# WHICH QUATERNION ALGEBRAS ACT ON A MODULAR ABELIAN VARIETY?

Victor Rotger

Για εσένα μούρη, που σε γνώρησα ξαφνικά ένα φθινόπορο στην Άνω Πόλη της Θεσσαλονίκης.

ABSTRACT. Let $A/\mathbb{Q}$ be a modular abelian variety. We establish criteria to prevent a given quaternion algebra $B$ over a totally real number field to be the endomorphism algebra of $A$ over $\bar{\mathbb{Q}}$. We accomplish this by analyzing the representation of $\mathrm{Gal}\,(\bar{\mathbb{Q}}/\mathbb{Q})$ on the points of $N$-torsion of $A$ at primes $N$ which ramify in $B$.

## 1. Introduction

Let $A/\mathbb{Q}$ be an abelian variety of $\mathrm{GL}_2$-type over $\mathbb{Q}$ of dimension $g \geq 1$, by which we mean that the ring of endomorphisms $R = \mathrm{End}_{\mathbb{Q}}(A)$ is an order in a number field $E$ of degree $[E : \mathbb{Q}] = g$.

Let $K/\mathbb{Q}$ be the minimal number field over which *all* endomorphisms of $A \times \bar{\mathbb{Q}}$ are defined and let $\mathcal{O} = \mathrm{End}_K(A)$. Let $B = \mathrm{End}_K^0(A) := \mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}$.

As a consequence of the recent work on Serre's modularity conjecture by Khare-Wintenberger [KaWi], Dieulefait [Di] and Kisin [Ki], the generalized Shimura-Taniyama Conjecture holds true. This amounts to say that $A$ is isogenous over $\mathbb{Q}$ to a factor of the Jacobian variety $J_1(L)$ of the modular curve $X_1(L)$ for some positive integer $L \geq 1$.

As in [BFGR, §1], christen $(\mathcal{O}, R)$ a *modular pair*. The *minimal level* of $(\mathcal{O}, R)$ is the minimal value of $L \geq 1$ as above. Similarly, we shall also say that a triplet $(\mathcal{O}, R, K)$ is modular if $\mathrm{End}_{\mathbb{Q}}(A) \simeq R$ and $\mathrm{End}_K(A) = \mathcal{O}$ for some modular abelian variety $A$.

A conjecture attributed to Coleman (cf. [BFGR, §1]) predicts that, for any fixed $g \geq 1$, there exist only finitely many isomorphism classes of modular pairs $(\mathcal{O}, R)$. Also, the possibilities for modular triplets $(\mathcal{O}, R, K)$ should also be very limited. The reader may consult [BFGR, §1] for further motivation of this conjecture.

It is the purpose of these notes to address this question for *absolutely simple modular abelian varieties $A/\mathbb{Q}$ such that $B \supsetneq E$.*

Under this assumption, it follows from Albert's classification of involuting simple algebras and the work of Shimura that $g$ is even and $B$ is a totally indefinite division quaternion algebra over a totally real field $F$ of degree $[F : \mathbb{Q}] = g/2$. In particular, $E$ is a quadratic extension over $F$ and a maximal subfield of $B$.

It is also known that $E$ is totally real and $K$ is imaginary quadratic (cf. Lemma 2.3 (i), (ii)). Write $E = F(\sqrt{m})$ for some totally positive square-free integral element $m \in R_F$. Although we choose $m$ square-free, note that there may exist a non principal ideal $\mathfrak{m}_0$ of $F$ such that $\mathfrak{m}_0^2 \mid mR_F$.

Write also $K = \mathbb{Q}(\sqrt{-d})$ for some square-free integer $d \geq 1$. By a theorem of Ribet (cf. [Ri2, Theorem 5.6]), the values of $m$ and $d$ are related by the isomorphism

$$(1) \qquad\qquad\qquad\qquad B \simeq (\frac{-d, m}{F}).$$

Write $\mathfrak{D} = \mathrm{disc}(B)$ for the reduced discriminant of $B$, that is, the *square-free* product of the finite ideals of $F$ which ramify in $B$. Since $(\frac{-d, m}{F})$ is split at all prime ideals $\mathfrak{N} \nmid 2dm$, it follows from (1) that

$$(2) \qquad\qquad\qquad \mathfrak{N} \mid d \text{ for all } \mathfrak{N} \mid \mathfrak{D}, \mathfrak{N} \nmid 2m.$$

In order to have a numerical flavour of the issue, let us report on some explicit computations. The table below lists relevant numerical data for all modular pairs $(\mathcal{O}, R)$ of minimal level $L \leq 5400$ such that $\mathfrak{D} \neq (1)$ and $[F : \mathbb{Q}] \leq 4$.

