# The Number of Curves of Genus Two with Elliptic Differentials

*Ernst Kani**

## Introduction

Let $C$ be a curve of genus 2 defined over an algebraically closed field $K$, and suppose that $C$ admits a non-constant morphism $f : C \to E$ to an elliptic curve $E$. If $f$ does not factor over an isogeny of $E$, then we say that $f$ is an *elliptic subcover* of $C$. Note that this last condition imposes no essential restriction since every non-constant $f : C \to E$ factors over a unique elliptic subcover $f_{\min} : C \to E_{\min}$.

A classical theorem due to Picard [Pi] and Bolza [Bo] of 1882/86 states that a curve $C$ of genus 2 has either none, two or infinitely many elliptic subcovers. This is in part due to the fact that the elliptic subcovers occur in pairs. More precisely, given an elliptic subcover $f : C \to E$, there is a canonical "complementary" elliptic subcover $f' : C \to E'$ of the same degree $N := \deg(f) = \deg(f')$ which is characterized by the requirement that the induced maps on the associated Jacobian varieties fit into an exact sequence

$$0 \to J_E \xrightarrow{f^*} J_C \xrightarrow{f'_*} J_{E'} \to 0; \tag{1}$$

cf. [FK] or Kuhn [Ku]. This, therefore, naturally suggests the question of whether all pairs $(E, E')$ of elliptic curves and all integers $N \geq 2$ arise in this way:

**Question**. Given two elliptic curves $E$ and $E'$ over $K$ and an integer $N \geq 2$, does there exist a curve *of type* $(E, E', N)$, i.e. a curve $C$ of genus 2 which admits two elliptic subcovers

$$f : C \to E, \quad f' : C \to E',$$

of degree $N$ such that the associated sequence (1) is exact?

If the two elliptic curves $E$ and $E'$ are not isogenous (and if $\mathrm{char}(K) \nmid N$), then it is not difficult to see that the above question has a positive answer; a proof of this may be found in [FK], where the existence of such curves $C$ was exploited to study the arithmetic of elliptic curves. However, if the elliptic curves are isogenous, then this question becomes rather delicate and requires a much more careful analysis of the situation; this is the purpose of the present paper and of its sequel [Ka4].

*NSERC University Research Fellow

The basic difficulty here is that it seems to be extremely difficult to exhibit a curve $C$ of type $(E, E', N)$ explicitly. Nevertheless, it is possible to determine the *total number* $n(E, E', N)$ of such curves (counted with multiplicity according to their automorphisms), and this is the main object of this paper. This number is finite if $\mathrm{char}(K) \not| N$; in fact, it is easy to see that then

$$n(E, E', N) \leq sl(N) := \#\mathrm{Sl}_2(\mathbb{Z}/N\mathbb{Z}) = N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right),$$

and that equality holds if $E$ and $E'$ are not isogenous. In the general case, the exact value of $n(E, E', N)$ is given by a much more complicated formula (cf. Theorem 3.4 below); however, if $N$ is prime then this formula reduces to the following relatively simple expression:

**Theorem 1** *If $N$ is a prime number not equal to* $\mathrm{char}(K)$*, then the number of curves of genus* 2 *of type $(E, E', N)$ is given by the formula*

$$n(E, E', N) = sl(N) - \frac{1}{2} \sum_{k=1}^{N-1} h(E, E', k(N-k)), \tag{2}$$

*where $h(E, E', m)$ denotes the number of isogenies $h : E \to E'$ of degree $m$.*

**Remarks.** 1) As was already remarked, the above theorem is only a special case of Theorem (3.4) which treats not only the case of composite $N$'s but also those for which $\mathrm{char}(K)|N$. In the latter case the number $n(E_1, E_2, N)$ may be infinite.

2) In [Fr], G. Frey obtains a number of very interesting applications of Theorem 1 (and/or of Theorem 3 below). For example, he is able to construct curves $C$ of genus 2 over a given finite field $\mathbb{F}_q$ with the remarkable property that $C$ admits an infinite tower of *geometric* unramified galois extensions over $C$ (all defined over $\mathbb{F}_q$).

By analyzing the sum on the right hand side of (2), it is possible (cf. Theorem 4.4) to derive the following lower bound on $n(E, E', N)$.

**Theorem 2 ("Existence Theorem")** *If $N$ is a prime number not equal to* $\mathrm{char}(K)$ *and $E$ or $E'$ is not supersingular, then we have*

$$\frac{1}{6} sl(N) < n(E, E', N) \leq sl(N). \tag{3}$$

*Thus, in this situation there always exists a curve $C$ of genus* 2 *of type $(E, E', N)$.*

In particular, we see that the above question has a positive answer whenever $N$ is prime and $\mathrm{char}(K) = 0$. In the sequel [Ka4] it will be shown that the above estimate is still true whenever $\mathrm{char}(K) \not| N$, as long as either $j(E) \neq 0$ or $E$ is not supersingular. In addition, the exceptional cases are analyzed further there.

The starting point of the proof of Theorem 1 is the "basic construction" of curves of genus 2 with elliptic subcovers which was explained in [FK] (cf. also [Ka1] or [Ka2]) and which is recalled in section 1 below. In this construction, each curve $C$ of type $(E, E', N)$ is constructed from the data $(E, E', \psi)$, where $\psi : E[N] \xrightarrow{\sim} E'[N]$

is an isomorphism of the groups of $N$-torsion points of $E$ and $E'$; more precisely, $\psi$ has to be an *anti-isometry* with respect to the Weil pairings. However, not every such triplet $(E, E', \psi)$ gives rise to a (smooth, irreducible) curve of genus 2 in this way, for the curve $C_\psi$ constructed by this procedure may turn out to be *reducible*. The cornerstone of this paper, therefore, is an analysis the *reducible* anti-isometries $\psi$; cf. Definition 1.2. It turns out that $\psi$ is reducible if and only if $\psi$ is "induced" by a suitable isogeny $h : E \to E'$. In the case that $N$ is prime, this may be formulated as follows (cf. Remark 2.5 below):

**Theorem 3 ("Reducibility Criterion")** *If $N$ is prime, then $\psi : E[N] \to E'[N]$ is reducible if and only if there is an isogeny $h : E \to E'$ of degree $k(N-k)$, for some $1 \leq k < N$, such that*

$$\psi \circ [k] = h \mid_{E[N]} .$$

If $N$ is composite, then a similar but more complicated result holds, for then one has to study those isogenies $h$ which admit two *factorizations* $h = h'_1 \circ h_1 = h'_2 \circ h_2$ that form a diamond (or square); such are called "isogeny diamond factorizations"; cf. Definition 2.1 and Theorem 2.6 for the precise definition and statement.

Even though Theorem 1 presents an explicit formula for $n(E, E', N)$, the task of extracting from this the lower bound (3) still requires considerable work, for naive estimates of the right hand side of (2) tend to be negative if $\mathrm{Hom}(E, E')$ is large. To circumvent this problem we prove the following "mass formula" which shows that "on average" the number $r(E, E', N)$ $(= sl(N) - n(E, E', N)$, if $\mathrm{char}(K) \nmid N)$ of reducible anti-isometries is much smaller than $sl(N)$ (cf. Theorem 4.1):

**Theorem 4 ("Mass Formula")** *Let $E$ be an elliptic curve over $K$. Then*

$$\sum_{E'} \frac{r(E, E', N)}{\#\mathrm{Aut}(E')} = \frac{1}{2} \sum_{k=1}^{N-1} \sigma(E, k(N-k), N), \tag{4}$$

*where the sum on the left extends over a system of representatives of the isomorphism classes of elliptic curves $E'/K$, and $\sigma(E, m, N)$ denotes the number of subgroups $H \leq E$ with $\#H = m$ and $E[q] \not\leq H$, for all primes $q \mid N$.*

Finally, it is perhaps useful to add some historical remarks. Indeed, curves with elliptic subcovers have a long history, dating back to Legendre and Jacobi, who wrote down the first examples in 1832. Later they were studied extensively by Bolza, Humbert, Picard, Poincaré, and many others, as is documented in chapter XI of Krazer's book [Kr]. At that time the main focus was on the associated *elliptic differential* $\omega = f^*\omega_E$, where $\omega_E$ denotes the holomorphic differential on $E$; for this reason such curves are often referred to as "curves with an elliptic differential". In more recent times, various aspects of these curves were studied by Hayashida and Nishi [HN], Lange [La1] (see also [La2]), Ibukiyama, Katsura and Oort [IKO], Kuhn [Ku], Murabayashi [Mur], and by Kani [Ka1], [Ka3]. Arithmetic applications of such curves were given by Moret-Bailly [MB], Serre [Se2], [Se3] and by [FK], [Ka2].

As should be evident already, this paper developed out of the joint work [FK] with G. Frey, whom I would like to thank very much for the many stimulating and fruitful discussions as well as for his continued interest in this research. In addition, I have benefitted from discussions with A. Brumer, I. Kiming, B. Mazur, F. Oort and J.-P. Serre on this topic. Above all, I would like to thank the referee for his careful reading of this paper and for his astute suggestions which greatly clarified and shortened the article. Finally, I would like to gratefully acknowledge support from the Natural Sciences and Engineering Research Council of Canada (NSERC).

# 1 Review of the basic construction

In this section we briefly outline the basic construction of curves of genus 2 with elliptic differentials (or subcovers) of degree $N$. This method was sketched in [FK] and was generalized in [Ka1] in order to construct the moduli space of curves of genus $g \geq 2$ with elliptic differentials.

Throughout, let $K$ be an algebraically closed field of arbitrary characteristic. Suppose first that $C$ is a smooth, projective curve of genus 2 over $K$ which admits a surjective morphism $f : C \to E$ to an elliptic curve $E$. Without essential loss of generality, we may assume that $f$ is *minimal* (or *maximal* [Se1] or *optimal* [Ku]) in the sense that $f$ does not factor over an isogeny or, equivalently, that the induced homomorphism $f^* : J_E \to J_C$ is closed immersion; we then say that $f : C \to E$ is an *elliptic subcover*. By duality, the kernel of the dual map $f_* = (f^*)\hat{} : \hat{J}_C \simeq J_C \to \hat{J}_E \simeq J_E$ is connected, and hence is (the Jacobian of) an elliptic curve $E'$; viz. $J_{E'} = \mathrm{Ker}(f_*)$. If we dualize the inclusion map $i : J_{E'} \hookrightarrow J_C$ and compose it with the "canonical map" $j : C \hookrightarrow J_C \simeq \hat{J}_C$, then we obtain a finite morphism $f' = \hat{i} \circ j : C \to \hat{J}_{E'} = E'$ which, as one easily checks, induces the exact sequence

$$0 \to J_E \xrightarrow{f^*} J_C \xrightarrow{f'_*} J_{E'} \to 0;$$

note that $f'$ is uniquely determined by this property up to isomorphism. It is then not difficult to see that

$$f^* J_E[N] = f'^* J_{E'}[N] = f^* J_E \cap f'^* J_{E'}, \tag{1.1}$$

where $J_E[N] = \mathrm{Ker}([N]_{J_E})$ denotes the subgroup scheme of $N$-torsion points of $J_E$. From this one concludes that $N := \deg(f) = \deg(f')$, and that there is a unique isomorphism $\psi = \psi_f : J_E[N] \xrightarrow{\sim} J_{E'}[N]$ such that

$$f^*_{|J_E[N]} = (f')^* \circ \psi. \tag{1.2}$$

Then $\psi$ is automatically an anti-isometry with respect to the $e_N$-pairings on $E$ and on $E'$:

$$e_N(\psi(x), \psi(y)) = e_N(x, y)^{-1}, \ \ \forall x, y \in J_E[N],$$

and this condition is equivalent to the assertion that the "graph subgroup scheme" $H_\psi = \mathrm{Graph}(\psi) \leq (J_E \times J_{E'})[N]$ is a (maximal) isotropic subgroup of $(J_E \times J_{E'})[N]$ (with respect to the $e_N$-pairing on $A = J_E \times J_{E'}$).

As was mentioned in the introduction, we want to calculate the number of elliptic coverings of fixed *type* $(J_E, J'_E, N)$. For this, we shall study the finer "invariant" $\psi : J_E[N] \to J_{E'}[N]$ which is in fact a *complete invariant* since the elliptic covering can be reconstructed from the data $(J_E, J_{E'}, \psi)$. Unfortunately, not every anti-isometry $\psi$ gives rise to an elliptic covering and so the basic problem here is to identify those that do. This will be done in two steps. First we show that these $\psi$ are precisely those which are *irreducible* in the sense defined below, and then we analyze in the next section the structure of the *reducible* anti-isometries.

The definition of a reducible/irreducible anti-isometry is somewhat indirect since it depends on the following general identification.

