JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Martin DJUKANOVIĆ

Families of split Jacobians with isogenous components

Tome 37, nº 1 (2025), p. 49-77.
https://doi.org/10.5802/jtnb.1312

Le Journal de Théorie des Nombres de Bordeaux *est membre du Centre Mersenne pour l'édition scientifique ouverte*
http://www.centre-mersenne.org/
e-ISSN : 2118-8572

Journal de Théorie des Nombres de Bordeaux **37** (2025), 49–77

Families of split Jacobians with isogenous components

par Martin DJUKANOVIĆ

Résumé. Nous présentons des conditions nécessaires et suffisantes sous lesquelles, sur un corps de caractéristique zéro, une N-isogénie entre deux courbes elliptiques sans multiplication complexe induit des courbes C de genre deux dont la jacobienne est (n,n)-isogène au produit des deux courbes elliptiques. Pour $n \leqslant 3$ et $N \leqslant 25$, nous présentons aussi une liste partielle de familles unidimensionnelles des courbes C dont la jacobienne est (n,n)-décomposée et a des composantes qui sont N-isogènes.

Abstract. We exhibit sufficient and necessary conditions under which, over a field of characteristic zero, an N-isogeny between two elliptic curves without complex multiplication induces curves C of genus two whose Jacobian is (n,n)-isogenous to the product of the two elliptic curves. For $n \leqslant 3$ and $N \leqslant 25$, we also present a partial list of one-dimensional families of curves C whose Jacobian is (n,n)-split and has N-isogenous components.

1. Introduction

A curve C of genus two whose Jacobian $\mathrm{Jac}(C)$ is (n,n)-isogenous to a product of two elliptic curves is an old concept, whose roots can be traced to the work of Legendre and Jacobi [14] on hyperelliptic integrals. Details about the classical approach to this topic can be found in [16, Ch. XI]. For the modern approach, the reader is referred to [12, 15, 18]. We give only a brief summary in this section.

Let us fix a base field K over which we consider the following varieties and morphisms between them. Let E be an elliptic curve and let C be a curve of genus two that admits a minimal covering $\phi\colon C \to E$ of degree n, that is, a covering that does not factor through a nontrivial isogeny over an algebraic closure of K.[1] Then there exists an elliptic curve E' such that $\mathrm{Jac}(C)$ is isogenous to $E \times E'$ via an isogeny of degree n^2 whose kernel is isomorphic to the n-torsion subgroups $E[n]$ and $E'[n]$ (as finite abelian group schemes over K). In addition, there exists a minimal covering $\phi'\colon C \to E'$ of degree n over a field over which C admits an embedding into $\mathrm{Jac}(C)$. If n is odd, such

Manuscrit reçu le 2 mai 2023, révisé le 14 janvier 2024, accepté le 20 septembre 2024.
2020 *Mathematics Subject Classification.* 14H10, 14H40, 14H52, 14K02.
Mots-clefs. split Jacobian, elliptic curve, isogeny, binary quadratic form.

[1] These coverings are also called *maximal* or *optimal* in the literature.

an embedding exists over K. Additionally, a minimal covering $\phi' \colon C \to E'$ exists over K if $n = 2$. The isogeny $\varphi \colon E \times E' \to \mathrm{Jac}(C)$ is *polarized* in the following sense. Equipping $E \times E'$ and $\mathrm{Jac}(C)$ with the usual principal polarizations $\lambda \colon E \times E' \xrightarrow{\sim} (E \times E')^\vee$ and $\mu \colon \mathrm{Jac}(C) \xrightarrow{\sim} \mathrm{Jac}(C)^\vee$ makes the following diagram commute:

$$\begin{array}{ccc} E \times E' & \xrightarrow{[n]\lambda} & (E \times E')^\vee \\ \downarrow{\scriptstyle \varphi} & & \uparrow{\scriptstyle \varphi^\vee} \\ \mathrm{Jac}(C) & \xrightarrow{\mu} & \mathrm{Jac}(C)^\vee \end{array}$$

Here the morphism $\varphi^\vee$ is the isogeny dual to φ and $[n]$ is multiplication by n. The principally polarized abelian surface $\mathrm{Jac}(C)$ is said to be (n, n)-*split* and the elliptic curves E and E', seen as embedded in $\mathrm{Jac}(C)$, are said to be *glued along the n-torsion*. We also say that the elliptic curves E and E' are each other's *complement* in $\mathrm{Jac}(C)$ or that they are mutually *complementary* (relative to the given C). We likewise say that the coverings ϕ and ϕ' are mutually complementary. A complete geometric description of the curves (C, E, E') and the minimal coverings (ϕ, ϕ') can be derived, in principle, using the method outlined in [18]. Namely, given $\phi \colon C \to E$, one can determine the complementary covering $\phi' \colon C \to E$. However, due to the high computational complexity of this approach, only the cases $n = 2$ and $n = 3$ are completely known, while the case $n = 4$ is known partially.

The problem can also be stated in reverse. Given elliptic curves E and E' and a maximal isotropic[2] subgroup Γ of the n-torsion subgroup $(E \times E')[n]$, the abelian surface $\mathfrak{A} = (E \times E')/\Gamma$ inherits a principal polarization from $E \times E'$. One wishes to determine a curve C such that $\mathfrak{A} \cong \mathrm{Jac}(C)$ as principally polarized abelian surfaces, assuming that $\mathfrak{A}$ is indeed a Jacobian, which it is generically. The necessary condition that Γ is a maximal isotropic subgroup can equivalently be stated as follows: the subgroup $\Gamma \subset (E \times E')[n]$ is the graph of an isomorphism $\alpha \colon E[n] \xrightarrow{\sim} E'[n]$ that inverts the Weil pairing e_n on $E[n]$ and $E'[n]$, which is to say that

$$e_n(P, Q) = e_n(\alpha(P), \alpha(Q))^{-1} \tag{1.1}$$

for all $P, Q \in E[n](\overline{K})$. We say that an isomorphism $\alpha \colon E[n] \xrightarrow{\sim} E'[n]$ satisfying (1.1) is *anti-symplectic* or we refer to it as an *anti-isometry*. Furthermore, we say that α is *irreducible* (respectively *reducible*) if $\mathfrak{A}$ is (respectively is not) a Jacobian of a curve of genus two (as a principally polarized abelian surface). This approach can be found in [12, 15]. The case $n = 2$ corresponds to *Richelot isogenies*, of which an explicit description

[2] with respect to the Weil pairing

can be found in [7, Ch. 9 & 14] and references therein. The cases $n = 3$ and $n = 4$ are treated in [11] and [6], respectively. Another approach can be found in [19], where moduli spaces of genus-two curves with an (n, n)-split Jacobian are described for $n \leqslant 11$.

In this paper we present the necessary and sufficient conditions under which an N-isogeny $E \to E'$ induces a set of genus-two curves C equipped with an (n, n)-isogeny $E \times E' \to \mathrm{Jac}(C)$, assuming $\mathrm{char}(K) = 0$ (Proposition 2.4). We derive these conditions as a simple consequence of the reducibility criterion of Kani [15]. They amount to a restriction on proper representations of n by integral positive definite diagonal binary quadratic forms of discriminant $-4N$. This explains the origin of the families of curves described in [11, §3C2], as well as some of the special loci presented in [19], and predicts the existence of various such special loci in general. For various $N \leqslant 25$, and not only if $\mathrm{char}(K) = 0$, we also present explicit one-dimensional families of genus-two curves C whose Jacobian admits a $(2, 2)$-isogeny or a $(3, 3)$-isogeny $\mathrm{Jac}(C) \to E \times E'$, where E and E' are N-isogenous elliptic curves (possibly after extending K). The question of existence of such curves was recently treated in [1] when $N \leqslant 7$ is a prime. However, the main proposition of [1] turns out to be incorrect, as the families of curves that we present provide explicit counter-examples to the authors' claims.

Notation and convention. Throughout, K denotes a field of characteristic $\mathrm{char}(K) \neq 2$ and $\overline{K}$ denotes an algebraic closure of K. The base field of curves and surfaces and their ambient spaces is assumed to be K, unless specified otherwise. The affine and the projective space of dimension d are denoted by $\mathbf{A}^d$ and $\mathbf{P}^d$, respectively. If S is a K-scheme, in some contexts we may write S instead of $S(\overline{K})$ for the set of its geometric points. For some purposes, we may implicitly equate a curve with its projective normalization. For an abelian variety A, we denote by $A^\vee$ its dual and for an isogeny $f\colon A \to B$ of abelian varieties we denote by $f^\vee\colon B^\vee \to A^\vee$ the dual isogeny. The Klein four-group is denoted by V_4, while the dihedral group of $2n$ elements is denoted by D_n. The set of *odd* primes is denoted by $\mathfrak{P}$. For two integers $a, b \in \mathbf{Z}$, we denote by (a, b) their greatest common divisor. For an integer n and a prime p, the valuation of n at p is denoted by $v_p(n)$. An integral binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is often denoted by $\langle a, b, c\rangle$ and referred to as a *form* for short. The set of primes represented by (the equivalence class of) the form $\langle a, b, c\rangle$ is denoted by $[a, b, c]$. We will rely on quite a few well established results about binary quadratic forms and representability of integers, for which [8] is a standard reference. A good elementary introduction can also be found in [9, Ch. V]. By $\mathfrak{M}_k$ we denote the set of positive integers N such that k is the genus of the modular curve $X_0(N)$, whose points correspond to elliptic curves that admit a cyclic

N-isogeny. In particular,

$$\mathfrak{M}_0 = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\}, \tag{1.2}$$

$$\mathfrak{M}_1 = \{11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49\}. \tag{1.3}$$

The curves $X_0(N)$ all have rational points for $N \in \mathfrak{M}_0$ (respectively for $N \in \mathfrak{M}_1$) and are therefore rational (respectively elliptic); see [3, 21].

2. Isogeny induced Jacobians

In this section we explain briefly how an N-isogeny $f\colon E \to E'$ induces a set of Jacobians $\mathrm{Jac}(C)$ that are (n, n)-isogenous to $E \times E'$ and we present the necessary and sufficient conditions on N and n under which this occurs.

Suppose that $(N, n) = 1$ so that the restriction $f|_{E[n]}$ of f to $E[n]$ is an isomorphism. Then for each $m \in \mathbf{Z}$ such that $m^2 N \equiv -1 \pmod{n}$ the map $\alpha = [m] \circ f|_{E[n]}$ is an isomorphism that inverts the Weil pairing. Note that the congruence condition on m implies $(m, n) = 1$ so α is indeed an isomorphism. Let Γ_α denote the graph of α and let $\mathfrak{A}_{f,m}$ denote the principally polarized abelian surface $(E \times E')/\Gamma_\alpha$. Note that $\mathfrak{A}_{f,m} \cong \mathfrak{A}_{f,-m}$.

Remark. More generally, if E and E' have complex multiplication, one can also consider $\alpha = \phi \circ f \circ \psi$, with $\psi \in \mathrm{End}(E)$ and $\phi \in \mathrm{End}(E')$. We will ignore this case.

Frey and Kani [12, p. 159] observed that if $m = 1$ and $\deg(f) = n - 1$ then $\mathfrak{A}_{f,m}$ is not a Jacobian. Indeed, we have the following.

