

ENDOMORPHISM ALGEBRAS OF GEOMETRICALLY SPLIT GENUS 2 JACOBIANS OVER \mathbb{Q}

FRANCESC FITÉ, ENRIC FLORIT, AND XAVIER GUITART

ABSTRACT. The main result of [FG20] classifies the 92 geometric endomorphism algebras of geometrically split abelian surfaces defined over \mathbb{Q} . We show that 54 of them arise as geometric endomorphism algebras of Jacobians of genus 2 curves defined over \mathbb{Q} , and that the remaining 38 do not. In particular, we exhibit 38 examples of $\overline{\mathbb{Q}}$ -isogeny classes of abelian surfaces defined over \mathbb{Q} that do not contain any Jacobian of a genus 2 curve defined over \mathbb{Q} , and for each of the 54 algebras that do arise we exhibit a curve realizing them.

1. INTRODUCTION

Let A be an abelian surface defined over \mathbb{Q} . We say that A is *geometrically split* if its base change $A_{\overline{\mathbb{Q}}}$ to $\overline{\mathbb{Q}}$ is isogenous to the product of two elliptic curves. By the *geometric endomorphism algebra of A* , denoted $\mathcal{X}(A)$, we refer to the ring of endomorphisms of $A_{\overline{\mathbb{Q}}}$ tensored with \mathbb{Q} . Let \mathcal{A} denote the set of isomorphism classes of $\mathcal{X}(A)$, where A runs over the set of geometrically split abelian surfaces over \mathbb{Q} . The finiteness of \mathcal{A} can be deduced from the theory of complex multiplication and Heilbronn's proof of the Gauss class number problem (see [Sha96, p. 103]).

The main result of [FG20], relying on previous results of [FG18], provides an explicit description of \mathcal{A} . In order to state it, we need to introduce some notations. Denote by \mathcal{D}_1 (resp. \mathcal{D}_2) the finite set of absolute values of discriminants of imaginary quadratic fields of class number 1 (resp. of class number 2). We also denote by $\mathcal{D}_{2,2}$ the finite set of absolute values of discriminants of imaginary quadratic fields with class group isomorphic to $C_2 \times C_2$. By the Gauss class number problem, the sets \mathcal{D}_1 , \mathcal{D}_2 , and $\mathcal{D}_{2,2}$ are finite. Using the discriminant bounds of [Wat03], for example, one can determine these sets, which are as displayed on the table below.

\mathcal{D}_1	3, 4, 7, 8, 11, 19, 43, 67, 163
\mathcal{D}_2	15, 20, 24, 35, 40, 51, 52, 88, 91, 115 123, 148, 187, 232, 235, 267, 403, 427
$\mathcal{D}_{2,2}$	84, 120, 132, 168, 195, 228, 280, 312, 340, 372, 408, 435 483, 520, 532, 555, 595, 627, 708, 715, 760, 795, 1012, 1435

Note that \mathcal{D}_1 , \mathcal{D}_2 , and $\mathcal{D}_{2,2}$ have cardinalities 9, 18, and 24 respectively. Then the main result of [FG20] is the following.

Theorem 1.1 ([FG20]). *The set \mathcal{A} consists of:*

- i) $\mathbb{Q} \times \mathbb{Q}$; $\mathbb{Q} \times \mathbb{Q}(\sqrt{-d})$ for $d \in \mathcal{D}_1$; $\mathbb{Q}(\sqrt{-d}) \times \mathbb{Q}(\sqrt{-d'})$ for distinct $d, d' \in \mathcal{D}_1$;*

Date: December 21, 2022.

ii) $M_2(\mathbb{Q}); M_2(\mathbb{Q}(\sqrt{-d}))$ for $d \in \mathcal{D}_1 \cup \mathcal{D}_2 \cup \mathcal{D}_{2,2}^S$, where

$$(1.1) \quad \mathcal{D}_{2,2}^S := \mathcal{D}_{2,2} \setminus \{195, 312, 340, 555, 715, 760\}.$$

In particular, the set \mathcal{A} has cardinality 92.

The challenging part of the proof of the above result is that involving quadratic imaginary fields of class number 4. In this case, the proof of the above theorem takes place in two steps. Suppose that A is an abelian surface for which $\mathcal{X}(A) \simeq M_2(\mathbb{Q}(\sqrt{-d}))$ for $d \in \mathcal{D}_{2,2}$. First, one establishes that A occurs as a factor of the restriction of scalars of a Gross \mathbb{Q} -curve from the Hilbert class field of $\mathbb{Q}(\sqrt{-d})$ down to \mathbb{Q} . Second, one determines the isogeny decomposition of any such restriction of scalars using a method due to Nakamura [Nak04]. Then the set $\mathcal{D}_{2,2}^S$ is obtained as a corollary of this computation. Note that a consequence of the first step in the proof is that for such an A the minimal field over which all endomorphisms of A are defined is the Hilbert class field of $\mathbb{Q}(\sqrt{-d})$, a result that will again play a key role in the present work.

In this article we consider the question (see [FG20, Question 4.4]) of determining the subset $\mathcal{B} \subseteq \mathcal{A}$ of geometric endomorphism algebras of Jacobians of genus 2 curves defined over \mathbb{Q} . We obtain a complete answer to this question.

Theorem 1.2. *The set \mathcal{B} consists of:*

i) $\mathbb{Q} \times \mathbb{Q}; \mathbb{Q} \times \mathbb{Q}(\sqrt{-d})$ for $d \in \mathcal{D}_1; \mathbb{Q}(\sqrt{-d}) \times \mathbb{Q}(\sqrt{-d'})$ for
 $(d, d') \in \{(4, 3), (7, 4), (8, 4)\}.$

ii) $M_2(\mathbb{Q}), M_2(\mathbb{Q}(\sqrt{-d}))$ for $d \in \mathcal{D}_1 \cup \mathcal{D}_2 \cup \mathcal{D}_{2,2}^J$, where

$$(1.2) \quad \mathcal{D}_{2,2}^J := \mathcal{D}_{2,2}^S \setminus \{280, 483, 595, 627, 795\}.$$

In particular, the set \mathcal{B} has cardinality 54.

The interesting cases of the proof of the above result are: a) that involving the product of two distinct quadratic imaginary fields; b) that involving a quadratic imaginary field of class number 4. The remaining cases are handled in §2, a section included for the sake of completeness, but whose results are well known to the experts. We do not claim any originality in this section, except maybe for the precise form of Proposition 2.4. This result provides a Galois group theoretic sufficiency criterion for applying the explicit gluing method of Howe, Leprévost, and Poonen [HLP00] to a CM elliptic curve over a quadratic field and its Galois conjugate along the 2-torsion. It allowed us finding some curves attached to quadratic imaginary fields of class number 2 that we were not able to locate anywhere else in the literature.

We effectuate the proof of Theorem 1.2 in the aforementioned case a) in §3. The proof relies on a criterion by Frey and Kani [FK91] that recasts the possibility of gluing two elliptic curves E and E' into a genus 2 curve in terms of the existence of an isomorphism of Galois modules $E[N] \simeq E'[N]$, for some $N \geq 2$, that is moreover an anti-isometry for the Weil pairings. We exploit the idea that, due to the presence of a large proportion of 0 Frobenius traces, only under exceptional circumstances may one find CM elliptic curves E and E' nonisogenous over \mathbb{Q} such that $E[N]$ and $E'[N]$ are isomorphic as Galois modules for some $N \geq 2$. In fact, to narrow down the possibilities for (d, d') to one of $(4, 3)$, $(7, 4)$, or $(8, 4)$ we make no use of the

anti-isometry requirement. This idea is made precise via a Chebotarev style type of argument.

The proof of Theorem 1.2 in the aforementioned case b) takes place in §4. Suppose that C is a genus 2 curve for which $\mathcal{X}(\text{Jac}(C)) \simeq \text{M}_2(\mathbb{Q}(\sqrt{-d}))$ for $d \in \mathcal{D}_{2,2}$. Combining the already mentioned result from [FG20] that the minimal field of definition over which all the endomorphisms of $\text{Jac}(C)$ are defined is the Hilbert class field of $\mathbb{Q}(\sqrt{-d})$ with [JKPRST18] and [Kan11], we infer that $\text{Jac}(C)$ is $\overline{\mathbb{Q}}$ -isomorphic to the product of two elliptic curves with complex multiplication by the maximal order of $\mathbb{Q}(\sqrt{-d})$. The necessity for d to belong to $\mathcal{D}_{2,2}^J$ then is deduced from the recent work by Narbonne [Nar22]. It then remains to show that the algebras $\text{M}_2(\mathbb{Q}(\sqrt{-d}))$ for every $d \in \mathcal{D}_{2,2}^J$ actually occur as geometric endomorphism algebras of genus 2 curves defined over \mathbb{Q} . For every $d \in \mathcal{D}_{2,2}^J$, a heuristic candidate curve was communicated to us either by Elkies or by Narbonne–Ritzenthaler. Finally, we certify the correctness of these curves using the work of Kumar [Kum15].

It follows from [Wei57] and the aforementioned result by Frei and Kani that any $\overline{\mathbb{Q}}$ -isogeny class of abelian surfaces defined over $\overline{\mathbb{Q}}$ contains the Jacobian of a curve defined over $\overline{\mathbb{Q}}$. As a byproduct of Theorems 1.1 and 1.2, we obtain 38 distinct $\overline{\mathbb{Q}}$ -isogeny classes of abelian surfaces containing an abelian surface defined over \mathbb{Q} but no Jacobian of a curve defined over \mathbb{Q} .

Some of the computations in this article are done with the help of mathematical software SageMath [S⁺09] and MAGMA [BCP97]. All code files that we have used can be found at the repository <https://github.com/xguitart/EndAlgebrasg2>.

Notation and terminology. Throughout the paper $\overline{\mathbb{Q}}$ will denote a fixed algebraic closure of \mathbb{Q} . All number fields considered are assumed to be contained in $\overline{\mathbb{Q}}$. For a number field F , let \mathcal{O}_F denote its ring of integers and let G_F be the absolute Galois group $\text{Gal}(\overline{\mathbb{Q}}/F)$. For an abelian variety A defined over F and an integer $N \geq 2$, let $A[N]$ denote the set of $\overline{\mathbb{Q}}$ -points of the N -torsion group scheme of A . For a prime ℓ , let $V_\ell(A) := \mathbb{Q}_\ell \otimes \varprojlim_n A[\ell^n]$ be the rational ℓ -adic Tate module of A , and denote by $\varrho_A := \varrho_{A,\ell}$ the ℓ -adic representation encoding the action of G_F on $V_\ell(A)$. For a nonzero integral prime \mathfrak{p} of \mathcal{O}_F of good reduction for A , define $a_{\mathfrak{p}}(A)$ as the trace $\text{Tr}(\varrho_A(\text{Frob}_{\mathfrak{p}}))$, where $\text{Frob}_{\mathfrak{p}}$ is a Frobenius element at \mathfrak{p} . We will denote by $\overline{\varrho}_{A,N}$ the representation given by the action of G_F on $A[N]$. We will denote by $F(A[N])$ the field obtained by adjoining the coordinates of the points of $A[N]$ to F (equivalently, $F(A[N])$ is the field cut out by the representation $\overline{\varrho}_{A,N}$). We will denote by $F(x(A[N]))$ the field obtained by adjoining the x -coordinates of the points of $A[N]$ to F . The geometric endomorphism algebra of A will be denoted by $\mathcal{X}(A)$. If C is a curve, we will simply write $\mathcal{X}(C)$ to denote $\mathcal{X}(\text{Jac}(C))$. If B is another abelian variety defined over F , then we write $A \sim B$ (resp. $A \simeq B$) to denote that A and B are isogenous (resp. isomorphic). We say that an elliptic curve E has complex multiplication (CM) by a quadratic imaginary field M if it has CM by some order \mathcal{O} in M . We use this phrasing when the specific choice of \mathcal{O} is irrelevant for the argument involved.

