Rev. Mat. Iberoamericana **27** (2011), no. 3, 733–750

Finiteness of endomorphism algebras of CM modular abelian varieties

Josep González

Abstract

Let A_f be the abelian variety attached by Shimura to a normalized newform $f \in S_2(\Gamma_1(N))^{\mathrm{new}}$. We prove that for any integer $n > 1$ the set of pairs of endomorphism algebras $\big(\mathrm{End}_{\overline{\mathbb{Q}}}(A_f)\otimes\mathbb{Q}, \mathrm{End}_{\mathbb{Q}}(A_f)\otimes\mathbb{Q}\big)$ obtained from all normalized newforms f with complex multiplication such that $\dim A_f = n$ is finite. We determine that this set has exactly 83 pairs for the particular case $n = 2$ and show all of them. We also discuss a conjecture related to the finiteness of the set of number fields $\mathrm{End}_{\mathbb{Q}}(A_f) \otimes \mathbb{Q}$ for the non-CM case.

1. Introduction

For an abelian variety A defined over a field $\mathbb{L}$, we denote by $\mathrm{End}_{\mathbb{L}}(A)$ the ring of all its endomorphisms defined over $\mathbb{L}$ and $\mathrm{End}^0_{\mathbb{L}}(A) := \mathrm{End}_{\mathbb{L}}(A) \otimes \mathbb{Q}$ denotes is endomorphism algebra over $\mathbb{L}$. There is the following conjecture attributed to Robert Coleman.

Conjecture 1.1 *Let $n, m \geq 1$ be positive integers. Then, up to isomorphism, there is only finitely many $\mathbb{Q}$-algebras M such that $M \simeq \mathrm{End}^0_{\mathbb{L}}(A)$ for some abelian variety A of dimension n defined over a number field $\mathbb{L}$ of degree m.*

This conjecture is the starting point of this article and, next, we focus our attention on modular abelian varieties. Let us denote by $A_f/\mathbb{Q}$ the abelian variety attached by Shimura to a normalized newform $f \in S_2(\Gamma_1(N))^{\mathrm{new}}$ with Fourier expansion $\sum_{n>0} a_n q^n$, where $q = e^{2\pi i z}$. It is well-known that A_f is a simple quotient over $\mathbb{Q}$ of the jacobian of the modular curve $X_1(N)$, whose endomorphism algebra $\mathrm{End}^0_{\mathbb{Q}}(A_f)$ is isomorphic to the number field $\mathbb{E}_f = \mathbb{Q}(\{a_n\})$ and, moreover, $[\mathbb{E}_f : \mathbb{Q}] = \dim A_f$. Also, we know that any simple

2000 Mathematics Subject Classification: 11G18, 14K22.
Keywords: Modular abelian varieties, complex multiplication.

quotient over $\mathbb{Q}$ of $\mathrm{Jac}(X_1(M))$ is isogenous over $\mathbb{Q}$ to A_f for some $f \in S_2(\Gamma_1(N))^{\mathrm{new}}$ with $N \mid M$.

The modular abelian varieties A_f can be classified in three types according to their endomorphism algebras over $\overline{\mathbb{Q}}$. Indeed, every A_f is isogenous over $\overline{\mathbb{Q}}$ to a power of an absolutely simple abelian variety B_f. The center of the algebra $\mathcal{A} = \mathrm{End}^0_{\overline{\mathbb{Q}}}(A_f)$ is either an imaginary quadratic field $\mathbb{K}$ or the totally real number field $\mathbb{F} = \mathbb{Q}\big(\{a_p^2/\varepsilon(p)\}_{p\nmid N}\big)$. In the first case, $\mathcal{A}$ is a matrix algebra over $\mathbb{K}$, B_f is an elliptic curve with complex multiplication by $\mathbb{K}$ and it is said that f has CM by $\mathbb{K}$. Otherwise, either $\mathcal{A}$ is a matrix algebra over $\mathbb{F}$, i.e. B_f has real multiplication by $\mathbb{F}$ (RM), or $\mathcal{A}$ is a matrix algebra over a quaternion algebra $\mathcal{B}$ with center $\mathbb{F}$, i.e. B_f has quaternionic multiplication by $\mathcal{B}$ (QM).

For an integer $n \geq 1$, we consider the set $\mathcal{S}_n$ consisting of the pairs of isomorphic classes of $\mathbb{Q}$-algebras $(\mathrm{End}^0_{\overline{\mathbb{Q}}}(A_f), \mathrm{End}^0_{\mathbb{Q}}(A_f))$, where f runs over the set of normalized newforms with $\dim A_f = n$. As we show in Section 2, the set of degrees of the smallest number fields where the abelian varieties A_f of dimension n have all their endomorphisms defined is bounded. According to Conjecture 1.1, the set $\mathcal{S}_n$ should be finite. Of course, we know that for $n = 1$ this is true and, more precisely, $\mathcal{S}_1$ has exactly 10 pairs: $(\mathbb{Q}, \mathbb{Q})$ and the pairs $(\mathbb{K}, \mathbb{Q})$, where $\mathbb{K}$ is an imaginary quadratic field of class number one.

Since the algebra of endomorphisms defined over $\mathbb{Q}$ of a simple abelian variety over $\mathbb{Q}$ of dimension n is a $\mathbb{Q}$-vector space of dimension at most n, the modular abelian varieties A_f can be viewed as those with a richer arithmetical structure. Thus, the finiteness of the sets $\mathcal{S}_n$ appears as an interesting case to test Coleman's conjecture. This finiteness has been studied for modular abelian varieties with quaternionic multiplication, and partial results can be found in [17] and, for the particular case of surfaces, in [3]. Here, we center our attention on the CM case.

The plan of this paper is as follows. Section 2 is preliminary and devoted to introduce notation and summarize some known facts concerning modular abelian varieties with CM. In Section 3 we prove the modular conjecture for this class of modular abelian varieties and we also determine the set of pairs $(\mathrm{End}^0_{\overline{\mathbb{Q}}}(A_f)$, $\mathrm{End}^0_{\mathbb{Q}}(A_f))$ for the particular case $\dim A_f = 2$, which turns out to be the most laborious part of this article. In the last section we discuss the non-CM case. For every integer $n > 1$, we introduce a value $\widetilde{B}(n) \in \mathbb{N} \cup \{+\infty\}$ which depends on the Fourier coefficients of the normalized newforms f without CM with $\dim A_f = n$. We present some evidence that show that $\widetilde{B}(n)$ could be finite and prove that if this is the case, then the set of number fields $\mathbb{E}_f$ with $\dim A_f = n$ is finite, which implies the finiteness of the set $\mathcal{S}_n$ for the RM case. We finish this paper by giving a lower bound for $\widetilde{B}(2)$.

2. On modular abelian varieties with CM

Let us denote by New_N the set of normalized newforms of $S_2(\Gamma_1(N))$. For a given $f \in \mathrm{New}_N$ with Fourier expansion $\sum_{n>0} a_n q^n$ and a Dirichlet character ν of conductor M, we denote by $f \otimes \nu$ the only normalized newform with q-expansion $\sum_{n>0} b_n q^n$ that satisfies $b_n = \nu(n)\, a_n$ for all integers n with $(n, N\,M) = 1$.

Let $\mathbb{K}$ be an imaginary quadratic field in a fixed algebraic closure $\overline{\mathbb{Q}}$. We denote by $\mathcal{O}$ its ring of integers and by χ the Dirichlet character attached to $\mathbb{K}$. Let $f = \sum_{n>0} a_n q^n \in \mathrm{New}_N$. By [16], we know that the following three conditions are equivalent:

(i) The newform f has CM by $\mathbb{K}$.

(ii) The newform f satisfies $f = f \otimes \chi$, i.e. $a_n = \chi(n) a_n$ for all positive integers with $(n, N) = 1$.

(iii) There is a primitive Hecke character $\psi : I(\mathfrak{m}) \to \overline{\mathbb{Q}}^*$ of conductor an integral ideal $\mathfrak{m}$ of $\mathbb{K}$ such that

$$f = \sum_{\mathfrak{a} \in I(\mathfrak{m}), \mathfrak{a} \subset \mathcal{O}} \psi(\mathfrak{a}) q^{\mathrm{N}(\mathfrak{a})}\,,$$

where $I(\mathfrak{m})$ denotes the multiplicative group of fractional ideals of $\mathbb{K}$ relatively prime to $\mathfrak{m}$ and $\mathrm{N}(\mathfrak{a})$ denotes the norm of the ideal $\mathfrak{a}$.

