How big is the image of the Galois representations attached to CM elliptic curves?

Francesco Campagna, Riccardo Pengo

HOW BIG IS THE IMAGE OF THE GALOIS REPRESENTATIONS ATTACHED TO CM ELLIPTIC CURVES?

FRANCESCO CAMPAGNA AND RICCARDO PENGO

Abstract. Using an analogue of Serre's open image theorem for elliptic curves with complex multiplication, one can associate to each CM elliptic curve E defined over a number field F a natural number $\mathcal{I}(E/F)$ which describes how big the image of the Galois representation associated to E is. We show how one can compute $\mathcal{I}(E/F)$, using a closed formula that we obtain from the classical theory of complex multiplication.

1. Introduction

Fix an algebraic closure $\overline{\mathbb{Q}}$ of the field of rational numbers $\mathbb{Q}$. Let E be an elliptic curve defined over a number field $F \subseteq \overline{\mathbb{Q}}$, and let:

$$\rho_E : G_F \to \mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}}) \tag{1}$$

be the representation of the absolute Galois group $G_F := \mathrm{Gal}(\overline{F}/F)$ associated to its action on the torsion points $E_{\mathrm{tors}} := E(\overline{F})_{\mathrm{tors}}$ of the elliptic curve E.

If E does not have complex multiplication (CM), *i.e.* $\mathrm{End}_{\overline{F}}(E) \cong \mathbb{Z}$, Serre's open image theorem [19, Théorème 3] implies that the index $\mathcal{I}(E/F) := |\mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}}) : \rho_E(G_F)|$ is finite. One is naturally led to investigate the dependence of $\mathcal{I}(E/F)$ on E and F. For instance, one can ask whether there exists an explicit, closed formula for $\mathcal{I}(E/F)$, whose terms can be effectively computed starting from a Weierstraß equation of E. At the time of writing, and to the best of the authors' knowledge, no such formula is available in the literature. The previous question can then be weakened, by asking whether there exists an upper bound for $\mathcal{I}(E/F)$, which can be effectively computed in terms of E. An affirmative answer to this second question has been provided by Lombardo in [12]. In fact, it has even been conjectured that there should exist such an upper bound which does not depend on E, but only on the field of definition F. This conjecture is explicitly mentioned for $F = \mathbb{Q}$ in the introduction to the recent work of Rouse, Sutherland and Zureick-Brown [17], and is known to hold true under the assumption of Serre's uniformity conjecture, by previous work of Zywina (see [26, Theorem 1.4]).

On the other hand, if E has complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field K, *i.e.* $\mathrm{End}_{\overline{F}}(E) \cong \mathcal{O}$, the index of the image of ρ_E inside $\mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}})$ is infinite. Nevertheless, as we recall in Section 2, one can formulate an analogue of Serre's open image theorem for E, by replacing $\mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}})$ with a smaller subgroup $\mathcal{G}(E/F) \subseteq \mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}})$, explicitly defined in (7), which is closed and of infinite index inside $\mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}})$. As a consequence, the index $\mathcal{I}(E/F) := |\mathcal{G}(E/F) : \rho_E(G_F)|$ is finite, and, as above, one can ask whether it can be expressed by means of an explicit and closed formula. The main goal of this paper is to show how to use the classical theory of complex multiplication to give the following affirmative answer to this question.

Theorem 1.1. *Let $\mathcal{O}$ be an order in an imaginary quadratic field $K \subseteq \overline{\mathbb{Q}}$. Let E be an elliptic curve that has complex multiplication by $\mathcal{O}$ and is defined over a number field $F \subseteq \overline{\mathbb{Q}}$. Denote by $K^{ab} \subseteq \overline{\mathbb{Q}}$ the maximal abelian extension of K contained in $\overline{\mathbb{Q}}$, and by $FK \subseteq \overline{\mathbb{Q}}$ and $FK^{ab} \subseteq \overline{\mathbb{Q}}$ the composita of F with K and K^{ab} respectively. Then:*

$$\mathcal{I}(E/F) = [(FK) \cap K^{ab} : H_{\mathcal{O}}] \cdot \frac{|\mathcal{O}^{\times}|}{[F(E_{tors}) : FK^{ab}]} \tag{2}$$

2020 *Mathematics Subject Classification.* Primary: 11G05, 14K22, 11F80, 11G15; Secondary: 11Y40.
Key words and phrases. Elliptic curves, Complex multiplication, Galois representations.

where $H_{\mathcal{O}} \subseteq K^{ab}$ is the ring class field *of K relative to the order $\mathcal{O}$ (see [9, § 9]), and $F(E_{tors}) \subseteq \overline{\mathbb{Q}}$ is the field obtained by adjoining to F all the coordinates of all the points lying in E_{tors}.*

Note that the right-hand side of (2) makes sense because the extension $K \subseteq H_{\mathcal{O}}$ is abelian, and, whenever $\mathrm{End}_{\overline{F}}(E) \cong \mathcal{O}$, one knows that $FK^{\mathrm{ab}} \subseteq F(E_{\mathrm{tors}})$ [5, § 4.1 and Remark 3.8], and $H_{\mathcal{O}} = K(j(E)) \subseteq FK$ [9, Theorem 11.1], where $j(E) \in F$ denotes the *j-invariant* of the elliptic curve E. Moreover, the classical theory of complex multiplication implies that the degree of the extension $FK^{\mathrm{ab}} \subseteq F(E_{\mathrm{tors}})$ is finite and divides $|\mathcal{O}^\times|$. We explain this in more detail in Section 3, which is mainly devoted to the proof of Theorem 1.1.

As an immediate consequence of Theorem 1.1, one has the divisibility:

$$\mathcal{I}(E/F) \,\Big|\, [(FK) \cap K^{\mathrm{ab}} : H_{\mathcal{O}}] \cdot |\mathcal{O}^\times| \tag{3}$$

which shows that $\mathcal{I}(E/F)$ can be bounded solely in terms of F, for every CM elliptic curve $E_{/F}$. This improves the upper bounds for $\mathcal{I}(E/F)$ previously proved by Lombardo [13, Theorem 6.6] and Bourdon and Clark [3, Corollary 1.5]. Moreover, Theorem 1.1 applied to any elliptic curve $E_{/\mathbb{Q}}$ which has complex multiplication by an imaginary quadratic order $\mathcal{O}$ shows that $\mathcal{I}(E/\mathbb{Q}) = |\mathcal{O}^\times|$. In the case $\mathcal{O} = \mathbb{Z}[i]$, this strengthens the conclusion of [14, Theorem 1.3].

The foregoing discussion shows that $\mathcal{I}(E/F)$ is very well understood in the CM case. However, it may not appear immediately clear how to apply (2) to compute $\mathcal{I}(E/F)$ in concrete examples. We explain how to do so in Section 4. In fact, after rewriting (2) appropriately (see Proposition 4.1), we obtain an algorithm that takes as inputs a number field F and a CM elliptic curve $E_{/F}$, and outputs $\mathcal{I}(E/F)$. More precisely, we rephrase Equation (2) in terms of a finite extension $L \supseteq FK$ such that $F(E_{\mathrm{tors}}) = LK^{\mathrm{ab}}$. We prove in Proposition 4.2 that one can always take $L = F(E[I])$ to be the *I-division field* generated by the coordinates of the points $P \in E[I]$ belonging to the *I-torsion subgroup*:

$$E[I] := \bigcap_{\alpha \in I} \ker\left(E(\overline{F}) \xrightarrow{[\alpha]_E} E(\overline{F})\right)$$

where $I \subseteq \mathcal{O}$ is any ideal such that $|\mathbb{Z}/(I \cap \mathbb{Z})| > \max(2, |\mathcal{O}^\times|/2)$, and $[\cdot]_E \colon \mathcal{O} \xrightarrow{\sim} \mathrm{End}_{\overline{F}}(E)$ is the normalised isomorphism described in Lemma 2.1. In practice, if $j(E) \neq 0$ one usually takes $L = F(E[3])$ in order to ease the computational burden. We devote Section 5 to the application of this algorithm to some explicit examples of elliptic curves E that have complex multiplication by imaginary quadratic orders $\mathcal{O}$ of class number two.

