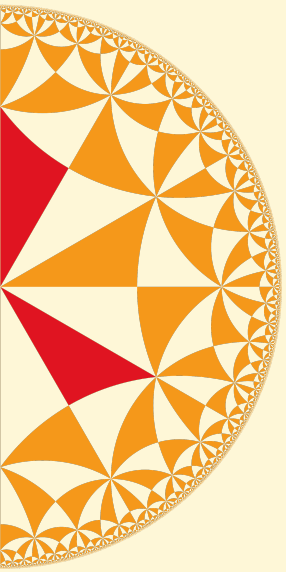
Université Grenoble Alpes



ANNALES DE
L'INSTITUT FOURIER

Francesca Balestrieri, Alexis Johnson & Rachel Newton

Explicit uniform bounds for Brauer groups of singular K3 surfaces

Tome 73, nº 2 (2023), p. 567-607.

https://doi.org/10.5802/aif.3526

Les *Annales de l'Institut Fourier* sont membres du Centre Mersenne pour l'édition scientifique ouverte
www.centre-mersenne.org e-ISSN : 1777-5310

Ann. Inst. Fourier, Grenoble
73, 2 (2023) 567-607

EXPLICIT UNIFORM BOUNDS FOR BRAUER GROUPS OF SINGULAR K3 SURFACES

by Francesca BALESTRIERI, Alexis JOHNSON & Rachel NEWTON (*)

Abstract. — Let k be a number field. We give an explicit bound, depending only on $[k : \mathbf{Q}]$ and the discriminant of the Néron–Severi lattice, on the size of the Brauer group of a K3 surface X/k that is geometrically isomorphic to the Kummer surface attached to a product of isogenous CM elliptic curves. As an application, we show that the Brauer–Manin set for such a variety is effectively computable. Conditional on GRH, we can also make the explicit bound depend only on $[k : \mathbf{Q}]$ and remove the condition that the elliptic curves be isogenous. In addition, we show how to obtain a bound, depending only on $[k : \mathbf{Q}]$, on the number of $\mathbf{C}$-isomorphism classes of singular K3 surfaces defined over k, thus proving an effective version of the strong Shafarevich conjecture for singular K3 surfaces.

Résumé. — Soit k un corps de nombres. On donne une borne explicite, dépendant uniquement de $[k : \mathbf{Q}]$ et du discriminant du réseau de Néron–Severi, pour la taille du groupe de Brauer de toute surface K3 X/k qui est géométriquement isomorphe à la surface Kummer attachée à un produit de courbes elliptiques de type CM isogènes. Comme application, on montre que l'ensemble de Brauer–Manin pour une telle variété est effectivement calculable. Sous l'hypothèse de Riemann généralisée, on peut de plus faire dépendre la borne explicite uniquement de $[k : \mathbf{Q}]$ et supprimer la contrainte d'isogénéité des courbes elliptiques. En outre, on montre comment obtenir une borne, dépendant uniquement de $[k : \mathbf{Q}]$, pour le nombre de classes d'isomorphismes sur $\mathbf{C}$ de surfaces K3 singulières définies sur k, prouvant ainsi une version effective de la conjecture forte de Shafarevich pour les surfaces K3 singulières.

1. Introduction

Let k be a number field with a fixed algebraic closure $\overline{k}$ and let X be a smooth, projective, geometrically integral variety over k with structure

Keywords: Brauer groups, K3 surfaces, uniform bounds, Brauer–Manin obstructions, effective strong Shafarevich conjecture.
2020 *Mathematics Subject Classification:* 11G35, 14J28, 14F22.
(*) Francesca Balestrieri was partially supported by the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant 840684. Rachel Newton was supported by EPSRC grant EP/S004696/1 and UKRI Future Leaders Fellowship MR/T041609/1.

morphism $s : X \to \operatorname{Spec} k$. The Brauer group of X is defined as $\operatorname{Br} X \coloneqq \mathrm{H}^2_{\text{ét}}(X, \mathbf{G}_m)$ and has a filtration

$$\operatorname{Br}_0 X \coloneqq \operatorname{im}\left(\operatorname{Br} k \xrightarrow{s^*} \operatorname{Br} X\right) \subset \operatorname{Br}_1 X \coloneqq \ker\left(\operatorname{Br} X \to \operatorname{Br} \overline{X}\right) \subset \operatorname{Br} X,$$

where $\overline{X} \coloneqq X \times_k \overline{k}$. In the 1970s, Manin proposed a systematic way to use the Brauer group to study the set $X(k)$ of rational points of X, as follows (see [19]). Consider the pairing

$$\langle\ ,\ \rangle_{\mathrm{BM}} : X(\mathbf{A}_k) \times \operatorname{Br} X \to \mathbf{Q}/\mathbf{Z}$$

given by $\langle (x_v)_v, \alpha\rangle_{\mathrm{BM}} \coloneqq \sum_{v\in\Omega_k} \operatorname{inv}_v(x_v^*(\alpha))$ where, for each non-trivial place $v \in \Omega_k$, the map $\operatorname{inv}_v : \operatorname{Br}(k_v) \to \mathbf{Q}/\mathbf{Z}$ is the local invariant map coming from class field theory. Then it is easily seen that the closure $\overline{X(k)}$ of $X(k)$ in the adelic topology is contained in the left kernel of this pairing. We call this left kernel the *Brauer–Manin set of* X and denote it by $X(\mathbf{A}_k)^{\mathrm{Br}}$. If X *satisfies the Hasse principle with Brauer–Manin obstruction*, meaning that $X(\mathbf{A}_k)^{\mathrm{Br}} = \emptyset$ if and only if $X(k) = \emptyset$, and if furthermore we have a way to *effectively* compute the Brauer–Manin set $X(\mathbf{A}_k)^{\mathrm{Br}}$, then it follows that we can effectively decide whether X has a rational point or not. Such effectivity results are related to Hilbert's famous tenth problem and its variations.

In this paper we focus on singular K3 surfaces and K3 surfaces that are geometrically Kummer surfaces of products of CM elliptic curves. It is conjectured by Skorobogatov (see [32]) that, for any K3 surface X over k, we have $\overline{X(k)} = X(\mathbf{A}_k)^{\mathrm{Br}}$. If this conjecture holds, then the problem of determining the qualitative arithmetic behaviour of the set of rational points of K3 surfaces is reduced to the problem of understanding their Brauer–Manin sets. A first step towards solving this problem is to study the relevant Brauer groups. By [15, Theorem 1], it turns out that for effectivity problems concerning the computation of these Brauer–Manin sets, it suffices to effectively bound the size of $\operatorname{Br} X/\operatorname{Br}_0 X$, which is finite for K3 surfaces (see [33]). Moreover, for K3 surfaces, Várilly-Alvarado has postulated the existence of *uniform* bounds for $\#(\operatorname{Br} X/\operatorname{Br}_0 X)$, although he makes no mention of effectivity of the bounds in the following conjecture:

Conjecture 1.1 (Strong uniform boundedness [40, Conjecture 4.6]). *Fix a positive integer n and a primitive lattice $\Lambda \hookrightarrow \Lambda_{K3} \coloneqq U^{\oplus 3} \oplus E_8^{\oplus 2}$. Let X be a K3 surface over a number field of degree n such that $\mathrm{NS}\,\overline{X} \cong \Lambda$ as abstract lattices. Then there is a constant $C(n, \Lambda)$, independent of X, such that $\#(\operatorname{Br} X/\operatorname{Br}_0 X) \leqslant C(n, \Lambda)$.*

When X is a K3 surface, explicit uniform bounds are already known for the size of $\mathrm{Br}_1 X/\mathrm{Br}_0 X$, see Remark 1.4. Hence the real content of Conjecture 1.1 is the existence of uniform bounds for the so-called transcendental part of the Brauer group, $\mathrm{Br}\, X/\mathrm{Br}_1 X$. Conjecture 1.1 can thus be viewed within the context of a more general question:

QUESTION 1.2 ([41, Question 1.1]). — *Let k be a number field. Let Y be a smooth, projective surface over k with trivial canonical sheaf. Is there a bound for $\#\,\mathrm{im}(\mathrm{Br}\, Y \to \mathrm{Br}\, \overline{Y})$ that is independent of Y, depending only on, say, $h^1(Y, \mathscr{O}_Y)$, the geometric Néron–Severi lattice $\mathrm{NS}\,\overline{Y}$, and $[k : \mathbf{Q}]$?*

Our main aim in this paper is to give *explicit uniform* bounds on the size of $\mathrm{Br}\, X/\mathrm{Br}_0 X$ in the case where X/k is either a singular K3 surface or geometrically isomorphic to the Kummer surface associated to a product of CM elliptic curves. Following [27], we write $M(n)$ for the smallest positive integer N such that the order of any finite subgroup of $\mathrm{GL}_n(\mathbf{Z})$ divides N. Minkowski gave a formula for $M(n)$ in [20]. Of particular relevance for our results is the constant $M(20) = 2^{38} \cdot 3^{14} \cdot 5^6 \cdot 7^3 \cdot 11^2 \cdot 13 \cdot 17 \cdot 19$. In our statements of the following results, we refer to the theorems in the body of the paper for more precise expressions.

THEOREM (Corollary of Theorem 7.3). — *Let k be a number field. Let Λ be the Néron–Severi lattice of the Kummer surface of a product of isogenous (not necessarily full) CM elliptic curves over $\overline{k}$ and let X/k be a K3 surface such that $\mathrm{NS}\,\overline{X} \cong \Lambda$ as abstract lattices. Then*

$$\#\frac{\mathrm{Br}\, X}{\mathrm{Br}_1 X} \leqslant 2^{34} \cdot 3^3 \cdot \pi^{-2} \cdot M(20)^4 \cdot |\mathrm{disc}\, \Lambda|^2 \cdot [k : \mathbf{Q}]^4. \tag{1.1}$$

Remark 1.3. — The proof of Theorem 7.3 shows that the bound given in (1.1) can be dramatically improved in special cases. For instance, if $\mathrm{NS}\,\overline{X}$ is generated by divisors that are defined over k then the $M(20)^4$ factor can be eliminated from (1.1). If X is isomorphic over k to the Kummer surface of a product of k-isogenous (not necessarily full) CM elliptic curves, then

$$\#\frac{\mathrm{Br}\, X}{\mathrm{Br}_1 X} \leqslant 2^{-2} \cdot \pi^{-2} \cdot |\Delta_K|^{-1} \cdot |\mathrm{disc}\, \Lambda|^2 \cdot [k : \mathbf{Q}]^4$$

where $K = \mathbf{Q}(\sqrt{\mathrm{disc}\, \Lambda})$, and if, furthermore, the class number of K is 1 then

$$\#\frac{\mathrm{Br}\, X}{\mathrm{Br}_1 X} \leqslant 2^{-4} \cdot |\Delta_K|^{-2} \cdot |\mathrm{disc}\, \Lambda|^2 \cdot [k : \mathbf{Q}]^4.$$

Shafarevich [28] has conjectured that, for all $d \in \mathbf{Z}_{>0}$, there are only finitely many lattices, up to isomorphism, which occur as the geometric Néron–Severi lattice of a K3 surface defined over a number field of degree

at most d. If this conjecture is true then the dependence on the lattice in Conjecture 1.1 can be eliminated. In the CM setting, Orr and Skorobogatov proved the stronger statement (proved by Shafarevich for singular K3 surfaces) that there are only finitely many $\overline{\mathbf{Q}}$-isomorphism classes of K3 surfaces of CM type which can be defined over number fields of given degree [22, Theorem B]. However, their methods are not effective and, in particular, they do not enable us to eliminate the dependence on $\operatorname{disc}\Lambda$ in the bounds we describe above. Nevertheless, under the assumption of the Generalised Riemann Hypothesis, we can eliminate the dependence on the lattice Λ and obtain the following result giving an explicit bound depending only on the degree $[k:\mathbf{Q}]$, at the expense of a larger power of the degree appearing in the bound.

THEOREM (Theorem 7.4). — *Suppose that the Generalised Riemann Hypothesis holds. Let k be a number field. Let X/k be such that $\overline{X}$ is a Kummer surface with* $\operatorname{rank}\mathrm{NS}\,\overline{X} = 20$. *Then there exists a finite extension L/k such that $X_L \cong \mathrm{Kum}(E \times E')$ for some elliptic curves E, E' over L and we have*

$$\#\frac{\operatorname{Br} X}{\operatorname{Br}_1 X} \leqslant (3.4)^2 \cdot 10^8 \cdot [L:\mathbf{Q}]^{12} \cdot \big((3.23)\cdot\log([L:\mathbf{Q}]) + (2.73)\cdot 109\big)^4.$$

Moreover, we can choose L such that $[L:k] \leqslant 2^9 \cdot 3 \cdot M(20)$.

For a generalisation of this result to singular K3 surfaces, see Theorem 7.5. For an analogous result in the case where X is geometrically isomorphic to the Kummer surface associated to a product of non-isogenous CM elliptic curves, see Theorem 7.6.

Remark 1.4. — For any K3 surface X over a number field, $\operatorname{Pic}\overline{X}$ is a free $\mathbf{Z}$-module of rank $r \leqslant 20$, whereby the proof of [41, Lemma 6.4] shows that $\#(\operatorname{Br}_1 X/\operatorname{Br}_0 X)$ divides $M(r)^r$. Hence Theorems 7.3 and 7.4 yield uniform bounds on the size of $\operatorname{Br} X/\operatorname{Br}_0 X$. This bound can be greatly improved in special cases – for example, if $\operatorname{Pic}\overline{X}$ has a set of generators that are defined over k then $\operatorname{Br}_1 X/\operatorname{Br}_0 X$ is trivial.

Using their proof of Shafarevich's conjecture for K3 surfaces of CM type, Orr and Skorobogatov proved Conjecture 1.1 for K3 surfaces of CM type by showing the existence of a bound depending only on the degree $[k:\mathbf{Q}]$, see [22, Corollary C.1]. However, it is not clear how to make their bound effective, let alone explicit. The value of our results lies in their explicit nature, which allows us to obtain the following effectivity result.

THEOREM (Theorem 7.7). — *Let k be a number field and let X/k be such that $\overline{X}$ is a Kummer surface with* $\operatorname{rank} \mathrm{NS}\, \overline{X} = 20$. *Then $X(\mathbf{A}_k)^{\mathrm{Br}}$ is effectively computable.*

Under the assumption of the Generalised Riemann Hypothesis, we obtain a similar effectivity result for a wider class of K3 surfaces – see Theorem 7.8. It is important to note that in results like Theorems 7.3 and 7.8 we allow complex multiplication by orders other than the full ring of integers of the CM field. In particular, our objects of study include varieties not tackled by Valloni in [39, §11], where he gave an effective algorithm which computes bounds on the size of $\operatorname{Br} \overline{X}^{\mathrm{Gal}(\overline{k}/k)}$ (and consequently on $\operatorname{Br} X/\operatorname{Br}_1 X$ and $\operatorname{Br} X/\operatorname{Br}_0 X$) in the case where X/k is a *principal* CM K3 surface. For examples of non-principal CM Kummer surfaces attached to products of CM elliptic curves, see [12, Example 9.8] for some cases where the elliptic curves are not isogenous, and [16] and [38, Theorem 3.2] for some cases where the elliptic curves are isogenous. It would be interesting to investigate whether Valloni's work can be used to obtain explicit uniform bounds for the transcendental parts of Brauer groups of principal CM K3 surfaces.

Our results for Kummer surfaces make use of the close relationship between the transcendental parts of the Brauer groups of abelian surfaces and the associated Kummer surfaces (see [34]). One of the inspirations for our work was the paper [41] of Várilly-Alvarado and Viray, in which they studied Question 1.2 for abelian surfaces and Kummer surfaces related to products of isogenous non-CM elliptic curves. In this context, they showed that the existence of uniform bounds (depending only on the degree of the base number field) on the odd order transcendental parts of the relevant Brauer groups is equivalent to the existence of a uniform bound on the odd parts of integers n for which there exist non-CM elliptic curves with abelian n-division fields. For a fixed prime ℓ, they gave uniform bounds on the ℓ-primary subgroups of the transcendental parts of the Brauer groups. In [2] Cantoral-Farfán, Tang, Tanimoto and Visse gave effective bounds for Brauer groups of Kummer surfaces associated to Jacobians of genus 2 curves over number fields. Their bounds depend on the Faltings height as well as the degree of the base field. For abelian varieties of arbitrary dimension, Gaudron and Rémond obtained bounds on the transcendental part of the Brauer group depending on the dimension, the Faltings height and the degree of the base field [7].

Our next result is an example of the kind of bound we obtain in the abelian setting, depending only on the degree of the base field and the geometric Néron–Severi lattice.

THEOREM (Corollary of Theorem 7.1). — *Let k be a number field and let A/k be an abelian surface such that* $\mathrm{NS}\,\overline{A}$ *contains a hyperbolic plane and* $\operatorname{rank}\mathrm{NS}\,\overline{A} = 4$. *Then*

$$\#\frac{\mathrm{Br}\,A}{\mathrm{Br}_1\,A} \leqslant 2^{18}\cdot 3^3\cdot \pi^{-2}\cdot |\mathrm{disc}\,\Lambda|^2\cdot [k:\mathbf{Q}]^4.$$

Conditional on the Generalised Riemann Hypothesis, we obtain the following uniform bound, which depends only on the degree of the base field:

THEOREM (Theorem 7.2). — *Suppose that the Generalised Riemann Hypothesis holds. Let k be a number field and let A/k be an abelian surface such that* $\mathrm{NS}\,\overline{A}$ *contains a hyperbolic plane and* $\operatorname{rank}\mathrm{NS}\,\overline{A} = 4$. *Let L/k be a finite extension such that* $\mathrm{End}(A_L) = \mathrm{End}(\overline{A})$. *Then*

$$\#\frac{\mathrm{Br}\,A}{\mathrm{Br}_1\,A} \leqslant (3.4)^2\cdot 10^8\cdot [L:\mathbf{Q}]^{12}\cdot\big((3.23)\cdot\log([L:\mathbf{Q}]) + (2.73)\cdot 109\big)^4.$$

Moreover, we can choose L such that $[L:k] \leqslant 2^4\cdot 3$.

In the course of our work, we obtain bounds for the conductors of endomorphism rings of CM elliptic curves over number fields, which may be of independent interest.

THEOREM (Corollary 4.4). — *Let k be a number field and let E/k be an elliptic curve with CM by an order of conductor $\mathfrak{f}$ in an imaginary quadratic field. Then*

$$\mathfrak{f} \leqslant \min\left\{3\cdot[k:\mathbf{Q}]^2, \max\{[k:\mathbf{Q}]^2, 7\}\right\}.$$

We use this and similar results to obtain bounds on the transcendental parts of Brauer groups related to products of CM elliptic curves. Our bounds on conductors also yield an explicit version of the main result of [28]:

THEOREM (Corollary 4.9). — *The number of $\mathbf{C}$-isomorphism classes of singular K3 surfaces defined over number fields of degree at most d is bounded above by*

$$3\cdot M(20)^3\cdot d^3\cdot(\log(3\cdot M(20)^2\cdot d^2)+1) \cdot \#\{K \text{ imaginary quadratic} \mid h_K \leqslant M(20)\cdot d\}.$$

Remarks 1.5.