Moreover, for a Hecke character ψ as above, the level N of f is $\mathrm{N}(\mathfrak{m})$ times D, where D is the absolute value of the discriminant of $\mathbb{K}$. Attached to ψ we also have:

- The number fields $\mathbb{E}_f = \mathbb{Q}(\{a_n\})$ and $\mathbb{E} = \mathbb{Q}(\{\psi(\mathfrak{a})\})$. One has

$$\mathbb{E} = \mathbb{E}_f \mathbb{K}.$$

- The character $\eta_\psi : (\mathcal{O}/\mathfrak{m})^* \to \overline{\mathbb{Q}}^*$ defined by $\eta_\psi(a) = \psi((a))/a$, which is also primitive of conductor $\mathfrak{m}$ and satisfies $\eta_\psi(u) = 1/u$ for $u \in \mathcal{O}^*$. For every primitive character η of conductor $\mathfrak{m}$ satisfying the last condition we have $\eta = \eta_\psi$ for some primitive Hecke character ψ of conductor $\mathfrak{m}$. When there is no risk of confusion, we shall write η instead of η_ψ.
- The Nebentypus ε of f, which is the Dirichlet character mod N defined by $\varepsilon(d) = \chi(d)\eta(d)$.
- The totally real number field $\mathbb{L}_\varepsilon = \overline{\mathbb{Q}}^{\ker \varepsilon}$. Here ε is viewed as a character of the absolute Galois group $\mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$.

Let us denote by Φ the set of $\mathbb{K}$-embeddings $\mathbb{E} \hookrightarrow \overline{\mathbb{Q}}$. In [10] the following is proved:

(i) There is a quotient abelian variety A of A_f defined over $\mathbb{K}$ equipped with an isomorphism $\iota : \mathbb{E} \xrightarrow{\simeq} \mathrm{End}_{\mathbb{K}}(A) \otimes \mathbb{Q}$ such that (A, ι) is of CM-type Φ over $\mathbb{K}$.

(ii) The abelian varieties A_f and A are $\mathbb{K}$-isogenous if and only if $\mathbb{K} \not\subseteq \mathbb{E}_f$. Otherwise, A_f is $\mathbb{K}$-isogenous to $A \times \overline{A}$, where the bar $^-$ stands for complex conjugation.

(iii) The smallest number field $\mathbb{L}$ where A has all its endomorphisms defined is a cyclic extension of the Hilbert class field $\mathbb{H}$ of $\mathbb{K}$ which is contained in the ray class field of $\mathbb{K}$ mod $\mathfrak{m}$ and such that $[\mathbb{L} : \mathbb{H}] = \mathrm{ord}\, \eta / |\mathcal{O}^*|$. The extension $\mathbb{L}/\mathbb{K}$ is characterized by the property that a prime ideal $\mathfrak{p} \in I(\mathfrak{m})$ splits completely in $\mathbb{L}$ if and only if $\psi(\mathfrak{p}) \in \mathbb{K}$.

(iv) There exists an elliptic curve E defined over $\mathbb{L}$ with CM by $\mathcal{O}$ such that $E^{\dim A}$ and A are isogenous over $\mathbb{L}$.

We say that a number field is the splitting field of an abelian variety if it is the smallest number field where the abelian variety has all its endomorphisms defined. Thus, the number field $\mathbb{L}$ in *(iii)* is the splitting field of A.

Given a Hecke character ψ of conductor $\mathfrak{m}$, the character $\psi_c : I(\overline{\mathfrak{m}}) \to \overline{\mathbb{Q}}$ defined by $\psi_c(\mathfrak{a}) = \overline{\psi(\overline{\mathfrak{a}})}$ is a Hecke character of conductor $\overline{\mathfrak{m}}$ whose attached newform is $\overline{f}$. The condition $\mathbb{K} \not\subseteq \mathbb{E}_f$ is equivalent to the equality $\psi_c = {}^{\sigma}\psi$ for some $\sigma \in \Phi$ and, in this case, $\mathbb{L}$ is the splitting field of A_f.

In the next section we will use the following result.

Proposition 2.1 *Let ψ be a Hecke character of $\mathbb{K}$ of conductor $\mathfrak{m}$ whose attached newform $f = \sum_{n \geq 0} a_n q^n \in \mathrm{New}_N$ has Nebentypus ε. Assume $\mathbb{K} \not\subseteq \mathbb{E}_f$. We have that*

(i) *The ideal $\mathfrak{m}$ coincides with $\overline{\mathfrak{m}}$.*

(ii) *The extension $\mathbb{L}/\mathbb{Q}$ is Galois.*

(iii) *The number field $\mathbb{L}_\varepsilon$ is contained in $\mathbb{L}$.*

(iv) *There exists an elliptic curve E with CM by $\mathcal{O}$ defined over $\mathbb{L}_0$ such that $E^{\dim A_f}$ and A_f are isogenous over $\mathbb{L}_0$, where $\mathbb{L}_0$ is the maximal real subfield of $\mathbb{L}$.*

Moreover, the following conditions are equivalent:

(a) *The Nebentypus ε is trivial, i.e., $f \in S_2(\Gamma_0(N))$.*

(b) *The number field $\mathbb{E}_f$ is totally real.*

(c) *The Hecke characters ψ and ψ_c agree.*

(d) *For all positive integers n coprime to N we have $\eta(n) = \chi(n)$.*

Proof. Part (i) is proved in Lemma 2.1 in [10]. Since $\psi_c = {}^{\sigma}\psi$ for $\sigma \in \Phi$, $\ker \eta = \ker \eta_{\psi_c}$ and, thus, $\ker \eta$ is stable under complex conjugation. This fact implies $\mathbb{L} = \overline{\mathbb{L}}$ (cf. Section 3 in [10]) and, therefore, $\mathbb{L}/\mathbb{Q}$ is a Galois extension. Next, we give two proofs for the inclusion $\mathbb{L}_\varepsilon \subset \mathbb{L}$, because the arguments involved in both of them will be used in the sequel.

Since $\mathbb{L}/\mathbb{Q}$ is a Galois extension, it suffices to prove that every rational prime $p \nmid N$ which splits completely in $\mathbb{L}$, also splits completely in $\mathbb{L}_\varepsilon$. Let $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ be the prime ideals of $\mathbb{K}$ over such a prime p. Due to the fact that $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ split completely in $\mathbb{L}$, we have $\psi(\mathfrak{p}), \psi(\overline{\mathfrak{p}}) \in \mathbb{K}$. The condition $\psi_c = {}^{\sigma}\psi$ for some $\sigma \in \Phi$ implies $\psi(\overline{\mathfrak{p}}) = \overline{\psi(\mathfrak{p})}$ and, thus, $a_p = \psi(\mathfrak{p}) + \psi(\overline{\mathfrak{p}}) \in \mathbb{Z}$. Since all elliptic curves with CM by $\mathcal{O}$ are ordinary at every prime of good reduction over a rational prime which splits in $\mathbb{K}$ and A_f has good reduction at all primes not dividing N, $a_p \not\equiv 0 \pmod{p}$ (see Proposition 5.2 in [2]) and, in particular, $a_p \neq 0$. Hence, $\varepsilon(p) = a_p/\overline{a_p} = 1$ and it follows that p splits completely in $\mathbb{L}_\varepsilon$.

Now, we present an alternative proof of part (iv). The Weil involution W_N of $X_1(N)$ is defined over the N-th cyclotomic field $\mathbb{Q}(\zeta_N)$ and satisfies ${}^{\tau_d}W_N = W_N \langle d \rangle$ for all $d \in (\mathbb{Z}/N\mathbb{Z})^*$, where τ_d is the element of $\mathrm{Gal}\,(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ mapping ζ_N to ζ_N^d and $\langle d \rangle$ denotes the diamond automorphism of $X_1(N)$, which is defined over $\mathbb{Q}$. The Weil involution and the diamonds induce automorphisms on A_f. Since $\langle d \rangle$ acts trivially on A_f if and only if $\varepsilon(d) = 1$, $\mathbb{L}_\varepsilon$ is the smallest field of definition for W_N acting on A_f and, thus, $\mathbb{L}_\varepsilon \subset \mathbb{L}$.

