Math. Res. Lett.
Volume 25, Number 6, 1893–1910, 2018

On the uniform Rasmussen-Tamagawa conjecture in the CM case

Davide Lombardo

We prove a uniform version of a finiteness conjecture due to Rasmussen and Tamagawa in the case of CM abelian varieties. This extends the result of [2] from elliptic curves to abelian varieties of arbitrary dimension.

1. Introduction

Motivated by previous work of Anderson and Ihara [1], in [19] and [18] Rasmussen and Tamagawa have formulated (and partially proven) a series of finiteness conjectures for abelian varieties A over number fields K such that the extension $K(A[\ell^\infty])/K(\mu_{\ell^\infty})$ is both pro-ℓ and unramified away from ℓ. The strongest form of their conjecture, as stated in [18, Conj. 2], is the following uniform finiteness statement:

Conjecture 1.1. *Let*

$$\mathscr{A}(K,g,\ell) = \left\{ A \text{ abelian variety over } K \;\middle|\; \begin{array}{c} \dim A = g \\ K(A[\ell^\infty])/K(\mu_{\ell^\infty}) \text{ is pro-}\ell \\ \text{and unramified outside } \ell \end{array} \right\}.$$

There is a function $B(n,g)$ such that, for every number field K of degree n and every prime $\ell > B(n,g)$, the set $\mathscr{A}(K,g,\ell)$ is empty.

Much progress has been made on this conjecture – in particular, Rasmussen and Tamagawa themselves have proven [18] that the Generalized Riemann Hypothesis implies Conjecture 1.1 for n odd – but an unconditional proof is only known for $g = 1$ and $[K : \mathbb{Q}]$ equal to either 1 or 3. More recently, Bourdon [2] has given an unconditional proof of a similar finiteness result for CM elliptic curves over arbitrary number fields:

Theorem 1.2. *(Bourdon [2]) Let K be a number field with $[K:\mathbb{Q}] = n$. There is a constant $C = C(n)$ depending only on n with the following property: if there exists a CM elliptic curve E/K with $K(E[\ell^\infty])$ a pro-ℓ extension of $K(\mu_\ell)$ for some rational prime ℓ, then $\ell \leq C$.*

A related result was proved by Ozeki:

Theorem 1.3. *(Ozeki [17, Corollary 1.3]) For fixed K and g, the set*

$$\{A \in \mathscr{A}(K,g,\ell) : A \text{ admits complex multiplication over } K\}$$

is empty for ℓ large enough (depending on K and g).

The purpose of this note is to extend Theorem 1.2 to CM abelian varieties of arbitrary dimension, or equivalently, to replace the dependence on K with a dependence on $[K:\mathbb{Q}]$ in Theorem 1.3. To be more precise, by an **abelian variety of CM type** over K we mean an abelian variety A/K such that $\mathrm{End}_{\overline{K}}(A) \otimes \mathbb{Q}$ contains an étale $\mathbb{Q}$-algebra of dimension equal to $2 \dim A$. We shall show the following higher-dimensional analogue of Theorem 1.2:

Theorem 1.4. *Let*

$$\mathscr{A}^{\mathrm{CM}}(K,g,\ell) = \left\{ A \text{ abelian variety over } K \;\middle|\; \begin{array}{c} \dim A = g \\ A \text{ of CM type} \\ K(A[\ell^\infty])/K(\mu_\ell) \text{ is pro-}\ell \end{array} \right\}.$$

There exists a function $C(n,g)$ with the following property: for every number field K of degree at most n the set $\mathscr{A}^{\mathrm{CM}}(K,g,\ell)$ is empty for all $\ell > C(n,g)$.

As it is clear, Theorem 1.4 yields a proof of Conjecture 1.1 in the special case of CM abelian varieties. Notice that since CM abelian varieties acquire everywhere good reduction over a finite extension of their field of definition, and this extension can be taken of degree bounded by a constant depending only on the dimension, the condition that $K(A[\ell^\infty])/K(\mu_{\ell^\infty})$ be unramified outside ℓ is inessential in the CM case. In general, however, we do not expect finiteness if we both drop the ramification requirement and leave the realm of CM abelian varieties.

We conclude this brief introduction with a quick overview of the material to be covered in this article. In Section 2 we show that in order to prove Theorem 1.4 one only needs to deal with geometrically simple abelian

varieties with multiplication by the full ring of integers of the corresponding CM field. In §3 we recall a lower bound on the degree of the division fields of CM abelian varieties (taken from [10]), while in §4 we show how a recent theorem of Tsimerman [29] gives a finiteness result for the set of CM fields that can act on g-dimensional CM abelian varieties defined over fields of degree at most n. In §5 we finish the proof of Theorem 1.4, while §6 contains a few remarks on the problem of effectivity, together with a more detailed study of the case $n = 1$, $g = 2$.

2. Preliminary reductions

The situation is simpler if we assume that our abelian varieties have all their endomorphisms defined over K. It is thus natural to consider the following subset of $\mathscr{A}^{\mathrm{CM}}(K, g, \ell)$:

$$\mathscr{A}^{\mathrm{CM},1}(K, g, \ell) = \left\{ A \in \mathscr{A}^{\mathrm{CM}}(K, g, \ell) \;\middle|\; \mathrm{End}_{\overline{K}}(A) = \mathrm{End}_K(A) \right\}.$$

Fortunately, as the following lemma shows, not much is lost in considering the smaller set $\mathscr{A}^{\mathrm{CM},1}(K, g, \ell)$ instead of $\mathscr{A}^{\mathrm{CM}}(K, g, \ell)$:

Lemma 2.1. *Suppose there exists a function $C^{(1)}(n, g)$ with the following property: for every number field K of degree at most n, the set $\mathscr{A}^{\mathrm{CM},1}(K, g, \ell)$ is empty for all $\ell > C^{(1)}(n, g)$. Then Theorem 1.4 holds.*

Proof. Recall that, for fixed g, there is a constant $D(g)$ with the following property: for every abelian variety A of dimension g over a number field K there exists an extension F of K, of degree at most $D(g)$, such that $\mathrm{End}_{\overline{K}}(A) = \mathrm{End}_F(A)$ (sharp bounds for $D(g)$ can be found in [26]). Set $C(n, g) = C^{(1)}(D(g) \cdot n, g)$. Let now K be a number field of degree at most n. If A/K is an element of $\mathscr{A}^{\mathrm{CM}}(K, g, \ell)$, then we can find a number field F such that $[F : \mathbb{Q}] = [F : K][K : \mathbb{Q}] \leq D(g)n$ and $\mathrm{End}_F(A) = \mathrm{End}_{\overline{F}}(A)$. The abelian variety A/F is then an element of $\mathscr{A}^{\mathrm{CM},1}(F, g, \ell)$, which by assumption is empty for $\ell > C^{(1)}(D(g)n, g)$. This clearly implies that $\mathscr{A}^{\mathrm{CM}}(K, g, \ell)$ is empty as long as $\ell > C^{(1)}(D(g)n, g) =: C(n, g)$. □

We can also restrict ourselves to geometrically simple varieties:

Lemma 2.2. *Let*

$$\mathscr{A}^{\mathrm{CM},2}(K,g,\ell) = \left\{ A \in \mathscr{A}^{\mathrm{CM},1}(K,g,\ell) \;\middle|\; A \text{ is absolutely simple} \right\}$$

and suppose there is a function $C^{(2)}(n,g)$ with the following property: for every number field K of degree at most n, the set $\mathscr{A}^{\mathrm{CM},2}(K,g,\ell)$ is empty for all $\ell > C^{(2)}(n,g)$. Then Theorem 1.4 holds.