(1) Using the Siegel–Tatuzawa Theorem [37], the quantity

$$\#\{K \text{ imaginary quadratic} \mid h_K \leqslant d\}$$

can be bounded explicitly in terms of d.

(2) In [36, Theorem 1], Soundararajan shows that for d sufficiently large

$$\#\{K \text{ imaginary quadratic} \mid h_K \leqslant d\} = \frac{3\zeta(2)}{\zeta(3)} \cdot d^2 + O_\epsilon\left(d^2 \cdot (\log d)^{-\frac{1}{2}+\epsilon}\right).$$

1.1. Notation and terminology

Throughout this paper, we use the following notation:

k	is a field of characteristic 0,
$\overline{k}$	is a fixed algebraic closure of k,
Γ_k	is the absolute Galois group $\mathrm{Gal}(\overline{k}/k)$ of k,
Ω_k	is the set of non-trivial k-places, when k is a number field,
X	is a variety over k,
X_l	is the base-change $X \times_{\mathrm{Spec}\, k} \mathrm{Spec}\, l$ of X to l/k,
$\overline{X}$	denotes $X_{\overline{k}}$,
$\mathrm{Br}_1 X$	denotes $\ker(\mathrm{Br}\, X \to \mathrm{Br}\, \overline{X})$,
$\mathrm{Br}_0 X$	denotes $\mathrm{im}(\mathrm{Br}\, k \to \mathrm{Br}\, X)$,
$\mathrm{Br}_1 X/\mathrm{Br}_0 X$	is the *algebraic* part of the Brauer group of X,
$\mathrm{Br}\, X/\mathrm{Br}_1 X$	is the *transcendental* part of the Brauer group of X.

For an abelian group scheme A over k and an integer $d \in \mathbf{Z}_{>0}$, we use the following notation:

$A[d]$	denotes the d-torsion subgroup of $A(\overline{k})$,
$A\{d\}$	denotes the d-primary part $\varinjlim_n A[d^n]$ of $A(\overline{k})$.

For an elliptic curve E defined over k, we use the following notation:

$\mathrm{End}(\overline{E})$	denotes the full ring of endomorphisms defined over $\overline{k}$,
$\mathrm{End}_k(E)$	denotes the subring of endomorphisms defined over k.

We say that E/k has complex multiplication (CM) by an order $\mathcal{O}$ in an imaginary quadratic field if $\mathrm{End}(\overline{E}) = \mathcal{O}$. We say that E/k has full CM if $\mathrm{End}(\overline{E})$ is isomorphic to the ring of integers of an imaginary quadratic field.

For an imaginary quadratic field K, we use the following notation:

Δ_K	denotes the discriminant of K,
h_K	denotes the class number of K,
$\mathcal{O}_K$	denotes the ring of integers of K,
$\mathcal{O}_{K,\mathfrak{f}}$	denotes the order of conductor $\mathfrak{f}$ inside $\mathcal{O}_K$,
$\mathcal{O}_\mathfrak{f}$	denotes the order of conductor $\mathfrak{f}$ inside $\mathcal{O}_K$ when K is clear,
$K_\mathfrak{f}$	denotes the ring class field associated to the order $\mathcal{O}_{K,\mathfrak{f}}$,

and for an order $\mathcal{O}$ in K:

$$h(\mathcal{O}) \quad \text{denotes the class number of } \mathcal{O}.$$

Throughout the paper we fix embeddings $k \hookrightarrow \overline{k} \hookrightarrow \mathbf{C}$ and consider all field extensions of k of finite degree as subfields of $\overline{k}$.

1.2. Acknowledgements

The authors are very grateful to Éric Gaudron and Gaël Rémond for pointing out some errors in a previous draft of this article and providing some useful references. They are also indebted to the anonymous referee whose helpful comments improved the article and its exposition. The authors thank Tim Browning, Jennifer Berg, Titus Hilberdink, Adam Logan, Jack Petok, Matthias Schütt, Alexei Skorobogatov, Domenico Valloni, Tony Várilly-Alvarado and Bianca Viray for useful discussions.

2. Abelian surfaces of product type

Definition 2.1. — *Let k be a field of characteristic 0. Denote by $\mathscr{A}_k$ the set of abelian surfaces A/k such that* $\mathrm{NS}\,\overline{A}$ *contains a hyperbolic plane. For a lattice Λ containing a hyperbolic plane, denote by $\mathscr{A}_{k,\Lambda}$ the set of abelian surfaces A/k such that* $\mathrm{NS}\,\overline{A}$ *is isomorphic to Λ (as an abstract lattice, with no Galois action).*

The lemma below shows that $\mathscr{A}_k$ consists of the surfaces that are geometrically isomorphic to products of elliptic curves.

Lemma 2.2 ([41, Lemma 2.8]). — *Let A be an abelian surface over an algebraically closed field such that* $\mathrm{NS}\,A$ *contains a hyperbolic plane. Then A is isomorphic to a product of elliptic curves. In addition,*

- *if* $\operatorname{rank}\mathrm{NS}\,A = 2$, *then the elliptic curves are not isogenous,*
- *if* $\operatorname{rank}\mathrm{NS}\,A = 3$, *then the elliptic curves are non-CM, isogenous, and the degree of a cyclic isogeny between them is* $\frac{1}{2}\operatorname{disc}\mathrm{NS}\,A$, *and*
- *if* $\operatorname{rank}\mathrm{NS}\,A = 4$, *then the elliptic curves are isogenous and CM.*

Next, we bound the degree of a number field over which an element of $\mathscr{A}_k$ becomes isomorphic to a product of elliptic curves.

PROPOSITION 2.3. — *Let k be a field of characteristic 0 and let $A \in \mathscr{A}_k$. Then there exist a finite extension L/k with $[L : k] \leqslant 2^4 \cdot 3$ and elliptic curves E and E' over L such that*

$$A_L \cong E \times E'.$$

Furthermore, if $\operatorname{rank} \mathrm{NS}\, \overline{A} = 2$, *then* $[L : k] \leqslant 2$. *If* $\operatorname{rank} \mathrm{NS}\, \overline{A} = 3$, *then* $[L : k] \in \{1, 2, 3, 4, 6, 8, 12\}$. *If* $\mathrm{NS}\, \overline{A}$ *is isomorphic (as an abstract lattice) to the Néron–Severi lattice of a product of isogenous elliptic curves with CM by K, then $K \subset L$, the elliptic curves E and E' have CM by K, and* $\mathrm{End}(A_L) = \mathrm{End}(\overline{A})$.

Proof. — By Lemma 2.2, there exist elliptic curves E and E' over $\overline{k}$ such that $\overline{A} \cong E \times E'$. By viewing the projections onto E and E' as endomorphisms of $\overline{A}$, one sees that if for some field extension L/k we have $\mathrm{End}(A_L) = \mathrm{End}(\overline{A})$ then it follows that A_L is isomorphic to a product of elliptic curves over L. As a consequence of [6, Theorem 4.3], there exists a Galois extension L/k of degree at most $2^4 \cdot 3$ such that $\mathrm{End}(A_L) = \mathrm{End}(\overline{A})$. (See also [24, Théorème 1.1] for a result for abelian varieties of arbitrary dimension.) If $\mathrm{NS}\, \overline{A}$ is isomorphic (as an abstract lattice) to the Néron–Severi lattice of a product of isogenous elliptic curves with CM by K then $\mathrm{End}(A_L) \otimes \mathbf{Q} \cong M_2(K)$ and, in particular, K is fixed by $\mathrm{Gal}(\overline{k}/L)$.

For the cases where $\operatorname{rank} \mathrm{NS}\, \overline{A} \leqslant 3$, we follow the proof of [41, Proposition 2.7]. Let $\mathcal{M}_{1,1} \coloneqq \mathbb{A}^1$ denote the coarse moduli space of elliptic curves, parametrised by the j-invariant. The coarse moduli space $\mathcal{A}_2$ of principally polarised abelian surfaces contains the Humbert surface $\mathcal{H}_1 \coloneqq \mathrm{Sym}^2 \mathcal{M}_{1,1}$, which is the locus of abelian surfaces with product structure. We have an isomorphism $\mathrm{Sym}^2 \mathcal{M}_{1,1} \cong \mathbb{A}^2$ given by sending the class of (j_1, j_2) to $(j_1 + j_2, j_1 \cdot j_2)$.

Since $\overline{A} \cong E \times E'$, the surface A gives rise to a point $x \in \mathcal{H}_1(\overline{k})$, which has coordinates $(j(E) + j(E'), j(E) \cdot j(E'))$ when viewed as a point in $\mathbb{A}^2(\overline{k})$. For any $\sigma \in \Gamma_k$, we have $\sigma(A) = A$, so $E \times E' \cong \sigma(E \times E')$, and thus $x \in \mathcal{H}_1(k)$. Therefore $j(E) + j(E')$ and $j(E) \cdot j(E')$ belong to k, and so there is an extension k_0/k of degree at most 2 such that $j(E), j(E') \in k_0$. Therefore, we may assume that E and E' are defined over k_0. Now A_{k_0} is a twist (as an abelian surface) of $E \times E'$ and hence corresponds to an element of $\mathrm{H}^1(k_0, \mathrm{Aut}(\overline{E} \times \overline{E'}))$. Let L/k_0 be a field extension. The abelian surface A_L is isomorphic to a product of elliptic curves over L if

$$[A_L] \in \mathrm{im}(\mathrm{H}^1(L, \mathrm{Aut}(\overline{E})) \times \mathrm{H}^1(L, \mathrm{Aut}(\overline{E'})) \to \mathrm{H}^1(L, \mathrm{Aut}(\overline{E} \times \overline{E'}))).$$

CASE 1: $\operatorname{rank} \mathrm{NS}\, \overline{A} = 2$. — *In this case* $\mathrm{Aut}(\overline{E} \times \overline{E'}) = \mathrm{Aut}(\overline{E}) \oplus \mathrm{Aut}(\overline{E'})$ *and hence* $\mathrm{H}^1(k_0, \mathrm{Aut}(\overline{E})) \times \mathrm{H}^1(k_0, \mathrm{Aut}(\overline{E'})) \to \mathrm{H}^1(k_0, \mathrm{Aut}(\overline{E} \times \overline{E'}))$ *is an*

isomorphism. Therefore, A_{k_0} is isomorphic to a product of elliptic curves over k_0.

Case 2: $\operatorname{rank} \mathrm{NS}\, \overline{A} = 3$. — *This is the case treated in* [41, Proposition 2.7]. *The authors show that for any $\phi \in \mathrm{H}^1(k_0, \mathrm{Aut}(\overline{E} \times \overline{E'}))$ there exists a field extension L/k_0 with $[L : k_0] \in \{1, 2, 3, 4, 6\}$ such that*

$$\mathrm{Res}_{L/k_0}\, \phi \in \mathrm{im}(\mathrm{H}^1(L, \mathrm{Aut}(\overline{E})) \times \mathrm{H}^1(L, \mathrm{Aut}(\overline{E'})) \to \mathrm{H}^1(L, \mathrm{Aut}(\overline{E} \times \overline{E'}))).$$

Observing that $[L : k] = [L : k_0] \cdot [k_0 : k]$ and $[k_0 : k] \leqslant 2$ yields the result. □

The following result is surely well known but we include it here for completeness since we will use it later.

Lemma 2.4. — *Let E and E' be elliptic curves defined over a field k of characteristic 0 such that $\mathrm{End}(\overline{E}) \otimes \mathbb{Q} \subset k$. Suppose that there exists a k-isogeny $\phi : E \to E'$. Then all isogenies between $\overline{E}$ and $\overline{E'}$ are induced by isogenies defined over k.*

Proof. — Let $\bar{\phi} : \overline{E} \to \overline{E'}$ denote the induced isogeny and let $\bar{\phi}^\vee$ denote its dual. Then $\psi \mapsto \bar{\phi}^\vee \circ \psi$ gives an injective map of Galois modules $\mathrm{Hom}(\overline{E}, \overline{E'}) \to \mathrm{End}(\overline{E})$. Since $\mathrm{End}(\overline{E}) \otimes \mathbb{Q} \subset k$, the action of Γ_k on $\mathrm{End}(\overline{E})$ is trivial and hence all elements of $\mathrm{Hom}(\overline{E}, \overline{E'})$ are fixed by Γ_k, as required. □

The final results in this section show how to read information about the CM orders of isogenous elliptic curves E_1 and E_2 from the Néron–Severi lattice of their product.

Proposition 2.5 ([14, Corollary 24]). — *Let E_1 and E_2 be isogenous elliptic curves over an algebraically closed field of characteristic 0. Then*

$$\mathrm{disc}\, \mathrm{NS}(E_1 \times E_2) = -(-2)^{\rho-2} \cdot \mathrm{disc}\, \mathrm{Hom}(E_1, E_2), \tag{2.1}$$

where $\rho := \operatorname{rank} \mathrm{NS}(E_1 \times E_2)$ and $\mathrm{Hom}(E_1, E_2)$ is a lattice with pairing $\langle \varphi, \psi \rangle := \frac{1}{2}(\deg(\varphi + \psi) - \deg \varphi - \deg \psi)$.

Note that Lemma 2.2 shows that $\rho - 2 = \operatorname{rank} \mathrm{Hom}(E_1, E_2)$. In [14], Kani considers the pairing $\langle \varphi, \psi \rangle := \deg(\varphi + \psi) - \deg \varphi - \deg \psi$ on $\mathrm{Hom}(E_1, E_2)$, whence the power of 2 in (2.1).

Proposition 2.6 ([13, Corollary 42]). — *Let E_1 and E_2 be elliptic curves over an algebraically closed field of characteristic 0 with CM by orders with conductors $\mathfrak{f}_1$ and $\mathfrak{f}_2$, respectively, in an imaginary quadratic field K. Then*

$$\mathrm{disc}\, \mathrm{Hom}(E_1, E_2) = -2^{-2} \cdot \mathrm{lcm}(\mathfrak{f}_1, \mathfrak{f}_2)^2 \cdot \Delta_K$$

where $\mathrm{Hom}(E_1, E_2)$ *is a lattice with pairing* $\langle \varphi, \psi \rangle \coloneqq \frac{1}{2}(\deg(\varphi+\psi) - \deg\varphi - \deg\psi)$.

Proof. — This follows immediately from [13, Corollary 42] upon noting that the author's $\Delta(q_{E_1,E_2})$ is equal to $-4 \cdot \operatorname{disc}\mathrm{Hom}(E_1, E_2)$. □

Combining Propositions 2.5 and 2.6 gives the following corollary.

COROLLARY 2.7. — *Let* E_1 *and* E_2 *be elliptic curves over an algebraically closed field of characteristic 0 with CM by orders with conductors* $\mathfrak{f}_1$ *and* $\mathfrak{f}_2$*, respectively, in an imaginary quadratic field* K*. Then*

$$\operatorname{disc}\mathrm{NS}(E_1 \times E_2) = \operatorname{lcm}(\mathfrak{f}_1, \mathfrak{f}_2)^2 \cdot \Delta_K.$$

3. The associated Kummer surfaces

DEFINITION 3.1 ([35, Definition 2.1]). — *Let* k *be a field of characteristic 0. Let* A *be an abelian surface over* k*. Any* k*-torsor* T *under* $A[2]$ *gives rise to a 2-covering* $\rho : V \to A$*, where* V *is the quotient of* $A \times_k T$ *by the diagonal action of* $A[2]$ *and* ρ *comes from the projection onto the first factor. Then* $T = \rho^{-1}(O_A)$ *and* V *has the structure of a* k*-torsor under* A*. The class of* T *maps to the class of* V *under the map* $\mathrm{H}^1_{\text{ét}}(k, A[2]) \to \mathrm{H}^1_{\text{ét}}(k, A)$ *induced by the inclusion of group schemes* $A[2] \to A$ *and, in particular, the period of* V *divides* 2*. Let* $\sigma : \widetilde{V} \to V$ *be the blow-up of* V *at* $T \subset V$*. The involution* $[-1] : A \to A$ *fixes* $A[2]$ *and induces involutions* ι *on* V *and* $\widetilde{\iota}$ *on* $\widetilde{V}$ *whose fixed point sets are* T *and the exceptional divisor, respectively. We call* $\mathrm{Kum}\, V \coloneqq \widetilde{V}/\widetilde{\iota}$ *the* Kummer surface associated to V (or T)*. We remark that the quotient* $\mathrm{Kum}\, V$ *is geometrically isomorphic to* $\mathrm{Kum}\, A$*, so in particular it is smooth.*

DEFINITION 3.2. — *For a lattice* Λ*, denote by* $\mathscr{K}_{k,\Lambda}$ *the set of smooth, projective K3 surfaces* X/k *such that* $\mathrm{NS}\,\overline{X}$ *is isomorphic to* Λ *(as an abstract lattice, with no Galois action). Let* S *be the set of lattices that occur as the Néron–Severi lattice of the Kummer surface of a product of elliptic curves over* $\overline{k}$*, and let* $\mathscr{K}_k \coloneqq \bigcup_{\Lambda \in S} \mathscr{K}_{k,\Lambda}$.

DEFINITION 3.3. — *Let* $X \coloneqq \mathrm{Kum}\, Y$ *be a Kummer surface over* k*, where* $Y \to A$ *is a 2-covering of some abelian surface* A *over* k*. Consider the natural blow-up map* $\overline{X} \to \overline{Y}/\iota_{\overline{k}}$*, where* $\iota_{\overline{k}} : \overline{A} \to \overline{A}$ *is the antipodal involution, whose exceptional divisor consists of 16 pairwise disjoint smooth rational* (-2)*-curves and forms a sublattice* $\mathbf{Z}^{16} \subset \mathrm{NS}\,\overline{X}$*. The* Kummer lattice associated to $\overline{X}$*, denoted by* Λ_K*, is the saturation of this sublattice.*

It can be shown that Λ_K is an even, negative-definite lattice of rank 16 and discriminant 2^6 whose isomorphism type is independent of the choice of Y. (For more details about the Kummer lattice, we refer the reader to e.g. [18].)

The next results allow us to bound the degree of a field extension over which an element of $\mathscr{K}_k$ becomes the Kummer surface attached to a product of elliptic curves.