Let us prove part (iv). We know that A_f is isogenous over $\mathbb{L}$ to $E^{\dim A_f}$ for some elliptic curve E with CM by $\mathcal{O}$. Since $\mathbb{L}$ is the splitting field of A_f, we can take E with j-invariant $j(\mathcal{O})$ together with an isomorphism $\mu : E \to \overline{E}$ defined over $\mathbb{L}$. Due to the action of μ and $\overline{\mu}$ on regular differentials of E and $\overline{E}$, we obtain that $\overline{\mu} \circ \mu = \mathrm{id}$. Therefore, by Weil's descent criterion (cf. [18]) we know that E admits a descent over $\mathbb{L}_0$ and, we can assume that E is defined over $\mathbb{L}_0$. By Faltings's criterion, to prove the statement it suffices to check, that for every prime $\mathfrak{P}_0$ of $\mathbb{L}_0$ over a prime $p \nmid N$ with $\mathrm{N}_{\mathbb{L}_0/\mathbb{Q}}(\mathfrak{P}_0) = p^m$, the reductions of A_f and $E^{\dim A_f}$ modulo $\mathfrak{P}_0$ are isogenous over $\mathbb{F}_{p^m}$. When $\mathfrak{P}_0$ splits in $\mathbb{L}$, this fact is obvious. Since $p \nmid N$, $\mathfrak{P}_0$ does not ramify in $\mathbb{L}$ so we can assume that $\mathfrak{P}_0$ is inert in $\mathbb{L}$. The prime p is also inert in $\mathbb{K}$ because $\mathbb{L} = \mathbb{L}_0\,\mathbb{K}$ and, thus, m is the residue degree of $p\,\mathcal{O}$ over $\mathbb{L}$. Since $\mathbb{L}_\varepsilon \subset \mathbb{L}_0$, $\varepsilon(p^m) = 1$ and $a_{p^2}^m = \psi(p\mathcal{O})^m = \eta(p^m)\,p^m = (-1)^m p^m$. Due to the fact that the residue degree of any prime ideal $\mathfrak{p} \in I(\mathfrak{m})$ in $\mathbb{L}$ is the smallest positive exponent e such that $\psi(\mathfrak{p})^e \in \mathbb{K}$, m is odd. Let us denote by $\mathfrak{P}$ the prime ideal of $\mathbb{L}$ over $\mathfrak{P}_0$. By the Eichler-Shimura congruence, the characteristic polynomial of the endomorphism $\mathrm{Frob}_{\mathfrak{P}}$ acting on the l-adic Tate module of the reduction of $A_f/\mathbb{L}$ modulo $\mathfrak{P}$ is $(x+p^m)^{2\dim A_f}$

and, consequently, the characteristic polynomial of the endomorphism $\mathrm{Frob}_{\mathfrak{P}}$ corresponding to the reduction of $E/\mathbb{L}$ modulo $\mathfrak{P}$ is $(x+p^m)^2$. It follows that the characteristic polynomials of the endomorphism $\mathrm{Frob}_{\mathfrak{P}_0}$ acting on the l-adic Tate modules of the reductions of $A_f/\mathbb{L}_0$ and $E/\mathbb{L}_0$ modulo $\mathfrak{P}_0$ are $(x^2+p^m)^{\dim A_f}$ and x^2+p^m respectively, which completes the proof of part (iv).

Finally, note that the equivalence between (a) and (b) holds for any newform in New_N. Indeed, if ε is trivial, then it is obvious that $\mathbb{E}_f$ is totally real. For the converse, see the proof of Lemma 6.17 of [1]. The remaining equivalences of the statement are immediate. ■

Remark 2.1 Observe that the splitting field of A_f is $\mathbb{L}\,\mathbb{L}_\varepsilon$. Indeed, by part (iii) of the above proposition, it is immediate for $\mathbb{K}\not\subseteq\mathbb{E}_f$. When $\mathbb{K}\subseteq\mathbb{E}_f$, it follows from the fact that $\mathbb{L}$ is the splitting field of A and $\mathbb{K}\,\mathbb{L}_\varepsilon$ is the smallest field of definition of the induced morphism by the Weil involution W_N between A and $\overline{A}$.

Proposition 2.2 *Let n be a positive integer. The set of degrees of the splitting fields of all abelian varieties A_f of dimension n (with or without CM) is bounded.*

Proof. Assume that $\dim A_f=n$ and let us denote by $\mathbb{M}$ the splitting field of A_f. Let k be the greatest integer such that $\varphi(k)\mid 2n$, where φ stands for Euler's function. It is clear that $[\mathbb{L}_\varepsilon:\mathbb{Q}]\le k$.

First, we consider the CM case. With the above notation, $\mathbb{M}=\mathbb{L}\,\mathbb{L}_\varepsilon$ and, moreover, $\operatorname{ord}\eta\le k$ since $\mathbb{Q}(\eta)\subseteq\mathbb{E}$. Due to the fact that the class number of $\mathbb{K}$ divides $[\mathbb{E}:\mathbb{K}]$ (cf. Theorem 3.1 of [19]) and $[\mathbb{E}:\mathbb{K}]$ divides n, we obtain

$$[\mathbb{M}:\mathbb{Q}]\le[\mathbb{L}:\mathbb{Q}]\,[\mathbb{L}_\varepsilon:\mathbb{Q}]\le[\mathbb{H}:\mathbb{Q}]\,\operatorname{ord}\eta\,k\le 2nk^2\,.$$

For the non-CM case, the number field $\mathbb{M}$ is described in Proposition 2.1 of [9] and it is easy to check that $[\mathbb{M}:\mathbb{Q}]\le 2^n\,k$. ■

3. Finiteness for the CM case

Let us denote by $\mathrm{New}_N^{\mathrm{cm}}$ the subset of New_N consisting of the newforms with CM by an imaginary quadratic field. For every integer $n>0$, let us define $\mathcal{S}_n^{\mathrm{cm}}$ as the set of pairs of number fields $(\mathbb{K},\mathbb{M})$ such that $\mathbb{K}$ is an imaginary quadratic field, $\mathbb{M}\simeq\mathbb{E}_f$ for some $f\in\mathrm{New}_N^{\mathrm{cm}}$ with CM by $\mathbb{K}$ and $[\mathbb{M}:\mathbb{Q}]=n$. It is clear that the map $\mathcal{S}_n^{\mathrm{cm}}\to\mathcal{S}_n$ sending a pair $(\mathbb{K},\mathbb{M})$ to $(\mathrm{M}_n(\mathbb{K}),\mathbb{M})$ yields a bijection between $\mathcal{S}_n^{\mathrm{cm}}$ and the subset of $\mathcal{S}_n$ obtained from newforms with CM.

Theorem 3.1 *For any $n > 0$, the set $\mathcal{S}_n^{\mathrm{cm}}$ is finite.*

Proof. Let us prove that the set $\{(\mathbb{K}, \mathbb{M}\cdot\mathbb{K}) : (\mathbb{K},\mathbb{M}) \in \mathcal{S}_n^{\mathrm{cm}}\}$ is finite, which is equivalent to the statement. Take $f \in \mathrm{New}_N^{\mathrm{cm}}$ attached to a Hecke character ψ of an imaginary quadratic field $\mathbb{K}$ such that $\dim A_f = n$. By Theorem 3.1 of [19], the class number h of $\mathbb{K}$ divides n and, moreover, the order k of η satisfies that $\varphi(k) \mid 2\,n$.

We set $\mathcal{N} = \{m \in \mathbb{Z}^+ : \varphi(m) \mid 2\,n\}$ and denote by $\mathcal{K}$ the set of imaginary quadratic fields whose class number divides n. It is clear that both sets are finite and, consequently, it suffices to prove that, for every pair $(\mathbb{K}, k) \in \mathcal{K}\times\mathcal{N}$, the set of number fields $\mathbb{Q}(\psi) = \mathbb{Q}(\{\psi(\mathfrak{a})\})$ obtained when ψ runs over the set of Hecke characters of $\mathbb{K}$ whose attached character η has order k is finite (even without fixing the degree of $\mathbb{Q}(\psi)$).

We denote by ζ_m a primitive m-th root of unity. Given a pair $(\mathbb{K}, k) \in \mathcal{K}\times\mathcal{N}$, take a Hecke character ψ of $\mathbb{K}$ of conductor $\mathfrak{m}$ for which η has order k. Let $\{\mathfrak{a}_1, \ldots, \mathfrak{a}_h\}$ be a set of representative ideals of the class group of $\mathbb{K}$ and let us denote by n_i, $1 \le i \le h$, the order of $\mathfrak{a}_i$ in $\mathrm{Gal}(\mathbb{H}/\mathbb{K})$. For every positive integer $i \le h$, we take $a_i \in \overline{\mathbb{Q}}$ such that $a_i^{n_i} \in \mathbb{K}$ and $a_i^{n_i}\mathcal{O} = \mathfrak{a}_i^{n_i}$. Choose $\alpha_i \in \mathbb{K}$ such that $\alpha_i\mathfrak{a}_i$ is relatively prime to $\mathfrak{m}$. Then, $\mathbb{Q}(\psi) = \mathbb{K}(\zeta_k)(\psi(\alpha_1\mathfrak{a}_1), \ldots, \psi(\alpha_h\mathfrak{a}_h))$. Since $\psi(\alpha_i\mathfrak{a}_i)^{n_i} = a_i^{n_i}\alpha_i^{n_i}\eta(a_i\alpha_i)^{n_i}$, the statement follows from the fact that $\mathbb{Q}(\psi)$ is a subfield of the number field $\mathbb{K}(\zeta_{k\,h})(a_1, \ldots, a_h)$. ■

Next, we focus our attention on the two dimensional case. In order to simplify the notation, we represent an element $(\mathbb{K},\mathbb{M}) \in \mathcal{S}_2^{\mathrm{cm}}$ by the pair $(-d, m)$, where d is the positive square-free integer such that $\mathbb{K} = \mathbb{Q}(\sqrt{-d})$ and $m \neq 1$ is the square-free integer such that $\mathbb{M} = \mathbb{Q}(\sqrt{m})$.

