

Generalized Humbert Schemes and Intersections of Humbert Surfaces

Ernst Kani

1 Introduction

In 1899 Humbert[[Hu](#)] attached to a principally polarized complex 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 12 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

$$(1) \quad H_m \cap H_n = \bigcup_q H(q),$$

where the union runs over all equivalence classes of positive definite binary quadratic forms q which primitively represent both m and n ; cf. Proposition 13.

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

Let $M_2 = M_2(K) \subset A_2(K)$ denote the open subset consisting of the Jacobians of smooth curves C/K of genus 2. Then $H_{N^2} \cap M_2$ consists of the isomorphism classes of such curves which have an elliptic subcover of degree N ; cf. [K1]. Thus, the intersection $H_{N^2} \cap H_m \cap M_2$ gives the set of isomorphism classes of such curves which have an elliptic subcover of degree N and also one of degree m . With suitable restrictions, such curves always exist, as the following partial refinement of Corollary 2 shows.

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

Actually, Corollary 3 is not a direct consequence of Theorem 1, for it requires further results from [K5]. Moreover, if $K = \overline{\mathbb{F}_p}$ is the algebraic closure of a finite field, then we also require Proposition 25 below, so its proof is given in §5.

The above result answers a question raised by Accola and Previato[AP] about Lange's moduli space $M_2(n, 1)$ which classifies isomorphism classes of curves which admit a morphism of degree n to some elliptic curve; cf. [La]. Their question was whether $M_2(n, 1)$ was connected, and this is indeed the case.

Corollary 4 *If $\text{char}(K) \nmid n$, then $M_2(n, 1) = \bigcup_{N|n, N>1} H_{N^2} \cap M_2$ is connected.*

Theorem 1 answers the question of when $H(q)$ is non-empty, and hence constitutes a first step towards understanding the nature of the intersection $H_{N^2} \cap H_m$. To go further and to determine the irreducible components of $H(q)$ (and hence of the intersection $H_{N^2} \cap H_m$) 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

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

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

Theorem 5 *If $q \in Q(N^2)$, then q is of type (N, m, d) , for unique integers $m|N$ and $d \geq 1$. Put $c_m(q) = \gcd(\text{cont}(q), m)$, where $\text{cont}(q)$ denotes the content of q , i.e., $\text{cont}(q) = \gcd(a, b, c)$, where a, b, c are the coefficients of q . Moreover, assume that $\text{char}(K) \nmid Nd$.*

(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 51 and 58.

Note that Theorem 5(a) implies the following *irreducibility criterion*, which generalizes that of the case $m = 1$ studied in [K3].

Corollary 6 *If q has type (N, m, d) and if $c_m(q) = 1$, then $H(q)$ is irreducible, provided that $\text{char}(K) \nmid Nd$.*

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

Corollary 7 *If $\text{char}(K) = 0$ 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 5 is 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 $\alpha \in \text{GL}_2^+(\mathbb{Q})$ 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

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

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

Theorem 8 *If q is a binary form of type (N, m, d) , and if $\text{char}(K) \nmid N$, then*

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

where the union is over all $\alpha \in \mathcal{M}_d$ such that q_α^N is equivalent to q . In particular, if $\text{char}(K) \nmid Nd$, then $H(q)$ 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 8 has the following consequence.

Corollary 9 *Let $M \equiv 0, 1 \pmod{4}$ be a positive integer. If $\text{char}(K) = 0$ or if $\text{char}(K) > \frac{N^2 M}{4}$, then $H_{N^2} \cap H_M$ is an equidimensional curve, provided that $N^2 \neq M$.*

While Theorem 8 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 10 *Let N, d be positive integers with $\text{char}(K) \nmid Nd$. If $\alpha_1, \alpha_2 \in \mathcal{M}_d$, then*

$$(4) \quad g\beta\alpha_1 g^{-1} \equiv \pm\beta\alpha_2 \pmod{N}, \text{ for some } g \in \text{SL}_2(\mathbb{Z}) \Rightarrow \overline{T}_{\alpha_1}^N = \overline{T}_{\alpha_2}^N.$$

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

From this result, it is clear that the $\text{SL}_2(\mathbb{Z}/N\mathbb{Z})$ -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 $d \leq N^4/(4m^2)$. In the case that $N = 2$ or 4 we prove here:

Theorem 11 *If q has type (N, m, d) , where $N = 2$ or $N = 4$, and if $\text{char}(K) \nmid 2d$, then $H(q)$ is irreducible.*

The case of an odd prime N much more difficult; cf. [K9].

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.

This paper is organized as follows. In §2 we recall from [K1], [K3] the definition of the refined Humbert invariant $q_{(A, \lambda)}$ and of the generalized Humbert schemes $H(q)$ and prove Theorem 1 and Corollary 2. In §3 we use the “basic construction morphism” β_N to show that H_{N^2} is a closed irreducible surface; cf. Theorem 15.

In §4 we study the modular correspondences T_α^N and their images $\overline{T}_\alpha^N$, and use these in §5 to prove Theorem 8, Corollaries 3, 4 and 9, and Theorem 10.

In §6 we use the work of Nobs[No] to study the SL_2 -conjugacy classes of 2×2 matrices mod N . This is used in §7 to prove Theorems 5 and 11, and Corollaries 6 and 7. Finally, in §8 we use the above results to work out some examples.

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 $\text{NS}(A) = \text{Div}(A)/\equiv$, where $\text{Div}(A)$ denotes the group of divisors on A and $\equiv$ denotes numerical equivalence.

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

$$(5) \quad \tilde{q}_{(A,\lambda)}(D) = (D \cdot \theta_\lambda)^2 - 2(D \cdot D), \quad \text{for } D \in \text{NS}(A),$$

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 $\text{NS}(A, \lambda) = \text{NS}(A)/\mathbb{Z}\theta_\lambda$; cf. [K1], §3. It is clear that the isomorphism class of the quadratic module $(\text{NS}(A, \lambda), q_{(A,\lambda)})$ 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 $D \in \text{NS}(A, \lambda)$ 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

$$(6) \quad H_\Delta = H_\Delta(K) := \{ \langle A, \lambda \rangle \in A_2(K) : q_{(A,\lambda)} \text{ primitively represents } \Delta \}$$

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

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

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

Note that if q is a 1-variable quadratic form $q_\Delta(x) = \Delta x^2$, then (6) 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 $A_2(K)$, so they inherit a scheme structure from A_2 and hence can be called *Humbert schemes*.

Remark 12 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 13 *If m and n are distinct positive integers, then*

$$(7) \quad H_m \cap H_n = \bigcup_q H(q),$$

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 by q , it follows that m also primitively represented by $q_{(A, \lambda)}$, so $\langle A, \lambda \rangle \in H_m$ by (6). Thus $H(q) \subset H_m$, and similarly, $H(q) \subset H_n$, so $H(q) \subset H_m \cap H_n$. This shows that the right side of (7) is contained in the left side.

Conversely, suppose that $\langle A, \lambda \rangle \in H_m \cap H_n$. Then there exist primitive vectors $v, w \in M := \text{NS}(A, \lambda)$ 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 (7), so $\langle A, \lambda \rangle \in \bigcup H(q)$.

Remark 14 (a) Note that there are only finitely many equivalence classes of forms q satisfying the conditions of Proposition 13 because their discriminants are bounded. Indeed, it follows from the above proof that we have $|\text{disc}(q)| \leq 4mn$ for any such q because $|\text{disc}(q)| \leq |\text{disc}(q_{|M_0|})| \leq 4mn$.

(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 (5) shows that $q_{(A, \lambda)}(D) \equiv (D.\theta_\lambda)^2 \pmod{4}$, for all $D \in \text{Div}(A)$. 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 $\text{char}(K) \nmid N$, 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 $\varepsilon = \text{rem}(m, 4) \in \{0, 1\}$ and consider the binary quadratic form $q_{N, m}(X, Y) := N^2 X^2 + 2\varepsilon NXY + MY^2 = (NX + \varepsilon Y)^2 + (m - \varepsilon)Y^2$ which is clearly positive definite. Since $q_{N, m}(1, 0) = N^2$ and $q_{N, m}(0, 1) = m$, we see that $q_{N, m}$ primitively represents N^2 and m , so $H(q) \subset H_{N^2} \cap H_m$ by Proposition 13.

Moreover, since $q_{N, m}(X, Y) \equiv (NX + \varepsilon Y)^2 \pmod{4}$, 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.

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

$$\beta_N : X(N) \times X(N) \rightarrow A_2$$

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 $\text{char}(K) \nmid N$, 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 [K7], §4, that the (affine) modular curve $X(N)/K$ (coarsely) represents the functor

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

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 $\mathcal{A}_2 = \mathcal{A}_{2,1,1} : (\text{Sch}/K) \rightarrow (\text{Sets})$ 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)

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

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

$$(8) \quad \psi = \psi_{\phi_1, \phi_2} := \phi_2 \circ \left[\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right]_N \circ \phi_1^{-1} : E_1[N] \rightarrow E_2[N],$$

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

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

$$(9) \quad \hat{\pi}_\psi \circ \lambda_\psi \circ \pi_\psi = N(\lambda_{E_1} \otimes \lambda_{E_2}),$$

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

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

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

$$\beta_N : X(N) \times X(N) \rightarrow \mathcal{A}_2.$$

Theorem 15 *The above morphism $\beta_N : X(N) \times X(N) \rightarrow \mathcal{A}_2$ is finite and its image is the Humbert surface H_{N^2} . In particular, H_{N^2} is an affine closed irreducible subscheme of $\mathcal{A}_2$ 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 $\text{Im}(\beta_N) = H_{N^2}$. 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 $\text{Im}(\beta_N) \subset H_{N^2}$. 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 $\psi : E[N] \rightarrow E'[N]$ such that $(A_\psi, \lambda_\psi) \simeq (A, \lambda)$. Since K is algebraically closed and $\text{char}(K) \nmid N$, 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 $\langle A, \lambda \rangle \in \text{Im}(\beta_N)$. This proves that $\text{Im}(\beta_N) = H_{N^2}$.