Lemma 2.1. *If $f\colon E \to E'$ is an isogeny of degree $n - 1$ then gluing E and E' along the n-torsion via $f|_{E[n]}$ results in the principally polarized abelian surface $E \times E'$.*

Proof. Consider the endomorphisms of $E \times E'$ given by

$$\varphi = \begin{pmatrix} 1 & f^\vee \\ -f & 1 \end{pmatrix}, \qquad \varphi^\vee = \begin{pmatrix} 1 & -f^\vee \\ f & 1 \end{pmatrix}.$$

It is readily verified that

$$\mathrm{Ker}(\varphi) = \{(P, f(P)) \mid P \in E[n]\}$$

and that $\varphi \circ \varphi^\vee = \varphi^\vee \circ \varphi = [n]$. Therefore φ is a polarized isogeny with the required kernel. □

We present a slight generalization of this result.

Proposition 2.2. *Let $f\colon E \to E'$ be an N-isogeny. Suppose that $n = a^2 + Nb^2$, where $(a, n) = (b, n) = (N, n) = 1$, and let $m = a^{-1} \pmod{n}$. Then gluing E and E' along the n-torsion via $\alpha = [mb] \circ f|_{E[n]}$ results in the principally polarized abelian surface $E \times E'$.*

Proof. The proof is analogous to that of Lemma 2.1. Note that α is indeed an anti-isometry because

$$\deg([mb]\circ f) = m^2b^2N = m^2(n-a^2) \equiv -1 \pmod{n}.$$

Consider $\varphi, \varphi^\vee \in \mathrm{End}(E\times E')$ given by

$$\varphi = \begin{pmatrix} [a] & [b]\circ f^\vee \\ -[b]\circ f & [a] \end{pmatrix}, \qquad \varphi^\vee = \begin{pmatrix} [a] & -[b]\circ f^\vee \\ [b]\circ f & [a] \end{pmatrix}.$$

It is readily seen that $\varphi\circ\varphi^\vee = \varphi^\vee\circ\varphi = [n]$. It remains to show that $\mathrm{Ker}(\varphi) = \Gamma_\alpha$. To that end, let $(P,Q)\in\mathrm{Ker}(\varphi)$ so that $[a]P + [b]f^\vee(Q) = 0$ and $[a]Q - [b]f(P) = 0$. Applying $[a]$ to both equations gives

$$\begin{aligned} 0 &= [a^2]P + [b]f^\vee([a]Q) = [a^2]P + [b]f^\vee([b]f(P)) = [a^2+Nb^2]P = [n]P, \\ 0 &= [a^2]Q - [b]f([a]P) = [a^2]Q - [b]f(-[b]f^\vee(Q)) = [a^2+Nb^2]Q = [n]Q, \end{aligned}$$

whence $(P,Q)\in(E\times E')[n]$. Since $[m]$ is an automorphism when restricted to $E'[n]$, we have $Q = [mb]f(P) = \alpha(P)$ and thus $\mathrm{Ker}(\varphi)\subseteq\Gamma_\alpha$. On the other hand, $ma - 1\equiv 0 \pmod{n}$ so for every $P\in E[n]$ we have

$$\varphi(P,\,[mb]f(P)) = ([a+m(n-a^2)]P,\,[b(ma-1)]f(P)) = (0,0).$$

This shows $\Gamma_\alpha\subseteq\mathrm{Ker}(\varphi)$, completing the proof. □

The connection between reducibility of $\alpha\colon E[n]\xrightarrow{\sim} E'[n]$ and isogenies $E\to E'$ was later expanded by Kani into an exact reducibility criterion.

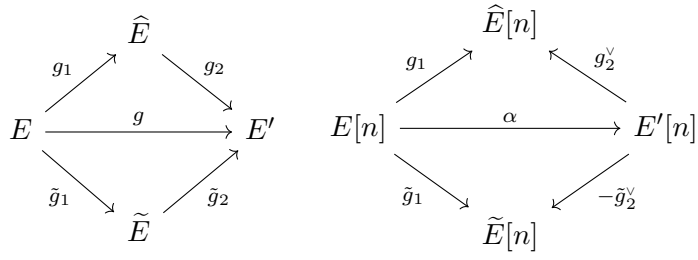
Lemma 2.3 (Kani [15, Corollary 2.4])**.** *The following is true over an algebraically closed field. Let $g\colon E\to E'$ be an isogeny such that $g = g_2\circ g_1 = \widetilde{g}_2\circ\widetilde{g}_1$, where $g_1, g_2, \widetilde{g}_1, \widetilde{g}_2$ are isogenies satisfying:*

(1) $\deg(g_1) + \deg(g_2) = n$,
(2) $\deg(g_1) = \deg(\widetilde{g}_2)$,
(3) $\mathrm{Ker}(g_1)\cap\mathrm{Ker}(\widetilde{g}_1) = \{0\}$.

Then there exists a unique reducible anti-isometry $\alpha\colon E[n]\xrightarrow{\sim} E'[n]$ such that $g_2^\vee\circ\alpha = g_1|_{E[n]}$ and $\widetilde{g}_2^\vee\circ\alpha = -\widetilde{g}_1|_{E[n]}$. Moreover, every reducible anti-isometry arises in this way.

In other words, $\alpha\colon E[n]\xrightarrow{\sim} E'[n]$ is reducible if and only if there exist elliptic curves $\widehat{E}$ and $\widetilde{E}$ and isogenies $g_1, g_2, \widetilde{g}_1, \widetilde{g}_2$ satisfying (1)–(3), such

that the following diagrams commute:



This leads to the following criterion.

Proposition 2.4. *Suppose* $\mathrm{char}(K) = 0$. *Let* $N \geqslant 1$ *and* $n \geqslant 2$ *be coprime integers and let* E *and* E' *be elliptic curves over* K, *without complex multiplication, that admit a cyclic isogeny* $f\colon E \to E'$ *of degree* N, *defined over* K. *Then for each* $m \in \mathbf{Z}$ *such that* $m^2N \equiv -1 \pmod{n}$ *the principally polarized abelian surface* $(E \times E')/\Gamma$, *where* Γ *is the graph of* $[m] \circ f|_{E[n]}$, *is a Jacobian if and only if the following condition holds: if* $a, b, r, s \in \mathbf{N}$ *satisfy* $N = rs$ *and* $ra^2 + sb^2 = n$ *and* $(a, b) = 1$ *then* $a \not\equiv mbs \pmod{n}$.

Proof. Let $f\colon E \to E'$ be a cyclic isogeny of degree N. By assumption, $\mathrm{char}(K) = 0$ and $\mathrm{End}_{\overline{K}}(E) \cong \mathrm{End}_{\overline{K}}(E') \cong \mathbf{Z}$, so $\mathrm{Hom}_{\overline{K}}(E, E') \cong \mathbf{Z}$ with f being a generator. Suppose $m \in \mathbf{Z}$ satisfies $m^2N \equiv -1 \pmod{n}$ so that $\alpha = [m] \circ f|_{E[n]}$ is an anti-isometry. We will show that α is reducible if and only if there exist $a, b, r, s \in \mathbf{N}$ such that

$$N = rs, \quad n = ra^2 + sb^2, \quad (a, b) = 1, \quad a \equiv mbs \pmod{n}.$$

Note that these equalities imply $(r, s) = 1$ since $(N, n) = 1$. The right-to-left implication can be seen as follows. A given factorization $N = rs$ with $(r, s) = 1$ corresponds to distinct isogeny factorizations $(\pm f_1, \pm f_2)$ and $(\pm \widetilde{f}_1, \pm \widetilde{f}_2)$ of f, over a field extension of K, i.e., $f = \widetilde{f}_2 \circ \widetilde{f}_1 = f_2 \circ f_1$, where $\mathrm{Ker}(f_1) \cap \mathrm{Ker}(\widetilde{f}_1) = \{0\}$ and $\deg(f_1) = \deg(\widetilde{f}_2) = r$. Given $a, b \in \mathbf{N}$ such that $n = ra^2 + sb^2$, let

$$g_1 = [a] \circ f_1, \quad g_2 = [b] \circ f_2, \quad \widetilde{g}_1 = [b] \circ \widetilde{f}_1, \quad \widetilde{g}_2 = [a] \circ \widetilde{f}_2, \tag{2.1}$$

and consider the isogeny $g \in \mathrm{Hom}_{\overline{K}}(E, E')$ defined by $g = \widetilde{g}_2 \circ \widetilde{g}_1 = g_2 \circ g_1$. This isogeny and its factorizations clearly satisfy the conditions (1)–(3) in Lemma 2.3. With the morphisms restricted to $E[n]$, conditions $g_2^\vee \circ \alpha = g_1$ and $\widetilde{g}_2^\vee \circ \alpha = -\widetilde{g}_1$ are equivalent to

$$\begin{aligned} [b] \circ f_2^\vee \circ [m] \circ f_2 \circ f_1 &= [b] \circ [m] \circ [s] \circ f_1 = [a] \circ f_1, \\ [a] \circ \widetilde{f}_2^\vee \circ [m] \circ \widetilde{f}_2 \circ \widetilde{f}_1 &= [a] \circ [m] \circ [r] \circ \widetilde{f}_1 = -[b] \circ \widetilde{f}_1. \end{aligned} \tag{2.2}$$

Since $(N,n)=1$, isogenies f_1 and $\widetilde{f}_1$ restrict to isomorphisms on $E[n]$ and therefore (2.2) is equivalent to congruences

$$mbs \equiv a \pmod{n}, \quad -mar \equiv b \pmod{n}.$$

These two congruences are equivalent. Indeed, since $m^2N \equiv -1 \pmod{n}$ and $N = rs$ with $r, s \in (\mathbf{Z}/n\mathbf{Z})^\times$, multiplying the second one by ms gives the first one. By Lemma 2.3, it follows that α is reducible. To show the left-to-right implication, suppose that α is reducible, i.e., there exists an isogeny $g \in \mathrm{Hom}_{\overline{K}}(E, E')$ with two distinct factorizations $g = g_2 \circ g_1 = \widetilde{g}_2 \circ \widetilde{g}_1$, satisfying the conditions of Lemma 2.3. Since $\mathrm{Hom}_{\overline{K}}(E, E')$ is generated by f, the isogeny g is an integer multiple of f. To complete the proof, it suffices to show that the two factorizations of g must be of the form (2.1). Since these factorizations satisfy the conditions (1)–(3) of Lemma 2.3, we must have

$$g_1 = [a] \circ h \circ f_1, \quad g_2 = [b] \circ f_2 \circ h^\vee, \quad \widetilde{g}_1 = [\widetilde{b}] \circ \widetilde{h} \circ \widetilde{f}_1, \quad \widetilde{g}_2 = [\widetilde{a}] \circ \widetilde{f}_2 \circ \widetilde{h}^\vee,$$

where $f_1, f_2, \widetilde{f}_1, \widetilde{f}_2$ are isogenies such that $f = f_2 \circ f_1 = \widetilde{f}_2 \circ \widetilde{f}_1$, and $a, b, \widetilde{a}, \widetilde{b}$ are integers such that $(a,b) = (\widetilde{a}, \widetilde{b}) = 1$, while h and $\widetilde{h}$ are cyclic isogenies whose degrees we will denote by d and $\widetilde{d}$ respectively; in other words, an integral factor $[d]$ (respectively $[\widetilde{d}]$) of g is split between g_1 and g_2 (respectively $\widetilde{g}_1$ and $\widetilde{g}_2$). We will show that $d = \widetilde{d} = 1$. Let $r = \deg(f_1)$ and $s = \deg(f_2)$ so that $N = rs$ and $n = \deg(g_1) + \deg(g_2) = d(ra^2 + sb^2)$. Restrictions of f_1 and $\widetilde{f}_1$ to $E[n]$ are isomorphisms and therefore the equalities $g_2^\vee \circ \alpha = g_1$ and $\widetilde{g}_2^\vee \circ \alpha = -\widetilde{g}_1$, satisfied by assumption, are equivalent to the following two equalities on $f_1(E)[n]$ and $\widetilde{f}_1(E)[n]$ respectively:

$$[mbs - a] \circ h = 0, \quad [mar + b] \circ \widetilde{h} = 0. \tag{2.3}$$

Since h and $\widetilde{h}$ are cyclic, equalities (2.3) are equivalent to the congruences

$$mbs \equiv a \pmod{n}, \quad -mar \equiv b \pmod{n}. \tag{2.4}$$

Let $k, l \in \mathbf{Z}$ be such that $m^2N = -1 + kn$ and $m^2b^2s^2 = a^2 + ln$. Multiplying the latter equation by N and substituting $m^2N = -1 + kn$, followed by $N = rs$ and $n = d(ra^2 + sb^2)$, we obtain $s(ra^2 + sb^2)(1 - b^2dsk + drl) = 0$. Since $s(ra^2 + sb^2) \neq 0$, this implies $d(b^2sk - rl) = 1$, which implies $d = 1$ and therefore $h = [\pm 1]$. A completely analogous argument shows that $\widetilde{h} = [\pm 1]$. By changing the sign of some among $a, b, \widetilde{a}, \widetilde{b}$ and replacing g by $-g$ if necessary, we may assume $h = [1]$, $\widetilde{h} = [1]$ and $a, b, \widetilde{a}, \widetilde{b} > 0$. Since $g = [ab] \circ f = [\widetilde{a}\widetilde{b}] \circ f$, we have $ab = \widetilde{a}\widetilde{b}$. The condition $\deg(g_1) = \deg(\widetilde{g}_2)$ implies $ra^2 = \widetilde{r}\widetilde{a}^2$ and $sb^2 = \widetilde{s}\widetilde{b}^2$, where $\widetilde{r} = \deg(\widetilde{f}_2)$ and $\widetilde{s} = \deg(\widetilde{f}_1)$. Let $u = (\widetilde{a}, b)$ and $v = (a, \widetilde{b})$. Since $(a,b) = 1 = (a,u) = (b,v)$, this implies $u^2 \mid r$ and $v^2 \mid s$, which in turn implies $u^2v^2 \mid N$ and $u^2v^2 \mid n$. Since $(n, N) = 1$,

Table 2.1. The list of all pairs (N, n) for $n \leqslant 41$ that correspond to genus-zero families of (n, n)-split Jacobians with N-isogenous components, induced by the N-isogeny; each pair (N, n) defines a unique family, up to isomorphism, in all these cases.

n	N	n	N
2	$3, 5, 7, 9, 13, 25$	19	$8, 13$
3	$5, 8$	22	7
4	7	23	5
5	$9, 16$	26	$3, 9$
7	$5, 13$	27	$5, 8$
8	7	29	$9, 16$
11	$8, 13$	31	13
13	$16, 25$	32	7
14	3	34	13
16	7	37	$16, 25$
17	$9, 25$	38	3
18	5	41	9

we have $u = v = 1$ and therefore $(a, b, r, s) = (\widetilde{a}, \widetilde{b}, \widetilde{r}, \widetilde{s})$, which means that the two factorizations of g are as in (2.1). □

Remark. If we assume $r < s$ then the same result holds if the last congruence inequality is replaced by $a \not\equiv \pm mbs \pmod{n}$.

Corollary 2.5. *Suppose* $\mathrm{char}(K) = 0$. *For any pair of integers* (N, n) *chosen according to Table 2.1 there exists a unique family of genus-two curves* C, *up to isomorphism, parametrized by a rational curve, such that the Jacobian* $\mathrm{Jac}(C)$ *is* (n, n)*-isogenous to the product of a pair of* N*-isogenous elliptic curves and such that the* (n, n)*-isogeny is induced by the* N*-isogeny.*

Proof. For each $N \in \mathfrak{M}_0$ there exists a rational parametrization of a family of elliptic curves admitting a cyclic N-isogeny over K (see [17, 21]). The isotropy condition on $\Gamma \subset (E \times E')[n]$ is trivial for $n = 2$. Since for odd N the restriction of an N-isogeny $\alpha\colon E \to E'$ to the 2-torsion is an isomorphism, the elliptic curves E and E' can be glued along the 2-torsion via α. By Lemma 2.3, the only obstacle to obtaining a Jacobian in this

way is α being the restriction of an isomorphism $E \xrightarrow{\sim} E'$. Thus for odd values of $N \in \mathfrak{M}_0$ and for each elliptic curve E in a corresponding family parametrized by $X_0(N)$, one obtains a Jacobian by gluing E and E' using the restriction of the N-isogeny to $E[2]$. Similarly, two elliptic curves can be glued along the 3-torsion via an isogeny whose degree N is congruent to 2 modulo 3, since the isotropy condition holds for precisely such N. Only the case $N = 2$ does not result in a Jacobian, by Lemma 2.3. It follows that for $N \in \{5, 8\}$ there is a rational family of curves C of genus two whose Jacobian is $(3, 3)$-split and has N-isogenous components. The remaining cases in Table 2.1 are similarly obtained, by eliminating values of $N \in \mathfrak{M}_0$ for each $n \leqslant 41$, using Proposition 2.4, which is a straightforward computation (e.g., one can perform an exhaustive search). In all listed cases (but not only in these cases) the integer m, such that $\alpha = [m] \circ f|_{E[n]}$ is an anti-isometry, is unique up to sign (modulo n). □

Remark. This contradicts [1], where it is claimed that if K is a number field then there exist only finitely many genus-two curves C, up to isomorphism, whose Jacobian is (n, n)-split as $E \times E'$, where E and E' are N-isogenous elliptic curves and either $n = 3$ and $N = 5$ or $n = 2$ and $N \in \{2, 3, 5, 7\}$ and $\mathrm{Aut}(C) \cong V_4$. We give explicit genus-zero and genus-one families for $n = 2$ and $n = 3$ in Sections 4–5. Note that the family of curves C is in general not unique for a given pair (N, n). For example, for $n = 42$ and $N = 5$ we have $m = \pm 5$ or $m = \pm 19$. The distribution of $N \in \mathfrak{M}_0$ for general n, i.e., the continuation of Table 2.1 beyond $n \leqslant 41$, is established in Proposition 2.9. Before we state it, we will require several lemmas (see, for example, [9, §46]).

Lemma 2.6. *Let N and n be positive integers. A binary quadratic form of discriminant $-4N$ properly represents n if and only if $-N \equiv u^2 \pmod{n}$ for some integer u. Moreover, every proper representation of n by such a form arises from a unique root $u \in (\mathbf{Z}/n\mathbf{Z})^\times$ of $-N$ via equivalence to the form $\langle n, \pm 2u, * \rangle$ and the two proper representations that correspond to $(x, y) = (\pm 1, 0)$.*

Lemma 2.7. *Let n be a positive integer whose prime factorization is $n = 2^k \prod_{i=1}^{r} p_i^{e_i}$, where p_i are pairwise distinct odd primes. Then for any given integer m, the congruence $m \equiv u^2 \pmod{n}$ has a solution u if and only if the congruences $m \equiv u^2 \pmod{p_i}$ and $m \equiv u^2 \pmod{2^k}$ all do. If $(m, n) = 1$ and $m \equiv u^2 \pmod{n}$ is solvable then the number of solutions $u \in (\mathbf{Z}/n\mathbf{Z})^\times$ is 2^r if $k \leqslant 1$, 2^{r+1} if $k = 2$, and 2^{r+2} if $k \geqslant 3$.*

Lemma 2.8. *Let N and n be coprime positive integers and let*

$$\mathcal{R} = \{u \in (\mathbf{Z}/n\mathbf{Z})^\times \mid u^2 \equiv -N \pmod{n}\}.$$

If n is odd then every form of discriminant $-4N$ that properly represents n is primitive. If n is even, so that $n = 2^k m$ with m odd and $k \geqslant 1$, then the following holds:

(1) *If $N \equiv 1 \pmod 4$ then $k = 1$ and $\langle n, \pm 2u, * \rangle$ is primitive for all $u \in \mathcal{R}$.*
(2) *If $N \equiv 3 \pmod 8$ then either $k = 1$ and $\langle n, \pm 2u, * \rangle$ is not primitive for any $u \in \mathcal{R}$ or $k = 2$ and it is primitive for all $u \in \mathcal{R}$.*
(3) *If $N \equiv 7 \pmod 8$ then either $k \leqslant 2$ and $\langle n, \pm 2u, * \rangle$ is not primitive for any $u \in \mathcal{R}$ or $k \geqslant 3$ and it is primitive for precisely half of $u \in \mathcal{R}$.*

Proof. For $u \in \mathcal{R}$ the third coefficient of the form $f = \langle n, \pm 2u, * \rangle$ is determined by the discriminant $-4N$ and equals $c = (u^2+N)/n$. Since $(N, n) = 1$ we must also have $(u, n) = 1$ so if n is odd then f is primitive and if n is even then f is primitive if and only if c is odd. Since 1 is the only nonzero square modulo 4 and modulo 8, we have the following. If $N = 4a + 1$ and $u^2 = 4b + 1$ for some $a, b \in \mathbf{Z}$ then $u^2 + N = 2(2a + 2b + 1) = nc = 2^k mc$, whence $k = 1$ and c is odd. If $N = 8a + 3$ and $u^2 = 8b + 1$ then $u^2 + N = 4(2a + 2b + 1) = 2^k mc$, whence either $k = 2$ and c is odd or $k = 1$ and c is even. Finally, if $N = 8a + 7$ and $u^2 = 8b + 1$ then we have $u^2 + N = 8(a + b + 1) = 2^k mc$, whence either $k \leqslant 2$ and c is even or $k \geqslant 3$, in which case $\mathcal{R}$ has exactly 2^{r+2} elements, exactly half of which are such that b is even, and therefore, whether a is even or odd, exactly half of the roots $u \in \mathcal{R}$ define a primitive form. □

Proposition 2.9. *Suppose* $\operatorname{char}(K) = 0$. *Let N and n be coprime positive integers, and suppose that $n = 2^k \prod_{i=1}^{r} p_i^{e_i}$ is the prime factorization of n, where p_i are pairwise distinct odd primes. Then there exists a rational family of curves C of genus two such that there exists an (n, n)-isogeny $E \times E' \to \operatorname{Jac}(C)$ that is induced by a cyclic N-isogeny $E \to E'$ if and only if one of the following holds:*

(1) *$N = 3$ and $p_i \equiv 1 \pmod 3$ and $n \equiv 2, 6 \pmod 8$;*
(2) *$N = 5$ and $p_i \equiv 1, 3, 7, 9 \pmod{20}$ and $n \equiv 2, 3, 7, 18 \pmod{20}$;*
(3) *$N = 7$ and $p_i \equiv 1, 2, 4 \pmod 7$ and $n \equiv 0 \pmod 2$;*
(4) *$N = 8$ and $p_i \equiv 1, 3 \pmod 8$ and $n \equiv 3 \pmod 8$;*
(5) *$N = 9$ and $p_i \equiv 1 \pmod 4$ and $n \equiv 2, 5 \pmod{12}$;*
(6) *$N = 13$ and $p_i \equiv 1, 7, 9, 11, 15, 17, 19, 25, 29, 31, 47, 49 \pmod{52}$ and $n \equiv 2, 6, 7, 11, 15, 18, 19, 31, 34, 46, 47, 50 \pmod{52}$;*
(7) *$N = 16$ and $p_i \equiv 1 \pmod 4$ and $n \equiv 5 \pmod 8$;*
(8) *$N = 25$ and $5 \neq p_i \equiv 1 \pmod 4$ and $n \equiv 2, 13, 17, 18 \pmod{20}$.*