Acknowledgements. We are indebted to several colleagues for contributions that made possible this work. Thanks to N. Elkies for providing a key argument to complete the proof of Proposition 3.2 and for supplying some extraordinary genus 2 curves that motivated the start of this article. Thanks to A. Sutherland for sharing a data base of pairs of isomorphic torsion Galois modules of elliptic curves (with

overwhelming evidence that Theorem 3.6 should be true) and for granting us access to the MIT server Legendre, where some of the computations of this article were carried out. Thanks to F. Narbonne for sharing with us the work [Nar22], essential in the proof of Proposition 4.5. Thanks to F. Narbonne and C. Ritzenthaler for supplying some extraordinary genus 2 curves that facilitated the completion of this article. Thanks to E. Costa, E. Howe, and S. Schiavone for helpful conversations. Thanks to the LMFDB as a source of examples used in §3.1. Guitart expresses his gratitude to the Massachusetts Institute of Technology for its warm hospitality during a visit in January 2020. Fité was financially supported by the Ramón y Cajal fellowship RYC-2019-027378-I and the Simons Foundation grant 550033. Florit and Guitart were partially funded by project PID2019-107297GB-I00. Florit was partially supported by the Spanish Ministry of Universities (FPU20/05059). Fité and Guitart acknowledge support from the María de Maeztu Program of excellence CEX2020-001084-M.

2. THE BASIC CASES

In this section we treat those cases of geometric endomorphism algebras involving at most one quadratic imaginary field, which we further assume of class number ≤ 2 . Along the way, we present a gluing construction of elliptic curves that will be also used in Section 3.

2.1. Class number 1. Examples of genus 2 curves C defined over \mathbb{Q} for which $\mathcal{X}(C) \simeq \mathbb{Q} \times \mathbb{Q}$ or $M_2(\mathbb{Q})$ are well known (see for example the rows for $N(G_{3,3})$ and E_1 of [FKRS12, Table 11], respectively). The next proposition provides examples of genus 2 curves C defined over \mathbb{Q} such that $\mathcal{X}(C) \simeq \mathbb{Q} \times M$, where M is an imaginary quadratic field of class number 1.

Proposition 2.1. *For each $d \in \mathcal{D}_1$, consider the pair $(a, b) \in \mathbb{Z}^2$ given by Table 1. If C denotes the curve given by $C: y^2 = x^6 + ax^2 + b$, then $\mathcal{X}(C) \simeq \mathbb{Q} \times \mathbb{Q}(\sqrt{-d})$.*

(a, b)	d	(a, b)	d	(a, b)	d
$(-15, 22)$	3	$(-30, -56)$	8	$(-3440, 77658)$	43
$(-11, 14)$	4	$(-264, 1694)$	11	$(-29480, 1948226)$	67
$(-35, 98)$	7	$(-152, 722)$	19	$(-8697680, 9873093538)$	163

TABLE 1. Coefficients for genus 2 curves C with $\mathcal{X}(C) \simeq \mathbb{Q} \times \mathbb{Q}(\sqrt{-d})$.

Proof. The curve C admits obvious degree 2 maps to the elliptic curves

$$E: y^2 = x^3 + ax + b, \quad E': y^2 = x(x^3 + ax + b).$$

A straightforward computation shows that, for each pair (a, b) of Table 1, the j -invariant of E is that of an elliptic curve with CM by $\mathbb{Q}(\sqrt{-d})$ (cf. [Sil94, page 183]), while the j -invariant of E' is not integral and thus E' does not have CM. \square

To conclude the exploration of cases involving fields of class number 1, we recall that the literature contains examples of genus 2 curves defined over \mathbb{Q} such that $\mathcal{X}(C) \simeq M_2(\sqrt{-d})$ for every $d \in \mathcal{D}_1$. For the sake of completeness, explicit examples of all of them are provided in §5. The curves $y^2 = x^6 + 1$ and $y^2 = x^5 - x$ are well known to correspond to the cases $d = 3, 8$. For $d = 4, 7$ we borrow examples from [Car01], and for $d = 11, 19, 43, 67, 163$ the curves are taken from [GHR19].

2.2. Gluing of elliptic curves. Although the results recalled in this section hold in greater generality, we will state them relative to a number field F . This will be enough for our purposes.

The following result of Frey and Kani (see [FK91, §1]) will be used in §4 as a fundamental tool to find an upper bound on the set \mathcal{B} of Theorem 1.2.

Proposition 2.2 ([FK91]). *Let C be a genus 2 curve defined over F such that $\text{Jac}(C)$ decomposes up to isogeny. Then there exist elliptic curves E and E' defined over F , a natural number $N \geq 2$ and an isomorphism $\psi: E[N] \rightarrow E'[N]$ of $(\mathbb{Z}/N\mathbb{Z})[G_F]$ -modules which is also an anti-isometry of the Weil pairings such that*

$$\text{Jac}(C) \simeq (E \times E') / \Gamma,$$

where Γ is the graph of ψ , that is, the group scheme with $\Gamma(\overline{\mathbb{Q}}) = \{(P, \psi(P))\}_{P \in E[N]}$.

For $N = 2$, there is an explicit converse of the above result due to Howe, Leprévost and Poonen (see [HLP00, Propositions 3 and 4]). It will be used in §2.3 and §3.2, in order to realize some of the elements in \mathcal{B} as geometric endomorphism algebras of Jacobians over \mathbb{Q} . Although it will not be used in this article, we note that there is also an explicit converse to the above result for $N = 3$ (see [BHLS15, Alg. 5.4, Thm. 5.5]).

Proposition 2.3 ([HLP00]). *Let E and E' be elliptic curves defined over F such that there exists an isomorphism $\psi: E[2] \rightarrow E'[2]$ of $(\mathbb{Z}/2\mathbb{Z})[G_F]$ -modules which is not the restriction to $E[2]$ of an isomorphism $E_{\overline{\mathbb{Q}}} \rightarrow E'_{\overline{\mathbb{Q}}}$. Then:*

i) *There exists a genus 2 curve C defined over F such that*

$$(2.1) \quad \text{Jac}(C) \simeq (E \times E') / \Gamma,$$

where Γ is the graph of ψ .

ii) *Suppose that E and E' are given by equations $y^2 = f(x)$ and $y^2 = g(x)$, where $f, g \in F[x]$ are monic and cubic. Let $\alpha_1, \alpha_2, \alpha_3$ (resp. $\beta_1, \beta_2, \beta_3$) be the roots of f (resp. g). Set $\alpha_{ij} = \alpha_i - \alpha_j$ and $\beta_{ij} = \beta_i - \beta_j$ and define*

$$\begin{aligned} a_1 &= \alpha_{32}^2 / \beta_{32} + \alpha_{21}^2 / \beta_{21} + \alpha_{13}^2 / \beta_{13}, & a_2 &= \alpha_1 \beta_{32} + \alpha_2 \beta_{13} + \alpha_3 \beta_{21}, \\ b_1 &= \beta_{32}^2 / \alpha_{32} + \beta_{21}^2 / \alpha_{21} + \beta_{13}^2 / \alpha_{13}, & b_2 &= \beta_1 \alpha_{32} + \beta_2 \alpha_{13} + \beta_3 \alpha_{21}. \end{aligned}$$

Let $A = \Delta_g a_1 / a_2$ and $B = \Delta_f b_1 / b_2$, where Δ_f and Δ_g are the discriminants of f and g , respectively. Then a model for C satisfying (2.1) is given by

$$y^2 = -(A\alpha_{21}\alpha_{13}x^2 + B\beta_{21}\beta_{13})(A\alpha_{32}\alpha_{21}x^2 + B\beta_{32}\beta_{21})(A\alpha_{13}\alpha_{32}x^2 + B\beta_{13}\beta_{32}).$$

2.3. Class number 2. Examples of genus 2 curves C defined over \mathbb{Q} such that $\mathcal{X}(C) \simeq M_2(\sqrt{-d})$, with $d \in \mathcal{D}_2 \setminus \{35, 91, 115, 187, 235, 403, 427\}$, can be found in the sources [Car01] and [GHR19] (for the reader's convenience we reproduce them in §5). We will find curves realizing the remaining discriminants by making use of the proposition and remark below.

Proposition 2.4. *Let M be an imaginary quadratic field of class number 2. Let H_2 denote the ray class field modulo 2 of M and let H^+ denote the maximal real subfield of the Hilbert class field H of M . Set $G = \text{Gal}(H_2/\mathbb{Q})$ and $G^+ = \text{Gal}(H_2/H^+)$, and let Z denote the centralizer of G^+ in G . Suppose that*

$$(2.2) \quad (G \setminus G^+) \cap Z$$

contains an element of order 2. Then there exists a genus 2 curve C defined over \mathbb{Q} such that $\mathcal{X}(C) \simeq M_2(M)$.

Proof. Since M has class number 2, the Hilbert class field H is a CM field, and thus H^+ is well defined. In fact, H^+ is the splitting field of the Hilbert class polynomial of discriminant $-d$. In other words, let E be an elliptic curve with CM by the ring of integers of M ; then H^+ coincides with $\mathbb{Q}(j(E))$. Since $j(E) \neq 0, 1728$, by [Sil94, Thm. 4.3, Thm. 5.6] we have that

$$H_2 = H(x(E[2])) = H(E[2]),$$

and thus the action of G_{H^+} on $E[2]$ factors through G^+ . Let σ be an element of order 2 in the intersection (2.2). We will apply part *i*) of Proposition 2.3 to the pair of elliptic curves E and ${}^\sigma E$ defined over the field $H^+ = \mathbb{Q}(j(E))$.