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 $\bar{D} \in \text{NS}(A, \lambda)$ 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 $S = \text{Spec}(R)$, 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 $\tilde{\phi}_i : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} \tilde{E}_i[N]$ (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} .

Remark 16 The above morphism β_N is closely connected with the notion of an N -presentation which was introduced in [K4], §2; cf. also [K5], §3.

Given a principally polarized abelian surface (A, λ) and an integer $N \geq 2$, an N -presentation of (A, λ) is a 4-tuple (E_1, E_2, ψ, π) consisting of two elliptic curves E_1 and E_2 , an anti-isomorphism $\psi : E_1[N] \rightarrow E_2[N]$ and an isogeny $\pi : E_1 \times E_2 \rightarrow A$ such that $\text{Ker}(\pi) = \text{Graph}(-\psi)$ and such that the analogue of (9) holds when we replace π_ψ and λ_ψ by π and λ , respectively. If (A, λ) has an N -presentation, then $(A, \lambda) \simeq (A_\psi, \lambda_\psi)$, and so the above proof of Theorem 15 shows that

$$H_{N^2}(K) = \{ \langle A, \lambda \rangle \in \mathcal{A}_2(K) : (A, \lambda) \text{ has an } N\text{-presentation} \}.$$

4 The modular correspondence T_α^N

From Theorem 15 we know that every curve on the Humbert surface H_{N^2} is the image of a curve on the product surface $X(N) \times X(N)$, so if the intersection $H_{N^2} \cap H_M$ is a closed set, then the irreducible curve components of this intersection 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 $\alpha \in \text{GL}_2^+(\mathbb{Q})$ acting on the upper half plane $\mathfrak{H}$ and hence is denoted by T_α^N .

As we shall see (cf. Theorem 8), 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 [K7]. However, in place of working with T_α^N directly, it is more convenient to work with the normalization $\tau_\alpha^N : X_\alpha^N \rightarrow T_\alpha^N$ 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 $f : E \rightarrow E'$ 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

$$(10) \quad f \circ \phi = \phi' \circ [\alpha]_N.$$

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.,

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

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 [K7].

Theorem 17 *If $\text{char}(K) \nmid Nd$, 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. [K7], Theorems 2 and 3.

Remark 18 It was also shown in [K7] 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 $\tau_\alpha^N : X_\alpha^N \rightarrow T_\alpha^N$ is induced by the forget morphism $\tilde{\tau}_\alpha^N = \{(\tau_\alpha^N)_S\}_S : \mathcal{X}_\alpha^N \rightarrow \mathcal{X}(N) \times \mathcal{X}(N)$, 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 $\tau_\alpha^N : X_\alpha^N \rightarrow X(N) \times X(N)$ and we have

Proposition 19 *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 is a birational map onto its image, and so X_α^N is the normalization of T_α^N .*

Proof. [K7], Corollary 36.

Remark 20 It follows from the above that if $x_i = \langle E_i/K, \phi_i \rangle \in X(N)(K)$, where $i = 1, 2$, and if $\text{char}(K) \nmid Nd$, then

$$(11) \quad (x_1, x_2) \in T_\alpha^N(K) \quad \Leftrightarrow \quad \exists \text{ a cyclic isogeny } f : E_1 \rightarrow E_2 \text{ of degree } d = \det(\alpha) \text{ such that } (\phi_1, f, \phi_2) \text{ is } \alpha\text{-compatible.}$$

Note that the right hand side of (11) also makes sense when $\text{char}(K) \mid d$. Thus, in this case we can define $T_\alpha^N = T_\alpha^N(K)$ by (11), and hence $T_\alpha^N(K)$ satisfies (11) for all $\alpha \in \mathcal{M}_d$, $d \geq 1$.

Corollary 21 *If $\text{char}(K) \nmid Nd$, then for every $\alpha \in \mathcal{M}_d$ there is a unique finite morphism*

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

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 $\psi = \psi_{\phi_1, \phi_2} : E_1[N] \rightarrow E_2[N]$ is defined by (8). Moreover, we have the relation

$$(12) \quad \phi_1^{-1} \circ \psi^{-1} \circ f \circ \phi_1 = [\beta\alpha]_N, \quad \text{where } \beta = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Proof. Consider the morphism $\beta_\alpha^N := \beta_N \circ \tau_\alpha^N : X_\alpha^N \rightarrow A_2$, where τ_α^N is as in Proposition 19 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 (12) follows directly from (11), (10) and (8).

Remark 22 (a) It follows from Corollary 21 and Theorem 17 that if $\text{char}(K) \nmid Nd$ 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

$$(13) \quad \alpha_1 \equiv \alpha_2 \pmod{N} \quad \Rightarrow \quad \overline{T}_{\alpha_1}^N = \overline{T}_{\alpha_2}^N, \quad \text{for all } \alpha_1, \alpha_2 \in \mathcal{M}_d.$$

(b) It is useful to rephrase Corollary 21 in terms of N -presentations (cf. Remark 16). Suppose that $\mathcal{P} = (E_1, E_2, \psi, \pi)$ is an N -presentation of (A, λ) , and let $\alpha \in \mathcal{M}_d$. Then we say that $\mathcal{P}$ *has type* α if there exists a level N -structure ϕ_1 on E_1 and a cyclic isogeny $f : E_1 \rightarrow E_2$ of degree d such that (12) holds. We then have:

$$(14) \quad \overline{T}_\alpha^N(K) = \{ \langle A, \lambda \rangle \in \mathcal{A}_2(K) : (A, \lambda) \text{ has an } N\text{-presentation of type } \alpha \}.$$

Indeed, Corollary 21 shows that the left hand side of (14) is contained in the right hand side. Conversely, if (E_1, E_2, ψ, π) is an N -presentation of (A, λ) of type α , and if ϕ_1 and f satisfy (12), then $\phi_2 := \psi \circ \phi_1 \circ [\beta]_N$ is a level N -structure on E_2 , and (12) shows that (ϕ_1, f, ϕ_2) is α -compatible. Thus $x := \langle E_1/K, \phi_1, E_2/K, \phi_2, f \rangle \in \mathcal{X}_\alpha^N(K)$, and hence $\langle A, \lambda \rangle = \beta_\alpha^N(x) \in \overline{T}_\alpha^N(K)$, which proves (14).

(c) If $\text{char}(K) \nmid N$, but $\text{char}(K) | d$, then the right hand side of (14) still makes sense, so in this case we can define the set $\overline{T}_\alpha^N = \overline{T}_\alpha^N(K)$ by (14). Thus, $\overline{T}_\alpha^N$ is given by (14) for all $\alpha \in \mathcal{M}_d$, $d \geq 1$. Moreover, by using Remark 20, we see that that the arguments of Corollary 21 and of Remark 8(b) show that we have that $\beta_N(T_\alpha^N(K)) = \overline{T}_\alpha^N(K)$, for all $\alpha \in \mathcal{M}_d$, $d \geq 1$.

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 23 *Let N and d be positive integers, and let $\alpha \in \mathcal{M}_d$ be a primitive matrix of determinant d . Write $\beta\alpha = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$, where $\beta = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, and put $g = \gcd(x - w, y, z, N)$, $m = \frac{N}{g}$, and $t = \text{trace}(\beta\alpha) = x + w$. 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*

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

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

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 $\text{GL}_2(\mathbb{Z})$ -equivalent to q_α^N .)

Assume now that $\text{char}(K) \nmid N$, and let $y = \langle A, \lambda \rangle \in \overline{T}_\alpha^N(K)$. Then by Remark 22 we know that (A, λ) has an N -presentation (E_1, E_2, ψ, π) of type α , so there exists a level N -structure ϕ_1 of E_1 and a cyclic isogeny $f : E_1 \rightarrow E_2$ of degree d such that (12) holds. From this 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_1 . 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 $q_{(A, \lambda)}$ primitively represents q_α^N , and so $y \in H(q_\alpha^N)(K)$. Thus $\overline{T}_\alpha^N(K) \subset H(q_\alpha^N)(K)$, as claimed.

Proof of Theorem 8. By Proposition 23 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 $y \in H(q)(K)$ be given by $\langle A, \lambda \rangle \in \mathcal{A}_2(K)$. Then the definition of $H(q)$ implies that $q_{(A, \lambda)}$ primitively represents q , and so there exists a primitive submodule $\tilde{\mathcal{G}}$ of $\text{NS}(A, \lambda)$ such that the restriction of $q_{(A, \lambda)}$ to $\tilde{\mathcal{G}}$ 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 $\mathcal{P} = (E, E', \psi, \pi)$ of (A, λ) , and a cyclic isogeny $h : E \rightarrow E'$ 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 $\text{GL}_2(\mathbb{Z})$ -equivalent to the form $q_{M, N, d, k} := [N^2, -2mT, \frac{m^2}{N^2}(T^2 + 4d)]$, where $T = -\text{tr}(M) + dk^3(\det(M) + d)$.

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 $\phi^{-1} \circ \psi^{-1} \circ h \circ \phi \in \text{End}((\mathbb{Z}/N\mathbb{Z})^2)$, it follows that there is an integral matrix $M \in M_2(\mathbb{Z})$ such that

$$(15) \quad \phi^{-1} \circ \psi^{-1} \circ h \circ \phi = [M]_N.$$

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 $\text{GL}_2(\mathbb{Z})$ -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 by Proposition 14 of [K5] we have that q is $\mathrm{GL}_2(\mathbb{Z})$ -equivalent to $q_{\beta\alpha, N, d, k} = q_\alpha^N$. Moreover, (15) shows that $\mathcal{P}$ is an N -presentation of type α , and hence $\langle A, \lambda \rangle \in \overline{T}_\alpha^N(K)$ by (14). This proves the opposite inclusion, and so (3) holds.