Theorem 3.2 *With the above notation, the set $\mathcal{S}_2^{\mathrm{cm}}$ has exactly the following 83 pairs:*

(i) *For the values of d such that $\mathbb{Q}(\sqrt{-d})$ has class number $h = 1$:*

d	1	3	$2, 7, 11, 19, 43, 67, 163$
m	$-1, \pm 2, \pm 3$	$-1, \pm 3$	$-1, -3, \pm d, 3d$

(ii) *For the values of d such that $\mathbb{Q}(\sqrt{-d})$ has class number $h = 2$:*

d	$3{\cdot}5,\ 7{\cdot}5,\ 3{\cdot}17,\ 7{\cdot}13,\ 5{\cdot}23,\ 3{\cdot}41,\ 11{\cdot}17,\ 5{\cdot}47,\ 3{\cdot}89,\ 13{\cdot}31,\ 7{\cdot}61$
m	$\pm p_1$

where p_1 is the unique prime dividing d such that $p_1 \equiv 1 \pmod 4$, and also

d	$5, 13, 37$	$2\cdot 3, 2{\cdot}11$	$2{\cdot}5, 2{\cdot}29$
m	$-1, d$	$-1, \pm 2$	$-1, \pm d/2$

.

Proof. We know that all $f \in \mathrm{New}_N^{\mathrm{cm}}$ with $\dim A_f = 2$ have CM by an imaginary quadratic field whose class number is either 1 or 2. From now on, $\mathbb{K}$ is an imaginary quadratic field of discriminant $-D$ and class number $h \leq 2$. The square-free part d of D is either D or $D/4$ depending on whether D is odd or not. Let us denote by w the order of $\mathcal{O}^*$, namely w is 2, 4 or 6 according to $D > 4$, $D = 4$ or $D = 3$, respectively.

Firstly, we prove that $(-d, -d) \in \mathcal{S}_2^{\mathrm{cm}}$ if and only if $h = 1$. Indeed, if $(-d, -d) \in \mathcal{S}_2^{\mathrm{cm}}$ then $\mathbb{E}_f = \mathbb{K}$ and $[\mathbb{E} : \mathbb{K}] = 1$, which implies $h = 1$. Conversely, assume $h = 1$ and let $\mathfrak{p}$ be a prime ideal over an odd prime p which splits in $\mathbb{K}$, so that $p \equiv 1 \pmod{w}$. We can choose p such that $p \equiv 1 + w \pmod{w^2}$ and, thus, there exists a character η of conductor $\mathfrak{p}$ and order w satisfying $\eta(u) = 1/u$ for all $u \in \mathcal{O}^*$. A Hecke character ψ of conductor $\mathfrak{m} = \mathfrak{p}$ and character η provides a newform f with $\mathbb{E} = \mathbb{K}$. Since $\mathfrak{m} \neq \overline{\mathfrak{m}}$, part 2 of Proposition 2.1 implies that $\mathbb{K} \subseteq \mathbb{E}_f$, and then $\mathbb{E}_f = \mathbb{E} = \mathbb{K}$. Therefore, for $h = 1$ all pairs $(-d, -d)$ lie in $\mathcal{S}_2^{\mathrm{cm}}$.

From now on, we focus our attention on Hecke characters ψ whose number field $\mathbb{E}$ is a biquadratic field $\mathbb{Q}(\sqrt{-d}, \sqrt{m})$ for which $\mathbb{E}_f = \mathbb{Q}(\sqrt{m}\,)$. We recall that, in this case, Proposition 2.1 applies and $\mathbb{L}$ is the splitting field of A_f. We split the proof in two cases according to the class number h, and for each of them we examine all possibilities for the values of $\mathrm{ord}(\eta)$.

(1) Case $h = 1$. In this case, $\mathbb{E} = \mathbb{K}(\eta)$ and $[\mathbb{K}(\eta) : \mathbb{K}] = 2$. Therefore, $\varphi(k)/\varphi(w) = 2$, where k is the order of η. So we have the following possibilities for k, $\mathbb{E}$ and m:

	$d = 1$		$d = 3$	$d \neq 1, 3$	
k	8 ;	12	12	4 ;	6
$\mathbb{E}$	$\mathbb{Q}(\sqrt{-1}, \sqrt{-2}\,)$;	$\mathbb{Q}(\sqrt{-1}, \sqrt{-3})$	$\mathbb{Q}(\sqrt{-1}, \sqrt{-3})$	$\mathbb{Q}(\sqrt{-d}, \sqrt{-1})$;	$\mathbb{Q}(\sqrt{-d}, \sqrt{-3})$
m	$-2, 2$;	$-3, 3$	$-1, 3$	$-1, d$;	$-3, 3d$

Next, we prove that all these possibilities for $(-d, m)$ do occur. Let $\mathfrak{l}$ be the prime ideal of $\mathbb{K}$ over the unique rational prime ℓ dividing D and consider the integral ideal $\mathfrak{m}_0$ defined by

$$\mathfrak{m}_0 = \begin{cases} \mathfrak{l} & \text{if } D \neq 3 \text{ is odd,} \\ \mathfrak{l}^2 & \text{if } D = 3, \\ \mathfrak{l}^3 & \text{if } D = 4, \\ \mathfrak{l}^5 & \text{if } D = 8\,. \end{cases}$$

Let η_0 be a character mod $\mathfrak{m}_0$ satisfying the following three conditions: the order of η_0 is w, $\eta_0(u) = 1/u$ for all $u \in \mathcal{O}^*$ and $\eta_0(n)\,\chi(n)$ is the trivial Dirichlet character mod D. Note that η_0 is unique except for $D = 8$.

Let ψ_0 be the unique Hecke character of conductor $\mathfrak{m}_0$ with character η_0. Since $\mathbb{Q}(\psi_0)=\mathbb{K}$ and the newform f_0 attached to ψ_0 has trivial Nebentypus, $\dim A_{f_0}=1$. By taking Dirichlet characters χ_1 of order 4 if $d\neq 1$ and χ_2 of order 3 if $d\neq 3$, the newforms $f_0\otimes\chi_1$ and $f_0\otimes\chi_2$ have CM by $\mathbb{K}$ and provide the values $m=-1$ and $m=-3$, respectively. This yields $(-d,-1),(-d,-3)\in\mathcal{S}_2^{\rm cm}$ for all d when $h=1$.

For $d\neq 3$, take an inert prime p in $\mathbb{K}$ such that $p\equiv -1 \pmod 3$. Choose a character η' mod $p\mathcal{O}$ of order 3. The newform obtained from a Hecke character of conductor $\mathfrak{m}=\mathfrak{m}_0\cdot p\,\mathcal{O}$ and character $\eta=\eta_0\times\eta'$ has trivial Nebentypus. Since $\mathbb{E}=\mathbb{Q}(\sqrt{-d},\sqrt{-3})$, it follows $(-d,3d)\in\mathcal{S}_2^{\rm cm}$.

For $d\neq 1$, take an inert prime $\mathfrak{p}$ in $\mathbb{K}$ such that $p\equiv -1 \pmod 4$ and choose a character η' mod $p\mathcal{O}$ of order 4. Proceeding as before for the character $\eta_0\times\eta'$, we obtain $(-d,d)\in\mathcal{S}_2^{\rm cm}$.

For $d=1$, take $p=7$ and the character η' mod $p\mathcal{O}$ of order 8 defined by $\eta'(2+i)=(1+i)\sqrt{2}/2$. For the character $\eta=\overline{\eta_0}\times\eta'$, we obtain $(-1,2)\in\mathcal{S}_2^{\rm cm}$.

To complete the case $h=1$, we need to prove $(-1,-2)\in\mathcal{S}_2^{\rm cm}$. Take the characters η_2 and η_3 mod $2\mathcal{O}$ and $3\mathcal{O}$, respectively, defined by $\eta_2(i)=-1$ and $\eta_3(1-i)=(1+i)\sqrt{2}/2$. The newform f obtained from a Hecke character with character $\eta_2\times\eta_3$ satisfies $\mathbb{E}_f=\mathbb{Q}(\sqrt{-2})$.