We claim that conjugation by σ induces an isomorphism $\psi_\sigma: E[2] \rightarrow {}^\sigma E[2]$ of $(\mathbb{Z}/2\mathbb{Z})[G^+]$ -Galois modules. Indeed, the $\mathbb{Z}/2\mathbb{Z}$ -linearity of ψ_σ is a direct consequence of the fact that ψ_σ is a bijection that maps 0 to 0; its G^+ -equivariance is a consequence of the fact that σ commutes with every element in G^+ . Since $\sigma \notin G^+$, we have that σ restricts to the nontrivial automorphism of H^+ and hence $j(E) \neq j({}^\sigma E)$. This implies that ψ_σ does not come from an isomorphism $E_{\overline{\mathbb{Q}}} \rightarrow {}^\sigma E_{\overline{\mathbb{Q}}}$. Let Γ_σ be the graph of ψ_σ . By Proposition 2.3, there exists a genus 2 curve \tilde{C} defined over H^+ and an isomorphism

$$\varphi_\sigma: \text{Jac}(\tilde{C}) \simeq (E \times {}^\sigma E) / \Gamma_\sigma,$$

of principally polarized abelian surfaces. We next show that \tilde{C} can be descended to \mathbb{Q} . Let $s: E \times {}^\sigma E \rightarrow {}^\sigma E \times E$ be the isomorphism that swaps E and ${}^\sigma E$. As σ has order 2, we have that $s({}^\sigma \Gamma_\sigma) = \Gamma_\sigma$ and that the composition

$$(2.3) \quad \nu_\sigma: {}^\sigma \text{Jac}(\tilde{C}) \xrightarrow{\varphi_\sigma} ({}^\sigma E \times E) / {}^\sigma \Gamma_\sigma \simeq (E \times {}^\sigma E) / \Gamma_\sigma \xrightarrow{\varphi_\sigma^{-1}} \text{Jac}(\tilde{C}),$$

where the central isomorphism is the one induced by s , is an isomorphism of principally polarized abelian surfaces. A trivial computation shows that the isomorphism ν_σ verifies that $\nu_\sigma \circ {}^\sigma \nu_\sigma = \text{id}$, that is, it provides Weil descent data for $\text{Jac}(\tilde{C})$ from H^+ to \mathbb{Q} .

It suffices to show that this descent data produces descent data for \tilde{C} . Any isomorphism ξ between curves induces by transport of structure an isomorphism $\text{Jac}(\xi)$ between their Jacobians. By Torelli's theorem [Lau01, Thm 1 in Appendice], there exists a *unique* isomorphism $\lambda_\sigma: {}^\sigma \tilde{C} \rightarrow \tilde{C}$ such that $\text{Jac}(\lambda_\sigma) = \nu_\sigma$. By functoriality, we have

$$\text{Jac}(\lambda_\sigma \circ {}^\sigma \lambda_\sigma) = \text{Jac}(\lambda_\sigma) \circ \text{Jac}({}^\sigma \lambda_\sigma) = \nu_\sigma \circ {}^\sigma \nu_\sigma = \text{id},$$

which by the unicity part of Torelli's theorem implies that $\lambda_\sigma \circ {}^\sigma \lambda_\sigma = \text{id}$. By [Wei56, Thm. 1] there exists C defined over \mathbb{Q} such that $C_{H^+} \simeq \tilde{C}$, and this completes the proof of the proposition. \square

Remark 2.5. Resume the notations of Proposition 2.4. We have verified with MAGMA that, for every $d \in \mathcal{D}_2 \setminus \{20, 52, 148\}$ there is an element σ of order 2 in $(G \setminus G^+) \cap Z$. To obtain a curve C as in the statement of the proposition we proceed by making effective each step of its proof. Indeed, we choose a root j of the Hilbert class polynomial of discriminant $-d$ and an elliptic curve E such that $j(E) = j$. We choose $\sigma \in (G \setminus G^+) \cap Z$ of order 2, and apply part *ii*) of Proposition 2.3 to E and ${}^\sigma E$

obtaining a genus 2 curve \tilde{C} defined over $\mathbb{Q}(j(E))$. We then compute the Cardona-Quer-Nart-Pujolàs invariants (g_1, g_2, g_3) of \tilde{C} (as defined in [CNP05], [CQ05]), which as predicted by Proposition 2.4 are rational numbers. From (g_1, g_2, g_3) , we construct a genus 2 curve C defined over \mathbb{Q} using MAGMA. In §5, we present the results of this computation for $d \in \{35, 91, 115, 187, 235, 403, 427\}$. The code used for this computation can be found in the file `SquareClassNumberTwo.m`.

3. PRODUCTS OF NONISOGENOUS CM ELLIPTIC CURVES

In §3.1 we show that if C is a genus 2 curve defined over \mathbb{Q} whose Jacobian is geometrically isogenous to the product of two nonisogenous CM elliptic curves, then $\mathcal{X}(C)$ is isomorphic to

$$(3.1) \quad \mathbb{Q}(\sqrt{-d}) \times \mathbb{Q}(\sqrt{-d'}), \quad \text{where } (d, d') \in \{(4, 3), (7, 4), (8, 4)\}.$$

In §3.2 we construct genus 2 curves over \mathbb{Q} realizing each of the above three pairs.

3.1. The upper bound. In this section, M and M' denote nonisomorphic imaginary quadratic fields of class number 1 and discriminants $-d$ and $-d'$, respectively. Write $\bar{\cdot}$ to denote complex conjugation.

Lemma 3.1. *Assume that $d \neq 3, 4$, and let E/\mathbb{Q} and E'/\mathbb{Q} be elliptic curves with CM by M and M' , respectively. Suppose that $p \geq 5$ is a prime of good reduction for E and E' , split in M and inert in M' . Then*

$$a_p(E) = \pm \text{Tr}_{M/\mathbb{Q}}(\pi) \quad \text{and} \quad a_p(E') = 0,$$

where π is any element in \mathcal{O}_M such that $p = \pi\bar{\pi}$.

Proof. Since p is supersingular for E' and $p \geq 5$, we have that $a_p(E') = 0$. By [Sil94, Exercise 2.30], we have that there exists $\pi' \in \mathcal{O}_M$ such that $a_p(E) = \text{Tr}_{M/\mathbb{Q}}(\pi')$ and $p = \pi'\bar{\pi}'$. Since $\mathcal{O}_M^\times = \{\pm 1\}$ by assumption, the element π' is uniquely determined up to sign. \square

Proposition 3.2. *Assume that $d \neq 3, 4$, and let $N \geq 2$ and $p_0 \geq 5$ be distinct rational primes. Suppose that:*

- i) p_0 is inert in M'/\mathbb{Q} .
- ii) p_0 is split in M/\mathbb{Q} and N does not divide $\text{Tr}_{M/\mathbb{Q}}(\pi_0)$, where $\pi_0 \in \mathcal{O}_M$ is such that $p_0 = \pi_0\bar{\pi}_0$.

Then for every pair of elliptic curves E and E' defined over \mathbb{Q} with CM by M and M' respectively, we have that $E[N]$ and $E'[N]$ are not isomorphic as $(\mathbb{Z}/N\mathbb{Z})[G_{\mathbb{Q}}]$ -modules.

Proof. Let a denote $\text{Tr}_{M/\mathbb{Q}}(\pi_0)$ and let $P_{a,N}$ be the set of primes p such that:

- i) p is inert in M'/\mathbb{Q} .
- ii) p is split in M/\mathbb{Q} and

$$\text{Tr}_{M/\mathbb{Q}}(\pi) \equiv a \pmod{N},$$

where $\pi \in \mathcal{O}_M$ is such that $p = \pi\bar{\pi}$.

We claim that $P_{a,N}$ is infinite. It suffices to show that there exist infinitely many primes $\pi \in \mathcal{O}_M$ of residue degree 1 such that

$$(3.2) \quad \pi \equiv \pi_0 \pmod{\text{lcm}(N, d')}.$$

Indeed, for such a π , we claim that $p = N_{M/\mathbb{Q}}(\pi)$ belongs to $P_{a,N}$. On the one hand, we have

$$p = N_{M/\mathbb{Q}}(\pi) \equiv N_{M/\mathbb{Q}}(\pi_0) = p_0 \pmod{d'},$$

and thus p is inert in M'/\mathbb{Q} . On the other hand, we have

$$\mathrm{Tr}_{M/\mathbb{Q}}(\pi) \equiv \mathrm{Tr}_{M/\mathbb{Q}}(\pi_0) = a \pmod{N}.$$

Note that π_0 is coprime to d' , since p_0 is inert in M'/\mathbb{Q} , and it is coprime to N by hypothesis. Then, the infiniteness of the set of primes π satisfying (3.2) follows from the analogue of Dirichlet's theorem over the ring of integers \mathcal{O}_M .

If $E[N]$ and $E'[N]$ were isomorphic as $(\mathbb{Z}/N\mathbb{Z})[G_{\mathbb{Q}}]$ -modules, then we would have that

$$a_p(E) \equiv a_p(E') \pmod{N},$$

for all but for a finite number of rational primes p . But together with Lemma 3.1 this implies that

$$0 = a_p(E') \equiv a_p(E) = \pm a \pmod{N},$$

for all but for a finite number of primes p in $P_{a,N}$. This contradicts the fact that N does not divide a . \square

Corollary 3.3. *Assume that $d \neq 3, 4$. Suppose that there exists a triple of natural numbers (p_1, p_2, a) , with $p_1, p_2 \geq 5$ different primes, such that:*

- i) p_i is split in M/\mathbb{Q} , inert in M'/\mathbb{Q} , and $\mathrm{Tr}_{M/\mathbb{Q}}(\pi_i) = a$, where $\pi_i \in \mathcal{O}_M$ is such that $p_i = \pi_i \bar{\pi}_i$ for $i = 1, 2$.*
- ii) For every pair of elliptic curves E and E' defined over \mathbb{Q} with CM by M and M' , and for every prime divisor q of a , the $(\mathbb{Z}/q\mathbb{Z})[G_{\mathbb{Q}}]$ -modules $E[q]$ and $E'[q]$ are not isomorphic.*

Then there is no genus 2 curve C defined over \mathbb{Q} such that $\mathcal{X}(C) \simeq M \times M'$.

Proof. Assume for the sake of contradiction that there exists C defined over \mathbb{Q} such that $\mathcal{X}(C) \simeq M \times M'$. By [FKRS12, Proposition 4.5], there exist elliptic curves E and E' defined over \mathbb{Q} with CM by M and M' , respectively, such that $\mathrm{Jac}(C) \sim E \times E'$. By the result of Frey and Kani recalled in §2.2 (cf. Proposition 2.2), there exists a prime $N \geq 2$ such that E and E' can be chosen so that $E[N]$ and $E'[N]$ are isomorphic as $(\mathbb{Z}/N\mathbb{Z})[G_{\mathbb{Q}}]$ -modules. Applying Proposition 3.2 with p_1 and taking hypothesis *ii*) into account, we obtain that $N = p_1$. One analogously obtains that $N = p_2$, which is a contradiction. \square

In order to prove the main theorem of this section, we will apply Corollary 3.3 to each pair (d, d') displayed in Table 2 using each of the displayed triples (p_1, p_2, a) . Before, we will describe the 3-torsion fields of certain elliptic curves. This will be useful in order to verify that the triples (p_1, p_2, a) displayed in Table 2 satisfy the hypotheses of Corollary 3.3.

For an elliptic curve E defined over \mathbb{Q} , let $\psi_{E,3}(x)$ denote its 3-division polynomial, so that $\mathbb{Q}(x(E[3]))$ coincides with the splitting field of $\psi_{E,3}(x)$. Recall that if E is given by the Weierstrass equation

$$(3.3) \quad y^2 = x^3 + ax + b, \quad \text{where } a, b \in \mathbb{Q}^\times,$$

then $\psi_{E,3}(x) = 3x^4 + 6ax^2 + 12bx - a^2$.