To prove the last assertion, note that if $\mathrm{char}(K) \nmid Nd$, then it follows from Remark 22(a) that the union on the right side of (3) consists of only finitely many distinct irreducible curves $\overline{T}_\alpha^N$. Since each of these is a closed subset of A_2 by Corollary 21, 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 24 As the above proof of Theorem 8 shows, there exists a closed subscheme $\mathbf{H}(q)_K$ of A_2/K such that its set of K -rational points equals $H(q)(K) \subset A_2(K)$, provided that $\mathrm{char}(K) \nmid Nd$. In what follows, we shall frequently write $H(q)$ in place of $\mathbf{H}(q)_K$ to simplify the notation.

We note that it follows from Theorem 8 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.

The above remark allows us to prove the following useful result.

Proposition 25 *Let q be a binary quadratic form of type (N, m, d) , and assume that $\mathrm{char}(K) \nmid N$. Then*

$$(16) \quad H(q) \cap M_2 \neq \emptyset \quad \Leftrightarrow \quad q(x, y) \neq 1, \quad \forall x, y \in \mathbb{Z},$$

provided that K is not the algebraic closure of a finite field. On the other hand, if $K = \overline{\mathbb{F}}_p$, then (16) still holds in the case that $p \nmid d$.

Proof. ($\Rightarrow$) If $\langle A, \lambda \rangle \in H(q) \cap M_2$, then by definition we have that $q_{(A, \lambda)} \rightarrow q$ and by Proposition 6 of [K3] we know that $q_{(A, \lambda)}(D) \neq 1$, for all $D \in \mathrm{NS}(A, \lambda)$, so in particular $q(x, y) \neq 1$, for all $x, y \in \mathbb{Z}$.

($\Leftarrow$) Suppose first that $K \neq \overline{\mathbb{F}}_p$, for any prime p . Then by Corollary 34 of [K5] there exists a curve C/K of genus 2 such that $q_C = q_{(J_C, \lambda_C)} \sim q$. Thus $\langle J_C, \lambda_C \rangle \in H(q) \cap M_2$, which proves (16) in this case.

Now suppose that $K = \overline{\mathbb{F}}_p$ and that $p \nmid d$. Then by Theorem 8 we know that $H(q)$ is closed equidimensional subscheme of A_2 of dimension 1, and thus $H(q) \cap M_2$ is an open subscheme of $H(q)$ because $M_2 = A_2 \setminus H_1$ is open in A_2 . Thus, if $H(q) \cap M_2$ is not the empty scheme, then $\dim(H(q) \cap M_2) = 1$.

Let K' be an algebraically closed extension field of K which is transcendental over K . Then by what was proved above, we see that $(H(q) \cap M_2)(K') \neq \emptyset$. Thus, $\dim(H(q) \cap M_2) = 1$, and so by base change (cf. Remark 22) we have that also $(H(q) \cap M_2)(K) \neq \emptyset$ because K is algebraically closed. This proves that (16) holds in this case as well.

Proof of Corollary 3. It clearly suffices find a positive binary quadratic form q such that $H(q) \cap M_2 \neq \emptyset$ and such that $H(q) \subset H_{N^2} \cap H_m$.

For this, consider $q = q_{N,m}$ as in the proof of Corollary 2. Thus q is a binary form such that $H(q) \subset H_{N^2} \cap H_m$, as was explained in Corollary 2. Since $\text{disc}(q_{N,m}) = -4N^2(m - \varepsilon^2)$ and since $q_{N,m} \equiv (NX + \varepsilon Y)^2 \pmod{4}$, it follows from Proposition 7 of [K5] that $q_{N,m}$ has type (N, N, d) with $d = \frac{m - \varepsilon^2}{4}$. 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 or that $\text{char}(K) \nmid d = \frac{m - \varepsilon^2}{4}$. Then by Proposition 25 we have that $H(q) \cap M_2 \neq \emptyset$, and the assertion holds in this case.

Now suppose that $K = \overline{\mathbb{F}}_p$ is the algebraic closure of a finite field and that $p \mid d = \frac{m - \varepsilon^2}{4}$. If $\varepsilon = 0$, then $p \mid \frac{m}{4}$, so consider the form $q_1(X, Y) = N^2X^2 + 4XY + mY^2 \equiv N^2X^2 \pmod{4}$. Since $\text{disc}(q_1) = -16(N\frac{m}{4} - 1)$, we see by Proposition 7 of [K5] that q_1 has type $(N, 1, d_1)$ with $d_1 = N(\frac{m}{4}) - 1$. Thus $p \nmid d_1$. We note that $q_1(x, y) \geq \min(N^2, m) \geq 4$, if $(x, y) \in \mathbb{Z}^2 \setminus (0, 0)$, because (after interchanging X and Y , if necessary) we have that q_1 is a reduced binary form. It thus follows from Proposition 25 that $H(q_1) \cap M_2 \neq \emptyset$. Moreover, since q_1 represents $N^2 = q_1(1, 0)$ and $m = q_1(0, 1)$ primitively, we have that $H(q_1) \subset H_{N^2} \cap H_m$, and hence the assertion holds in this case as well.

Next, suppose that $\varepsilon = 1$, so $p \mid \frac{m-1}{4}$. If $N \equiv 0 \pmod{2}$, then consider the form $q_2(X, Y) = N^2X^2 + mY^2 \equiv Y^2$. Thus, since $\text{disc}(q_2) = -4N^2m = -16(\frac{N}{2})^2m$, we see that q_2 has type $(N, \frac{N}{2}, m)$. Since clearly $p \nmid m$ and since $q_2(x, y) \geq \min(N^2, m) \geq 4$, if $(x, y) \in \mathbb{Z}^2 \setminus (0, 0)$, it follows from Proposition 25 that $H(q_2) \cap M_2 \neq \emptyset$. Moreover, since q_2 represents $N^2 = q_2(1, 0)$ and $m = q_2(0, 1)$ primitively, we conclude as before that the assertion holds in this case.

Finally, suppose that $\varepsilon = 1$ and that $N \equiv 1 \pmod{2}$. In this case we consider the form $q_3(X, Y) = N^2X^2 + 2XY + mY^2 \equiv (X + Y)^2 \pmod{2}$. Here $\text{disc}(q_3) = -4(N^2m - 1)$. Since $N^2m \equiv 1 \pmod{4}$, we see that q_3 has type $(N, 1, d_3)$ with $d_3 = \frac{N^2m-1}{4}$. Now since $q_3(x, y) \geq \min(N^2, m) \geq 4$, if $(x, y) \in \mathbb{Z}^2 \setminus (0, 0)$, it follows from Proposition 25 that $H(q_3) \cap M_2 \neq \emptyset$. Moreover, since q_3 represents $N^2 = q_3(1, 0)$ and $m = q_3(0, 1)$ primitively, we conclude as before that the assertion holds in this case and hence in all cases.

Proof of Corollary 4. The fact that $M_2(n, 1) = \bigcup_{N \mid n, N > 1} H_{N^2} \cap M_2$ follows from the

fact that every morphism $f : C \rightarrow E$ of degree n factors uniquely over an elliptic subcover $f' : C \rightarrow E'$ of degree $N|n$; cf. [K6], Corollary 1.2. Thus, by Theorem 15 we see that the surfaces $H_{N^2} \cap M_2$ with $N|n$, $N > 1$, are the irreducible components of $M_2(n, 1)$. Now it follows from Corollary 3 that any two such irreducible components of $M_2(n, 1)$ meet, so in particular $M_2(n, 1)$ is connected.

Proof of Corollary 9. From Corollary 2 it follows that $H_{N^2} \cap H_M \neq \emptyset$ and by Proposition 13 and Theorem 5 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 $\text{disc}(q) = -16m^2d$, we see that $d \leq m^2d = \frac{|\text{disc}(q)|}{16} \leq \frac{N^2M}{4}$ by Remark 14. Thus, by the given hypothesis we see that $\text{char}(K) \nmid Nd$, and so by Theorem 8 we have that each such $H(q)$ is an equidimensional curve, and hence so is $H_{N^2} \cap H_M$.

For later use, we note the following partial refinement of Theorem 8.

Proposition 26 *Let q be a form of type (N, m, d) and let $\alpha \in \mathcal{M}_{d_1}$. If $\text{char}(K) \nmid Ndd_1$, then $\overline{T}_\alpha^N \subset H(q)$ if and only if q is $\text{GL}_2(\mathbb{Z})$ -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 also 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 $\text{End}(E) = \mathbb{Z}$.

Lemma 27 *Let $\alpha \in \mathcal{M}_d$ and $N \geq 1$, and suppose that $\text{char}(K) \nmid Nd$ 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 $\text{End}(E_i) = \mathbb{Z}$. 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 $h_i : E_i \rightarrow E'_i := E_i/C_i[d]$ be the quotient isogeny. Then by [K7], 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 $\alpha_d = \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}$. Now $\alpha = g_1 \alpha_d g_2$, for some $g_1, g_2 \in \text{SL}_2(\mathbb{Z})$, 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 $E_i \not\cong E_j$), and so we obtain infinitely many non-CM points.

(b) By Proposition 23 we know that $q_{(J, \lambda)}$ primitively represents q_α^N . But since $\text{Hom}(E, E') \simeq \mathbb{Z}$, we see that $\text{rank}(q_{(J, \lambda)}) = 2$, and so it follows that $q_{(J, \lambda)} \sim q_\alpha^N$.

Proof of Proposition 26. 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 23.

Now suppose conversely that $\overline{T}_\alpha^N \subset H(q)$. Since both are closed subsets of A_2 (cf. Remark 22 and Theorem 8), we have that $\overline{T}_\alpha^N(K') \subset H(q)(K')$ for every extension field K' of K , so we may assume that K' is not the algebraic closure of a finite field. Then by Lemma 27 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 $\langle J, \lambda \rangle \in H(q)(K')$, we have that $q_{(J, \lambda)}$ primitively represents q , so $q_{(J, \lambda)} \sim q$ because both are binary forms, and hence $q_\alpha^N \sim q$, as claimed.

To prove the last assertion, recall from Proposition 23 that q_α^N has type (N, m_1, d_1) for some $m_1 | N$ and some $d_1 \geq 1$ 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 26 has the following interesting application.