Proof. Recall that the possible values of N are restricted to the set $\mathfrak{M}_0$, defined by (1.2), since we are looking for families parametrized by rational curves. For each $N \in \mathbf{Z}$, a necessary condition for a cyclic N-isogeny

$E \to E'$ to induce an isogeny $E \times E' \to \mathrm{Jac}(C)$ is the existence of $m \in \mathbf{Z}$ such that $(N, m) = 1$ and $m^2 N \equiv -1 \pmod{n}$. Note that this condition is equivalent to $-N$ being a quadratic residue in $(\mathbf{Z}/n\mathbf{Z})^\times$ and that there is a 1-to-1 correspondence between the solutions m to $m^2 N \equiv -1 \pmod{n}$ and the solutions u to $-N \equiv u^2 \pmod{n}$, given by $u = m^{-1} \pmod{n}$. Let us therefore suppose that $N \in \mathfrak{M}_0$ and that $-N$ is a quadratic residue in $(\mathbf{Z}/n\mathbf{Z})^\times$. For each $N \in \mathfrak{M}_0$ this condition is equivalent to the congruence restrictions on the primes p_i and the exponent k, by Lemma 2.7 and the law of quadratic reciprocity and its supplements. Moreover, this condition implies that $n/2^k$ admits a proper representation by a reduced binary quadratic form of discriminant $-4N$ and that n admits such a representation if and only if 2^k does; these representations are obtained by reducing the primitive forms $\langle n, \pm 2u, * \rangle$ to equivalent reduced forms. By Lemma 2.6, for all proper representations $n = ra^2 + sb^2$ with $N = rs$ and $(a, b) = (r, s) = 1$, if any exist, the integers a and b satisfy $a \equiv mbs \pmod{n}$ for some m because they arise from the root $u = m^{-1} = sba^{-1} \pmod{n}$ of $-N$. This means that the only way for some m to not satisfy $a \equiv mbs \pmod{n}$ is if there exist more roots $u \in (\mathbf{Z}/n\mathbf{Z})^\times$ of $-N$ than there are proper representations of n by diagonal reduced forms of discriminant $-4N$. This can happen for precisely one of the following three reasons:

(i) n is properly representable by a nondiagonal reduced form;
(ii) n (or, equivalently, 2^k) is not properly representable by any form;
(iii) $N \equiv 7 \pmod{8}$ and $n \equiv 0 \pmod{8}$.

Reduced forms of discriminant $-4N$ form a group (with composition of forms) that is isomorphic to the class group of the order $\mathbf{Z}[\sqrt{-N}]$, which can be effectively computed. Note that this class group is trivial precisely for $N \in \{1, 2, 3, 4, 7\} \subset \mathfrak{M}_0$. In that case the only reduced form of discriminant $-4N$ is the principal form $\langle 1, 0, N \rangle$. For the remaining values of $N \in \mathfrak{M}_0$, the class group is isomorphic to $\mathbf{Z}/2\mathbf{Z}$ and the two reduced forms are in different genera, which can be separated by congruences modulo $4N$. Case (i) is only possible if the class group is isomorphic to $\mathbf{Z}/2\mathbf{Z}$ and, given the structure of the class group, it is equivalent to the factorization of n containing an odd number of primes that are represented by the nonprincipal form, counting with multiplicity, assuming the nonprincipal form is nondiagonal. Cases (ii) and (iii) are decided by Lemma 2.7. To complete the proof, all that remains is to consider all the possible cases (i)–(iii) for each N, which is a simple exercise omitted here. □

The following is the analogous result for genus one.

Proposition 2.10. *Suppose* $\mathrm{char}(K) = 0$. *Let* N *and* n *be coprime positive integers. Then there exists a genus-one family of curves* C *of genus two such that there exists an* (n, n)*-isogeny* $E \times E' \to \mathrm{Jac}(C)$ *that is induced*

by a cyclic N-isogeny $E \to E'$ if and only if $-N$ is a quadratic residue in $(\mathbf{Z}/n\mathbf{Z})^\times$ and one of the following holds:

(1) $N = 11$ *and* $n \equiv 0 \pmod 2$ *or* $v_p(n) \not\equiv 0 \pmod 3$ *for some* $p \in [3, 2, 4]$*;*
(2) $N = 14$ *and* $n \equiv 3, 5, 13, 19, 27, 45 \pmod{56}$*;*
(3) $N = 15$ *and* $n \equiv 0 \pmod 2$*;*
(4) $N = 17$ *and either* $v_p(n) \equiv 1 \pmod 2$ *for some* $p \in [3, 2, 6]$ *or there is no such* p *and*

$$\sum_{p\in[2,2,9]} v_p(n) \ + \sum_{p\in[3,2,6]} \tfrac{1}{2}v_p(n) \equiv 1 \pmod 2;$$

(5) $N = 19$ *and* $n \equiv 0 \pmod 2$ *or* $v_p(n) \not\equiv 0 \pmod 3$ *for some* $p \in [4, 2, 5]$*;*
(6) $N = 20$ *and* $n \equiv 3, 7 \pmod{20}$*;*
(7) $N = 21$ *and* $n \equiv 2, 5, 11, 17, 23, 26, 38, 41, 50, 62, 71, 74 \pmod{84}$*;*
(8) $N = 24$ $n \equiv 5, 7 \pmod{24}$*;*
(9) $N = 27$ *and* $n \equiv 0 \pmod 2$ *or* $v_p(n) \not\equiv 0 \pmod 3$ *for some* $p \in [4, 2, 7]$*;*
(10) $N = 32$ *and either* $v_p(n) \equiv 1 \pmod 2$ *for some* $p \in [3, 2, 11]$ *or there is no such* p *and*

$$\sum_{p\in[4,4,9]} v_p(n) \ + \sum_{p\in[3,2,11]} \tfrac{1}{2}v_p(n) \equiv 1 \pmod 2;$$

(11) $N = 36$ *and* $n \equiv 2 \pmod 3$*;*
(12) $N = 49$ *and either* $v_p(n) \equiv 1 \pmod 2$ *for some* $p \in [5, 2, 10]$ *or there is no such* p *and*

$$\sum_{p\in[2,2,25]} v_p(n) \ + \sum_{p\in[5,2,10]} \tfrac{1}{2}v_p(n) \equiv 1 \pmod 2;$$

Proof. The proof is analogous to the proof of Proposition 2.9. The main difference is that the class number of $\mathbf{Z}[\sqrt{-N}]$ can be greater than 2 for $N \in \mathfrak{M}_1$. In particular, case (i) is different, depending on whether the class group is isomorphic to $\mathbf{Z}/2\mathbf{Z}$, which occurs for $N = 15$, or $\mathbf{Z}/3\mathbf{Z}$, which occurs for $N \in \{11, 19, 27\}$, or $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$, which occurs for $N \in \{21, 24\}$, or $\mathbf{Z}/4\mathbf{Z}$, which occurs for $N \in \{14, 17, 20, 32, 36, 49\}$. If the class group is isomorphic to $\mathbf{Z}/4\mathbf{Z}$ then we distinguish between the cases in which the principal genus contains a nondiagonal form, which occurs for $N \in \{17, 32, 49\}$, from the cases in which it does not, which occurs for $N \in \{14, 20, 36\}$. Note that there can exist at most one diagonal nonprincipal reduced form of discriminant $-4N$ for $N \in \mathfrak{M}_1$ because all such N have at most two distinct prime factors. This leads to five different types of cases to consider, depending on N, three of which can be easily described by congruences because in each of them there is no genus containing both

TABLE 2.2. The list of all pairs (N, n) for $n \leqslant 29$ that correspond to genus-one families of (n, n)-split Jacobians with N-isogenous components, induced by the N-isogeny; a pair (N, n) defines a unique family, up to isomorphism, in all these cases.

n	N	n	N
2	$11, 15, 17, 19, 21, 27, 49$	16	15
3	$11, 14, 17, 20, 32$	17	$19, 21, 32, 36, 49$
4	$11, 15, 19, 27$	18	11
5	$11, 14, 19, 21, 24, 36, 49$	19	$14, 27, 32$
6	$11, 17$	20	$11, 19$
7	$17, 19, 20, 24, 27$	21	17
8	15	22	$17, 19$
9	$11, 17, 32$	23	$11, 17, 20, 21$
10	$11, 19, 49$	25	$11, 19, 49$
11	$17, 19, 21, 32$	26	$27, 49$
12	11	27	$14, 17, 20, 32$
13	$14, 17, 27, 49$	28	$19, 27$
14	$17, 19, 27$	29	$24, 36, 49$
15	11		

diagonal and nondiagonal reduced forms. In the two remaining types of cases we have a cyclic class group and a simple argument based on the class group structure leads to the desired conclusion. We omit the details. The sufficient and necessary conditions for $-N$ to be a quadratic residue in $(\mathbf{Z}/n\mathbf{Z})^\times$ and for a prime p to be in one of the sets $[3, 2, 4]$, $[2, 2, 9]$, $[3, 2, 6]$, $[4, 2, 5]$, $[4, 2, 7]$, $[4, 4, 9]$, $[3, 2, 11]$, $[2, 2, 25]$, $[5, 2, 10]$ are given in the Appendix. □

Corollary 2.11. *Suppose* $\mathrm{char}(K) = 0$. *For any pair of integers* (N, n) *chosen according to Table 2.2 there exists a unique family of genus-two curves* C, *parametrized by an elliptic curve, such that the Jacobian* $\mathrm{Jac}(C)$ *is* (n, n)*-isogenous to the product of a pair of* N*-isogenous elliptic curves and the* (n, n)*-isogeny is induced by the* N*-isogeny.*

Remark. As in the genus-zero case, the family of curves C is not uniquely defined by the pair (N, n) in general. For example, for $n = 30$ and $N = 11$ one has $m = \pm 7$ or $m = \pm 13$.

3. Characterizations of (2, 2)-split and (3, 3)-split Jacobians

In this section we state some important prerequisites and summarize our approach to computing, for various N, explicit families of genus-two curves with a $(2, 2)$-split or a $(3, 3)$-split Jacobian with N-isogenous components.

Lemma 3.1. *Let K be a field of characteristic* $\mathrm{char}(K) \neq 2$. *Every $\overline{K}$-isomorphism class of curves of genus two with a $(2, 2)$-split Jacobian is represented by an affine plane model of the form*

$$C\colon y^2 = x^6 + ax^4 + bx^2 + c \tag{3.1}$$

for some $a, b, c \in K$ such that $c(a^2b^2 - 4b^3 - 4a^3c + 18abc - 27c^2) \neq 0$. The curve C admits involutions $(x, y) \mapsto (\pm x, y)$ and it is a double cover of elliptic curves

$$E\colon y^2 = x^3 + ax^2 + bx + c, \quad E'\colon y^2 = x^3 + bc^{-2}x^2 + ac^{-3}x + c^{-4},$$

via $(x, y) \mapsto (x^2, y)$ and $(x, y) \mapsto (c^{-1}x^{-2}, c^{-2}x^{-3}y)$, respectively. The j-invariants of E and E' are

$$\begin{aligned} j(E) &= \frac{256(a^2 - 3b)^3}{a^2b^2 - 4b^3 - 4a^3c + 18abc - 27c^2}, \\ j(E') &= \frac{256(b^2 - 3ac)^3}{c^2(a^2b^2 - 4b^3 - 4a^3c + 18abc - 27c^2)}. \end{aligned} \tag{3.2}$$

Proof. This follows ultimately from [4, §2]. See also [7, Ch. 14] or Corollary 2.7 in [11]. □

There is an analogue for $n = 3$ in the form of the following, more recent result.