(2) Case $\boldsymbol{h=2}$. If $[\mathbb{E}:\mathbb{Q}]=4$, then the order k of η can only be 2, 4 or 6 and, moreover, k must divide $2\,D$ (cf. Theorem 3.5 of [19]). Note that, in this particular setting, $\mathbb{E}_f$ is a quadratic field if and only if $\psi_c={}^{\sigma}\psi$ for some $\sigma\in\Phi$. Therefore, for all $\alpha\in(\mathcal{O}/\mathfrak{m})^*$, we have $\eta(\overline{\alpha})=\overline{\eta(\alpha)}$ if ε is trivial and, otherwise, $\eta(\overline{\alpha})=\overline{{}^{\sigma}\eta(\alpha)}=\eta(\alpha)$ for the non-trivial $\sigma\in\operatorname{Gal}(\mathbb{E}/\mathbb{K})$ (for $k=2$, both conditions agree). In particular, if $\mathfrak{m}=\mathfrak{m}_1{\cdot}\mathfrak{m}_2$ with $(\mathfrak{m}_1,\mathfrak{m}_2)=1$, $\mathfrak{m}_i=\overline{\mathfrak{m}}_i$ for $i\leq 2$, and $\eta=\eta_1\times\eta_2$, where η_i is a character mod $\mathfrak{m}_i$, then each η_i has to satisfy the same condition as η for all $\alpha\in(\mathcal{O}/\mathfrak{m}_i)^*$.

When $h=2$, D has exactly two prime divisors. Let ℓ be such a prime satisfying that the prime ideal of $\mathbb{K}$ over ℓ is non-principal. For a given non-principal prime ideal $\mathfrak{p}\in I(\mathfrak{m})$, we have $\mathfrak{p}^2=\alpha^2\,\ell\mathcal{O}$ for some $\alpha\in\mathbb{K}^*$ and, thus, $\psi(\mathfrak{p})^2=\alpha^2\,\ell\eta(\alpha^2\,\ell)$ and $\sqrt{\ell\,\eta(\alpha^2\,\ell)}\in\mathbb{E}$. Therefore, we have to consider the only following possibilities for k and $\mathbb{E}$:

	D	$4\mid D$	$3\mid D$
k	2	4	6
$\mathbb{E}$	$\mathbb{Q}(\sqrt{-d},\sqrt{\ell})$, $\mathbb{Q}(\sqrt{-d},\sqrt{-\ell})$	$\mathbb{Q}(\sqrt{-d},\sqrt{-1})$	$\mathbb{Q}(\sqrt{-d},\sqrt{-3})$

Next, we split the proof according to the value of k.

(*i*) *Subcase* $k=2$. In this case, $\mathbb{L}=\mathbb{H}$ and, again by Theorem 3.5 of [19], we know that $[\mathbb{E}:\mathbb{K}]=2$ for any Hecke character of $\mathbb{K}$ with $k=2$.

Let p_1 be the prime that divides d such that the field $\mathbb{K}'=\mathbb{Q}(\sqrt{p_1})$ is the real quadratic subfield of $\mathbb{H}$. Let us now prove that, for $h=2$ and $k=2$, the pair $(-d,m)$ lies in $\mathcal{S}_2^{\rm cm}$ if and only if $D\not\equiv 4 \pmod 8$ and $\mid m\mid = p_1$.

Let ψ be a Hecke character such that $\operatorname{ord}\eta=2$ and $\mathbb{E}_f=\mathbb{Q}(\sqrt{m})$. Since $\mathbb{H}$ is the splitting field of A_f, there exists an elliptic curve defined over $\mathbb{H}$ with CM by $\mathcal{O}$ which has all the isogenies to its Galois conjugates defined over $\mathbb{H}$. The case $D\equiv 4 \pmod 8$, i.e. $D=4\cdot p_1$ with $p_1\equiv 1 \pmod 4$, cannot occur because there are no elliptic curves with CM by $\mathcal{O}$ satisfying this property (see 11.3 in [11]). If $D\not\equiv 4 \pmod 8$, then d/p_1 is the other prime p_2 that divides D and, moreover, the number field $\mathbb{E}$ is either $\mathbb{Q}(\sqrt{-d},\sqrt{p_1})$ or $\mathbb{Q}(\sqrt{-d},\sqrt{-p_1})$, which implies $\mid m\mid\in\{p_1,p_2\}$. By Proposition 2.1, there exists an elliptic curve E with CM by $\mathcal{O}$ defined over $\mathbb{K}'$ such that A_f is isogenous over $\mathbb{Q}$ to the Weil restriction $\operatorname{Res}_{\mathbb{K}'}E$. Since $\mathbb{E}_f=\mathbb{Q}(\sqrt{m})$, for the non-trivial $\sigma\in\operatorname{Gal}(\mathbb{K}'/\mathbb{Q})$ there is $\mu\in\operatorname{Hom}_{\mathbb{K}'}(E,{}^\sigma E)\otimes\mathbb{Q}$ such that $\mu\circ{}^\sigma\mu=[m]$, which implies that m is a norm of $\mathbb{K}'$. Due to the fact that neither p_2 nor $-p_2$ are norms of $\mathbb{K}'$, it follows that $\mid m\mid = p_1$.

Next, we prove that, for $D\not\equiv 4 \pmod 8$, the pairs $(d,\pm p_1)\in\mathcal{S}_2^{\rm cm}$. Let us denote by $\mathfrak{p}_1$ and $\mathfrak{p}_2$ the ideals over p_1 and p_2, respectively. Take the integral ideals

$$\mathfrak{m}_0=\begin{cases}\mathfrak{p}_1\cdot\mathfrak{p}_2 & \text{if } p_1 \text{ and } p_2 \text{ are odd},\\ \mathfrak{p}_1\cdot\mathfrak{p}_2^5 & \text{if } p_2=2,\\ \mathfrak{p}_1^5\cdot\mathfrak{p}_2 & \text{if } p_1=2,\end{cases}\qquad\text{and}\quad \mathfrak{m}_1=\begin{cases}\mathfrak{p}_2 & \text{if } p_2 \text{ is odd},\\ \mathfrak{p}_2^5 & \text{if } p_2=2.\end{cases}$$

For a quadratic character η_0 of conductor $\mathfrak{m}_0$ such that $\eta_0(n)=\chi(n)$ for all integers n coprime to D, we obtain a Hecke character ψ whose newform has trivial Nebentypus and, thus, $\mathbb{E}_f$ is a real quadratic field. Therefore $m=p_1$. For an odd quadratic character η_1 of conductor $\mathfrak{m}_1$, we obtain a Hecke character ψ whose newform f has non-trivial Nebentypus and its Fourier coefficient a_{p_1} satisfies $a_{p_1}^2=-p_1$. Therefore, $\mathbb{E}=\mathbb{K}(\sqrt{-p_1})$. It can be easily proved that, for a prime $\mathfrak{p}$ of $\mathbb{K}$, one has $\psi(\mathfrak{p})=\psi_c(\mathfrak{p})\in\mathbb{K}$ when $\mathfrak{p}$ is principal and, otherwise, $\psi(\mathfrak{p})=-\psi_c(\mathfrak{p})$ and $\psi(\mathfrak{p})\sqrt{-p_1}\in\mathbb{K}$. Hence, $\psi_c={}^\sigma\psi$ for the non-trivial $\sigma\in\operatorname{Gal}(\mathbb{E}/\mathbb{K})$ and, thus, $\mathbb{E}_f=\mathbb{Q}(\sqrt{-p_1})$.

(ii) Subcase $k=4$. For a Hecke character with $k=4$, we know by [19] that $[\mathbb{E}:\mathbb{K}]=2$ if and only if $4\mid D$ and $\eta(2\,\alpha^2)$ has order 4 for some (and every) $\alpha\in\mathbb{K}^*$ such that $2\,\alpha^2\mathcal{O}\in I(\mathfrak{m})$. The last condition amounts to saying that, for any generator β of the square of some (and every) non-principal prime ideal $\mathfrak{p}\in I(\mathfrak{m})$, $\eta(\beta)$ has order 4. If this is the case, $\mathbb{E}=\mathbb{Q}(\sqrt{-d},\sqrt{d})$ and we only have to consider the cases $m=-1$ and $m=d$. So we can assume $4\mid D$ and, in this case, D has a unique odd prime divisor p_1. We denote by $\mathfrak{p}_1$ and $\mathfrak{p}_2$ the prime ideals over p_1 and 2, respectively.

We first prove that, for $k = 4$, $(-d, d) \in \mathcal{S}_2^{\rm cm}$ if and only if d is odd, *i.e.*, $D \equiv 4 \pmod 8$.

For d odd, take $\mathfrak{m} = \mathfrak{p}_1 \cdot \mathfrak{p}_2^3$ and $\eta = \eta_1 \times \eta_2$, where η_1 is the quadratic character mod $\mathfrak{p}_1$ and η_2 is a character mod $\mathfrak{p}_2^3$ of order 4 ($\eta_2(\sqrt{-p_1}) = \pm i$). For each possible value of d ($d = 5, 13, 37$), it is easy to find a generator β of the square of a non-principal prime ideal $\mathfrak{p}$ and check that its real part is even. So $\eta(\beta) = \pm\eta_2(\beta)$ has order 4 because $\eta_2(\beta^2) = -1$ and $\mathbb{E} = \mathbb{Q}(\sqrt{-d}, \sqrt{d})$. Since $\varepsilon = 1$, we obtain $(-d, d) \in \mathcal{S}_2^{\rm cm}$.

