 \pmod 8$, when $8|N$. If this is the case, then the assertion (for $q \sim q_1$) follows from Remark 46 and Lemma 52.

Now suppose that $q \sim q_2 := [N^2, N^2, \frac{N^2}{4} + 4d]$. Here again $\mathrm{disc}(q) = -16N^2 d$, so $m = N$. Thus again $4|c_m = \gcd(N, \frac{N^2}{4} + 4d) \Leftrightarrow 4|N$, and so by a similar argument as in the case $q \sim q_1$ we see that the assertion holds for $q \sim q_2$ with $\tilde{\Delta} = \frac{N^2}{16} + d$.

(c) If q is as in part (b), then by the proof of part (b) we see that we are in the exceptional case of Proposition 45, and so by (45) and Lemma 50 we see that $\mathrm{Irr}(H(q)) = \frac{1}{2} i_m(\tau, \delta) = 2^{\omega'(c_m)-1} w(q)$.

Now assume that q is not as in part (b). We observe that the third case of (44) does not occur here because $4 \nmid c_m(q_3)$, where $q_3 := [N^2, \varepsilon N^2, \varepsilon^2 \frac{N^2}{4} + d]$ with $2|N$, $\varepsilon \in \{0,1\}$, and $d \equiv 1 + \varepsilon N \,(\mathrm{mod}\ 4)$. Indeed, since $\mathrm{disc}(q_3) = -4N^2 d$, we see that $m = \frac{N}{2}$, so $4 \nmid c_m = \gcd(\frac{N}{2}, d)$ because $d \equiv 1 \,(\mathrm{mod}\ 4)$ if $4|N$.

From this (and the proof of part (b)) it follows that q does not satisfy the conditions of the exceptional case of Proposition 45 and so by (43) and Lemma 50 it follows that $\mathrm{Irr}(H(q)) = i_m(\tau, \delta) = 2^{\omega'(c_m)} w(q)$.

Corollary 56 *If q has type $(4, m, d)$ and if $\mathrm{char}(K) \nmid 2d$, then $H(q)$ is irreducible.*

Proof. If $c_m \neq 4$, then the assertion follows from Corollary 50 because the condition $c_m \neq 4$ implies that $c_m|2$ (since $c_m|N = 4$). Thus, assume that $c_m = 4$, so we are in the situation of Theorem 55. Moreover, we have that $m = 4$ and $4|\mathrm{cont}(q)$.

Since $m = 4$, we have that $q \sim [4^2, 8t, t^2 + 4d]$ with $0 \leq t \leq \frac{4^2}{2 \cdot 4} = 2$, and since $4|\mathrm{cont}(q)$, we see that $2|t$. Thus, $q \sim [16, 0, 4d]$ or $q \sim [16, 16, 4 + 4d]$, which are precisely the two exceptional cases of Theorem 55(b) when $N = 4$. Put $\tilde{\Delta} = d$ in the first case and $\tilde{\Delta} = d + 1$ in the second case, so $w(q) = w_4(\tilde{\Delta})$ by (49).

If $\tilde{\Delta} \equiv 1, 2 \,(\mathrm{mod}\ 4)$, then $w(q) = w_4(\tilde{\Delta}) = 1$ by definition (cf. §6), and thus $|\mathrm{Irr}(H(q))| \leq 2^0 = 1$ by Theorem 55(a), so $H(q)$ is irreducible in this case.

If $\tilde{\Delta} \not\equiv 1, 2 \,(\mathrm{mod}\ 4)$, then $w(q) = w_4(\tilde{\Delta}) = 2$ by definition, and thus $|\mathrm{Irr}(H(q))| = \frac{1}{2} w(q) = 1$ by Theorem 55(b), so $H(q)$ is irreducible in this case as well. Thus, $H(q)$ is irreducible in all cases.

Proof of Theorem 4. The first assertion follows from Proposition 7 of [K5].

(a) This follows from Theorem 40 and (26). Alternately, if $4 \nmid c_m(q)$, then this follows from Theorem 49(a) and if $4||c_m(q)$, then this follows from Theorem 55(a) because $w(q)|2$ when $4||m$.

(b) From Lemma 29 we know that the given hypothesis on d implies that condition (17) of Theorem 28 holds for q. Since $c_m(q)|N$ and $2 \nmid N$, we are thus in the situation of Theorem 49(c), and hence the assertion follows from that theorem because the last two cases of (44) do not occur when $2 \nmid N$.

Proof of Corollaries 5 and 6. The first corollary is the special case $c_m(q) = 1$ of Theorem 4(a). (Alternately, it is a special case of Corollary 50.)