(d, d')	p_1	p_2	a	(d, d')	p_1	p_2	a
(7, 3)	29	113	2	(43, 19)	97	269	1
(8, 3)	17	41	6	(67, 3)	17	419	1
(8, 7)	73	1153	2	(67, 4)	151	419	1
(11, 3)	5	71	3	(67, 7)	17	419	1
(11, 4)	223	619	1	(67, 8)	151	821	1
(11, 7)	223	619	1	(67, 11)	17	151	1
(11, 8)	223	1213	1	(67, 19)	151	2027	1
(19, 3)	5	233	1	(67, 43)	151	419	1
(19, 4)	43	3463	1	(163, 3)	41	1019	1
(19, 7)	5	1069	1	(163, 4)	367	1019	1
(19, 8)	5	1069	1	(163, 7)	41	367	1
(19, 11)	43	233	1	(163, 8)	367	1997	1
(43, 3)	11	269	1	(163, 11)	41	1019	1
(43, 4)	11	6719	1	(163, 19)	41	1019	1
(43, 7)	97	269	1	(163, 43)	1019	1997	1
(43, 8)	269	1301	1	(163, 67)	41	367	1
(43, 11)	9041	10331	1				

TABLE 2. For each pair (d, d') , a triple (p_1, p_2, a) satisfying the hypotheses of Corollary 3.3.

Remark 3.4. Let E' be a quadratic twist of E . We may assume that E' is given by the Weierstrass equation

$$y^2 = x^3 + a/d^2x + b/d^3, \quad \text{where } d \in \mathbb{Q}^\times.$$

One trivially has $d^4\psi_{E',3}(x) = \psi_{E,3}(dx)$ and thus $\mathbb{Q}(x(E[3])) = \mathbb{Q}(x(E'[3]))$.

Lemma 3.5. *Let E be an elliptic curve defined over \mathbb{Q} with CM by $M = \mathbb{Q}(\sqrt{-d})$.*

- i) If $d = 8$ or 11 , then $\mathbb{Q}(E[3])$ is a polyquadratic extension of $M(\sqrt{-3})$.*
- ii) If $d = 3$, then either:*

- a) $\mathbb{Q}(E[3])$ has degree divisible by 3; or*
- b) E is of the form $y^2 = x^3 + b$, where $b \in \mathbb{Q}^\times$ is such that $4b \in \mathbb{Q}^{\times,3}$, and $\mathbb{Q}(E[3]) = \mathbb{Q}(\sqrt{-3}, \sqrt{b})$.*

Proof. As for part *i*), it suffices to show that $\mathbb{Q}(x(E[3])) = M(\sqrt{-3})$. If $d = 8$, then E is a quadratic twist of the elliptic curve E_0 attached to the j -invariant $2^6 \cdot 5^3$ on [Sil94, page 483]. By Remark 3.4, the field $\mathbb{Q}(x(E[3]))$ is the splitting field of

$$\psi_{E_0,3} = (x^2 - 48x + 864)(x^2 + 48x - 7200),$$

which is $\mathbb{Q}(\sqrt{-2}, \sqrt{-3})$. If $d = 11$, then E is a quadratic twist of the elliptic curve E_0 attached to the j -invariant -2^{15} on [Sil94, page 483]. By Remark 3.4, the field $\mathbb{Q}(x(E[3]))$ is the splitting field of

$$\psi_{E_0,3} = (x^2 - 132x + 4752)(x^2 + 132x - 6336),$$

which is $\mathbb{Q}(\sqrt{-11}, \sqrt{-3})$.

We now turn to part *ii*). By [Sil94, page 483], E pertains to one of the $\overline{\mathbb{Q}}$ -isomorphism classes corresponding to the j -invariants 0 , $2^4 \cdot 3^3 \cdot 5^3$ and $2^{15} \cdot 3 \cdot 5^3$.

If $j(E) = 2^4 \cdot 3^3 \cdot 5^3$, then we see as in the previous case that $\mathbb{Q}(x(E[3]))$ is the splitting field of

$$(x - 3)(x^3 + 3x^2 - 21x + 25),$$

whose degree is divisible by 3. If $j(E) = 2^{15} \cdot 3 \cdot 5^3$, then $\mathbb{Q}(x(E[3]))$ is the splitting field of

$$(x - 108)(x^3 + 108x^2 - 66096x + 4665600),$$

whose degree is divisible by 3. Finally, suppose that $j(E) = 0$. Then E is given by (3.3) with $a = 0$, and $\mathbb{Q}(x(E[3]))$ is the splitting of $x^3 + 4b$, which either has degree divisible by 3 or $-4b \in \mathbb{Q}^{\times,3}$. In the latter case, let $c := -(b/2)^{1/3} \in \mathbb{Q}^{\times}$. A straightforward calculation shows that $E[3]$ is generated by the points $P := (2c, \sqrt{-3b})$ and $Q := (0, \sqrt{b})$. It follows that $\mathbb{Q}(E[3]) = \mathbb{Q}(\sqrt{-3}, \sqrt{b})$. \square

Theorem 3.6. *Let C be a genus 2 curve defined over \mathbb{Q} such that $\mathcal{X}(C) \simeq M \times M'$. Then*

$$\mathcal{X}(C) \simeq \mathbb{Q}(\sqrt{-d}) \times \mathbb{Q}(\sqrt{-d'}),$$

where $(d, d') \in \{(4, 3), (7, 4), (8, 4)\}$.

Proof. It is a straightforward computation to verify that all triples displayed on Table 2 satisfy hypothesis *i*) of Corollary 3.3. The reader can find a SageMath code that verifies this at the file `find_primes_dirichlet.sage`. When $a = 1$, hypothesis *ii*) is vacuous, from which we immediately deduce that

$$(d, d') \in \{(4, 3), (7, 3), (7, 4), (8, 3), (8, 4), (8, 7), (11, 3)\}.$$

By Corollary 3.3, to rule out $(d, d') = (7, 3)$, it will suffice to show that there do not exist elliptic curves E and E' defined over \mathbb{Q} such that E has CM by $M = \mathbb{Q}(\sqrt{-7})$, E' has CM by $M' = \mathbb{Q}(\sqrt{-3})$, and $E[2] \simeq E'[2]$ as $(\mathbb{Z}/2\mathbb{Z})[G_{\mathbb{Q}}]$ -modules. It will suffice to show that for elliptic curves with these prescribed CM fields, the 2-torsion fields $\mathbb{Q}(E[2])$ and $\mathbb{Q}(E'[2])$ never coincide. On the one hand, by [Sil94, page 483], E pertains to one of the $\overline{\mathbb{Q}}$ -isomorphism classes corresponding to the j -invariants $-3^3 \cdot 5^3$ and $3^3 \cdot 5^5 \cdot 17^3$. As $\overline{\mathbb{Q}}$ -isomorphic elliptic curves with these j -invariants are quadratic twists of each other, the field $\mathbb{Q}(E[2])$ is invariant in each of these two $\overline{\mathbb{Q}}$ -isomorphism classes (this can be seen by comparing Weierstrass equations). This yields two possibilities for $\mathbb{Q}(E[2])$: $\mathbb{Q}(\sqrt{-7})$ or $\mathbb{Q}(\sqrt{7})$. On the other hand, as recalled in the proof of Lemma 3.5, E' pertains to one of the $\overline{\mathbb{Q}}$ -isomorphism classes corresponding to the j -invariants 0 , $2^4 \cdot 3^3 \cdot 5^3$ and $2^{15} \cdot 3 \cdot 5^3$. Arguing as before we see that if $j(E') = 2^4 \cdot 3^3 \cdot 5^3$, then $\mathbb{Q}(E'[2]) = \mathbb{Q}(\sqrt{3})$ and that if $j(E') = 2^{15} \cdot 3 \cdot 5^3$, then $\mathbb{Q}(E'[2])$ is the splitting field of $x^3 - 30x + 253/4$, which has degree divisible by 3. If $j(E') = 0$, then E' is given by (3.3) with $a = 0$, and $\mathbb{Q}(E'[2])$ is the splitting of $x^3 + b$, which is either $\mathbb{Q}(\sqrt{-3})$ or has degree divisible by 3. In any case, we find that $\mathbb{Q}(E[2])$ and $\mathbb{Q}(E'[2])$ do not coincide.

By Corollary 3.3, to rule out $(d, d') = (8, 7)$, it will suffice to show that there do not exist elliptic curves E and E' defined over \mathbb{Q} such that E has CM by $M = \mathbb{Q}(\sqrt{-8})$, E' has CM by $M' = \mathbb{Q}(\sqrt{-7})$, and $E[2] \simeq E'[2]$ as $(\mathbb{Z}/2\mathbb{Z})[G_{\mathbb{Q}}]$ -modules. As recalled in the proof of Lemma 3.5, E pertains to the $\overline{\mathbb{Q}}$ -isomorphism class of j -invariant $2^6 \cdot 5^3$, which as previously argued implies that $\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{2})$. On the other hand, as we saw in the previous paragraph, we have that $\mathbb{Q}(E'[2]) = \mathbb{Q}(\sqrt{7})$ or $\mathbb{Q}(\sqrt{-7})$. In particular, $\mathbb{Q}(E[2])$ and $\mathbb{Q}(E'[2])$ do not coincide.

By Corollary 3.3, to rule out $(d, d') = (11, 3)$, it will suffice to show that there do not exist elliptic curves E and E' defined over \mathbb{Q} such that E has CM by

$\mathbb{Q}(\sqrt{-11})$, E' has CM by $\mathbb{Q}(\sqrt{-3})$, and $E[3] \simeq E'[3]$ as $(\mathbb{Z}/3\mathbb{Z})[G_{\mathbb{Q}}]$ -modules. By Lemma 3.5, $\mathbb{Q}(E[3])$ and $\mathbb{Q}(E'[3])$ can not coincide.