**Proposition 1.1** *Let $A$ be an abelian variety of dimension $d$ with a principal polarization $\lambda = \lambda_\Theta : A \xrightarrow{\sim} \widehat{A}$ defined by an ample divisor $\Theta \in \mathrm{Div}(A)$, and let $p : A \to A'$ be an isogeny. Then the following conditions are equivalent:*

*a)* $\mathrm{Ker}(p)$ *is a maximally isotropic subgroup of $A[N] = K(N\Theta)$ with respect to the symplectic pairing $e^{N\Theta}$.*

*b)* $\deg(p) = N^d$ *and there exists $\Theta' \in \mathrm{Div}(A')$ such that $p^*\Theta' \sim N\Theta$.*

*c) There is a principal polarization $\lambda' : A' \to \widehat{A'}$ such that $\hat{p} \circ \lambda' \circ p = [N] \circ \lambda$.*

*Furthermore, the map $p \mapsto \mathrm{Ker}(p)$ establishes a bijection between*

*(1) the set of equivalence classes of pairs $(p, \lambda')$ where $p : A \to A'$ is an isogeny and $\lambda'$ is a principal polarization on $A'$ satisfying condition c), and*

*(2) the set of maximally isotropic subgroups of $A[N]$.*

*Here, two pairs $(p, \lambda')$ and $(p', \lambda'')$ are said to be equivalent if there is an isomorphism $\varphi : A' \xrightarrow{\sim} A''$ such that $p' = \varphi \circ p$ and $\lambda' = \hat{\varphi} \circ \lambda'' \circ \varphi$.*

*Proof.* a) $\Leftrightarrow$ b): Since $\Theta$ defines a principal polarization, we have $K(N\Theta) = A[N]$, and so by Mumford[Mu], p. 231 we see that $H := \mathrm{Ker}(p)$ is an isotropic subgroup of $A[N] \Leftrightarrow \exists \Theta' \in \mathrm{Pic}(A')$ such that $p^*\Theta' \sim N\Theta$. Furthermore, by [Mu], p. 233 we have that $H$ is maximally isotropic if and only if $\#H = \#K(N\Theta)^{\frac{1}{2}} = N^d$.

b) $\Rightarrow$ c): Let $\lambda' = \lambda_{\Theta'} : A' \to \widehat{A'}$ be the polarization defined by $\Theta'$. By [Mu], p. 232, we have $K(\Theta') = H^\perp/H = \{0\}$ since $H = \mathrm{Ker}(p)$ maximally isotropic, and so $\lambda'$ is a principal polarization. Furthermore, we have $\hat{p} \circ \lambda_{\Theta'} \circ p = \lambda_{p^*\Theta'} = \lambda_{N\Theta} = [N] \circ \lambda_\Theta$, the latter by the Theorem of the Square. Thus, $\lambda'$ satisfies the conditions of c).

c) $\Rightarrow$ a): The formula of c) shows that $H := \mathrm{Ker}(p) \leq A[N]$. Furthermore, since $\lambda' = \lambda_{\Theta'}$ for some $\Theta' \in \mathrm{Pic}(A')$, we have $\lambda_{p^*\Theta'} = \hat{p} \circ \lambda' \circ p = \lambda_{N\Theta}$. Thus $p^*\Theta' \equiv N\Theta$, and so it follows from the functorial properties of $e^{\mathcal{L}}$([Mu], p. 228, particularly properties (1) and (3)) that $H$ is isotropic with respect to $e^{N\Theta}$. Finally, since

$\deg(\hat{p}) \cdot \deg(p) = \deg([N]) = N^{2d}$ and $\deg(\hat{p}) = \deg(p)$, we have that $\deg(p) = N^d$, and so $H$ is maximally isotropic.

Finally, suppose that $p : A \to A'$ and $p' : A \to A''$ are two isogenies satifying the above conditions with $\lambda' = \lambda_{\Theta'} : A' \to \widehat{A'}$ and $\lambda'' = \lambda_{\Theta''} : A'' \to \widehat{A''}$. If $\mathrm{Ker}(p) = \mathrm{Ker}(p')$, then there is a unique isomorphism $\varphi : A' \to A''$ such that $p' = \varphi \circ p$. Then as above one has $p^*\Theta' \equiv N\Theta \equiv (p')^*\Theta'' = p^*(\varphi^*\Theta'')$. Thus, applying $p_*$ we obtain $\deg(p)\Theta' \equiv \deg(p)\varphi^*(\Theta'')$, and so $\Theta' \equiv \varphi^*(\Theta'')$ since the Neron-Severi group $NS(A')$ has no torsion. But this means that $\widehat{\varphi} \circ \lambda'' \circ \varphi = \lambda'$, and so the last assertion follows.

**Definition 1.2** Let $(A, \lambda)$ be a principally polarized abelian surface and $H \leq A[N]$ be a maximally isotropic subgroup. Then $H$ is called *reducible* if the unique principal polarization $\lambda_H$ on $A_H = A/H$ defined by $H$ (and $\lambda$) via Proposition 1.1 is a *product polarization*, i.e. if there is an isomorphism $\varphi : (A_H, \lambda_H) \xrightarrow{\sim} (E_1 \times E_2, \lambda_{E_1,E_1})$ of polarized abelian varieties to a product surface $E_1 \times E_2$ with product polarization $\lambda_{E_1,E_2} = \lambda_{\Theta_{E_1,E_2}}$, where $\Theta_{E_1,E_2} = pr_1^*(0_{E_1}) + pr_2^*(0_{E_2})$.

Furthermore, an anti-isometry $\psi : E[N] \to E'[N]$ is called *reducible* if its graph subgroup $H_\psi = \mathrm{Graph}(\psi) \leq A[N]$ is has this property with repect to the product polarization $\lambda_{E,E'}$ on $A = E \times E'$.

**Remark 1.3** The justification for the above terminology lies in a theorem of Weil [We] from which it follows that a principally polarized abelian surface $(A, \lambda_\Theta)$ is isomorphic to a product surface $(E_1 \times E_2, \lambda_{E_1,E_2})$ if and only if the associated theta divisor $\Theta$ is reducible.

**Example 1.4** Let $\psi = \psi_f : J_E[N] \to J_{E'}[N]$ be the anti-isometry associated to an elliptic covering $f : C \to E$ as above. Then by (1.1) and (1.2) we have $H_\psi = \mathrm{Ker}(\pi)$, where $\pi := f^* + (f')^* : J_E \times J_{E'} \to J_C$ and by the discussion of [FK], p. 157, we see that $\hat{\pi} \circ \lambda_C \circ \pi = [N]\lambda_{J_E,J_{E'}}$, where $\lambda_C$ is the canonical polarization of $J_C$ defined by $C$. Since $C$ is irreducible by hypothesis, $\lambda_C$ cannot be a product polarization, and hence $\psi_f$ is irreducible.

Conversely, if $\psi : J_E \to J_{E'}$ is an irreducible anti-isometry, then by Weil's theorem ([We], Satz 2), its associated principally polarized quotient variety $(J_\psi, \lambda_\psi)$ *is* the Jacobian of a smooth curve $C$ of genus 2 which, as is easy to see, has type $(J_E, J_{E'}, N)$ (cf. [FK]). We have thus sketched the proof of the following result (which is implicit in [FK] but is explicitly stated in [Ka1]):

**Theorem 1.5** *Fix elliptic curves $E$ and $E'$ over $K$ and an integer $N \geq 2$. Then the assignment*

$$(f : C \to E) \mapsto (\psi_f : J_E[N] \to J_{E'}[N])$$

*induces a bijection between the set $\mathcal{M}(E, E', N)$ of isomorphism classes of elliptic subcovers $f : C \to E$ of type $(J_E, J_{E'}, N)$ and the set $\overline{\mathcal{I}}(J_E, J_{E'}, N)$ of isomorphism classes of irreducible anti-isometries $\psi : J_E[N] \to J_{E'}[N]$.*

# 2 The Reducibility Criterion

The above Theorem 1.5 reduces the problem of constructing curves of genus 2 of prescribed type $(E_1, E_2, N)$ to the problem of finding anti-isometries $\psi : E_1 \to E_2$ which are irreducible, and so we require an overview of such anti-isometries. As a first step, we classify here more generally all the reducible maximally isotropic subgroups $H \leq (E_1 \times E_2)[N]$ which are *non-diagonal*, i.e. $H \neq H_1 \times H_2$, where $H_i \leq E_i$; the second step consists in identifying those that come from anti-isometries. It turns out that these are closely related to factorizations of isogenies $f : E_1 \to E_2$, and for this reason we introduce the following terminology.

**Definition 2.1** Let $E_1$ and $E_2$ be two elliptic curves over $K$ and $N \geq 2$ be an integer. An *isogeny factorization configuration of order $N$* from $E_1$ to $E_2$ is a triplet $(f, H_1, H_2)$ consisting of an isogeny $f : E_1 \to E_2$ and two subgroup schemes $H_1, H_2 \leq \mathrm{Ker}(f)$ such that

$$\#H_1 + \#H_2 = N \quad \text{and} \quad \#H_1 \cdot \#H_2 = \deg(f), \tag{2.1}$$

where $\#H_i$ denotes the order (or rank) of the subgroup scheme $H_i$. If, in addition we have $H_1 \cap H_2 = \{0\}$, then we say that $(f, H_1, H_2)$ is an *isogeny diamond configuration*. Two isogeny factorization configurations $(f, H_1, H_2)$ and $(f', H_1', H_2')$ are said to be *equivalent*, i.e. $(f, H_1, H_2) \sim (f', H_1', H_2')$, if and only if either $f' = -f, H_1' = H_2$ and $H_2' = H_1$ or if $f' = f, H_1' = H_1$ and $H_2' = H_2$.

**Remark 2.2** If $f : E_1 \to E_2$ is any isogeny which has two factorizations

$$f = f_1' \circ f_1 = f_2' \circ f_2 \quad \text{such that} \quad \deg(f_1) = \deg(f_2'), \tag{2.2}$$

where $f_i : E_1 \to E_i'$ and $f_i' : E_i' \to E_2$ are suitable isogenies, then $(f, \mathrm{Ker}(f_1), \mathrm{Ker}(f_2))$ is an isogeny factorization configuration of order $N := \deg(f_1) + \deg(f_2)$. Conversely, each isogeny factorization configuration arises in this way, for the condition $H_i \leq \mathrm{Ker}(f)$ means that $f$ factors over $f_i : E_1 \to E_i' = E_1/H_i$, and $f_i$ is uniquely defined by $H_i$ up to isomorphism. We call the collection $(f, f_1, f_1', f_2, f_2')$ an *isogeny factor set* representing $(f, H_1, H_2)$.

**Theorem 2.3 ("Reducibility Theorem")** *Let $E_1$ and $E_2$ be two elliptic curves over $K$ and let $N \geq 2$ be an integer. Then there is a natural bijection between*

*a) the set $\overline{\mathcal{IFC}}(E_1, E_2, N)$ of equivalence classes of isogeny factorization configurations $(f, H_1, H_2)$ of order $N$ from $E_1$ to $E_2$, and*

*b) the set $\mathcal{NRI}(E_1, E_2, N)$ of non-diagonal, reducible, maximally isotropic subgroups $H \leq (E_1 \times E_2)[N]$.*

*Proof.* We first construct a map $\eta : \overline{\mathcal{IFC}}(E_1, E_2, N) \to \mathcal{NRI}(E_1, E_2, N)$ and then show that it is bijective. For this, let $\mathbf{f} := (f, f_1, f_1', f_2, f_2')$ be an isogeny factor set

representing the isogeny factorization configuration $(f, H_1, H_2)$ as in Remark 2.2, and define the isogeny $p := p_{\mathbf{f}} : E_1 \times E_2 \to E_1' \times E_2'$ by the rule

$$p(x_1, x_2) = (f_1(x_1) - \widetilde{f_1'}(x_2), f_2(x_1) + \widetilde{f_2'}(x_2)),$$

where $\widetilde{f_i'} := \lambda_{E_i}^{-1} \circ \widehat{f_i'} \circ \lambda_{E_2} : E_2 \to E_i'$ denotes the "dual map" of $f_i'$.