Proof. It suffices to show that there exists a function $C^{(1)}(n,g)$ as in Lemma 2.1. We claim that we can take $C^{(1)}(n,g) = \max_{g' \leq g} C^{(2)}(n,g')$. To see this, suppose by contradiction that there exists a number field K of degree at most n and a prime $\ell > \max_{g' \leq g} C^{(2)}(n,g')$ such that $\mathscr{A}^{\mathrm{CM},1}(K,g,\ell)$ is nonempty. Let A/K be an element of this set. By definition we have $\mathrm{End}_{\overline{K}}(A) = \mathrm{End}_K(A)$, so all the abelian subvarieties of A are defined over K. Let A'/K be an absolutely simple subvariety of A/K, and let g' be its dimension. It is clear that A' has complex multiplication over K, and that the extension $K(A'[\ell^\infty])/K(\mu_\ell)$ is pro-ℓ since it is a sub-extension of the (pro-ℓ) extension $K(A[\ell^\infty])/K(\mu_\ell)$. It follows that A' is an element of $\mathscr{A}^{\mathrm{CM},2}(K,g',\ell)$, but this is a contradiction, because by assumption $\mathscr{A}^{\mathrm{CM},2}(K,g',\ell)$ is empty for $\ell > C^{(2)}(K,g',\ell)$. □

Finally, it will be useful to reduce to the case of abelian varieties having complex multiplication by the full ring of integers of their corresponding CM field. To this end, we shall need the following result:

Theorem 2.3. *([20, Theorem 1.1], [31, Proposition 2.5.4]) Let A/K be an abelian variety and let $R = \mathrm{End}_K(A)$ be its endomorphism algebra. Let N be a positive integer and $\mathcal{O}$ be a maximal order of $E := R \otimes \mathbb{Q}$ such that $N^{-1}R$ contains $\mathcal{O}$. There exists an abelian variety B/K and K-isogenies $\varphi : A \to B$, $\psi : B \to A$ such that $\mathrm{End}_K(B) = \mathcal{O}$ and $\psi \circ \varphi = [N]$. In particular, if $\mathrm{End}_K(A) \otimes \mathbb{Q}$ is a field E, there exists an abelian variety B/K that is K-isogenous to A and such that $\mathrm{End}_K(B)$ is the ring of integers $\mathcal{O}_E$ of E.*

Lemma 2.4. *Let K be a number field, A, B be abelian varieties over K that are isogenous over K, and ℓ be a prime number. The fields $K(A[\ell^\infty])$ and $K(B[\ell^\infty])$ coincide.*

Proof. Let φ be a K-isogeny between A and B. Denote by $V_\ell(A)$ (resp. $V_\ell(B)$) the rational ℓ-adic Tate module of A (resp. B), that is, $V_\ell(A) := T_\ell(A) \otimes_{\mathbb{Z}_\ell}$

$\mathbb{Q}_\ell$ (resp. $V_\ell(B) := T_\ell(B) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$). Consider the representation

$$\rho_{\ell,A} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T_\ell(A)) \hookrightarrow \mathrm{Aut}(V_\ell(A))$$

and the analogous representation $\rho_{\ell,B}$ attached to B. The isogeny φ induces a Galois-equivariant isomorphism $V_\ell(A) \to V_\ell(B)$, so $\rho_{\ell,A}$ and $\rho_{\ell,B}$ are equivalent as representations of $\mathrm{Gal}(\overline{K}/K)$, and in particular they have the same kernel. Since the fixed field of $\ker \rho_{\ell,A}$ (resp. $\ker \rho_{\ell,B}$) is $K(A[\ell^\infty])$ (resp. $K(B[\ell^\infty])$, this proves our claim. □

We then obtain the desired reduction to the case of CM by the maximal order:

Lemma 2.5. *Let*

$$\mathscr{A}^{\mathrm{CM},3}(K,g,\ell) = \left\{ A \in \mathscr{A}^{\mathrm{CM},2}(K,g,\ell) \;\middle|\; \begin{array}{c} \mathit{End}_K(A) \text{ is the maximal} \\ \text{order of } \mathrm{End}_K(A) \otimes \mathbb{Q} \end{array} \right\}.$$

The set $\mathscr{A}^{\mathrm{CM},2}(K,g,\ell)$ is empty if and only if the set $\mathscr{A}^{\mathrm{CM},3}(K,g,\ell)$ is empty. In particular, if there exists a function $C^{(3)}(n,g)$ such that $\mathscr{A}^{\mathrm{CM},3}(K,g,\ell)$ is empty for all number fields K of degree at most n and for all $\ell > C^{(3)}(n,g)$, then Theorem 1.4 holds.

Proof. It suffices to show that if $\mathscr{A}^{\mathrm{CM},2}(K,g,\ell)$ is nonempty then $\mathscr{A}^{\mathrm{CM},3}(K,g,\ell)$ is also nonempty. Assume $\mathscr{A}^{\mathrm{CM},2}(K,g,\ell) \neq \emptyset$ and take $A \in \mathscr{A}^{\mathrm{CM},2}(K,g,\ell)$. By Theorem 2.3 there is a K-abelian variety B, isogenous to A over K, such that $\mathrm{End}_K(B)$ is the maximal order of $\mathrm{End}_K(B) \otimes \mathbb{Q} = \mathrm{End}_K(A) \otimes \mathbb{Q}$. By Lemma 2.4 we have $K(B[\ell^\infty]) = K(A[\ell^\infty])$, which shows that B lies in $\mathscr{A}^{\mathrm{CM}}(K,g,\ell)$. On the other hand, it is clear that B is absolutely simple and that all its endomorphisms are defined over K. Since by construction $\mathrm{End}_K(B)$ is the maximal order of $\mathrm{End}_K(B) \otimes \mathbb{Q}$, we see that B belongs to $\mathscr{A}^{\mathrm{CM},3}(K,g,\ell)$ as desired. The last assertion is now an immediate consequence of Lemma 2.2. □

3. Bounding ℓ in terms of $\mathrm{disc}(\mathrm{End}_K(A) \otimes \mathbb{Q})$

It remains to establish the existence of a function $C^{(3)}(n,g)$ as in Lemma 2.5. A key step in doing so is the following proposition:

Proposition 3.1. *Let A/K be an element of $\mathscr{A}^{\mathrm{CM},3}(K,g,\ell)$ and let $E := \mathrm{End}_K(A) \otimes \mathbb{Q}$. Either ℓ is at most $[K:\mathbb{Q}](g+2)^{3(g+1)}$ or it divides the discriminant of E.*

Proof. Recall that, by definition of $\mathscr{A}^{\mathrm{CM},3}(K,g,\ell)$, the ring $\mathrm{End}_K(A)$ is the maximal order $\mathcal{O}_E$ of the CM field E. We shall suppose from the start that ℓ does not divide the discriminant of E, that is, that ℓ is unramified in E, and prove the claimed bound. Consider the tower of extensions $K(A[\ell^\infty])/K(A[\ell])/K(\mu_\ell)$. Since by assumption $K(A[\ell^\infty])/K(\mu_\ell)$ is pro-ℓ, this holds a fortiori for the extension $K(A[\ell])/K(\mu_\ell)$.