Assume now that d is even and $\mathbb{E}_f = \mathbb{Q}(\sqrt{d})$. Since $\mathfrak{m} = \overline{\mathfrak{m}}$, η is primitive of conductor $\mathfrak{m}$ and $\eta(n) = \chi(n)$ for all integers n coprime to the level N of f, it must be that:

- The ideal $\mathfrak{m}$ is of the form $\mathfrak{p}_1 \cdot \mathfrak{p}_2^5 \cdot \prod_{i=1}^r p_i'\mathcal{O}$ for some primes p_i' with $(p_i', D) = 1$,
- The character η is of the form $\eta_1 \times \eta_2 \times \prod_{i=1}^r \eta_i'$, where η_1 is quadratic mod $\mathfrak{p}_1$, η_2 is of order 2 or 4 mod $\mathfrak{p}_2^5$, and each η_i' is of order 2 or 4 and primitive of conductor $p_i'\mathcal{O}$,
- The following conditions have to be satisfied:

  (*i*) $\eta_1(n) \cdot \eta_2(n) = \chi(n)$ for all integers n coprime to D ,

  (*ii*) for each $i \leq r$, $\eta_i'(n) = 1$ for all integers n coprime to p_i' and $\eta'(\overline{\alpha}) = \overline{\eta'(\alpha)}$ for all $\alpha \in (\mathcal{O}/p_i'\mathcal{O})^*$.

If $\mathfrak{m}$ were the ideal $\mathfrak{p}_1 \times \mathfrak{p}_2^5$ and η_2 a character of order 4, then $\eta_2(1 + \sqrt{-d})^2 = -1$. In this case, the degree $[\mathbb{E} : \mathbb{Q}]$ would be greater than 4 since for each possible value of d ($d = 6, 10, 22, 58$) it can be found a generator β of the square of a non-principal prime ideal $\mathfrak{p} \in I(\mathfrak{m})$ and checked that $\eta_2(\beta)^2 = 1$. So $\eta'(\beta)$ must necessarily have order 4, which leads to a contradiction. Indeed, for an inert prime p_i' in $\mathbb{K}$, $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\beta) = p^2$ implies that β is a square in the finite field $\mathcal{O}/p_i'\mathcal{O}$ and, thus, $\eta_i'(\beta)^2 = 1$. For the split case, the conditions $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\beta) = p^2$ and $\eta_i'(\overline{\beta}) = \overline{\eta_i'(\beta)}$ also implies that $\eta_i'(\beta)^2 = 1$. So $(-d, d) \notin \mathcal{S}_2^{\rm cm}$ for d even.

Let us now prove that, for $k = 4$, $(-d, -1) \in \mathcal{S}_2^{\rm cm}$ for all d.

Assume $p_1 \equiv 1 \pmod 4$. We take $\mathfrak{m} = \mathfrak{p}_1$ and let η be a character mod $\mathfrak{p}_1$ of order 4. It is clear that $\eta(\alpha) = \eta(\overline{\alpha})$ for all $\alpha \in (\mathcal{O}/\mathfrak{m})^*$. Moreover, since $p_1 \not\equiv 1 \pmod 8$, $\eta(-1) = -1$ and $\eta(2) = \pm i$. Due to the fact that $\eta(2)$ has order 4, for any Hecke character ψ with attached character η we have $\mathbb{E} = \mathbb{Q}(\sqrt{-d}, \sqrt{d})$ and, moreover, $\psi(\mathfrak{p}_2) = \pm(1 \pm i)$. Let $\mathfrak{p}$ be a prime ideal over a prime p which splits in $\mathbb{K}$. By using the fact that $\mathfrak{p}$ is either principal or $\mathfrak{p} = \alpha\mathfrak{p}_2$ with $(\alpha) \in I(\mathfrak{m})$, we obtain $a_p \in \mathbb{Q}(i)$ and, thus, $\mathbb{E}_f = \mathbb{Q}(i)$.

For $p_1 \not\equiv 1 \pmod 4$, we take $\mathfrak{m} = \mathfrak{p}_1 \cdot \mathfrak{p}_2^7$ and $\eta = \eta_1 \times \eta_2$, where η_1 is a quadratic character mod $\mathfrak{p}_1$ and η_2 is an even character of conductor $\mathfrak{p}_2^7$ and order 4 such that $\eta_2(1+\sqrt{-d}) = \eta_2(5) = \pm i$. It is easy to check that for any Hecke character ψ with character η we have $\operatorname{ord}\varepsilon = 4$ and $\mathbb{E}_f = \mathbb{Q}(i)$.

(iii) Subcase $k = 6$. By [19], we know that $[\mathbb{E} : \mathbb{K}] = 2$ implies $3 \mid D$. Assume $3 \mid D$ and set $p_1 = 3$, so that $p_2 = d/p_1$ is the other prime divisor of D. Now, $\mathbb{H} = \mathbb{K}(\sqrt{p_2})$. Let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be the prime ideals over p_1 and p_2, respectively.

Although we have already proved that $(-d, p_2) \in \mathcal{S}_2^{\mathrm{cm}}$ when $k = 2$, we point out that, for $k = 6$, this pair is also attained. Let us now prove that $(-d, -3) \notin \mathcal{S}_2^{\mathrm{cm}}$. Assume that there exists a Hecke character for which η has order 6 and $\mathbb{E}_f = \mathbb{Q}(\sqrt{-3})$. The Nebentypus ε is non-trivial and its order divides 6. Since the newform $g = f \otimes \varepsilon$ has CM by $\mathbb{K}$, $\mathbb{E}_g = \mathbb{Q}(\sqrt{-3})$ and its Nebentypus is ε^3, which must have order 2. So, we can assume that ε has order 2. Due to the fact that $\varepsilon \neq 1$, the Weil involution W_N acting on A_f is non-trivial and, thus, provides an elliptic quotient E of the abelian surface A_f defined over the real quadratic field $\mathbb{K}' = \mathbb{L}_\varepsilon$. The curve E has CM by an order $\mathcal{O}'$ of $\mathbb{K}$ and the ring class field of $\mathcal{O}'$, which contains $\mathbb{H}$, is $\mathbb{K}'\,\mathbb{K}$. Therefore, $\mathbb{H} = \mathbb{K}'\,\mathbb{K}$ and $\mathbb{K}'$ must be $\mathbb{Q}(\sqrt{p_2})$. Since A_f is isogenous over $\mathbb{Q}$ to $\operatorname{Res}_{\mathbb{K}'/\mathbb{Q}} E$ and $\mathbb{E}_f = \mathbb{Q}(\sqrt{-3})$, -3 should be a norm of $\mathbb{K}'$ but this condition does not occur when $3 \mid D$. ■

4. On the finiteness for endomorphism algebras over $\mathbb{Q}$

This section is devoted to present evidences about a behavior of the Fourier coefficients of normalized newforms. We show that this conjectural behavior implies the finiteness of the set of number fields $\mathbb{E}_f$ with degree n and, thus, the finiteness of the set $\mathcal{S}_n$ for the RM case.

For $f \in \mathrm{New}_N$, we denote by $S_2(A_f)$ the $\mathbb{C}$-vector space generated by the Galois conjugates of f, whose dimension is $\dim A_f$. We consider the positive integer defined by

$$B(f) := \max\left\{ \operatorname{ord}_{i\infty} h : h \in S_2(A_f)\right\}.$$

In other words, $B(f)$ is the positive integer for which there is a single cuspidal form in $S_2(A_f)$ whose q-expansion is $q^{B(f)} + \sum_{m>B(f)} a_m\, q^m$.

Since $\Omega^1(A_f) \simeq S_2(A_f)\, dq/q \subseteq \Omega^1(X_1(N))$, we know that

$$\dim A_f \le B(f) \le 2g_1 - 1\,,$$

where g_1 denotes the genus of $X_1(N)$. If there exists a curve C defined over $\mathbb{C}$ along with a morphism $\pi : X_1(N) \twoheadrightarrow C$ such that $S_2(A_f)\, dq/q \subseteq \pi^*(\Omega^1(C))$, then we can improve the upper bound of $B(f)$ since $B(f) \leq 2g(C) - 1$, where $g(C)$ denotes the genus of C. But, we cannot ensure the existence of such a curve with a genus less or equal than a constant depending on $\dim A_f$. In fact there is a conjecture about the finiteness of such curves (see Conjecture 1.1 in [1]).

It is natural to ask about the asymptotic behavior of $B(f)$ when f runs over the set of normalized newforms f whose abelian varieties A_f have a given dimension.