We first claim that $H_{\mathbf{f}} = \mathrm{Ker}(p_{\mathbf{f}})$ is a reducible, maximally isotropic subgroup of $A[N]$ with respect to the product polarization $\lambda_{E_1,E_2}$ on $A = E_1 \times E_2$. For this, we observe that by Proposition 1.1 and the definition of reducibility, it is enough to show that

$$\widehat{p} \circ \lambda_{E_1',E_2'} \circ p = \lambda_{E_1,E_2} \circ [N]_A. \tag{2.3}$$

To verify this equation, we first note that it is equivalent to the matrix equation

$$\widetilde{M}(p) \cdot M(p) = \mathrm{diag}([N]_{E_1}, [N]_{E_2}), \tag{2.4}$$

where, for any isogeny $p \in Hom(E_1 \times E_2, E_1' \times E_2')$ with matrix $M(p) = \left(\begin{smallmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{smallmatrix}\right)$, where $p_{ij} \in Hom(E_j, E_i')$, the *adjoint matrix* $\widetilde{M}(p)$ is defined by $\widetilde{M}(p) = \left(\begin{smallmatrix} \widetilde{p_{11}} & \widetilde{p_{21}} \\ \widetilde{p_{12}} & \widetilde{p_{22}} \end{smallmatrix}\right)$. Indeed, if $\widetilde{p} \in Hom(E_1' \times E_2', E_1 \times E_2)$ is the isogeny defined by the matrix $\widetilde{M}(p)$, then the equivalence of these two formulae follows immediately from the well-known formula

$$\widetilde{p} = \varphi_A \circ \widetilde{p} \circ \varphi_{A'}^{-1},$$

in which $\varphi_A : \widehat{A} \to \widehat{E}_1 \times \widehat{E}_2$ is the canonical isomorphism such that $\varphi_A \circ \lambda_{E_1,E_2} = \lambda_{E_1} \times \lambda_{E_2}$ and $\varphi_{A'}$ is defined similarly for $A' = E_1' \times E_2'$.

It thus remains to verify (2.4) for $p = p_{\mathbf{f}}$. Now since by definition

$$M(p_{\mathbf{f}}) := \begin{pmatrix} f_1 & -\widetilde{f_1'} \\ f_2 & \widetilde{f_2'} \end{pmatrix}, \quad \text{we see that} \quad \widetilde{M}(p_{\mathbf{f}}) = \begin{pmatrix} \widetilde{f_1} & \widetilde{f_2'} \\ -f_1' & f_2' \end{pmatrix},$$

and hence (2.3) and (2.4) are equivalent to the equations

$$\widetilde{f_1} \circ f_1 + \widetilde{f_2} \circ f_2 = [\deg(f_1)]_{E_1} + [\deg(f_2)]_{E_1} = [N]_{E_1} \tag{2.5}$$

$$\widetilde{f_1} \circ (-\widetilde{f_1'}) + \widetilde{f_2} \circ \widetilde{f_2'} = 0 \tag{2.6}$$

$$(-f_1') \circ f_1 + f_2' \circ f_2 = 0 \tag{2.7}$$

$$(-f_1') \circ (-\widetilde{f_1'}) + f_2' \circ \widetilde{f_2'} = [\deg(f_1')]_{E_2} + [\deg(f_2')]_{E_2} = [N]_{E_2}. \tag{2.8}$$

Now these equations hold by definition of an isogeny factor set: (2.5) is true since $\deg(f_1) + \deg(f_2) = N$, (2.6) and (2.7) hold by the factorization property, and (2.8) is valid because $\deg(f_1') = \deg(f_2)$ and $\deg(f_2') = \deg(f_1)$, and hence $\deg(f_1') + \deg(f_2') = N$.

Thus, $H_{\mathbf{f}}$ is a reducible, maximally isotropic subgroup of $A[N]$. In addition, $H_{\mathbf{f}}$ is not diagonal, for if $H_{\mathbf{f}} = H_1' \times H_2'$ with $H_i' \leq E_i$, then $\mathrm{Ker}(f_1) \geq H_1'$ and $\mathrm{Ker}(\widetilde{f_2'}) \geq H_2'$. But since $\#H_{\mathbf{f}} = N^2$, we must have either $\#H_1' \geq N$ or $\#H_2' \geq N$, which is a contradiction since $\deg(f_1) = N - \deg(f_2) < N$ and $\deg(\widetilde{f_2'}) = \deg(f_1) < N$.

Next we note that the subgroup $H_{\mathbf{f}}$ depends only on $(f, H_1, H_2)$ and not the representative $\mathbf{f}$. Indeed, if $\mathbf{g} = (g, g_1, g_1', g_2, g_2')$ is another such representative, then $f = g$ and there are two isomomorphisms $\varphi_i$ such that $g_i = \varphi_i \circ f_i$ and $g_i' = f_i' \circ \varphi_i^{-1}$, and so we have $p_{\mathbf{g}} = (\varphi_1 \times \varphi_2) \circ p_{\mathbf{f}}$ and $H_{\mathbf{f}} = H_{\mathbf{g}}$.

In addition, if $-\mathbf{f} := (-f, -f_2, f_2', -f_1, f_1')$, then we have $p_{-\mathbf{f}} = -\tau \circ p_{\mathbf{f}}$, where $\tau : E_1' \times E_2' \to E_2' \times E_1'$ is the isomorphism which interchanges the two factors, and so in particular $H_{-\mathbf{f}} = H_{\mathbf{f}}$. This, therefore, shows that the assignment $\mathbf{f} \mapsto H_{\mathbf{f}}$ is compatible with the above equivalence relation and hence induces the desired map $\eta : \overline{\mathcal{IFC}}(E_1, E_2, N) \to \mathcal{NRI}(E_1, E_2, N)$.

To show that $\eta$ is injective, let $\mathbf{f}$ and $\mathbf{g}$ be two isogeny factor sets such that $\mathrm{Ker}(p_{\mathbf{f}}) = \mathrm{Ker}(p_{\mathbf{g}})$. Then, since $p_{\mathbf{f}}$ and $p_{\mathbf{g}}$ both satisfy (2.3), it follows from Proposition 1.1 that there is an isomorphism $\varphi$ such that $p_{\mathbf{g}} = \varphi \circ p_{\mathbf{f}}$ and $\lambda_{E_1', E_2'} = \hat{\varphi} \circ \lambda_{E_1'', E_2''} \circ \varphi$. But any such $\varphi$ either has the form $\varphi = \varphi_1 \times \varphi_2$ with $\varphi_i \in Hom(E_i', E_i'')$, or the form $\varphi = \tau \circ \varphi_1 \times \varphi_2$ $(= -\tau \circ (-\varphi_1) \times (-\varphi_2))$ with $\varphi_1 : E_1' \xrightarrow{\sim} E_2''$ and $\varphi_2 : E_2' \xrightarrow{\sim} E_1''$. Now from the previous discussion it follows that in the first case $\mathbf{f}$ and $\mathbf{g}$ define the same isogeny factorization configuration, whereas in the second case they define equivalent configurations, and so $\eta$ is injective.

Finally we show that $\eta$ is surjective. Thus, let $H \in \mathcal{NRI}(E_1, E_2, N)$ be a non-diagonal, reducible, maximally isotropic subgroup of $A[N]$. Then by definition there is an isogeny $p : A = E_1 \times E_2 \to A' = E_1' \times E_2'$ satisfying (2.3) such that $H = \mathrm{Ker}(p)$. Let $M(p) = \left(\begin{smallmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{smallmatrix}\right)$ be the matrix associated to $p$, and put $f_1 = p_{11}$, $f_2 = p_{21}$, $f_1' = -\widetilde{p_{12}}$, and $f_2' = \widetilde{p_{22}}$. In addition, put $f = f_1' \circ f_1$. We claim that $\mathbf{f} := (f, f_1, f_1', f_2, f_2')$ is an isogeny factor set of order $N$. Indeed, since $p$ satisfies (2.3), it follows that the formulae (2.5) – (2.8) hold for $f_1, f_1', f_2, f_2'$. From (2.7) we see that $f := f_1' \circ f_1 = f_2' \circ f_2$, and from (2.5) we have $\deg(f_1) + \deg(f_2) = N$. Furthermore, since $N(N - (\deg(f_2) + \deg(f_2'))) = (N - \deg(f_2))(N - \deg(f_2')) - \deg(f_1)\deg(f_1') = 0$ by (2.7) and (2.5),(2.8), we see that $\deg(f_2) + \deg(f_2') = N$, and hence $\deg(f_1) = \deg(f_2')$ by (2.5). Finally, $f$ is an isogeny, for if $f_1 = 0$, then also $f_2' = 0$ and then $\mathrm{Ker}(p)$ is a diagonal subgroup, and we obtain a similar contradiction if $f_1' = 0$. This shows that $\mathbf{f}$ is an isogeny factor set of order $N$, and hence $\eta$ is bijective.

**Corollary 2.4** *If $\mathbf{f} = (f, f_1, f_1', f_2, f_2')$ is any isogeny factor set of order $N$ with $\mathrm{Ker}(f_1) \cap \mathrm{Ker}(f_2) = (0)$, then there is a unique reducible anti-isometry $\psi = \psi_{\mathbf{f}} : E_1[N] \to E_2[N]$ such that*

$$\widetilde{f_1'} \circ \psi = f_{1|E_1[N]} \quad \text{and} \quad \widetilde{f_2'} \circ \psi = -f_{2|E_1[N]}, \tag{2.9}$$

*and every reducible anti-isometry arises in this way. Thus, the bijection of Theorem 2.3 restricts to a bijection between*

*a) the set $\overline{\mathcal{IDC}}(E_1, E_2, N)$ of equivalence classes of isogeny diamond configurations of order $N$ from $E_1$ to $E_2$, and*

*b) the set $\mathcal{R}(E_1, E_2, N)$ of reducible anti-isometries $\psi : E_1[N] \to E_2[N]$.*

*Proof.* Let $p_{\mathbf{f}}$ be the associated isogeny as in Theorem 2.3 and put $H = \mathrm{Ker}(p_{\mathbf{f}})$ and $H_i = \mathrm{Ker}(f_i)$. Since $\mathrm{Ker}(p_{\mathbf{f}}) \cap (E_1 \times (0)) = (H_1 \cap H_2) \times (0)$, it follows from the hypothesis $H_1 \cap H_2 = (0)$ that $(pr_2)_{|H} : H \to E_2[N]$ is injective and hence bijective since $\#H = N^2 = \#E_2[N]$. Thus, if we put $\psi' := pr_1 \circ (pr_2)_{|H}^{-1} : E_2[N] \to E_1[N]$, then its "dual graph" is $H$, i.e. $H = \{(\psi'(y), y) : y \in E_2[N]\}$. But since $H$ is an isotropic subgroup of $A[N]$ (by Theorem 2.3), we see that $\psi'$ is an anti-isometry, and hence so is its inverse $\psi = (\psi')^{-1}$. By construction, $\mathrm{Ker}(p_{\mathbf{f}}) = \mathrm{Graph}(\psi)$, which is equivalent to (2.9). Uniqueness is clear: if $\psi_1$ is another homomorphism satisfying (2.9), then $\mathrm{Graph}(\psi_1) \leq \mathrm{Ker}(p) = \mathrm{Graph}(\psi)$, and hence $\psi_1 = \psi$.

Conversely, if $\psi : E_1[N] \to E_2[N]$ is a reducible anti-isometry, then by the theorem there is an isogeny factor set $\mathbf{f} = (f, f_1, f_1', f_2, f_2')$ such that $\mathrm{Ker}(p_{\mathbf{f}}) = \mathrm{Graph}(\psi)$ and so (2.9) holds. But since $\psi$ is an isomorphism we have $\mathrm{Graph}(\psi) \cap (E_1 \times (0)) = (0)$, and so $\mathrm{Ker}(f_1) \cap \mathrm{Ker}(f_2) = (0)$, as claimed.

**Remark 2.5** Note that by applying $f_1'$ to both sides of the first equation of (2.9) we obtain the relation

$$[n_2] \circ \psi = f_{|E_1[N]}, \quad \text{where } n_2 = \deg(f_2) = \deg(f_1'); \tag{2.10}$$

which clearly characterizes $\psi$ *if and only if* $(n_2, N) = 1$.

In particular, we see that if $N$ is prime, then an anti-isometry $\psi : E_1[N] \to E_2[N]$ is reducible if and only if there is an isogeny $f : E_1 \to E_2$ of degree $k(N-k)$ (for some $k$ with $0 < k < N$) such that (2.10) holds (with $n_2 = N - k$), for any such $f$ gives rise to the isogeny diamond configuration $(f, \mathrm{Ker}(f)[k], \mathrm{Ker}(f)[N-k])$.

Although the above Corollary 2.4 gives a complete characterization of the reducible anti-isometries $\psi : E_1[N] \to E_2[N]$, the description of the associated anti-isometry by rule (2.9) is somewhat implicit, particularly since it involves the "dual isogenies" $\widetilde{f_i'}$. For this reason we present the following more explicit description which may be viewed as a generalization of the characterization (2.10) to the case of composite $N$'s.