Lemma 3.2. *Let K be a field of characteristic* $\mathrm{char}(K) \neq 2$. *With one exception, every $\overline{K}$-isomorphism class of curves of genus two with a $(3, 3)$-split Jacobian is represented by an affine plane model of the form*

$$C\colon y^2 = (x^3 + ax^2 + bx + c)(4cx^3 + b^2x^2 + 2bcx + c^2) \tag{3.3}$$

for some $a, b, c \in K$ such that $c(b^3 - 27c^2)(a^2b^2 - 4a^3c - 4b^3 + 18abc - 27c^2)$ is nonzero. The j-invariants of the components E and E' of $\mathrm{Jac}(C)$ *are*

$$\begin{aligned} j(E) &= \frac{16(a^2b^4 + 216a^2bc^2 - 126ab^3c + 12b^5 - 972ac^3 + 405b^2c^2)^3}{(b^3 - 27c^2)^3(a^2b^2 - 4a^3c + 18abc - 4b^3 - 27c^2)^2}, \\ j(E') &= \frac{256(a^2 - 3b)^3}{a^2b^2 - 4a^3c + 18abc - 4b^3 - 27c^2}. \end{aligned} \tag{3.4}$$

The exception occurs if $\mathrm{char}(K) \neq 3$ *and it is the* $\overline{K}$*-isomorphism class of the curve* $y^2 = (x^3+1)(4x^3+1)$*, whose Jacobian has components of* j*-invariant 1728.*

Proof. See [18, §6], where this result first appeared. Some additional details can be found in [11, §3]. □

Remark. It should be noted here that the cases $n = 2$ and $n = 3$ differ in some fundamental ways (see [18]). For us it is important that curves defined by (3.1) have additional involutions, whereas curves defined by (3.3) generically do not have any additional (geometric) automorphisms. This means that for $n = 2$ there are additional quadratic twists to consider in order to get the complete picture over K. This is explained in Theorem 4.5.2 in [22], for example.

Lemma 3.3. *For every positive integer* N *there exists an effectively computable polynomial* $\Phi_N(X,Y) \in \mathbf{Z}[X,Y]$ *such that if* $\mathrm{char}(K)$ *is either zero or coprime to* N *then two elliptic curves* E_1, E_2 *over* $\overline{K}$ *admit a cyclic* N*-isogeny* $E_1 \to E_2$ *if and only if* $\Phi_N(j(E_1), j(E_2)) = 0$*.*

Proof. The theoretical background can be found in [20, Ch. 5] and [8, §11], for example. For recent work on the computational aspects, see [2]. □

In the remaining sections we will employ these three lemmas to compute families of $(2,2)$-split and $(3,3)$-split Jacobians with isogenous components, relying substantially on the computer algebra system Magma [5] in the process. Some details will be omitted but the reader can verify the results using publicly available code [10]. What follows is the summary of our strategy. For $n \in \{2,3\}$ concrete parametrizations of the coefficients of the defining equations of (C, E, E') are known, up to twists, in terms of parameters $(a,b,c) \in \mathbf{A}^3(K)$, excluding a singular locus (Lemmas 3.1 and 3.2). These parametrizations are such that $(\lambda a, \lambda^2 b, \lambda^3 c)$ defines the same $\overline{K}$-isomorphism class of (C, E, E') for every $\lambda \in K^\times$, so we consider the point (a,b,c) as a representative of the point $[a:b:c]$ in the weighted projective space $\mathbf{P}(1,2,3)$. Thus for both $n = 2$ and $n = 3$, with $j(E)$ and $j(E')$ as in the corresponding lemma, the equation $\Phi_N(j(E), j(E')) = 0$ defines a scheme in this weighted projective space, that we shall denote by $\mathcal{S}_n(N)$. After extending K if necessary, factoring $\Phi_N(j(E), j(E'))$ yields the irreducible components of $\mathcal{S}_n(N)$, which are typically curves of low genus. If $\mathcal{X}$ is one of these curves and its genus is $g(\mathcal{X}) = 0$ and we can find a smooth K-rational point on it, then we can in principle parametrize the curve, i.e., compute a birational map $\rho\colon \mathbf{A}^1 \to \mathcal{X}$, and so obtain a one-dimensional family (in terms of a parameter $t \in K$) of genus-two curves C whose Jacobian has components that are N-isogenous, but not necessarily over K. In particular, it can happen that our choice of parametrization is

such that the corresponding models for E and E' are such that E is only N-isogenous to a quadratic twist of E', with some (square-free) twisting factor $d = d(t) \in K[t]$. This is easily remedied when $n = 2$, by taking instead of C a corresponding d-twist, namely $C_{d,1}\colon y^2 = d^3x^6 + ad^2x^4 + bdx + c$ or $C_{d,2}\colon y^2 = x^6 + adx^4 + bd^2x + cd^3$, equipped with the same pair of 2-to-1 coverings, namely $(x, y) \mapsto (x^2, y)$ and $(x, y) \mapsto (1/x^2, y/x^3)$. Alternatively, we can impose on t the condition that $d(t)$ is a square. If the equation $s^2 = d(t)$ defines a curve of genus zero with a smooth K-rational point then we can parametrize it and compose with ρ, thus obtaining a one-dimensional family of K-curves (C, E, E'), such that E and E' are N-isogenous over K. We execute this strategy for $K = \mathbf{Q}$ (or a quadratic extension, where appropriate) to the extent allowed by the computational power at our disposal. From this we derive families over a general field K, excluding only finitely many values of $\mathrm{char}(K)$.

If $g(\mathcal{X}) = g > 0$ then it is typically computationally expensive to find an arithmetically simple affine plane model of $\mathcal{X}$ and determine whether it has a smooth K-rational point (although one often finds that one of the points with $c = 0$ is smooth for many irreducible components $\mathcal{X}$). In these cases one can consider the quotient of $\mathcal{X}$ by the involution $[a : b : c] \mapsto [b : ac : c^2]$, which corresponds to swapping E and E'. If one can find a K-rational parametrization of the quotient then it is a relatively simple task to lift this to a birational map between $\mathcal{X}$ and an affine plane curve of genus g. We give explicitly only one family of this kind, parametrized by $X_0(11)$, in Subsection 4.5.

On the other hand, the genus-zero cases are all relatively easy to handle and all of the genus-zero families for which the N-isogeny $E \to E'$ induces the (n, n)-isogeny $E \times E' \to \mathrm{Jac}(C)$, in the sense described in Section 2, are given explicitly in Subsection 4.2.

4. Isogenous components of (2, 2)-split Jacobians

In this section we give a list of genus-zero families of genus-two curves C such that the components E and E' of $\mathrm{Jac}(C)$ are N-isogenous, for $N \leqslant 25$. We demonstrate the strategy in detail only for the simple case $N = 1$. For the remaining cases we provide only the tables with the families of curves C. When introducing twists of curves, some notation will be repurposed, but should cause no confusion. For each family, the curve C is given in the form $y^2 = f(x^2)$ for a cubic $f(x) \in K[x]$. The elliptic curve E is always in the isomorphism class of the image of C under $(x, y) \mapsto (x^2, y)$. The coefficients defining each family are chosen so that the N-isogeny $E \to E'$ is always separable (the cases $\mathrm{char}(K) \mid N$ are also covered by our models). The singular loci for which the discriminants of the curves are zero can be

easily computed and are omitted. Explicit models and the j-invariants of E and E' are likewise omitted.

4.1. Isomorphic components. Let C, E, E' be as in Lemma 3.1 and suppose that E and E' are isomorphic over $\overline{K}$, so that $j(E) = j(E')$. Equating the two expressions in (3.2), we obtain

$$(b^3 - a^3c)(b^3 + a^3c - 9abc + 27c^2) = 0, \tag{4.1}$$

which describes a union of two curves of genus zero in $\mathbf{P}(1,2,3)$, both of which can be easily parametrized. The factor $b^3 - a^3c$ defines the family of genus-two curves

$$C\colon y^2 = x^6 + tx^4 + tx^2 + 1 \tag{4.2}$$

for $t \notin \{-1, 3\}$. In this case we have $E = E'$ and the curve (4.2) covers the elliptic curve

$$E\colon y^2 = x^3 + tx^2 + tx + 1, \tag{4.3}$$

with $j(E) = 256t^3/(t+1)$, in two distinct ways. Note that the curve C also admits another involution, namely $(x, y) \mapsto (1/x, y/x^3)$, and is isomorphic to

$$2y^2 = (t+1)x^6 - (t-15)x^4 - (t-15)x^2 + (t+1),$$

via $(x, y) \mapsto ((x-1)/(x+1), 4y/(x+1)^3)$. In fact, $\mathrm{Aut}(C) \cong D_4$ holds generically in this case. Thus C is also a double cover of the elliptic curve

$$\widetilde{E}\colon y^2 = x^3 - 2(t-15)x^2 - 4(t-15)(t+1)x + 8(t+1)^3,$$

whose j-invariant is $j(\widetilde{E}) = -16(t-15)^3/(t+1)^2$, again in two distinct ways. The elliptic curves $\widetilde{E}$ and E are 2-isogenous and the kernels of the isogenies $E \to \widetilde{E}$ and $\widetilde{E} \to E$ are respectively generated by the points $P = (-1, 0)$ and $\widetilde{P} = (-2t-2, 0)$. Moreover, $\mathrm{Jac}(C)$ is obtained by gluing the curve E (respectively $\widetilde{E}$) with itself via the 2-torsion automorphism that fixes P (respectively $\widetilde{P}$) and swaps the other two points of order two (cf. [1], where it is claimed that $\mathrm{Jac}(C)$ is $(2,2)$-isogenous to $E \times \widetilde{E}$).

Parametrizing the curve defined by the second factor in (4.1), and taking an appropriate twist of the corresponding genus-two curve, yields the family

$$C\colon y^2 = x^6 + (t+3)x^4 + tx^2 - 1, \tag{4.4}$$

where $t^2 + 3t + 9 \neq 0$. The curve C defined by (4.4) is a double cover of the elliptic curve

$$E\colon y^2 = x^3 + (t+3)x^2 + tx - 1,$$

whose j-invariant is $j(E) = 256(t^2 + 3t + 9)$, via two distinct coverings, namely $(x, y) \mapsto (x^2, y)$ and $(x, y) \mapsto (-(x^2+1)/x^2,\ y/x^3)$. In this case, the discriminant of E is a square and $\mathrm{Jac}(C)$ is obtained by gluing E with itself via an automorphism of $E[2]$ that does not fix any points of order two.

Generically, two given elliptic curves E and E' can be glued along the 2-torsion in six different ways (over $\overline{K}$, up to isomorphism). This is because the isotropy condition is trivial in the case $n = 2$ and there are six ways to choose an isomorphism $E[2] \xrightarrow{\sim} E'[2]$. Since gluing two elliptic curves along the n-torsion via an isogeny of degree $n - 1$ does not result in a Jacobian (recall Lemma 2.1), there are generically five values of $t \in \overline{K}$ for a given value of $j(E) = j(E')$, rather than six. Moreover, if in (4.4) we replace t with the other value that results in the same value of $j(E)$, we obtain a twist, i.e., a curve in the same $\overline{K}$-isomorphism class. On the other hand, generically, the three curves defined by (4.2) that respectively cover three elliptic curves with the same j-invariant correspond to three distinct $\overline{K}$-isomorphism classes of genus-two curves.