Corollary 28 *Let $q_i \in Q(N, m_i, d_i)$, where $i = 1, 2$, be two binary forms which are not equivalent. If $\text{char}(K) \nmid Nd_1d_2$, then $H(q_1) \cap H(q_2)$ consists of finitely many points, and none of these can be images of non-CM points.*

Proof. If $H(q_1) \cap H(q_2)$ were infinite, then it follows from Theorem 8 that $H(q_1)$ and $H(q_2)$ would contain a common irreducible curve component $\overline{T}_\alpha^N$, for some $\alpha \in \mathcal{M}_{d_1}$. By Proposition 26 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 26 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 10 of the introduction. The first assertion follows easily from the following lemma.

Lemma 29 *Let $\alpha_1, \alpha_2 \in \mathcal{M}_d$. Suppose that $\text{char}(K) \nmid Nd$ and that*

$$(17) \quad \beta\alpha_2 \equiv \varepsilon g^{-1}\beta\alpha_1 g \pmod{N}, \quad \text{for some } g \in \text{SL}_2(\mathbb{Z}) \text{ and } \varepsilon \in \{1, -1\}.$$

If $x_1 := \langle E/K, \phi, E'/K, \phi', h \rangle \in \mathcal{X}_{\alpha_1}^N(K)$ and if $g' := \beta^{-1}g\beta$, then $x_2 := \langle E/K, \phi \circ [g]_N, E'/K, \phi' \circ [g']_N, \varepsilon h \rangle \in \mathcal{X}_{\alpha_2}^N(K)$, and we have that $\beta_{\alpha_1}^N(x_1) = \beta_{\alpha_2}^N(x_2)$. In particular, if (17) holds, then $\overline{T}_{\alpha_1}^N = \overline{T}_{\alpha_2}^N$.

Proof. Since g is in $\text{SL}_2(\mathbb{Z})$, so $g' = \beta^{-1}g\beta$, and hence 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 $\varepsilon h \circ \phi \circ [g]_N = \phi' \circ [\varepsilon\alpha_1 g]_N = \phi' \circ [g'\alpha_2]_N = \phi' \circ [g']_N \circ [\alpha_2]_N$. This proves the first assertion.

To prove the second assertion, let $\psi = \psi_{\phi, \phi'} : E[N] \rightarrow E'[N]$ be defined as in (8), so $\beta_{\alpha_1}^N(x_1) = \langle A_\psi, \pi_\psi \rangle$, where $A = E \times E'$; cf. Corollary 21. 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 $\beta_{\alpha_1}^N(x_1) = \beta_{\alpha_2}^N(x_2)$.

From the second assertion it follows that $\overline{T}_{\alpha_1}^N = \beta_{\alpha_1}^N(X_{\alpha_1}^N) \subset \beta_{\alpha_2}^N(X_{\alpha_2}^N) = \overline{T}_{\alpha_2}^N$. Moreover, by interchanging the roles of α_1 and α_2 , we see that we also have the opposite inclusion, and so $\overline{T}_{\alpha_1}^N = \overline{T}_{\alpha_2}^N$.

It is more difficult to prove the second assertion of Theorem 10. For this, we will prove the following more general assertion.

Theorem 30 *Let q be a form of type (N, m, d) which satisfies the condition*

$$(18) \quad |\{(X, Y) \in \mathbb{Z}^2 : \gcd(X, Y) = 1 \text{ and } q(X, Y) = N^2\}| = 2.$$

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

$$(19) \quad g\beta_{\alpha_1}g^{-1} \equiv \pm\beta_{\alpha_2} \pmod{N}, \text{ for some } g \in \text{SL}_2(\mathbb{Z}) \Leftrightarrow \overline{T}_{\alpha_1}^N = \overline{T}_{\alpha_2}^N.$$

Before proving Theorem 30, we first observe that the hypothesis (18) follows from the hypothesis on d and N which was made in Theorems 5 and 10, as the following result shows.

Lemma 31 *If q is a form of type (N, m, d) with $d > N^4/(4m^2)$, then q satisfies condition (18).*

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 $N^2 = q(X, Y) = (NX + \frac{m}{N}tY)^2 + \frac{4m^2d}{N^2}Y^2 \geq \frac{4m^2d}{N^2}$, 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 (18).

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 $t \in \mathbb{Z}$; cf. [K5], Lemma 9. By what was just proved, the condition (18) holds for q' and hence also for q because the left hand side of (18) is the same for all $q \sim q'$.

We next observe that Theorem 30 and Lemma 29 imply Theorem 10.

Proof of Theorem 10 (using Theorem 30). The first assertion follows from Lemma 29.

To prove the second assertion, suppose that $\overline{T}_{\alpha_1}^N = \overline{T}_{\alpha_2}^N$. Then $\overline{T}_{\alpha_1}^N \subset H(q_{\alpha_2}^N)$ by Proposition 23, so $q_{\alpha_1}^N \sim q_{\alpha_2}^N$ by Proposition 26. (Recall that $q_{\alpha_2}^N$ has type (N, m_2, d) , for some $m_2|N$, by Proposition 23.) Thus, $q_{\alpha_1}^N \sim q_{\alpha_2}^N$, and so both have the same type (N, m, d) .

By Lemma 31 we know that the hypothesis $d > N^4/(4m^2)$ implies that $q_{\alpha_i}^N$ satisfies (18), and so the converse implication of (4) follows from (19).

To prove Theorem 30, we will use the following fact which will be proved below in §6; cf. Corollary 39.

Lemma 32 *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 $\beta\alpha^*\beta^{-1} \equiv g\alpha g^{-1} \pmod{N}$.*

The following is the key result used in the proof of Theorem 30.

Proposition 33 *Let $\alpha_1, \alpha_2 \in \mathcal{M}_d$ and suppose that $\mathrm{char}(K) \nmid Nd$. For $i = 1, 2$, let $x_i = \langle E_i, \phi_i, E'_i, \phi'_i, h_i \rangle \in \mathcal{X}_{\alpha_i}^N(K)$ be two non-CM points such that $\beta_{\alpha_1}^N(x_1) = \beta_{\alpha_2}^N(x_2)$, 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*

$$(20) \quad \varphi\pi_2(E_2 \times \{0\}) = \pi_1(E_1 \times \{0\}) \quad \text{or} \quad \varphi\pi_2(\{0\} \times E'_2) = \pi_1(E_1 \times \{0\}),$$

where $\pi_i = \pi_{\psi_i} : E_i \times E'_i \rightarrow A_{\psi_i}$ 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. (This means that $\mathrm{Ker}(\pi_i) = \mathrm{Graph}(-\psi_i)$ and that $\hat{\pi}_i \circ \lambda_{\psi_i} \circ \phi_i = N(\lambda_{E_i} \otimes \lambda_{E'_i})$.) 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) because $\mathrm{Ker}(\varphi\pi_2) = \mathrm{Graph}(-\psi_2)$ and $(\varphi\pi_2)^\wedge \circ \lambda_{\psi_1} \circ \varphi\pi_2 = N(\lambda_{E_2} \otimes \lambda_{E'_2})$. 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 (12) 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 29.

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 $\eta : E'_2 \times E_2 \rightarrow E_2 \times E'_2$ be defined by $\eta(x', x) = (x, x')$, and put $\pi'_2 = \varphi \circ \pi_2 \circ \eta : E'_2 \times E_2 \rightarrow J$. Since $\eta^{-1}(\mathrm{Graph}(-\psi_2)) = \mathrm{Graph}(-\psi_2^{-1})$ and $\hat{\eta} \circ (\lambda_{E_2} \otimes \lambda_{E'_2}) \circ \eta = \lambda_{E'_2} \otimes \lambda_{E_2}$, we see that $(E'_2, E_2, \psi_2^{-1}, \pi'_2)$ 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 $[\varepsilon\beta\alpha_2^*]_N = [g_1\beta\alpha_1g_1^{-1}]_N$. On the other hand, by Lemma 32 (applied to $\beta\alpha_2$), 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 $g = g_2g_1$ shows that $[\varepsilon\beta\alpha_2]_N = [g\beta\alpha_1g^{-1}]_N$, and so $\overline{T}_{\alpha_1}^N = \overline{T}_{\alpha_2}^N$ as before.

Corollary 34 *Let $\alpha_1, \alpha_2 \in \mathcal{M}_d$ and suppose that $\mathrm{char}(K) \nmid Nd$ and that $q = q_{\alpha_1}^N$ satisfies condition (18). 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 $g\beta\alpha_1g^{-1} \equiv \pm\beta\alpha_2 \pmod{N}$, 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 33. By Lemma 27 we know that $q_{(J, \lambda)} \sim q_{\alpha_1}^N = q$, so by Theorem 18 of [K4] we see that the condition (18) 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 (20) holds and so the assertion follows from Proposition 33.

Proof of Theorem 30. The one implication of (19) follows from Lemma 29. 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 27 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 34, and so (19) follows.

6 Conjugacy classes of matrices

In view of Theorems 10 and 30, 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 $\mathrm{SL}_2(\mathbb{Z}) \rightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is surjective.

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

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

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

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

$$(21) \quad \begin{aligned} \tau_{\alpha,N} &:= (\text{tr}(\alpha) - 2\bar{x})/g = (x + w - 2\bar{x})/g \quad \text{and} \\ \delta_{\alpha,N} &:= (\det(\alpha) + \bar{x}^2 - \text{tr}(\alpha)\bar{x})/g^2 = (\det(\alpha) - \bar{x}^2 - \bar{x}g\tau_{\alpha,N})/g^2. \end{aligned}$$

Lemma 35 *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*

$$(22) \quad \text{tr}(\alpha)^2 - 4\det(\alpha) = (\tau_{\alpha,N}^2 - 4\delta_{\alpha,N})g_{\alpha,N}^2.$$

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 $\text{tr}(\alpha') = (\text{tr}(\alpha) - 2\bar{x})/g = \tau_{\alpha,N}$, so $\tau_{\alpha,N} = \text{tr}(\alpha') \in \mathbb{Z}$. Moreover, $\det(\alpha) = \det(\bar{x}I + g\alpha') = \bar{x}^2 + \bar{x}g\text{tr}(\alpha') + g^2\det(\alpha')$, so we also have that $\delta_{\alpha,N} = \det(\alpha') \in \mathbb{Z}$.