PROPOSITION 3.4 ([41, Proposition 2.1]). — *There is a positive integer N such that for any number field k, and any K3 surface X/k with $\mathrm{NS}\,\overline{X}$ containing a sublattice isomorphic to Λ_K, there is an extension k_0/k of degree at most N such that X_{k_0} is a Kummer surface.*

THEOREM 3.5. — *Let $X \coloneqq \mathrm{Kum}\,Y$ be a Kummer surface over a field k of characteristic 0, where $Y \to A$ is a 2-covering of some abelian surface A over k. Assume that $X \in \mathscr{K}_k$. Then there exist a field extension L/k with $[L:k] \leqslant 2^4 \cdot 3$ and elliptic curves E and E' over L such that*

$$A_L \cong E \times E'.$$

Furthermore, if $\mathrm{rank}\,\mathrm{NS}\,\overline{X} = 18$, then $[L:k] \leqslant 2$. If $\mathrm{rank}\,\mathrm{NS}\,\overline{X} = 19$, then $[L:k] \in \{1,2,3,4,6,8,12\}$. If $\mathrm{NS}\,\overline{A}$ is isomorphic (as an abstract lattice) to the Néron–Severi lattice of a product of isogenous elliptic curves with CM by K, then $K \subset L$, the elliptic curves E and E' have CM by K, and $\mathrm{End}(A_L) = \mathrm{End}(\overline{A})$.

Proof. — There is an exact sequence of lattices

$$0 \to \Lambda_K \to \mathrm{NS}\,\overline{X} \to \mathrm{NS}\,\overline{Y} \to 0,$$

where Λ_K is the Kummer lattice and the map $\Lambda_K \to \mathrm{NS}\,\overline{X}$ is the natural inclusion (see [34, Remark 2], for example). Since $X \in \mathscr{K}_k$, this implies that $\mathrm{NS}\,\overline{Y}$ is isomorphic as an abstract lattice to $\mathrm{NS}(\overline{E} \times \overline{E'})$ for some elliptic curves $\overline{E}$ and $\overline{E'}$ defined over $\overline{k}$. Since $\overline{Y} \cong \overline{A}$, this shows that $A \in \mathscr{A}_k$. Now apply Proposition 2.3. □

COROLLARY 3.6. — *There exists a positive integer M_0 such that, for all number fields k and all surfaces $X \in \mathscr{K}_k$, there exist: a field extension L_0/k of degree at most M_0, elliptic curves E and E' over L_0, and a 2-covering $Y \to E \times E'$ such that*

$$X_{L_0} \cong \mathrm{Kum}\,Y.$$

Proof. — This follows immediately from Proposition 3.4 and Theorem 3.5. □

Remark 3.7. — The proof of [41, Proposition 2.1] shows that one may take $N = 2 \cdot M(20)$ in Proposition 3.4. Therefore, by Theorem 3.5 one may take $M_0 = 2^5 \cdot 3 \cdot M(20)$ in Corollary 3.6. With more information about the K3 surface X, this bound can be improved. If, for example, $X \in \mathscr{K}_k$ satisfies $\operatorname{rank} \mathrm{NS}\, \overline{X} = 18$ then one may take $N = 2 \cdot M(18)$ and $M_0 = 2^2 \cdot M(18)$.

PROPOSITION 3.8. — *Let A be an abelian surface over a field k of characteristic 0 and let $Y \to A$ be a 2-covering. Then there exists a field extension L_1/k with $[L_1 : k] \leqslant 2^4$ such that $Y_{L_1} \cong A_{L_1}$.*

Proof. — Since $f : Y \to A$ is a 2-covering, there exists a field extension L_1/k with $[L_1 : k] \leqslant \#A[2] = 2^4$ such that $Y_{L_1} \cong A_{L_1}$. □

Remark 3.9. — In Proposition 3.8, if $Y \to A$ is the trivial 2-covering then we can take $L_1 = k$.

COROLLARY 3.10. — *Let E and E' be elliptic curves over a field k of characteristic 0, let $Y \to E \times E'$ be a 2-covering and let $X := \operatorname{Kum} Y$. Then there exists a field extension L_1/k with $[L_1 : k] \leqslant 2^4$ such that, for all $n \in \mathbf{Z}_{>0}$,*

$$\frac{\operatorname{Br} X_{L_1}[n]}{\operatorname{Br}_1 X_{L_1}[n]} \hookrightarrow \frac{\operatorname{Br}(E_{L_1} \times E'_{L_1})[n]}{\operatorname{Br}_1(E_{L_1} \times E'_{L_1})[n]}, \tag{3.1}$$

and hence

$$\frac{\operatorname{Br} X_{L_1}}{\operatorname{Br}_1 X_{L_1}} \hookrightarrow \frac{\operatorname{Br}(E_{L_1} \times E'_{L_1})}{\operatorname{Br}_1(E_{L_1} \times E'_{L_1})}. \tag{3.2}$$

Proof. — By Proposition 3.8 there exists an extension L_1/k with $[L_1 : k] \leqslant 2^4$ such that $Y_{L_1} \cong E_{L_1} \times E'_{L_1}$ and therefore $X_{L_1} \cong \operatorname{Kum}(E_{L_1} \times E'_{L_1})$. By [34, Theorem 2.4], we have an injection

$$\frac{\operatorname{Br} X_{L_1}[n]}{\operatorname{Br}_1 X_{L_1}[n]} \hookrightarrow \frac{\operatorname{Br}(E_{L_1} \times E'_{L_1})[n]}{\operatorname{Br}_1(E_{L_1} \times E'_{L_1})[n]}$$

which is an isomorphism if n is odd. The statement (3.2) follows from (3.1) since the Brauer groups in question are torsion by [9, Proposition 1.4]. □

Remark 3.11. — For n odd, (3.1) holds with $L_1 = k$ and, furthermore, the injection in (3.1) is an isomorphism. Indeed, if n is odd, apply [41, Proposition 3.3] to the 2-covering $f : Y \to E \times E'$ to get an isomorphism $f^* : \frac{\operatorname{Br}(E \times E')[n]}{\operatorname{Br}_1(E \times E')[n]} \to \frac{\operatorname{Br} Y[n]}{\operatorname{Br}_1 Y[n]}$.

The next two results show how to obtain information about the CM orders of isogenous elliptic curves E_1 and E_2 from the Néron–Severi lattice of $\operatorname{Kum}(E_1 \times E_2)$.

THEOREM 3.12 ([29, Theorem 3.3]). — *Let E_1 and E_2 be elliptic curves over an algebraically closed field of characteristic 0. Then*

$$|\operatorname{disc} \mathrm{NS}(\mathrm{Kum}(E_1 \times E_2))| = 2^4 \cdot |\operatorname{disc} \mathrm{Hom}(E_1, E_2)|,$$

where $\mathrm{Hom}(E_1, E_2)$ *is a lattice with pairing* $\langle \varphi, \psi \rangle := \frac{1}{2}(\deg(\varphi+\psi) - \deg \varphi - \deg \psi)$.

COROLLARY 3.13. — *Let E_1 and E_2 be elliptic curves over an algebraically closed field k of characteristic 0 with CM by orders with conductors $\mathfrak{f}_1$ and $\mathfrak{f}_2$, respectively, in an imaginary quadratic field K. Then*

$$|\operatorname{disc} \mathrm{NS}(\mathrm{Kum}(E_1 \times E_2))| = 2^2 \cdot \operatorname{lcm}(\mathfrak{f}_1, \mathfrak{f}_2)^2 \cdot |\Delta_K|.$$

Proof. — This is an immediate consequence of Theorem 3.12 and Proposition 2.6. □

4. Bounds on conductors and the Shafarevich conjecture for singular K3 surfaces

The main results of this section are Theorem 4.8 and Corollary 4.9 which yield an explicit version of Shafarevich's finiteness result for **C**-isomorphism classes of singular K3 surfaces defined over a number field. We begin with an auxiliary result giving bounds on conductors of orders in CM fields. These bounds are used in Corollary 4.5 and Proposition 4.6 to bound the number of **C**-isomorphism classes of elliptic curves defined over number fields of bounded degree. They are also used in the proof of Theorem 4.8 and they appear again in Section 5 where they are used to obtain bounds on the transcendental part of the Brauer group of a self-product of a CM elliptic curve.

PROPOSITION 4.1. — *Let K be an imaginary quadratic field and let $\mathcal{O}_\mathfrak{f}$ be an order of conductor $\mathfrak{f} > 0$ in $\mathcal{O}_K$. Let $K_\mathfrak{f}$ denote the ring class field associated to $\mathcal{O}_\mathfrak{f}$. Then*

(1) *if $K = \mathbf{Q}(\sqrt{-7})$, we have $\mathfrak{f} \leqslant \max\{[K_\mathfrak{f} : K]^2, 2\}$;*
(2) *if $K = \mathbf{Q}(i)$, we have $\mathfrak{f} \leqslant \max\{[K_\mathfrak{f} : K]^2, 5\}$;*
(3) *if $K = \mathbf{Q}(\zeta_3)$, we have $\mathfrak{f} \leqslant \max\{[K_\mathfrak{f} : K]^2, 7\}$;*
(4) *in all other cases, $\mathfrak{f} \leqslant [K_\mathfrak{f} : K]^2$.*

In all cases,

$$\mathfrak{f} \leqslant 3 \cdot [K_\mathfrak{f} : K]^2.$$

Remark 4.2. — We note that the bounds given in Proposition 4.1 are far from optimal, as is clear by considering, for example, the case when $\mathfrak{f} = 1$ (i.e. when $\mathcal{O}_\mathfrak{f} = \mathcal{O}_K$).

Proof. — Recall the well-known formula for the class number (see e.g. [4, Theorem 7.24])

$$[K_\mathfrak{f} : K] = h(\mathcal{O}_\mathfrak{f}) = \frac{h_K \cdot \mathfrak{f}}{[\mathcal{O}_K^\times : \mathcal{O}_\mathfrak{f}^\times]} \cdot \prod_{p \mid \mathfrak{f}} \left(1 - \left(\frac{\Delta_K}{p}\right)\frac{1}{p}\right), \tag{4.1}$$

where the symbol $\left(\frac{\Delta_K}{p}\right)$ denotes the Legendre symbol for odd primes, while for the prime 2, the Legendre symbol is replaced by the Kronecker symbol $\left(\frac{\Delta_K}{2}\right)$, defined as

$$\left(\frac{\Delta_K}{2}\right) = \begin{cases} 0 & \text{if } 2 \mid \Delta_K, \\ 1 & \text{if } \Delta_K \equiv 1 \pmod 8, \\ -1 & \text{if } \Delta_K \equiv 5 \pmod 8. \end{cases}$$

Then

$$\mathfrak{f} = h_K^{-1} \cdot [K_\mathfrak{f} : K] \cdot [\mathcal{O}_K^\times : \mathcal{O}_\mathfrak{f}^\times] \cdot \prod_{p \mid \mathfrak{f}} \frac{p}{p - \left(\frac{\Delta_K}{p}\right)}. \tag{4.2}$$

On the other hand, since $\prod_{p \mid \mathfrak{f}} p \leqslant \mathfrak{f}$ we obtain

$$\prod_{p \mid \mathfrak{f}} p \leqslant h_K^{-1} \cdot [K_\mathfrak{f} : K] \cdot [\mathcal{O}_K^\times : \mathcal{O}_\mathfrak{f}^\times] \cdot \prod_{p \mid \mathfrak{f}} \frac{p}{p - \left(\frac{\Delta_K}{p}\right)}$$

and hence

$$\prod_{p \mid \mathfrak{f}} \left(p - \left(\frac{\Delta_K}{p}\right)\right) \leqslant h_K^{-1} \cdot [K_\mathfrak{f} : K] \cdot [\mathcal{O}_K^\times : \mathcal{O}_\mathfrak{f}^\times]. \tag{4.3}$$

Now we prove statements (1) – (4). If we can show that

$$[\mathcal{O}_K^\times : \mathcal{O}_\mathfrak{f}^\times]^2 \cdot \prod_{p \mid \mathfrak{f}} p \leqslant h_K^2 \cdot \prod_{p \mid \mathfrak{f}} \left(p - \left(\frac{\Delta_K}{p}\right)\right)^2 \tag{4.4}$$

then rearranging gives

$$\prod_{p \mid \mathfrak{f}} \frac{p}{p - \left(\frac{\Delta_K}{p}\right)} \leqslant h_K^2 \cdot [\mathcal{O}_K^\times : \mathcal{O}_\mathfrak{f}^\times]^{-2} \cdot \prod_{p \mid \mathfrak{f}} \left(p - \left(\frac{\Delta_K}{p}\right)\right)$$

and substituting this into (4.2) and applying (4.3) yields $\mathfrak{f} \leqslant [K_\mathfrak{f} : K]^2$. We will show that (4.4) holds except in some exceptional cases as described in statements (1) – (3).

Since K is an imaginary quadratic field, $\#\mathcal{O}_K^\times \leqslant 6$. For any $\mathfrak{f}$, we have $\pm 1 \in \mathcal{O}_\mathfrak{f}^\times$, whereby $[\mathcal{O}_K^\times : \mathcal{O}_\mathfrak{f}^\times] \leqslant 3$. First, we consider the case where $[\mathcal{O}_K^\times : \mathcal{O}_\mathfrak{f}^\times] = 1$. For all primes $p \geqslant 3$, we have

$$p \leqslant (p-1)^2 \leqslant \left(p - \left(\frac{\Delta_K}{p}\right)\right)^2.$$

Moreover, if $h_K > 1$, then $2 < h_K^2 \leqslant h_K^2 \cdot \left(2 - \left(\frac{\Delta_K}{2}\right)\right)^2$. We only run into trouble in proving (4.4) if $h_K = 1$ and $\left(\frac{\Delta_K}{2}\right) = 1$. The unique imaginary quadratic field satisfying these two hypotheses is $K = \mathbf{Q}(\sqrt{-7})$ with $\Delta_K = -7$. In this case, we have $2 \cdot p \leqslant \left(p - \left(\frac{-7}{p}\right)\right)^2$ for all primes $p \geqslant 3$ so the only way the product $\prod_{p|\mathfrak{f}} \left(p - \left(\frac{\Delta_K}{p}\right)\right)^2$ can be less than $\prod_{p|\mathfrak{f}} p$ is if $\mathfrak{f} = 2^n$ for some $n \geqslant 1$. In this case, (4.1) gives

$$[K_\mathfrak{f} : K] = 2^n \cdot \left(1 - \frac{1}{2}\right) = 2^{n-1}.$$

Hence, $\mathfrak{f} \leqslant [K_\mathfrak{f} : K]^2$ unless $\mathfrak{f} = 2$.

Now consider the special case where $[\mathcal{O}_K^\times : \mathcal{O}_\mathfrak{f}^\times] = 2$, meaning that $K = \mathbf{Q}(i)$, $\Delta_K = -4$ and $\mathfrak{f} > 1$. For $p = 3$ and all primes $p \geqslant 7$ we have $4 \cdot p \leqslant \left(p - \left(\frac{-4}{p}\right)\right)^2$. For $p \in \{2, 5\}$ we have $p \leqslant \left(p - \left(\frac{-4}{p}\right)\right)^2$. So we only run into trouble in proving (4.4) if $\mathfrak{f} = 2^a \cdot 5^b$ for some $a, b \in \mathbf{Z}_{\geqslant 0}$. In this case, (4.1) gives

$$[K_\mathfrak{f} : K] = 2^{a-1} \cdot 5^b \cdot \prod_{p|\mathfrak{f}} \left(1 - \left(\frac{-4}{p}\right)\frac{1}{p}\right) = \begin{cases} 2^{a-1} & \text{if } b = 0, \\ 2^{a+1} \cdot 5^{b-1} & \text{if } b \geqslant 1. \end{cases}$$

Now observe that $[K_\mathfrak{f} : K]^2 \geqslant \mathfrak{f}$ unless $\mathfrak{f} \in \{2, 5\}$.

Finally, consider the special case where $[\mathcal{O}_K^\times : \mathcal{O}_\mathfrak{f}^\times] = 3$, meaning that $K = \mathbf{Q}(\zeta_3)$, $\Delta_K = -3$ and $\mathfrak{f} > 1$. For $p \geqslant 11$ we have $9 \cdot p \leqslant (p-1)^2 \leqslant \left(p - \left(\frac{-3}{p}\right)\right)^2$ and for all p we have $3 \cdot p \leqslant \left(p - \left(\frac{-3}{p}\right)\right)^2$. Therefore, the only way that the product $\prod_{p|\mathfrak{f}} \left(p - \left(\frac{-3}{p}\right)\right)^2$ can be less than $9 \cdot \prod_{p|\mathfrak{f}} p$ is if $\mathfrak{f} \in \{2, 3, 5, 7\}$.

To see that in all cases $\mathfrak{f} \leqslant 3 \cdot [K_\mathfrak{f} : K]^2$, observe that in the exceptional cases with $\mathfrak{f} > [K_\mathfrak{f} : K]^2$, we have $\mathfrak{f} \leqslant 7$ and if $\mathfrak{f} > 3$ then $[K_\mathfrak{f} : K] = 2$. □

Remark 4.3. — An alternative bound is given by

$$\mathfrak{f} \leqslant \max\left\{[K_\mathfrak{f} : K]^2, \frac{5}{2} \cdot [\mathcal{O}_K^\times : \mathcal{O}_\mathfrak{f}^\times] \cdot [K_\mathfrak{f} : K]\right\}.$$

It can be easily checked that the inequality $\mathfrak{f} \leqslant \frac{5}{2} \cdot [\mathcal{O}_K^\times : \mathcal{O}_\mathfrak{f}^\times] \cdot [K_\mathfrak{f} : K]$ holds in all the exceptional cases in the proof of Proposition 4.1.

COROLLARY 4.4. — *Let k be a number field and let E/k be an elliptic curve with CM by an order of conductor $\mathfrak{f}$ in an imaginary quadratic field K. Then $K_\mathfrak{f} \subset Kk$ and hence $\mathfrak{f}$ satisfies the bounds of Proposition 4.1 with $[Kk : K]$ or $[k : \mathbf{Q}]$ in place of $[K_\mathfrak{f} : K]$. In particular,*

$$\mathfrak{f} \leqslant \max\{[k : \mathbf{Q}]^2, 7\} \quad \text{and} \quad \mathfrak{f} \leqslant 3 \cdot [k : \mathbf{Q}]^2.$$

Proof. — The theory of complex multiplication tells us that $K_\mathfrak{f} = K(j(E))$. Since E is defined over k, we have $K(j(E)) \subset Kk$. □

COROLLARY 4.5. — *Let $d \in \mathbf{Z}_{>0}$ and let K be an imaginary quadratic field. Then the number of $\mathbf{C}$-isomorphism classes of elliptic curves defined over number fields of degree at most d with (not necessarily full) CM by K is equal to*

$$\begin{aligned} &2 \text{ if } d = 1 \text{ and } K \in \{\mathbf{Q}(\sqrt{-7}), \mathbf{Q}(i)\};\\ &3 \text{ if } d = 1 \text{ and } K = \mathbf{Q}(\zeta_3);\\ &9 \text{ if } d = 2 \text{ and } K = \mathbf{Q}(\zeta_3). \end{aligned}$$

In all other cases, the number of $\mathbf{C}$-isomorphism classes of elliptic curves defined over number fields of degree at most d with (not necessarily full) CM by K is bounded above by d^3.