4.2. Isogenous components glued via the isogeny. The six families of curves C from Corollary 2.5 for $n = 2$ are the ones given in Table 4.1 (up to isomorphism over K). These families are identified among the other genus-zero families by using explicit Richelot formulas (e.g., see Proposition 4 in [13]), that allow one to compute the curve C, up to $\overline{K}$-isomorphism, given an anti-isometry $\alpha\colon E[2] \xrightarrow{\sim} E'[2]$. The model of the curve C in each of the families in Table 4.1 is given in the form $y^2 = x^6 - ax^4 + bx^2 - c$. The minuses appear because we need to take a twist of the genus-two curve defined by our chosen parametrization of the corresponding irreducible component of $\mathcal{S}_2(N)$ in order to ensure that E and E' are N-isogenous over K. The first entry of Table 4.1, with $N = 3$, is the family of curves C that generically satisfy $\mathrm{Aut}(C) \cong D_6$.

4.3. General families. Table 4.2 contains the genera of the irreducible components of $\mathcal{S}_2(N)$ for $N \leqslant 14$; the question mark stands for a component whose genus we were not able to determine due to computational complexity.

Table 4.3 contains the corresponding genus-zero families, excluding the ones already listed in Table 4.1.

4.4. Additional splittings. A description of the moduli spaces of genus-two curves with an (n, n)-split Jacobian is given in [19] for $n \leqslant 11$. This can be used to check whether a given curve of genus two has an (n, n)-split Jacobian over $\overline{K}$. Doing so for the families of curves given in Tables 4.1 and 4.3 yields the conclusions listed in the following paragraph (see [10] for the computational details). We emphasize that these statements are not necessarily true over K, except in the case of $(3, 3)$-splittings, where the corresponding isogenies are K-rational and known explicitly [11, §3C].

For curves listed in Table 4.1 the following is true over $\overline{K}$:

$N = 5$: $\mathrm{Jac}(C)$ is $(3, 3)$-split as $E \times E'$;
$N = 7$: $\mathrm{Jac}(C)$ is $(4, 4)$-split as $E \times E'$;

TABLE 4.1. Families of curves of genus two whose Jacobian is $(2,2)$-split and has N-isogenous components that are glued via the isogeny.

N	$C\colon y^2 = x^6 - ax^4 + bx^2 - c$
3	$a = t + 18$ $b = 2t + 81$ $c = t$
5	$a = t^2 + 16t + 50$ $b = 2t^2 + 80t + 625$ $c = t^2$
7	$a = t^3 + 16t^2 + 80t + 98$ $b = 2t^3 + 80t^2 + 784t + 2401$ $c = t^3$
9	$a = t^4 + 16t^3 + 96t^2 + 240t + 162$ $b = 2t^4 + 80t^3 + 864t^2 + 3888t + 6561$ $c = t^4$
13	$a = t^6 + 16t^5 + 112t^4 + 432t^3 + 944t^2 + 1040t + 338$ $b = 2t^6 + 80t^5 + 944t^4 + 5616t^3 + 18928t^2 + 35152t + 28561$ $c = t^6$
25	$a = t^{12} + 16t^{11} + 128t^{10} + 672t^9 + 2560t^8 + 7408t^7 + 16608t^6$ $+ 28912t^5 + 38528t^4 + 37920t^3 + 25600t^2 + 10000t + 1250$ $b = 2t^{12} + 80t^{11} + 1024t^{10} + 7584t^9 + 38528t^8 + 144560t^7$ $+ 415200t^6 + 926000t^5 + 1600000t^4 + 2100000t^3$ $+ 2000000t^2 + 1250000t + 390625$ $c = t^{12}$

$N = 9$: $\mathrm{Jac}(C)$ is $(5,5)$-split as $E \times E'$ and $(3,3)$-split as $\widetilde{E} \times \widetilde{E}$, where $\widetilde{E}$ is 3-isogenous to E and E';

$N = 13$: $\mathrm{Jac}(C)$ is $(7,7)$-split as $E \times E'$.

For curves listed in Table 4.3 the following is true over $\overline{K}$:

$N = 1$: the second family is such that $\mathrm{Jac}(C)$ is $(4,4)$-split as $E \times E$;

$N = 2$: the second family is such that $\mathrm{Jac}(C)$ is $(3,3)$-split as $\widetilde{E} \times \widehat{E}$, where $\widetilde{E}$ and $\widehat{E}$ are elliptic curves admitting a chain of 2-isogenies $E \to \widetilde{E} \to \widehat{E} \to E'$;

$N = 3$: the first family is such that $\mathrm{Jac}(C)$ is $(8,8)$-split as $E \times E'$, while the second family is such that $\mathrm{Jac}(C)$ is $(4,4)$-split as $\widetilde{E} \times \widehat{E}$, where $\widetilde{E}$ and $\widehat{E}$ are such that there exist a 3-isogeny $\widetilde{E} \to \widehat{E}$ and 2-isogenies $E \to \widetilde{E}$ and $E' \to \widehat{E}$;

Table 4.2. Genera of the geometrically irreducible components $\mathcal{X}$ of $\mathcal{S}_2(N)$, defined over $\mathbf{Q}$.

N	$g(\mathcal{X})$	N	$g(\mathcal{X})$
1	$0, 0$	8	$1, 1$
2	$0, 0$	9	$0, 0, 1$
3	$0, 0, 0$	10	$1, 3$
4	$0, 0$	11	$1, 2, 2$
5	$0, 0, 1$	12	$1, ?$
6	$1, 1$	13	$0, 1, 2$
7	$0, 0, 1$	14	$3, 5$

$N = 4$: $\mathrm{Jac}(C)$ is $(4, 4)$-split as $\widetilde{E} \times \widetilde{\widetilde{E}}$, where $\widetilde{\widetilde{E}}$ is 4-isogenous to E and E';
$N = 5$: $\mathrm{Jac}(C)$ is $(6, 6)$-split as $\widetilde{E} \times \widehat{E}$ and there exist a 5-isogeny $\widetilde{E} \to \widehat{E}$ and 2-isogenies $E \to \widetilde{E}$ and $E' \to \widehat{E}$;
$N = 9$: $\mathrm{Jac}(C)$ is $(10, 10)$-split as $\widetilde{E} \times \widehat{E}$ and there exist a 9-isogeny $\widetilde{E} \to \widehat{E}$ and 2-isogenies $E \to \widetilde{E}$ and $E' \to \widehat{E}$. Moreover, $\mathrm{Jac}(C)$ is $(6, 6)$-split as $\bar{E} \times \bar{E}$, where $\bar{E}$ is 3-isogenous to $\widetilde{E}$ and $\widehat{E}$.

4.5. A genus-one family. In this subsection, we describe explicitly a family of genus-two curves parametrized by $X_0(11)$, namely the family corresponding to $n = 2$ and $N = 11$ in Table 2.2. This description is obtained by parametrizing the quotient of the genus-one irreducible component of $\mathcal{S}_2(11)$ under the involution that corresponds to swapping E and E'.

Consider the affine plane curve

$$\mathcal{C}\colon s^2 = (t-1)(t^3 + 17t^2 + 19t + 7).$$

It is birational to the elliptic curve $\mathcal{E}\colon y^2 + y = x^3 - x^2 - 10x - 20$, which is a model of the modular curve $X_0(11)$, via

$$x = \frac{5t+6}{t-1}, \quad y = \frac{11s - (t-1)^2}{2(t-1)^2}.$$

Let $(t, s) \in \mathcal{C}(K)$ be such that $t(t-1)(2t^5 - 38t^4 + 6t^3 + 30t^2 - 9) \neq 0$ and let

$$\begin{aligned} a &= 2 \cdot (2t^5 - 38t^4 + 6t^3 + 30t^2 - 9), \\ b &= 2 \cdot (t^3(t+6)(t^2-1)(t^2+12t-9)s + t^{10} + 26t^9 + 175t^8 \\ &\quad + 108t^7 - 625t^6 + 72t^5 + 567t^4 - 54t^3 - 270t^2 + 54), \\ c &= -2b, \end{aligned}$$

TABLE 4.3. Families of curves of genus two whose Jacobian is $(2,2)$-split and has N-isogenous components that are *not* glued via the N-isogeny.

N	$C\colon y^2 = f(x^2)$
1	$y^2 = x^6 + tx^4 + tx^2 + 1 = (x^2+1)\cdot(x^4 + tx^2 - x^2 + 1)$
1	$y^2 = x^6 + (t+3)x^4 + tx^2 - 1$
2	$y^2 = (2tx^2-1)\cdot(4x^4 + 4(t^2+t+1)x^2 + t^2)$
2	$y^2 = (x^2-t^2)\cdot(tx^2+t+2)\cdot((t+1)x^2+4)$
3	$y^2 = tx^6 + (t^4+8t^3+42t^2+144t-243)x^4$ $+ 16(t^4-16t^3-126t^2-648t-2187)x^2 - 4096t^3$
3	$y^2 = ((t+1)x^2+16(t+9))\cdot(tx^4+(t^4+4t^3-10t^2+36t+81)x^2+256t^3)$
4	$y^2 = (tx^2+1)\cdot(x^4 + 2(2t^4-4t^3+5t^2-4t+2)x^2 + t^4)$
4	$y^2 = ((t-1)x^2 + 4(t+1)(t^2+1))\cdot((t+1)^4x^2 - 4(t-1)^2)$ $\cdot(2(t^2+1)x^2 - (t-1)^2t^3)$
5	$y^2 = (tx^4 - (t-1)^2(t^6-2t^5-5t^4-12t^3-25t^2-50t+125)x^2$ $+ 256t^5(t-1)^4)\cdot(x^2+16(t-5)^2)$
7	$y^2 = tx^6 + (t^8+8t^7+38t^6+128t^5+327t^4+640t^3+910t^2+784t$ $-343)x^4 + (16t^8-256t^7-2080t^6-10240t^5-36624t^4$ $-100352t^3-208544t^2-307328t-268912)x^2 - 4096t^7$
9	$y^2 = ((t^3-1)x^4+t^4(t^{12}-8t^{11}+24t^{10}-24t^9-32t^8+96t^7-64t^6+64t^5$ $-288t^4+352t^3+192t^2+384t+32)x^2+256(t^2-t)^8(t^3-1))$ $\cdot(x^2+16(t+2)^4)$

$$
\begin{aligned}
u_1 &= 121t^{15} + 3751t^{14} + 34364t^{13} + 69212t^{12} - 189970t^{11} - 180806t^{10}\\
&\quad + 368484t^9 + 175140t^8 - 270639t^7 - 135369t^6 + 92961t^5 + 60453t^4\\
&\quad - 8829t^3 - 13041t^2 - 1944t + 1458,\\
u_2 &= 121t^{13} + 2783t^{12} + 15851t^{11} - 605t^{10} - 74415t^9 + 44439t^8 + 69885t^7\\
&\quad - 65187t^6 - 29646t^5 + 39690t^4 + 9963t^3 - 14013t^2 - 1458t + 1944,\\
u &= (u_1 - u_2 s)(2t^5 - 38t^4 + 6t^3 + 30t^2 - 9).
\end{aligned}
$$

Then the hyperelliptic curve $C\colon y^2 = x^6 + aux^4 + bu^2x^2 + cu^3$ has a Jacobian that is $(2,2)$-split as $E \times E'$ in such a way that E and E' are glued along

Table 5.1. Genera of the geometrically irreducible components $\mathcal{X}$ of $\mathcal{S}_3(N)$, defined over $\mathbf{Q}(\sqrt{-3})$.