On the other hand, the hypothesis $\mathrm{End}_{\overline{K}}(A) = \mathrm{End}_K(A)$ entails that the action of $\mathrm{Gal}\left(\overline{K}/K\right)$ on $A[\ell]$ factors through $\mathrm{Gal}\left(\overline{K}/K\right)^{ab} \to (\mathcal{O}_E \otimes \mathbb{F}_\ell)^\times$. To see this, notice first that $T_\ell A$ is a free $\mathcal{O}_{E,\ell} := \mathcal{O}_E \otimes \mathbb{Z}_\ell$ module by [22, Remark on page 502], hence in particular (comparing $\mathbb{Z}_\ell$-ranks) we have $T_\ell A \cong \mathcal{O}_{E,\ell}$. Furthermore, by [22, Corollary 2 to Theorem 5] the equality $\mathrm{End}_{\overline{K}}(A) = \mathrm{End}_K(A)$ implies that the action of $\mathrm{Gal}\left(\overline{K}/K\right)$ on $T_\ell(A)$ factors through $\mathcal{O}_{E,\ell}^\times$. Since $A[\ell] \cong T_\ell(A)/\ell T_\ell(A) \cong \mathcal{O}_{E,\ell}/\ell\mathcal{O}_{E,\ell} \cong \mathcal{O}_E \otimes \mathbb{F}_\ell$, the action of an element r of $\mathcal{O}_{E,\ell}$ on $A[\ell]$ is through its class $[r]$ in $\mathcal{O}_{E,\ell}/\ell\mathcal{O}_{E,\ell} = \mathcal{O}_E \otimes \mathbb{F}_\ell$, so when we consider the composition

$$\mathrm{Gal}\left(\overline{K}/K\right)^{ab} \to \mathcal{O}_{E,\ell}^\times \hookrightarrow \mathrm{Aut}\, T_\ell(A) \to \mathrm{Aut}\, A[\ell]$$

we see that the map $\mathcal{O}_{E,\ell}^\times \to \mathrm{Aut}\, A[\ell]$ (hence also the Galois action on $A[\ell]$) factors through $(\mathcal{O}_E \otimes \mathbb{F}_\ell)^\times$ as claimed. Furthermore, as ℓ is unramified in E, the group $(\mathcal{O}_E \otimes \mathbb{F}_\ell)^\times$ has order prime to ℓ, hence the same is true for $G_\ell := \mathrm{Gal}\,(K(A[\ell])/K)$. Since on the other hand $K(\mu_\ell)/K$ is a sub-extension of $K(A[\ell])/K$, and by hypothesis $\mathrm{Gal}\,(K(A[\ell])/K(\mu_\ell))$ is an ℓ-group, this implies $K(A[\ell]) = K(\mu_\ell)$.

Also remark that the Mumford-Tate group of A is a subtorus of $\mathrm{Res}_{E/\mathbb{Q}}(\mathbb{G}_{m,E})$, which has good reduction at ℓ by the Galois criterion: in particular, $\mathrm{MT}(A)$ defines a torus over $\mathbb{F}_\ell$, and the Galois group G_ℓ is a subgroup of $\mathrm{MT}(A)(\mathbb{F}_\ell)$. Notice furthermore that the degree $[K(\mu_\ell) : K]$ is at most $\varphi(\ell) = \ell - 1$.

We now give a lower bound for the degree $K(A[\ell])/K$. We take the notation of [10]: we denote by r the rank of $\mathrm{MT}(A)$, by μ the number of roots of unity in E, by E^* the reflex field of E, and by T_E (resp. T_{E^*}) the algebraic group $\mathrm{Res}_{E/\mathbb{Q}}(\mathbb{G}_{m,E})$ (resp. $\mathrm{Res}_{E^*/\mathbb{Q}}(\mathbb{G}_{m,E^*})$). Finally, we denote by F the group of connected components of $\ker\left(T_{E^*} \xrightarrow{N} T_E\right)$, where N is the reflex norm. Since $G_\ell \subseteq \mathrm{MT}(A)(\mathbb{F}_\ell)$ and ℓ is unramified in E, we see by [10, Theorems 1.2 and 1.3] that the degree of $K(A[\ell])/K$ is at least

$$\frac{1}{[\mathrm{MT}(A)(\mathbb{F}_\ell) : G_\ell]}\,|\mathrm{MT}(A)(\mathbb{F}_\ell)| \geq \frac{(1-1/\ell)^r \ell^r}{\mu \cdot [K : E^*] \cdot |F|^{2r}}.$$

We now give (rough) estimates for the various terms appearing in this expression:

- the degree $[K : E^*] = \dfrac{[K : \mathbb{Q}]}{[E^* : \mathbb{Q}]}$ does not exceed $\frac{1}{2}[K : \mathbb{Q}]$;
- the number μ of roots of unity in E satisfies $\varphi(\mu) \leq [E : \mathbb{Q}] = 2g$; since $\varphi(x) \geq \frac{\sqrt{x}}{2}$ for all positive integers x, we have $\mu \leq (4g)^2$;
- again by [10, Theorem 1.3] we have $|F| \leq 2\left(\dfrac{r+1}{4}\right)^{(r+1)/2}$.

Putting everything together we find $[K(A[\ell]) : K] \geq \dfrac{2^{2r^2+1}}{16g^2} \cdot \dfrac{(\ell-1)^r}{[K : \mathbb{Q}]}(r+1)^{-r(r+1)}$. A theorem of Ribet [21, Formula (3.5)] yields the inequality $r \geq 2 + \log_2(g)$, so that we have $2^{2r^2+1} \geq 2^9 g^2$; we thus obtain the inequality

$$[K(A[\ell]) : K] \geq 2^5 \frac{(\ell-1)^r}{[K : \mathbb{Q}]}(r+1)^{-(r+1)},$$

which, combined with $[K(A[\ell]) : K] = [K(\mu_\ell) : K] \leq \ell - 1$, leads to $\ell - 1 \geq 2^5 \cdot \dfrac{(\ell-1)^r}{[K : \mathbb{Q}]}(r+1)^{-r(r+1)}$, and finally to

$$\begin{aligned}\ell - 1 &\leq \left(\frac{[K : \mathbb{Q}]}{32}\right)^{1/(r-1)} \cdot (r+1)^{r(r+1)/(r-1)} < [K : \mathbb{Q}](r+1)^{3r} \\ &\leq [K : \mathbb{Q}](g+2)^{3(g+1)}\end{aligned}$$

as claimed. □

Remark 3.2. As it is clear from the proof, one can obtain much sharper inequalities for large g: for example, as long as $g \geq 2$, we have $r \geq 3$ by Ribet's inequality, and in the very last step of the previous proof we obtain $\ell - 1 \leq [K : \mathbb{Q}]^{1/2}(r+1)^{2r}$.