By Corollary 3.3, to rule out $(d, d') = (8, 3)$, it will suffice to show that there do not exist elliptic curves E and E' defined over \mathbb{Q} such that E has CM by $\mathbb{Q}(\sqrt{-8})$, E' has CM by $\mathbb{Q}(\sqrt{-3})$, and $E[N] \simeq E'[N]$ as $(\mathbb{Z}/N\mathbb{Z})[G_{\mathbb{Q}}]$ -modules for $N = 2$ or $N = 3$. We first show that this is impossible for $N = 2$. We have already seen that $\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{2})$, and that $\mathbb{Q}(E'[2])$ is either $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{3})$, or has degree 3. Suppose that $E[3] \simeq E'[3]$ as $(\mathbb{Z}/3\mathbb{Z})[G_{\mathbb{Q}}]$ -modules. A simple argument using Lemma 3.5, shows that if $\mathbb{Q}(E[3])$ and $\mathbb{Q}(E'[3])$ coincide, then b lies either in $-2 \cdot \mathbb{Q}^{\times,6}$ or in $2 \cdot 3^3 \cdot \mathbb{Q}^{\times,6}$. We may thus assume that E' is given by either

$$y^2 = x^3 - 2, \quad \text{or} \quad y^2 = x^3 + 54.$$

In the first case, $P = (2, \sqrt{6})$ and $Q = (0, \sqrt{-2})$ constitute a basis of $E'[3]$. In the second case, a basis is given by $P = (-6, 9\sqrt{-2})$ and $Q = (0, 3\sqrt{6})$. Using this basis, it is easy to see that for any prime p of good reduction for E' split in $\mathbb{Q}(\sqrt{-3})$ and inert in $\mathbb{Q}(\sqrt{-2})$ we have

$$\text{Tr}(\overline{\rho}_{E',3}(\text{Frob}_p)) \equiv 1 \pmod{3}.$$

This contradicts the fact that for any prime p of good reduction for E and inert in $\mathbb{Q}(\sqrt{-2})$ we have that $\text{Tr}(\overline{\rho}_{E',3}(\text{Frob}_p)) \equiv a_p(E) = 0 \pmod{3}$. \square

Remark 3.7. We note that for $(d, d') \in \{(4, 3), (7, 4), (8, 4)\}$, there does not exist a triple (p_1, p_2, a) satisfying the hypotheses of Corollary 3.3. Obviously, this needs a justification only if $d = 7$ or 8 . In that case, it is an elementary exercise to show that $\text{Tr}_{M/\mathbb{Q}}(\pi)$ is even for every prime π in \mathcal{O}_M of residue degree 1. But as we will see in the next section, there are choices of elliptic curves E and E' with CM by M and M' , respectively, for which $E[2]$ and $E'[2]$ are isomorphic as $\mathbb{Z}/2\mathbb{Z}[G_{\mathbb{Q}}]$ -modules.

3.2. The three realizable pairs. The elliptic curves

$$E_1: y^2 = x^3 - 1, \quad E'_1: y^2 = x^3 + 3x.$$

have CM by $\mathbb{Q}(\sqrt{-3})$ and by $\mathbb{Q}(\sqrt{-4})$ respectively. They both have a rational point of order 2 and $\mathbb{Q}(E_1[2]) = \mathbb{Q}(E'_1[2]) = \mathbb{Q}(\sqrt{-3})$. Label the 2-torsion points of E_1 and E'_1 as

$$E_1[2] = \{O, P_1, P_2, P_3\}, \quad E'_1[2] = \{O, Q_1, Q_2, Q_3\}$$

in such a way that $P_1 \in E_1(\mathbb{Q})$ and $Q_1 \in E'_1(\mathbb{Q})$. Then the map $\psi: E_1[2] \rightarrow E'_1[2]$ given by $\psi(P_i) = Q_i$ is an isomorphism of $G_{\mathbb{Q}}$ -modules that does not arise from an isomorphism between E_1 and E'_1 (since $j(E_1) \neq j(E'_1)$). Applying the method of Proposition 2.3 gives the equation

$$y^2 = -4251528x^6 + 6377292x^4 - 6377292x^2 + 2125764.$$

The coefficients of the right hand side are divisible by square factors, clearing them out we obtain the curve

$$C_1: y^2 = -2x^6 + 3x^4 - 3x^2 + 1,$$

whose Jacobian is isogenous over \mathbb{Q} to $E_1 \times E'_1$.

The same method can be applied to the curves

$$E_2: y^2 = x^3 + 7x, \quad E'_2: y^2 + xy + y = x^3 - x^2 - 55x - 178.$$

They have CM by $\mathbb{Q}(\sqrt{-4})$ and $\mathbb{Q}(\sqrt{-7})$, respectively, and $\mathbb{Q}(E_2[2]) = \mathbb{Q}(E'_2[2]) = \mathbb{Q}(\sqrt{-7})$. The obtained curve is

$$C_2: y^2 = 21870000x^6 - 1002375x^4 + 2025x^2 - 30,$$

whose Jacobian is isogenous over \mathbb{Q} to $E_2 \times E'_2$.

Finally, the curves

$$E_3: y^2 = x^3 - 2x, \quad E'_3: y^2 = x^3 - x^2 - 3x - 1$$

have CM by $\mathbb{Q}(\sqrt{-4})$ and $\mathbb{Q}(\sqrt{-8})$, respectively, and $\mathbb{Q}(E_3[2]) = \mathbb{Q}(E'_3[2]) = \mathbb{Q}(\sqrt{2})$. The same method as above produces the curve

$$C_3: y^2 = -46656x^6 - 1296x^4 + 108x^2 - 1,$$

whose Jacobian is isogenous over \mathbb{Q} to $E_3 \times E'_3$.

4. CLASS NUMBER 4

Throughout this section let $M = \mathbb{Q}(\sqrt{-d})$, where $d \in \mathcal{D}_{2,2}$. That is, M is a quadratic imaginary field with class group $C_2 \times C_2$. Let \mathcal{O}_M denote the ring of integers of M and let H be the Hilbert class field of M . The results of this section complete the proof of Theorem 1.2. Recall the sets $\mathcal{D}_{2,2}^J \subseteq \mathcal{D}_{2,2}^S \subseteq \mathcal{D}_{2,2}$ defined by (1.1) and (1.2). Kani's theorem [Kan11, Thm. 2] applied to our particular setting produces the following description.

Proposition 4.1 (Kani). *Suppose that $d \in \mathcal{D}_{2,2}$ and that A is an abelian surface defined over \mathbb{Q} such that there is an elliptic curve E_0 defined over $\overline{\mathbb{Q}}$ with CM by M and such that $A_{\overline{\mathbb{Q}}} \sim E_0^2$. Then there exist elliptic curves E and E' defined over $\overline{\mathbb{Q}}$ with CM by M such that $A_{\overline{\mathbb{Q}}} \simeq E \times E'$.*

The goal of §4.1 and 4.2 is to refine the above result by showing that E and E' can be chosen to have CM by \mathcal{O}_M . Once this is shown, we are in the setting of [GHR19] and [Nar22], and in §4.3 we use their classification results to find the upper bound $\mathcal{D}_{2,2}^J$ in Theorem 1.2. In §4.4, we certify that the upper bound $\mathcal{D}_{2,2}^J$ is sharp relying on the parametrizations of [Kum15].

4.1. The first reduction step. The fundamental point of the next result is that if A is an abelian surface defined over \mathbb{Q} such that $\mathcal{X}(A) \simeq M_2(M)$ for $d \in \mathcal{D}_{2,2}$, then all the endomorphisms of A are defined over H . This was shown in the course of the proof of the main result of [FG20].

Proposition 4.2. *Suppose that $d \in \mathcal{D}_{2,2}$ and that A is an abelian surface defined over M such that $\mathcal{X}(A) \simeq M_2(M)$. Then $d \in \mathcal{D}_{2,2}^S$ and there is an elliptic curve E_0 defined over H with CM by \mathcal{O}_M and such that $A_H \sim E_0^2$.*

Proof. The existence of an elliptic curve E_0 defined over H with CM by M such that $A_H \sim E_0^2$ and the fact that $M \in \mathcal{D}_{2,2}^S$ are proven in the course of [FG20, Proof of Thm. 1.2; page 1416]. Suppose now that E_0 has CM by an order \mathcal{O}_f in M of conductor f , and let us show that $f = 1$. Let H_f denote the ring class field of conductor f . Then, by the theory of complex multiplication, the field of definition of E_0 must contain H_f , and thus we deduce that H and H_f coincide. From the formula

$$[H_f : H] = f \prod_{p|f} \left(1 - \left(\frac{-d}{p} \right) \frac{1}{p} \right)$$

(see [Cox98, Cor. 7.24], for example), we deduce that $H_f = H$ if and only if either $f = 1$ or $f = 2$ and 2 is split in M . But one readily verifies that 2 does not split in $\mathbb{Q}(\sqrt{-d})$ for any $d \in \mathcal{D}_{2,2}^S$, and therefore we must have $f = 1$. \square

4.2. The second reduction step. After describing the H -isogeny class of an abelian surface A defined over \mathbb{Q} such that $\mathcal{X}(A) \simeq M_2(M)$ for $d \in \mathcal{D}_{2,2}^S$, we will characterize the H -isomorphism classes it contains.

Proposition 4.3. *Suppose that $d \in \mathcal{D}_{2,2}^S$ and that A is an abelian surface defined over H such that there is an elliptic curve E_0 defined over H with CM by \mathcal{O}_M and such that $A \sim E_0^2$. Then there exist elliptic curves E and E' defined over H with CM by \mathcal{O}_M such that $A \simeq E \times E'$.*

Proof. Let us also derive this result from [JKPRST18]. Let \mathcal{I} denote the category of torsion free finitely generated \mathcal{O}_M -modules, and let \mathcal{P} denote the category of abelian varieties defined over H which are isogenous to a power of E_0 . Let

$$\mathcal{H}om_{\mathcal{O}_M}(-, E_0): \mathcal{I} \rightarrow \mathcal{P}, \quad \text{Hom}(-, E_0): \mathcal{P} \rightarrow \mathcal{I}$$

be the functors defined in loc. cit. By [JKPRST18, Thm. 7.5], the abelian surfaces defined over H which lie in the essential image of $\mathcal{H}om_{\mathcal{O}_M}(-, E_0)$ are those isomorphic to the product of two elliptic curves with CM by \mathcal{O}_M . In order to complete the proof of the theorem, it will suffice to show that $\mathcal{H}om_{\mathcal{O}_M}(-, E_0)$ and $\text{Hom}(-, E_0)$ are inverse equivalences of categories. This is verified in the proposition below. \square

Proposition 4.4. *Suppose that $d \in \mathcal{D}_{2,2}^S$ and that E_0 is an elliptic curve defined over H with CM by \mathcal{O}_M . Then the functors $\mathcal{H}om_{\mathcal{O}_M}(-, E_0)$ and $\text{Hom}(-, E_0)$ are inverse equivalences of categories.*

Proof. Recall that $\overline{\rho}_{E_0, \ell}$ denotes the representation obtained from the action of G_H on $E_0[\ell]$. By [JKPRST18, Thm. 7.7], the functors $\mathcal{H}om_{\mathcal{O}_M}(-, E_0)$ and $\text{Hom}(-, E_0)$ are inverse equivalences of categories if and only if for every prime ℓ the image of $\overline{\rho}_{E_0, \ell}$ is not contained in the group of scalar matrices. It is well known that $\overline{\rho}_{E_0, \ell}$ factors as

$$\overline{\rho}_{E_0, \ell}: G_H \rightarrow (\mathcal{O}_M/\ell\mathcal{O}_M)^\times \subseteq \text{Aut}(E[\ell]).$$

In fact, by a result of Stevenhagen [Ste01] (see also [BC, Thm. 1.4]), the image of $\overline{\rho}_{E_0, \ell}$ in $(\mathcal{O}_M/\ell\mathcal{O}_M)^\times/\{\pm 1\}$ is surjective. This implies that

$$\#\text{im}(\overline{\rho}_{E_0, \ell}) \geq \frac{\#(\mathcal{O}_M/\ell\mathcal{O}_M)^\times}{2} = \begin{cases} (\ell-1)(\ell-1)/2 & \text{if } \ell \text{ is split in } M, \\ (\ell^2-1)/2 & \text{if } \ell \text{ is inert in } M, \\ \ell(\ell-1)/2 & \text{if } \ell \text{ ramifies in } M. \end{cases}$$