Proof. — Let $\mathcal{O}_\mathfrak{f}$ denote the order of conductor $\mathfrak{f}$ in $\mathcal{O}_K$. Then the theory of complex multiplication shows that the number of isomorphism classes of complex elliptic curves with CM by $\mathcal{O}_\mathfrak{f}$ is equal to the class number $h(\mathcal{O}_\mathfrak{f})$. We call a conductor $\mathfrak{f}$ *d-permissible* if there exists an elliptic curve E defined over a number field of degree at most d with $\mathrm{End}(\overline{E}) = \mathcal{O}_\mathfrak{f}$. In this case the theory of complex multiplication shows that $h(\mathcal{O}_\mathfrak{f}) = [K(j(E)) : K] \leqslant d$. The total number of $\mathbf{C}$-isomorphism classes of elliptic curves defined over number fields of degree at most d with CM by K is given by

$$\sum_{d-\text{permissible } \mathfrak{f}} h(\mathcal{O}_\mathfrak{f}) \leqslant \sum_{d-\text{permissible } \mathfrak{f}} d.$$

Corollary 4.4 and Proposition 4.1 show that in most cases if $\mathfrak{f}$ is d-permissible then $\mathfrak{f} \leqslant d^2$, which gives the desired result. The exceptional cases are

(1) $K = \mathbf{Q}(\sqrt{-7})$ and $d = 1$, in which case $\mathfrak{f} \leqslant 2$;
(2) $K = \mathbf{Q}(i)$ and $d \leqslant 2$, in which case $\mathfrak{f} \leqslant 5$;
(3) $K = \mathbf{Q}(\zeta_3)$ and $d \leqslant 2$, in which case $\mathfrak{f} \leqslant 7$.

The results for the exceptional cases listed above with $d = 1$ are well known – see [31, Appendix A §3], for example. It remains to tackle cases (2) and (3) when $d = 2$. For this, we use Corollary 4.4 and Proposition 4.1.

First we tackle case (2). The number of $\mathbf{C}$-isomorphism classes of elliptic curves defined over number fields of degree at most 2 with CM by $\mathbf{Q}(i)$ is given by

$$\sum_{\substack{\mathfrak{f} \leqslant 5 \\ 2-\text{permissible } \mathfrak{f}}} h(\mathcal{O}_{\mathfrak{f}}). \tag{4.5}$$

We calculate that $h(\mathbf{Z}[i]) = h(\mathbf{Z}[2i]) = 1$ and $h(\mathcal{O}_{\mathfrak{f}}) = 2$ for $3 \leqslant \mathfrak{f} \leqslant 5$. So $\sum_{\mathfrak{f}=1}^{5} h(\mathcal{O}_{\mathfrak{f}}) = 1 + 1 + 2 + 2 + 2 = 8 = d^3$ and so this case is compatible with the usual bound for the non-exceptional cases.

Now we tackle case (3). The number of $\mathbf{C}$-isomorphism classes of elliptic curves defined over number fields of degree at most 2 with CM by $\mathbf{Q}(\zeta_3)$ is given by

$$\sum_{\substack{\mathfrak{f} \leqslant 7 \\ 2-\text{permissible } \mathfrak{f}}} h(\mathcal{O}_{\mathfrak{f}}). \tag{4.6}$$

We calculate that $h(\mathcal{O}_{\mathfrak{f}}) = 1$ for $1 \leqslant \mathfrak{f} \leqslant 3$, $h(\mathcal{O}_{\mathfrak{f}}) = 2$ for $\mathfrak{f} \in \{4, 5, 7\}$ and $h(\mathcal{O}_6) = 3$, so 6 is not 2-permissible. Using Sage [25] for example, one can check that the other values of $\mathfrak{f}$ are all 2-permissible – there are two non-rational CM j-invariants defined over $\mathbf{Q}(\sqrt{3})$ with CM by the order of conductor 4 in $\mathbf{Z}[\zeta_3]$, for example. □

PROPOSITION 4.6. — *Let $d \in \mathbf{Z}$ with $d \geqslant 2$. Then the number of $\mathbf{C}$-isomorphism classes of elliptic curves defined over number fields of degree at most d with (not necessarily full) CM is bounded above by*

$$d^3 \cdot \#\{K \text{ imaginary quadratic} \mid h_K \leqslant d\}.$$

The number of $\mathbf{C}$-isomorphism classes of elliptic curves defined over $\mathbf{Q}$ with (not necessarily full) CM is 13.

Proof. — We say that an imaginary quadratic field K is d-permissible if there exists an elliptic curve E defined over a number field of degree at most d with $\mathrm{End}(\overline{E}) = \mathcal{O}$ for some order $\mathcal{O}$ in K. In this case, since $h_K \mid h(\mathcal{O})$ and $h(\mathcal{O}) = [K(j(E)) : K] \leqslant d$, we have $h_K \leqslant d$. The result will follow from applying Corollary 4.5 and summing over d-permissible fields K. The result for $\mathbf{Q}$ is well known. It follows from Corollary 4.5 and the fact that there are 9 imaginary quadratic fields K with class number 1. For $d \geqslant 3$, the result follows immediately from Corollary 4.5. Now suppose that $d = 2$. Corollary 4.5 shows that the contribution from $\mathbf{Q}(\zeta_3)$ is 9,

rather than $d^3 = 8$. However, this is compensated for by the fact that the contribution from $\mathbf{Q}(\sqrt{-7})$ is at most 4, as we now show. The contribution from $\mathbf{Q}(\sqrt{-7})$ is given by

$$\sum_{2-\text{permissible } \mathfrak{f}} h(\mathcal{O}_{\mathfrak{f}})$$

and if $\mathfrak{f}$ is 2-permissible then $h(\mathcal{O}_{\mathfrak{f}})$ is at most 2, whence Proposition 4.1 shows that $\mathfrak{f} \leqslant 4$. Now (4.1) gives

$$h(\mathcal{O}_{\mathfrak{f}}) = \mathfrak{f} \cdot \prod_{p|\mathfrak{f}} \left(1 - \left(\frac{-7}{p}\right)\frac{1}{p}\right)$$

whereby $h(\mathcal{O}_3) = 4$ and hence 3 is not 2-permissible. Thus, the contribution from $\mathbf{Q}(\sqrt{-7})$ is bounded above by $h(\mathcal{O}_{\mathbf{Q}(\sqrt{-7})}) + h(\mathcal{O}_2) + h(\mathcal{O}_4) = 1 + 1 + 2 = 4$. □

Remark 4.7. — In [5, Theorem 1.1], Daniels and Lozano-Robledo show that if $k/\mathbf{Q}$ is an extension of odd degree then the number of distinct CM j-invariants defined over k is at most $13 + 2\log_3([k : \mathbf{Q}])$. However, the odd degree case is very rare – in [5, Corollary 2.4] the authors show that if $K/\mathbf{Q}$ is an imaginary quadratic field with odd class number then $K = \mathbf{Q}(\sqrt{-d})$ where d is equal to $1, 2$ or a prime $q \equiv 3 \pmod 4$. For a numerical illustration of the scarcity of CM j-invariants defined over fields of odd degree compared to those defined over fields of even degree, see [5, Table 2].

THEOREM 4.8. — *For a number field k, let S_k denote the set of $\mathbf{C}$-isomorphism classes of singular K3 surfaces X such that both X and a set of generators for $\operatorname{NS}\overline{X}$ are defined over k. For $d \in \mathbf{Z}_{>0}$, let $S_d = \bigcup_{[k:\mathbf{Q}]\leqslant d} S_k$. Then*

$$\#S_d \leqslant 3 \cdot d^3 \cdot (\log(3 \cdot d^2) + 1) \cdot \#\{K \text{ imaginary quadratic} \mid h_K \leqslant d\}.$$

Proof. — Let k be a number field of degree at most d and let $X \in S_k$. The isomorphism class of $X_{\mathbf{C}}$ is determined by the isomorphism class of its transcendental lattice $T(X_{\mathbf{C}})$ (see [10, §14, Corollary 3.21]). Let $\mathfrak{c} = \operatorname{disc} T(X_{\mathbf{C}})$ and let $K = \mathbf{Q}(\sqrt{\mathfrak{c}})$. Define $\mathfrak{f} \in \mathbf{Z}_{>0}$ by letting $\mathfrak{c} = \mathfrak{f}^2 \cdot \Delta_K$. Then by [26, Theorem 2], the ring class field $K_{\mathfrak{f}}$ is contained in kK and hence $[K_{\mathfrak{f}} : K] \leqslant [kK : K] \leqslant [k : \mathbf{Q}] \leqslant d$. Now Proposition 4.1 shows that

$$\mathfrak{f} \leqslant 3[K_{\mathfrak{f}} : K]^2 \leqslant 3[k : \mathbf{Q}]^2 \leqslant 3 \cdot d^2. \tag{4.7}$$

Also, since the Hilbert class field is contained in $K_{\mathfrak{f}}$, we have $h_K \leqslant d$.

Work of Shioda and Inose in [30] shows that $T(X_{\mathbf{C}}) = T(A)$ for $A = \mathbf{C}/\mathcal{O}_{K,\mathfrak{f}} \times \mathbf{C}/\mathfrak{a}$ where $\mathcal{O}_{K,\mathfrak{f}}$ denotes the order of conductor $\mathfrak{f}$ in $\mathcal{O}_K$ and $\mathfrak{a}$

is a lattice in K with ring of multipliers $\mathcal{O}_{K,\mathfrak{f}_\mathfrak{a}}$ with $\mathfrak{f}_\mathfrak{a} \mid \mathfrak{f}$. The number of homothety classes of lattices with ring of multipliers $\mathcal{O}_{K,\mathfrak{f}_\mathfrak{a}}$ is equal to the class number $h(\mathcal{O}_{K,\mathfrak{f}_\mathfrak{a}})$. Our observations thus far show that

$$\#S_d \leqslant \sum_{\substack{K \text{ imaginary quadratic} \\ h_K \leqslant d}} \sum_{\mathfrak{f} \leqslant 3\cdot d^2} \sum_{\mathfrak{f}_\mathfrak{a} \mid \mathfrak{f}} h(\mathcal{O}_{K,\mathfrak{f}_\mathfrak{a}}). \tag{4.8}$$

Since $\mathfrak{f}_\mathfrak{a} \mid \mathfrak{f}$, we have $K_{\mathfrak{f}_\mathfrak{a}} \subset K_\mathfrak{f} \subset kK$. Therefore,

$$h(\mathcal{O}_{K,\mathfrak{f}_\mathfrak{a}}) = [K_{\mathfrak{f}_\mathfrak{a}} : K] \leqslant [k : \mathbf{Q}] \leqslant d. \tag{4.9}$$

Substituting (4.9) into (4.8) and writing τ for the number-of-divisors function gives

$$\#S_d \leqslant d \cdot \sum_{\substack{K \text{ imaginary quadratic} \\ h_K \leqslant d}} \sum_{\mathfrak{f} \leqslant 3\cdot d^2} \tau(\mathfrak{f}). \tag{4.10}$$

Now recall that $\sum_{n=1}^{M} \tau(n) = \sum_{r=1}^{M} \lfloor \frac{M}{r} \rfloor \leqslant M \sum_{r=1}^{M} \frac{1}{r} \leqslant M(\log M + 1)$. Using this in (4.10) yields

$$\#S_d \leqslant 3 \cdot d^3 \cdot (\log(3 \cdot d^2) + 1) \cdot \#\{K \text{ imaginary quadratic} \mid h_K \leqslant d\}. \quad \square$$

COROLLARY 4.9. — *The number of* $\mathbf{C}$*-isomorphism classes of singular K3 surfaces defined over number fields of degree at most* d *is bounded above by*

$$3 \cdot M(20)^3 \cdot d^3 \cdot (\log(3 \cdot M(20)^2 \cdot d^2) + 1) \cdot \#\{K \text{ imaginary quadratic} \mid h_K \leqslant M(20) \cdot d\}.$$

Proof. — Let X be a singular K3 surface defined over a number field k. Recall that $\mathrm{NS}\,\overline{X} = \mathrm{Pic}\,\overline{X}$ is a free $\mathbf{Z}$-module of rank 20 whose generators are all defined over some finite extension of k. Since the order of any finite subgroup of $\mathrm{GL}_{20}(\mathbf{Z})$ divides $M(20)$, the Galois representation $\rho : \Gamma_k \to \mathrm{Aut}\,\mathrm{NS}\,\overline{X} \hookrightarrow \mathrm{GL}_{20}(\mathbf{Z})$ factors through $\mathrm{Gal}(k_0/k)$ for a Galois extension k_0/k of degree at most $M(20)$. Now apply Theorem 4.8 to X_{k_0}. $\square$

5. The transcendental part of the Brauer group of the self-product of a CM elliptic curve

In this section, we obtain uniform bounds for the transcendental part of the Brauer group of $E \times E$, where E is an elliptic curve over a number field. The key result that we will use to compute the transcendental part of the Brauer group of a product of elliptic curves is the following:

THEOREM 5.1 (Skorobogatov–Zarhin, [34, Proposition 3.3]). — *Let E and E' be elliptic curves over a field k of characteristic 0 and let $n \in \mathbf{Z}_{>0}$. Then there is a canonical isomorphism of abelian groups*

$$\frac{\mathrm{Br}(E \times E')[n]}{\mathrm{Br}_1(E \times E')[n]} \cong \frac{\mathrm{Hom}_{\Gamma_k}(E[n], E'[n])}{(\mathrm{Hom}(\overline{E}, \overline{E'}) \otimes \mathbf{Z}/n\mathbf{Z})^{\Gamma_k}}.$$

We will apply this result in the case where $E = E'$. The special case where E has full CM was addressed in [21]. The following definition is needed for the description of the ℓ-primary part of $\mathrm{Br}(E \times E)/\mathrm{Br}_1(E \times E)$ in Theorem 5.3 below.

DEFINITION 5.2 ([21, Definition 1]). — *Let E be an elliptic curve over a number field k with CM by the ring of integers of an imaginary quadratic field K. For a prime number $\ell \in \mathbf{Z}_{>0}$, define $m_\ell(E)$ to be the largest integer n such that for all primes $\mathfrak{q}$ of kK that are of good reduction for E and coprime to ℓ, the Grössencharakter $\psi_{E/kK}$ satisfies*

$$\psi_{E/kK}(\mathfrak{q}) \in \mathcal{O}_{K,\ell^n},$$

where $\mathcal{O}_{K,\ell^n}$ denotes the order in $\mathcal{O}_K$ of conductor ℓ^n.

THEOREM 5.3 (Newton). — *Let E be an elliptic curve over a number field k with CM by the ring of integers of an imaginary quadratic field K, let ℓ be a prime number and let $m := m_\ell(E)$ be as defined in Definition 5.2. Then*

(5.1)

$$\frac{\mathrm{Br}(E \times E)}{\mathrm{Br}_1(E \times E)}\{\ell\} \cong \begin{cases} \left(\mathbf{Z}/\ell^m\mathbf{Z}\right)^2 & \text{if } K \subset k, \\ \mathbf{Z}/2^m\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} & \text{if } K \not\subset k, \ell = 2 \text{ and } E[2] = E[2](k), \\ \mathbf{Z}/\ell^m\mathbf{Z} & \text{otherwise.} \end{cases}$$

Proof. — See [21, Theorems 2.5 and 2.9]. □

Remark 5.4. — Since the Grössencharakter determines the action of Γ_{kK} on $E[2]$, we note that $E[2] = E[2](k)$ implies $m_2(E) \geqslant 1$. If $K \not\subset k$, then $E[2] = E[2](k)$ also implies $2 \mid \Delta_K$. This is seen by taking a basis $\left\{P, \left(\frac{\Delta_K + \sqrt{\Delta_K}}{2}\right)P\right\}$ for $E[2]$ and considering the action of complex conjugation.

In order to use Theorem 5.3 to obtain uniform bounds on the size of the transcendental part of the Brauer group of $E \times E$, we need to bound $\prod_{\ell \text{ prime}} \ell^{m_\ell(E)}$ in terms of the degree of the field of definition of E. This is achieved by the following lemma in combination with Proposition 4.1.

LEMMA 5.5. — *Let k be a number field. Let E be a CM elliptic curve over k with $\mathrm{End}(\overline{E}) = \mathcal{O}_K$ for some imaginary quadratic field $K/\mathbf{Q}$. Let $m_\ell := m_\ell(E)$ be as in Definition 5.2. Let $\mathfrak{c} := \prod_{\ell \text{ prime}} \ell^{m_\ell}$ and let $K_\mathfrak{c}$ denote the ring class field associated to $\mathcal{O}_\mathfrak{c}$. Then*

$$K_\mathfrak{c} \subset kK.$$

Proof. — Let $\mathfrak{q}$ be a finite prime of kK of good reduction for E and coprime to $\mathfrak{c}$. We will show that $\mathfrak{q}$ splits completely in $kK_\mathfrak{c}/kK$. Then [3, Exercise 6.1] will allow us to conclude that $K_\mathfrak{c} \subset kK$, as desired.