We refer the reader to [BFGR, Prop. 1.3] for $L \leq 7000$ when $F = \mathbb{Q}$; see also [Ha] for explicit details when $L \leq 3000$ and $F = \mathbb{Q}$. When $[F : \mathbb{Q}] = 2, 3$ or 4, J. Quer performed the necessary computations.

Column $L$ lists the minimal level of the modular pair. In column $\mathfrak{D}$ we provide the norms $\mathrm{N}_{F/\mathbb{Q}}(\mathfrak{N})$ of the prime ideals $\mathfrak{N} \mid \mathfrak{D}$.

| $L$ | $[F : \mathbb{Q}]$ | $\mathrm{disc}(F)$ | $\mathfrak{D}$ | $\mathrm{N}_{F/\mathbb{Q}}(m)$ | $\mathrm{disc}(K)$ |
|---|---|---|---|---|---|
| 675 | 1 | 1 | $[2, 3]$ | 2 | $-3$ |
| 1568 | 1 | 1 | $[2, 3]$ | 3 | $-4$ |
| 243 | 1 | 1 | $[2, 3]$ | 6 | $-3$ |
| 2700 | 1 | 1 | $[2, 5]$ | 10 | $-3$ |
| 1568 | 1 | 1 | $[2, 7]$ | 7 | $-4$ |
| 3969 | 1 | 1 | $[3, 5]$ | 15 | $-7$ |
| 1089 | 2 | 5 | $[9, 11]$ | 11 | $-3$ |
| 2592 | 2 | 33 | $[2, 3]$ | 27 | $-4$ |
| 3872 | 2 | 5 | $[4, 11]$ | 11 | $-4$ |
| 3872 | 2 | 5 | $[4, 11]$ | 55 | $-4$ |
| 4356 | 2 | 5 | $[5, 11]$ | 55 | $-3$ |
| 4761 | 2 | 41 | $[2, 5]$ | 10 | $-3$ |
| 2187 | 3 | 81 | $[3, 17]$ | 51 | $-3$ |
| 2187 | 3 | 81 | $[3, 8]$ | 24 | $-3$ |
| 3969 | 3 | 321 | $[3, 3]$ | 81 | $-7$ |
| 4563 | 3 | 1436 | $[2, 3]$ | 6 | $-3$ |
| 3267 | 4 | 5725 | $[9, 11]$ | 11 | $-3$ |
| 3267 | 4 | 13525 | $[5, 9]$ | 5 | $-3$ |

**Table 1.** Modular pairs of minimal level $L \leq 5400$ and $[F : \mathbb{Q}] \leq 4$.

**Definition 1.1.** *The set $\mathcal{N}_\ell$ of exceptional prime ideals of $F$ for a given prime $\ell$ is*

$$\mathcal{N}_\ell \,=\, \{\mathfrak{N} : \mathfrak{N} \mid \ell, \ a^2 - s\ell \ \text{ or } \ a^4 - 4a^2\ell + \ell^2\},$$

*for some $s = 0, 1, 2, 3, 4$ and some $a \in R_F$, $a \neq \sqrt{s\ell}, \ \sqrt{2\ell \pm \sqrt{3}\ell}$, such that $|\tau(a)| \leq 2\sqrt{\ell}$ for all $\tau : F \hookrightarrow \mathbb{R}$.*

This is obviously a finite set of prime ideals, rather small for small values of $[F : \mathbb{Q}]$ and $\ell$. When $F = \mathbb{Q}$, we have for instance $\mathcal{N}_2 = \{2, 3, 5, 7\}$ and $\mathcal{N}_3 = \{2, 3, 5, 11, 23\}$.

Given $\mathcal{O}$, $R$, $K$, the results of this note provide necessary conditions for the existence of a modular abelian variety $A/\mathbb{Q}$ such that $\mathrm{End}_\mathbb{Q}(A) \simeq R$ and $\mathrm{End}_K(A) \simeq \mathcal{O}$. For the sake of clarity and applicability, we gather in the theorem below a simplified version of the results which are obtained throughout the article. See the remaining sections for slightly more general statements.

Below, let $\zeta_n$ denote a $n$-th primitive root of 1. Also, let $\mathcal{O}_\mathfrak{D}$ denote a maximal order in the division quaternion algebra $B$ of reduced discriminant $\mathfrak{D} \neq (1)$. Recall that an order $\mathcal{O}$ in $B$ is maximal if and only if $\mathrm{disc}(\mathcal{O}) = \mathfrak{D}$ (cf. [Vi, p. 84]).