2. Analogues of Serre's open image theorem for CM elliptic curves

Let E be an elliptic curve defined over a number field $F \subseteq \overline{\mathbb{Q}}$. Then, the absolute Galois group G_F naturally acts both on the set $E_{\mathrm{tors}} = \varinjlim_N E[N]$, and on the adelic Tate module $\mathcal{T}(E) := \varprojlim_N E[N]$. The first action gives rise to the Galois representation ρ_E appearing in (1), whereas the action on $\mathcal{T}(E)$ induces another Galois representation $\varrho_E \colon G_F \to \mathrm{Aut}_{\widehat{\mathbb{Z}}}(\mathcal{T}(E))$. As done in [19, § 4.1, Remarque (1)], one can construct an isomorphism:

$$\nu \colon \mathrm{Aut}_{\widehat{\mathbb{Z}}}(\mathcal{T}(E)) \xrightarrow{\sim} \mathrm{Aut}_{\widehat{\mathbb{Z}}}(E_{\mathrm{tors}}) = \mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}})$$

such that $\rho_E = \nu \circ \varrho_E$. As a consequence, one can indifferently study the Galois representation ρ_E, as done in this paper, or its twin ϱ_E, as done in some of our references.

If E does not have complex multiplication, *i.e.* if $\mathrm{End}_F(E) \cong \mathrm{End}_{\overline{F}}(E) \cong \mathbb{Z}$, then the celebrated "open image theorem", proved by Serre in [19, Théorème 3], shows that the image of the Galois representation ρ_E is a subgroup of finite index inside $\mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}}) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}})$, where $\widehat{\mathbb{Z}} := \varprojlim_N (\mathbb{Z}/N\mathbb{Z})$ denotes the profinite completion of $\mathbb{Z}$. On the other hand, if the elliptic curve E has complex multiplication, the image of ρ_E is not open inside $\mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}})$. However, one can formulate a CM analogue of Serre's open image theorem by replacing $\mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}})$ with an appropriate closed subgroup $\mathcal{G}(E/F) \subseteq \mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}})$, which we now describe.

Suppose now that $\mathrm{End}_{\overline{F}}(E) \ncong \mathbb{Z}$. Then the endomorphism ring $\mathrm{End}_{\overline{F}}(E)$ can be canonically identified with an order inside an imaginary quadratic field, as the following classical lemma shows.

Lemma 2.1. *Let F be a number field, and $E_{/F}$ be an elliptic curve such that $\mathrm{End}_{\overline{F}}(E) \ncong \mathbb{Z}$, where $\overline{F}$ denotes a fixed algebraic closure of F. Then, there exists an imaginary quadratic field K and an order $\mathcal{O} \subseteq K$ such that $\mathrm{End}_{\overline{F}}(E) \cong \mathcal{O}$. Moreover, for each embedding $\iota\colon K \hookrightarrow \overline{F}$, there exists a unique isomorphism:*

$$[\cdot]_{E,\iota}\colon \mathcal{O} \xrightarrow{\sim} \mathrm{End}_{\overline{F}}(E)$$

such that $[\alpha]^*_{E,\iota}(\omega) = \iota(\alpha)\cdot\omega$ for every $\alpha \in \mathcal{O}$ and every invariant differential ω defined over $E_{\overline{F}}$, where $[\alpha]^*_{E,\iota}(\omega)$ denotes the pull-back of ω along the endomorphism $[\alpha]_{E,\iota}$.

Proof. See [23, Chapter III, Corollary 9.4] for the existence of K and $\mathcal{O}$. Moreover, the existence of $[\cdot]_{E,\iota}$ follows from [22, Chapter II, Proposition 1.1], after fixing an embedding $\overline{F} \hookrightarrow \mathbb{C}$. Finally, observe that for any two isomorphisms $[\cdot], [\cdot]'\colon \mathcal{O} \xrightarrow{\sim} \mathrm{End}_{\overline{F}}(E)$, there exists an automorphism $\sigma\colon \mathcal{O} \xrightarrow{\sim} \mathcal{O}$ such that $[\alpha] = [\sigma(\alpha)]'$ for every $\alpha \in \mathcal{O}$. Hence, if these isomorphisms satisfy the requirements of the lemma, we see that $\iota(\alpha - \sigma(\alpha)) \cdot \omega = 0$ for every $\alpha \in \mathcal{O}$ and every invariant differential ω. Thus, we have that $\sigma = \mathrm{Id}_{\mathcal{O}}$, which allows us to conclude. □

Now, suppose at first that $E_{/F}$ is an elliptic curve such that $\mathrm{End}_F(E) \cong \mathrm{End}_{\overline{F}}(E) \cong \mathcal{O}$ for some order $\mathcal{O}$ inside an imaginary quadratic field K. Then by [20, Chapter II, Proposition 30] we necessarily have $K \subseteq F$ and one can easily show (using for instance [22, Chapter II, Theorem 2.2]) that the absolute Galois group G_F of F acts as $\mathcal{O}$-module automorphisms on E_{tors}. Thus, we see that:

$$\rho_E(G_F) \subseteq \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) =: \mathcal{G}(E/F) \tag{4}$$

where $\mathcal{G}(E/F)$ is an abelian group canonically isomorphic to $\widehat{\mathcal{O}}^\times$, the unit group of the profinite completion $\widehat{\mathcal{O}} := \varprojlim_N (\mathcal{O}/N\mathcal{O})$. In particular, the extension $F \subseteq F(E_{\mathrm{tors}})$ is abelian. Note also that $\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}})$ is closed inside $\mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}})$, since we have:

$$\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) = \bigcap_{N\in\mathbb{N}} \mathrm{res}_N^{-1}(\mathrm{Aut}_{\mathcal{O}}(E[N]))$$

where $\mathrm{res}_N : \mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}}) \to \mathrm{Aut}_{\mathbb{Z}}(E[N])$ denotes the natural restriction map. On the other hand, $\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}})$ is not open inside $\mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}}) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}})$, because the latter does not contain any abelian subgroup of finite index. However, the subgroup $\rho_E(G_F)$ is open in $\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}})$, as shown in [19, § 4.5] using the classical theorems of complex multiplication. Since $\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) \cong \widehat{\mathcal{O}}^\times$ is a profinite group, this in particular implies that the index of $\rho_E(G_F)$ inside $\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}})$ is finite. We can regard this result as an analogue of Serre's open image theorem for those CM elliptic curves whose field of definition contains the field K.

Assume now that the elliptic curve $E_{/F}$ satisfies $\mathrm{End}_F(E) \cong \mathbb{Z}$ and $\mathrm{End}_{\overline{F}}(E) \cong \mathcal{O}$, for some order $\mathcal{O}$ inside an imaginary quadratic field K. Again by [20, Chapter II, Proposition 30], under these assumptions we must have $K \nsubseteq F$. Since not all the geometric endomorphisms of E are defined over the base field, in this case the Galois group G_F does not respect the $\mathcal{O}$-module structure on E_{tors}. More precisely, since we fixed an embedding $\mathcal{O} \subseteq K \subseteq \overline{\mathbb{Q}} = \overline{F}$, there exists a unique isomorphism $[\cdot]_E : \mathcal{O} \xrightarrow{\sim} \mathrm{End}_{\overline{F}}(E)$ such that for every $\alpha \in \mathcal{O}$ and every invariant differential ω on the elliptic curve $E_{\overline{F}}$, the equality $[\alpha]^*_E(\omega) = \alpha\omega$ holds. then an automorphism $\sigma \in G_F$ acts on $[\alpha]_E(P)$ as:

$$\sigma\left([\alpha]_E(P)\right) = [\sigma(\alpha)]_E(\sigma(P)) \tag{5}$$

as follows from [22, Chapter II, Theorem 2.2]. We then see that for every $\sigma \in G_F$ and each fixed $\tau \in G_F$ restricting to the unique non-trivial element in $\mathrm{Gal}(FK/F)$, exactly one among σ and $\sigma\tau$ acts $\mathcal{O}$-linearly on E_{tors}. We deduce that:

$$\rho_E\left(G_F\right) \subseteq \langle \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}), \rho_E(\tau)\rangle := \mathcal{G}(E/F) \tag{6}$$

and one can easily show that the group $\mathcal{G}(E/F)$ does not actually depend on τ, thus justifying the notation. Indeed, if both $\tau, \tau' \in G_F$ restrict to the unique non-trivial element of $\mathrm{Gal}(FK/F)$, one has that $\tau\tau' \in \mathrm{Gal}(\overline{F}/FK)$, hence $\rho_E(\tau\tau') \in \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}})$, which shows that $\langle \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}), \rho_E(\tau)\rangle = \langle \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}), \rho_E(\tau')\rangle$ as wanted. Moreover, $\rho_E(\tau)$ normalises $\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}})$, as follows from (5) and the fact that $\rho_E(\tau)^2 \in \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}})$. Hence, we see

that $\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}})$ is a normal subgroup of $\mathcal{G}(E/F)$ with index $|\mathcal{G}(E/F) : \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}})| = 2$. As a consequence, $\mathcal{G}(E/F)$ is closed inside $\mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}})$, and so it is a profinite group. On the other hand, $\mathcal{G}(E/F)$ is not open inside $\mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}})$, because it contains the abelian group $\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}})$ as a finite-index subgroup. Thus, $\rho_E(G_F)$ cannot be open inside $\mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}})$. Nevertheless, $\rho_E(G_F)$ is open inside the closed subgroup $\mathcal{G}(E/F)$, as the following lemma shows.