4. A result of Tsimerman

To finish the proof of Theorem 1.4 we shall need a way to control the possible endomorphism algebras of CM abelian varieties of a given dimension. This is made possible by Corollary 4.3 below, which is in turn a consequence of a recent result of Tsimerman (Theorem 4.2).

Definition 4.1. *Let $A/\overline{\mathbb{Q}}$ be an abelian variety of CM type. The field of moduli of A is the intersection of all the number fields F such that there exists an abelian variety A_F over F that satisfies $(A_F)_{\overline{\mathbb{Q}}} = A$.*

Theorem 4.2. *([29, Theorem 1.1]) For every positive g there exist constants $k_g, \delta_g > 0$ such that if E is a CM field of degree $2g$ and if A is any abelian variety over $\overline{\mathbb{Q}}$ of dimension g with endomorphism ring equal to the full ring of integers $\mathcal{O}_E$ of E, then the field of moduli F of A satisfies*

$$[F : \mathbb{Q}] \geq k_g |\operatorname{disc}(E)|^{\delta_g}.$$

Corollary 4.3. *Let n, g be fixed positive integers. Consider the set $\mathcal{A}(n, g)$ all g-dimensional, geometrically simple abelian varieties A/K of CM type, where K is a number field of degree at most n. The set*

$$\mathcal{R}(n, g) = \left\{ \operatorname{End}_K(A) \otimes \mathbb{Q} \;\middle|\; A \in \mathcal{A}(n, g) \right\}$$

is finite.

Proof. Consider an abelian variety $A \in \mathcal{A}(n, g)$ with field of definition K, and let E denote $\operatorname{End}_{\overline{K}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$. As in the proof of Lemma 2.1, there exists an extension K' of K (with $[K' : K]$ bounded by a constant $D(g)$ depending only on g) such that $\operatorname{End}_{K'}(A) = \operatorname{End}_{\overline{K}}(A)$. Now A is K'-isogenous to an abelian variety B/K' with multiplication by the full ring of integers of E (Theorem 2.3); let F be the field of moduli of B. Since B has a model over K', we have $nD(g) \geq [K' : \mathbb{Q}] \geq [F : \mathbb{Q}]$, and applying the previous theorem we find

$$nD(g) \geq [K' : \mathbb{Q}] \geq [F : \mathbb{Q}] \geq k_g |\operatorname{disc}(E)|^{\delta_g};$$

in particular, $\operatorname{disc}(E)$ is bounded (in absolute value), hence there are only finitely many possibilities for $\operatorname{End}_{\overline{K}}(B) \otimes \mathbb{Q} = \operatorname{End}_{\overline{K}}(A) \otimes \mathbb{Q}$. As $\operatorname{End}_K(A) \otimes \mathbb{Q}$ is a subfield of $\operatorname{End}_{\overline{K}}(A) \otimes \mathbb{Q}$, this finishes the proof. □

Remark 4.4. The case $g = 1$ (that is, the case of elliptic curves) of this Corollary is well known, and is also a key ingredient for the arguments of [2]. To see why the case $g = 1$ follows from the classical theory of elliptic curves, consider all number fields K of degree at most n, and all elliptic curves E_1/K with (potential) complex multiplication. If E_1/K is such an elliptic curve, with complex multiplication by an order R in the quadratic imaginary field F, then the action of R on E_1 is defined over the compositum FK, and we can find an elliptic curve E_2/FK, isogenous to E_1 over FK,

that has full complex multiplication by the ring of integers of F. Now it is well-known that the j-invariant of E_2 generates the Hilbert class field H of F, and on the other hand $j(E_2)$ is in FK by assumption, so it follows that

$$h(F) = [H : F] \leq [FK : \mathbb{Q}] \leq 2[K : \mathbb{Q}] \leq 2n$$

is bounded by n alone. It is a result of Heilbronn [6] (which can be now obtained as a consequence of the Brauer-Siegel theorem) that there are only finitely many imaginary quadratic fields F with $h(F) \leq 2n$, and the finiteness of $\mathcal{R}(n, 1)$ follows.

Remark 4.5. Recent work of Orr and Skorobogatov gives even more precise finiteness results (that take into account the *ring* structure of $\mathrm{End}_K(A)$), see [16].

5. Conclusion

We are now ready to prove Theorem 1.4:

Theorem 5.1. *There exists a function $C(n, g)$ such that $\mathscr{A}^{\mathrm{CM}}(K, g, \ell)$ is empty for all number fields K of degree at most n and all primes $\ell > C(n, g)$.*

Proof. By Lemma 2.5 it suffices to show the existence of a function $C^{(3)}(n, g)$ such that $\mathscr{A}^{\mathrm{CM},3}(K, g, \ell)$ is empty for all number fields K of degree at most n and for all $\ell > C^{(3)}(n, g)$. Consider the set $\mathcal{R}(n, g)$ of Corollary 4.3 and let Δ be the maximum of the absolute discriminants $|\operatorname{disc}(E)|$ for E varying in $\mathcal{R}(n, g)$. We claim that we can take $C^{(3)}(n, g) = \max\left\{\Delta, n(g+2)^{3(g+1)}\right\}$. To see this, consider a number field K of degree at most n and an element A/K of $\mathscr{A}^{\mathrm{CM},3}(K, g, \ell)$, and set $E = \mathrm{End}_K(A) \otimes \mathbb{Q}$. By Proposition 3.1, we have either $\ell \leq n(g+2)^{3(g+1)} \leq C^{(3)}(n, g)$ or $\ell \leq |\operatorname{disc}(E)| \leq \Delta \leq C^{(3)}(n, g)$; in particular, $\mathscr{A}^{\mathrm{CM},3}(K, g, \ell)$ is empty for $\ell > C^{(3)}(n, g)$ as claimed. □

6. Some remarks on effectivity

Unlike Theorem 1.2, our Theorem 1.4 is unfortunately non-effective: the source of this can be traced back to the proof of Theorem 4.2, and more specifically to Corollary 3.2 of [29], whose proof depends on the full strength of the Brauer-Siegel theorem, which is not known to be effective at present. Notice that other parts of Tsimerman's argument also require the Brauer-Siegel theorem, but they can be made effective by using the results of [27], so

[29, Corollary 3.2] is really the crux of the matter. By contrast, notice that the proof of the case $g = 1$ of Corollary 4.3 sketched in Remark 4.4 *can* be made effective: as it is well known, the problem of determining all imaginary quadratic fields of a given class number can be solved effectively. This fact is exploited in [2] to produce explicit bounds for the function $C(n, 1)$ for various values of n.