Put $\tau = \tau_{\alpha,N}$ and $\delta = \delta_{\alpha,N}$. From (21) we have that $\text{tr}(\alpha)^2 - 4\det(\alpha) = (2\bar{x} + g\tau)^2 - 4(\bar{x}^2 + \bar{x}g\tau + g^2\delta) = g^2(\tau^2 - 4\delta)$, as claimed.

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

Proposition 36 *Let $N \geq 1$, and let $\alpha_i \in M_2(\mathbb{Z})$, $i = 1, 2$, be two matrices such that*

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

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

$$(23) \quad \tau_{\alpha_1,N} \equiv \tau_{\alpha_2,N} \pmod{m} \quad \text{and} \quad \delta_{\alpha_1,N} \equiv \delta_{\alpha_2,N} \pmod{m}.$$

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 $g_{\alpha_2,N} = g_{\alpha_1,N}$.

Put $\alpha'_i = (\alpha_i - \bar{x}_i I)/g$, where $\bar{x}_i = x_{\alpha_i,N}$ and $g = g_{\alpha_1,N}$. Then $\alpha'_i \in M_2(\mathbb{Z})$, and $\tau_i := \tau_{\alpha_i,N} = \text{tr}(\alpha'_i)$ and $\delta_i := \delta_{\alpha_i,N} = \det(\alpha'_i)$, as we saw in the proof of Lemma 35. 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 $\text{tr}(\alpha'_1) \equiv \text{tr}(\alpha'_2) \pmod{m}$ and $\det(\alpha'_1) \equiv \det(\alpha'_2) \pmod{m}$, and hence (23) follows.

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

Proposition 37 *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*

$$(24) \quad \gamma\alpha\gamma^{-1} \equiv \bar{x}I + g \begin{pmatrix} 0 & -\delta z' \\ z & \tau \end{pmatrix} \pmod{N}, \quad \text{for some } \gamma \in \text{SL}_2(\mathbb{Z}).$$

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 $\gamma_1 \in \text{SL}_2(\mathbb{Z})$ such that $\gamma_1\alpha'\gamma_1^{-1} \equiv \alpha_1 \pmod{m}$, where $\alpha_1 = \begin{pmatrix} * & * \\ z & * \end{pmatrix}$, with $\gcd(z, m) = 1$. Choose z' such that $zz' \equiv 1 \pmod{m}$, and put $\alpha_2 = \begin{pmatrix} 0 & -\delta z' \\ z & \tau \end{pmatrix}$. Then $\det(\alpha_2) \equiv \delta = \det(\alpha') \equiv \det(\alpha_1) \pmod{m}$ and $\text{tr}(\alpha_2) = \tau = \text{tr}(\alpha') \equiv \text{tr}(\alpha_1) \pmod{m}$, so by Nobs[No], Lemma 5, there exists $\gamma_2 \in \text{SL}_2(\mathbb{Z})$ 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 (24) 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:

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

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 38 *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 $\alpha'_i = \begin{pmatrix} * & * \\ z_i & * \end{pmatrix}$ with $\gcd(z_i, m) = 1$, for $i = 1, 2$, where $m = N/g$. Put $\tau = \text{tr}(\alpha'_1)$ 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 $\gamma \in \text{SL}_2(\mathbb{Z})$ such that $\gamma\alpha_1\gamma^{-1} \equiv \alpha_2 \pmod{N}$.*
- (ii) *$\text{tr}(\alpha'_2) \equiv \tau \pmod{m}$, $\det(\alpha'_2) \equiv \delta \pmod{m}$ 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

$$(25) \quad \text{There exists } \gamma \in \text{SL}_2(\mathbb{Z}) \text{ such that } \gamma\alpha'_1\gamma^{-1} \equiv \alpha'_2 \pmod{m}.$$

If $m = p^r$ is a prime power, then the equivalence of (25) and (ii) follows from Nobs[No], Lemma 5, and hence the general case follows from this by using the Chinese remainder theorem.

Corollary 39 *If $\alpha \in M_2(\mathbb{Z})$ and $N \geq 1$, and if $\beta = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, then there exists a $\gamma \in \text{SL}_2(\mathbb{Z})$ such that*

$$(26) \quad \beta\alpha^*\beta \equiv \gamma\alpha\gamma^{-1} \pmod{N}.$$

Proof. Note first that if $\alpha = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$, then $\beta\alpha^*\beta = \begin{pmatrix} w & y \\ z & x \end{pmatrix}$. Thus, if $\alpha \equiv \alpha_1 \pmod{N}$, then $\beta\alpha^*\beta \equiv \beta\alpha_1^*\beta \pmod{N}$.

Put $g = g_{\alpha,N}$, $m = \frac{N}{g}$, and let $\bar{x}$, $\tau = \tau(\alpha)$, $\delta = \delta(\alpha)$ be defined as in (21). By Proposition 37 there exists $\alpha_1 = \begin{pmatrix} 0 & \delta z' \\ z & \tau \end{pmatrix}$ with $zz' \equiv 1 \pmod{m}$ such that if $\alpha' = \bar{x}I + g\alpha_1$, then $\alpha' \equiv \gamma_1\alpha\gamma_1^{-1} \pmod{N}$, for some $\gamma_1 \in \text{SL}_2(\mathbb{Z})$. Then $\beta(\alpha')^*\beta = \bar{x}I + g\beta(\alpha_1)^*\beta$. Since $\beta(\alpha_1)^*\beta = \begin{pmatrix} \tau & \delta z' \\ z & 0 \end{pmatrix}$, it follows from Proposition 38 that there exists $\gamma_2 \in \text{SL}_2(\mathbb{Z})$ such that $\beta(\alpha')^*\beta \equiv \gamma_2\alpha'\gamma_2^{-1} \pmod{N}$. Now since $\alpha \equiv \gamma_1^{-1}\alpha'\gamma_1 \pmod{N}$, we have that $\beta\alpha^*\beta \equiv \beta(\gamma_1^{-1}\alpha'\gamma_1)^*\beta \pmod{N}$. 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 $\gamma_3 = \beta(\gamma_1^{-1})\beta \in \text{SL}_2(\mathbb{Z})$, and so $\beta\alpha^*\beta \equiv \gamma_3\beta(\alpha')^*\beta\gamma_3^{-1} \equiv \gamma_3\gamma_2\alpha'\gamma_2^{-1}\gamma_3^{-1} \equiv \gamma_3\gamma_2\gamma_1\alpha\gamma_1^{-1}\gamma_2^{-1}\gamma_3^{-1} \pmod{N}$, which shows that (26) holds with $\gamma = \gamma_3\gamma_2\gamma_1$.

In view of Proposition 38, 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 40 *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*

$$(27) \quad i_N(\tau, \delta) := [R_N^\times : S_N(\tau, \delta)] \leq 2^{\omega(\Delta_N)},$$

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

$$(28) \quad i_N(\tau, \delta) = 2^{\omega'(\Delta_N)}.$$

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

$$(29) \quad i_N(\tau, \delta) = \prod_{k=1}^r i_{p_k^{e_k}}(\tau, \delta).$$

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

$$(30) \quad S_{p_k^{e_k}}(\tau, \delta) = (R_{p_k^{e_k}}^\times)^2 \quad \text{and} \quad i_{p_k^{e_k}}(\tau, \delta) = 2, \quad \text{provided that } p_k \neq 2.$$

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

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

From the table in Nobs[No] and (29) we deduce:

Proposition 41 *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:*

$$(31) \quad i_N(\tau, \delta) = \begin{cases} 2^{\omega'(\Delta_N)} w_4(\tilde{\Delta}) & \text{if } 4||N, \\ 2^{\omega'(\Delta_N)} w_8(\tilde{\Delta}) & \text{if } 8|N, \end{cases}$$

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

We now apply the above results on conjugacy classes to refine Theorem 8 as follows.

Theorem 42 *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 (21), and let $z'_i \in \mathbb{Z}$ be such that $z_i z'_i \equiv 1 \pmod{m}$, for $1 \leq i \leq s$. Then there exist primitive matrices $\alpha_1, \dots, \alpha_s \in \mathcal{M}_d$ such that*

$$\beta\alpha_i \equiv \bar{x}I + g \begin{pmatrix} 0 & -\delta z'_i \\ z_i & \tau \end{pmatrix} \pmod{N}, \quad \text{for } 1 \leq i \leq s,$$

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

$$(32) \quad H(q) = \bigcup_{i=1}^s \bar{T}_{\alpha_i}^N,$$

and hence the number of irreducible components of $H(q)$ satisfies the estimate

$$(33) \quad |\text{Irr}(H(q))| \leq i_m(\tau, \delta) := [R_m^\times : S_m(\tau, \delta)].$$

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

Proposition 43 *Suppose that $\text{char}(K) \nmid N$ 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 $h \in \text{Hom}(E, E')$ of degree d such that if $\alpha' \in \mathcal{M}_d$ satisfies the relation*

$$(34) \quad (\psi^{-1}h)_{|E[N]} = \phi \circ [\beta\alpha']_N \circ \phi^{-1},$$

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

$$(35) \quad \text{tr}(\beta\alpha') \equiv \text{tr}(\beta\alpha) \pmod{Ng},$$

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

$$(36) \quad \tau_{\beta\alpha',N} \equiv \tau_{\beta\alpha,N} \pmod{m} \quad \text{and} \quad \delta_{\beta\alpha',N} \equiv \delta_{\beta\alpha,N} \pmod{m}.$$

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

Lemma 44 *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 $k\bar{x}_{\beta\alpha,N} \equiv 1 \pmod{N}$, and for any such k we have that*

$$(37) \quad r_{\beta\alpha,k,N} := -(\text{tr}(\beta\alpha) + kd(k^2d + 3))/g^2 \in \mathbb{Z}.$$

Proof. Since $\beta\alpha = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$ 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 $-2m\text{tr}(\beta\alpha) = 2mT = 2m(kd(k^2d + 3) + rg^2)$, where T is defined as in equation (6) of [K5], so we see that $r_{\beta\alpha,k,N} = r \in \mathbb{Z}$.