N	$g(\mathcal{X})$	N	$g(\mathcal{X})$
1	0, 0	5	0, 0, 1, 1
2	0, 0, 0, 0	6	2, ?
3	1, 1	7	3, 3
4	1, 1	8	0, 1, 1, 2

the 2-torsion via the restriction of an 11-isogeny $E \to E'$. The j-invariants of E and E' are the roots of the polynomial

$$\begin{aligned} x^2 + (t^{11} + 55t^{10} + 1188t^9 + 12716t^8 + 69630t^7 + 177408t^6 + 133056t^5 \\ - 132066t^4 - 187407t^3 - 40095t^2 + 24300t + 6750)x \\ + (t^4 - 228t^3 + 486t^2 + 540t + 225)^3 \in K[x]. \end{aligned}$$

Example 4.1. Taking $(t, s) = (2, \pm 11)$, which corresponds to a point of order five on $X_0(11)$, we obtain the hyperelliptic curve

$$C\colon y^2 = x^6 + 55x^4 + 847x^2 + 121,$$

which is a double cover of complementary 11-isogenous elliptic curves

$$\begin{aligned} E\colon y^2 &= x^3 + 55x^2 + 847x + 121, \\ E'\colon y^2 &= x^3 + 847x^2 + 6655x + 14641, \end{aligned}$$

whose j-invariants are $j(E) = -121$ and $j(E') = -24729001$.

5. Isogenous components of (3, 3)-split Jacobians

In this section, $\omega \in \overline{K}$ denotes an element satisfying $1 + \omega + \omega^2 = 0$, i.e., a primitive third root of unity if $\mathrm{char}(K) \neq 3$. Given that a full description of minimal degree-3 coverings $C \to E$ is known from the work of Kuhn [18] (Lemma 3.2), the strategy employed in Section 4 is equally applicable to $(3, 3)$-split Jacobians. Computing the irreducible components of $\mathcal{S}_3(N)$ over $\mathbf{Q}(\sqrt{-3})$ for $N \leqslant 8$ yields curves whose genera are listed in Table 5.1. One irreducible component of $\mathcal{S}_3(2)$ is defined by $c = 0$ and does not correspond to a family of genus-two curves. Of the three remaining irreducible components of $\mathcal{S}_3(2)$, one is defined over $\mathbf{Q}$, while the other two are conjugates defined over $\mathbf{Q}(\sqrt{-3})$. The genus-one components of $\mathcal{S}_3(5)$ and $\mathcal{S}_3(8)$ are also pairs of conjugates defined over $\mathbf{Q}(\sqrt{-3})$. In the remaining cases in Table 5.1, all irreducible components are defined over $\mathbf{Q}$. The question mark in the table stands for a component whose genus we were not able to determine.

Some of the corresponding families of genus-two curves C with a $(3,3)$-split Jacobian with isogenous components have already appeared in the literature. The two families for which $\mathrm{Jac}(C)$ has isomorphic components are described in [11, §3C1]. The two families mentioned in Corollary 2.5 for $n = 3$, namely those for which E and E' are either 5-isogenous or 8-isogenous and glued via the isogeny, are described in [11, §3C2]. One of the former two families and both of the latter two families are such that $\mathrm{Aut}_K(C)$ contains a subgroup isomorphic to V_4, so that $\mathrm{Jac}(C)$ is also $(2,2)$-split. In fact, we have already seen these three families in Section 4. We briefly go over the known families (with slightly simplified parametrizations) before describing additional ones.

For the appropriate values of $t \in K$, the family of genus-two curves given by

$$\begin{aligned}(5.1)\quad C\colon y^2 = {} & \big(x^3 + (t^2+8t+18)x^2 + (2t^2+24t+81)x + t^2\big) \\ & \cdot \big(x^3 - (t^2+8t+18)x^2 + (2t^2+24t+81)x - t^2\big)\end{aligned}$$

has a Jacobian that is $(3,3)$-split as $E \times E$ and also $(2,2)$-split as $E_1 \times E_2$, where the elliptic curves E, E_1, E_2 admit a chain of 3-isogenies

$$E_1 \to E \to E_2.$$

Moreover, the j-invariants of these three elliptic curves are as follows:

$$\begin{aligned} j(E) &= \frac{(t+3)^3(t+9)^3(t^2+27)^3}{t^3(t^2+9t+27)^3}, \\ j(E_1) &= \frac{(t+3)^3(t^3+9t^2+27t+3)^3}{t(t^2+9t+27)}, \\ j(E_2) &= \frac{(t+9)^3(t^3+243t^2+2187t+6561)^3}{t^9(t^2+9t+27)}. \end{aligned}$$

This family of curves is the fourth entry in Table 4.1.

The other family with a $(3,3)$-split Jacobian and isomorphic components can be given, assuming $\mathrm{char}(K) \neq 3$, as $C\colon y^2 = P(x)Q(x)$, where

$$\begin{aligned} P(x) = {} & 4t(t^2-6t-3)x^3 - 3(t^2-6t-3)(t^2w - w^2t - 3)x^2 \\ & + 12tx(t^2+3tw-3w^2) + 4t(t^2+3t-3), \\ Q(x) = {} & 4(t^2+3t-3)(t^2-6t-3)x^3 + 9(t^2+3tw-3w^2)^2x^2 \\ & + 6(t^2+3t-3)(t^2+3tw-3w^2)x + (t^2+3t-3)^2, \end{aligned}$$

for $t \in K(\omega)$ outside a singular locus. The elliptic curve E such that $\mathrm{Jac}(C)$ is $(3,3)$-isogenous to $E \times E$ has j-invariant $j(E) = 27(t-3)^3(t+1)^3/t^3$. Using the explicit description of the moduli spaces of genus-two curves with an (n,n)-split Jacobian given in [19], one can verify that $\mathrm{Jac}(C)$ is also geometrically $(6,6)$-isogenous to $E \times E$ in this case.

If $\mathrm{char}(K) = 3$, we also have the family of genus-two curves

$$C\colon y^2 = x^6 + t^2x^5 + (t^3 - 1)x^3 + 1,$$

each of which is a triple cover of two corresponding supersingular elliptic curves defined by $y^2 = x^3 \pm tx + 1$ for $t \neq 0$.

The family

$$\begin{aligned} C\colon y^2 = {} & (x^3 + (t+10)x^2 + (2t+25)x + t) \\ & \cdot (x^3 - (t+10)x^2 + (2t+25)x - t) \end{aligned} \tag{5.2}$$

of genus-two curves is the second entry in Table 4.1. It is such that $\mathrm{Jac}(C)$ is both $(2,2)$-isogenous and $(3,3)$-isogenous to $E \times E'$, where E and E' are 5-isogenous and glued via the isogeny, both along the 2-torsion and along the 3-torsion. The j-invariants of the two elliptic curves are

$$j(E) = \frac{(t^2 + 10t + 5)^3}{t}, \quad j(E') = \frac{(t^2 + 250t + 3125)^3}{t^5}.$$

The second family mentioned in Corollary 2.5 (Table 2.1, to be precise) for $n = 3$ is equivalent to the fourth entry in Table 4.3 and can also be given as

$$C\colon y^2 = (x^2 - (t-1)^2) \cdot (tx^2 + 4) \cdot ((t-1)x^2 + t + 1). \tag{5.3}$$

The curve C defined by (5.3) is such that $\mathrm{Jac}(C)$ is $(3,3)$-isogenous to $E \times E'$ and $(2,2)$-isogenous to $\widetilde{E} \times \widehat{E}$, where the four elliptic curves admit a chain of 2-isogenies $E \to \widetilde{E} \to \widehat{E} \to E'$. Moreover, we have

$$\begin{aligned} j(E) &= -\frac{16(t^4 - 16t^2 + 16)^3}{t^8(t-1)(t+1)}, \quad j(E') = -\frac{4(t^4 - 60t^3 + 134t^2 - 60t + 1)^3}{t(t-1)^2(t+1)^8}, \\ j(\widetilde{E}) &= \frac{256(t^4 - t^2 + 1)^3}{t^4(t-1)^2(t+1)^2}, \qquad j(\widehat{E}) = \frac{16(t^4 + 14t^2 + 1)^3}{t^2(t-1)^4(t+1)^4}. \end{aligned}$$

In the remainder of the section, we present families of genus-two curves corresponding to the three remaining genus-zero cases from Table 5.1. Henceforth, we assume that $\mathrm{char}(K) \neq 3$.

We deal with the case $N = 2$ first. For the appropriate values of $t \in K$, consider the genus-two curve defined by $C\colon y^2 = xP(x)Q(x)$, where

$$\begin{aligned} P(x) &= 2(t-2)(t^2 + 2t + 4)x^2 + t(t-8)(t-2)(t^2 + 2t + 4)x \\ &\quad - t^2(2t^2 + t + 8)^2, \\ Q(x) &= 4(t-2)^3(t^2 + 2t + 4)x^2 - 12t(t-2)^2(2t-1)(t^2 + 2t + 4)x \\ &\quad + 9t^3(2t^2 + t + 8)^2. \end{aligned} \tag{5.4}$$

The curve C is a triple cover of elliptic curves E and E', whose j-invariants are

$$j(E) = -\frac{8(t^3-32)^3}{t^6}, \quad j(E') = \frac{64(t^3-2)^3}{t^3}.$$

The curves E and E' are 2-isogenous over $K(s)$, where

$$s^2 = -3(t^2+2t+4). \tag{5.5}$$

We note that (5.5) defines a curve of genus zero over $\mathbf{Q}$ that does not have rational points, unlike its twist $s^2 = t^2+2t+4$ that does and that can be easily parametrized. Doing so, reparametrizing the family defined by (5.4) accordingly, and taking a twist to simplify, yields the following family of genus-two curves. Let

$$\begin{aligned}
P(x) &= (2t-1)^3(t^2-t+1)^2(t^2+2t-2)x^2 \\
&\quad + 2(2t-1)(t^2-1)(t^2-t+1)^2(t^2+2t-2)(t^2+8t-5)x \\
&\quad + (t^2-1)^2(4t^4-2t^3+9t^2-14t+7)^2, \\
Q(x) &= 4(2t-1)^2(t^2-t+1)^2(t^2+2t-2)^3x^2 \\
&\quad + 12(2t-1)(t^2-1)(t^2-t+1)^2(t^2+2t-2)^2(4t^2+2t-5)x \\
&\quad + 9(t^2-1)^3(4t^4-2t^3+9t^2-14t+7)^2,
\end{aligned}$$

for suitable values of $t \in K(\omega)$. The genus-two curve $C\colon y^2 = xP(x)Q(x)$ is then a triple cover of elliptic curves E and E' that are 2-isogenous over $K(\omega)$. The j-invariants of E and E' are

$$\begin{aligned}
j(E) &= \frac{64(t^6-3t^4+32t^3-45t^2+24t-5)^3}{(2t-1)^3(t^2-1)^6}, \\
j(E') &= \frac{64(4t^6-12t^4+8t^3+6t-5)^3}{(2t-1)^6(t^2-1)^3}.
\end{aligned}$$

Again using [19], one finds that $\mathrm{Jac}(C)$ is also geometrically $(9,9)$-isogenous to $E \times E'$.

Of the two remaining families for $N = 2$, over $K(\omega)$, we present only one since the other one is obtained by replacing ω by ω^2. Let

$$\begin{aligned}
P(x) &= 16x^2 + t(t^3+(32\omega+4)t^2-(32\omega+88)t+64\omega^2)x \\
&\quad + \omega t^2(t+1)(t^2+(9\omega+2)t-8)^2, \\
Q(x) &= 16(t-8)x^2 + 24\omega t(t^3+(7\omega-4)t^2-(28\omega+32)t-8\omega)x \\
&\quad + 9\omega^2t^3(t^2+(9\omega+2)t-8)^2.
\end{aligned}$$

For suitable values of $t \in K(\omega)$, the genus-two curve $C\colon y^2 = xP(x)Q(x)$ is a triple cover of elliptic curves E and E' that are 2-isogenous over $K(\omega)$.