On the other hand, even if one is willing to assume the truth of the Generalized Riemann Hypothesis (which – as it is well known – implies effective versions of the Brauer-Siegel theorem), the argument of [29] gives for the constant δ_g of Theorem 4.2 a very small value, intimately tied to a certain exponent appearing in the so-called Isogeny Theorem of Masser and Wüstholz [13] [12]; the Brauer-Siegel theorem is only used to determine the value of k_g, and has no influence on δ_g. Using the (currently) best available isogeny bound, due to Gaudron and Rémond [5], we see for example that Theorem 4.2 holds for all values of δ_2 strictly smaller than 2^{-16}: clearly this number is so small that it makes it impossible in practice to use Theorem 4.2 to determine the set $\mathcal{R}(n, g)$. Conditionally on GRH, sharper results are known, but none of them seems to be completely explicit at present: in the context of giving lower bounds on Galois orbits of special points on Shimura varieties, Tsimerman, Ullmo and Yafaev have proven various lower bounds on the degree of the field of moduli of a CM abelian variety (cf. for example [30] and [28]), but their results contain some non-explicit constants that seem hard to compute in practice.

Slightly different techniques – mainly coming from classical analytic number theory – can however yield results on the sets $\mathcal{R}(n, g)$ for certain small values of g and n, which in turn allows us to determine an admissible value for $C(n, g)$ – and sometimes even the optimal value – via the argument described in the previous sections. For example, we can show:

Proposition 6.1. *We can take* $C(1, 2) = 163$*, and this value is optimal.*

As can be expected from our previous discussion, in order to prove this result we shall require some control on the endomorphism rings of CM abelian varieties defined over $\mathbb{Q}$. While the information we require is essentially contained in the literature, we could not find the exact statement we need in print, so we give some details.

Proposition 6.2. *Let* $A/\mathbb{Q}$ *be an abelian surface such that* $\mathrm{End}_{\overline{\mathbb{Q}}}(A)$ *is (isomorphic to) an order* R *in a CM field* E*. Then either* $A_{\overline{\mathbb{Q}}}$ *is isogenous to the product of two elliptic curves, or* E *is one of the 19 fields listed in [8, Theorem 2.4.5].*

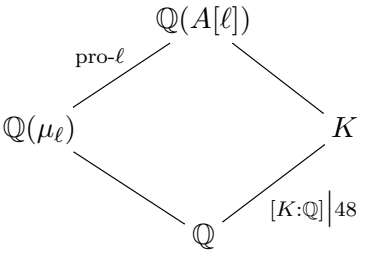
Proof. Suppose that A is geometrically simple. The field E is not biquadratic, because biquadratic fields give rise to non-primitive CM types, whose corresponding abelian varieties are geometrically split, see [24, §8.2]. Likewise, E cannot have Galois closure with Galois group D_4 by [23, Proposition 5.17] (in the D_4 case, the extension $E^*/\mathbb{Q}$ is not normal). It follows that $E/\mathbb{Q}$ is a cyclic quartic CM field. By [9, Chapter 3, Theorem 1.1], all the endomorphisms of A are defined over E^*, hence by Theorem 2.3 we see that there exists an abelian variety B/E^* with $\mathrm{End}_{E^*}(B) \cong \mathcal{O}_E$. Let (E, Φ) be the CM type of B (and $(E^* = E, \Phi^*)$ be its reflex) and fix an E^*-polarization $\mathcal{C}$ on B. The field of moduli k_0 of $(B, \mathcal{C})$ is contained in E^*. Denote by I_{E^*} the group of invertible fractional ideals of E^*. By [25, Main Theorem 1 on p. 128], the compositum $k_0E^* = E^*$ is the unramified class field over E^* corresponding to the ideal group

$$I_0(\Phi^*) = \left\{ \mathfrak{a} \in I_{E^*} : \exists \alpha \in E^* \text{ such that } N_{\Phi^*}(\mathfrak{a}) = (\alpha), N_{E^*/\mathbb{Q}}(\mathfrak{a}) = \alpha\bar{\alpha} \right\},$$

where N_{Φ^*} is the reflex norm associated with (E^*, Φ^*). We have just seen that $I_0(\Phi^*)$ defines the trivial extension of E^*: this means precisely that E has "CM class number one" in the sense of P. Kılıçer's thesis [8]. All cyclic quartic CM fields $E/\mathbb{Q}$ with CM class number one have been determined in [8, Theorem 2.4.5] (see also [7]) by applying results of Murabayashi [14] and Louboutin [11]. □

We can now prove Proposition 6.1:

Proof. It is clear by definition that we must have $C(1,2) \geq C(1,1) = 163$, where the optimal value of $C(1,1) = 163$ is taken from [19] (see also [2]). Consider now an abelian surface $A/\mathbb{Q}$ admitting potential complex multiplication, and suppose first that $A_{\overline{\mathbb{Q}}}$ is isogenous to the product of two elliptic curves. Let ℓ be a prime larger than 163: we claim that $\mathbb{Q}(A[\ell])/\mathbb{Q}(\mu_\ell)$ cannot be pro-ℓ. Suppose the contrary: we shall obtain a contradiction. We shall need to rely on the results of [4], so we take the notation of that paper for the "Galois type" of our abelian variety A. Let K be a minimal field of definition for the endomorphisms of A; by [4], we have $[K : \mathbb{Q}] \mid 48$, and K is contained in $\mathbb{Q}(A[\ell])$ by [26, Propositions 2.2 and 2.3]. In fact we know even more, namely that $K/\mathbb{Q}$ is normal, with Galois group isomorphic to a subgroup of either $S_4 \times \mathbb{Z}/2\mathbb{Z}$ or $D_6 \times \mathbb{Z}/2\mathbb{Z}$ ([4, Table 8]). Consider now the following diagram of field extensions:



Let G_K (resp. $G_{\mathbb{Q}(\mu_\ell)}$, $G_{\mathbb{Q}}$) be the Galois group of $\mathbb{Q}(A[\ell])$ over K (resp. $\mathbb{Q}(\mu_\ell)$, $\mathbb{Q}$). Then $[K:\mathbb{Q}] = [G_{\mathbb{Q}} : G_K]$ is prime to ℓ, hence G_K contains a maximal ℓ-Sylow subgroup of $G_{\mathbb{Q}}$. On the other hand, $G_{\mathbb{Q}(\mu_\ell)}$ is a maximal ℓ-Sylow subgroup of $G_{\mathbb{Q}}$ (notice that $\ell \nmid [\mathbb{Q}(\mu_\ell) : \mathbb{Q}]$), and it is normal in $G_{\mathbb{Q}}$ because $\mathbb{Q}(\mu_\ell)$ is Galois over $\mathbb{Q}$. Now since all the maximal ℓ-Sylow subgroups of a group are conjugate to each other, this proves that $G_{\mathbb{Q}}$ has a unique maximal ℓ-Sylow, namely $G_{\mathbb{Q}(\mu_\ell)}$. It follows that G_K contains $G_{\mathbb{Q}(\mu_\ell)}$, hence that K is contained in $\mathbb{Q}(\mu_\ell)$. In particular, $K/\mathbb{Q}$ is a cyclic extension, and since its Galois group is a subgroup of either $S_4 \times \mathbb{Z}/2\mathbb{Z}$ or $D_6 \times \mathbb{Z}/2\mathbb{Z}$ the group $\mathrm{Gal}(K/\mathbb{Q})$ must be cyclic of order 1, 2, 3, 4 or 6. Depending on whether the simple factors of $A_{\overline{\mathbb{Q}}}$ are isogenous or not, the following are then the only possibilities for the Galois type of A:

1) $A_{\overline{\mathbb{Q}}}$ is isogenous to the square of an elliptic curve: by what we have just proved, combined with [4, Table 8], the Galois type of A is $\mathbf{F}[C_n]$ ($n \in \{1,2,3,4,6\}$), $\mathbf{F}[C_2, C_1, \mathbb{H}]$, $\mathbf{F}[C_2, C_1, \mathrm{M}_2(\mathbb{R})]$, $\mathbf{F}[C_4, C_2]$, $\mathbf{F}[C_6, C_3, \mathrm{M}_2(\mathbb{R})]$, or $\mathbf{F}[C_6, C_3, \mathbb{H}]$;

2) the two elliptic curves appearing as simple factors of $A_{\overline{\mathbb{Q}}}$ are non-isogenous: the Galois type of A is one of $\mathbf{D}[C_1]$, $\mathbf{D}[C_2, \mathbb{R}\times\mathbb{C}]$, $\mathbf{D}[C_2, \mathbb{R}\times\mathbb{R}]$, $\mathbf{D}[C_4]$.

We claim that there exists a quadratic extension M of $\mathbb{Q}$ such that A_M admits a 1-dimensional abelian subvariety defined over M (equivalently, A_M is M-isogenous to the product of two elliptic curves defined over M).

Case (2) is easy to deal with: according to [4, Theorem 4.3], only type $\mathbf{D}[C_4]$ can arise for an abelian surface A defined over $\mathbb{Q}$, and in this case $A_{\overline{\mathbb{Q}}}$ is simple ([4, §4.3 and 4.4]), contradicting our assumption. We can therefore focus on case (1). Let us first notice that, among the various subcases of (1), only cases $\mathbf{F}[C_2, C_1, \mathrm{M}_2(\mathbb{R})]$ and $\mathbf{F}[C_6, C_3, \mathrm{M}_2(\mathbb{R})]$ can arise for A defined over $\mathbb{Q}$ ([4, Theorem 4.3]). As for these two Galois types, the claim about the existence of M is obvious for $\mathbf{F}[C_2, C_1, \mathrm{M}_2(\mathbb{R})]$, because in this case K is itself a quadratic extension of $\mathbb{Q}$, and since all the endomorphisms of A are defined

over K, so are its abelian subvarieties. For case $\mathbf{F}[C_6, C_3, \mathrm{M}_2(\mathbb{R})]$, we know by [4, §4.5.2] that $\mathrm{End}_K(A) \otimes \mathbb{R} \cong \mathrm{M}_2(\mathbb{C})$, and the action of $\mathrm{Gal}\,(K/\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z}$ on it is determined by the fact that there is a generator g of $\mathbb{Z}/6\mathbb{Z}$ that acts on 2×2 complex matrices by the formula $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \bar{d} & \zeta_3\bar{c} \\ \overline{\zeta_3} b & \bar{a} \end{pmatrix}$. It follows that g^2 acts as $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & \zeta_3^2 b \\ \overline{\zeta_3}^2 c & d \end{pmatrix}$, so the fixed ring of g^2 is isomorphic to $\mathbb{C} \times \mathbb{C}$ (matrices with $b = c = 0$). If we denote by M the fixed field of g^2, then $M/\mathbb{Q}$ is a quadratic extension, and $\mathrm{End}(A_M) \otimes \mathbb{R} \cong \mathrm{M}_2(\mathbb{C})^{\langle g^2 \rangle} = \mathbb{C} \times \mathbb{C}$. Since by assumption $\mathrm{End}_M(A)$ cannot be a number field of degree 4, it follows that $\mathrm{End}_M(A)$ is not an integral domain, hence that A_M is nonsimple as claimed. Let now A_1/M be an elliptic curve contained in A_M: the field extension $M(A_1[\ell])/M(\mu_\ell)$, being contained in $M(A[\ell])/M(\mu_\ell)$, is pro-ℓ, but by definition of $C(2,1)$ this is impossible for $\ell > C(2,1) = 163$ (this value is taken from [2]), which finishes the proof in this case.

Consider then the case of $A/\mathbb{Q}$ being a geometrically simple abelian surface with (potential) complex multiplication by the ring $R := \mathrm{End}_{\overline{\mathbb{Q}}}(A)$. Let $E := R \otimes \mathbb{Q}$ and let ℓ be a prime strictly larger than 61. By Proposition 6.2 and the explicit list of fields given in [8, Theorem 2.4.5] we see that ℓ is unramified in E (indeed, 61 is the largest prime dividing the discriminant of one of the fields listed in [8, Theorem 2.4.5]). Since all the endomorphisms of A are defined over E^* ([9, Chapter 3, Theorem 1.1]), applying Theorem 2.3 we see that there is an abelian variety B/E^* that is E^*-isogenous to A and satisfies $\mathrm{End}_{E^*}(B) = \mathcal{O}_E$. If $\mathbb{Q}(A[\ell^\infty])/\mathbb{Q}(\mu_\ell)$ is pro-ℓ, the same is true for $E^*(A[\ell^\infty])/E^*(\mu_\ell)$, and therefore, by Lemma 2.4, also for $E^*(B[\ell^\infty])/E^*(\mu_\ell)$. This implies in particular that the degree $[E^*(B[\ell]) : E^*(\mu_\ell)]$ is a power of ℓ. On the other hand, since $\mathrm{End}_{E^*}(B) = \mathcal{O}_E$, as in the proof of Proposition 3.1 we see that the representation $\mathrm{Gal}\left(\overline{E^*}/E^*\right) \to \mathrm{Aut}\, B[\ell]$ factors through $(\mathcal{O}_E \otimes \mathbb{F}_\ell)^\times$, which is a group of order prime to ℓ since ℓ is unramified in E. It follows that $E^*(B[\ell]) = E^*(\mu_\ell)$, hence $[E^*(B[\ell]) : E^*] \leq \ell - 1$. Observe now that (in the notation of the proof of Proposition 3.1) we have $|F| = 1$ and $r = 3$, because this is true for all absolutely simple CM abelian surfaces; we then obtain from [10, Theorems 1.2 and 1.3] the inequality $[E^*(B[\ell]) : E^*] \geq \frac{1}{\mu}(\ell - 1)^3$. Since $[E : \mathbb{Q}] = 4$, it is easy to see that $\mu \leq 12$, whence

$$\ell - 1 \geq [E^*(\mu_\ell) : E^*] = [E^*(B[\ell]) : E^*] \geq \frac{1}{12}(\ell - 1)^3,$$

i.e. $\ell \leq 3$, a contradiction. □

Remark 6.3. It is interesting to notice that if we only consider *absolutely simple* abelian surfaces over $\mathbb{Q}$, then the value 61 obtained in the course of the previous proof is optimal, as the following example shows. We know from [15] that there exists an absolutely simple abelian surface $A/\mathbb{Q}$, with good reduction everywhere except at 61, which admits (potential) complex multiplication by the full ring of integers of $K = \mathbb{Q}\left(\sqrt{-(61+6\sqrt{61})}\right)$.