Lemma 2.2. *Let $E_{/F}$ be an elliptic curve with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field $K \not\subseteq F$, and let $E' := E_{FK}$ denote the base-change of E to the compositum FK. Then $\rho_E(G_F)$ is open in $\mathcal{G}(E/F)$, and the following equality:*

$$\mathcal{I}(E/F) := |\mathcal{G}(E/F) : \rho_E(G_F)| = |\mathrm{Aut}_{\mathcal{O}}(E'_{tors}) : \rho_{E'}(G_{FK})| =: \mathcal{I}(E/FK)$$

holds.

Proof. Since $\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}})$ is closed and of finite index in $\mathcal{G}(E/F)$, it is also open in the same group. Moreover, by [19, § 4.5, Corollaire] the inclusion $\rho_{E'}(G_{FK}) \subseteq \mathrm{Aut}_{\mathcal{O}}(E'_{\mathrm{tors}})$ is open, and clearly $\rho_{E'}(G_{FK}) = \rho_E(G_{FK})$ and $\mathrm{Aut}_{\mathcal{O}}(E'_{\mathrm{tors}}) = \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}})$. Thus we see that $\rho_E(G_{FK})$ is an open subgroup of $\rho_E(G_F)$ and we conclude that the latter is open in $\mathcal{G}(E/F)$. In particular, $\rho_E(G_F)$ is a closed subgroup of finite index inside $\mathcal{G}(E/F)$.

To prove the equality of indices, we use the fact that $FK \subseteq F(E_{\mathrm{tors}})$, by [4, Lemma 3.15]. Since ρ_E induces an injective Galois representation $\mathrm{Gal}(F(E_{\mathrm{tors}})/F) \hookrightarrow \mathcal{G}(E/F)$, we have $|\rho_E(G_F) : \rho_E(G_{FK})| = 2$. Now, the computation:

$$|\mathcal{G}(E/F) : \rho_E(G_F)| = \frac{1}{2}\,|\mathcal{G}(E/F) : \rho_E(G_{FK})| = |\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) : \rho_E(G_{FK})|$$

allows us to conclude. □

We summarise our discussion so far. Given a number field F and an elliptic curve $E_{/F}$ with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field K, we define, following (4) and (6):

$$\mathcal{G}(E/F) := \begin{cases} \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) & \text{if } K \subseteq F, \\ \langle \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}), \rho_E(\tau) \rangle & \text{if } K \not\subseteq F \end{cases} \tag{7}$$

where, if $K \not\subseteq F$, we let $\tau \in G_F$ be any automorphism that restricts to the unique non-trivial element of $\mathrm{Gal}(FK/F)$. Then, in the previous discussion, we have shown that $\mathcal{G}(E/F)$ is a profinite group, which contains $\rho_E(G_F)$ as an open subgroup. Moreover, if we define the *CM index* $\mathcal{I}(E/F)$ to be:

$$\mathcal{I}(E/F) := |\mathcal{G}(E/F) : \rho_E(G_F)| \tag{8}$$

then by Lemma 2.2 we have that $\mathcal{I}(E/F) = \mathcal{I}(E/FK)$ is finite.

3. A formula for the index

The aim of this section is to provide a proof of Theorem 1.1. We place ourselves in the setting of the theorem, by fixing an order $\mathcal{O}$ inside an imaginary quadratic field $K \subseteq \overline{\mathbb{Q}}$ and an elliptic curve E which has complex multiplication by $\mathcal{O}$ and is defined over a number field $F \subseteq \overline{\mathbb{Q}}$. We explained in Lemma 2.2 that $\mathcal{I}(E/F) = \mathcal{I}(E/FK)$, hence we will assume without loss of generality that $K \subseteq F$. This in particular implies that $H_{\mathcal{O}} \subseteq F$, where, as in Theorem 1.1, $H_{\mathcal{O}}$ denotes the ring class field of K relative to the order $\mathcal{O}$.

The formula (2) appearing in Theorem 1.1 is a byproduct of the first main theorem of complex multiplication (see [11, Chapter 10, Theorem 8]). The latter asserts the existence of a unique continuous group homomorphism $\mu\colon \mathbb{A}_F^\times \to K^\times$ such that, for every $s \in \mathbb{A}_F^\times$ and every complex uniformisation $\xi\colon \mathbb{C} \twoheadrightarrow E(\mathbb{C})$ with $\Lambda := \ker(\xi) \subseteq K$, the following diagram:

$$\begin{array}{ccc} K/\Lambda & \xrightarrow{\left(\mu(s)\,\mathrm{N}_{F/K}(s^{-1})\right)\cdot} & K/\Lambda \\ \downarrow{\scriptstyle \xi} & & \downarrow{\scriptstyle \xi} \\ E_{\mathrm{tors}} & \xrightarrow{[s,F]} & E_{\mathrm{tors}} \end{array}$$

commutes. Here $\mathrm{N}_{F/K}\colon \mathbb{A}_F^\times \to \mathbb{A}_K^\times$ denotes the idelic norm map, $[\cdot, K]\colon \mathbb{A}_K^\times \twoheadrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$ denotes the global Artin map, and the upper horizontal arrow is given by the idelic multiplication map (see [11, Page 100]). In particular, the action of the idèle $\mu(s)\,\mathrm{N}_{F/K}(s^{-1}) \in \mathbb{A}_K^\times$ on the set of lattices contained in K, described in [11, Chapter 8, Theorem 10], fixes Λ. Since Λ is an invertible fractional ideal of $\mathcal{O}$, this implies that $\mu(s)\,\mathrm{N}_{F/K}(s^{-1})$ fixes also $\mathcal{O}$. Thus, the finite idèle $(\mu(s)\,\mathrm{N}_{F/K}(s^{-1}))_{\mathrm{fin}}$ lies in the subgroup $\widehat{\mathcal{O}}^\times \subseteq \mathbb{A}_K^\times$. Hence, the association $s \mapsto (\mu(s)\,\mathrm{N}_{F/K}(s^{-1}))_{\mathrm{fin}}$ defines a continuous group homomorphism $\theta_E\colon \mathbb{A}_F^\times \to \widehat{\mathcal{O}}^\times$, which makes the following diagram:

$$\begin{array}{ccc} \mathbb{A}_F^\times & \xrightarrow{\quad\theta_E\quad} & \widehat{\mathcal{O}}^\times \\ {\scriptstyle [\cdot,F]|_{F(E_{\mathrm{tors}})}}\big\downarrow & & \big\downarrow{\scriptstyle \wr} \\ \mathrm{Gal}(F(E_{\mathrm{tors}})/F) & \xhookrightarrow{\rho_E} & \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) \end{array} \tag{9}$$

commute. We are now ready to prove Theorem 1.1.

Proof of Theorem 1.1. Define ψ_E to be the surjective group homomorphism:

$$\psi_E : \ \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) \cong \widehat{\mathcal{O}}^\times \xrightarrow{\mathfrak{a}_{\mathcal{O}}} \mathrm{Gal}(K^{\mathrm{ab}}/H_{\mathcal{O}})$$

where $\mathfrak{a}_{\mathcal{O}}\colon \widehat{\mathcal{O}}^\times \twoheadrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/H_{\mathcal{O}})$ is the composition of the natural embedding $\widehat{\mathcal{O}}^\times \hookrightarrow \mathbb{A}_K^\times$ with the map $\mathbb{A}_K^\times \twoheadrightarrow G_K^{\mathrm{ab}}$ given by $s \mapsto [s^{-1}, K]$. It is easy to show that ψ_E fits in a short exact sequence:

$$1 \to \mathrm{Aut}_F(E) \to \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) \xrightarrow{\psi_E} \mathrm{Gal}(K^{\mathrm{ab}}/H_{\mathcal{O}}) \to 1 \tag{10}$$

because $\ker(\mathfrak{a}_{\mathcal{O}}) = \ker([\cdot, K]) \cap \widehat{\mathcal{O}}^\times = K^\times \cap \widehat{\mathcal{O}}^\times = \mathcal{O}^\times$. Then, we can form the following square:

$$\begin{array}{ccc} \mathrm{Gal}(F(E_{\mathrm{tors}})/F) & \xhookrightarrow{\rho_E} & \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) \\ \big\downarrow & & \big\downarrow{\scriptstyle \psi_E} \\ \mathrm{Gal}(K^{\mathrm{ab}}/F \cap K^{\mathrm{ab}}) & \xhookrightarrow{\iota} & \mathrm{Gal}(K^{\mathrm{ab}}/H_{\mathcal{O}}) \end{array} \tag{11}$$

where the map on the left is defined by the composition:

$$\mathrm{Gal}(F(E_{\mathrm{tors}})/F) \twoheadrightarrow \mathrm{Gal}(FK^{\mathrm{ab}}/F) \xrightarrow{\sim} \mathrm{Gal}(K^{\mathrm{ab}}/F \cap K^{\mathrm{ab}})$$

of a restriction map and a natural isomorphism coming from Galois theory. We claim that (11) commutes. Indeed, extending (11) by diagram (9) gives the following square:

$$\begin{array}{ccc} \mathbb{A}_F^\times & \xrightarrow{\quad\theta_E\quad} & \widehat{\mathcal{O}}^\times \\ {\scriptstyle [\cdot,F]|_{K^{\mathrm{ab}}}}\big\downarrow & & \big\downarrow{\scriptstyle \mathfrak{a}_{\mathcal{O}}} \\ \mathrm{Gal}(K^{\mathrm{ab}}/F \cap K^{\mathrm{ab}}) & \xhookrightarrow{\iota} & \mathrm{Gal}(K^{\mathrm{ab}}/H_{\mathcal{O}}) \end{array} \tag{12}$$

which commutes because, for every $s \in \mathbb{A}_F^\times$, one has:

$$\mathfrak{a}_{\mathcal{O}}(\theta_E(s)) = [(\mu(s) \cdot \mathrm{N}_{F/K}(s^{-1}))^{-1}, K] = [\mathrm{N}_{F/K}(s), K] = \iota([s, F]|_{K^{\mathrm{ab}}})$$

using the fact that $K^\times \cdot (K \otimes_{\mathbb{Q}} \mathbb{R})^\times \subseteq \ker([\cdot, K])$, as explained in [1, Chapter IX, Theorem 3], and the functoriality of class field theory [15, Chapter VI, Proposition 5.2]. Thus (11) commutes, because (12) does, and the vertical maps in the commutative diagram (9) are surjective.

Now, (10) and (11) induce the following commutative diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(F(E_{\mathrm{tors}})/FK^{\mathrm{ab}}) & \longrightarrow & \mathrm{Gal}(F(E_{\mathrm{tors}})/F) & \longrightarrow & \mathrm{Gal}(K^{\mathrm{ab}}/F\cap K^{\mathrm{ab}}) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \iota'} & & \downarrow{\scriptstyle \rho_E} & (11) & \downarrow{\scriptstyle \iota} & & \\ 1 & \longrightarrow & \mathrm{Aut}_F(E) & \longrightarrow & \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) & \xrightarrow[\psi_E]{} & \mathrm{Gal}(K^{\mathrm{ab}}/H_{\mathcal{O}}) & \longrightarrow & 1 \end{array} \tag{13}$$

whose rows are exact. This shows in particular that the degree of the extension $FK^{\mathrm{ab}} \subseteq F(E_{\mathrm{tors}})$ is finite and divides $|\mathrm{Aut}_F(E)| = |\mathcal{O}^\times|$. Finally, the snake lemma gives:

$$\mathcal{I}(E/F) = |\mathrm{coker}(\rho_E)| = |\mathrm{coker}(\iota)| \cdot |\mathrm{coker}(\iota')| = [F\cap K^{\mathrm{ab}} : H_{\mathcal{O}}] \cdot \frac{|\mathcal{O}^\times|}{[F(E_{\mathrm{tors}}) : FK^{\mathrm{ab}}]}$$

which allows us to conclude. □

An immediate consequence of Theorem 1.1 is the following improvement of the bounds provided by [13, Theorem 6.6] and [3, Corollary 1.5].

Corollary 3.1. *Let $\mathcal{O}$ be an order inside an imaginary quadratic field K. For every number field $F \subseteq \overline{\mathbb{Q}}$, and every elliptic curve $E_{/F}$ with complex multiplication by $\mathcal{O}$, the index $\mathcal{I}(E/F)$ divides $[(FK)\cap K^{ab} : H_{\mathcal{O}}] \cdot |\mathcal{O}^\times|$.*

Moreover, Theorem 1.1 can be rephrased in a simpler fashion, if one assumes that $|\mathcal{O}^\times| = 2$, which holds for every order $\mathcal{O}$ of discriminant $\Delta_{\mathcal{O}} < -4$.

Corollary 3.2. *Let $\mathcal{O}$ be an order inside an imaginary quadratic field K, and suppose that $\Delta_{\mathcal{O}} < -4$. Let E be an elliptic curve with complex multiplication by $\mathcal{O}$, defined over a number field $F \subseteq \overline{\mathbb{Q}}$. Then, the following equality:*

$$\frac{\mathcal{I}(E/F)}{[(FK)\cap K^{ab} : H_{\mathcal{O}}]} = \begin{cases} 2, & \text{if } F(E_{tors}) = FK^{ab} \\ 1, & \text{otherwise} \end{cases} \tag{14}$$

holds.

The dichotomy provided by (14) reflects a property of CM elliptic curves introduced by Shimura in [21, Pages 216-218], and studied in [5, § 5]. In particular, Corollary 3.2 generalises [5, Corollary 5.8], which was proved by different means.

Remark 3.3. Specializing Theorem 1.1 to $F = \mathbb{Q}(j(E))$ we see that $\mathcal{I}(E/F) \in \{1, |\mathcal{O}^\times|\}$. However, this does not allow to describe explicitly the image $\rho_E(G_F)$ as a subgroup of $\mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}}) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}})$, since the latter can vary amongst infinitely many possible subgroups, as it happens already for $F = \mathbb{Q}$ (see [5, Theorem 6.3]). On the other hand, the image of $\rho_E(G_F)$ under the natural projections $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$ for $\ell \in \mathbb{N}$ a prime, belongs, up to conjugation, to a finite list of subgroups which has been explicitly determined by Lozano-Robledo [14].

To conclude this section, we observe that Theorem 1.1 implies that the index $\mathcal{I}(E/F)$ is invariant under appropriate twisting of the elliptic curve E, as specified by the following corollary.

Corollary 3.4. *Let $\mathcal{O}$ be an order inside an imaginary quadratic field K, and set $d := |\mathcal{O}^\times|$. Let $E_{/F}$ be an elliptic curve defined over a number field $F \subseteq \overline{\mathbb{Q}}$ such that $\mathrm{End}_F(E) \cong \mathcal{O}$. Suppose that E is the twist of another elliptic curve $E'_{/F}$ by $\sqrt[d]{\alpha}$, for some $\alpha \in F^\times$ such that $L := F(\sqrt[d]{\alpha}) \subseteq FK^{ab}$. Then $\mathcal{I}(E/F) = \mathcal{I}(E'/F)$.*

Proof. First of all, note that the extension $F \subseteq L$ is well defined, because we have the inclusion $K \subseteq F$, by the hypothesis $\mathrm{End}_F(E) \cong \mathcal{O}$. Thus, the group of d-th roots of unity $\mathcal{O}^\times$ is also contained in F. Then, one has:

$$\rho_E(\sigma) = \rho_{E'}(\sigma) \cdot \chi_\alpha(\sigma) \tag{15}$$

for every $\sigma \in G_F$, where $\rho_E : G_F \to \mathcal{G}(E/F) \cong \widehat{\mathcal{O}}^\times$ and $\rho_{E'} : G_F \to \mathcal{G}(E'/F) \cong \widehat{\mathcal{O}}^\times$ are the Galois representations associated to E and E'. Moreover, $\chi_\alpha : G_F \to \mathcal{O}^\times \subseteq \widehat{\mathcal{O}}^\times$ is the Kummer character attached to the extension $F \subseteq L$, defined by the equality $\sigma(\sqrt[d]{\alpha}) = \chi_\alpha(\sigma) \cdot \sqrt[d]{\alpha}$ for every $\sigma \in G_F$.