**Theorem 2.6 ("Reducibility Criterion")** *Let $\mathbf{f} = (f, H_1, H_2)$ be an isogeny diamond configuration of order $N$ from $E_1$ to $E_2$, and put $n = N/d$ and $k_i = n_i/d$, where $d = (n_1, n_2)$ and $n_i = \#H_i$. Then $f$ factors (uniquely) over $[d]$, i.e. $f = \overline{f} \circ [d]$, and there is a unique reducible anti-isometry $\psi = \psi_{\mathbf{f}} : E_1[N] \to E_2[N]$ such that*

$$\psi(k_1 x_1 + k_2 x_2) = \overline{f}(x_2 - x_1), \quad \forall x_i \in \widetilde{H_i} = [n]^{-1}(H_i), \tag{2.11}$$

*and every reducible anti-isometry is of this form. Furthermore, if $\mathbf{f}' = (f', H_1', H_2')$ is another isogeny diamond configuration, then we have $\psi_{\mathbf{f}} = \psi_{\mathbf{f}'} \Leftrightarrow \mathbf{f} \sim \mathbf{f}'$.*

*Proof.* Let $H_0 = \mathrm{Ker}(f)$ and $H_i[d] = H_i \cap E_1[d]$, for $i = 0, 1, 2$. Then $H_0[d] = H_1[d] \times H_2[d] \leq E_1[d]$. Now since $d | n_i$ we have $d | \#H_i[d]$ (cf. Proposition 2.10a), and

so $d^2|H_0[d]$. But $\#E_1[d] = d^2$, and so $H_0[d] = E_1[d]$. Thus, $E_1[d] \leq H_0$, and hence $f$ factors over $[d]$, as asserted.

Let $(f, f_1, f_1', f_2, f_2)$ be an isogeny factor set associated to $(f, K_1, K_2)$. Then $\widetilde{f_1'} \circ \overline{f} \circ [d] = \widetilde{f_1'} \circ f_1' \circ f_1 = n_2 f_1 = k_2 f_1 \circ [d]$, and similarly $\widetilde{f_2'} \circ \overline{f} \circ [d] = k_1 f_2 \circ [d]$. Thus we have

$$\widetilde{f_1'} \circ \overline{f} = k_2 f_1 \quad \text{and} \quad \widetilde{f_2'} \circ \overline{f} = k_1 f_2. \tag{2.12}$$

By Corollary 2.4 there is a unique anti-isometry $\psi : E_1[N] \to E_2[N]$ such that (2.9) holds. We claim that $\psi$ satisfies (2.11). For this, let $x_i \in \widetilde{H_i}$. Then $k_i x_i \in E_1[N]$, for $N k_i x_i = n_i n x_i = 0$ (because $n x_i \in H_i$ and $\#H_i = n_i$), and so the left hand side of (2.11) is defined. Next we observe that $\mathrm{Ker}(\widetilde{f_1'}) \cap \mathrm{Ker}(\widetilde{f_2'}) = (0)$, for otherwise (by duality) $f_1'$ and $f_2'$ would factor over a common isogeny, which is impossible since $f_1, f_1', f_2, f_2'$ form a diamond. Thus, to verify (2.11), it is enough to show that (2.11) is valid after applying $\widetilde{f_i'}$, for $i = 1, 2$. But by (2.9) and (2.12) we have $\widetilde{f_1'}(\psi(k_1x_1 + k_2x_2)) = f_1(k_1x_1 + k_2x_2) = f_1(nx_1 + k_2(x_2 - x_1)) = \widetilde{f_1'}(\overline{f}(x_2 - x_1))$, where we have used the fact that $nx_1 \in H_1 = \mathrm{Ker}(f_1)$. Similarly, $\widetilde{f_2'}(\psi(k_1x_1 + k_2x_2)) = -f_2(k_1x_1 + k_2x_2) = f_2(k_1(x_2 - x_1) - nx_2) = \widetilde{f_2'}(\overline{f}(x_2 - x_1))$, and so $\psi$ satifies (2.11).

Since every reducible anti-isometry $\psi$ has the form (2.9) by Corollary 2.4, we see by the above that every such $\psi$ satisfies (2.11). It thus remains to show that equation (2.11) defines a unique map $\psi : E_1[N] \to E_2[N]$. This clearly follows from the fact that $[k_1]\widetilde{H_1} + [k_2]\widetilde{H_2} = E[N]$, which seems to be more involved and which is proven in Proposition 2.10d) below.

In the above proof we required some basic facts about finite subgroup schemes of an elliptic curve $E$. Since these will be required again in the next section, we develop them in some detail here. A basic important notion is that of an *m-primitive* subgroup scheme which we study first.

**Definition 2.7** A finite subgroup scheme $H \leq E$ of an elliptic curve $E/K$ is called *primitive*, if $E[m] \leq H \Rightarrow m = \pm 1$. More generally, if $m \geq 1$ is any integer, then we say that $H$ is *m-primitive*, if $H[m] := H \cap E[m] = \mathrm{Ker}([m]_H)$ is primitive, or equivalently, if

$$E[q] \not\leq H, \quad \text{for all primes } q|m. \tag{2.13}$$

Similarly, an isogeny $f : E \to E'$ is called *m-primitive* if $\mathrm{Ker}(f)$ is $m$-primitive or, equivalently, if $f$ does not factor over $[q]$, for any prime $q|m$.

**Lemma 2.8** *Let $H \leq E$ be a subgroup of order $n \neq 1$, and let $p = \mathrm{char}(K)$.*

*a) Suppose $p \nmid n$. Then $H$ is primitive $\iff$ $H$ is cyclic.*

*b) Suppose $n = p^r$, and $E$ is ordinary. Then $H$ is primitive $\iff$ $H \simeq \mu_n$ or $H \simeq \mathbb{Z}/n\mathbb{Z}$.*

*c) Suppose $n = p^r$ and $E$ is supersingular. Then $H$ is primitive $\iff$ $\#H = p$.*

*Proof.* a) Here $H$ is étale. By group theory, $H$ is cyclic $\iff$ there does not exist a subgroup of type $(p,p) \iff H$ is primitive.

b) By hypothesis, $H \leq E[n] \simeq \mu_n \times \mathbb{Z}/n\mathbb{Z}$ (cf. [Mu], p. 147). Thus all subgroups of order $n$ are of the form $\mu_{p^s} \times \mathbb{Z}/p^{n-s}\mathbb{Z}$, $n \geq s \geq 0$. However, such a group is primitive if and only if $s = 0$ or $n - s = 0$, for otherwise $E[p] = \mu_p \times \mathbb{Z}/p\mathbb{Z} \leq \mu_{p^r} \times \mathbb{Z}/p^{n-r}\mathbb{Z}$.

c) Since the $p$-rank of $E$ is 0 by hypothesis, we have that $E[n]$ is local-local of order $p^{2r}$. Since $[\kappa(E) : \kappa(E)^p] = p$, there is only one subgroup of height 1, and hence (by induction) there is a unique subgroup $H_r$ of order $p^r$, and these form an ascending chain $(0) = H_0 \leq H_1 \leq H_2 = E[p] \leq H_3 \leq \cdots \leq H_{2s} = E[p^s] \leq \cdots$. In particular, $H_i \neq (0)$ is primitive if and only if $i = 1$.

**Remark 2.9** The above lemma actually describes *all* primitive subgroup schemes, for each finite commutative group scheme $G$ of order $n = p_1^{r_1} \cdots p_s^{r_s}$ has a unique decomposition

$$G \cong G(p_1) \times \cdots \times G(p_s)$$

into its $p_i$-primary components $G(p_i)$. We note the following rules:

$$\#(G(p_i)) = (\#G)(p_i) := p_i^{r_i}, \tag{2.14}$$

$$(G[m])(p_i) = G(p_i)[m(p_i)], \text{ for any } m \in \mathbb{N}, \tag{2.15}$$

$$(G_1 \cap G_2)(p_i) = G_1(p_i) \cap G_2(p_i), \text{ for subgroups } G_1, G_2 \leq G; \tag{2.16}$$

in particular, we see that $G$ is $m$-primitive if and only if $G(q)$ is $m(q)$-primitive, for all primes $q \mid (m,n)$.

**Proposition 2.10** *a) If $H \leq E$ is a subgroup scheme of order $n$ and $d|n$ then also $d|\#H[m]$, and equality holds if $(d, \frac{n}{d}) = 1$.*

*b) If $H \leq E$ is an $m$-primitive subgroup scheme of order $n$ and $d \mid (n,m)$, then we have $\#H[d] = d$, $\#H[k] = k$ and $[d]H = H[k]$, where $k = \frac{n}{d}$.*

*c) Let $H_1$ and $H_2$ be two subgroup schemes of $E$ with $H_1 \cap H_2 = (0)$. Then $H_i$ is $d$-primitive, where $d = (n_1, n_2)$ and $n_i = \#H_i$. Furthermore, if $E$ is supersingular, then* $\mathrm{char}(K) \nmid d$.

*d) In the situation of c), let $\widetilde{H}_i = [n]^{-1}(H_i)$ and $H_i' = [k_i](\widetilde{H}_i)$, where $k_i = n_i/d$ and $n = k_1 + k_2$. Then $\#\widetilde{H}_i[k_i] = k_i$, $\#H_i' = Nn$, where $N = n_1 + n_2 = nd$, and we have*

$$H_1' + H_2' = E[N] \quad \text{and} \quad H_1' \cap H_2' = E[n]. \tag{2.17}$$

*Proof.* a) To prove the first assertion, it is enough to show that $H$ has a subgroup scheme $H' \leq H$ of order $d$, for then $H' \leq H[d]$ and so $d \mid \#H[d]$. For this, we note that by the structure theorem of finite commutative group schemes (cf. [Mu], p. 136), it is enough to verify this if $H$ is a group of type $(r,r)$, $(l,r)$, $(r,l)$ or $(l,l)$.

In the first three cases this is clear, for then $H$ is a product of étale groups $\mathbb{Z}/m\mathbb{Z}$ and multiplicative groups $\mu_m$. On the other hand, if a subgroup $H \leq E$ of type $(l,l)$ appears at all, then $E$ is supersingular, in which case $E$ has a unique subgroup scheme of order $p^i$, for each $i \in \mathbb{N}$ (cf. the proof of Lemma 2.8c)). Since these form a chain, the assertion is here true as well.

Finally, suppose $(d,k) = 1$, where $k = n/d$. Then $H = H[dk] = H[d] \times H[k]$, and by the above we have $dk \leq \#H[d] \cdot \#H[k] = \#H = nk$. Thus, equality must hold throughout, so in particular $\#H[d] = d$.

b) We prove the first assertion by induction on $n$. If $n = 1$ or, more generally, if $d = 1$, then the assertion is trivial. Thus, assume that there exists a prime $q|d$. Then $\#H[q] = q$, for by a) we have $q|\#H[q]$ but $\#H[q]$ divides $\#E[q] = q^2$ properly since $H$ is $q$-primitive. Therefore, if $H' = [q](H)$, then $\#H' = \#H/\#H[q] = \frac{n}{q}$. Since $H' \leq H$ is again $m$-primitive, the induction hypothesis implies that $\#H'[\frac{d}{q}] = \frac{d}{q}$. But since $[q]H[d] = H'[\frac{d}{q}]$, we see that $\#H[d] = \#H[q]\#[q]H[d] = q \cdot \frac{d}{q} = d$, and so the first assertion is true.

To prove the last two assertions we note that since $[d]H \leq H[k]$ and $\#[d]H = \#H/\#H[d] = n/d = k$, it is enough to verify the last assertion. For this, write $n = n(d)n'$, where $n(d) = \prod_{p|d} p^{v_p(n)}$ denotes the $d$-component of $n$. Since $(n(d), n') = 1$ we have by a) that $\#H[n'] = n'$. On the other hand, since $k = k'n'$ where $k' = \frac{n(d)}{d}$, we have $H[k] = H[k'] \times H[n']$. But since $k'|(n, m^r)$ (for some $r \geq 1$), it follows from what was proved above (by replacing $d$ by $k'$) that $\#H[k'] = k'$, and so $\#H[k] = k'n' = k$, as desired.

c) If $H_1$ were not $d$-primitive, then there is a prime $q|d$ such that $E[q] \leq H_1$. Since $q|d|n_2$, we have by a) that $(0) \neq E[q] \cap H_2 = E[q] \cap H_1 \cap H_2 = (0)$, which is a contradiction. Thus, $H_1$ (and similarly, $H_2$) is $d$-primitive.

If $E$ is supersingular, then there is a unique subgroup of order $p^i$ (cf. the proof of Lemma 2.8c)), so $H_1 \cap H_2 = (0)$ is only possible if $p \nmid d$.

d) First note that since $(n, k_i) = 1$, it follows that

$$[n]^{-1}(H_i[k_i]) = \widetilde{H}_i[k_i] \times E[n]. \tag{2.18}$$

(Indeed, the one inclusion is clear. Conversely, if $h \in [n]^{-1}(H_i[k_i]) \leq E[nk_i] = E[k_i] \times E[n]$, then $h = h_1 + h_2$ with $h_1 \in E[k_i]$ and $h_2 \in E[n]$. But then $nh_1 = nh \in H_i[k_i]$, so $h_1 \in \widetilde{H}_i$ and hence $h \in \widetilde{H}_i[k_i] \times E[n]$.) From (2.18) and b) it follows that $\#\widetilde{H}_i[k_i] = \#H_i[k_i] = k_i$, and hence $\#H_i' = \#\widetilde{H}_i/\#\widetilde{H}_i[k_i] = n^2 n_i/k_i = n^2 d = nN$, which proves the first two assertions.