The discriminant of K is 61^3, so K is ramified at 61 only, and we have $(61)\mathcal{O}_K = \mathfrak{P}^4$ for a certain prime $\mathfrak{P}$ of $\mathcal{O}_K$. The extension $K/\mathbb{Q}$ is cyclic of degree 4, so – since it is furthermore unramified outside 61 – we see by the Kronecker-Weber theorem that it is a sub-extension of $\mathbb{Q}(\mu_{61})/\mathbb{Q}$. Writing $\mathrm{Gal}(K/\mathbb{Q}) = \{\mathrm{Id}, \sigma, \sigma^2, \sigma^3\}$, the CM type of $A/\mathbb{Q}$ is $\{\mathrm{Id}, \sigma\}$, and the reflex norm is $\Phi(x) = x \cdot \sigma^3(x)$. Recall that the reflex norm induces a group morphism $I_K \to I_K$, where I_K is the group of idèles of K, by acting on the idèles componentwise. As $K/\mathbb{Q}$ is cyclic, K is its own reflex field, and as a consequence all the endomorphisms of A are defined over K. The class number of K is 1, so if $\omega : I_K \to \mathrm{Gal}\left(K^{\mathrm{ab}}/K\right)$ denotes the reciprocity map of global class field theory we see that $\omega\left(\prod_v \mathcal{O}_{K,v}^{\times}\right)$ is all of $\mathrm{Gal}\left(K^{\mathrm{ab}}/K\right)$. Hence, in order to describe the Hecke character ε attached to A_K it suffices to describe its restriction to $\prod_v \mathcal{O}_{K,v}^{\times}$, and by the explicit construction of [15, pp. 664 and 667] we have

$$\begin{array}{rccc} \varepsilon: & \prod_v \mathcal{O}_{K,v}^{\times} & \to & \{\pm 1\} \\ & (a_v) & \mapsto & \begin{cases} 1, \text{ if } a_{\mathfrak{P}} \text{ is a square in } \mathbb{F}_{\mathfrak{P}}^{\times} \\ -1, \text{ otherwise} \end{cases} \end{array}.$$

By [22, Corollary 2 to Theorem 5] we know that, since $\mathrm{End}_K(A) = \mathcal{O}_K$, the representation $\mathrm{Gal}\left(\overline{K}/K\right) \to \mathrm{Aut}\, A[61]$ factors as

$$\mathrm{Gal}\left(\overline{K}/K\right) \to \mathrm{Gal}\left(\overline{K}/K\right)^{\mathrm{ab}} \xrightarrow{\rho} (\mathcal{O}_K \otimes \mathbb{F}_{61})^{\times} \hookrightarrow \mathrm{Aut}\, A[61],$$

and the map ρ can be described on idèle classes as

$$\rho((a_v)) = \varepsilon((a_v)) \cdot \Phi(a_{\mathfrak{P}}).$$

We claim that the image of $\mathrm{Gal}\left(\overline{K}/K\right) \to (\mathcal{O}_K \otimes \mathbb{F}_{61})^{\times}$ is contained in the kernel of the natural map $(\mathcal{O}_K \otimes \mathbb{F}_{\mathfrak{P}})^{\times} \to \mathbb{F}_{\mathfrak{P}}^{\times} \to \frac{\mathbb{F}_{\mathfrak{P}}^{\times}}{\mathbb{F}_{\mathfrak{P}}^{\times 4}}$. Notice first that if (a_v) is any idèle class, then $\rho((a_v))$ only depends on $a_{\mathfrak{P}}$. Thus to prove our claim it suffices to check that given an element $a_{\mathfrak{P}} \in \mathcal{O}_{K,\mathfrak{P}}^{\times}$ the product $\varepsilon(a_{\mathfrak{P}})\Phi(a_{\mathfrak{P}})$ reduces to a fourth power in $\mathbb{F}_{\mathfrak{P}}^{\times}$. Notice furthermore that $\sigma \in \mathrm{Gal}\,(K/\mathbb{Q})$

acts trivially on $\mathbb{Z}_{61} \subseteq \mathcal{O}_{K,\mathfrak{P}}$, so $\Phi(x) = x\sigma^3(x)$ induces the map $x \mapsto x^2$ on $\mathbb{F}_{\mathfrak{P}}^{\times}$. We can now prove our claim. Suppose first that $a_{\mathfrak{P}}$ is a square in $\mathbb{F}_{\mathfrak{P}}^{\times}$: then we have $\varepsilon(a_{\mathfrak{P}}) = 1$, and $\varepsilon(a_{\mathfrak{P}})\Phi(a_{\mathfrak{P}})$ reduces to $1 \cdot (a_{\mathfrak{P}})^2$ in $\mathbb{F}_{\mathfrak{P}}^{\times}$; since $a_{\mathfrak{P}}$ is a square in $\mathbb{F}_{\mathfrak{P}}^{\times}$, the product $\varepsilon(a_{\mathfrak{P}})\Phi(a_{\mathfrak{P}})$ is a fourth power in $\mathbb{F}_{\mathfrak{P}}^{\times}$ as claimed. Suppose on the other hand that $a_{\mathfrak{P}}$ is not a square in $\mathbb{F}_{\mathfrak{P}}^{\times}$: then $a_{\mathfrak{P}}^2$ is a square but not a fourth power, and we have $\varepsilon(a_{\mathfrak{P}}) = -1$, which again is a square but not a fourth power in $\mathbb{F}_{\mathfrak{P}}^{\times} \cong \mathbb{F}_{61}^{\times}$: the product $\varepsilon(a_{\mathfrak{P}})\Phi(a_{\mathfrak{P}})$ is then a fourth power in $\mathbb{F}_{\mathfrak{P}}^{\times}$ as claimed.