Now, for every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/LF(E'_{\mathrm{tors}}))$, we have that $\rho_{E'}(\sigma) = \chi_\alpha(\sigma) = 1$, hence (15) implies that $\rho_E(\sigma) = 1$. Thus, the inclusion $F(E_{\mathrm{tors}}) \subseteq LF(E'_{\mathrm{tors}})$ holds. On the other hand, if $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/F(E_{\mathrm{tors}}))$, the hypothesis $L \subseteq FK^{\mathrm{ab}}$ and the inclusion $FK^{\mathrm{ab}} \subseteq F(E_{\mathrm{tors}})$ imply that τ fixes L, and thus that $\rho_E(\tau) = \chi_\alpha(\tau) = 1$. Therefore, (15) gives that $\rho_{E'}(\tau) = 1$. Hence, the opposite inclusion $LF(E'_{\mathrm{tors}}) \subseteq F(E_{\mathrm{tors}})$ holds. Thus, we have that $F(E_{\mathrm{tors}}) = LF(E'_{\mathrm{tors}}) = F(E'_{\mathrm{tors}})$, where the last equality follows from the hypothesis $L \subseteq FK^{\mathrm{ab}}$ and the inclusion $FK^{\mathrm{ab}} \subseteq F(E'_{\mathrm{tors}})$. Finally, using Theorem 1.1, one gets that $\mathcal{I}(E/F) = \mathcal{I}(E'/F)$, as we wanted to prove. □

4. How to compute the index in practice

In this section we show how one can concretely compute the index $\mathcal{I}(E/F)$ for any given CM elliptic curve E defined over a number field F. Thanks to Lemma 2.2, we can and will assume throughout this section, without loss of generality, that the number field F contains the CM field K.

The starting point of our discussion is the formula (2) provided by Theorem 1.1. Let us observe that (2), albeit completely explicit, involves the degree of the finite extension $FK^{\mathrm{ab}} \subseteq F(E_{\mathrm{tors}})$ which *a priori* can not be implemented in a computer, because FK^{ab} is an infinite algebraic extension of $\mathbb{Q}$. Nevertheless, the following result shows how one can rewrite (2) as an equality involving only finite abelian groups and number fields.

Proposition 4.1. *Let $\mathcal{O}$ be an order inside an imaginary quadratic field $K \subseteq \overline{\mathbb{Q}}$. Fix a number field $F \subseteq \overline{\mathbb{Q}}$ and an elliptic curve $E_{/F}$ such that $\mathrm{End}_F(E) \cong \mathcal{O}$. Then, we have:*

$$\mathcal{I}(E/F) = \frac{|\mathcal{O}^\times| \cdot [L \cap K^{ab} : K]}{|\mathrm{Pic}(\mathcal{O})| \cdot [L : F]} \tag{16}$$

for every finite extension $F \subseteq L$ such that $F(E_{tors}) = LK^{ab}$ is the compositum of L and K^{ab} inside $\overline{\mathbb{Q}}$.

Proof. Combining Theorem 1.1 with the equality:

$$[F(E_{\mathrm{tors}}) : FK^{\mathrm{ab}}] = [LK^{\mathrm{ab}} : FK^{\mathrm{ab}}] = \frac{[L : F]}{[L \cap K^{\mathrm{ab}} : F \cap K^{\mathrm{ab}}]} = \frac{[L : F][F \cap K^{\mathrm{ab}} : K]}{[L \cap K^{\mathrm{ab}} : K]}$$

allows us to conclude, because $[F \cap K^{\mathrm{ab}} : K] = [F \cap K^{\mathrm{ab}} : H_{\mathcal{O}}] \cdot |\mathrm{Pic}(\mathcal{O})|$. □

Using Proposition 4.1, we can now reduce the computation of $\mathcal{I}(E/F)$ to the following steps:

S.1 compute $|\mathcal{O}^\times|$ and $|\mathrm{Pic}(\mathcal{O})|$;
S.2 find a finite extension $F \subseteq L$ such that $F(E_{\mathrm{tors}}) = LK^{\mathrm{ab}}$, and compute $[L : F]$;
S.3 compute $[L \cap K^{\mathrm{ab}} : K]$, *i.e.* the degree of the maximal abelian sub-extension of $K \subseteq L$.

To achieve S.1 one can use for instance the algorithms described in [7, § 5.3] for the computation of $|\mathrm{Pic}(\mathcal{O})|$, and the fact that $|\mathcal{O}^\times| = 2$ unless $\mathcal{O} = \mathbb{Z}[i]$, for which $|\mathcal{O}^\times| = 4$, or $\mathcal{O} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, for which $|\mathcal{O}^\times| = 6$. Moreover, once S.2 has been carried out, and the extension $F \subseteq L$ is known, one can deal with the last step S.3 in (at least) two different ways:

- one can use the isomorphism:

$$\mathrm{Gal}(L \cap K^{\mathrm{ab}}/K) \cong \mathrm{Gal}(L'/K)^{\mathrm{ab}} \tag{17}$$

  where $K \subseteq L' \subseteq L$ denotes the maximal sub-extension of $K \subseteq L$ which is Galois over K and the notation S^{ab} stands for the abelianization of a finite group S (*i.e.* its maximal abelian quotient). In order to compute the right hand side of (17), note that, if $G := \mathrm{Gal}(\widetilde{L}/K)$ denotes the Galois group of the Galois closure $\widetilde{L}$ of the extension $K \subseteq L$, and $H^G \subseteq G$ denotes the normal closure of the subgroup $H := \mathrm{Gal}(\widetilde{L}/L)$ inside G, then we have $\mathrm{Gal}(L'/K) \cong G/H^G$. Since both G and H can be computed as subgroups of the symmetric group $\mathfrak{S}_n$ on $n = [L : K]$ letters (see [7, § 6.3]), the abelian group $(G/H^G)^{\mathrm{ab}}$ can also be explicitly computed, for instance using the functions NormalClosure and MaximalAbelianQuotient in GAP [10];

- one can compute $[L \cap K^{\mathrm{ab}} : K]$ as the index of the norm group $\mathrm{T}_{\mathfrak{m}}(L/K) \subseteq \mathrm{Cl}_{\mathfrak{m}}(K)$, where $\mathfrak{m} := \delta_{L/K}$ is the relative discriminant of $K \subseteq L$, and $\mathrm{Cl}_{\mathfrak{m}}(K)$ denotes the ray class group of K modulo $\mathfrak{m}$ (see [15, Chapter VI, § 7]). This norm group $\mathrm{T}_{\mathfrak{m}}(L/K)$ can be computed using an adaptation of [8, Algorithm 4.4.5] to the non-Galois case. More precisely:
  - in the fourth step of the aforementioned algorithm, one can proceed even if the polynomials T_j do not have the same degree, by taking as f the greatest common divisor of their degrees. Indeed, $\mathrm{T}_{\mathfrak{m}}(L/K)$ is by definition generated by the classes of $\mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}$, where $\mathfrak{p} := \mathfrak{P} \cap O_K$ and $\mathfrak{P}$ varies amongst the prime ideals of O_L coprime with $\mathfrak{m} \cdot O_L$, and the inertia degrees $f(\mathfrak{P}/\mathfrak{p})$ correspond exactly to the degrees of the polynomials T_j mentioned above;
  - in the second step of the same algorithm, one should always output the matrix M even if $\det(M) \neq [L : K]$. In fact, $\det(M)$ will be precisely the index of the norm group inside $\mathrm{Cl}_{\mathfrak{m}}(K)$, *i.e.* the equality $[L \cap K^{\mathrm{ab}} : K] = \det(M)$ holds.

  Note that this modification does indeed work (assuming the validity of the Generalised Riemann Hypothesis), because $\mathrm{T}_{\mathfrak{m}}(L/K) = \mathrm{T}_{\mathfrak{m}}(L \cap K^{\mathrm{ab}}/K)$ by [1, Chapter XIV, Theorem 7].

Thus, in order to have a complete procedure for the computation of the CM index $\mathcal{I}(E/F)$, we only need to prove that one can always find a finite extension $F \subseteq L$ such that $F(E_{\mathrm{tors}}) = LK^{\mathrm{ab}}$ as in S.2. The next proposition shows that one can take L to be essentially any division field.