One readily verifies that if $\ell > 3$ then the right-hand side of the above inequality is $> \ell - 1$ in each of the three cases, and therefore for $\ell > 3$ the image of $\overline{\rho}_{E_0, \ell}$ cannot be contained in the group of scalar matrices. In order to verify that the action of G_H on $E_0[\ell]$ for $\ell = 2, 3$ is not by scalars, it will suffice to verify that $[H(x(E_0[\ell])) : H] > \ell - 1$, as we have

$$\#\text{im}(\overline{\rho}_{E_0, \ell}) = [H(E_0[\ell]) : H] \geq [H(x(E_0[\ell])) : H].$$

The degree $[H(E_0[\ell]) : H]$ depends on the H -isomorphism class of E_0 , but the degree $[H(x(E_0[\ell])) : H]$ only depends on the $\overline{\mathbb{Q}}$ -isomorphism class of E_0 , as it coincides with the degree over H of the splitting field of the ℓ -division polynomial

$\psi_{E_0, \ell}(x)$ of E_0 , which is invariant under quadratic twist as we have already observed. For each E_0 representing one of the 72 $\overline{\mathbb{Q}}$ -isomorphism classes of elliptic curves with CM by \mathcal{O}_M for $d \in \mathcal{D}_{2,2}^S$, one readily verifies that the degree of the splitting field of $\psi_{E_0, \ell}(x)$ over H is $> \ell - 1$ for $\ell = 2, 3$. This completes the proof of the proposition. \square

4.3. The third reduction step. Let $d \in \mathcal{D}_{2,2}^S$ and $M = \mathbb{Q}(\sqrt{-d})$. G elin, Howe, and Ritzenthaler [GHR19] have determined the finite set $\mathcal{P}(d)$ of isomorphism classes of indecomposably principally polarized abelian surfaces A defined over $\overline{\mathbb{Q}}$ with field of moduli \mathbb{Q} such that $A \simeq E^2$, where E is an elliptic curve defined over $\overline{\mathbb{Q}}$ with CM by \mathcal{O}_M . Extending their work, Narbonne [Nar22] has recently determined the finite set $\mathcal{Q}(d) \supseteq \mathcal{P}(d)$ of isomorphism classes of indecomposably principally polarized abelian surfaces A defined over $\overline{\mathbb{Q}}$ with field of moduli \mathbb{Q} such that $A \simeq E \times E'$, where E and E' are elliptic curves defined over $\overline{\mathbb{Q}}$ with CM by \mathcal{O}_M . The cardinalities of $\mathcal{P}(d)$ and $\mathcal{Q}(d)$ may be found in [GHR19, Table 2] and [Nar22, Table 1], and the corresponding polarizations are available on the authors webpages.

Let $\mathcal{P}^*(d)$ (resp. $\mathcal{Q}^*(d)$) denote the subset of $\mathcal{P}(d)$ (resp. $\mathcal{Q}(d)$) consisting of $\overline{\mathbb{Q}}$ -isomorphism classes containing an abelian surface defined over \mathbb{Q} . Propositions 4.2 and 4.3, together with Weil's equivalence [Wei57] between indecomposably principally polarized abelian surfaces and Jacobians, imply that the algebra $M_2(M)$ belongs to \mathcal{B} if and only if $\mathcal{Q}^*(d)$ is nonempty.

We will show the following proposition by proving that $\mathcal{Q}^*(d) = \emptyset$ for $d \notin \mathcal{D}_{2,2}^J$.

Proposition 4.5. *If $d \notin \mathcal{D}_{2,2}^J$, then there does not exist a genus 2 curve C defined over \mathbb{Q} such that*

$$\text{Jac}(C)_{\overline{\mathbb{Q}}} \simeq E \times E',$$

where E and E' are elliptic curves defined over $\overline{\mathbb{Q}}$ with CM by \mathcal{O}_M .

Proof. By Proposition 4.2, it suffices to assume that $d \in \{280, 483, 595, 627, 795\}$. Suppose that $d = 280$. From [Nar22, Table 1], we know that $\#\mathcal{Q}(280) = 4$. Table 3 exhibits Igusa–Clebsch invariants of four genus 2 curves C_1, \dots, C_4 defined over $\overline{\mathbb{Q}}$. Let $i \in \{1, \dots, 4\}$. The Igusa–Clebsch invariants of the C_i being rational and pairwise distinct (as points in the weighted projective space) implies that the field of moduli of the C_i is \mathbb{Q} , and that the C_i are pairwise non $\overline{\mathbb{Q}}$ -isomorphic. A computation from the Igusa–Clebsch invariants shows that $\text{Aut}(C_i) \simeq C_2$, and that Mestre's obstruction [Mes91] for each of the C_i is nontrivial over \mathbb{Q} and trivial over M . Hence we may assume that the C_i are defined over M , which we do from now on. In §4.5 we will show that $\text{Jac}(C_i) \sim E_0^2$, where E_0 is an elliptic curve defined over $\overline{\mathbb{Q}}$ with CM by M . By Propositions 4.2 and 4.3, there exist elliptic curves E and E' defined over H with CM by \mathcal{O}_M such that $\text{Jac}(C_i) \simeq E \times E'$. Moreover, since the C_i are pairwise non $\overline{\mathbb{Q}}$ -isomorphic, Torelli's theorem implies that the $\text{Jac}(C_i)$ are pairwise non $\overline{\mathbb{Q}}$ -isomorphic as principally polarized abelian surfaces. Putting the last two conclusions together, we infer that $\mathcal{Q}(d)$ is precisely the set of the $\text{Jac}(C_i)_{\overline{\mathbb{Q}}}$. We claim that $\mathcal{Q}^*(280) = \emptyset$. Suppose for the sake of contradiction that there is a genus 2 curve C defined over \mathbb{Q} such that $\text{Jac}(C)_{\overline{\mathbb{Q}}} \simeq E \times E'$, where E and E' are elliptic curves defined over $\overline{\mathbb{Q}}$ with CM by \mathcal{O}_M . Then for some of the C_i we have that $\text{Jac}(C)_{\overline{\mathbb{Q}}} \simeq \text{Jac}(C_i)_{\overline{\mathbb{Q}}}$, as principally polarized abelian surfaces. Torelli's theorem implies that $C_{\overline{\mathbb{Q}}} \simeq C_{i, \overline{\mathbb{Q}}}$, and hence C and C_i share the same Igusa–Clebsch

invariants. This is a contradiction with the fact that Mestre's obstruction over \mathbb{Q} is trivial for C , but nontrivial for C_i . As for the remaining discriminants, we read from [Nar22, Table 1] that

$$\mathcal{Q}(483) = \mathcal{Q}(627) = \emptyset, \quad \mathcal{Q}(595) = \mathcal{P}(595), \quad \mathcal{Q}(795) = \mathcal{P}(795).$$

It thus remains to show that $\mathcal{P}^*(595)$ and $\mathcal{P}^*(795)$ are empty. This may be verified exactly as in the previous paragraph we verified that $\mathcal{Q}^*(280)$ is empty. This is in fact accomplished in [GHR19]. \square

Remark 4.6. In the proof of the above proposition we have addressed the cases $d \in \mathcal{D}_{2,2}^S \setminus \mathcal{D}_{2,2}^J$ using Proposition 4.2. As a consistency check, we also confirmed the emptiness of $\mathcal{Q}^*(d)$ for these values of d using the strategy applied to the cases $d \in \{280, 483, 595, 627, 795\}$ in the above proposition.

4.4. Curves realizing the discriminants with $d \in \mathcal{D}_{2,2}^J$. There is a vast literature on the problem of parametrizing pairs (C, E) , where C is a genus 2 curve and E is an elliptic curve with the property that there is an optimal map $\phi: C \rightarrow E$ of fixed degree $n > 1$. We write $\tilde{\mathcal{L}}_n$ for the moduli space of such pairs. This goes back to Legendre and Jacobi for $n = 2$, and to Hermite, Goursat and Bolza among others for $n = 3$ and 4. This topic has been revisited more recently by Kuhn for $n = 3$ (see [Kuh88]), and by Shaska and his collaborators for $2 \leq n \leq 5$ (see [Sha04], [MSV09], and [SWWW08]). The connection of this problem to split Jacobians is that for such C and E , the Jacobian $\text{Jac}(C)$ is isogenous to the product of elliptic curves $E \times E'$, where $E' = \text{Jac}(C)/\phi^*(E)$.

In this section we will use the more recent approach by Kumar [Kum15], who computes $\tilde{\mathcal{L}}_n$ for $2 \leq n \leq 11$ by exploiting the fact that it is birational to the Hilbert modular surface $Y_-(n^2)$ that parametrizes pairs (A, ι) of principally polarized abelian surfaces with an embedding $\iota: \mathcal{O}_{n^2} \hookrightarrow \text{End}(A)$, where \mathcal{O}_{n^2} denotes the quadratic order of discriminant n^2 .

For each such $n = 2, \dots, 11$, [Kum15] provides a birational model for $\tilde{\mathcal{L}}_n$ of the form

$$z^2 = f(r, s),$$

along with expressions of the Igusa–Clebsch invariants of the curve C corresponding in the moduli space with a point (C, E) with coordinates (z, r, s) . We note that these invariants do not depend on the z coordinate, since the two points with the same z coordinate correspond to points on the Hilbert modular surface having the same abelian surface and conjugate embeddings. In addition, [Kum15] also provides the j -invariants associated to the two quotient curves E and E' . For example, for $n = 3$, a birational model for $\tilde{\mathcal{L}}_3$ is

$$z^2 = 11664r^2 - 8(54s^3 + 27s^2 - 72s + 23)r + (s - 1)^4(2s - 1)^2.$$

The Igusa–Clebsch invariants of a curve corresponding to a point (C, E) with coordinates r and s are:

$$\begin{aligned}
 I_2 &= 8s^2 + 32s - 16, \\
 I_4 &= 4s^4 - 16s^3 - 192rs + 24s^2 + 768r - 16s + 4, \\
 (4.1) \quad I_6 &= 8s^6 + 16s^5 - 320rs^3 - 168s^4 + 1152rs^2 + 352s^3 \\
 &\quad - 2304r^2 + 6336rs - 328s^2 - 2560r + 144s - 24, \\
 I_{10} &= 2^{14}r^3.
 \end{aligned}$$

If we denote by j_1 and j_2 the j -invariants of E and E' , then we have the following expressions for their product and sum:

$$\begin{aligned}
 (4.2) \quad j_1 + j_2 &= (2s^9 - 17s^8 - 324rs^6 + 64s^7 + 1350rs^5 - 140s^6 \\
 &\quad + 17496r^2s^3 - 2097rs^4 + 196s^5 - 23328r^2s^2 \\
 &\quad + 1368rs^3 - 182s^4 - 314928r^3 + 9720r^2s - 162rs^2 \\
 &\quad + 112s^3 - 432r^2 - 198rs - 44s^2 + 63r + 10s - 1)/r^2, \\
 j_1 \cdot j_2 &= (s^4 - 4s^3 + 432rs + 6s^2 - 288r - 4s + 1)^3/r^3,
 \end{aligned}$$

from which one can easily compute j_1 and j_2 .