Let $d = 61^k a$ (with $(61, a) = 1$) be the degree of the extension $K(A[61])/K$: by what we just showed, a divides

$$\left|\ker\left((\mathcal{O}_K \otimes \mathbb{F}_{\mathfrak{P}})^{\times} \to \mathbb{F}_{\mathfrak{P}}^{\times} \,/\, \mathbb{F}_{\mathfrak{P}}^{\times 4}\right)\right| = \left|\mathbb{F}_{\mathfrak{P}}^{\times 4}\right| \times |\mathbb{F}_{\mathfrak{P}}|^3 = 15 \cdot 61^3,$$

so $a \mid 15$. Then since $[K(\mu_{61}) : K] \geq \frac{1}{[K:\mathbb{Q}]}\varphi(61) = 15$ and $K(\mu_{61})$ is contained in $K(A[61])$, we see that $[K(\mu_{61}) : K] = 15$ and $K(A[61])/K(\mu_{61})$ is a pro-61 extension. Finally, since K is contained in $\mathbb{Q}(\mu_{61})$, we have $K(\mu_{61}) = \mathbb{Q}(\mu_{61})$ and $K(A[61]) = \mathbb{Q}(A[61])$, and therefore $\mathbb{Q}(A[61])/\mathbb{Q}(\mu_{61})$ is a pro-61 extension. This shows, as claimed, that the constant 61 is optimal for absolutely simple abelian surfaces with CM.

As a final remark, we note that the computation of an explicit value for $C(2, 2)$ might be within reach with the current state of knowledge on quartic CM fields, and there is work in progress related to the determination of the set $\mathcal{R}(2, 2)$, see for example [3] and the aforementioned [7].

Acknowledgements

I am grateful to the referee for their useful comments and for pointing out a problem in the first version of this paper. I thank Abbey Bourdon for an interesting conversation that prompted me to look into this problem. This work was carried out at the Université Paris-Sud, and the author acknowledges financial support from the Fondation Mathématique Jacques Hadamard ("Programme des Investissements d'Avenir").

References

[1] G. Anderson and Y. Ihara, *Pro-ℓ branched coverings of* $\mathbf{P}^1$ *and higher circular ℓ-units*, Ann. of Math. (2) **128** (1988), no. 2, 271–293.

[2] A. Bourdon, *A uniform version of a finiteness conjecture for CM elliptic curves.*, Math. Res. Lett. **22** (2015), no. 2, 403–416.

[3] F. Bouyer and M. Streng, *Examples of CM curves of genus two defined over the reflex field*, LMS J. Comput. Math. **18** (2015), no. 1, 507–538.

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

[5] É. Gaudron and G. Rémond, *Polarisations et isogénies*, Duke Math. J. **163** (2014), no. 11, 2057–2108.

[6] H. Heilbronn, *On the class-number in imaginary quadratic fields*, The Quarterly Journal of Mathematics **5** (1934) 150–160.

[7] P. Kılıçer and M. Streng, *The CM class number one problem for curves of genus* 2, arXiv e-prints (2015).

[8] P. Kılıçer, *The CM class number one problem for curves*, Ph.D. thesis, Universiteit Leiden (2016).

[9] S. Lang, Complex Multiplication, Vol. 255 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], Springer-Verlag, New York (1983), ISBN 0-387-90786-6.

[10] D. Lombardo, *Galois representations attached to abelian varieties of CM type*, Bulletin de la Société Mathématique de France **145** (2017), fascicule 3, 469–501.

[11] S. Louboutin, *CM-fields with cyclic ideal class groups of* 2*-power orders*, J. Number Theory **67** (1997), no. 1, 1–10.

[12] D. W. Masser and G. Wüstholz, *Isogeny estimates for abelian varieties, and finiteness theorems*, Ann. of Math. (2) **137** (1993), no. 3, 459–472.

[13] D. W. Masser and G. Wüstholz, *Periods and minimal abelian subvarieties*, Ann. of Math. (2) **137** (1993), no. 2, 407–458.

[14] N. Murabayashi, *The field of moduli of abelian surfaces with complex multiplication*, J. Reine Angew. Math. **470** (1996) 1–26.

[15] N. Murabayashi, *Determination of simple CM abelian surfaces defined over* $\mathbb{Q}$, Math. Ann. **342** (2008), no. 3, 657–671.

[16] M. Orr and A. N. Skorobogatov, *Finiteness theorems for K3 surfaces and abelian varieties of CM type*, Compositio Mathematica **154** (2018), no. 8, 1571–1592.

[17] Y. Ozeki, *Non-existence of certain CM abelian varieties with prime power torsion*, Tohoku Math. J. (2) **65** (2013), no. 3, 357–371.

[18] C. Rasmussen and A. Tamagawa, *Arithmetic of abelian varieties with constrained torsion*, Trans. Amer. Math. Soc. **369** (2017), no. 4, 2395–2424.

[19] C. Rasmussen and A. Tamagawa, *A finiteness conjecture on abelian varieties with constrained prime power torsion*, Math. Res. Lett. **15** (2008), no. 6, 1223–1231.

[20] G. Rémond, *Variétés abéliennes et ordres maximaux*, Revista Matemática Iberoamericana **33** (2017), no. 4, 1173–1195

[21] K. A. Ribet, *Division fields of abelian varieties with complex multiplication*, Mém. Soc. Math. France (N.S.) (1980/81), no. 2, 75–94. Abelian functions and transcendental numbers (Colloq., École Polytech., Palaiseau, 1979).

[22] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517.

[23] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions, Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo; Princeton University Press, Princeton, N.J. (1971). Kanô Memorial Lectures, No. 1.

[24] G. Shimura, Abelian Varieties with Complex Multiplication and Modular Functions, Vol. 46 of Princeton Mathematical Series, Princeton University Press, Princeton, NJ (1998), ISBN 0-691-01656-9.

[25] G. Shimura and Y. Taniyama, Complex Multiplication of Abelian Varieties and Its Applications to Number Theory, Vol. 6 of Publications of the Mathematical Society of Japan, The Mathematical Society of Japan, Tokyo (1961).

[26] A. Silverberg, *Fields of definition for homomorphisms of abelian varieties*, J. Pure Appl. Algebra **77** (1992), no. 3, 253–262.

[27] H. M. Stark, *Some effective cases of the Brauer-Siegel theorem*, Invent. Math. **23** (1974), 135–152.

[28] J. Tsimerman, *Brauer-Siegel for arithmetic tori and lower bounds for Galois orbits of special points*, J. Amer. Math. Soc. **25** (2012), no. 4, 1091–1117.

[29] J. Tsimerman, *A proof of the André-Oort conjecture for* $\mathcal{A}_g$, Ann. of Math. (2) **187** (2018), no. 2, 379–390.

[30] E. Ullmo and A. Yafaev, *Nombre de classes des tores de multiplication complexe et bornes inférieures pour les orbites galoisiennes de points spéciaux*, Bull. Soc. Math. France **143** (2015), no. 1, 197–228.

[31] J. Wilson, *Curves of genus* 2 *with real multiplication by a square root of 5*, PhD Thesis (1998). Available at `http://eprints.maths.ox.ac.uk/32/`.

Dipartimento di Matematica, Università di Pisa
Largo Bruno Pontecorvo 5, 56127 Pisa, Italy
E-mail address: `davide.lombardo@unipi.it`

Received January 14, 2016