Next we observe that $\widetilde{H}_1 \cap \widetilde{H}_2 = [n]^{-1}(H_1 \cap H_2) = [n]^{-1}(\,(0)\,) = E[n]$; in particular, $\widetilde{H}_i \geq E[n]$ and hence also $H_i' = [k_i]\widetilde{H}_i \geq [k_i]E[n] = E[n]$. Thus $E[n] \leq H_1' \cap H_2' \leq \widetilde{H}_1 \cap \widetilde{H}_2 = E[n]$, and so we must have equality throughout, which proves the second identity of (2.17). To prove the first, we note that since $H_i' \leq E[N]$ (because $h \in \widetilde{H}_i \Rightarrow Nk_ih = n_inh = 0$, since $nh \in H_i$ and $\#H_i = n_i$), it is enough to show that $\#(H_1' + H_2') = \#E[N] = N^2$. But this true

since $\#(H_1' + H_2') = (\#H_1' \cdot \#H_2')/(\#(H_1' \cap H_2')) = (nN)^2/n^2 = N^2$, and so the first identity of (2.17) is also valid.

As an application of this proposition we prove the following result which may be viewed as a "structure theorem" for isogeny diamond configurations. It is fundamental for the counting procedure of the next section.

**Corollary 2.11** *a) Let $(f, H_1, H_2)$ be an isogeny diamond configuration of order $N$. Then $f$ factors as $f = \overline{f} \circ [d]$, where $d = (n_1, n_2)$ and $n_i = \#H_i$ and $\overline{H} := \mathrm{Ker}(\overline{f}) = [d](\mathrm{Ker}(f))$ is $N$-primitive. Furthermore, we have $[d]H_i = H_i[k_i] = \overline{H}[k_i]$, where $k_i = n_i/d$.*

*b) Conversely, suppose that $\overline{f} : E_1 \to E_2$ is an isogeny of degree $k_1k_2$ where $(k_1, k_2) = 1$ and that $H_1$ and $H_2$ are two subgroup schemes of $E_1$ with $H_1 \cap H_2 = (0)$ such that $\#H_i = dk_i$ (for some $d$) and $H_i \geq \mathrm{Ker}(\overline{f})[k_i]$, for $i = 1, 2$. Then $(\overline{f} \circ [d], H_1, H_2)$ is an isogeny diamond configuration of order $N := d(k_1 + k_2)$, and hence $\mathrm{Ker}(\overline{f})$ is $N$-primitive and $H_i[k_i] = \mathrm{Ker}(\overline{f})[k_i]$.*

*Proof.* a) The existence of $\overline{f}$ was already proved in Theorem 2.6. Since $\overline{f}$ is an isogeny (and is hence is universally surjective), it follows that $[d]\mathrm{Ker}(f) = \mathrm{Ker}(\overline{f})$. Furthermore, $H_i$ is $d$-primitive by Proposition 2.10c), and hence $[d]H_i = H_i[k_i]$ has order $k_i$ by Proposition 2.10c). Thus, $[d]H_i \leq [d]\mathrm{Ker}(f) \cap E_1[k_i] = \overline{H}[k_i]$ and so we have equality because $\overline{H}[k_i] = k_i$ (since $\overline{H} = k_1k_2$ and $(k_1, k_2) = 1$). This proves the last two assertions.

Finally, since $\overline{H}[k_i] = H_i[k_i]$ is $d$-primitive and since $(k_i, N)|d$ and $(k_1, k_2) = 1$, it follows that $\overline{H}[k_i]$ and hence also $\overline{H}$ is $N$-primitive.

b) Since the last two assertions follow from a), it is enough to verify the first. For this it is enough to show that $H_i \leq \mathrm{Ker}(f)$, where $f = \overline{f} \circ [d]$. Now by the hypotheses we have $H_i[k_i] \geq \overline{H}[k_i]$ and $\#\overline{H}[k_i] = k_i$. On the other hand, it follows from Proposition 2.10c), b) that $H_i$ is $d$-primitive, and hence that $[d]H_i = H_i[k_i]$ has order $k_i$. Thus, $[d]H_i = \overline{H}[k_i] \leq \overline{H}$, and so $H_i \leq [d]^{-1}(\overline{H}) = \mathrm{Ker}(f)$, as desired.

# 3 A formula for $r(E_1, E_2, N)$

The Reducibility Criterion of the previous section enables us to count the number $r(E_1, E_2, N) = \#\mathcal{R}(E_1, E_2, N)$ of reducible anti-isometries $\psi : E_1[N] \to E_2[N]$, and this leads to a formula for the (weighted) number $n(E_1, E_2, N)$ of curves of genus 2 of type $(E_1, E_2, N)$; cf. Theorem 3.4. To state the result, let

(3.1) $h(E_1, E_2, n, m) = \#\{f \in \mathrm{Hom}(E_1, E_2) : \deg(f) = n \text{ and } f \text{ is } m\text{-primitive}\}$.

denote the number of $m$-primitive isogenies (cf. Definition 2.7) of degree $n$. Note that this number can be expressed in terms of the number $h(E_1, E_2, n)$ of all isogenies

of degree $n$ by using the Moebius $\mu$-function; explicitly, we have

$$h(E_1, E_2, n, m) = \sum_{\substack{k|m \\ k^2|n}} \mu(k) h\left(E_1, E_2, \frac{n}{k^2}\right). \tag{3.2}$$

This is clear by the usual inclusion/exclusion principle since the set $\mathcal{H}(E_1, E_2, n, m)$ of $m$-primitive isogenies of degree $n$ is related to the set $\mathcal{H}(E_1, E_2, n)$ of all isogenies of degree $n$ by the formula $\mathcal{H}(E_1, E_2, n, m) = \mathcal{H}(E_1, E_2, n) \setminus \bigcup_{\substack{p|m \\ p^2|n}} \mathcal{H}\left(E_1, E_2, \frac{n}{p^2}\right) \circ [p]$.

Since the numbers $h(E_1, E_2, n, m)$ will mainly occur in a very specific form, it is useful to introduce the abbreviation

$$h^*(E_1, E_2, k, N) := h\left(E_1, E_2, \frac{k(N-k)}{(k,N)^2}, N\right). \tag{3.3}$$

In addition to these numbers we also need the following "weighting factor" $w(E, k, N)$ which is essentially an expession involving the *Dedekind $\psi$-function*

$$\psi(n) = n \prod_{p|n} \left(1 + \frac{1}{p}\right),$$

but with minor modifications when $\mathrm{char}(K)|N$. For this reason we define

$$\psi(p, n) = \begin{cases} \psi(n), & \text{if } p \nmid n, \\ 2\psi(n/n(p)), & \text{if } p \mid n, \end{cases} \tag{3.4}$$

where $n(p) = p^{v_p(n)}$ denotes the $p$-primary component of $n$ (and $n(p) = 1$ if $p = 0$), and put

$$w(p, k, N) = \frac{\psi(p, k(N-k))}{\psi(p, \frac{k}{d})\psi(p, \frac{N}{d} - \frac{k}{d})}, \quad \text{where } d = (k, N), \tag{3.5}$$

$$= \frac{\psi(k(N-k))}{\psi(\frac{k}{d})\psi(\frac{N}{d} - \frac{k}{d})} = d^2 \prod_{\substack{q|d \\ q \nmid \frac{k(N-k)}{d^2}}} \left(1 + \frac{1}{q}\right), \quad \text{if } p \nmid N. \tag{3.6}$$

Furthermore, if $E$ is an elliptic curve over a field $K$ of characteristic $p$, then define

$$w(E, k, N) = \varepsilon(E, d) w(p, k, N), \tag{3.7}$$

where $d = (k, N)$ and

$$\varepsilon(E, d) = \begin{cases} 0 & \text{if } E \text{ is supersingular and } p \mid d \\ 1 & \text{otherwise.} \end{cases} \tag{3.8}$$

**Theorem 3.1** *The number $r(E_1, E_2, N) = \#\mathcal{R}(E_1, E_2, N)$ of reducible anti-isometries $\psi : E_1[N] \to E_2[N]$ is given by the formula*

$$\begin{aligned} r(E_1, E_2, N) &= \frac{1}{2} \sum_{k=1}^{N-1} w(E_1, k, N) h^* (E_1, E_2, k, N) \\ &= \frac{1}{2} \sum_{\substack{d|N \\ d \neq N}} \varepsilon(E_1, d) \sum_{\substack{k=1 \\ (k, N/d)=1}}^{N/d} \frac{\psi(p, dk(N-dk))}{\psi(p,k)\psi(p, \frac{N}{d} - k)} h(E_1, E_2, k(\tfrac{N}{d} - k), N). \end{aligned}$$

As is evident from the Reducibilty Theorem, the proof of Theorem 3.1 requires a careful enumeration of certain configurations of finite subgroup schemes of an elliptic curve $E$; more precisely, Corollary 2.11 shows that we need to compute the following number $\omega(E, d, K_1, K_2)$.

**Proposition 3.2** *Let $K_1$ and $K_2$ be two subgroup schemes of an elliptic curve $E$ such that $(k_1, k_2) = 1$ where $k_i = \#K_i$, for $i = 1, 2$. For each positive integer $d$, let*

$$\Omega(E, d, K_1, K_2) = \{(H_1, H_2) : H_1 \cap H_2 = (0), E \geq H_i \geq K_i, \#H_i = dk_i, i = 1, 2\},$$

*and let $\Omega'(E, d, K_1, K_2)$ denote the subset of those pairs $(H_1, H_2) \in \Omega(E, d, K_1, K_2)$ satisfying in addition the condition $H_i[k_i] = K_i$, for $i = 1, 2$. Then $\Omega(E, d, K_1, K_2) = \Omega'(E, d, K_1, K_2)$, and their common cardinality $\omega(E, d, K_1, K_2)$ is given by*

$$\omega(E, d, K_1, K_2) = \chi(K_1, d)\chi(K_2, d) \cdot w(E, dk_1, d(k_1 + k_2)), \tag{3.9}$$

*where $\chi(K_i, d) = 1$ if $K_i$ is $d$-primitive and $\chi(K_i, d) = 0$ otherwise.*

Before proving this proposition, let us see how Theorem 3.1 follows from it.

*Proof of Theorem 3.1.* Let $\mathcal{IDC}(E_1, E_2, N)$ denote the set of isogeny diamond configurations of degree $N$ from $E_1$ to $E_2$ and, as in Corollary 2.4, let $\overline{\mathcal{IDC}}(E_1, E_2, N)$ denote the set of equivalence classes. We then have by Corollary 2.4 and the fact that each equivalence class consists of precisely 2 elements that

$$r(E_1, E_2, N) = \#\overline{\mathcal{IDC}}(E_1, E_2, N) = \frac{1}{2}\#\mathcal{IDC}(E_1, E_2, N). \tag{3.10}$$

It thus remains to calculate $\#\mathcal{IDC}(E_1, E_2, N)$. For this, consider the map

$$\rho : \mathcal{IDC}(E_1, E_2, N) \to \dot{\bigcup_{k=1}^{N-1}} \{k\} \times \mathcal{H}\left(E_1, E_2, \frac{k(N-k)}{(k, N)^2}, N\right)$$

which is defined by the rule $\rho(f, H_1, H_2) = \{\#H_1\} \times \overline{f}$, where $f = \overline{f} \circ [d]$ and $d = (n_1, n_2)$, $n_i = \#H_i$. (Recall that $\overline{f}$ exists and is $N$-primitive by Corollary

2.11a).) Now if $(k,\overline{f}) \in \{k\} \times \mathcal{H}(E_1, E_2, \frac{k(N-k)}{(k,N)^2}, N)$, then by Corollary 2.11b) we see that

$$\rho^{-1}(k,\overline{f}) = \Omega(E_1, d, \mathrm{Ker}(\overline{f})[k_1], \mathrm{Ker}(\overline{f})[k_2])),$$

where $d = (k,N)$, $k_1 = k/d$ and $k_2 = (N-k)/d$, and hence by Proposition 3.2 we obtain

$$\#\rho^{-1}(k,\overline{f}) = w(E_1,k,N)$$

because $\chi(\mathrm{Ker}(\overline{f}),N) = 1$ implies that $\chi(\mathrm{Ker}(\overline{f}[k_i],d) = 1$. Since the right hand side of this equation is independent of $f \in \mathcal{H}(E_1, E_2, \frac{k(N-k)}{(k,N)^2}, N)$, it follows that

$$\begin{aligned} \#\mathcal{IDC}(E_1,E_2,N) &= \sum_{k=1}^{N-1} \#\rho^{-1}(k,f)\#\mathcal{H}(E_1,E_2,\frac{k(N-k)}{(k,N)^2},N) \\ &= \sum_{k=1}^{N-1} w(E_1,k,N)h^*(E_1,E_2,k,N), \end{aligned}$$

and so the formula of Theorem 3.1 follows by substituting this expression in (3.10).