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

Proposition 45 *Let (E, E', ψ, π) be an N -presentation of $\langle J, \lambda \rangle \in \mathcal{A}_2(K)$, and let $h \in \text{Hom}(E, E')$ be a cyclic isogeny of degree $d \geq 1$. Assume that $\text{char}(K) \nmid N$. Then there exists $\alpha \in \mathcal{M}_d$ such that*

$$(38) \quad (\psi^{-1}h)_{|E[N]} = \phi \circ [\beta\alpha]_N \circ \phi^{-1},$$

holds for some level N -structure ϕ of E . If we fix a 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

$$(39) \quad m(rD_1 + D_2) \in \pi^* \text{NS}(J),$$

where $m = \frac{N}{g}$ and $r = r_{\beta\alpha,k,N}$. Moreover, $r \pmod{m}$ is uniquely determined by (39).

Proof. Fix a level N -structure ϕ . As in the proof of Proposition 28 of [K5], we see that $\phi^{-1} \circ \psi^{-1} \circ h_{|E[N]} \circ \phi \in \text{End}(E[N])$ 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 (38) holds. Note that by Lemma 44 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 (39) holds for some $r \in \mathbb{Z}$ which is uniquely determined mod m by (39). 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 43. Put $g = g_{\beta\alpha,N}$ and $m = \frac{N}{g}$. By Lemma 44 $\exists k \in \mathbb{Z}$ such that $k\bar{x}_{\beta\alpha,N} \equiv 1 \pmod{N}$. Fix such a k and put $r := r_{\beta\alpha,k,N}$ as in Lemma 44. Since $q_{-\alpha}^N = q_{\beta\alpha,N,d,k}$ in the notation of Proposition 11 of [K5], we have by equation (7) of [K5] that $q_{-\alpha}^N = q_{N,n,d,k,r}$. Thus $q_{\alpha}^N \sim q_{-\alpha}^N = q_{N,n,d,k,r}$.

Since $\langle J, \lambda \rangle \in H(q_{\alpha}^N)$, 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 $h : E \rightarrow E'$ 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 (39) 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 $\beta\alpha' = \begin{pmatrix} x' & y' \\ z' & w' \end{pmatrix}$, 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 (39), so by the uniqueness assertion of Proposition 45 we see that

$$r = r_{\beta\alpha,k,N} \equiv r_{\beta\alpha',k,N} \pmod{m}.$$

Thus $g^2 r_{\beta,k,N} \equiv g^2 r_{\beta\alpha',k,N} \pmod{Ng}$, and so (35) follows. In view of Lemma 46 below, this implies that (36) also holds.

Lemma 46 *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*

$$(40) \quad \text{tr}(\alpha_1) \equiv \text{tr}(\alpha_2) \pmod{Ng}, \quad \text{and} \quad \det(\alpha_1) \equiv \det(\alpha_2) \pmod{Ng},$$

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

$$(41) \quad \tau_{\alpha_1,N} \equiv \tau_{\alpha_2,N} \pmod{N} \quad \text{and} \quad \delta_{\alpha_1,N} \equiv \delta_{\alpha_2,N} \pmod{m}.$$

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

Proof of Theorem 42. The existence of $\alpha \in \mathcal{M}_d$ with $q_{\alpha}^N \sim q$ follows from Theorem 16 of [K5]. Thus $g_{\beta\alpha,N} = g$ by Proposition 23. Moreover, $\gcd(\bar{x}_{\beta\alpha,N}, g) = 1$, as we saw in the proof of Lemma 44.

Put $\bar{\alpha}_i := \bar{x}I + g \begin{pmatrix} 0 & -\delta z'_i \\ z_i & \tau \end{pmatrix}$. 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 $t := \text{tr}(\alpha)$, then $t = 2\bar{x} + 2\tau$ by (21), and

$$(42) \quad \text{tr}(\bar{\alpha}_i) = t \quad \text{and} \quad \det(\bar{\alpha}_i) \equiv -d \pmod{Ng}, \quad \text{for } 1 \leq i \leq s.$$

Indeed, $\text{tr}(\bar{\alpha}_i) = 2\bar{x} + g\tau = t$, and $\det(\bar{\alpha}_i) = \bar{x}^2 + \bar{g}\tau + g^2\delta z_i z_i^* \equiv \bar{x}^2 + \bar{g}\tau + g^2\delta \pmod{g^2m}$, so $\det(\bar{\alpha}_i) \equiv -d \pmod{g^2m}$ by the definition of δ . This proves (42).

It follows from (42) that $\det(\bar{\alpha}_i) \equiv -d \pmod{N}$, so by Lemma 30 of [K5] there exists a primitive matrix α'_i of determinant $-d$ such that $\alpha'_i \equiv \bar{\alpha}_i \pmod{N}$. Put $\alpha_i := \beta\alpha'_i$. Then $\alpha_i \in \mathcal{M}_d$, and $\beta\alpha_i = \alpha'_i \equiv \bar{\alpha}_i \pmod{N}$. This proves the existence of the matrices $\alpha_1, \dots, \alpha_s$.

To prove (32), let $k \in \mathbb{Z}$ be such that $k\bar{x} \equiv 1 \pmod{g}$, and put $t_i := -\text{tr}(\alpha_i) - dk^3(\det(\bar{\alpha}_i) + d)$. Then by (42) we see that $t_i \equiv -t \pmod{Ng}$, 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 $\beta\alpha_i \equiv \bar{\alpha}_i \pmod{N}$, 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 8 that $\bar{T}_{\alpha_i}^N \subset H(q)$. This proves that the right hand side of (32) 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 43 (and by Proposition 45) there exists an N -presentation (E, E', ψ, π) of (J, λ) , a cyclic isogeny $h : E \rightarrow E'$ of degree d and a matrix $\alpha' \in \mathcal{M}_d$ such that (34) 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 (34) shows that (ϕ, h, ϕ') is α' -compatible in the sense of (10), 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 21 that

$$(43) \quad \langle J, \lambda \rangle = \beta_{\alpha'}^N(x) \in \beta_{\alpha'}^N(X_{\alpha'}^N) = \bar{T}_{\alpha'}^N.$$

By the second part of Proposition 43 we know that $\beta\alpha'$ has the same invariants $g, \bar{x}, \tau, \delta$ as $\beta\alpha$. Thus, by Proposition 37 there exists $z \in R_m^{\times}$ and $\gamma_1 \in \text{SL}_2(\mathbb{Z})$ such that $\gamma_1\beta\alpha'\gamma_1^{-1} \equiv \alpha'' := \bar{x}I + g \begin{pmatrix} 0 & -\delta z' \\ z & \tau \end{pmatrix} \pmod{N}$, where $z'z \equiv 1 \pmod{m}$. Then $z \equiv z_k\sigma \pmod{m}$, for some k with $1 \leq k \leq s$ and $\sigma \in S_m(\tau, \delta)$ by our hypothesis on the z_i 's. Then by Lemma 35 and Proposition 38 there exists $\gamma_2 \in \text{SL}_2(\mathbb{Z})$ 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 $\bar{T}_{\alpha'}^N = \bar{T}_{\alpha_k}^N$, and so $\langle J, \lambda \rangle \in \bar{T}_{\alpha_k}^N$ by (43). This shows that opposite inclusion of (32) holds, and so concludes the proof of (32). From this (33) follows immediately since the $\bar{T}_{\alpha_i}^N$'s are irreducible (but not necessarily distinct) components of $H(q)$; cf. Remark 22 and Theorem 8.

Theorem 42 provides us with an upper bound for the number of irreducible components of $H(q)$; cf. (33). To go further and to compute the number of components *precisely* in the situation of Theorem 5(b) (or of Theorem 30) requires further work.

Indeed, although the previous section analyzed the SL_2 -conjugacy classes of matrices mod N , the conditions (4) and (19) 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 47 *Let q be binary form of type (N, m, d) which satisfies the condition (18) of Theorem 30, and let τ, δ be as in Theorem 42. If $\mathrm{char}(K) \nmid Nd$, then the number of irreducible components of $H(q)$ is given by the formula*

$$(44) \quad |\mathrm{Irr}(H(q))| = i_m(\tau, \delta) = [R_m^\times : S_m(\tau, \delta)],$$

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

$$(45) \quad [N^2, 0, 4d], \quad [N^2, N^2, (N^2 + 16d)/4], \quad [N^2, \varepsilon N^2, (\varepsilon^2 N^2 + 4d)/4],$$

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

$$(46) \quad |\mathrm{Irr}(H(q))| = i_m(t, \delta)/2.$$

Proof. Suppose that the $\bar{T}_{\alpha_i}^N$ constructed in Theorem 42 are not all distinct. Then there exists i and j with $1 \leq i < j \leq s$ such that $\bar{T}_{\alpha_i}^N = \bar{T}_{\alpha_j}^N$, so by Theorem 19 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

$$(47) \quad \gamma\beta\alpha_i\gamma^{-1} \equiv -\beta\alpha_j \pmod{N},$$

because the other case is ruled out by our choice of the α_k 's; cf. Proposition 38. Thus, since $\beta\alpha_k$ has the invariants $\bar{x}$, $\tau \pmod{m}$ and $\delta \pmod{m}$, for all k , it follows from (47) and Proposition 36 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 (47) and Proposition 38 we see that the residues of z_i and $-z_j \pmod{m}$ 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

$q \sim q_\alpha^N \sim [N^2, 0, 4d]$ 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 (45).

Case 2: $g = 2$.