**Theorem 1.2.** *Let $K$ be an imaginary quadratic field, let $F$ be a totally real number field and let $m \in R_F$ be a square-free totally positive element. If $(\mathcal{O}_\mathfrak{D}, R_{F(\sqrt{m})}, K)$ is modular, then*

    (i) *$mR_F = \mathfrak{m}_0^2 \cdot \mathfrak{m}$, with $\mathfrak{m}_0$ and $\mathfrak{m}$ ideals of $R_F$, $\mathfrak{m} \mid \mathfrak{D}$. If $h(F) = 1$, $\mathfrak{m}_0 = 1$.*

    (ii) *Any $\mathfrak{N} \mid \mathfrak{D}$, $\mathfrak{N} \nmid 2m$, lies above a prime $N \equiv 3 \mod 4$.*

    (iii) *Assume $\mathfrak{D} \nmid 2m$ and $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) \not\subset F$ for $n \neq 1, 2, 3, 4, 6$. For any prime $\ell$ such that $(\frac{K}{\ell}) \neq -1$ and $\sqrt{\ell}, \sqrt{2\ell}, \sqrt{3\ell}, \sqrt{2\ell \pm \sqrt{3}\ell} \notin F$, either*

        • *$\mathfrak{N} \in \mathcal{N}_\ell$ for all $\mathfrak{N} \mid \frac{\mathfrak{D}}{(\mathfrak{D}, 2m)}$, or*

        • *$(\frac{-\ell}{\mathfrak{N}}) \neq 1$ for all $\mathfrak{N} \mid \mathfrak{D}$.*

In the remaining sections of this note we shall develop the necessary machinery to prove this result. Let us now illustrate and describe it in more detail.

Part $(i)$ is proved in Corollary 2.4. It was already known when $F = \mathbb{Q}$. In fact, if $F = \mathbb{Q}$, it was shown in [RSY, Theorem 3.1] that either

(3) $$\mathfrak{D} = (m) \text{ or } (mN) \text{ for some prime } N.$$

The proof of this result relies on a careful study of the closed fibers of Morita's model of the Atkin-Lehner quotients of the Shimura curve of discriminant $\mathfrak{D}$; it is reasonable to expect that, under certain hypothesis, a similar result should hold for higher degree number fields $F$. See the discussion following Corollary 3.8 for an approach to this question by a different method.

In Table 1 we quote the existence of a modular abelian variety $A/\mathbb{Q}$ of dimension 4 and level 3872 such that $\mathrm{End}_\mathbb{Q}^0(A) = F(\sqrt{m})$, where $m \in F = \mathbb{Q}(\sqrt{5})$, $\mathrm{N}_{F/\mathbb{Q}}(m) = 55$, and $\mathcal{O} = \mathrm{End}_{\mathbb{Q}(\sqrt{-1})}(A)$ is an order in the quaternion algebra $B$ over $F$ of discriminant $\mathfrak{D} = 2 \cdot (4 + \sqrt{5})$. By $(i)$, $\mathcal{O}$ is not maximal in $B$.

Part $(ii)$ is proved in Corollary 3.7 and $(iii)$ in Theorem 4.1.

As for $(iii)$, note firstly that for a given fixed $g$, the condition on $F$ not to contain $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ for any $n \neq 1, 2, 3, 4, 6$ excludes only finitely many fields $F$. For instance,

when $g = 2$ this condition is empty, whereas for $g = 4$ this only excludes $F = \mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$.

In fact, the restriction on $F$ can be relaxed (by allowing $\zeta_n + \zeta_n^{-1} \in F$ for larger values of $n$) at the cost of additional items in part $(iii)$. This can be achieved by following the proof of Theorem 4.1; we leave the details to the interested reader.

The condition on $\ell$ not to be inert in $K$ can not be removed; as for the requirement that $\sqrt{\ell}$, $\sqrt{2\ell}$, $\sqrt{3\ell}$, $\sqrt{2\ell \pm \sqrt{3}\ell} \notin F$, see Theorem 4.1 for a statement without this hypothesis.

Roughly, $(iii)$ claims that for *half* of the primes $\ell$, we have $(\frac{-\ell}{\mathfrak{N}}) = -1$ for all $\mathfrak{N} \mid \mathfrak{D}$ unless all $\mathfrak{N} \mid \frac{\mathfrak{D}}{(\mathfrak{D}, 2m)}$ lie in the exceptional set $\mathcal{N}_\ell$. Here, by half of the primes we mean those $\ell$ such that $(\frac{K}{\ell}) \neq -1$ and $\sqrt{\ell}$, $\sqrt{2\ell}$, $\sqrt{3\ell}$, $\sqrt{2\ell \pm \sqrt{3}\ell} \notin F$.