It thus remains to prove Proposition 3.2. For this, we require the following auxiliary result which is also of independent interest:

**Proposition 3.3** *Let $H_0 \leq E$ be a subgroup scheme of order $m$ and let $n$ be a positive integer. As usual, $p = \mathrm{char}(K)$.*

*a) The number $\psi(E,n,H_0)$ of primitive subgroup schemes $H \leq E$ of order $mn$ with $H \geq H_0$ is*

$$\psi(E,n,H_0) = \varepsilon'(E,n,m)\chi(H_0,m)\frac{\psi(p,nm)}{\psi(p,m)}, \tag{3.11}$$

*where $\chi(H_0,m)$ is as in Proposition 3.2 and*

$$\varepsilon'(E,n,m) = \begin{cases} 0 & \text{if } E \text{ is supersingular and } p^2 \mid mn \\ \frac{1}{2} & \text{if } E \text{ is supersingular and } p||n \text{ and } p \not| m \\ 1 & \text{otherwise.} \end{cases}$$

*b) The number $\psi'(E,n,H_0)$ of $n$-primitive subgroup schemes $H \leq E$ of order $mn$ with $H \geq H_0$ is*

$$\psi'(E,n,H_0) = \varepsilon'(E,n,m))\chi(H_0,n)\frac{\psi(p,nm)}{\psi(p,m)}. \tag{3.12}$$

*c) Assume that $n|m$. Then the number $\tau(E,n,H_0)$ of subgroup schemes $H$ of order $n$ with $H \cap H_0 = (0)$ is*

$$\tau(E,n,H_0) = \varepsilon(E,n)\chi(H_0,n)\frac{n}{n(p)}. \tag{3.13}$$

*Proof.* a) First of all, we may assume that $H_0$ is primitive for otherwise we have trivially that $\psi(E,n,H_0)=0$, and then both sides of (3.11) are zero. By Remark 2.9 we have

$$\psi(E,n,H_0)=\prod_{q|mn}\psi(E,n(q),H(q)),$$

and hence it is enough to verify (3.11) is the case that $n=q^r,\ m=q^s$ are prime powers. If $q=p$ and $E$ is ordinary, then $\psi(E,p^r,H_0)=2$ if $H_0=0$, and $\psi(E,p^r,H_0)=1$ if $H_0\neq 0$ (because if $H_0=\mu_{p^s}$ then necessarily $H=\mu_{p^r}$, and if $H_0=\mathbb{Z}/p^s\mathbb{Z}$ then $H=\mathbb{Z}/p^r\mathbb{Z}$; cf. Lemma 2.8b)). Thus (3.11) holds in this case.

If $q=p$ and $E$ is supersingular, then $\psi(E,p^r,H_0)=0$ if $r+s\geq 2$ because there is no primitive subgroup of order $p^{r+s}\geq p^2$ (cf. Lemma 2.8c)), and so both sides of (3.11) are 0. Thus, assume $r+s\leq 1$. Then $\psi(E,p^r,H_0)=1$, and the same is true of the right hand side of (3.11) by distinguishing cases.

Finally, if $q\neq p$, then let $\Psi(n)$ denote the set of primitive subgroups $H$ of order $n$, which by Lemma 2.8a) is the same as the set of cyclic subgroups $H\leq E[n]\simeq \mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$. In particular, we see that $\Psi(n)$ has cardinality $\psi(n)$. Now consider the map

$$p_n:\Psi(nm)\to\Psi(m)$$

given by $p_n(H)=[n]H=H[m]\in\Psi(m)$ (by Proposition 2.10b)). Since $[n]:E[nm]\to E[m]$ is surjective, one sees easily that $p_n$ is also surjective. Next we observe that the group $G_{nm}=\mathrm{Gl}_2(\mathbb{Z}/nm\mathbb{Z})=\mathrm{Aut}(E[nm])$, which acts transitively on $\Psi(nm)$, acts also transitively on the set of fibres of $p_n$ (because $G_m$ acts transitively on $\Psi(m)$ and the natural map $G_{nm}\to G_m$ is surjective). Thus, since the elements of $G_{mn}$ map fibres to fibres, it follows that all the fibres have the same cardinality, and hence we obtain

$$\psi(E,n,H_0)=\#p_n^{-1}(H_0)=\#\Psi(mn)/\#\Psi(m)=\frac{\psi(mn)}{\psi(m)}.$$

b) It is enough to show that

$$\psi'(E,n,H_0)=\prod_{q|nm}\psi'(E,n(q),H_0(q))=\prod_{q|n}\psi(E,n(q),H_0(q)),\tag{3.14}$$

for then the assertion follows from a) since $\chi(H_0,n)=\prod_{q|n}\chi(H_0(q),n(q))$ by Remark 2.9 and since $\varepsilon'(E,n,m)=\varepsilon'(E,n(p),m(p))$.

To prove (3.14), we first note that the first equality is obvious by Remark 2.9. To verify the second, may assume that $n=q^r$ and $m=q^s$ are prime powers. If $r=0$, i.e. $q\nmid n$, then $H=H_0$ (and $H[n]=(0)$), so $\psi'(E,n,H_0)=1$ in this case, as claimed. If $r>0$ then $H$ is $n$-primitive $\Leftrightarrow$ $H$ is primitive because $H$ is a $q$-group, and so $\psi'(E,n,H_0)=\psi(E,n,H_0)$ in this case, which proves (3.14).

c) By Proposition 2.10c) we have $\tau(E,n,H_0)=0$ if $\varepsilon(E,n)=0$ or $\chi(H_0,n)=0$, so assume $\varepsilon(E,n)=\chi(H_0,n)=1$. Thus $H_0$ is $n$-primitive and hence $\#H_0[n]=n$

by Proposition 2.10b). Moreover, we have $\tau(E,n,H_0) = \tau(E,n,H_0[n])$ because $H \cap H_0 = H \cap H_0[n]$, if $\#H = n$, and hence we may assume (after replacing $H_0$ by $H_0[n]$) that $\#H_0 = n$.

Furthermore, as before we may assume that $n = q^r$ is a prime power. If $q = p$ and $E$ is supersingular then $r = 0$ (since $\varepsilon(E,n) = 1$), so (3.13) holds trivially. If $q = p$ and $E$ is ordinary, then either $H_0 = \mu_n$ or $H_0 = \mathbb{Z}/n\mathbb{Z}$ and then $H = \mathbb{Z}/n\mathbb{Z}$ (respectively, $H = \mu_n$) is the only possibility. Thus $\tau(E,n,H_0) = 1$ in this case.

Finally, assume $q \neq p$. Then by Propositions 2.10c) and 2.8a), $H_0 = \langle x \rangle$ and $H = \langle y \rangle$ are cyclic subgroups of order $n$ which generate $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Thus, if $H' =< y' >$ is another such subgroup, then there exists $g = \left(\begin{smallmatrix} a & 0 \\ c & d \end{smallmatrix}\right) \in \mathrm{Gl}_2(\mathbb{Z}/n\mathbb{Z})$ such that $g\binom{x}{y} = \binom{x'}{y'}$. Since the number of such matrices is $\phi(n)^2 n$, and exactly $\phi(n)^2$ matrices yield the same pair of subgroups, the formula (3.13) follows.

*Proof of Proposition 3.2.* The asserted equality $\Omega = \Omega'$ follows immediately from Corollary 2.11b). To prove (3.9), let us first consider the case that $K_1 = (0)$. Then (3.9) reduces to

$$\omega(E,d,(0),K_2) = \varepsilon(E,d)\chi(K_2,d)\frac{\psi(p,d^2k_2)}{\psi(p,k_2)}. \tag{3.15}$$

To prove this, suppose that $(H_1,H_2) \in \Omega(E,d,(0),K_2)$. Then $H_2$ is $d$-primitive by Proposition 2.10c), and so by Proposition 3.3a) we have $\psi'(E,d,K_2)$ choices for $H_2$. On the other hand, for a fixed $H_2$ with these properties, we have by definition $\tau(E,d,H_2)$ possible choices for $H_1$. By Proposition 3.3c), this number does not depend on $H_2$, and so the total number of choices is

$$\omega(E,d,(0),K_2) = \tau(E,d,H_2)\psi'(E,d,K_2) = \varepsilon(E,d)\frac{d}{d(p)}\varepsilon'(E,d,k_2)\chi(K_2,d)\frac{\psi(p,k_2)}{\psi(p,k_2)}$$

by Proposition 3.3b),c). But since $\varepsilon(E,d)\varepsilon'(E,d,k_2) = \varepsilon(E,d)$ and $\frac{d}{d(p)}\psi(p,dk_2) = \psi(p,d^2k_2)$, we see that (3.15) holds.

From (3.15) it follows that we have

$$\omega(E,d,K_1,K_2) = \varepsilon(E,d)\chi(K_1,d)\chi(K_2,d)\frac{\psi(p,d^2k_1k_2)}{\psi(p,k_1)\psi(p,k_2)}, \tag{3.16}$$

whenever $k_i = q^{s_i}$, for $i = 1,2$ because the hypothesis $(k_1,k_2) = 1$ forces that either $K_1 = (0)$ or $K_2 = (0)$. But then the general case follows by multiplicativity because we have by Remark 2.9 that

$$\omega(E,d,K_1,K_2) = \prod_q \omega(E,d(q),K_1(q),K_2(q)).$$

This concludes the proof of Proposition 3.2, for the right hand sides of (3.9) and (3.16) are equal by the definition (3.7) of $w(E,k,N)$.

Now that we have obtained in Theorem 3.1 a formula for $r(E_1, E_2, N)$, the number of *reducible* anti-isometries, we can also derive a formula for $n(E_1, E_2, N) := \#\mathcal{I}(E_1, E_2, N)$, the number of *irreducible* anti-isometries (which may, however, be infinite in some cases). We observe that by Theorem 1.5 this number may be interpreted as the *weighted number* of isomorphism classes of elliptic subcovers $f : C \to E_1$ of type $(E_1, E_2, N)$, where the weights are determined by the length of the orbits of the group $\mathrm{Aut}(E_1, E_2) := (\mathrm{Aut}(E_1) \times \mathrm{Aut}(E_2))/\{\pm 1\}$ acting on $\mathcal{I}(E_1, E_2, N)$; in particular, we have that the actual number $\#\mathcal{M}(E_1, E_2, N)$ of these isomorphism classes satisfies the estimates

$$n(E_1, E_2, N) \geq \#\mathcal{M}(E_1, E_2, N) \geq \frac{2n(E_1, E_2, N)}{\mathrm{Aut}(E_1)\mathrm{Aut}(E_2)}. \tag{3.17}$$

**Theorem 3.4** *If $p = \mathrm{char}(K) \nmid N$ or if $E_1$ and $E_2$ are ordinary, then the weighted number of curves of genus 2 of type $(E_1, E_2, N)$ is finite and is given by the formula*

$$n(E_1, E_2, N) = sl(p, N) - r(E_1, E_2, N) = sl(p, N) - \frac{1}{2}\sum_{k=1}^{N-1} w(p, k, N) h^*(E_1, E_2, k, N)$$

*where $h^*(E_1, E_2, N)$ and $w(p, k, N)$ are as in (3.3) and (3.6), and*

$$sl(p, N) = \#\mathrm{Sl}_2(\mathbb{Z}/\overline{N}(p)\mathbb{Z})N(p) = \frac{N^3}{N(p)^2}\prod_{\substack{q|N \\ q\neq p}}\left(1 - \frac{1}{q^2}\right),$$

*where $N(p) = p^{v_p(N)}$ denotes the $p$-component of $N$ and $\overline{N}(p) = N/N(p)$.*

*On the other hand, if $p|N$ and one of $E_1$ and $E_2$ is supersingular while the other is not, then $n(E_1, E_2, N) = 0$, whereas if both are supersingular, then there are infinitely many curves of genus 2 of type $(E_1, E_2, N)$.*

*Proof.* The second equation follows immediately from Theorem 3.1 since in this case we have $\varepsilon(E_1, (k, N)) = 1$, for all $0 < k < N$. Furthermore, since by definition

$$n(E_1, E_2, N) = s(E_1, E_2, N) - r(E_1, E_2, N),$$

where $s(E_1, E_2, N)$ denotes the number of anti-isometries $\psi : E_1[N] \to E_2[N]$, we see that all the assertions of the theorem follow once we have shown that

$$s(E_1, E_2, N) = \begin{cases} sl(p, N) & \text{if } p \nmid N \text{ or if } E_1 \text{ and } E_2 \text{ are ordinary} \\ \infty & \text{if } p \mid N \text{ and } E_1 \text{ and } E_2 \text{ are supersingular} \\ 0 & \text{otherwise.} \end{cases} \tag{3.18}$$

To prove this, let us first observe that the last case is trivial: if $p|N$ and (say) $E_1$ is supersingular but $E_2$ is ordinary, then $E_1[N] \not\cong E_2[N]$ (because $E_1[N]$ contains

a component of type $(l,l)$ wheras $E_2[N]$ does not), so there cannot be any anti-isometries.