Here $m = \frac{N}{2}$ and $\bar{x} = 1$, so $\bar{\alpha}_k = I + 2 \begin{pmatrix} 0 & -\delta z'_k \\ z_k & \tau \end{pmatrix}$, for all k , where $\bar{\alpha}_k$ is as in the proof of Theorem 42. (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 $2\tau_{-\bar{\alpha}_j, N} = \text{tr}(-\bar{\alpha}_j) - 2 = -\text{tr}(\bar{\alpha}_j) - 2 = -(2\tau + 2) - 2 = -2\tau - 4$, 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 (47) and Proposition 36 that

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

so $\tau \equiv -1 \pmod{m}$, and hence $t := \text{tr}(\beta\alpha) = 2\tau + 2 \equiv 0 \pmod{2m}$. Since $2m = N$, we thus see that $t \equiv \varepsilon N \pmod{2N}$, where $\varepsilon \in \{0, 1\}$, and so $q_\alpha^N = [N^2, Nt, (t^2 + 4d)/4] \sim q' := [N^2, \varepsilon N^2, (\varepsilon^2 N^2 + 4d)/4]$; 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 (45).

Now suppose that we are in the exceptional cases. Then $-1 \notin S_m(\tau, \delta)$, so $2|s = i_m(\tau, \delta)$. Choose $z_1, \dots, z_{\frac{s}{2}}$ 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 $k = \frac{s}{2} + 1, \dots, s$. Then $z_1, \dots, z_s$ satisfy the conditions of Theorem 42. Moreover, since $\bar{x}, g, \tau$ and δ satisfy the above conditions, we see that $\beta\alpha_k \equiv -\beta\alpha_{k + \frac{s}{2}} \pmod{N}$, for $1 \leq k \leq \frac{s}{2}$. Thus, $\bar{T}_{\alpha_k}^N = \bar{T}_{\alpha_{k + \frac{s}{2}}}^N$, for these k 's. On the other hand, by construction (and by Proposition 38) we have that $\gamma\beta\alpha_i\gamma^{-1} \not\equiv \pm\beta\alpha_j$, for any $\gamma \in \text{SL}_2(\mathbb{Z})$ and $1 \leq i < j \leq \frac{s}{2}$, so by Theorem 30 it follows that $\bar{T}_{\alpha_i}^N \neq \bar{T}_{\alpha_j}^N$, for $1 \leq i < j \leq \frac{s}{2}$, and so (46) follows.

Remark 48 As the above proof shows, even if the hypothesis (18) does not hold for q , but if $-1 \notin S_m(\tau, \delta)$ and q is equivalent to one of the forms of (45), then we still have the estimate

$$(48) \quad |\text{Irr}(H(q))| \leq i_m(\tau, \delta)/2.$$

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

Lemma 49 *If q has type (N, m, d) and if α, τ , and δ are as Theorem 42, then $q_\alpha^N = [N^2, 2mt, \Delta]$, where $t = \text{tr}(\beta\alpha)$ and $\Delta = \Delta(\tau, \delta) = \tau^2 - 4\delta$. Thus, if $\text{cont}(q) = \text{gcd}(a, b, c)$ denotes the content of $q = [a, b, c]$, then we have*

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

Proof. By definition, $q_\alpha^N = [N^2, 2mt, (t^2 + 4d)/g^2]$, so the first assertion follows from (22) because $\det(\beta\alpha) = -d$. Thus $\gcd(m, \text{cont}(q_\alpha^N)) = \gcd(m, N, 2mt, \Delta) = \gcd(m, \Delta)$. Since $q \sim q_\alpha^N$, we have that $\text{cont}(q) = \text{cont}(q_\alpha^N)$, and so the assertion follows.

Lemma 50 *Let $\tau, \delta \in \mathbb{Z}$ and let $m \geq 1$. 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 $p \mid \Delta_m(\tau, \delta)$.*

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

$$(49) \quad S_m(\tau, \delta) \simeq \prod_{i=1}^r S_{p_i^{e_i}}(\tau, \delta),$$

so $-1 \in S_m(\tau, \delta) \Leftrightarrow -1 \in S_{p_i^{e_i}}(\tau, \delta)$, for $1 \leq i \leq r$. Since $-1 \in S_2(\tau, \delta) = R_2^\times = \{1\}$ and since for an odd prime p we have by (30) that $-1 \notin S_{p^e}(\tau, \delta) \Leftrightarrow p \mid \Delta_{p^e}(\tau, \delta)$ and $(\frac{-1}{p}) = -1 \Leftrightarrow p \mid \Delta_{p^e}(\tau, \delta)$ and $p \equiv 3 \pmod{4}$, we see that the assertion follows.

We are now ready to prove the following refinement of Theorem 5.

Theorem 51 *Let q be a binary form of type (N, m, d) and assume that $4 \nmid c_m = \gcd(\text{cont}(q), m)$ and that $\text{char}(K) \nmid Nd$. Let $\omega' = \omega'(c_m) = |\{p \mid c_m : p \text{ is an odd prime}\}|$.*

- (a) *We always have that $|\text{Irr}(H(q))| \leq 2^{\omega'}$.*
- (b) *If there exists a prime $p \mid \gcd(N, d)$ with $p \equiv 3 \pmod{4}$ and if q is equivalent to one of the forms of (45), then then $|\text{Irr}(H(q))| \leq 2^{\omega'-1}$.*
- (c) *Suppose that q satisfies condition (18). If q satisfies the conditions of part (b), then equality holds in part (b), otherwise equality holds in part (a).*

Proof. By Lemma 49 we have that $c_m = \Delta_m(\tau, \delta)$, where τ and δ are as in Theorem 42, and so by (28) we have that $i_m(\tau, \delta) = 2^{\omega'}$ since $4 \nmid c_m$. Thus, part (a) follows from (33). Moreover, in the situation of part (b) we have that $-1 \notin S_m(\tau, \delta)$ by Lemma 50 and the fact that $p \mid c_m \Leftrightarrow p \mid \gcd(N, d)$ for the forms of (45), so part (b) follows from Remark 48. Finally, part (c) follows from Proposition 47.

Corollary 52 *If q is a binary form of type (N, m, d) with $c_m(q) \mid 2$, then $H(q)$ is irreducible, provided that $\text{char}(K) \nmid Nd$.*

Proof. Since $4 \nmid c_m = c_m(q)$ and $\omega'(c_m) = 0$, it follows from Theorem 51(a) that $|\text{Irr}(H(q))| \leq 2^0 = 1$, so $H(q)$ is irreducible.

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

Proposition 53 *If q has type $(2, m, d)$, and if $\text{char}(K) \nmid 2d$, 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 52 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 28.

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 also involves the quantities $w_4(\tilde{\Delta})$ and $w_8(\tilde{\Delta})$, as we saw in Proposition 41. 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) , so $c_m(q) := \gcd(m, \text{cont}(q)) = \gcd(m, c)$. If $4 \nmid c_m(q)$, then put $w(q) = 1$, and if $4|c_m(q)$, then put

$$(50) \quad w(q) = \begin{cases} w_4\left(\frac{c}{4}\right) & \text{if } 4||m, \\ w_8\left(\frac{c}{4}\right) & \text{if } 8|m. \end{cases}$$

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

Lemma 54 *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 . Then $c_m := \gcd(m, \text{cont}(q_\alpha^N)) = \gcd(m, \tau^2 - 4\delta)$, and we have that*

$$(51) \quad i_m(\tau, \delta) = 2^{\omega'(c_m)} w(q_\alpha^N).$$

Proof. By definition and (22) we have $q_\alpha^N = [N^2, 2mt, \Delta]$, where $t = \text{tr}(\beta\alpha)$ and $\Delta = \tau^2 - 4\delta$, and so $c_m = \gcd(m, \text{cont}(q_\alpha^N)) = \gcd(m, \Delta)$. Thus, if $4 \nmid c_m$, then (51) is just a restatement of formula (28) because $w(q_\alpha^N) = 1$ by definition. On the other hand, 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 in these cases (51) follows from formula (31).

It is useful to observe that the value of $w(q)$ depends only 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 55 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

$$(52) \quad \frac{c_1}{4} \equiv \frac{c_2}{4} \pmod{2^r},$$

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 $\gamma = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in \text{GL}_2(\mathbb{Z})$ such that $\gamma^t M(q_1) \gamma = M(q_2)$, where $M(q_i) = \begin{pmatrix} N^2 & mt_i \\ mt_i & c_i \end{pmatrix}$, for $i = 1, 2$. Thus

$$\begin{pmatrix} N^2 & mt_2 \\ mt_2 & c_2 \end{pmatrix} = \begin{pmatrix} N^2 x^2 + 2mt_1 xz + c_1 z^2 & N^2 xy + mt_1(wx + yz) + c_1 wz \\ N^2 xy + mt_1(wx + yz) + c_1 wz & N^2 y^2 + 2mt_1 wy + c_1 w^2 \end{pmatrix}.$$

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

$$(53) \quad c_1 z^2 \equiv 0 \pmod{4m} \quad \text{and} \quad c_1 w^2 \equiv c_2 \pmod{4m}.$$

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 (53), it follows that $\frac{c_1}{4} \equiv \frac{c_1}{4} w^2 \equiv \frac{c_2}{4} \pmod{2^r}$. Thus, (52) holds in this case.

Now suppose that $2|w$. Then $2 \nmid z$ because $\gcd(z, w) = 1$, so by the first equation of (53) we obtain that $c_1 \equiv c_1 z^2 \equiv 0 \pmod{2^{s+2}}$, where $s = v_2(m)$. Thus $\frac{c_1}{4} \equiv 0 \pmod{2^s}$, so by the second equation of (53) 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 (52) holds in all cases.

To prove the last assertion, suppose first that $4||m$, so $r = 2$. Since the value of $w_4(c_i/4)$ depends only on the residue class of $c_i/4 \pmod{4}$, we have $w_4(c_1/4) = w_4(c_2/4)$ by (52) 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 56 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].

Corollary 57 In the situation of Lemma 54 we have that

$$(54) \quad -1 \notin S_m(\tau, \delta) \quad \Leftrightarrow \quad \exists \text{ a prime } p|c_m \text{ with } p \equiv 3 \pmod{4} \text{ or } w(q_\alpha^N)^* > 1,$$

where $w(q_\alpha^N)^* = 1$, if $8|m$, $4|c_m$ and $\tilde{\Delta} = \frac{\tau^2 - 4\delta}{4} \equiv 2 \pmod{8}$, and $w(q_\alpha^N)^* = w(q_\alpha^N)$, otherwise.