Recall that, given an abelian extension of number fields M/F and a prime ideal $\mathfrak{r}$ of $\mathcal{O}_F$ that is unramified in M/F, the Artin symbol $(\mathfrak{r}, M/F)$ is the unique element $\sigma \in \mathrm{Gal}(M/F)$ such that, for all $\alpha \in \mathcal{O}_M$,

$$\sigma(\alpha) \equiv \alpha^{N_{F/\mathbf{Q}}(\mathfrak{r})} \pmod{\mathfrak{s}}$$

where $\mathfrak{s}$ is a prime of M above $\mathfrak{r}$. Showing that $\mathfrak{q}$ splits completely in $kK_\mathfrak{c}/kK$ is equivalent to showing that $(\mathfrak{q}, kK_\mathfrak{c}/kK) = 1$. It will suffice to show that the restriction $(\mathfrak{q}, kK_\mathfrak{c}/kK)|_{K_\mathfrak{c}} \in \mathrm{Gal}(K_\mathfrak{c}/K)$ is trivial. Let $N_{kK/K}(\mathfrak{q}) = \mathfrak{p}^{f_{\mathfrak{q}/\mathfrak{p}}}$, where $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$ and $f_{\mathfrak{q}/\mathfrak{p}} = [\mathcal{O}_{kK}/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p}]$. Then $N_{kK/\mathbf{Q}}(\mathfrak{q}) = N_{K/\mathbf{Q}}(\mathfrak{p})^{f_{\mathfrak{q}/\mathfrak{p}}}$. We have

$$(\mathfrak{q}, kK_\mathfrak{c}/kK)|_{K_\mathfrak{c}} = (\mathfrak{p}, K_\mathfrak{c}/K)^{f_{\mathfrak{q}/\mathfrak{p}}} = (\mathfrak{p}^{f_{\mathfrak{q}/\mathfrak{p}}}, K_\mathfrak{c}/K). \tag{5.2}$$

By [31, Theorems II.9.1 and II.9.2], the value $\psi_{E/kK}(\mathfrak{q})$ of the Grössencharakter at $\mathfrak{q}$ generates the principal ideal $N_{kK/K}(\mathfrak{q}) = \mathfrak{p}^{f_{\mathfrak{q}/\mathfrak{p}}}$. By definition of m_ℓ, we have $\psi_{E/kK}(\mathfrak{q}) \in \mathcal{O}_{\ell^{m_\ell}} = \mathbf{Z} + \ell^{m_\ell}\mathcal{O}_K$ for all prime numbers ℓ. Thus, $\psi_{E/kK}(\mathfrak{q}) \in \bigcap_\ell \mathcal{O}_{\ell^{m_\ell}} = \mathcal{O}_\mathfrak{c} = \mathbf{Z} + \mathfrak{c}\mathcal{O}_K$. By definition of the ring class field $K_\mathfrak{c}$, this implies that $(\mathfrak{p}^{f_{\mathfrak{q}/\mathfrak{p}}}, K_\mathfrak{c}/K) = ((\psi_{E/kK}(\mathfrak{q})), K_\mathfrak{c}/K) = 1$, as required. □

Now we deal with the more general case where the elliptic curve E has CM by an order in the ring of integers of an imaginary quadratic field. In the next lemma we compute $(\mathrm{End}(\overline{E}) \otimes \mathbf{Z}/n\mathbf{Z})^{\Gamma_k}$.

LEMMA 5.6. — *Let E be an elliptic curve over a field k of characteristic 0, with CM by an order of conductor $\mathfrak{f}$ in an imaginary quadratic field K. Let $n \in \mathbf{Z}_{>0}$.*

(1) *If $K \subset k$ then $(\mathrm{End}(\overline{E}) \otimes \mathbf{Z}/n\mathbf{Z})^{\Gamma_k} = \mathrm{End}(\overline{E}) \otimes \mathbf{Z}/n\mathbf{Z} \cong (\mathbf{Z}/n\mathbf{Z})^2$.*
(2) *If $K \not\subset k$ then*

$$(\mathrm{End}(\overline{E}) \otimes \mathbf{Z}/n\mathbf{Z})^{\Gamma_k} \cong \begin{cases} \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} & \text{if } 2 \mid \mathfrak{f} \cdot \Delta_K \text{ and } 2 \mid n; \\ \mathbf{Z}/n\mathbf{Z} & \text{otherwise.} \end{cases}$$

Proof. — If $K \subset k$, then Γ_k acts trivially on $\mathrm{End}(\overline{E})$, and (1) follows immediately. It remains to prove (2). Henceforth, we assume that $K = \mathbf{Q}(\sqrt{-d}) \not\subset k$.

First suppose that $2 \nmid \Delta_K$. Then any $\phi \in \mathrm{End}(\overline{E})$ is of the form $a + b\mathfrak{f}(\frac{1+\sqrt{-d}}{2})$ for some $a, b, \in \mathbf{Z}$, and a simple calculation shows that the image of ϕ in $\mathrm{End}(\overline{E}) \otimes \mathbf{Z}/n\mathbf{Z}$ is fixed by Γ_k if and only if $2b \equiv \mathfrak{f}b \equiv 0 \pmod{n}$. If either $\mathfrak{f}$ or n is odd then these congruences imply that $b \equiv 0 \pmod{n}$ and hence $(\mathrm{End}(\overline{E}) \otimes \mathbf{Z}/n\mathbf{Z})^{\Gamma_k} \cong \mathbf{Z}/n\mathbf{Z}$. If both $\mathfrak{f}$ and n are even then the two congruences simply reduce to $2b \equiv 0 \pmod{n}$ and $(\mathrm{End}(\overline{E}) \otimes \mathbf{Z}/n\mathbf{Z})^{\Gamma_k} \cong \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, as claimed.

Now suppose that $2 \mid \Delta_K$. Then any $\phi \in \mathrm{End}(\overline{E})$ is of the form $a + b\mathfrak{f}\sqrt{-d}$ for some $a, b, \mathfrak{f} \in \mathbf{Z}$, and the image of ϕ in $\mathrm{End}(\overline{E}) \otimes \mathbf{Z}/n\mathbf{Z}$ is fixed by Γ_k if and only if $2b \equiv 0 \pmod{n}$. This yields the desired result. □

To make use of Theorem 5.1, we must also analyse $\mathrm{End}_{\Gamma_k}(E[n])$. For this we use some ideas from [41] and [42]. Let n be a positive integer and let E be an elliptic curve over a field k of characteristic 0. Let

$$\rho_{E,n} : \Gamma_k \to \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$$

denote the Galois representation coming from the action of Galois on the n-torsion of E.

Definition 5.7 ([42, Definition A.1]). — *Let n be a positive integer. A subgroup H of $\mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$ is liftable abelian if there exists an abelian subgroup $\widehat{H} < \mathrm{GL}_2(\widehat{\mathbf{Z}})$ such that $\widehat{H}$ surjects onto H under the natural quotient map $\mathrm{GL}_2(\widehat{\mathbf{Z}}) \to \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$. (In particular, a liftable abelian subgroup is abelian.)*

Proposition 5.8 ([42, Corollary A.4]). — *Let E be an elliptic curve over a field k of characteristic 0 and let $n \in \mathbf{Z}_{>0}$. Then we have an isomorphism of abelian groups*

$$\mathrm{End}_{\Gamma_k}(E[n]) \cong \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/s_{E,n}\mathbf{Z} \times (\mathbf{Z}/t_{E,n}\mathbf{Z})^2$$

for positive integers $t_{E,n} \mid s_{E,n} \mid n$. Furthermore, $s_{E,n}$ is the largest integer s dividing n such that $\mathrm{Gal}(k(E[s])/k)$ is liftable abelian and $t_{E,n}$ is the largest integer t dividing n such that $\mathrm{Gal}(k(E[t])/k) \subset (\mathbf{Z}/t\mathbf{Z})^\times$ where $a \in (\mathbf{Z}/t\mathbf{Z})^\times$ acts by $P \mapsto aP$.

Remark 5.9. — An example where $\mathrm{im}\,\rho_{E,n}$ is abelian but not liftable abelian is as follows. Take $k = \mathbf{Q}(\sqrt{2})$ and let E/k be the elliptic curve 64.1-a3 in the LMFDB tables (see [17, Elliptic Curve 64.1-a3]) with CM by $\mathbf{Z}[\sqrt{-2}]$. Choose a basis of the form $P, \sqrt{-2}P$ for $E[4]$. With respect to

such a basis, one can calculate using the methods of [21] that the $\mathbf{Z}/4\mathbf{Z}$-submodule of $\mathrm{End}(E[4])$ generated by $\operatorname{im}\rho_{E,4}$ is equal to the $\mathbf{Z}/4\mathbf{Z}$-span of I, $\left(\begin{smallmatrix}2&0\\0&0\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}0&0\\2&0\end{smallmatrix}\right)$. Thus, $\operatorname{im}\rho_{E,4}$ is abelian but [42, Lemma A.7] shows that it is not liftable abelian.

LEMMA 5.10. — *Let E and E' be elliptic curves over a field k of characteristic 0 and let $\varphi : E \to E'$ be an isogeny of degree d defined over k. Then for all primes ℓ and all $n \in \mathbf{Z}_{\geqslant 0}$, φ induces a Galois-equivariant surjection*

$$\varphi : E[\ell^{n+\mathrm{ord}_\ell d}] \twoheadrightarrow E'[\ell^n]$$

and hence a surjection

$$\mathrm{Gal}(k(E[\ell^{n+\mathrm{ord}_\ell d}])/k) \twoheadrightarrow \mathrm{Gal}(k(E'[\ell^n])/k).$$

Proof. — Let $P' \in E'[\ell^n]$. Then $P' = \varphi(P)$ for some $P \in E(\overline{k})$. Since

$$[\ell^n]P' = ([\ell^n] \circ \varphi)(P) = (\varphi \circ [\ell^n])(P),$$

we have $[\ell^n]P \in \ker(\varphi)$. Writing $\hat{\varphi}$ for the dual isogeny, we have

$$[d\ell^n]P = (\hat{\varphi} \circ \varphi)([\ell^n]P) = 0.$$

Therefore, $P = P_1 + P_2$ for some $P_1 \in E[\ell^{n+\mathrm{ord}_\ell d}]$ and $P_2 \in E[\frac{d}{\ell^{\mathrm{ord}_\ell d}}]$. Since $\varphi(P_1)$ is a point of E' with order a power of ℓ, the same is true for $\varphi(P_2) = P' - \varphi(P_1)$. Since $P_2 \in E[\frac{d}{\ell^{\mathrm{ord}_\ell d}}]$, and $\ell \nmid \frac{d}{\ell^{\mathrm{ord}_\ell d}}$, we deduce that $\varphi(P_2) = 0$, and hence $P' = \varphi(P_1)$. This proves the existence of the first surjection. Since φ is defined over k, it is Galois equivariant, whence the second surjection. □

The following fact is well known, but we give a proof here since we were unable to find one in the literature.

LEMMA 5.11. — *Let k be a field of characteristic 0. Let E be an elliptic curve over k with CM by an order $\mathcal{O}$ of conductor $\mathfrak{f}$ in an imaginary quadratic field K. Then there exists a cyclic k-isogeny $\varphi : E \to E'$ of degree $\mathfrak{f}$, where E' is an elliptic curve over k with CM by $\mathcal{O}_K$.*

Proof. — The complex elliptic curve $E_{\mathbf{C}}$ corresponds to $\mathbf{C}/L$ for some lattice L. Since E has CM by $\mathcal{O}$, the lattice L is homothetic to $\mathfrak{b}$ for some invertible $\mathcal{O}$-ideal $\mathfrak{b}$. In other words $L = \lambda\mathfrak{b}$ for some $\lambda \in \mathbf{C}^\times$. Now the natural surjection $\mathbf{C}/\lambda\mathfrak{b} \twoheadrightarrow \mathbf{C}/\lambda\mathfrak{b}\mathcal{O}_K$ corresponds to a cyclic $\mathbf{C}$-isogeny $\varphi : E_{\mathbf{C}} \to E'_{\mathbf{C}}$ where $E'_{\mathbf{C}}$ has CM by $\mathcal{O}_K$. Moreover, $\deg\varphi = [\lambda\mathfrak{b}\mathcal{O}_K : \lambda\mathfrak{b}] = [\mathcal{O}_K : \mathcal{O}] = \mathfrak{f}$.

Now let L' be an arbitrary lattice containing $\lambda\mathfrak{b}$ as a sublattice of index $\mathfrak{f}$ such that $\{z \in \mathbf{C} \mid zL' \subset L'\} = \mathcal{O}_K$. Any such lattice corresponds to an elliptic curve $E''_{\mathbf{C}}$ with CM by $\mathcal{O}_K$ and with a $\mathbf{C}$-isogeny $E_{\mathbf{C}} \to E''_{\mathbf{C}}$ of degree

$\mathfrak{f}$. Now $\lambda^{-1}\mathfrak{b}^{-1}L'$ contains $\mathcal{O}$ as a sublattice of index $\mathfrak{f}$. Furthermore, since $\{z \in \mathbf{C} \mid zL' \subset L'\} = \mathcal{O}_K$, we know that L' is homothetic to an invertible $\mathcal{O}_K$-ideal. Therefore, we can write $\lambda^{-1}\mathfrak{b}^{-1}L' = \mu\mathfrak{a}$ for some invertible $\mathcal{O}_K$-ideal $\mathfrak{a}$ and some $\mu \in \mathbf{C}^\times$. Since $1 \in \mathcal{O} \subset \mu\mathfrak{a}$, we have $\mu = a^{-1}$ for some $a \in \mathfrak{a}$. Writing out $[a^{-1}\mathcal{O}_K : \mathcal{O}]$ in two different ways gives

$$[a^{-1}\mathcal{O}_K : \mathcal{O}_K][\mathcal{O}_K : \mathcal{O}] = [a^{-1}\mathcal{O}_K : a^{-1}\mathfrak{a}][a^{-1}\mathfrak{a} : \mathcal{O}].$$

Since $[a^{-1}\mathfrak{a} : \mathcal{O}] = [\lambda^{-1}\mathfrak{b}^{-1}L' : \mathcal{O}] = \mathfrak{f} = [\mathcal{O}_K : \mathcal{O}]$ we obtain

$$[a^{-1}\mathcal{O}_K : \mathcal{O}_K] = [a^{-1}\mathcal{O}_K : a^{-1}\mathfrak{a}].$$

Therefore $\lambda^{-1}\mathfrak{b}^{-1}L' = a^{-1}\mathfrak{a} = \mathcal{O}_K$ and hence $L' = \lambda\mathfrak{b}\mathcal{O}_K$. Thus any $\mathbf{C}$-isogeny of degree $\mathfrak{f}$ to an elliptic curve with CM by $\mathcal{O}_K$ has the same kernel as φ. In particular, noting that any $\mathbf{C}$-isogeny is actually already defined over $\overline{k}$, if $\sigma \in \Gamma_k$ then $\sigma \circ \varphi \circ \sigma^{-1}$ gives a $\mathbf{C}$-isogeny of degree $\mathfrak{f}$ to an elliptic curve with CM by $\mathcal{O}_K$. Its kernel is $\sigma(\ker\varphi)$. Hence, by the argument above, $\sigma(\ker\varphi) = \ker\varphi$. Since this is true for any $\sigma \in \Gamma_k$, we deduce that $\ker\varphi$ is defined over k. Now the natural surjection $E \to E/\ker\varphi$ is our desired k-isogeny. □

COROLLARY 5.12. — *Let k be a field of characteristic 0. Let E be an elliptic curve over k with CM by an order of conductor $\mathfrak{f}$ in an imaginary quadratic field K. Let $\varphi : E \to E'$ be an isogeny of degree $\mathfrak{f}$ to an elliptic curve with CM by $\mathcal{O}_K$ as in Lemma 5.11. Let ℓ be a prime and let $n \in \mathbf{Z}_{\geqslant 0}$. Then*

$$s_{E,\ell^{n+\mathrm{ord}_\ell\mathfrak{f}}} \leqslant \ell^{\mathrm{ord}_\ell\mathfrak{f}} \cdot s_{E',\ell^n} \text{ and } t_{E,\ell^{n+\mathrm{ord}_\ell\mathfrak{f}}} \leqslant \ell^{\mathrm{ord}_\ell\mathfrak{f}} \cdot t_{E',\ell^n}.$$

Proof. — This follows from Lemma 5.10. □

We will use the following well-known fact several times in the proof of Theorem 5.13 below. Let E, E' be elliptic curves over a number field. Then

$$\mathrm{Br}(\overline{E} \times \overline{E'}) \cong (\mathbf{Q}/\mathbf{Z})^{6-\rho} \tag{5.3}$$

where $\rho = \operatorname{rank}\mathrm{NS}(\overline{E} \times \overline{E'})$. This follows from work of Grothendieck.

THEOREM 5.13. — *Let E be an elliptic curve over a number field k with CM by an order of conductor $\mathfrak{f}$ in an imaginary quadratic field K. Let $\varphi : E \to E'$ be an isogeny of degree $\mathfrak{f}$ to an elliptic curve with CM by $\mathcal{O}_K$ as in Lemma 5.11. Let ℓ be a prime.*

(1) *If $K \subset k$, then*

$$\frac{\mathrm{Br}(E \times E)}{\mathrm{Br}_1(E \times E)}\{\ell\} \cong (\mathbf{Z}/\ell^a\mathbf{Z})^2$$

for some $a \leqslant m_\ell(E') + \mathrm{ord}_\ell\mathfrak{f}$.

(2) *If $K \not\subset k$, then*

$$\frac{\mathrm{Br}(E \times E)}{\mathrm{Br}_1(E \times E)}\{\ell\} \cong \mathbf{Z}/\ell^a\mathbf{Z}$$

for some $a \leqslant m_\ell(E') + \mathrm{ord}_\ell \mathfrak{f}$, unless $\ell = 2$ and $E[2] = E[2](k)$, in which case

$$\frac{\mathrm{Br}(E \times E)}{\mathrm{Br}_1(E \times E)}\{2\} \cong \mathbf{Z}/2^a\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$$

for some $a \leqslant m_2(E') + \mathrm{ord}_2 \mathfrak{f} + 1$. In fact, $a \leqslant m_2(E') + \mathrm{ord}_2 \mathfrak{f}$ unless $2 \mid \Delta_K$ and $E'[2] \neq E'[2](k)$.

Remark 5.14. — Note that if $K \not\subset k$, then $E[2] = E[2](k)$ implies that $2 \mid \mathfrak{f} \cdot \Delta_K$. This is seen by considering the action of complex conjugation on $E[2]$, as in Remark 5.4. Furthermore, if $2 \nmid \mathfrak{f}$ then Lemma 5.10 shows that $E[2] = E[2](k)$ if and only if $E'[2] = E'[2](k)$.

Proof of Theorem 5.13. — By [21, Lemma 2.1], we have

$$\frac{\mathrm{Br}(E \times E)}{\mathrm{Br}_1(E \times E)}\{\ell\} = \frac{\mathrm{Br}(E \times E)\{\ell\}}{\mathrm{Br}_1(E \times E)\{\ell\}}.$$

Let $n \in \mathbf{Z}_{\geqslant 0}$ and apply Theorem 5.1 to $E \times E$. Let $m = m_\ell(E')$.

(1). — If $K \subset k$ then Lemma 5.6 and Proposition 5.8 give

$$\frac{\mathrm{End}_{\Gamma_k}(E[\ell^n])}{(\mathrm{End}(\overline{E}) \otimes \mathbf{Z}/\ell^n\mathbf{Z})^{\Gamma_k}} \cong (\mathbf{Z}/t_{E,\ell^n}\mathbf{Z})^2.$$

To see this, apply Proposition 5.8 to get

$$\mathrm{End}_{\Gamma_k}(E[\ell^n]) \cong \mathbf{Z}/\ell^n\mathbf{Z} \times \mathbf{Z}/s_{E,\ell^n}\mathbf{Z} \times (\mathbf{Z}/t_{E,\ell^n}\mathbf{Z})^2.$$

Now, by Lemma 5.6, we have

$$(\mathrm{End}(\overline{E}) \otimes \mathbf{Z}/\ell^n\mathbf{Z})^{\Gamma_k} \cong (\mathbf{Z}/\ell^n\mathbf{Z})^2 \subset \mathrm{End}_{\Gamma_k}(E[\ell^n]).$$

Since $t_{E,\ell^n} \mid s_{E,\ell^n} \mid \ell^n$, it follows that $s_{E,\ell^n} = \ell^n$, whence the claim.