Next, consider the case that $p \not| N$. Then $E_1[N] \simeq E_2[N] \simeq (\mathbb{Z}/N\mathbb{Z})^2$ is étale, and hence $\mathrm{Hom}(E_1[N], E_2[N]) \simeq \mathrm{Gl}_2(\mathbb{Z}/N\mathbb{Z})$ which means that $s(E_1, E_2, N) = \#\mathrm{Sp}_2(\mathbb{Z}/N\mathbb{Z}) = \#\mathrm{Sl}_2(\mathbb{Z}/N\mathbb{Z}) = sl(p, N)$.

We now turn to the case that $p|N$. Since an each isomorphism $\psi : E_1[N] \to E_2[N]$ is the product of its $q$-primary components $\psi_q : E_1[N(q)] \to E_2[N(q)]$ and $\psi$ is an anti-isometry if and only if each $\psi_q$ is, we see that $s(E_1, E_2, N)$ is a multiplicative function. Thus, since the case $p \not| N$ has already been verified, it is enough to consider the case $N = p^r$.

Suppose first that $E_1$ and $E_2$ are both ordinary. Then $E_1[N] \simeq E_2[N] \simeq \mu_N \times \mathbb{Z}/N\mathbb{Z}$, and so $\mathrm{Hom}(E_1[N], E_2[N]) \simeq \mathbb{Z}/N\mathbb{Z}id_{\mu_N} \oplus \mathbb{Z}/N\mathbb{Z}id_{\mathbb{Z}/N\mathbb{Z}}$. But $m \cdot id_{mu_N} \oplus n \cdot id_{\mathbb{Z}/N\mathbb{Z}}$ is an anti-isometry if and only id $m + n \equiv -1 \pmod{N}$, so there are $N$ anti-isometries in total. This proves the formula (3.18) in this case.

It remains to consider the case that $E_1$ and $E_2$ are both supersingular. In this case $E_1[N] \simeq E_2[N] =: G$ is a group of type $(l,l)$ and we claim that there are an infinite number of anti-isometries. To see this, let $M(G) = \mathrm{Hom}(G, C)$ denote the associated Dieudonné module, where, as in [Od], $C$ denotes the functor of Witt co-vectors. Recall that $M(G)$ is $\mathbb{D}$-module of finite $\mathbb{W}$-length, where $\mathbb{D} = \mathbb{W}[F, V]$ (with the usual commuting relations) is the Dieudonné ring and $\mathbb{W} = \mathbb{W}(K)$ denotes the ring of Witt vectors; in fact, one can show that $M(D) = \mathbb{D}/(F - V, p^r)$ (cf. Oort[Oo], p. 39, for the case $r = 1$). By functoriality, the $e_N$-pairing on $E_1[N]$ induces a non-degenerate $\mathbb{D}$-linear pairing

$$\varepsilon : M(G) \times M(G) \to M(\mathbb{G}_m) = \mathbb{W}/p^r\mathbb{W},$$

and so by the fundamental result of Dieudonne-Cartier (cf. [Od]), the assertion follows once we have shown that the set $\{f \in \mathrm{End}_{\mathbb{D}}(M(G)) : \varepsilon \circ f \times f = -\varepsilon\}$ is infinite.

To prove this, let us restrict for simplicity to the case $r = 1$. (The proof for $r > 1$ is similar.) Then $M(G)$ is a 2-dimensional $K$-vector space with a basis $\{e, Fe\}$, and we have (cf. [MB], p. 139)

$$\varepsilon(xe + yFe, x'e + y'Fe) = (xy' - yx')\theta,$$

where $\theta := \varepsilon(e, Fe) \in K^\times$ satisfies $\theta^p = -\theta$; in particular, $\theta \in \mathbb{F}_{p^2}$. Moreover, the map $f \mapsto (a, b)$, where $f(e) = ae + bFe$, induces a bijection

$$\mathrm{End}_{\mathbb{D}}(M(G)) \simeq \mathbb{F}_{p^2} \oplus K;$$

cf. [Oo]. If we denote the inverse by $(a, b) \mapsto f_{a,b}$, then a short computation shows that

$$\varepsilon(f_{a,b}(m), f_{a,b}(m')) = a^{p+1}\varepsilon(m, m'), \forall m, m' \in M(G),$$

and so $f_{a,b}$ is an anti-isometry if and only if $a^{p+1} = -1$. Since such an element $a = \alpha \in \mathbb{F}_{p^2}$ exists (take $\alpha = \zeta^{\frac{p-1}{2}}$, where $\zeta \in \mathbb{F}_{p^2}^\times$ is a primitive $p^2 - 1$-root of unity), the maps $f_{\alpha,b}$, with $b \in K$ arbitrary, give rise to infinitely many anti-isometries of $G$.

# 4 A "Mass Formula" for $r(E_1, E_2, N)$

The formula of Theorem 3.1 for the number $r(E_1, E_2, N)$ of reducible anti-isometries $\psi : E_1[N] \xrightarrow{\sim} E_2[N]$ is not only complicated but also difficult to study since the number $h(E_1, E_2, n)$ of isogenies of fixed degree $n$ between $E_1$ and $E_2$ depends heavily on the elliptic curves $E_1$ and $E_2$ and hence cannot be expressed in a convenient (general) form. However, if we fix one elliptic curve $E_1$ and take the weighted sum over all elliptic curves $E_2$ then we obtain a number which is essentially independent of $E_1$ in the sense that it depends only on $p = \mathrm{char}(K)$ and on whether or not $E_1$ is supersingular.

**Theorem 4.1 ("Mass Formula")** *Let $E_1$ be an elliptic curve over $K$. Then*

$$\sum_{E_2} \frac{r(E_1, E_2, N)}{\#\mathrm{Aut}(E_2)} = \frac{1}{2} \sum_{k=1}^{N-1} \sigma(E_1, k(N-k), N), \tag{4.1}$$

*where the sum extends over a system of representatives of the isomorphism classes of elliptic curves $E_2$ over $K$, and $\sigma(E_1, n, m)$ denotes the number of subgroup schemes $H \leq E_1$ of order $n$ which are $m$-primitive. Furthermore we have*

$$\sum_{k=1}^{N-1} \sigma(E_1, k(N-k), N) \leq \sum_{k=1}^{N-1} \sigma(k(N-k), N), \tag{4.2}$$

*and equality holds if and only if $p = \mathrm{char}(K) = 0$ or if $N \leq p$. Here $\sigma(m, N)$ is the arithmetical function defined by*

$$\sigma(n, m) := \sum_{\substack{d|m \\ d^2|n}} \mu(d)\sigma(n/d^2) = \psi(n(m))\sigma(n/n(m)). \tag{4.3}$$

*where $\sigma(n) = \sum_{d|n} d$ and $n(m) = \prod_{p|m} p^{v_p(n)}$ denotes the $m$-component of $n$.*

**Remark 4.2** In [Ka4] the above sums (4.1) and (4.2) are examined in more detail. Specifically, it is shown there that the right side of (4.2) is equal to $\left(\frac{5}{24} - \frac{1}{4N}\right) sl(N)$, which therefore serves as an explicit upper bound of (4.1). Moreover, in the case that $E_1$ is a supersingular curve, the order of magnitude of (4.1) is determined.

Before proving this theorem, let us complement it by calculating the number $\sigma(E, n, m)$ mentioned above. We observe that this number is closely related to the numbers $\psi(E, n, H_0)$ and $\psi'(E, n, H_0)$ of Proposition 3.3 since $\sigma(E, n, n) = \psi(E, n, (0)) = \psi'(E, n, (0))$, and that hence the following result may be viewed as a partial generalization of that proposition.

**Proposition 4.3** *Let $E/K$ be an elliptic curve and let $p = \mathrm{char}(K)$.*

*a) The number of all subgroup schemes of $E$ of order $n$ is*

$$\sigma(E,n) = \sum_{d^2|n} \psi\left(E, \frac{n}{d^2}\right) = \begin{cases} \sigma\left(\frac{n}{n(p)}\right) d(n(p)) & \text{if } E \text{ is ordinary} \\ \sigma\left(\frac{n}{n(p)}\right) & \text{if } E \text{ is supersingular} \end{cases} \tag{4.4}$$

*where $\psi(E,n)$ denotes the number of primitive subgroup schemes of $E$ of order $n$, which is given by*

$$\psi(E,n) = \begin{cases} \psi(p,n), & \text{if } E \text{ is ordinary,} \\ \psi\left(\frac{n}{n(p)}\right)\mu(n(p))^2, & \text{if } E \text{ is supersingular,} \end{cases} \tag{4.5}$$

*b) The number of $m$-primitive subgroup schemes $H \leq E$ of order $n$ is given by*

$$\sigma(E,n,m) = \sum_{\substack{d|m \\ d^2|n}} \mu(d)\sigma(E, n/d^2) = \psi(E, n(m))\sigma(E, n/n(m)). \tag{4.6}$$

*c) Let $n_1, n_2 \in \mathbb{N}$ be integers and put $N = n_1 + n_2$, $d = (n_1, n_2)$, and $k_i = n_i/d$, for $i = 1, 2$. Then the number of pairs $(H_1, H_2)$ of subgroup schemes $H_i \leq E$ of order $n_i$ $(i = 1, 2)$ with $H_1 \cap H_2 = (0)$ is*

$$\pi(E, n_1, n_2) = w(E, n_1, N)\sigma(E, k_1k_2, N) = \sigma(E, n_1n_2, N). \tag{4.7}$$

*Proof.* a) First note that since $\psi(E,n) = \psi(E,n,(0))$, equation (4.5) is a special case of (3.11), and so the second equality of (4.4) follows easily. The first is immediate, for if $H$ is any subgroup scheme of $E$ of order $n$, then there is a unique largest integer $d > 0$ such that $E[d] \leq H$, and then $\overline{H} = H/E[d] \leq \overline{E} = E/E[d] \simeq E$ is a primitive subgroup of $E$.

b) Let $\Sigma(E,n,m)$ denote the set of subgroup schemes of order $n$ which are $m$-primitive. Then clearly

$$\Sigma(E,n,m) = \Sigma(E,n,1) \setminus \bigcup_{\substack{p|m \\ p^2|n}} [p]^{-1}\Sigma(E, n/p^2, 1),$$

and so the first equality of (4.6) follows as in the proof of (3.2). To prove the second equality, viz.

$$\sigma(E,n,m) = \psi(E, m(m))\sigma(E, n/n(m)), \tag{4.8}$$

we may assume by multiplicativity that $n = q^r$, $m = q^s$ are prime powers. If $s = 0$ then $n(m) = 1$, and clearly $\sigma(E,n,1) = \sigma(E,n)$. If $s > 0$ then $n(m) = n$ and $H$ is $m$-primitive if and only if $H$ is primitive (because $H$ is a $q$-group). Thus $\sigma(E,n,m) = \psi(E,n) = \psi(E,n(m))\sigma(E,n/n(m))$, and so (4.8) holds.

c) Let $\Pi(E, n_1, n_2)$ denote the set of pairs $(H_1, H_2)$ in question and consider the map

$$s : \Pi(E, n_1, n_2) \to \Sigma(E, k_1, N) \times \Sigma(E, k_2, N)$$

defined by $s(H_1, H_2) = (H_1[k_1], H_2[k_2])$; note that by Proposition 2.10c), b) we have in fact $H_i[k_i] \in \Sigma(E, k_i, d) = \Sigma(E, k_i, N)$. Now if $K_i \in \Sigma(E, k_i, N)$, for $i = 1, 2$, then by definition (cf. Proposition 3.2) we have

$$s^{-1}(K_1, K_2) = \Omega'(E, d, K_1, K_2).$$

By Proposition 3.2, all these fibres have the same cardinality $w(E, n_1, N)$, and so we obtain

$$\pi(E, n_1, n_2, K_0) = w(E, n_1, N)\sigma(E, k_1, N)\sigma(E, k_2, N) = w(E, n_1, N)\sigma(E, k_1k_2, N),$$

since $(k_1, k_2) = 1$. This proves the first equality.

It remains to prove the rather mysterious identity

$$w(E, n_1, N)\sigma(E, k_1k_2, N) = \sigma(E, n_1n_2, N). \tag{4.9}$$

(It is mysterious because there seems to be no natural map which establishes a bijection between the two sets $\Pi(E, n_1, n_2)$ and $\Sigma(E, n_1n_2, N)$ when $d > 1$.)