Proof. If $4 \nmid c_m$, then the assertion follows from Lemma 50 because $\Delta_m(\tau, \delta) = c_m$ by the proof of Lemma 54. Thus, assume that $4 \mid c_m$. If there exists a prime $p \equiv 3 \pmod{4}$ with $p \mid c_m$, then the proof of Lemma 50 shows that $-1 \in S_m(\tau, \delta)$. Moreover, if $w(q_\alpha^N)^* > 1$, then $4 \mid c_m$ by the definition of $w(q_\alpha^N)^*$. If $8 \mid m$, then by the definitions of $w(q_\alpha^N)^*$ and of $w(q_\alpha^N) = w_8(\tilde{\Delta})$, where $\tilde{\Delta} := \frac{\tau^2 - 4\delta}{4}$, we see that $w(q_\alpha^N)^* > 1$ if and only if $\tilde{\Delta} \not\equiv 1, 2, 5 \pmod{8}$. Thus $-1 \notin S_m(\tau, \delta)$ in this case by Lemma 56(b). If $4 \parallel m$, then $w(q_\alpha^N)^* = w(q_\alpha^N) = w_4(\tilde{\Delta})$, so here $w(q_\alpha^N)^* > 1$ if and only if $\tilde{\Delta} \not\equiv 1, 2 \pmod{4}$, and hence $-1 \notin S_m(\tau, \delta)$ in this case by Lemma 56(a).

Conversely, if $-1 \notin S_m(\tau, \delta)$, then by (49) we must have that $-1 \notin S_{p_i^{e_i}}(\tau, \delta)$, for some $p_i^{e_i} \parallel m$. If $p_i > 2$, then $p_i \equiv 3 \pmod{4}$. If $p_i = 2$, then $4 \mid c_m$ by Lemma 50, and then Lemma 56 and the above analysis show that $w(q_\alpha^N)^* > 1$.

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

Theorem 58 *Let q be a binary form of type (N, m, d) and assume that $4 \mid c_m := c_m(q)$ and that $\text{char}(K) \nmid Nd$.*

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

(b) *Suppose that q is equivalent to either $[N^2, 0, 4d]$ or to $[N^2, N^2, \frac{N^2}{4} + 4d]$, where $4 \mid N$. 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 $4 \parallel N$ or if $\tilde{\Delta} \not\equiv 1, 2, 5 \pmod{8}$ when $8 \mid N$, then $|\text{Irr}(H(q))| \leq 2^{\omega'(c_m)-1} w(q)$.*

(c) *Suppose that q satisfies condition (18). 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 42. Then the assertion follows directly from (33) and Lemma 54.

(b) Suppose first $q \sim q_1 := [N^2, 0, 4d]$, so $\text{disc}(q) = -16N^2d$ and hence $m = N$. Note that $4 \mid c_m = \gcd(N, 4d) \Leftrightarrow 4 \mid N$. 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 (22). By (54) we see that $-1 \notin S_N(\tau, \delta)$ if and only if either there exists $p \equiv 3 \pmod{4}$ with $p \mid c_m = \gcd(N, 4d)$ or if $w(q_\alpha^M)^* > 1$. Since here $m = N$, the proof of Corollary 57 shows that the latter condition is equivalent to the condition that $d = \tilde{\Delta} \not\equiv 1, 2 \pmod{4}$, when $4 \parallel N$, and to $d = \tilde{\Delta} \not\equiv 1, 2, 5 \pmod{8}$, when $8 \mid N$. If this is the case, then the assertion (for $q \sim q_1$) follows from Remark 48 and Lemma 54.

Now suppose that $q \sim q_2 := [N^2, N^2, \frac{N^2}{4} + 4d]$. Here again $\text{disc}(q) = -16N^2d$, so $m = N$. Thus again $4 \mid c_m = \gcd(N, \frac{N^2}{4} + 4d) \Leftrightarrow 4 \mid N$, 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 47, and so by (46) and Lemma 51 we see that $|\text{Irr}(H(q))| = \frac{1}{2} i_m(\tau, \delta) = 2^{\omega'(c_m)-1} w(q)$.

Now assume that q is not as in part (b). We observe that the third case of (45) 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 $2 \mid N$, $\varepsilon \in \{0, 1\}$, and $d \equiv 1 + \varepsilon N \pmod{4}$. Indeed, since $\text{disc}(q_3) = -4N^2d$, we see that $m = \frac{N}{2}$, so $4 \nmid c_m = \gcd(\frac{N}{2}, d)$ because $d \equiv 1 \pmod{4}$ if $4 \mid N$.

From this (and the proof of part (b)) it follows that q does not satisfy the conditions of the exceptional case of Proposition 47 and so by (44) and Lemma 51 it follows that $\text{Irr}(H(q)) = i_m(\tau, \delta) = 2^{\omega'(c_m)} w(q)$.

We can now prove the remaining results stated in the introduction.

Proof of Theorem 5. The first assertion follows from Proposition 7 of [K5].

(a) This follows from Theorem 42 and (27). Alternately, if $4 \nmid c_m(q)$, then this follows from Theorem 51(a) and if $4 \mid c_m(q)$, then this follows from Theorem 58(a) because $w(q) \mid 2$ when $4 \mid m$.

(b) From Lemma 31 we know that the given hypothesis on d implies that condition (18) of Theorem 30 holds for q . Since $c_m(q) \mid N$ and $2 \nmid N$, we are thus in the situation of Theorem 51(c), and hence the assertion follows from that theorem because the last two cases of (45) do not occur when $2 \nmid N$.

Proof of Corollaries 6 and 7. The first corollary is the special case $c_m(q) = 1$ of Theorem 5(a). (Alternately, it is a special case of Corollary 52.)

To prove Corollary 7, let $q \in Q(N^2)$. Then by Theorem 1 we know that q has type (N, m, d) for some $m \mid N$ 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 primitively represents M and N^2 . Thus, the content $\text{cont}(q)$ of q divides N^2 and M , so $\text{cont}(q) = 1$ (because $\gcd(N, M) = 1$), and hence also $c_m(q) = \gcd(\text{cont}(q), m) = 1$. Thus $H(q)$ is irreducible by Corollary 6.

Proof of Theorem 11. If $N = 2$, then the assertion follows from Proposition 53, so assume that $N = 4$.

If $c_m \neq 4$, then the assertion follows from Corollary 52 because the condition $c_m \neq 4$ implies that $c_m \mid 2$ (since $c_m \mid N = 4$). Thus, assume that $c_m = 4$, so we are in the situation of Theorem 58. Moreover, we have that $m = 4$ and $4 \mid \text{cont}(q)$.

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 $4 \mid \text{cont}(q)$, we see that $2 \mid t$. Thus, $q \sim [16, 0, 4d]$ or $q \sim [16, 16, 4 + 4d]$, which are precisely the two exceptional cases of Theorem 58(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 (50).

If $\tilde{\Delta} \equiv 1, 2 \pmod{4}$, then $w(q) = w_4(\tilde{\Delta}) = 1$ by definition (cf. §6), and thus $|\text{Irr}(H(q))| \leq 2^0 = 1$ by Theorem 58(a), so $H(q)$ is irreducible in this case.

If $\tilde{\Delta} \not\equiv 1, 2 \pmod{4}$, then $w(q) = w_4(\tilde{\Delta}) = 2$ by definition, and thus $|\text{Irr}(H(q))| = \frac{1}{2} w(q) = 1$ by Theorem 58(b), so $H(q)$ is irreducible in this case as well. Thus, $H(q)$ is irreducible in all cases.

8 Examples

By using the above results, 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 59 (a) *The nontrivial intersections of H_1 with H_M for $M \leq 9$ are:*

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

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

(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 $\text{char}(K) \neq 2, 3, 5$.

Proof. Let q be a form which appears on the right hand side of the formula (7) 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 5.

(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 6 that they are irreducible if $\text{char}(K) \neq 2$.

(b) Here $N = 2$. By the classification of type $(2, m, d)$ (cf. the proof of Proposition 53) 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 53 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 28.

Remark 60 The method of analyzing the components of $H_{N^2} \cap H_M$ which was used in the proof of Proposition 59 can be extended to other cases, but the situation becomes more involved. On the one hand there are more forms to consider and on 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 13 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 $H_M = \emptyset$.

However, in order to obtain a complete table, we require another result which is proven in [K9]. To state the result, 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 61 *If q has type (N, m, d) , where N is an odd prime, and if $\text{char}(K) \nmid Nd$, then $H(q)$ has at most 2 irreducible components. Furthermore, if $N \equiv 1 \pmod{4}$, then*

$$(55) \quad H(q) \text{ is irreducible} \Leftrightarrow q \text{ is primitive, i.e., } \text{cont}(q) = 1,$$

whereas if $N \equiv 3 \pmod{4}$, then

$$(56) \quad H(q) \text{ is irreducible} \Leftrightarrow q \text{ is primitive or ambiguous.}$$

Using this, we obtain:

Proposition 62 *If $\text{char}(K) = 0$, 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:*

$N^2 \setminus M$	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 59. For $N \geq 3$ we use again Proposition 13 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 14.

For $N = 4$ all the $H(q)$'s appearing in $H_{16} \cap H_M$ are irreducible by Theorem 11.

For the cases $N = 3$ and $N = 5$ we apply Theorem 61. 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 61.

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 61 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.
- [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, Elliptic subcovers of hyperelliptic curves. *Math. Nachr.* **290** (2017), 2890–2900.
- [K7] E. Kani, Modular correspondences on $X(N)$. Preprint, 2017; 22 pp.
- [K8] E. Kani, Modular curves on Humbert surfaces. Preprint.
- [K9] E. Kani, The number of irreducible components of a generalized Humbert scheme. 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 $SL_2(\mathbb{Z}_p)$, insbesondere $SL_2(\mathbb{Z}_2)$. *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.