Proposition 4.2. *Let O be an order inside an imaginary quadratic field K and let $E_{/F}$ be an elliptic curve defined over a number field $F \subseteq \overline{\mathbb{Q}}$ such that $\mathrm{End}_F(E) \cong O$. Fix an ideal $I \subseteq O$ and let $L := F(E[I])$ be the I-division field associated to E. Then $F(E_{tors}) = LK^{ab}$ whenever $|\mathbb{Z}/(I \cap \mathbb{Z})| > 2$ if $j(E) \neq 0$, and $|\mathbb{Z}/(I \cap \mathbb{Z})| > 3$ otherwise.*

Proof. The inclusion $LK^{\mathrm{ab}} \subseteq F(E_{\mathrm{tors}})$ is clear, and the other containment can be proved as in [5, Proposition 5.7]. More precisely, fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and a complex uniformisation $\xi : \mathbb{C} \twoheadrightarrow E(\mathbb{C})$, such that $\ker(\xi) = \Lambda$ for some lattice $\Lambda \subseteq K$. Then [21, Theorem 5.4] shows that, for every field automorphism $\sigma : \mathbb{C} \to \mathbb{C}$ which fixes FK^{ab}, there exists a complex uniformisation $\xi' : \mathbb{C} \twoheadrightarrow E(\mathbb{C})$ such that $\sigma(\xi(z)) = \xi'(z)$ for every $z \in K$. This implies in particular that there exists $\varepsilon \in O^\times$ such that $\sigma(P) = [\varepsilon]_E(P)$ for every $P \in E_{\mathrm{tors}}$. If now σ fixes also the division field $L = F(E[I])$, one must have $\varepsilon = 1$ by our assumptions on I. We conclude that σ fixes the entire $F(E_{\mathrm{tors}})$, which in turn implies that $F(E_{\mathrm{tors}}) \subseteq LK^{\mathrm{ab}}$ as we wanted to show. □

Using Proposition 4.2, we see that S.1, S.2 and S.3 indeed describe a procedure to compute the index $\mathcal{I}(E/F)$ for any CM elliptic curve defined over any number field F. In practice, in S.2 it is convenient to choose a "small" division field $L = F(E[I])$, for instance by using $I = 3O$ (when $j(E) \neq 0$), which gives $[L : F] \leq 8$. However, if one already knows an elliptic curve $E'_{/F}$ such that $j(E') = j(E)$ and $F(E'_{\mathrm{tors}}) = FK^{\mathrm{ab}}$, then the subsequent Proposition 4.3, whose proof is analogous to that of Corollary 3.4, shows that one can take L to be a Kummer extension of F with degree $[L : F] \leq |O^\times| \leq 6$. Since computations involving division fields of elliptic curves are typically hard, taking such an L is certainly more advantageous in this situation.

Proposition 4.3. *Let O be an order inside an imaginary quadratic field K, and set $d := |O^\times|$. Let $E_{/F}$ be an elliptic curve defined over a number field $F \subseteq \overline{\mathbb{Q}}$ such that $\mathrm{End}_F(E) \cong O$. Suppose that there exists another elliptic curve $E'_{/F}$ such that $F(E'_{tors}) = FK^{ab}$, and that E is the twist of E' by $\sqrt[d]{\alpha}$, for some $\alpha \in F^\times$. Then $F(E_{tors}) = LK^{ab}$, where $L = F(\sqrt[d]{\alpha})$.*

Proof. If $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/LF(E'_{\mathrm{tors}}))$, we see from the twisting formula (15) that $\rho_{E'}(\sigma) = \chi_\alpha(\sigma) = \rho_E(\sigma) = 1$, hence $F(E_{\mathrm{tors}}) \subseteq LF(E'_{\mathrm{tors}})$. Vice versa, if $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/F(E_{\mathrm{tors}}))$ then $\rho_E(\tau) = 1$ and $\rho_{E'}(\tau) = \chi_\alpha(\tau^{-1}) \in O^\times$. However, (13) shows that $\rho_{E'}(G_F) \cap O^\times = \{1\}$, because $F(E'_{\mathrm{tors}}) = FK^{\mathrm{ab}}$ by assumption. Hence $\rho_{E'}(\tau) = \chi_\alpha(\tau) = 1$, which allows us to conclude that $F(E_{\mathrm{tors}}) = LF(E'_{\mathrm{tors}}) = LK^{\mathrm{ab}}$, as we wanted to show. □

Remark 4.4. Note that the condition $F(E'_{\mathrm{tors}}) = FK^{\mathrm{ab}}$ is invariant under base change along a finite extension $F \subseteq F'$. In particular, if $\mathrm{Pic}(O) = \{1\}$, one can take as E' any base change to F of an elliptic curve $E_{/K}$ which

has complex multiplication by $\mathcal{O}$. On the other hand, if $\mathrm{Pic}(\mathcal{O}) \neq \{1\}$, constructing such an elliptic curve is a non-trivial matter, as we will see in the next section.

5. Explicit examples

We now want to provide some examples of index computations for CM elliptic curves E defined over the corresponding field of moduli $\mathbb{Q}(j(E))$. A way of constructing such curves is to consider an elliptic curve $\mathcal{E}$ defined over the function field $\mathbb{Q}(j)$, with j-invariant $j(\mathcal{E}) = j$ and discriminant $\Delta_{\mathcal{E}} \in \mathbb{Q}(j)$, and then specialise the parameter to $j = j_0$ for some CM j-invariant $j_0 \in \overline{\mathbb{Q}}$ such that $\Delta_{\mathcal{E}}(j_0) \neq 0$. When we want to emphasize that the specialization at j_0 of the elliptic curve $\mathcal{E}$ has complex multiplication by some order $\mathcal{O}$, we say that $j_0 \in \overline{\mathbb{Q}}$ is *relative to the order* $\mathcal{O}$. With a view towards doing explicit calculations in the mostly popular computer algebra systems in computational number theory, we consider and compare the following choices of $\mathcal{E}$:

(1) the curve:
$$\mathcal{E}_{\mathrm{SAGE}} : y^2 = x^3 + (-3j^2 + 5184j)x - 2j^3 + 6912j^2 - 5971968j$$
implemented in SageMath [18] under the command EllipticCurve_from_j(j,False). We warn the reader that, without setting the second optional parameter equal to False, the command EllipticCurve_from_j, applied to a rational number $j_0 \in \mathbb{Q}$, returns an elliptic curve $E_{/\mathbb{Q}}$ which has j-invariant $j(E) = j_0$, and minimal conductor among all its twists. This curve, in general, can be different from the specialization of $\mathcal{E}_{\mathrm{SAGE}}$ at $j = j_0$;

(2) the curve:
$$\mathcal{E}_{\mathrm{PARI}} : y^2 = x^3 + (-3j^2 + 5184j)x + 2j^3 - 6912j^2 + 5971968j$$
implemented in PARI/GP [16] under the command ellfromj(j);

(3) the curve:
$$\mathcal{E}_{\mathrm{MAGMA}} : y^2 + xy = x^3 - \frac{36}{j - 1728}x - \frac{1}{j - 1728}$$
implemented in MAGMA [2] under the command EllipticCurveFromjInvariant(j).

The above families are clearly all defined over $\mathbb{Q}(j)$, and their singular specializations occur only at the values $j_0 \in \{0, 1728\}$. Moreover, it is easily verified that $\mathcal{E}_{\mathrm{PARI}}$ and $\mathcal{E}_{\mathrm{SAGE}}$ are isomorphic over $\mathbb{Q}(j, \sqrt{-1})$ while $\mathcal{E}_{\mathrm{SAGE}}$ and $\mathcal{E}_{\mathrm{MAGMA}}$ are isomorphic over $\mathbb{Q}\left(j, \sqrt{\frac{1728-j}{3}}\right)$.

Now, for every CM j-invariant $j_0 \in \overline{\mathbb{Q}}$ relative to an order of class number 2, we want to compute the index $\mathcal{I}(E_{j_0}/\mathbb{Q}(j_0))$ where E_{j_0} is the fiber over j_0 in any of the three families described above (one can check that all these fibers are non-singular). First of all, we show that for every CM invariant $j_0 \in \overline{\mathbb{Q}}$ the CM fibers E_{j_0} in the above families have the same index $\mathcal{I}(E_{j_0}/\mathbb{Q}(j_0))$.