Our task is now to bound t_{E,ℓ^n} for n large. By Corollary 5.12 it suffices to show that, for all $r \in \mathbf{Z}_{\geqslant 0}$, $t_{E',\ell^r} \leqslant \ell^m$. This follows from Lemma 5.6, Proposition 5.8 and Theorem 5.3 applied to E'.

(2). — If $K \not\subset k$ and at least one of $\ell, \mathfrak{f} \cdot \Delta_K$ is odd then Lemma 5.6 and Proposition 5.8 give

$$\frac{\mathrm{End}_{\Gamma_k}(E[\ell^n])}{(\mathrm{End}(\overline{E}) \otimes \mathbf{Z}/\ell^n\mathbf{Z})^{\Gamma_k}} \cong \mathbf{Z}/s_{E,\ell^n}\mathbf{Z} \times (\mathbf{Z}/t_{E,\ell^n}\mathbf{Z})^2.$$

By (5.3), $\mathrm{Br}(E \times E)/\mathrm{Br}_1(E \times E)$ is an abelian group of rank at most 2. Therefore, $t_{E,\ell^n} = 1$. It remains to bound s_{E,ℓ^n} for n large. By Corollary 5.12 it suffices to show that, for all $r \in \mathbf{Z}_{\geqslant 0}$, we have $s_{E',\ell^r} \leqslant \ell^m$. This

follows from Lemma 5.6, Proposition 5.8, Theorem 5.3 and Remark 5.4 applied to E'.

From now on, we assume that $K \not\subset k$, $\ell = 2$ and $2 \mid \mathfrak{f} \cdot \Delta_K$. So Lemma 5.6 and Proposition 5.8 give

$$\frac{\mathrm{End}_{\Gamma_k}(E[2^n])}{(\mathrm{End}(\overline{E}) \otimes \mathbf{Z}/2^n\mathbf{Z})^{\Gamma_k}} \cong \frac{\mathbf{Z}/s_{E,2^n}\mathbf{Z} \times (\mathbf{Z}/t_{E,2^n}\mathbf{Z})^2}{\mathbf{Z}/2\mathbf{Z}}.$$

Since $\mathrm{Br}(E \times E)/\mathrm{Br}_1(E \times E)$ has rank at most 2 we find that $t_{E,2^n} \leqslant 2$.

First suppose that $E[2] \neq E[2](k)$. Then $t_{E,2^n} = 1$ for all $n \geqslant 0$ and hence

$$\frac{\mathrm{End}_{\Gamma_k}(E[2^n])}{(\mathrm{End}(\overline{E}) \otimes \mathbf{Z}/2^n\mathbf{Z})^{\Gamma_k}} \cong \frac{\mathbf{Z}/s_{E,2^n}\mathbf{Z}}{\mathbf{Z}/2\mathbf{Z}} \cong \frac{\mathbf{Z}}{(s_{E,2^n}/2)\mathbf{Z}}.$$

Now Lemma 5.6, Proposition 5.8 and Theorem 5.3 applied to E' show that, for all $r \in \mathbf{Z}_{\geqslant 0}$, we have $s_{E',2^r} \leqslant 2^{m+1}$. Hence, Corollary 5.12 shows that, for all $r \in \mathbf{Z}_{\geqslant 0}$, we have $s_{E,2^{r+\mathrm{ord}_2\,\mathfrak{f}}} \leqslant 2^{m+1+\mathrm{ord}_2\,\mathfrak{f}}$. Therefore, for large n we have $s_{E,2^n}/2 \leqslant 2^{m+\mathrm{ord}_2\,\mathfrak{f}}$, as required.

Now suppose that $E[2] = E[2](k)$, i.e. $k(E[2]) = k$. Then, by definition of $t_{E,2^n}$, we have $t_{E,2^n} \geqslant 2$ for all $n \geqslant 1$. We already saw above that $t_{E,2^n} \leqslant 2$. Hence $t_{E,2^n} = 2$ and

$$\frac{\mathrm{End}_{\Gamma_k}(E[2^n])}{(\mathrm{End}(\overline{E}) \otimes \mathbf{Z}/2^n\mathbf{Z})^{\Gamma_k}} \cong \frac{\mathbf{Z}/s_{E,2^n}\mathbf{Z} \times (\mathbf{Z}/2\mathbf{Z})^2}{\mathbf{Z}/2\mathbf{Z}}.$$

Again, since $\mathrm{Br}(E \times E)/\mathrm{Br}_1(E \times E)$ has rank at most 2 we find that

$$\frac{\mathrm{End}_{\Gamma_k}(E[2^n])}{(\mathrm{End}(\overline{E}) \otimes \mathbf{Z}/2^n\mathbf{Z})^{\Gamma_k}} \cong \mathbf{Z}/s_{E,2^n}\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}.$$

By Corollary 5.12, for all $r \in \mathbf{Z}_{\geqslant 0}$, we have $s_{E,2^{r+\mathrm{ord}_2\,\mathfrak{f}}} \leqslant 2^{\mathrm{ord}_2\,\mathfrak{f}} \cdot s_{E',2^r}$. For large n, it follows from Lemma 5.6, Proposition 5.8 and Theorem 5.3 applied to E' that $s_{E',2^n} \leqslant 2^{m+1}$. When performing this calculation, one observes that the upper bound on $s_{E',2^n}$ can only be achieved if $2 \mid \Delta_K$ and $t_{E',2^n} = 1$. The latter condition is equivalent to $E'[2] \neq E'[2](k)$. □

Corollary 5.15. — *Let E be an elliptic curve over a number field k with CM by an order of conductor $\mathfrak{f}$ in an imaginary quadratic field K. Then*

$$\#\frac{\mathrm{Br}(E \times E)}{\mathrm{Br}_1(E \times E)} \mid 2 \cdot \mathfrak{f}^2 \cdot [k : \mathbf{Q}]^4 \cdot \prod_{\substack{\ell \text{ prime},\ \ell \nmid [k:\mathbf{Q}] \\ \left(\ell - \left(\frac{\Delta_K}{\ell}\right)\right) \mid [\mathcal{O}_K^\times : \mathcal{O}_\ell^\times] \cdot [k:\mathbf{Q}]}} \ell^2. \tag{5.4}$$

If $[k : \mathbf{Q}] \geqslant 2$ then

$$\#\frac{\mathrm{Br}(E \times E)}{\mathrm{Br}_1(E \times E)} \leqslant \mathfrak{f}^2 \cdot [k : \mathbf{Q}]^4. \tag{5.5}$$

Remark 5.16. — Note that $[\mathcal{O}_K^\times : \mathcal{O}_\ell^\times]$ divides 6. Therefore 6 could be used in place of $[\mathcal{O}_K^\times : \mathcal{O}_\ell^\times]$ in (5.4).

Proof of Corollary 5.15. — We begin by proving (5.5). Let $\varphi : E \to E'$ be an isogeny of degree $\mathfrak{f}$ to an elliptic curve with CM by $\mathcal{O}_K$ as in Lemma 5.11. Let $m_\ell := m_\ell(E')$ and let $\mathfrak{c} := \prod_{\ell \text{ prime}} \ell^{m_\ell}$. First we consider the case where $K \subset k$. Then taking a product over all primes in Theorem 5.13 gives

$$\#\frac{\mathrm{Br}(E \times E)}{\mathrm{Br}_1(E \times E)} \mid \mathfrak{f}^2 \cdot \mathfrak{c}^2. \tag{5.6}$$

By Lemma 5.5 we have $K_\mathfrak{c} \subset kK = k$ and hence $2 \cdot [K_\mathfrak{c} : K] \leqslant [k : \mathbf{Q}]$. Now Proposition 4.1 gives

$$\mathfrak{c} \leqslant 3 \cdot [K_\mathfrak{c} : K]^2 < [k : \mathbf{Q}]^2,$$

which gives the desired upper bound in this case.

Now we assume that $K \not\subset k$. Taking a product over all primes in Theorem 5.13 gives

$$\#\frac{\mathrm{Br}(E \times E)}{\mathrm{Br}_1(E \times E)} \mid 4 \cdot \mathfrak{f} \cdot \mathfrak{c}. \tag{5.7}$$

For $K \notin \{\mathbf{Q}(i), \mathbf{Q}(\zeta_3)\}$, Proposition 4.1 gives

$$\mathfrak{c} \leqslant [k : \mathbf{Q}]^2, \tag{5.8}$$

since $K_\mathfrak{c} \subset kK$ by Lemma 5.5. (Note that (5.8) holds for $K = \mathbf{Q}(\sqrt{-7})$ since $[k : \mathbf{Q}] \geqslant 2$.) Now the desired upper bound follows by noting that $4 \cdot \mathfrak{f} \cdot [k : \mathbf{Q}]^2 \leqslant \mathfrak{f} \cdot [k : \mathbf{Q}]^4$ when $[k : \mathbf{Q}] \geqslant 2$. For $K = \mathbf{Q}(\zeta_3)$, Theorem 5.13 and Remark 5.14 yield

$$\#\frac{\mathrm{Br}(E \times E)}{\mathrm{Br}_1(E \times E)} \mid \mathfrak{f}^2 \cdot \mathfrak{c} \tag{5.9}$$

and Proposition 4.1 gives $\mathfrak{c} \leqslant 3 \cdot [K_\mathfrak{c} : K]^2 \leqslant 3 \cdot [k : \mathbf{Q}]^2 < [k : \mathbf{Q}]^4$. For $K = \mathbf{Q}(i)$, Proposition 4.1 shows that the only possible value of $\mathfrak{c}$ violating the desired bound $\mathfrak{c} \leqslant [k : \mathbf{Q}]^2$ is $\mathfrak{c} = 5$. But if $\mathfrak{c} = 5$ then Theorem 5.13 and Remark 5.14 give

$$\#\frac{\mathrm{Br}(E \times E)}{\mathrm{Br}_1(E \times E)} \mid 2 \cdot \mathfrak{f}^2 \cdot \mathfrak{c} = 10 \cdot \mathfrak{f}^2 < \mathfrak{f}^2 \cdot [k : \mathbf{Q}]^4. \tag{5.10}$$

This completes the proof of (5.5).

For the divisibility statement (5.4), we first claim that if $m_\ell \geqslant 1$ then $\ell^{m_\ell - 1} \mid [k : \mathbf{Q}]$. We have $K_{\ell^{m_\ell}} \subset K_{\mathfrak{c}} \subset kK$ so $[K_{\ell^{m_\ell}} : K] \mid [k : \mathbf{Q}]$. By (4.1),

$$\begin{aligned}[K_{\ell^{m_\ell}} : K] &= \ell^{m_\ell - 1} \cdot \frac{h_K}{[\mathcal{O}_K^\times : \mathcal{O}_{\ell^{m_\ell}}^\times]} \cdot \left(\ell - \left(\frac{\Delta_K}{\ell}\right)\right) \\ &= \ell^{m_\ell - 1} \cdot [K_\ell : K],\end{aligned}$$

because $\mathcal{O}_{\ell^n}^\times = \{\pm 1\}$ for all $n \geqslant 1$. Thus, $\ell^{m_\ell - 1} \mid [K_{\ell^{m_\ell}} : K]$, proving the claim.

Now if $m_\ell \geqslant 2$ then $\ell^{m_\ell} \mid \ell^{2(m_\ell - 1)} \mid [k : \mathbf{Q}]^2$. It remains to deal with the primes ℓ for which $m_\ell = 1$. By (4.1) we have

$$[K_\ell : K] \cdot [\mathcal{O}_K^\times : \mathcal{O}_\ell^\times] = h_K \cdot \left(\ell - \left(\frac{\Delta_K}{\ell}\right)\right).$$

Therefore,

$$\mathfrak{c} \mid [k : \mathbf{Q}]^2 \cdot \prod_{\substack{\ell \text{ prime},\ \ell \nmid [k:\mathbf{Q}] \\ \left(\ell - \left(\frac{\Delta_K}{\ell}\right)\right) \mid [\mathcal{O}_K^\times : \mathcal{O}_\ell^\times] \cdot [k:\mathbf{Q}]}} \ell.$$

Now observe that in all cases Theorem 5.13 and Remark 5.14 imply that

$$\# \frac{\mathrm{Br}(E \times E)}{\mathrm{Br}_1(E \times E)} \mid 2 \cdot \mathfrak{f}^2 \cdot \mathfrak{c}^2 \tag{5.11}$$

to complete the proof of (5.4). □

Remark 5.17. — Similar results can be obtained for $\# \mathrm{Br}(\overline{E} \times \overline{E})^{\Gamma_k}$. For example, if E has CM by $\mathcal{O}_K$ then [21, Theorems 2.6 and 2.8], Lemma 5.5 and Proposition 4.1 show that

$$\# \mathrm{Br}(\overline{E} \times \overline{E})^{\Gamma_k} = |\Delta_K| \cdot \prod_{\ell \text{ prime}} \ell^{2 \cdot m_\ell(E)} \leqslant 3^2 \cdot |\Delta_K| \cdot [k : \mathbf{Q}]^4.$$

Corollary 5.18. — *Let E be an elliptic curve over a number field k with CM by an order in an imaginary quadratic field K. Then, for $k = \mathbf{Q}$,*

$$\# \frac{\mathrm{Br}(E \times E)}{\mathrm{Br}_1(E \times E)} \leqslant \begin{cases} 4 & \text{if } K = \mathbf{Q}(\sqrt{-7}); \\ 8 & \text{if } K = \mathbf{Q}(i); \\ 9 & \text{if } K = \mathbf{Q}(\zeta_3); \\ 1 & \text{otherwise.} \end{cases} \tag{5.12}$$

For $[k : \mathbf{Q}] \geqslant 2$,

$$\# \frac{\mathrm{Br}(E \times E)}{\mathrm{Br}_1(E \times E)} \leqslant [k : \mathbf{Q}]^8. \tag{5.13}$$

In all cases,

$$\#\frac{\mathrm{Br}(E\times E)}{\mathrm{Br}_1(E\times E)} \mid 2\cdot[k:\mathbf{Q}]^8\cdot \prod_{\substack{\ell \text{ prime},\ \ell\nmid[k:\mathbf{Q}]\\ \left(\ell-\left(\frac{\Delta_K}{\ell}\right)\right)\mid[\mathcal{O}_K^\times:\mathcal{O}_\ell^\times]\cdot[k:\mathbf{Q}]}} \ell^4. \tag{5.14}$$

Proof. — Let $\mathrm{End}(\overline{E})=\mathcal{O}_\mathfrak{f}$ and let $\mathfrak{c}$ be as in the proof of Corollary 5.15. To obtain (5.13) and (5.14), repeat the proof of Corollary 5.15 noting that at each stage the bounds given for $\mathfrak{c}$ also apply to $\mathfrak{f}$ by Corollary 4.4. We finish by proving (5.12). By Lemma 5.5 and Corollary 4.4, we have $K_\mathfrak{c}=K_\mathfrak{f}=K$; we will use this in our applications of Proposition 4.1. If $K\notin\{\mathbf{Q}(\sqrt{-7}),\mathbf{Q}(\zeta_3),\mathbf{Q}(i)\}$ then Proposition 4.1 shows that $\mathfrak{c}=\mathfrak{f}=1$. If $\mathfrak{f}=1$ then the result follows from [21, Theorem 3.1], Theorem 5.3 and Remark 5.4. Henceforth, suppose that $\mathfrak{f}>1$ and $K\in\{\mathbf{Q}(\sqrt{-7}),\mathbf{Q}(\zeta_3),\mathbf{Q}(i)\}$.

If $K=\mathbf{Q}(\sqrt{-7})$ then Proposition 4.1 shows that $\mathfrak{c},\mathfrak{f}\leqslant 2$. Thus, the result follows from Theorem 5.13 if we can show that any elliptic curve $E/\mathbf{Q}$ with $\mathrm{End}(\overline{E})=\mathbf{Z}[\sqrt{-7}]$ satisfies $E[2]\neq E[2](\mathbf{Q})$. Up to a quadratic twist (which does not change the Galois module structure of the 2-torsion), we may assume that E is the elliptic curve [17, Elliptic Curve 49.a.1], which has Mordell–Weil group $\mathbf{Z}/2\mathbf{Z}$.

If $K=\mathbf{Q}(\zeta_3)$ then Proposition 4.1 shows that $\mathfrak{c},\mathfrak{f}\leqslant 3$. For $\mathfrak{f}=3$, the result follows directly from Theorem 5.13 and Remark 5.14 since $2\nmid\Delta_K$. For $\mathfrak{f}=2$ we must verify that any elliptic curve $E/\mathbf{Q}$ with $\mathrm{End}(\overline{E})=\mathbf{Z}[\sqrt{-3}]$ satisfies $E[2]\neq E[2](\mathbf{Q})$. As above, we need only check this for one specific curve since $\mathrm{Aut}\,\overline{E}=\{\pm1\}$ and hence any twist of $E/\mathbf{Q}$ is a quadratic twist. We can take E to be [17, Elliptic Curve 36.a.1] which has Mordell–Weil group $\mathbf{Z}/2\mathbf{Z}$, for example.

If $K=\mathbf{Q}(i)$ then (4.1) shows that $\mathfrak{c},\mathfrak{f}\leqslant 2$. By the same reasoning as above, the result follows from the fact that the elliptic curve [17, Elliptic Curve 32.a.1] has Mordell–Weil group $\mathbf{Z}/2\mathbf{Z}$. □

6. The transcendental part of the Brauer group of a product of CM elliptic curves

In this section we give uniform bounds on the transcendental part of the Brauer group of a product $E_1\times E_2$ of CM elliptic curves. The curves may or may not be isogenous – we deal with these two cases separately. In the case where E_1 and E_2 are isogenous we will use the isogeny to reduce to the case where $E_1=E_2$, which was dealt with in the previous section. We begin by

bounding the difference in size of the transcendental parts of the Brauer groups of isogenous abelian varieties in terms of the degree of the isogeny.

PROPOSITION 6.1. — *Let A and A' be abelian varieties of dimension g over a field k of characteristic 0. Suppose that there exists a k-isogeny $\phi : A \to A'$ of degree d. Then the kernel of the induced map $\phi^* : \operatorname{Br} \overline{A'} \to \operatorname{Br} \overline{A}$ is contained in $\operatorname{Br} \overline{A'}[d]$. Consequently,*

$$\#(\operatorname{Br} \overline{A'})^{\Gamma_k} \mid d^{g(2g-1)-\rho} \cdot \#(\operatorname{Br} \overline{A})^{\Gamma_k}$$

and

$$\#\frac{\operatorname{Br} A'}{\operatorname{Br}_1 A'} \mid d^{g(2g-1)-\rho} \cdot \#\frac{\operatorname{Br} A}{\operatorname{Br}_1 A},$$

where ρ is the rank of $\operatorname{NS} \overline{A'}$ and we have $1 \leqslant \rho \leqslant g^2$.