To prove Corollary 6, let $q \in Q(N^2)$. Then by Theorem 1 we know that q has type (N, m, d) for some $m|N$ and d, and so by Corollary 34 of [K5] there exists $(A, \lambda) \in A_2(K)$ such that $q_{(A,\lambda)} \sim q$. Since $(A, \lambda) \in H(q) \subset H_M$, this implies that $q \to M$ and $q \to N^2$. Thus, the content $\mathrm{cont}(q)$ of q divides N^2 and M, so $\mathrm{cont}(q) = 1$ (because $\gcd(N, M) = 1$), and hence also $c_m(q) = \gcd(\mathrm{cont}(q), m) = 1$. Thus $H(q)$ is irreducible by Corollary 5.

8 Examples

By using the above results (including Theorem 10, which is proved in [K7]), together with the reduction theory of binary quadratic forms, it is possible to work out explicitly the irreducible components of $H_{N^2} \cap H_M$ for small values of N and M. For example:

Proposition 57 (a) *The nontrivial intersections of H_1 with H_M for $M \leq 9$ are:*

$$H_1 \cap H_4 = H_1 \cap H_5 = H[1,0,4],\ H_1 \cap H_8 = H[1,0,4] \cup H[1,0,8],\ H_1 \cap H_9 = H[1,0,8].$$

The listed $H(q)$'s are all irreducible if $\mathrm{char}(K) \neq 2$.

(b) *We have the following intersections.*

$$\begin{aligned}
H_4 \cap H_5 &= H[1,0,4] \cup H[4,0,5] \cup H[4,4,5], \\
H_4 \cap H_8 &= H[1,0,4] \cup H[4,4,8] \cup H[4,0,4] \cup H[4,0,8], \\
H_4 \cap H_9 &= H[4,0,5] \cup H[4,0,9] \cup H[4,4,9], \\
H_4 \cap H_{12} &= H[4,4,4] \cup H[4,4,12] \cup H[4,0,8] \cup H[4,0,12], \\
H_4 \cap H_{13} &= H[4,0,1] \cup [4,0,9] \cup [4,0,13] \cup [4,4,5] \cup [4,4,13].
\end{aligned}$$

Moreover, the listed $H(q)$'s are irreducible if $\mathrm{char}(K) \neq 2, 3, 5$.

Proof. Let q be a form which appears on the right hand side of the formula (9) for $H_{N^2} \cap H_M$. Then q primitively represents N^2 and M. Assume that $H(q) \neq \emptyset$. Then $q \in Q(N^2)$ by Theorem 1, so q has type (N, m, d) for some m and d; cf. Theorem 4.

(a) If $N = 1$, then every form q of type $(1, m, d)$ is equivalent to $[1, 0, 4d]$. Since such a form does not represent any numbers strictly between 1 and $4d$, we must have $4d \leq M$. For each such form q, we make a table of the values n which are primitively represented by q (for $n \leq 9$). It is then an easy check to see which of these forms represent a given M. Since these forms all have type $(1, 1, d)$ with $d|2$, it follows from Corollary 5 that they are are irreducible if $\mathrm{char}(K) \neq 2$.

(b) Here $N = 2$. By the classification of type $(2, m, d)$ (cf. the proof of Proposition 51) we know that $q \sim [4, 0, n]$ or $q \sim [4, 4, n]$ for some $n \geq 1$. If $n > 4$, then these forms do not represent any numbers strictly between 4 and n, so if $M \geq 5$, then $n \leq M$. Thus, we need to look at only $2M$ forms and decide which of these has type $(2, m, d)$ and primitively represents M, which is an easy exercise. From this list and Proposition 51 we see that $H(q)$ is irreducible for these forms under the given hypotheses.

Note that the above forms are reduced (in the sense of reduction theory) when $n \geq 4$, so if they are distinct, then they are not equivalent. We thus see that the associated $H(q)$'s are distinct by Corollary 26.

Remark 58 The method of analyzing the components of $H_{N^2} \cap H_M$ which was used in the proof of Proposition 57 can be extended to other cases, but the situation becomes more involved. On the one hand there are more forms to consider and one the other hand one has to apply the reduction algorithm to the forms to be sure to have distinct $H(q)$'s. For example, we have

$$H_5 \cap H_9 = H[4,0,5] \cup H[5,2,9] \cup H[5,4,8],$$

where the first form is the reduction of the form $[9,8,4]$ of type $(3,1,5)$, the second is the reduction of the form $[9,2,5]$ of type $(3,1,11)$ and the third is the reduction of the form $[9,6,5]$ of type $(3,3,1)$.

Similarly, by using a computer we can use the results of the previous sections (together with Proposition 12 and reduction theory) to determine the number of irreducible components of the intersection $H_{N^2} \cap H_m$ for slightly larger values of N and M. Recall that M has to satisfy $M \equiv 0, 1 \pmod 4$, for otherwise $H_M = \emptyset$.