For every integer $n > 0$ and every $x \in \mathbb{R}$ we define

$$B(n,x) := \max\{B(f) : f \in \mathrm{New}_N, \dim A_f = n,\ N \leq x\}\,,$$
$$B(n) := \lim_{x\to+\infty} B(n,x)\,.$$

Of course, $B(1) = 1$. After computing $B(f)$ for $n = 2$ and $N \leq 3000$ with f running over the set of all normalized newforms with trivial Nebentypus, we obtained the results displayed in the following table:

$B(f)$	2	3	5	7	11	13	17	19
$\#\{A_f\}$	1372	1536	1155	504	139	43	11	2

Note that if $\dim A_f = 2$, then $B(f) = k$ if and only if $a_i \in \mathbb{Z}$ for all $i < k$ and $a_k \notin \mathbb{Z}$, where $f = \sum_{m>0} a_m q^m$. By the properties of the Fourier coefficients, if the order of the Nebentypus of f is 1 or 2, then $B(f)$ is a prime.

With regard to the above computational table, one could think that $B(n) < +\infty$ for $n > 1$. Nevertheless, this assertion is not right. In fact, $B(n)$ would be $+\infty$ if we only took into account newforms with CM to define $B(n,x)$. Indeed, take for instance $\mathbb{K} = \mathbb{Q}(\sqrt{-7})$ and $n = 2$. For any integer $k > 7$, let $p_1 < \cdots < p_r$ be the primes $\leq k$ and let $p > k$ be a prime such that $p \equiv -1 \pmod 4$ and splits in $\mathbb{K}$. Choose a prime $\mathfrak{p}_i$ over each p_i and a prime $\mathfrak{p}$ over p. Let $\mathfrak{m}' = \mathfrak{p}_1^2 \cdot \prod_{i=2}^r \mathfrak{p}_i$. We take $\mathfrak{m}$ to be either $\mathfrak{m}'$ or $\mathfrak{m}' \cdot \mathfrak{p}$, depending on whether the primitive quadratic character of conductor $\mathfrak{m}'$ is odd or not. Let η be the primitive quadratic character of conductor $\mathfrak{m}$ and let ψ be the corresponding Hecke character. It is clear that $\mathbb{E}_f = \mathbb{Q}(\sqrt{-7})$ and $a_m = 0$ for all $1 < m \leq k$. It follows that $\mathrm{ord}_{i\infty} f - \overline{f} > k$ and, thus, $B(f) > k$.

For newforms without CM, we can use a similar procedure that consists on twisting a newform f by suitable quadratic Dirichlet characters of large conductor to obtain newforms g with $B(g) > k$ and $\dim A_f = \dim A_g$. For this reason, we shall refine the above definitions to avoid the distortion caused by the effect of twists.

In the sequel χ stands for a Dirichlet character of any conductor and order. For an integer $n \geq 1$, we say that a normalized newform f without CM is n-primitive if $\dim A_f = n$ and $\dim A_{f\otimes\chi} \geq n$ for all Dirichlet characters χ. The reason to exclude the CM case in this definition is the following. For two Hecke characters ψ and ψ' of $\mathbb{K}$, ψ' can be viewed as a twist of ψ by a character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$ and it may be that the corresponding newforms f and f' satisfy that $\dim A_{f'} < \dim A_f = n$ and $\dim A_{f\otimes\chi} \geq n$ for all Dirichlet characters χ.

Now, we define

$$\begin{aligned}
\widetilde{B}(f) &:= \min\left\{B(f\otimes\chi) : \dim A_{f\otimes\chi} = \dim A_f\right\},\\
\widetilde{B}(n,x) &:= \max\left\{\widetilde{B}(f) : f\in \mathrm{New}_N\setminus \mathrm{New}_N^{\mathrm{cm}}\,, N\leq x\,, f \text{ is } n\text{-primitive}\right\},\\
\widetilde{B}(n) &:= \lim_{x\to+\infty}\widetilde{B}(n,x)\,.
\end{aligned}$$

The range $N \leq 3000$ is too small to detect the effect of twists, but we can see in the above table the quick decrease in the number of abelian surfaces A_f when $B(f)$ increases. Now, one suspects that an affirmative answer to the question $\widetilde{B}(n) < +\infty$ should be considered. Next, we show two important consequences about this hypothesis.

Proposition 4.1 *Let $n > 1$ be an integer. Assume that $\widetilde{B}(m) < +\infty$ for all positive integers $m \leq n$. Then,*

- (i) *The set of number fields $\mathbb{E}_f$ of degree n obtained when f runs over the set of all normalized newforms is finite.*
- (ii) *If $n = 2$, then $4\,\widetilde{B}(2) - 1$ is an upper bound for all primes $p \equiv 1 \pmod 4$ such that the modular curve $X_0^+(p) = X_0(p)/\langle w_p\rangle$ has non cuspidal rational points without CM.*

Proof. Let us prove (i). By Theorem 3.1 we can restrict our attention to the non-CM case. First, we assume that $f \in \mathrm{New}_N\setminus\mathrm{New}_N^{\mathrm{cm}}$ is n-primitive. Let $g = f\otimes\chi = \sum_{m>0} a_m\, q^m$ be such that $\dim A_f = \dim A_g$ and $B(g) = \widetilde{B}(f)$. Let us denote by $\tau_1,\dots,\tau_n$ the $\mathbb{Q}$-embeddings of $\mathbb{E}_g$ into $\overline{\mathbb{Q}}$. The matrix $({}^{\tau_i}a_j)_{i\leq n, j\leq B(g)+1}$ has rank n and, thus, $\{a_1,\dots,a_{B(g)+1}\}$ is a system of generators of the $\mathbb{Q}$-vector space $\mathbb{E}_g$. Under the assumption $\widetilde{B}(n) < +\infty$, we have that $\mathbb{E}_g$ is the field $\mathbb{Q}(a_2,\dots,a_{\widetilde{B}(n)+1})$. For any integer $m > 1$, a_m is an algebraic integer of degree at most n such that $\mid {}^{\tau_i}a_m \mid\leq \sigma_0(m)\sqrt{m}$ for all $i \leq n$, where $\sigma_0(m) = \sum_{0<d|m} 1$. Therefore, there are only finitely many possibilities for the values a_m and, thus, finitely many possibilities for $\mathbb{E}_g$. The condition $\dim A_{g\otimes\chi^{-1}} = n$ implies that the order k of χ satisfies $\varphi(k) \mid n$. Therefore the number field $\mathbb{E}_f$ is a subfield of the compositum of $\mathbb{E}_g$ with the k-th cyclotomic field, and it follows that the set of number

fields $\mathbb{E}_f$ obtained for n-primitive newforms f is finite. If $\dim A_f = n$ and f is not n-primitive, let χ be a Dirichlet character such that $f_0 = f \otimes \chi$ is m-primitive for some $m < n$. By using that there are finitely many possibilities for $\mathbb{E}_{f_0}$ and for $\mathbb{Q}(\chi)$, it follows that the set of number fields $\mathbb{E}_f$ for the case that $\dim A_f = n$ and f is not n-primitive is also finite.

Let us prove (ii). The existence of a non cuspidal point in $X_0^+(p)(\mathbb{Q})$ without CM implies the existence of an elliptic curve E without CM defined over a quadratic field $\mathbb{K}$ along with a p-isogeny $\mu : E \to {}^{\sigma}E$, where σ is the non-trivial element of $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$. If $p \equiv 1 \pmod 4$, then p is a norm of $\mathbb{K}$ (cf. [8]) and, thus, we can choose E such that μ is defined over $\mathbb{K}$ and $\mu \circ {}^{\sigma}\mu = [p]$. Therefore, the Weil restriction $A = \mathrm{Res}_{K/\mathbb{Q}}(E)$ is an abelian surface such that $\mathrm{End}_{\mathbb{Q}}(A) \otimes \mathbb{Q}$ is $\mathbb{Q}(\sqrt{p})$, i.e., A is of GL_2-type with real multiplication by $\sqrt{p}$. Due to recent results on Serre's modularity conjecture by Khare-Wintenberger [12], Dieulefait [5] and Kissin [13], the abelian surface A is modular and there exists a normalized newform f with trivial Nebentypus such that A is $\mathbb{Q}$-isogenous to A_f. It is clear that f is 2-primitive. Let χ be a quadratic Dirichlet character such that the newform $g = f \otimes \chi = q + \sum_{m>1} a_m q^m$ satisfies $\widetilde{B}(f) = B(g)$. Due to the fact that g has an inner-twist by the quadratic character attached to $\mathbb{K}$ and its Nebentypus is trivial, the Fourier coefficients of g satisfy the next condition: If $a_m \notin \mathbb{Z}$ then $a_m^2/p \in \mathbb{Z}$. Let p_0 be the least prime such that $a_{p_0} \notin \mathbb{Z}$. Hence, $p_0 \le \widetilde{B}(2)$. The statement follows from the inequality $p \le a_{p_0}^2 \le (2\sqrt{p_0})^2 \le 4\,\widetilde{B}(2)$. ■

Remark 4.1 In view of the results in [15], in the QM case we do not see any reason to derive the finiteness of the set $\mathcal{S}_n$ from the finiteness of the set of number fields $\mathbb{E}_f$ of degree n and, thus, from the condition $\widetilde{B}(n) < +\infty$.