Proof. — The isogeny ϕ induces an injection of function fields

$$\phi^* : \overline{k}(\overline{A'}) \hookrightarrow \overline{k}(\overline{A})$$

such that $[\overline{k}(\overline{A}) : \phi^*(\overline{k}(\overline{A'}))] = d$. The map $\phi^* : \operatorname{Br} \overline{A'} \to \operatorname{Br} \overline{A}$ coincides with the restriction map $\operatorname{Res}_\phi : \operatorname{Br} \overline{k}(\overline{A'}) \to \operatorname{Br} \overline{k}(\overline{A})$. Since $\operatorname{Cor}_\phi \circ \operatorname{Res}_\phi = [d]$, the kernel of $\phi^* : \operatorname{Br} \overline{A'} \to \operatorname{Br} \overline{A}$ is contained in $\operatorname{Br} \overline{A'}[d]$. The proof of [1, Lemma 4.2] shows that $\#\operatorname{Br} \overline{A'}[d] = d^{g(2g-1)-\rho}$. The fact that $1 \leqslant \rho \leqslant g^2$ is well known.

To complete the proof, recall that for any abelian variety B, there is an injection $\operatorname{Br} B/\operatorname{Br}_1 B \hookrightarrow (\operatorname{Br} \overline{B})^{\Gamma_k}$ by definition of $\operatorname{Br}_1 B$, and $(\operatorname{Br} \overline{B})^{\Gamma_k}$ is finite by [33, Theorem 1.1]. The kernels of the induced maps $\phi^* : (\operatorname{Br} \overline{A'})^{\Gamma_k} \to (\operatorname{Br} \overline{A})^{\Gamma_k}$ and $\phi^* : \operatorname{Br} A'/\operatorname{Br}_1 A' \to \operatorname{Br} A/\operatorname{Br}_1 A$ are contained in the kernel of $\phi^* : \operatorname{Br} \overline{A'} \to \operatorname{Br} \overline{A}$. □

Next, we bound the degree of an isogeny between CM elliptic curves in terms of the CM data.

PROPOSITION 6.2. — *Let E_1 and E_2 be elliptic curves over $\mathbf{C}$ with complex multiplication by an order $\mathcal{O}$ of conductor $\mathfrak{f}$ in an imaginary quadratic field K. Then there is an isogeny $\varphi : E_1 \to E_2$ such that*

$$\deg \varphi \leqslant 2 \cdot \pi^{-1} \cdot \mathfrak{f} \cdot \sqrt{|\Delta_K|}.$$

Proof. — First note that all elliptic curves over $\mathbf{C}$ with CM by $\mathcal{O}$ are isogenous and that, up to isomorphism, any isogeny between elliptic curves over $\mathbf{C}$ with CM by $\mathcal{O}$ is of the form $\phi_\mathfrak{a} : E_\mathfrak{b} \to E_{\mathfrak{a}^{-1}\mathfrak{b}}$ for invertible $\mathcal{O}$-ideals $\mathfrak{a}$ and $\mathfrak{b}$. Here $E_\mathfrak{b}$ corresponds to $\mathbf{C}/\mathfrak{b}$ and $\phi_\mathfrak{a}$ is the natural map coming from the inclusion of lattices $\mathfrak{b} \subset \mathfrak{a}^{-1}\mathfrak{b}$. See [4, Corollary 10.20], for example. We have $\deg \phi_\mathfrak{a} = N(\mathfrak{a}) = [\mathcal{O} : \mathfrak{a}]$ by [4, Lemma 11.26], for example. Note that replacing $\mathfrak{a}$ by $\lambda\mathfrak{a}$ for $\lambda \in K^\times$ corresponds to replacing $\mathfrak{a}^{-1}\mathfrak{b}$ by a homothetic

lattice and hence does not change the isomorphism class of $E_{\mathfrak{a}^{-1}\mathfrak{b}}$. A simple application of Minkowski's theorem shows that there exists an $\mathcal{O}$-ideal $\mathfrak{c}$ in the same ideal class as $\mathfrak{a}$ such that $N(\mathfrak{c}) \leqslant 2 \cdot \pi^{-1} \cdot \mathfrak{f} \cdot \sqrt{|\Delta_K|}$, since $\mathfrak{f}^2 \cdot |\Delta_K|$ is the absolute value of the discriminant of $\mathcal{O}$. Therefore $\phi_{\mathfrak{c}}$ is a suitable isogeny. □

COROLLARY 6.3. — *Let E_1 and E_2 be elliptic curves over $\mathbf{C}$ with complex multiplication by orders with conductors $\mathfrak{f}_1$ and $\mathfrak{f}_2$, respectively, in an imaginary quadratic field K. Then there is an isogeny $\varphi : E_1 \to E_2$ such that*

$$\deg \varphi \leqslant 2 \cdot \pi^{-1} \cdot \mathfrak{f}_1 \cdot \mathfrak{f}_2 \cdot \sqrt{|\Delta_K|}.$$

Proof. — Lemma 5.11 shows the existence of isogenies $\phi_1 : E_1 \to E_1'$ and $\phi_2 : E_2 \to E_2'$ with degrees $\mathfrak{f}_1$ and $\mathfrak{f}_2$, respectively, where E_1' and E_2' have CM by $\mathcal{O}_K$. Proposition 6.2 shows the existence of an isogeny $\varphi : E_1' \to E_2'$ such that $\deg \varphi \leqslant 2 \cdot \pi^{-1} \cdot \sqrt{|\Delta_K|}$. Let $\hat{\phi}_2 : E_2' \to E_2$ be the dual of ϕ_2. Now the isogeny $\hat{\phi}_2 \circ \varphi \circ \phi_1 : E_1 \to E_2$ has degree at most $2 \cdot \pi^{-1} \cdot \mathfrak{f}_1 \cdot \mathfrak{f}_2 \cdot \sqrt{|\Delta_K|}$, as desired. □

Now we combine the results obtained so far to obtain bounds for the transcendental parts of Brauer groups of products of CM elliptic curves. At several points we use the fact that for a variety X/k and a finite extension L/k we have

$$\frac{\operatorname{Br} X}{\operatorname{Br}_1 X} \hookrightarrow \frac{\operatorname{Br} X_L}{\operatorname{Br}_1 X_L}. \tag{6.1}$$

THEOREM 6.4. — *Let k be a number field and let E_1 and E_2 be elliptic curves over k with complex multiplication by orders with conductors $\mathfrak{f}_1$ and $\mathfrak{f}_2$, respectively, in an imaginary quadratic field K. Let M/Kk be a finite extension such that all isogenies $\overline{E}_2 \to \overline{E}_1$ are induced by isogenies defined over M. Then*

$$\#\frac{\operatorname{Br}(E_1 \times E_2)}{\operatorname{Br}_1(E_1 \times E_2)} \leqslant 2^2 \cdot \pi^{-2} \cdot \mathfrak{f}_1^2 \cdot \mathfrak{f}_2^2 \cdot |\Delta_K| \cdot [M : \mathbf{Q}]^4.$$

Furthermore, if the class number of K is 1 then

$$\#\frac{\operatorname{Br}(E_1 \times E_2)}{\operatorname{Br}_1(E_1 \times E_2)} \leqslant \mathfrak{f}_1^2 \cdot \mathfrak{f}_2^2 \cdot [M : \mathbf{Q}]^4.$$

In all cases we can choose M such that $[M : Kk] \mid \#\mathcal{O}_K^\times$.

Proof. — Let $\varphi : E_{2,M} \to E_{1,M}$ be an M-isogeny. For $i = 1, 2$ let $\psi_i : E_i \to E_i'$ be the k-isogeny of degree $\mathfrak{f}_i$ to an elliptic curve over k with CM by

$\mathcal{O}_K$ provided by Lemma 5.11. Then $\psi_{1,M}\circ\varphi\circ\psi_{2,M}^{\vee} : E'_{2,M} \to E'_{1,M}$ is an M-isogeny. Thus, by Lemma 2.4, all isogenies $\overline{E'}_2 \to \overline{E'}_1$ are defined over M. Let $\theta : E'_{2,M} \to E'_{1,M}$ be an isogeny of minimal degree. By Proposition 6.2,

$$\deg\theta \leqslant 2\cdot\pi^{-1}\cdot\sqrt{|\Delta_K|}. \tag{6.2}$$

Now $(\mathrm{id},\theta)\circ(\psi_{1,M},\psi_{2,M}) : E_{1,M}\times E_{2,M} \to E'_{1,M}\times E'_{1,M}$ is an M-isogeny of degree $\mathfrak{f}_1\cdot\mathfrak{f}_2\cdot\deg\theta$. Now by (6.1) and Proposition 6.1,

$$\#\frac{\mathrm{Br}(E_1\times E_2)}{\mathrm{Br}_1(E_1\times E_2)} \mid \#\frac{\mathrm{Br}(E_{1,M}\times E_{2,M})}{\mathrm{Br}_1(E_{1,M}\times E_{2,M})} \mid (\mathfrak{f}_1\cdot\mathfrak{f}_2\cdot\deg\theta)^2\cdot\#\frac{\mathrm{Br}(E'_{1,M}\times E'_{1,M})}{\mathrm{Br}_1(E'_{1,M}\times E'_{1,M})}.$$

Recall that $K\subset M$ and hence $[M:\mathbf{Q}]\geqslant 2$, whereby Corollary 5.15 gives

$$\#\frac{\mathrm{Br}(E'_{1,M}\times E'_{1,M})}{\mathrm{Br}_1(E'_{1,M}\times E'_{1,M})} \leqslant [M:\mathbf{Q}]^4.$$

Putting everything together yields the desired result. If the class number of K is 1 then all elliptic curves with CM by $\mathcal{O}_K$ are isomorphic over $\overline{k}$ and hence $\deg\theta = 1$.

Finally, by [24, Proposition 1.3] all isogenies $\overline{E}_2 \to \overline{E}_1$ are induced by isogenies defined over a Galois extension of Kk with degree dividing $\#\mathcal{O}_K^{\times}$. □

Under the assumption of the Generalised Riemann Hypothesis, the following result gives a bound that only depends on the degree of the base field.

THEOREM 6.5. — *Suppose that the Generalised Riemann Hypothesis holds. Let k be a number field, let K be an imaginary quadratic field, and let E_1, E_2 be elliptic curves over k, each with (not necessarily full) CM by K. Let M/Kk be a finite extension such that all isogenies $\overline{E}_2 \to \overline{E}_1$ are induced by isogenies defined over M. Then $\#\frac{\mathrm{Br}(E_1\times E_2)}{\mathrm{Br}_1(E_1\times E_2)}$ is at most*

$$(3.4)^2\cdot 10^8\cdot[M:k]^4\cdot[k:\mathbf{Q}]^{12}\cdot\big((3.23)\cdot\log([k:\mathbf{Q}])+(2.73)\cdot 109\big)^4.$$

Moreover, we can choose M such that $[M:Kk] \mid \#\mathcal{O}_K^{\times}$.

Proof. — By [24, Proposition 1.3] and [8, Théorème 1.4], there exists a number field M with $[M:Kk] \mid \#\mathcal{O}_K^{\times}$ and an M-isogeny $\varphi : E_{1,M} \to E_{2,M}$ with

$$\deg\varphi \leqslant (3.4)\cdot 10^4\cdot[k:\mathbf{Q}]^2\cdot\max\left\{h_F(E_1)+\frac{1}{2}\cdot\log([k:\mathbf{Q}]),1\right\}^2,$$

where h_F is the stable Faltings height. Under the assumption of the Generalised Riemann Hypothesis, [43, Corollary 2.18] gives $h_F(E_1) \leqslant (2.73)\cdot$

$(109 + \log([k : \mathbf{Q}]))$ and hence

$$\deg \varphi \leqslant (3.4) \cdot 10^4 \cdot [k : \mathbf{Q}]^2 \cdot \big((3.23) \cdot \log([k : \mathbf{Q}]) + (2.73) \cdot 109\big)^2. \tag{6.3}$$

By (6.1) and Proposition 6.1,

$$\#\frac{\mathrm{Br}(E_1 \times E_2)}{\mathrm{Br}_1(E_1 \times E_2)} \mid \#\frac{\mathrm{Br}(E_{1,M} \times E_{2,M})}{\mathrm{Br}_1(E_{1,M} \times E_{2,M})} \mid (\deg \varphi)^2 \cdot \#\frac{\mathrm{Br}(E_{1,M} \times E_{1,M})}{\mathrm{Br}_1(E_{1,M} \times E_{1,M})}. \tag{6.4}$$

Since $K \subset M$, we have $[M : \mathbf{Q}] \geqslant 2$ whereby Corollary 5.15 gives

$$\#\frac{\mathrm{Br}(E_{1,M} \times E_{1,M})}{\mathrm{Br}_1(E_{1,M} \times E_{1,M})} \leqslant \mathfrak{f}_1^2 \cdot [M : \mathbf{Q}]^4,$$

where E_1 has CM by the order of conductor $\mathfrak{f}_1$ in K. Combining this with (6.4) yields

$$\#\frac{\mathrm{Br}(E_1 \times E_2)}{\mathrm{Br}_1(E_1 \times E_2)} \leqslant (\deg \varphi)^2 \cdot \mathfrak{f}_1^2 \cdot [M : \mathbf{Q}]^4. \tag{6.5}$$

If $K \notin \{\mathbf{Q}(\sqrt{-7}), \mathbf{Q}(i), \mathbf{Q}(\zeta_3)\}$ then Corollary 4.4 gives $\mathfrak{f}_1 \leqslant [k : \mathbf{Q}]^2$, whereby the result follows from (6.3) and (6.5). On the other hand, if $K \in \{\mathbf{Q}(\sqrt{-7}), \mathbf{Q}(i), \mathbf{Q}(\zeta_3)\}$ then the result follows from Theorem 6.4 and Corollary 4.4. □

THEOREM 6.6. — *Suppose that the Generalised Riemann Hypothesis holds. Let E_1 and E_2 be geometrically non-isogenous elliptic curves over a number field k such that E_i has (not necessarily full) CM by an imaginary quadratic field K_i. Then $\#\frac{\mathrm{Br}(E_1 \times E_2)}{\mathrm{Br}_1(E_1 \times E_2)}$ is at most*

$$2^{316} \cdot (241)^{24} \cdot [kK_1K_2 : \mathbf{Q}]^{24} \cdot \big((5.46) \cdot (109 + \log([k : \mathbf{Q}])) + 3\big)^{24}.$$

Proof. — By the definition of the transcendental part of the Brauer group, we have

$$\frac{\mathrm{Br}(E_1 \times E_2)}{\mathrm{Br}_1(E_1 \times E_2)} \hookrightarrow \mathrm{Br}(\overline{E}_1 \times \overline{E}_2)^{\mathrm{Gal}(\overline{k}/kK_1K_2)}.$$

By [7, Théorèmes 1.5(3) and 1.8] the exponent of $\mathrm{Br}(\overline{E}_1 \times \overline{E}_2)^{\mathrm{Gal}(\overline{k}/K_1K_2k)}$ is at most $2 \cdot d^{3/2}$, with

$$d \leqslant (241)^4 \cdot 2^{52} \cdot [kK_1K_2 : \mathbf{Q}]^4 \cdot \max\{\log([kK_1K_2 : \mathbf{Q}]), h_F(E_1 \times E_2) + 3\}^4, \tag{6.6}$$

where h_F is the stable Faltings height, which satisfies $h_F(E_1 \times E_2) = h_F(E_1) + h_F(E_2)$. Under the assumption of the Generalised Riemann Hypothesis, [43, Corollary 2.18] gives

$$h_F(E_i) \leqslant (2.73) \cdot (109 + \log([k : \mathbf{Q}])). \tag{6.7}$$

By (5.3) we have $\mathrm{Br}(\overline{E}_1 \times \overline{E}_2) \cong (\mathbf{Q}/\mathbf{Z})^4$ and hence

$$\frac{\mathrm{Br}(E_1 \times E_2)}{\mathrm{Br}_1(E_1 \times E_2)} \leqslant (2 \cdot d^{3/2})^4 = 2^4 \cdot d^6. \tag{6.8}$$

Combining (6.6)–(6.8) gives the desired result. □

7. Uniform bound results for certain classes of abelian and K3 surfaces

Let k be a number field. In this section, we use the results obtained for products of CM elliptic curves in Section 6 alongside the results of Sections 2 and 3 to deduce bounds on the transcendental parts of the Brauer groups of singular abelian surfaces in $\mathscr{A}_k$ and certain elements of $\mathscr{K}_k$ related to products of CM elliptic curves. We begin with the results for abelian surfaces.

THEOREM 7.1. — *Let Λ be a rank 4 lattice containing a hyperbolic plane, let $K \coloneqq \mathbf{Q}(\sqrt{\operatorname{disc}\Lambda})$, let $A \in \mathscr{A}_{k,\Lambda}$ and let L/k be a finite extension such that $\mathrm{End}(A_L) = \mathrm{End}(\overline{A})$. Then*

$$\#\frac{\mathrm{Br}\, A}{\mathrm{Br}_1\, A} \leqslant 2^2 \cdot \pi^{-2} \cdot |\Delta_K|^{-1} \cdot |\operatorname{disc}\Lambda|^2 \cdot [L : \mathbf{Q}]^4.$$

If K has class number 1 then

$$\#\frac{\mathrm{Br}\, A}{\mathrm{Br}_1\, A} \leqslant |\Delta_K|^{-2} \cdot |\operatorname{disc}\Lambda|^2 \cdot [L : \mathbf{Q}]^4.$$

In all cases we can choose L such that $[L : k] \leqslant 2^4 \cdot 3$.

Proof. — By Lemma 2.2 and Proposition 2.3 there exist a finite extension L/k with $[L : k] \leqslant 2^4 \cdot 3$ and isogenous CM elliptic curves E_1 and E_2 over L such that

$$A_L \cong E_1 \times E_2$$

and $\mathrm{End}(A_L) = \mathrm{End}(\overline{A})$. Furthermore, Corollary 2.7 shows that the CM field is K and

$$\operatorname{disc}\Lambda = \operatorname{disc}\mathrm{NS}(\overline{E}_1 \times \overline{E}_2) = \operatorname{lcm}(\mathfrak{f}_1, \mathfrak{f}_2)^2 \cdot \Delta_K$$

where E_1 and E_2 have CM by orders in K of conductors $\mathfrak{f}_1$ and $\mathfrak{f}_2$, respectively. Proposition 2.3 shows that $K \subset L$. Since $\mathrm{End}(A_L) = \mathrm{End}(\overline{A})$, all isogenies between E_1 and E_2 are defined over L. Now the result follows from (6.1) and Theorem 6.4 applied to A_L. □

Under the assumption of the Generalised Riemann Hypothesis, the next result gives a bound that only depends on $[k : \mathbf{Q}]$.