Proposition 59 *If* $\mathrm{char}(K) = 0$*, then the number of irreducible components of the intersection* $H_{N^2} \cap H_M$ *of Humbert surfaces for* $N \leq 5$ *and* $M \leq 25$ *is given in the following table:*

$N^2 \backslash m$	1	4	5	8	9	12	13	16	17	20	21	24	25
1	$*$	1	1	2	1	2	2	2	3	3	2	3	3
4	1	$*$	3	4	3	4	5	5	5	6	5	6	6
9	1	3	3	5	$*$	6	5	6	8	7	**8**	**10**	9
16	2	5	5	6	6	9	9	$*$	9	12	10	11	12
25	3	6	**7**	8	9	9	10	12	15	**16**	11	13	$*$

Moreover, all the $H(q)$*'s appearing in these intersections are irreducible, with the exception of the cases* $(N,m) = (3,21)$*,* $(3,24)$*,* $(5,5)$*, and* $(5,20)$*. For these cases, the number of irreducible components is given in bold type in the above table.*

Proof. (Sketch.) The cases $N = 1$ and $N = 2$ are handled by a similar method as in the proof of Proposition 57. For $N \geq 3$ we use again Proposition 12 together with the fact that if $H(q)$ appears in the intersection $H_{N^2} \cap H_M$, then q has type (N,m,d) with $m^2 d \leq \frac{N^2 M}{4m^2}$; cf. Remark 13.

For $N = 4$ all the $H(q)$'s appearing in $H_{16} \cap H_M$ are irreducible by Corollary 56.

For the cases $N = 3$ and $N = 5$ we apply Theorem 10. By that result (and computer computations) we see that all the $H(q)$'s which appear in the intersection $H_{N^2} \cap H_M$ for $M \leq 25$ are irreducible, with the following exceptions: 1) $H[9,6,21]$, which appears in $H_9 \cap H_{21}$ and in $H_9 \cap H_{24}$; 2) $H[25,10,5]$, which appears in $H_{25} \cap H_5$ and in $H_{25} \cap H_{20}$; 3) $H[25,20,20]$, which appears in $H_{25} \cap H_{20}$; and 4) $H[25,0,20]$,

which also appears in $H_{25} \cap H_{20}$. All these exceptions have two irreducible components by Theorem 10.

Note also that $H[9,6,9]$, which appears in $H_9 \cap H_{12}$ and in $H_9 \cap H_{24}$, is irreducible by Theorem 10 because $[9,6,9] \sim [24,24,9]$ is an ambiguous form.

References

[AP] R. Accola, E. Previato, Covers of tori: genus 2. *Letters Math. Phys.* **76** (2006), 135–161.

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

[FPR] M. Franciosi, R. Pardini, S. Rollenske, (p,d)-elliptic curves of genus 2. Preprint, 16pp. ArXiv:1611.06756v1.

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

[EGA] A. Grothendieck, J. Dieudonné, Eléments de Géométrie Algébrique. *Publ. Math. I.H.E.S.* **8, 11, 17, 20, 24, 28, 32** (1961-68).

[Hu] G. Humbert, Sur les fonctions abéliennes singulières. I-III. *J. de Math.* (ser. 5) **5** (1899), 233–350; **6** (1900), 279–386; **7** (1901), 97-123. = Œuvres, vol. II, Gauthier-Villars et Cie., Paris, 1929, pp. 297–527.

[K1] E. Kani, Elliptic curves on abelian surfaces. *Manus. math.* **84** (1994), 199–223.

[K2] E. Kani, The Hurwitz space of genus 2 covers of an elliptic curve. *Collect. Math.* **54** (2003), 1–51.

[K3] E. Kani, The moduli spaces of Jacobians isomorphic to a product of two elliptic curves. *Collect. Math.* **67** (2016), 21–54.

[K4] E. Kani, Elliptic subcovers of curves of genus 2 I. The isogeny defect. *Annales math. Québec* **43** (2019), 281–303.

[K5] E. Kani, Elliptic subcovers of curves of genus 2 II. The refined Humbert invariant. *J. Number Th.* **193** (2018), 302–335.

[K6] E. Kani, Modular correspondences on $X(N)$. Preprint, 2017; 22 pp.

[K7] E. Kani, Modular curves on Humbert surfaces. Preprint (in preparation).

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

[La] H. Lange, Über die Modulvarietät der Kurven vom Geschlecht 2. *J. reine angew. Math.* **281** (1976), 80–96.

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

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

[M1] D. Mumford, *Geometric Invariant Theory.* Springer-Verlag, Berlin, 1965.

[M2] D. Mumford, *Abelian Varieties.* Oxford U Press, Oxford, 1970.

[No] A. Nobs, Die irreduziblen Darstellungen der Gruppen $\mathrm{SL}_2(\mathbb{Z}_p)$, insbesondere $\mathrm{SL}_2(\mathbb{Z}_2)$. *Comment. Math. Helv.* **51** (1976), 465–489.

[ST] J.-P. Serre, J. Tate, Good reduction of abelian varieties. *Ann. Math.* **88** (1968), 492–517 = J.-P. Serre, Œuvres/Collected Papers II, Springer-Verlag, Berlin, pp. 472–497.

[Sh] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions.* Princeton University Press, Princeton, NJ, 1971.

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