Fix now a CM j-invariant $j_0 \in \overline{\mathbb{Q}} \setminus \{0, 1728\}$ relative to an order $\mathcal{O}$. Let moreover $(E_{j_0}, E'_{j_0}, E''_{j_0})$ be the specialisations of the families $(\mathcal{E}_{\mathrm{SAGE}}, \mathcal{E}_{\mathrm{PARI}}, \mathcal{E}_{\mathrm{MAGMA}})$ to $j = j_0$. If $H_{\mathcal{O}} = K(j_0)$ denotes the ring class field relative to the order $\mathcal{O}$ then by Lemma 2.2 we have $\mathcal{I}(E_{j_0}/\mathbb{Q}(j_0)) = \mathcal{I}(E_{j_0}/H_{\mathcal{O}})$ and similarly with the other two elliptic curves, so we assume that everything is base-changed to the ring class field. Since by the discussion above E_{j_0} and E'_{j_0} are twisted over $H_{\mathcal{O}}$ by $\alpha = -1$ and $H_{\mathcal{O}}(\sqrt{-1}) \subseteq K^{\mathrm{ab}}$ (being the compositum of two abelian extensions of K), Corollary 3.4 allows us to conclude that $\mathcal{I}(E_{j_0}/\mathbb{Q}(j_0)) = \mathcal{I}(E'_{j_0}/\mathbb{Q}(j_0))$. Furthermore, the elliptic curve $\mathcal{E}_{\mathrm{MAGMA}}$ admits a short Weierstraß form:
$$y^2 = x^3 - \left(\frac{27j}{j - 1728}\right)x + \frac{54j}{j - 1728}$$
whose discriminant is given by $\Delta_j := 6^{12} \cdot j^2/(j - 1728)^3$. Thus, we see that:
$$H_{\mathcal{O}}(\sqrt{j_0 - 1728}) = H_{\mathcal{O}}(\sqrt{\Delta_{j_0}}) \subseteq H_{\mathcal{O}}(E''_{j_0}[2])$$

for every CM j-invariant $j_0 \in \overline{\mathbb{Q}}$, relative to the order $\mathcal{O}$. Since $H_{\mathcal{O}}(E''_{j_0}[2])$ is generated over $H_{\mathcal{O}}$ by the Weber functions evaluated at 2-torsion points, we have that $H_{\mathcal{O}}(E''_{j_0}[2]) \subseteq K^{\mathrm{ab}}$ (see [5, Theorem 4.7]). Thus $H_{\mathcal{O}}\left(\sqrt{(1728-j_0)/3}\right)$ is abelian over K, and Corollary 3.4 shows that $\mathcal{I}(E_{j_0}/\mathbb{Q}(j_0)) = \mathcal{I}(E''_{j_0}/\mathbb{Q}(j_0))$. Hence, we can conclude that the three families $\mathcal{E}_{\mathrm{PARI}}, \mathcal{E}_{\mathrm{SAGE}}$ and $\mathcal{E}_{\mathrm{MAGMA}}$, when specialised to the same CM j-invariant, have the same CM index. We will use in the rest of the paper, the elliptic curves E_{j_0} obtained by specialising the family $\mathcal{E}_{\mathrm{SAGE}}$. Note that, once the imaginary quadratic order $\mathcal{O}$ is fixed, the index $\mathcal{I}(E_{j_0}/\mathbb{Q}(j_0))$ does not depend on the particular j-invariant $j_0 \in \overline{\mathbb{Q}}$ relative to $\mathcal{O}$ to which one specializes the family $\mathcal{E}_{\mathrm{SAGE}}$, because all these j-invariants are conjugate under the action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (see [9, Proposition 13.2]).

Let us turn now to the computation of the index $\mathcal{I}(E_{j_0}/\mathbb{Q}(j_0))$, where $j_0 \in \overline{\mathbb{Q}}$ is a CM j-invariant relative to an order of class number 2. The procedure described in Section 4 simplifies considerably in this case. Indeed, in general, for any imaginary quadratic order $\mathcal{O} \neq \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ and any elliptic curve E with complex multiplication by $\mathcal{O}$ and defined over the ring class field $H_{\mathcal{O}}$, one has that:

$$\mathcal{I}(E/H_{\mathcal{O}}) = \frac{2}{[H_{\mathcal{O}}(E[3]) : H_{\mathcal{O}}(E[3]) \cap K^{\mathrm{ab}}]} \tag{18}$$

as one can see by combining Proposition 4.1 and Proposition 4.2. Moreover, since:

$$[H_{\mathcal{O}}(E[3]) : H_{\mathcal{O}}(E[3]) \cap K^{\mathrm{ab}}] = \begin{cases} 1, & \text{if the extension } K \subseteq H_{\mathcal{O}}(E[3]) \text{ is abelian;} \\ 2, & \text{otherwise (as follows from (18), since } \mathcal{I}(E/H_{\mathcal{O}}) \in \mathbb{N}), \end{cases}$$

we see, using Lemma 2.2, that the computation of $\mathcal{I}(E_{j_0}/\mathbb{Q}(j_0))$ reduces to understanding whether or not the 3-division field of E_{j_0} is an abelian extension of K. We implemented this computation in SageMath (importing also the functions polredbest and rnfisabelian from Pari/Gp), as shown in Algorithm 5.1. We ran this algorithm for all the j-invariants relative to orders $\mathcal{O}$ of class number 2, whose discriminants $\Delta_{\mathcal{O}}$ are given by the following list:

$$\begin{aligned} \Delta_{\mathcal{O}} \in \{ &-15, -20, -24, -32, -35, -36, -40, -48, -51, -52, -60, -64, -72, -75, -88, -91, \\ &-99, -100, -112, -115, -123, -147, -148, -187, -232, -235, -267, -403, -427\} \end{aligned}$$

Input: Delta = $\Delta_{\mathcal{O}}$, the discriminant of $\mathcal{O}$.

```
from sage.libs.pari.convert_sage import gen_to_sage
R.<x> = PolynomialRing(QQ)
K.<D> = NumberField(x^2-Delta)
F.<j> = K.extension(hilbert_class_polynomial(Delta))
E = EllipticCurve_from_j(j,F)
Fabs.<a> = NumberField(gen_to_sage(pari(F.absolute_polynomial()).polredbest(),{'x' : x}) )
Eabs = E.base_extend(F.embeddings(Fabs)[0])
F3.<f3> = Eabs.division_field(3)
F3best.<f3best> = NumberField(gen_to_sage(pari(F3.absolute_polynomial()).polredbest(),{'x' : x}) )
F3rel.<f3rel> = F3best.relativize(K.embeddings(F3best)[0])
if F3rel.is_galois_relative() == True:
    Index = gp.rnfisabelian(pari('y^2 + '+str(-Delta)).nfinit() ,pari(F3rel.relative_polynomial())) + 1
else:
    Index = 1
```

Output: Index = $\mathcal{I}(E_{j_0}/\mathbb{Q}(j_0))$, for any CM j-invariant j_0 relative to the order $\mathcal{O}$

Algorithm 5.1. SageMath code to compute the index $\mathcal{I}(E_{j_0}/\mathbb{Q}(j_0))$, relative to the elliptic curve E_{j_0} obtained by specialising the family $\mathcal{E}_{\mathrm{SAGE}}$ to a CM j-invariant j_0.

which can be obtained either by applying the algorithms described in [25], and implemented in SageMath under the function SAGE.SCHEMES.ELLIPTIC_CURVES.CM.DISCRIMINANTS_WITH_BOUNDED_CLASS_NUMBER, or by appealing to the classical result [24, Theorem 1], and then applying the class number formula [9, Theorem 7.24]. The results of this computation show that $\mathcal{I}(E_{j_0}/\mathbb{Q}(j_0)) = 1$ unless $\Delta_{\mathcal{O}} = -15$, in which case $\mathcal{I}(E_{j_0}/\mathbb{Q}(j_0)) = 2$.

To conclude, consider the order $\mathcal{O} = \mathbb{Z}[\sqrt{-5}]$ of discriminant $\Delta_{\mathcal{O}} = -20$, such that $\mathcal{I}(E_{j_0}/\mathbb{Q}(j_0)) = 1$ for every CM j-invariant $j_0 \in \overline{\mathbb{Q}}$ relative to $\mathcal{O}$. We now construct, by a suitable twist of $E := E_{j_0}$ over the Hilbert class field $H := H_{\mathcal{O}}$, another elliptic curve $E'_{/H}$ with complex multiplication by $\mathcal{O}$, with the property that $\mathcal{I}(E'/H) = 2$. To do so, we specialize $j_0 = 282880\sqrt{5} + 632000$, so that $E := E_{j_0}$ is given by:

$$E\colon y^2 = x^3 + 29736960(36023\sqrt{5} - 80550)x - 55826186240(16154216\sqrt{5} + 36121925) \tag{19}$$

and we follow the procedure described in the proof of [5, Theorem 5.11].