We claim that for every $d \in \mathcal{D}_{2,2}^J$ the Jacobian of the curve C_d given in Table 6 has geometric endomorphism algebra isomorphic to $M_2(\mathbb{Q}(\sqrt{-d}))$. To prove this claim for example for $d = 84$, one checks that the following values of r and s :

$$\begin{aligned}
 r &= \frac{728973}{2048}g^2 - \frac{80180415}{8}, \\
 s &= -\frac{5}{1024}g^2 + \frac{531}{4},
 \end{aligned}$$

where g is a root of $x^4 - 28160x^2 + 65536$, produce in (4.1) Igusa-Clebsch invariants that are equivalent (in the weighted projective space) to the Igusa-Clebsch invariants of C_d . This implies that there is a degree 3 optimal map from C_d to an elliptic curve E , and that $\text{Jac}(C_d)$ is geometrically isogenous to a product of elliptic curves $E \times E'$. We can compute the j -invariants of E and E' using (4.2), and one can check that the resulting j_1 and j_2 turn out to be roots of the Hilbert class polynomial of discriminant -84 . That is, E and E' have CM by (the maximal order of) $\mathbb{Q}(\sqrt{-84})$. Since all curves with CM by the same imaginary quadratic field are geometrically isogenous, we obtain that $\text{Jac}(C_d)$ is geometrically isogenous to E^2 , as we aimed to see.

We have performed analogous computations for all the remaining curves in Table 6. Equations for $\tilde{\mathcal{L}}_n$, the Igusa-Clebsch invariants of the curves in the tautological family of genus 2 curves above $\tilde{\mathcal{L}}_n$, and the j -invariants of the corresponding elliptic quotients for the rest of values $2 \leq n \leq 11$ are available in [Kum15] (to be more precise, for $n = 10, 11$ they are not in the article but they are available in the source files of the arXiv submission of the article <https://arxiv.org/abs/1412.2849>). We display in the Table 6 the value of the degree n of the optimal map in each case. For lack of space we do not display the values of r and s found for each curve, but they have been computed using the software SageMath and MAGMA. The reader can find the code (which can be executed and computes the values of r and s in each case and performs the verifications) at the file `curves_all_endomorphisms_genus_two.sage`.

For the sake of completeness, and as a double check, the code also verifies the correctness of the entries of Tables 4 and 5. Observe that this is not strictly necessary, as the correctness of these curves either had been already established before in the literature, or it has been proved in the previous sections of the present article.

4.5. Curves of discriminant -280 . Table 3 lists the Igusa–Clebsch invariants of four curves C_1, \dots, C_4 . To check that each $\text{Jac}(C_i)$ is geometrically isogenous to a product $E \times E'$ of elliptic curves with CM by $\mathbb{Q}(\sqrt{-280})$, we proceed similarly as in §4.4. That is to say, for each tuple of invariants (I_2, I_4, I_6, I_{10}) we find a value of n and algebraic values r, s such that the point (C, E) of $\tilde{\mathcal{L}}_n$ with coordinates r and s has the property that the Igusa–Clebsch invariants of C are equivalent to (I_2, I_4, I_6, I_{10}) . Then we compute the j -invariants of the elliptic quotients E, E' of $\text{Jac}(C)$ and we verify that they correspond to elliptic curves with CM by $\mathbb{Q}(\sqrt{-280})$. In Table 3 we list the value of n found for each curve. The corresponding values of r and s for each curve, the verification that they have the stated CM, and the verification that the Mestre conic is obstructed over \mathbb{Q} and unobstructed over $\mathbb{Q}(\sqrt{-280})$ can be found by executing the SageMath code `curves_280.sage`.

TABLE 3. Igusa–Clebsch invariants (I_2, I_4, I_6, I_{10}) for genus 2 curves C_i whose endomorphism algebra is $M_2(\mathbb{Q}(\sqrt{-280}))$. The n is the minimal degree of a cover from C to an elliptic curve.

Curve	(I_2, I_4, I_6, I_{10})	n
C_1	$\left(2^3, \frac{2^6 3^4 5^3 23^5 223}{29^2 383^2 1783^2}, \frac{2^9 3^3 5^5 23^5 31 \cdot 4613569}{29^3 383^3 1783^3}, \frac{2^{14} 3^7 5^6 23^{12}}{29^5 383^5 1783^5}\right)$	3
C_2	$\left(2^3, \frac{2^{10} 3^4 7^2 11^6 23^4}{29^2 13537009^2}, \frac{2^{13} 3^3 7^2 11^6 1923^4 353 \cdot 1180303}{5^2 29^3 13537009^3}, \frac{2^{26} 3^7 7^6 11^{12} 23^{12}}{5^5 29^5 13537009^5}\right)$	6
C_3	$\left(2^3, \frac{2^4 3^4 5^3 7^2 11^4 23^4 59}{5431080691^2}, -\frac{2^6 3^3 5^4 7^2 11^4 23^4 474621 \cdot 60923}{5431080691^3}, \frac{2^8 3^7 5^6 7^6 11^{12} 23^{12}}{5431080691^5}\right)$	6
C_4	$\left(2^3, \frac{2^4 3^4 5^3 11^5 23^4 101}{109^2 4392541^2}, \frac{2^6 3^3 5^3 11^5 1923^4 107 \cdot 30845219}{109^3 4392541^3}, -\frac{2^8 3^7 5^6 11^{12} 23^{12}}{109^5 4392541^5}\right)$	8

5. EXPLICIT EXAMPLES

This section contains equations of genus 2 curves realizing each one of the possible 54 geometric endomorphism algebras of geometrically split Jacobians of curves defined over \mathbb{Q} .

TABLE 4. Curves whose geometric endomorphism algebra is $M_2(\mathbb{Q})$, a product of fields, or $M_2(\mathbb{Q}(\sqrt{-d}))$ with $d \in \mathcal{D}_1$.

Algebra	Curve	Source
$M_2(\mathbb{Q})$	$y^2 = x^6 + x^4 + x^2 + 1$	[FKRS12, Table 11, Row E_1]
$\mathbb{Q} \times \mathbb{Q}$	$y^2 = x^6 + x^5 + x - 1$	[FKRS12, Table 11, Row $N(G_{3,3})$]
$\mathbb{Q} \times \mathbb{Q}(\sqrt{-3})$	$y^2 = x^6 - 15x^2 + 22$	Proposition 2.1
$\mathbb{Q} \times \mathbb{Q}(\sqrt{-4})$	$y^2 = x^6 - 11x^2 + 14$	Proposition 2.1
$\mathbb{Q} \times \mathbb{Q}(\sqrt{-7})$	$y^2 = x^6 - 35x^2 + 98$	Proposition 2.1
$\mathbb{Q} \times \mathbb{Q}(\sqrt{-8})$	$y^2 = x^6 - 30x^2 + 56$	Proposition 2.1
$\mathbb{Q} \times \mathbb{Q}(\sqrt{-11})$	$y^2 = x^6 - 264x^2 + 1694$	Proposition 2.1
$\mathbb{Q} \times \mathbb{Q}(\sqrt{-19})$	$y^2 = x^6 - 152x^2 + 722$	Proposition 2.1
$\mathbb{Q} \times \mathbb{Q}(\sqrt{-43})$	$y^2 = x^6 - 3440x^2 + 77658$	Proposition 2.1
$\mathbb{Q} \times \mathbb{Q}(\sqrt{-67})$	$y^2 = x^6 - 29480x^2 + 1948226$	Proposition 2.1
$\mathbb{Q} \times \mathbb{Q}(\sqrt{-163})$	$y^2 = x^6 - 8697680x^2 + 9873093538$	Proposition 2.1
$\mathbb{Q}(\sqrt{-3}) \times \mathbb{Q}(\sqrt{-4})$	$y^2 = -2x^6 + 3x^4 - 3x^2 + 1$	Method of [HLP00, §3]
$\mathbb{Q}(\sqrt{-4}) \times \mathbb{Q}(\sqrt{-7})$	$y^2 = 21870000x^6 - 1002375x^4 + 2025x^2 - 30$	Method of [HLP00, §3]
$\mathbb{Q}(\sqrt{-4}) \times \mathbb{Q}(\sqrt{-8})$	$y^2 = -46656x^6 - 1296x^4 + 108x^2 - 1$	Method of [HLP00, §3]
$M_2(\mathbb{Q}(\sqrt{-3}))$	$y^2 = x^6 + 1$	[FKRS12, Table 11, Row C_1]
$M_2(\mathbb{Q}(\sqrt{-4}))$	$y^2 = x^5 + x^3 + \frac{81}{196}x$	[Car01, p. 112]
$M_2(\mathbb{Q}(\sqrt{-7}))$	$y^2 = x^5 + x^3 + \frac{3969}{16900}x$	[Car01, p. 112]
$M_2(\mathbb{Q}(\sqrt{-8}))$	$y^2 = x^5 - x$	[FKRS12, Table 11, Row C_2]
$M_2(\mathbb{Q}(\sqrt{-11}))$	$y^2 = 2x^6 + 11x^3 - 22$	[GHR19, Table 4]
$M_2(\mathbb{Q}(\sqrt{-19}))$	$y^2 = x^6 + 1026x^5 + 627x^4 + 38988x^3 - 11913x^2 + 370386x - 6859$	[GHR19, Table 4]
$M_2(\mathbb{Q}(\sqrt{-43}))$	$y^2 = x^6 + 48762x^5 + 1419x^4 + 4193532x^3 - 61017x^2 + 90160938x - 79507$	[GHR19, Table 4]
$M_2(\mathbb{Q}(\sqrt{-67}))$	$y^2 = x^6 + 785106x^5 + 2211x^4 + 105204204x^3 - 148137x^2 + 3524340834x - 300763$	[GHR19, Table 4]
$M_2(\mathbb{Q}(\sqrt{-163}))$	$y^2 = x^6 + 1635420402x^5 + 5379x^4 + 533147051052x^3 - 876777x^2 + 43451484660738x - 4330747$	[GHR19, Table 4]