Suppose first that $\varepsilon(E, d) = 0$. Then both sides of (4.9) are 0: the left by definition (3.7), and the right by Lemma 2.8c) since here $E$ is supersingular and $p|d$, which means that $p^2|n_1n_2$.

Next, suppose that $\varepsilon(E, d) = 1$. Write $n_i' = n_i(N)$ and $n_i'' = n_i/n_i'$ for $i = 1, 2$; then $(n_1'', n_2'') = 1$ and $k_i(N) = n_i'/d$. Now by definition (3.5) and multiplicativity we have $w(E, n_1, N) = \frac{\psi(p,n_1n_2)}{\psi(p,k_1)\psi(p,k_2)} = \frac{\psi(p,n_1'n_2')\psi(p,n_1'')\psi(p,n_2'')}{\psi(p,n_1'/d)\psi(p,n_1'')\psi(p,n_2'/d)\psi(p,n_2'')} = \frac{\psi(p,n_1'n_2')}{\psi(p,n_1'/d)\psi(p,n_2'/d)}$. Thus, applying (4.6) we obtain

$$w(E, n_1, N)\sigma(E, k_1k_2, N) = \frac{\psi(p, n_1'n_2')}{\psi(p, n_1'/d)\psi(p, n_2'/d)}\psi(E, n_1'n_2'/d^2)\sigma(E, n_1''n_2''). \tag{4.10}$$

Since $\varepsilon(E, d) = 1$, we have that $E$ is ordinary or that $p \nmid d$ ($\Rightarrow \ p \nmid n_1'n_2'$). Then by (4.5) we have $\psi(E, n_1'n_2'/d^2) = \psi(p, n_1'n_2'/d^2) = \psi(p, n_1'/d)\psi(p, n_2'/d)$, and also $\psi(E, n_1'n_2') = \psi(p, n_1'n_2')$, and hence the right hand side of (4.10) reduces (by (4.6) again) to $\psi(E, n_1', n_2')\sigma(E, n_1'', n_2'') = \sigma(E, n_1n_2, N)$, which proves (4.9).

*Proof of Theorem 4.1.* We begin by proving (4.2). For this we first note that if $E_0$ is any elliptic curve over a field $K_0$ of characteristic 0, then by Proposition 4.3 (and (4.5)) we have $\sigma(n, m) = \sigma(E_0, n, m)$ and $\psi(n) = \psi(E_0, n)$, and so we see that (4.3) is a special case of (4.8). We therefore obtain from (4.6), (4.5) and (4.3) the inequality

$$\sigma(E_1, n, m) = \psi(E_1, n(m))\sigma\left(E_1, \frac{n}{n(m)}\right) \leq \psi(n(m))\sigma\left(\frac{n}{n(m)}\right) = \sigma(n, m), \tag{4.11}$$

in which equality holds if and only if $\mathrm{char}(K) \nmid (n, m)$. From this the inequality (4.2) is immediate, and so we see that equality holds in (4.2) if and only if $\mathrm{char}(K) = 0$ or if $N \leq \mathrm{char}(K)$.

We now turn to the proof of (4.1). For this, let $\Pi(E_1, k, N-k)$ be as in the proof of Proposition 4.3c), and let $\Pi(E_1, E_2, k, N-k) = \{(H_1, H_2) \in \Pi(E_1, k, N-k) : E_1/(H_1 + H_2) \simeq E_2\}$. Then the reducibility theorem (Corollary 2.4) yields

$$\frac{r(E_1, E_2, N)}{\#\mathrm{Aut}(E_2)} = \frac{1}{2} \sum_{k=1}^{N-1} \#\Pi(E_1, E_2, k, N-k), \tag{4.12}$$

for if $(f, H_1, H_2)$ is an isogeny diamond configuration of order $N$, then $(H_1, H_2) \in \Pi(E_1, E_2, k, N-k)$ with $k = \#H_1$ and conversely, each $(H_1, H_2) \in \Pi(E_1, E_2, k, N-k)$ comes from an isogeny diamond configuration $(f, H_1, H_2)$, where $f$ is uniquely determined by the condition $\mathrm{Ker}(f) = H_1 + H_2$ up to an automorphism of $E_2$.

From (4.12) we obtain

$$\sum_{E_2} \frac{r(E_1, E_2, N)}{\#\mathrm{Aut}(E_2)} = \frac{1}{2} \sum_{E_2} \sum_{k=1}^{N-1} \#\Pi(E_1, E_2, k, N-k) = \frac{1}{2} \sum_{k=1}^{N-1} \#\Pi(E_1, k, N-k),$$

from which formula (4.1) follows in view of Proposition 4.3c).

We are now ready to derive lower bounds for $n(E_1, E_2, N)$ and thus prove the existence theorem announced in the introduction.

**Theorem 4.4 ("Existence Theorem")** *If $N \neq \mathrm{char}(K)$ is a prime number and $E_1$ or $E_2$ is not supersingular, then*

$$\frac{1}{6} sl(N) < n(E_1, E_2, n) \leq sl(N). \tag{4.13}$$

*Thus, in this situation there always exists a curve $C$ of genus 2 of type $(E_1, E_2, N)$.*

*Proof.* The upper bound in (4.13) follows directly from Theorem 3.4 since by definition $r(E_1, E_2, N) \geq 0$ and $sl(N) = sl(p, N)$. For the lower bound, we shall prove the equivalent inequality

$$r(E_1, E_2, N) < \frac{5}{6} sl(N) = \frac{5}{6} N(N^2 - 1). \tag{4.14}$$

For this, suppose first that $\mathrm{Min}(a(E_1), a(E_2)) \leq 4$ where $a(E_i) := \#\mathrm{Aut}(E_i)$. Then by the mass formula (4.1) together with the symmetry of $r(E_1, E_2, N)$ in $E_1$ and $E_2$ we obtain from (4.2) the estimate

$$r(E_1, E_2, N) \leq 4 \left( \frac{1}{2} \sum_{k=1}^{N-1} \sigma(E_1, k(N-k), N) \right) \leq 2 \sum_{k=1}^{N-1} \sigma(k(N-k)). \tag{4.15}$$

Next we use the following identity:

$$(4.16)\quad \sum_{k=1}^{N-1}\sigma(k(N-k)) = \sum_{k=1}^{N-1}\sigma(k)\sigma(N-k)) = \frac{1}{12}\left(5\sigma_3(N)-(6N-1)\sigma(N)\right) = \left(\frac{5}{12}-\frac{1}{2N}\right)sl(N).$$

Here, the first and third equalities hold because $N$ is prime, whereas the second is a general formula of Glaisher [Gl] (cf. [Ka4] for further discussion of this formula).

Combining (4.15) and (4.16) yields $r(E_1,E_2,N)\le\left(\frac{5}{6}-\frac{1}{N}\right)sl(N)$, which proves (4.14) in the case that $\mathrm{Min}(a(E_1),a(E_2))\le 4$.

Now suppose that $\mathrm{Min}(a(E_1),a(E_2))>4$. Looking at the table of groups of automorphisms of elliptic curves, we see that we then must have $j(E_1)=j(E_2)=0$ (cf. Silverman [Si], p. 103). Thus, to finish the proof it remains to consider the case that $j(E_1)=j(E_2)=0$ and that $E=E_1\simeq E_2$ is ordinary. Here we shall prove the following slightly better result:

$$(4.17)\qquad r(E_1,E_2,N)<\frac{5}{16}sl(N).$$

This, however, follows easily from the estimate

$$(4.18)\qquad h(E,E,m)\le\frac{3}{2}\sigma(m),\ \text{if } m\ge 2,$$

for by Theorem 3.1 and equations (4.18) and (4.16) we obtain

$$r(E,E,N) = \frac{1}{2}\sum_{k=1}^{N-1}h(E,E,k(N-k)) \le \frac{3}{4}\sum_{k=1}^{N-1}\sigma(k(N-k)) = \frac{3}{4}\left(\frac{5}{12}-\frac{1}{2N}\right)sl(N) < \frac{5}{16}sl(N).$$

To prove (4.18), recall that $\mathrm{End}(E)=\mathbb{Z}[\rho]$ where $\rho=\frac{-1+\sqrt{-3}}{2}$. Since this has class number 1 and $|\mathbb{Z}[\rho]^\times|=6$, it follows that $h(E,E,m)=6\nu(m)$, where $\nu(m)$ denotes the number of ideals of $\mathcal{O}=\mathbb{Z}[\rho]$ of norm $m$. From the decomposition of primes in $\mathcal{O}$ one easily sees that (4.18) holds (for more detail, see the proof of Proposition 2.2 of [Ka4]), which finishes the proof of Theorem 4.4.

# References


[Bo] O. Bolza: Über die Reduktion hyperelliptischer Integrale erster Ordnung und erster Gattung auf elliptische, insbesondere über die Reduktion durch eine Transformation vierten Grades. Inaugural Dissertation, Göttingen, 1886.

[Fr] G. Frey: On elliptic curves with isomorphic torsion structures and corresponding elliptic curves of genus 2; in: "Elliptic Curves, Modular Forms & Fermat's Last Theorem" ( J. Coates, S.T. Yau, eds.) International Press Incorporated, Boston, 1995, pp. 79–98.

[FK] G. Frey, E. Kani: Curves of genus 2 covering elliptic curves and an arithmetical application in: "Arithmetic Algebraic Geometry" (G. van der Geer, F. Oort, J. Steenbrink, eds.) Progress in Math. **89**, Birkhäuser, Boston, 1991, pp. 153–176.

[Gl] J. W. L. Glaisher: On the square of the series in which the coefficients are the sums of the divisors of the exponents. *Messenger of Math.* **14** (1884/5), 156–163.

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

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

[Ka1] E. Kani: Curves with elliptic differentials. Preprint.

[Ka2] E. Kani: Curves of genus 2 with elliptic differentials and the height conjecture for elliptic curves; in: "Proc. Conf. Number Theory and Arithmetic Geometry" (G. Frey, ed.) *Publ. Inst. Exp. Math. Essen*, Preprint No. **18** (1991) pp. 30–39.

[Ka3] E. Kani: Elliptic curves on abelian surfaces. *Manuscr. math.* **84** (1994), 199-223.

[Ka4] E. Kani: The existence of curves of genus 2 with elliptic differentials. To appear in *J. Number Theory.*

[Kr] A. Krazer: Lehrbuch der Thetafunktionen. Leipzig, 1903. (Chelsea Reprint, 1970)

[Ku] R. Kuhn: Curves of genus 2 with split Jacobian. *Trans. Am. Math. Soc.* **307** (1988), 41-49.

[La1] H. Lange: Über die Modulvarietät der Kurven vom Geschlecht 2. *J. reine angew. Math.* **281** (1976), 80–96.

[La2] H. Lange: Kurven mit rationaler Abbildung. *J. reine angew. Math.* **295** (1977), 80–115.

[MB] L. Moret-Bailly: Familles des courbes et des variétés abéliennes sur $\mathbb{P}^1$, II. Examples; in: "Seminaire sur les pinceaux des courbes de genre au moins deux" (L. Szpiro, ed.) *Astérisque SMF* **86** (1981), pp. 125–140.

[Mu] D. Mumford: Abelian Varieties. Oxford University Press, London, 1970.

[Mur] N. Murabayashi: The moduli space of curves of genus 2 covering elliptic curves. *Manuscr. math.* **84** (1994), 185-198.

[Od] T. Oda: The first DeRham cohomology group and Dieudonné modules. *Ann. Sci. École Norm. Sup.* **2** (1969), 63–135.

[Oo] F. Oort: Which abelian surfaces are products of elliptic curves? *Math. Ann.* **214** (1975), 35–47.

[Pi] É. Picard: Sur la réduction du nombres des périodes des intégrales abéliennes et, en particular, dans le cas des courbes du second genre. *Bull. Soc. Math. France* **11** (1883), 25-53.

[Se1] J.-P. Serre: Groupes algébriques et corps de classes. Hermann, Paris, 1958.

[Se2] J.-P. Serre: Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini. *C. R. Acad. Sci. Paris* **296** (1983), 397–402 = Oeuvres/Collected Papers III, pp. 658–663.

[Se3] J.-P. Serre: Nombres de points des courbes algébriques sur $\mathbb{F}_q$. *Sem. Th. Nombres Bordeaux* **22** (1982/3) = Oeuvres/Collected Papers III, pp. 664–668.

[Si] J. Silverman: The Arithmetic of Elliptic Curves. Springer-Verlag, New York, 1986.

[We] A. Weil: Zum Beweis des Torellischen Satzes. *Göttinger Nachrichten* 1957, no. 2, 33–53 = Oeuvres Scientifiques/Collected Papers II, pp. 307–327.