We conclude by giving a better lower bound for $\widetilde{B}(2)$ than the one provided by the above computations for newforms of level ≤ 3000 and trivial Nebentypus.

Proposition 4.2 *There is a 2-primitive normalized newform $f \in S_2(\Gamma_0(2 \cdot 5^2 \cdot 31159^2))$ such that $\widetilde{B}(f) = B(f) = 59$. In particular, $\widetilde{B}(2) \ge 59$.*

Proof. Consider the elliptic curve $E : y^2 = x^3 + A\,x + B$, where

$$A = 13709960(2643250204357 - 285242082633\sqrt{-D})$$

$$B = 348980800\big(-18224167668804803284533 + 63802091292233830777\sqrt{-D}\big),$$

and $D = 31159$. It can be checked that the conductor of E is the integral ideal of $\mathbb{K} = \mathbb{Q}(\sqrt{-D})$ generated by $2 \cdot 5^2 \cdot 31159$. The pair $(E, \overline{E})$ provides a non-CM rational point on the curve $X_0^+(137)$, i.e. E is a quadratic $\mathbb{Q}$-curve without CM of degree 137 (cf. [6]).

We claim that the isogeny $\mu : E \to \overline{E}$ of degree 137 is defined over $\mathbb{K}$. Indeed, let $x_1, \ldots, x_{136}$ be the x-coordinates of the non-trivial points of the kernel of μ. By [7], it suffices to prove that $-137 \cdot \mathrm{N}_{\mathbb{K}/\mathbb{Q}}(s_1) \in (\mathbb{K}^*)^2$, where $s_1 = \sum_{i=1}^{136} x_i$. One way to determine s_1 is to compute the 137-th division polynomial of E, which has degree 9384, and then to factorize it over $\mathbb{K}$. A better though approximate way is to determine a basis $\{\omega_1, \omega_2\}$ of periods of E such that $\tau = \omega_1/\omega_2$ is in the upper half-plane and satisfies $j(137\,\tau) = \overline{j(\tau)}$. Then, $s_1 = \sum_{i=1}^{136} \wp(i/\omega_2; \omega_1, \omega_2)$, where $\wp(z; \omega_1, \omega_2)$ denotes the Weierstrass function attached to the period lattice of E. After computing, we obtain

$$\begin{aligned}
\omega_1 &= -0.0000059349200452413239\ldots - 0.0000134040043086026752\ldots i, \\
\omega_2 &= 0.0003360230301664207601\ldots + 0.0008081258226439434557\ldots i\,, \\
s_1 &= 103120(1152883 + 56273\sqrt{-D})\,.
\end{aligned}$$

It is now immediate to check that $-137\,\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(s_1)$ is a square in $\mathbb{K}^*$.

Since μ is defined over $\mathbb{K}$ and $\mu \circ \overline{\mu} = [137]$, the Weil restriction $A = \mathrm{Res}_{\mathbb{K}/\mathbb{Q}}(E)$ satisfies $\mathrm{End}_{\mathbb{Q}}(A) \otimes \mathbb{Q} = \mathbb{Q}(\sqrt{137})$ and, thus, $A/\mathbb{Q}$ is modular. By Milne's formula in [14], the conductor of A is

$$\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\mathrm{cond}(E)) \cdot D^2 = 2^2 \cdot 5^4 \cdot 31159^4$$

and, thus, there exists a normalized newform $f = \sum_{n>0} a_n q^n \in S_2(\Gamma_0(N))$ such that A_f is $\mathbb{Q}$-isogenous to A, where

$$N = \sqrt{\mathrm{cond}(A)} = 2 \cdot 5^2 \cdot 31159^2$$

(cf. [4]). The newform f has an inner-twist by the quadratic Dirichlet character attached to $\mathbb{K}$. The Fourier coefficients a_n lie in $\mathbb{Q}(\sqrt{137})$ and we know that, if $a_p \notin \mathbb{Z}$ for a prime p, then A has good reduction at p, p is inert in $\mathbb{K}$ and $a_p/\sqrt{137} \in \mathbb{Z}$. Then, we have to determine the first inert prime p_0 such that $a_{p_0} \neq 0$. By the Eichler-Shimura congruence, for a prime $p \nmid N$, the polynomial $(x^2 - a_p\, x + p)(x - {}^\sigma a_p\, x + p)$ is the characteristic polynomial of Frob_p acting on the l-adic Tate module of the reduction of A mod p. Therefore, the characteristic polynomial of Frob_{p^2} acting on the on the l-adic Tate module of the reduction of E mod p is $x^2 - (a_p^2 - 2\,p)\,x + p^2$. After computing, we obtain $p_0 = 59$ and $a_{59} = \pm\sqrt{137}$. Then, the q-expansion of $(f - {}^\sigma f)/(2\sqrt{137})$ is $\pm q^{59} + O(q^{60})$ and, thus, $B(f) = 59$.

Let $g = f \otimes \chi = \sum_{n>0} b_m q^m$, where χ is any quadratic Dirichlet character. For every inert prime $p < 59$ of $\mathbb{K}$ at which A_g has god reduction, we know that A_f has also good reduction at p. Therefore, $b_p = \chi(p)\, a_p = 0$ and, thus, $\widetilde{B}(f) = B(f)$. ■

References

[1] Baker, M. H., González-Jiménez, E., González, J. and Poonen, B.: Finiteness results for modular curves of genus at least 2. *Amer. J. Math.* **127** (2005), no. 6, 1325–1387.

[2] Bayer, P. and González, J.: On the Hasse-Witt invariants of modular curves. *Experiment. Math.* **6** (1997), no. 1, 57–76.

[3] Bruin, N., Flynn, E. V., González, J. and Rotger, V.: On finiteness conjectures for endomorphism algebras of abelian surfaces. *Math. Proc. Cambridge Philos. Soc.* **141** (2006), no. 3, 383–408.

[4] Carayol, H.: Sur les représentations l-adiques associées aux formes modulaires de Hilbert. *Ann. Sci. École Norm. Sup. (4)* **19** (1986), no. 3, 409–468.

[5] Dieulefait, L. V.: Remarks on Serre's modularity conjecture. Preprint avalaible in `http://arxiv.org/abs/math/0603439v11`, 2011.

[6] Galbraith, S. D.: Rational points on $X_0^+(p)$. *Experiment. Math.* **8** (1999), no. 4, 311–318.

[7] González, J.: Isogenies of polyquadratic $\mathbb{Q}$-curves to their Galois conjugates. *Arch. Math. (Basel)* **77** (2001), no. 5, 383–390.

[8] González, J.: On the j-invariants of the quadratic $\mathbf{Q}$-curves. *J. London Math. Soc. (2)* **63** (2001), no. 1, 52–68.

[9] González, J. and Lario, J.-C.: $\mathbf{Q}$-curves and their Manin ideals. *Amer. J. Math.* **123** (2001), no. 3, 475–503.

[10] González, J. and Lario, J-C.: Modular elliptic directions with complex multiplication (with an application to Gross's elliptic curves). *Comment. Math. Helv.* **86** (2011), no. 2, 317–351.

[11] Gross, B. H.: *Arithmetic on elliptic curves with complex multiplication.* Lecture Notes in Mathematics **776**. Springer, Berlin, 1980.

[12] Khare, C. and Wintenberger, J.-P.: Serre's Modularity Conjecture (I) and (II). *Invent. Math.* **178** (2009), no. 3, 485–504 and 505–586.

[13] Kisin, M.: Modularity of 2-adic Barsotti-Tate representations. *Invent. Math.* **178** (2009), no. 3, 587–634.

[14] Milne, J. S.: On the arithmetic of abelian varieties. *Invent. Math.* **17** (1972), 177–190.

[15] Quer, J.: Fields of definition of building blocks. *Math. Comp.* **78** (2009), no. 265, 537–554.

[16] Ribet, K. A.: Galois representations attached to eigenforms with Nebentypus. In *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, 17–51. Lecture Notes in Mathematics **601**. Springer, Berlin, 1977.

[17] Rotger, V.: Which quaternion algebras act on a modular abelian variety? *Math. Res. Lett.* **15** (2008), no. 2, 251–263.

[18] Weil, A.: The field of definition of a variety. *Amer. J. Math.* **78** (1956), 509–524.

[19] Yang, T.: On CM abelian varieties over imaginary quadratic fields. *Math. Ann.* **329** (2004), no. 1, 87–117.

Recibido: 5 de noviembre de 2009

Josep González
Universitat Politècnica de Catalunya
Escola Politècnica Superior d'Enginyeria de Vilanova i la Geltrú
Av. Victor Balaguer s/n
08800 Vilanova i la Geltrú, Spain
josepg@ma4.upc.edu

The author is partially supported by DGICYT Grant MTM2009-13060-C02-02.