The j-invariants of E and E' are

$$j(E) = \frac{(t+4)^3(t^3-12t^2+48t+64)^3}{(t-8)^2(t+1)t^6},$$
$$j(E') = \frac{(t-2)^3(t^3-6t^2-12t-8)^3}{(t-8)(t+1)^2t^3}.$$

Now suppose additionally that $\mathrm{char}(K) \neq 5$. Parametrizing the remaining genus-zero component of $\mathcal{S}_3(5)$, we obtain the family $C\colon y^2 = P(x)Q(x)$ of genus-two curves, where, for suitable values of $t \in K$,

$$\begin{aligned}
P(x) &= x^3 + (t^2-2t+5)(t^8-2t^7-4t^6+19t^5-11t^4-37t^3+44t^2+5t+25)x^2 \\
&\quad + 48t^2(t^2-2t+5)(t^6+3t^5-18t^4+22t^3+45t^2-150t+125)x \\
&\quad - 64t^3(t^2-2t+5)^2(t^2-5t+5)(t^6-3t^5-3t^4+37t^3-15t^2-75t+125), \\
Q(x) &= (t^2-5t+5)(t^6-3t^5-3t^4+37t^3-15t^2-75t+125)x^3 \\
&\quad - 9t(t^6+3t^5-18t^4+22t^3+45t^2-150t+125)^2x^2 \\
&\quad + 24t^2(t^2-2t+5)(t^2-5t+5)(t^6-3t^5-3t^4+37t^3-15t^2-75t+125) \\
&\quad\quad \cdot (t^6+3t^5-18t^4+22t^3+45t^2-150t+125)x \\
&\quad - 16t^3(t^2-2t+5)^2(t^2-5t+5)^2(t^6-3t^5-3t^4+37t^3-15t^2-75t+125)^2.
\end{aligned}$$

The curve C is a triple cover of elliptic curves E and E', with j-invariants

$$j(E) = \frac{(t^6+10t^3+5)^3}{t^3}, \quad j(E') = \frac{(t^6+250t^3+3125)^3}{t^{15}}.$$

Moreover, E and E' are 5-isogenous over $K(s)$, where

$$s^2 = -3(t^4+2t^3-t^2+10t+25). \tag{5.6}$$

Similarly to the previous family, we find that the genus-one curve defined by (5.6) over $\mathbf{Q}$ does not have points everywhere locally, unlike

$$s^2 = t^4+2t^3-t^2+10t+25$$

that does and that defines an elliptic curve over $\mathbf{Q}$ defined by the affine model

$$\mathcal{E}\colon y^2+xy+y = x^3+x^2-5x+2. \tag{5.7}$$

The j-invariant of $\mathcal{E}$ is $13997521/225$, while its conductor is 15. Considering the curves over $K(\omega)$, we find a birational map from (5.7) to (5.6) and pre-compose with our parametrization of the family, whence we conclude the following. Taking $t = -(u+v+2)/u$ for $(u,v) \in \mathcal{E}(K(\omega))$ results in a family of genus-two curves C such that $\mathrm{Jac}(C)$ is $(3,3)$-split with 5-isogenous components over $K(\omega)$.

Appendix

Herein we include additional details regarding Proposition 2.10. If $N \in \mathfrak{M}_1$ and $n = 2^k \prod_{i=1}^r p_i^{e_i}$, where p_i are pairwise distinct odd primes, then $-N$ is a quadratic residue in $(\mathbf{Z}/n\mathbf{Z})^\times$ if and only if one of the following holds:

(1) $N = 11$ and $k \leqslant 2$ and $p_i \equiv 1, 3, 4, 5, 9 \pmod{11}$;
(2) $N = 14$ and $k = 0$ and
$p_i \equiv 1, 3, 5, 9, 13, 15, 19, 23, 25, 27, 39, 45 \pmod{56}$;
(3) $N = 15$ and $p_i \equiv 1, 2, 4, 8 \pmod{15}$;
(4) $N = 17$ and $k \leqslant 1$ and
$p_i \equiv 1, 3, 7, 9, 11, 13, 21, 23, 25, 27, 31, 33, 39, 49, 53, 63 \pmod{68}$;
(5) $N = 19$ and $k \leqslant 2$ and $p_i \equiv 1, 4, 5, 6, 7, 9, 11, 16, 17 \pmod{19}$;
(6) $N = 20$ and $k = 0$ and $p_i \equiv 1, 3, 7, 9 \pmod{20}$;
(7) $N = 21$ and $k \leqslant 1$ and
$p_i \equiv 1, 5, 11, 17, 19, 23, 25, 31, 37, 41, 55, 71 \pmod{84}$;
(8) $N = 24$ and $k = 0$ and $p_i \equiv 1, 5, 7, 11 \pmod{24}$;
(9) $N = 27$ and $k \leqslant 2$ and $p_i \equiv 1 \pmod{3}$;
(10) $N = 32$ and $k = 0$ and $p_i \equiv 1, 3 \pmod{8}$;
(11) $N = 36$ and $k = 0$ and $p_i \equiv 1 \pmod{4}$;
(12) $N = 49$ and $k \leqslant 1$ and $p_i \equiv 1 \pmod{4}$.

This is a consequence of the law of quadratic reciprocity, its supplements, and the Chinese remainder theorem. Additionally, one has (see [8, Ch. 2]):

$$[3,2,4] = \left\{ p \in \mathfrak{P} \;\middle|\; \begin{array}{l} p \equiv 1, 3, 4, 5, 9 \pmod{11} \text{ and} \\ x^3 - x^2 - x - 1 \text{ has no roots in } \mathbf{F}_p \end{array} \right\},$$

$$[2,2,9] = \{2\} \cup \left\{ p \in \mathfrak{P} \;\middle|\; \begin{array}{l} p \equiv 1, 9, 13, 21, 25, 33, 49, 53 \pmod{68} \text{ and} \\ x^4 - x^2 - 4 \text{ has no roots in } \mathbf{F}_p \end{array} \right\},$$

$$[3,2,6] = \{p \in \mathfrak{P} \mid p \equiv 3, 7, 11, 23, 27, 31, 39, 63 \pmod{68}\},$$

$$[4,2,5] = \left\{ p \in \mathfrak{P} \;\middle|\; \begin{array}{l} p \equiv 1, 4, 5, 6, 7, 9, 11, 16, 17 \pmod{19} \text{ and} \\ x^3 - 2x - 2 \text{ has no roots in } \mathbf{F}_p \end{array} \right\},$$

$$[4,2,7] = \{p \in \mathfrak{P} \mid p \equiv 1 \pmod{3} \text{ and } x^3 + 2 \text{ has no roots in } \mathbf{F}_p\},$$

$$[4,4,9] = \{p \in \mathfrak{P} \mid p \equiv 1 \pmod{8} \text{ and } x^4 + 4x^3 + 2 \text{ has no roots in } \mathbf{F}_p\},$$

$$[3,2,11] = [3,2,3] = \{p \in \mathfrak{P} \mid p \equiv 3 \pmod{8}\},$$

$$[2,2,25] = \{2\} \cup \left\{ p \in \mathfrak{P} \;\middle|\; \begin{array}{l} p \equiv 1, 9, 25 \pmod{28} \text{ and} \\ x^4 - 7x^2 - 14x - 7 \text{ has no roots in } \mathbf{F}_p \end{array} \right\},$$

$$[5,2,10] = \{p \in \mathfrak{P} \mid p \equiv 5, 13, 17 \pmod{28}\}.$$

Acknowledgments. The author wishes to thank Centre International de Rencontres Mathématiques for providing the environment and the support that made a significant portion of this work possible. The author is also grateful to Pınar Kılıçer for her insightful remarks and to Robin de Jong and the anonymous referee for their helpful feedback on the first draft.

References

[1] L. Beshaj, A. Elezi & T. Shaska, "Isogenous components of Jacobian surfaces", *Eur. J. Math.* **6** (2020), no. 4, p. 1276-1302.

[2] A. J. Best, J. Bober, A. R. Booker, E. Costa, J. E. Cremona, M. Derickx, M. Lee, D. Lowry-Duda, D. Roe, A. V. Sutherland & J. Voight, "Computing classical modular forms", in *Arithmetic geometry, number theory, and computation*, Simons Symposia, Springer, 2021, p. 131-213.

[3] B. J. Birch & W. Kuyk (eds.), *Modular functions of one variable. IV. Proceedings of the International Summer School on Modular Functions of One Variable and Arithmetical Applications, RUCA, University of Antwerp, Antwerp, July 17–August 3, 1972*, Lecture Notes in Mathematics, vol. 476, Springer, 1975.

[4] O. Bolza, "On Binary Sextics with Linear Transformations into Themselves", *Am. J. Math.* **10** (1887), no. 1, p. 47-70.

[5] W. Bosma, J. J. Cannon & C. Playoust, "The Magma Algebra System I: The Use Language", *J. Symb. Comput.* **24** (1997), p. 235-265, Magma's homepage is at `http://magma.maths.usyd.edu.au/magma`.

[6] N. Bruin & K. Doerksen, "The arithmetic of genus two curves with $(4, 4)$-split Jacobians", *Can. J. Math.* **63** (2011), no. 5, p. 992-1024.

[7] J. W. S. Cassels & E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, London Mathematical Society Lecture Note Series, vol. 230, Cambridge University Press, 1996.

[8] D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, third ed., AMS Chelsea Publishing, vol. 387, American Mathematical Society, 2022.

[9] L. E. Dickson, *Introduction to the Theory of Numbers*, University of Chicago Press, 1929.

[10] M. Djukanović, "split-jacobians", GitHub repository, `https://github.com/martin-djukanovic/split-jacobians`.

[11] ———, "Families of (3,3)-split Jacobians", *Rocky Mt. J. Math.* **54** (2024), no. 6, p. 1621-1654.

[12] G. Frey & E. Kani, "Curves of genus 2 covering elliptic curves and an arithmetical application", in *Arithmetic algebraic geometry (Texel, 1989)*, Progress in Mathematics, vol. 89, Birkhäuser, 1991, p. 153-176.

[13] E. W. Howe, F. Leprévost & B. Poonen, "Large torsion subgroups of split Jacobians of curves of genus two or three", *Forum Math.* **12** (2000), no. 3, p. 315-364.

[14] C. G. J. Jacobi, "Review of Legendre's 'Traité des fonctions elliptiques, troisième supplément"', *J. Reine Angew. Math.* **8** (1832), p. 413-417.

[15] E. Kani, "The number of curves of genus two with elliptic differentials", *J. Reine Angew. Math.* **485** (1997), p. 93-121.

[16] A. Krazer, *Lehrbuch der Thetafunktionen*, Chelsea Publishing Company, 1970.

[17] D. S. Kubert, "Universal bounds on the torsion of elliptic curves", *Compos. Math.* **38** (1979), no. 1, p. 121-128.

[18] R. M. Kuhn, "Curves of genus 2 with split Jacobian", *Trans. Am. Math. Soc.* **307** (1988), no. 1, p. 41-49.

[19] A. Kumar, "Hilbert modular surfaces for square discriminants and elliptic subfields of genus 2 function fields", *Res. Math. Sci.* **2** (2015), article no. 24 (46 pages).

[20] S. Lang, *Elliptic functions*, second ed., Graduate Texts in Mathematics, vol. 112, Springer, 1987.

[21] B. Mazur & D. Goldfeld, "Rational isogenies of prime degree", *Invent. Math.* **44** (1978), p. 129-162.
[22] B. Poonen, *Rational points on varieties*, Graduate Studies in Mathematics, vol. 186, American Mathematical Society, 2017.

Martin Djukanović
Groningen, The Netherlands
E-mail: martin.djukanovic@prona.org