TABLE 5. Curves whose geometric endomorphism algebra is $M_2(\mathbb{Q}(\sqrt{-d}))$ with $d \in \mathcal{D}_2$

d	Curve	Source
15	$y^2 = x^6 + x^3 + \frac{1}{20}$	[Car01, p. 112]
20	$y^2 = x^5 + 5x^3 + 5x$	[GHR19, Table 4]
24	$y^2 = 3x^5 + 8x^3 + 6x$	[GHR19, Table 4]
35	$y^2 = 83x^6 - 184x^5 + 405x^4 + 80x^3 - 255x^2 + 136x + 127$	Remark 2.5
40	$y^2 = 9x^5 + 40x^3 + 45x$	[GHR19, Table 4]
51	$y^2 = x^6 + x^3 + \frac{4}{17}$	[Car01, p. 112]
52	$y^2 = 9x^5 + 65x^3 + 117x$	[GHR19, Table 4]
88	$y^2 = 99x^5 + 280x^3 + 198x$	[GHR19, Table 4]
91	$y^2 = 8477x^6 + 11340x^5 - 30513x^4 - 15336x^3 + 42135x^2 - 11124x + 1637$	Remark 2.5
115	$y^2 = 2647x^6 - 5736x^5 + 7545x^4 + 1520x^3 - 4995x^2 + 4824x + 3483$	Remark 2.5
123	$y^2 = x^6 + x^3 + \frac{256}{1025}$	[Car01, p. 112]
148	$y^2 = 441x^5 + 5365x^3 + 16317x$	[GHR19, Table 4]
187	$y^2 = 258093x^6 + 519750x^5 - 364518x^4 - 1612000x^3 + 286356x^2 + 719000x + 248616$	Remark 2.5
232	$y^2 = 9801x^5 + 105560x^3 + 284229x$	[GHR19, Table 4]
235	$y^2 = 63847x^6 - 89256x^5 - 89655x^4 - 27280x^3 + 135405x^2 + 105624x + 48843$	Remark 2.5
267	$y^2 = x^6 + x^3 + \frac{62500}{250001}$	[Car01, p. 112]
403	$y^2 = 19149677x^6 - 28664274x^5 + 11992662x^4 - 83358256x^3 + 76850532x^2 - 3824904x + 53478712$	Remark 2.5
427	$y^2 = 178773643x^6 + 67725720x^5 - 770837595x^4 - 7030800x^3 + 871950585x^2 - 303837480x + 27419167$	Remark 2.5

TABLE 6. Curves whose geometric endomorphism algebra is $M_2(\mathbb{Q}(\sqrt{-d}))$ with $d \in \mathcal{D}_{2,2}^J$. The curves corresponding to discriminants 1012 and 1435 were provided to us by Narbonne-Ritzenthaler, and the rest were provided to us by Elkies. The column n denotes the degree of the optimal map from the curve to an elliptic curve.

d	n	Curve
84	3	$y^2 = (2x^2 - 6x - 9)(4x^4 - 24x^3 - 4x - 3)$
120	6	$y^2 = (2x^2 - 2x - 1)(6x^2 - 20x + 25)(18x^2 + 24x + 5)$
132	5	$y^2 = (x^2 - 2x - 10)(121x^4 + 572x^3 + 176x^2 + 40x + 4)$
168	8	$y^2 = (2x^2 + 26x - 3)(14x^2 - 16x + 1)(14x^2 + 28x + 23)$
228	5	$y^2 = (x^2 + 2x - 2)(15625x^4 + 62500x^3 - 5832x + 2916)$
372	7	$y^2 = 1771561x^6 - 10629366x^5 + 10629366x^4 + 10797488x^3$ $+ 5062500x^2 + 10125000x + 3375000$
408	10	$y^2 = 350354606x^6 - 590700831x^5 - 816200091x^4 + 1046797684x^3$ $+ 824978466x^2 - 502917081x - 378640481$
435	7	$y^2 = 10466471x^6 + 11098203x^5 - 95645550x^4 - 106834905x^3$ $+ 95572050x^2 - 49559037x + 7237649$
520	6	$y^2 = (19x^2 + 54x + 37)(319x^2 - 444x + 171)(445083x^2 + 396482x - 144363)$
532	3	$y^2 = (50251x^2 + 27624x - 17865)(29x^4 - 128x^3 + 114x^2 + 160x - 75)$
708	11	$y^2 = (6655x^2 - 3278x - 1966)(14225761x^4 + 9092252x^3 - 47672800x^2 + 48112648x + 6781636)$
1012	5	$y^2 = -(x^2 - 1350x + 2326)(8385623x^4 + 15948252x^3 - 44642960x^2 - 12762360x - 1510324)$
1435	11	$y^2 = 539468307211x^6 + 8859839654637x^5 + 71566557542400x^4 + 152349804189405x^3$ $- 44616942974400x^2 - 3819661212483x + 1228993875229$

REFERENCES

- [BCP97] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
- [BC] A. Bourdon, P. Clark, *Torsion points and Galois representations on CM elliptic curves*. To appear in *Pacific J. Math*.
- [BHLS15] R. Bröker, E. Howe, K. Lauter, P. Stevenhagen, *Genus-2 curves and Jacobians with a given number of points*. *LMS Journal of Computation and Mathematics*, 18(1) (2015), 170–197.
- [Car01] G. Cardona, *Models racionals de corbes de gènere 2*, Tesi Doctoral, Universitat Politècnica de Catalunya, 2001, available on <https://www.researchgate.net>.
- [CNP05] G. Cardona, E. Nart, and J. Pujolàs, *Curves of genus two over fields of even characteristic*, *Math. Z.* **250** (2005), 177–201.
- [CQ05] G. Cardona and J. Quer, *Field of moduli and field of definition for curves of genus 2*, in *Computational aspects of algebraic curves*, *Lecture Notes Ser. Comput.* **13**, World Sci. Publ. (2005), 71–83.
- [Cox98] D. A. Cox, *Primes of the form $x^2 + ny^2$* , Fermat, class field theory and complex multiplication, A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1989.
- [FKRS12] F. Fité, K.S. Kedlaya, V. Rotger, and A.V. Sutherland, *Sato–Tate distributions and Galois endomorphism modules in genus 2*, *Compos. Math.* **148** (2012), 1390–1442.
- [FG18] F. Fité and X. Guitart, *Fields of definition of elliptic k -curves and the realizability of all genus 2 Sato–Tate groups over a number field*. *Trans. Amer. Math. Soc.*, **370**(7) (2018), 4623–4659.
- [FG20] F. Fité, X. Guitart, *Endomorphism algebras of geometrically split abelian surfaces over \mathbb{Q}* , *Algebra & Number Theory* 14-6 (2020), 1399–1421.
- [FK91] G. Frey, E. Kani, *Curves of genus 2 covering elliptic curves and an arithmetical application*, In: G. van der Geer., F. Oort, J. Steenbrink (eds.), *Arithmetic Algebraic Geometry*. *Progress in Mathematics*, vol **89**. Birkhäuser, Boston, MA, 1991.
- [GHR19] A. Gélin, E. Howe, C. Ritzenthaler, *Principally polarized squares of elliptic curves with field of moduli equal to \mathbb{Q}* . *Proceedings of the Thirteenth Algorithmic Number Theory Symposium*, 257–274, *Open Book Ser.*, 2, Math. Sci. Publ., Berkeley, CA, 2019.
- [Hei34] H. Heilbronn, *On the class number in imaginary quadratic fields*, *Quart. J. Math. Oxford Ser. 2* **5** (1934), 150–160.
- [HLP00] E. Howe, F. Leprévost, B. Poonen, *Large torsion subgroups of split Jacobians of curves of genus two or three*. *Forum Math.* **12** (2000), no. 3, 315–364.
- [JKPRST18] B. Jordan, A. Keeton, B. Poonen, E. Rains, N. Shepherd-Barron, and J. Tate, *Abelian varieties isogenous to a power of an elliptic curve*, *Compositio Mathematica*, **154**(5), 934–959 (2018).
- [Kan11] E. Kani, *Products of CM elliptic curves*, *Collect. Math.* **62** (2011), 297–339.
- [Kuh88] R. M. Kuhn, *Curves of genus 2 with split Jacobian*, *Trans. Amer. Math. Soc.* **307** no. 1 (1988), 41–49.
- [Kum15] A. Kumar, *Hilbert modular surfaces for square discriminants and elliptic subfields of genus 2 function fields*, *Res. Math. Sci.* **2** Art. 24 (2015), 46 pages.
- [Lau01] K. Lauter, with an Appendix by J.-P. Serre, *Geometric Methods for Improving the Upper Bounds on the Number of Rational Points on Algebraic Curves over Finite Fields*, *Journal of Algebraic Geometry* 10 (2001), no. 1, 19–36.
- [MSV09] K. Magaard, T. Shaska, and H. Völklein, *Genus 2 curves that admit a degree 5 map to an elliptic curve*, *Forum Math.* **21** no. 3 (2009), 547–566.
- [Mes91] J.-F. Mestre, *Construction de courbes de genre 2 à partir de leurs modules*. In *Effective methods in algebraic geometry (Castiglione, 1990)*, pages 313–334. Birkhäuser Boston, Boston, MA, 1991.
- [Nak04] T. Nakamura, *A classification of \mathbb{Q} -curves with complex multiplication*, *J. Math. Soc. Japan* **56**:2 (2004), 635–648.
- [Nar22] F. Narbonne, *Polarized products of elliptic curves with complex multiplication and field of moduli \mathbb{Q}* , arXiv:2203.11982.

- [S⁺09] W. A. Stein et al., *Sage Mathematics Software (Version 8.2)*, The Sage Development Team, 2018, <http://www.sagemath.org>.
- [Sha96] I. R. Shafarevich, *On the arithmetic of singular K 3-surfaces*, pp. 103–108 in Algebra and analysis (Kazan, Russia, 1994), edited by M. M. Arslanov et al., de Gruyter, Berlin, 1996.
- [Sha04] T. Shaska, *Genus 2 fields with degree 3 elliptic subfields*, Forum Math. **16** (2004), no. 2, 263–280.
- [SWWW08] T. Shaska, G. S. Wijesiri, S. Wolf, L. Woodland, *Degree 4 coverings of elliptic curves by genus 2 curves*, Albanian J. Math. **2** no. 4 (2008), 307–318.
- [Sil94] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*. Graduate Texts in Mathematics **151**, Springer-Verlag, New York, 1994. xiv+525 pp. ISBN: 0-387-94328-5.
- [Ste01] P. Stevenhagen, *Hilbert’s 12th problem, complex multiplication and Shimura reciprocity. Class field theory – its centenary and prospect* (Tokyo, 1998), 161–176, Adv. Stud. Pure Math. **30**, Math. Soc. Japan, Tokyo, 2001.
- [Wat03] M. Watkins, *Class numbers of imaginary quadratic fields*, Math. Comp. **73** (2004), no. 246, 907–938.
- [Wei56] A. Weil, *The field of definition of a variety*, Am. J. Math **78** (1956), 509–524.
- [Wei57] A. Weil, *Zum Beweis des Torellischen Satzes*, volume 2 of Nachrichten der Akademie der Wissenschaften in Göttingen, Mathematisch-Physikalische Klasse. Vandenhoeck & Ruprecht, 1957.

DEPARTAMENT DE MATEMÀTIQUES I INFORMÀTICA, UNIVERSITAT DE BARCELONA AND CENTRE DE RECERCA MATEMÀTICA, GRAN VIA DE LES CORTS CATALANES, 585, 08007 BARCELONA, CATALONIA

Email address: ffite@ub.edu

URL: <https://www.ub.edu/nt/ffite/>

DEPARTAMENT DE MATEMÀTIQUES I INFORMÀTICA, UNIVERSITAT DE BARCELONA, GRAN VIA DE LES CORTS CATALANES, 585, 08007 BARCELONA, CATALONIA

Email address: enricflorit@ub.edu

URL: <https://enricflorit.com/>

DEPARTAMENT DE MATEMÀTIQUES I INFORMÀTICA, UNIVERSITAT DE BARCELONA AND CENTRE DE RECERCA MATEMÀTICA, GRAN VIA DE LES CORTS CATALANES, 585, 08007 BARCELONA, CATALONIA

Email address: xevi.guitart@gmail.com

URL: <http://www.maia.ub.es/~guitart/>