More precisely, observe that $H = \mathbb{Q}(\sqrt{-5}, i)$ and $3 \cdot \mathcal{O} = \mathfrak{p}_3 \cdot \overline{\mathfrak{p}}_3$ with $\mathfrak{p}_3 = (3, \sqrt{-5}+1)$ and $\overline{\mathfrak{p}}_3 = (3, \sqrt{-5}-1)$. By [5, Theorem 4.6] one has that $H_{\mathfrak{p}_3} = H_{\overline{\mathfrak{p}}_3} = H$, where $H_{\mathfrak{p}_3}$ and $H_{\overline{\mathfrak{p}}_3}$ denote respectively the ray class fields of K modulo $\mathfrak{p}_3$ and $\overline{\mathfrak{p}}_3$. This in particular implies, using [22, Chapter II, Theorem 5.6], that the x-coordinates of the points $P \in E[\mathfrak{p}_3] \cup E[\overline{\mathfrak{p}}_3]$ lie in H. Moreover, it follows from [3, Lemma 2.4] that $|E[\mathfrak{p}_3]| = |E[\overline{\mathfrak{p}}_3]| = 3$, which shows that each non-trivial $\mathfrak{p}_3$-torsion point has the same x-coordinate, and similarly for non-trivial $\overline{\mathfrak{p}}_3$-torsion points. From the factorization:

$$\begin{aligned}\phi_{E,3}(x) = 3\cdot&(x + 594880 + 59840i - 26048\sqrt{-5} + 266816\sqrt{5})\cdot\\ &(x + 594880 - 59840i + 26048\sqrt{-5} + 266816\sqrt{5})\cdot\\ &(x^2 - (1189760 + 533632\sqrt{5})x - 2668089262080 - 1193205432320\sqrt{5})\end{aligned}$$

of the 3-division polynomial $\phi_{E,3} \in H[x]$, one can verify that $x_3 := -594880 - 59840i + 26048\sqrt{-5} - 266816\sqrt{5}$ is the x-coordinate of all the non-trivial $\mathfrak{p}_3$-torsion points. Hence $H(E[\mathfrak{p}_3]) = H(\sqrt{\alpha})$, where:

$$\alpha := 13956546560 \cdot (1190435 + 2307955i - 1032149\sqrt{-5} + 532379\sqrt{5})$$

is obtained by substituting x_3 in the right hand side of (19). It can be checked that the extension $K \subseteq H(\sqrt{\alpha})$ is not Galois, and in particular not abelian, which is compatible with the fact that $\mathcal{I}(E/\mathbb{Q}(j_0)) = 1$.

Thus, the twisted elliptic curve $E' := E^{(\alpha)}$, given by the global minimal Weierstraß model:

$$E'\colon y^2 - \left(\frac{1 - i + \sqrt{-5} + \sqrt{5}}{2}\right)xy - \left(\frac{1 + i + \sqrt{-5} + \sqrt{5}}{2}\right)y = x^3 + x^2 + \left(2i - \sqrt{5}\right)x - 1 + 2i \tag{20}$$

has index $\mathcal{I}(E'/H) = 2$, as follows from (18). Indeed, the first point of [5, Proposition 5.1] implies that $H(E'[\mathfrak{p}_3]) = H_{\mathfrak{p}_3}$, which entails that $H(E'[3])$ coincides with the 3-ray class field of K, as can also be checked by direct computation. Note finally that $H(E'_{\mathrm{tors}}) = K^{\mathrm{ab}}$, as follows from Corollary 3.2.

Remark 5.1. The interested reader can find at [6] a SageMath notebook in which we implemented the computations carried out to find the elliptic curve E' appearing in (20).

Acknowledgements

We would like to thank François Brunault, Ian Kiming, Fabien Pazuki and Peter Stevenhagen for many useful discussions. We also thank the anonymous referees for their helpful comments and suggestions.

The first author is supported by ANR-20-CE40-0003 Jinvariant. Moreover, he wishes to thank the Max Planck Institute for Mathematics in Bonn for its financial support, great work conditions and an inspiring atmosphere.

The second author performed this work within the framework of the LABEX MILYON (ANR-10-LABX-0070) of Université de Lyon, within the program "Investissements d'Avenir" (ANR-11-IDEX-0007) operated by the French National Research Agency (ANR).

References

[1] E. Artin and J. Tate. *Class field theory*. W. A. Benjamin, Inc., New York-Amsterdam, 1968 (cit. on pp. 5, 8).

[2] W. Bosma, J. Cannon, and C. Playoust. "The Magma algebra system. I. The user language". In: *J. Symbolic Comput.* 24.3-4 (1997). Computational algebra and number theory (London, 1993), pp. 235–265 (cit. on p. 9).

[3] A. Bourdon and P. Clark. "Torsion points and Galois representations on CM elliptic curves". In: *Pacific Journal of Mathematics* 305.1 (2020), pp. 43–88 (cit. on pp. 2, 6, 11).

[4] A. Bourdon, P. Clark, and J. Stankewicz. "Torsion points on CM elliptic curves over real number fields". In: *Transactions of the American Mathematical Society* 369.12 (2017), pp. 8457–8496 (cit. on p. 4).

[5] F. Campagna and R. Pengo. "Entanglement in the family of division fields of elliptic curves with complex multiplication". To appear in *Pacific Journal of Mathematics* (cit. on pp. 2, 6, 8, 10, 11).

[6] F. Campagna and R. Pengo. "Finding explicitly a CM elliptic curve with small Galois image". SageMath notebook, available at: https://bit.ly/3oyzOOb (cit. on p. 11).

[7] H. Cohen. *A course in computational algebraic number theory*. Vol. 138. Graduate Texts in Mathematics. Springer-Verlag, Berlin, 1993 (cit. on p. 7).

[8] H. Cohen. *Advanced topics in computational number theory*. Vol. 193. Graduate Texts in Mathematics. Springer-Verlag, New York, 2000 (cit. on p. 8).

[9] D. A. Cox. *Primes of the form $x^2 + ny^2$*. Second edition. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, 2013 (cit. on pp. 2, 10, 11).

[10] *GAP – Groups, Algorithms, and Programming*. Version 4.11.1. The GAP Group. 2021 (cit. on p. 7).

[11] S. Lang. *Elliptic functions*. Second edition. Vol. 112. Graduate Texts in Mathematics. Springer-Verlag, New York, 1987 (cit. on pp. 4, 5).

[12] D. Lombardo. "Bounds for Serre's open image theorem for elliptic curves over number fields". In: *Algebra & Number Theory* 9.10 (2015), pp. 2347–2395 (cit. on p. 1).

[13] D. Lombardo. "Galois representations attached to abelian varieties of CM type". In: *Bulletin de la Société Mathématique de France* 145.3 (2017), pp. 469–501 (cit. on pp. 2, 6).

[14] Á. Lozano-Robledo. "Galois representations attached to elliptic curves with complex multiplication". To appear in *Algebra & Number Theory* (cit. on pp. 2, 6).

[15] J. Neukirch. *Algebraic Number Theory*. Vol. 322. Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 1999 (cit. on pp. 5, 8).

[16] The PARI Group. *PARI/GP version 2.11.2*. Univ. Bordeaux, 2019 (cit. on p. 9).

[17] J. Rouse, A. V. Sutherland, and D. Zureick-Brown. "ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$". arXiv:2106.11141. (2021) (cit. on p. 1).

[18] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.0)*. 2020 (cit. on p. 9).

[19] J.-P. Serre. "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques". In: *Inventiones mathematicæ* 15.4 (1971), pp. 259–331 (cit. on pp. 1–4).

[20] G. Shimura. *Abelian varieties with complex multiplication and modular functions*. Vol. 46. Princeton Mathematical Series. Princeton University Press, Princeton, NJ, 1998 (cit. on p. 3).

[21] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*. Vol. 11. Publications of the Mathematical Society of Japan. Princeton University Press, Princeton, NJ, 1994 (cit. on pp. 6, 8).

[22] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves.* Vol. 151. New York, NY: Springer-Verlag, 1994, pp. xiii + 525 (cit. on pp. 3, 11).

[23] J. H. Silverman. *The arithmetic of elliptic curves.* 2nd ed. Vol. 106. New York, NY: Springer, 2009, pp. xx + 513 (cit. on p. 3).

[24] H. M. Stark. "On Complex Quadratic Fields with Class-Number Two". In: *Mathematics of Computation* 29.129 (1975), pp. 289–302 (cit. on p. 11).

[25] M. Watkins. "Class numbers of imaginary quadratic fields". In: *Mathematics of Computation* 73.246 (2004), pp. 907–938 (cit. on p. 11).

[26] D. Zywina. "Possible indices for the Galois image of elliptic curves over $\mathbb{Q}$". arXiv:1508.07663. (2015) (cit. on p. 1).

Francesco Campagna - Max Planck Institute for Mathematics, Vivatsgasse 7, 53111 Bonn, Germany
Email address: campagna@mpim-bonn.mpg.de

Riccardo Pengo - École normale supérieure de Lyon, Unité de Mathématiques Pures et Appliquées, 46 allée d'Italie, 69007 Lyon, France
Email address: riccardo.pengo@ens-lyon.fr