THEOREM 7.2. — *Suppose that the Generalised Riemann Hypothesis holds. Let $A \in \mathscr{A}_k$ with $\operatorname{rank} \mathrm{NS}\, \overline{A} = 4$ and let L/k be a finite extension such that $\mathrm{End}(A_L) = \mathrm{End}(\overline{A})$. Then*

$$\#\frac{\mathrm{Br}\, A}{\mathrm{Br}_1\, A} \leqslant (3.4)^2 \cdot 10^8 \cdot [L : \mathbf{Q}]^{12} \cdot \big((3.23) \cdot \log([L : \mathbf{Q}]) + (2.73) \cdot 109\big)^4.$$

Moreover, we can choose L such that $[L : k] \leqslant 2^4 \cdot 3$.

Proof. — By Lemma 2.2 and Proposition 2.3 there exist a finite extension L/k with $[L : k] \leqslant 2^4 \cdot 3$ and isogenous CM elliptic curves E_1 and E_2 over L such that

$$A_L \cong E_1 \times E_2$$

and $\mathrm{End}(A_L) = \mathrm{End}(\overline{A})$. By (6.1) we have

$$\#\frac{\mathrm{Br}\, A}{\mathrm{Br}_1\, A} \mid \#\frac{\mathrm{Br}\, A_L}{\mathrm{Br}_1\, A_L} = \#\frac{\mathrm{Br}(E_1 \times E_2)}{\mathrm{Br}_1(E_1 \times E_2)}.$$

Now apply Theorem 6.5 to $E_1 \times E_2$ over L, noting that since $\mathrm{End}(A_L) = \mathrm{End}(\overline{A})$ we can take $M = L$ in Theorem 6.5. □

Next we give our results for K3 surfaces related to products of CM elliptic curves. The bounds obtained depend on whether the elliptic curves are isogenous.

THEOREM 7.3. — *Let Λ be the Néron–Severi lattice of the Kummer surface of a product of isogenous (not necessarily full) CM elliptic curves over $\overline{k}$, let $K := \mathbf{Q}(\sqrt{\operatorname{disc} \Lambda})$, and let $X \in \mathscr{K}_{k,\Lambda}$. Then there exist a finite extension L/k and elliptic curves E_1, E_2 over L with $X_L \cong \mathrm{Kum}(E_1 \times E_2)$ and we have*

$$\#\frac{\mathrm{Br}\, X}{\mathrm{Br}_1\, X} \leqslant 2^{-2} \cdot \pi^{-2} \cdot |\Delta_K|^{-1} \cdot |\operatorname{disc} \Lambda|^2 \cdot [L : \mathbf{Q}]^4.$$

If K has class number 1 then

$$\#\frac{\mathrm{Br}\, X}{\mathrm{Br}_1\, X} \leqslant 2^{-4} \cdot |\Delta_K|^{-2} \cdot |\operatorname{disc} \Lambda|^2 \cdot [L : \mathbf{Q}]^4.$$

In all cases we can choose L such that $[L : k] \leqslant 2^9 \cdot 3 \cdot M(20)$.

Proof. — By Proposition 3.4, Theorem 3.5, and Proposition 3.8, there exist a finite extension L/k and isogenous (not necessarily full) CM elliptic curves E_1, E_2 over L such that $X_L \cong \mathrm{Kum}(E_1 \times E_2)$. Corollary 3.13 shows that the CM field is K and

$$|\mathrm{disc}\,\Lambda| = |\mathrm{disc}\,\mathrm{NS}(\mathrm{Kum}(\overline{E}_1 \times \overline{E}_2))| = 2^2 \cdot \mathrm{lcm}(\mathfrak{f}_1, \mathfrak{f}_2)^2 \cdot |\Delta_K|,$$

where E_1 and E_2 have CM by orders in K of conductors $\mathfrak{f}_1$ and $\mathfrak{f}_2$, respectively. By Remark 3.7, Theorem 3.5, and Proposition 3.8, we have $K \subset L$ and

$$[L : k] \leqslant 2 \cdot M(20) \cdot 2^4 \cdot 3 \cdot 2^4 = 2^9 \cdot 3 \cdot M(20).$$

The result now follows from (6.1), [34, Theorem 2.4] (cf. Corollary 3.10), and Theorem 6.4. □

THEOREM 7.4. — *Suppose that the Generalised Riemann Hypothesis holds. Let $X \in \mathscr{K}_k$ be such that* $\mathrm{rank}\,\mathrm{NS}\,\overline{X} = 20$. *Then there exists a finite extension L/k such that $X_L \cong \mathrm{Kum}(E_1 \times E_2)$ for some elliptic curves E_1, E_2 over L and we have*

$$\#\frac{\mathrm{Br}\,X}{\mathrm{Br}_1\,X} \leqslant (3.4)^2 \cdot 10^8 \cdot [L : \mathbf{Q}]^{12} \cdot \big((3.23) \cdot \log([L : \mathbf{Q}]) + (2.73) \cdot 109\big)^4.$$

Moreover, we can choose L such that $[L : k] \leqslant 2^9 \cdot 3 \cdot M(20)$.

Proof. — By Remark 3.7, Theorem 3.5 and Corollary 3.10, there exists an extension L/k with $[L : k] \leqslant 2^9 \cdot 3 \cdot M(20)$ and elliptic curves E_1, E_2 over L such that

$$\frac{\mathrm{Br}\,X}{\mathrm{Br}_1\,X} \hookrightarrow \frac{\mathrm{Br}(E_1 \times E_2)}{\mathrm{Br}_1(E_1 \times E_2)}$$

and $\mathrm{End}(E_1 \times E_2) = \mathrm{End}(\overline{E}_1 \times \overline{E}_2)$. Now the result follows from Theorem 7.2. □

THEOREM 7.5. — *Suppose that the Generalised Riemann Hypothesis holds. Let X/k be a singular K3 surface, i.e. a K3 surface with* $\mathrm{rank}\,\mathrm{NS}\,\overline{X} = 20$. *Then*

$$\#\frac{\mathrm{Br}\,X}{\mathrm{Br}_1\,X} \leqslant 2^{130} \cdot 3^{12} \cdot 5^8 \cdot (3.4)^2 \cdot M(20)^{12} \cdot [k : \mathbf{Q}]^{12} \cdot \big((3.23) \cdot \log(2^{10} \cdot 3 \cdot M(20) \cdot [k : \mathbf{Q}]) + (2.73) \cdot 109\big)^4.$$

Proof. — The proof of [28, Theorem 1] shows there is a double cover $\varphi : Y \dashrightarrow X$ such that Y and φ are defined over an extension k'/k of degree at most $2 \cdot M(20)$ and $\overline{Y}$ is a Kummer surface with $\mathrm{rank}\,\mathrm{NS}\,\overline{Y} = 20$. Then Theorem 7.4 gives

$$\#\frac{\mathrm{Br}\,Y}{\mathrm{Br}_1\,Y} \leqslant (3.4)^2 \cdot 10^8 \cdot [L : \mathbf{Q}]^{12} \cdot \big((3.23) \cdot \log([L : \mathbf{Q}]) + (2.73) \cdot 109\big)^4$$

where L is a finite extension of k' built from the field extensions in Proposition 3.4, Theorem 3.5 and Corollary 3.10. Comparing the proofs of [41, Proposition 2.1] and [28, Theorem 1] shows that the field extension in Proposition 3.4 is at most quadratic over k', since $\Gamma_{k'}$ acts trivially on $\mathrm{NS}\,\overline{X}$ by construction. Consequently, $[L : k'] \leqslant 2^9 \cdot 3$ and hence $[L : k] \leqslant 2^{10} \cdot 3 \cdot M(20)$. The proof of [11, Corollary 2.2] shows that φ induces a map $\varphi^* : \mathrm{Br}\, X_{k'}/\mathrm{Br}_1\, X_{k'} \to \mathrm{Br}\, Y/\mathrm{Br}_1\, Y$ whose kernel is killed by 2. Therefore, $\ker\varphi \hookrightarrow \mathrm{Br}\,\overline{X}[2]$ and, using (6.1), this yields

$$\#\frac{\mathrm{Br}\, X}{\mathrm{Br}_1\, X} \leqslant \#\,\mathrm{Br}\,\overline{X}[2] \cdot \#\frac{\mathrm{Br}\, Y}{\mathrm{Br}_1\, Y}.$$

Now use that $\mathrm{Br}\,\overline{X} \cong (\mathbf{Q}/\mathbf{Z})^2$, as follows from work of Grothendieck. □

THEOREM 7.6. — *Suppose that the Generalised Riemann Hypothesis holds. Let $X \in \mathscr{K}_k$ be geometrically isomorphic to the Kummer surface of the product of two non-isogenous (not necessarily full) CM elliptic curves over $\mathbf{C}$. Then $\#\frac{\mathrm{Br}\, X}{\mathrm{Br}_1\, X}$ is at most*

$$2^{508}\cdot(241)^{24}\cdot M(18)^{24}\cdot[k:\mathbf{Q}]^{24}\cdot\big((5.46)\cdot(109+\log(2^6\cdot M(18)\cdot[k:\mathbf{Q}]))+3\big)^{24}.$$

Proof. — By Remark 3.7, Theorem 3.5, and Corollary 3.10, there exist a finite extension L/k with $[L : k] \leqslant 2^6 \cdot M(18)$ and elliptic curves E_1 and E_2 over L such that

$$\frac{\mathrm{Br}\, X}{\mathrm{Br}_1\, X} \hookrightarrow \frac{\mathrm{Br}(E_1 \times E_2)}{\mathrm{Br}_1(E_1 \times E_2)}.$$

Now apply Theorem 6.6. □

THEOREM 7.7. — *Let k be a number field and let X/k be such that $\overline{X}$ is a Kummer surface with $\mathrm{rank}\,\mathrm{NS}\,\overline{X} = 20$. Then $X(\mathbf{A}_k)^{\mathrm{Br}}$ is effectively computable.*

Proof. — This follows from [15, Theorem 1], [23, Theorem 8.38], Theorem 7.3 and Remark 1.4. □

THEOREM 7.8. — *Suppose that the Generalised Riemann Hypothesis holds. Let X/k be a singular K3 surface or a surface that is geometrically isomorphic to the Kummer surface of the product of elliptic curves E_1 and E_2 over $\mathbf{C}$, where E_i has CM by an order $\mathcal{O}_i$ in a CM field K_i for $i = 1, 2$. Then $X(\mathbf{A}_k)^{\mathrm{Br}}$ is effectively computable.*

Proof. — This follows from [15, Theorem 1], [23, Theorem 8.38], Theorems 7.4, 7.5, 7.6, and Remark 1.4. □

BIBLIOGRAPHY

[1] F. Balestrieri & R. Newton, "Arithmetic of Rational Points and Zero-cycles on Products of Kummer Varieties and K3 Surfaces", *International Mathematics Research Notices* **2021** (2019), no. 6, p. 4255-4279.

[2] V. Cantoral-Farfán, Y. Tang, S. Tanimoto & E. Visse, "Effective bounds for Brauer groups of Kummer surfaces over number fields", *J. Lond. Math. Soc. (2)* **97** (2018), no. 3, p. 353-376.

[3] J. W. S. Cassels & A. Fröhlich, *Algebraic Number Theory*, London Mathematical Society, 2010.

[4] 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, xiv+351 pages.

[5] H. B. Daniels & A. Lozano-Robledo, "On the number of isomorphism classes of CM elliptic curves defined over a number field", *J. Number Theory* **157** (2015), p. 367-396.

[6] F. Fité, K. Kedlaya, V. Rotger & A. Sutherland, "Sato–Tate distributions and Galois endomorphism modules in genus 2", *Compos. Math.* **148** (2012), no. 5, p. 1390-1442.

[7] É. Gaudron & G. Rémond, "Nouveaux théorèmes d'isogénie", to appear in *Mém. Soc. Math. France*.

[8] ———, "Théorème des périodes et degrés minimaux d'isogénies", *Comment. Math. Helv.* **89** (2014), no. 2, p. 343-403.

[9] A. Grothendieck, "Le groupe de Brauer. II. Théorie cohomologique", in *Dix exposés sur la cohomologie des schémas*, Adv. Stud. Pure Math., vol. 3, North-Holland, Amsterdam, 1968, p. 67-87.

[10] D. Huybrechts, *Lectures on K3 surfaces*, Cambridge Studies in Advanced Mathematics, vol. 158, Cambridge University Press, Cambridge, 2016, xi+485 pages.

[11] E. Ieronymou & A. Skorobogatov, "Odd order Brauer-Manin obstruction on diagonal quartic surfaces", *Adv. Math.* **270** (2015), p. 181-205, corrigendum: *Advances in Mathematics* 307 (2017), 1372-1377.

[12] K. Ito, "On the Supersingular Reduction of K3 Surfaces with Complex Multiplication", *International Mathematics Research Notices* **2020** (2018), no. 20, p. 7306-7346.

[13] E. Kani, "Products of CM elliptic curves", *Collect. Math.* **62** (2011), no. 3, p. 297-339.

[14] ———, "The moduli spaces of Jacobians isomorphic to a product of two elliptic curves", *Collect. Math.* **67** (2016), no. 1, p. 21-54.

[15] A. Kresch & Yu. Tschinkel, "Effectivity of Brauer–Manin obstructions on surfaces", *Adv. Math.* **226** (2011), no. 5, p. 4131-4144.

[16] R. Laface, "Decompositions of singular abelian surfaces", *Asian J. Math.* **23** (2019), no. 1, p. 157-172.

[17] The LMFDB Collaboration, "The L-functions and Modular Forms Database", 2019, `http://www.lmfdb.org` Online; accessed 30 October 2019.

[18] E. Looijenga & C. Peters, "Torelli theorems for Kähler $K3$ surfaces", *Compositio Math.* **42** (1980/81), no. 2, p. 145-186.

[19] Yu. I. Manin, "Le groupe de Brauer–Grothendieck en géométrie diophantienne", in *Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 1*, Gauthier-Villars, Paris, 1971, p. 401-411.

[20] H. Minkowski, "Zur Theorie der positiven quadratischen Formen", *J. Reine Angew. Math.* **101** (1887), p. 196-202.

[21] R. Newton, "Transcendental Brauer groups of products of CM elliptic curves", *J. Lond. Math. Soc. (2)* **93** (2016), no. 2, p. 397-419.

[22] M. Orr & A. N. Skorobogatov, "Finiteness theorems for K3 surfaces and abelian varieties of CM type", *Compos. Math.* **154** (2018), no. 8, p. 1571-1592.

[23] B. Poonen, D. Testa & R. van Luijk, "Computing Néron–Severi groups and cycle class groups", *Compos. Math.* **151** (2015), no. 4, p. 713-734.

[24] G. Rémond, "Degré de définition des endomorphismes d'une variété abélienne", *J. Eur. Math. Soc. (JEMS)* **22** (2020), no. 9, p. 3059-3099.

[25] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 9.0)*, 2020, `https://www.sagemath.org`.

[26] M. Schütt, "$K3$ surfaces with Picard rank 20", *Algebra Number Theory* **4** (2010), no. 3, p. 335-356.

[27] J.-P. Serre, "Bounds for the orders of the finite subgroups of $G(k)$", in *Group representation theory*, EPFL Press, Lausanne, 2007, p. 405-450.

[28] I. R. Shafarevich, "On the arithmetic of singular $K3$-surfaces", in *Algebra and analysis (Kazan, 1994)*, de Gruyter, Berlin, 1996, p. 103-108.

[29] T. Shioda, "Correspondence of elliptic curves and Mordell-Weil lattices of certain elliptic $K3$'s", in *Algebraic cycles and motives. Vol. 2*, London Math. Soc. Lecture Note Ser., vol. 344, Cambridge Univ. Press, Cambridge, 2007, p. 319-339.

[30] T. Shioda & H. Inose, "On singular $K3$ surfaces", in *Complex analysis and algebraic geometry* (W. L. B. Jr & T. Shioda, eds.), Iwanami Shoten, Tokyo, 1977, p. 119-136.

[31] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994, xiv+525 pages.

[32] A. N. Skorobogatov, "Diagonal quartic surfaces", *Explicit Methods in Number Theory. Oberwolfach report* (2009), no. 33, p. 76-79.

[33] A. N. Skorobogatov & Y. G. Zarhin, "A finiteness theorem for the Brauer group of abelian varieties and $K3$ surfaces", *J. Algebraic Geom.* **17** (2008), no. 3, p. 481-502.

[34] ———, "The Brauer group of Kummer surfaces and torsion of elliptic curves", *J. Reine Angew. Math.* **666** (2012), p. 115-140.

[35] ———, "Kummer varieties and their Brauer groups", *Pure Appl. Math. Q.* **13** (2017), no. 2, p. 337-368.

[36] K. Soundararajan, "The number of imaginary quadratic fields with a given class number", *Hardy-Ramanujan J.* **30** (2007), p. 13-18.

[37] T. Tatuzawa, "On a theorem of Siegel", *Jpn. J. Math.* **21** (1951), p. 163-178.

[38] D. Valloni, "The theory of complex multiplication for K3 surfaces", 2018, preprint, `https://arxiv.org/abs/1804.08763v1`.

[39] ———, "Complex multiplication and Brauer groups of K3 surfaces", *Adv. Math.* **385** (2021), article no. 107772 (54 pages).

[40] A. Várilly-Alvarado, "Arithmetic of K3 surfaces", in *Geometry over nonclosed fields*, Simons Symp., Springer, Cham, 2017, p. 197-248.

[41] A. Várilly-Alvarado & B. Viray, "Abelian n-division fields of elliptic curves and Brauer groups of product Kummer & abelian surfaces", *Forum Math. Sigma* **5** (2017), article no. e26 (42 pages).

[42] ———, "Corrigendum to "Abelian n-division fields of elliptic curves and Brauer groups of product Kummer and abelian surfaces"", appendix in `https://arxiv.org/abs/1606.09240`, 2020.

[43] B. Winckler, "Problème de Lehmer sur les courbes elliptiques à multiplications complexes", *Acta Arith.* **182** (2018), no. 4, p. 347-396.

Manuscrit reçu le 3 novembre 2020,
révisé le 11 mars 2021,
accepté le 23 juin 2021.

Francesca BALESTRIERI
The American University of Paris
5 Boulevard de La Tour-Maubourg
75007 Paris (France)
fbalestrieri@aup.edu

Alexis JOHNSON
Department of Mathematics
University of Minnesota
206 Church St SE
Minneapolis, MN 55455 (USA)
akjohns@umn.edu

Rachel NEWTON
Department of Mathematics
King's College London
Strand, London WC2R 2LS (UK)
rachel.newton@kcl.ac.uk