When $F = \mathbb{Q}$ and $\mathfrak{D} = (mN)$ for an odd prime $N$, $(iii)$ -for $\ell = 2, 3$, use the slightly stronger Theorem 4.1- says that for any $\ell$ such that $(\frac{K}{\ell}) \neq -1$, either

- $N \in \mathcal{N}_\ell$, or
- For all primes $p \mid \mathfrak{D}$: $(\frac{-\ell}{p}) \neq 1$ if $\ell \neq 2$ (resp. $p \not\equiv 1 \bmod 8$ if $\ell = 2$).

When trying to apply $(iii)$ to preclude explicit families of pairs $(\mathcal{O}, R)$ from being modular, it naturally arises the question of how does $K$ depend on $(\mathcal{O}, R)$. By means of the theory of descent applied to certain unramified covers of Shimura varieties, we prove in [Ro] the following fact. See [RSY, §5] for a particular case with $F = \mathbb{Q}$.

**Proposition 1.3.** *Let $(\mathcal{O}_\mathfrak{D}, R_{F(\sqrt{m})}, K)$ be a modular triplet. Assume that*

- *$mR_F$ is a square-free ideal, with $m = 3$ or $\tau(m) > 4$ for some embedding $\tau : F \hookrightarrow \mathbb{R}$, and*
- *There exists $\mathfrak{N} \mid \mathfrak{D}$, $\mathfrak{N} \nmid 2m$, of odd residual degree $f(\mathfrak{N}/N)$.*

*Then $K$ is unramified away from $\mathrm{N}_{F/\mathbb{Q}}(\mathfrak{D}) \cdot \mathrm{disc}(F/\mathbb{Q})$.*

The virtue of the above result is that, when the hypothesis is satisfied, there is a *finite* number of possibilities for $K$. Observe that, when $F = \mathbb{Q}$, the hypothesis of Proposition 1.3 simply require that $\mathfrak{D} = (mN)$ with $m, N > 2$.

In addition, notice that the isomorphism (1) $B \simeq (\frac{-d, m}{F})$ and Corollary 3.8 impose further restrictions on $K$. Let us illustrate how the combination of these results can be used to prevent triplets $(\mathcal{O}, R, K)$ from being modular.

**Theorem 1.4.** *Let $F = \mathbb{Q}$. Let $M, N$ be two different odd primes and assume $(\mathcal{O}_{MN}, R_{\mathbb{Q}(\sqrt{M})})$ is a modular pair. Then $N \equiv 3 \bmod 4$ and $(\frac{-N}{M}) = -1$. Moreover,*

(i) *If $M \equiv 3 \bmod 4$, then $K = \mathbb{Q}(\sqrt{-N})$ and $(\frac{-\ell}{M}) = -1$ for any odd prime $\ell$ such that $(\frac{\ell}{N}) = 1$ and $N \notin \mathcal{N}_\ell$.*

(ii) *If $M \equiv 1 \bmod 4$, then $K = \mathbb{Q}(\sqrt{-d})$ with $d = N$ or $MN$. If $d = N$, then $(\frac{-\ell}{M}) = -1$ for any $\ell$ such that $(\frac{\ell}{N}) = 1$ and $N \notin \mathcal{N}_\ell$. If $d = MN$, then $N \equiv 3 \bmod 8$ and $N \in \mathcal{N}_\ell$ for all odd primes $\ell$ such that $(\frac{-MN}{\ell}) = 1$.*

This is proved in Section 4. Since the finite sets $\mathcal{N}_\ell$ are easily computable, notice that, by taking explicit values of $\ell$, the above criterion precludes infinitely many pairs $(\mathcal{O}_{MN}, R_{\mathbb{Q}(\sqrt{M})})$ from being modular. Similar examples with higher degree number fields $F$ can easily be worked out in the same way.

The material of this note can be used to prove the non-existence of rational points (or at least, non-trivial rational points) on Atkin-Lehner quotients of Shimura varieties associated with totally indefinite quaternion algebras over totally real number fields. Care must be taken though because rational points over a field $K$ on these varieties do not quite correspond to abelian varieties (with extra structure) defined over $K$, but rather to those with $K$ as field of moduli; details will appear in [Ro].

See also [PY] for (non-overlapping) results in this direction in dimension 1, where it should be noticed that the methods used there in are completely different.

**Acknowledgement.** It is a pleasure to thank B. Jordan, J. Gonzalez, D. Lorenzini, J. Quer and the referee for their helpful remarks.

## 2. Quaternion multiplication over number fields

Let $A/\mathbb{Q}$ be an abelian variety of (even) dimension $g$ of GL$_2$-type over $\mathbb{Q}$ and let $R = \operatorname{End}_{\mathbb{Q}}(A) \subset E = \operatorname{End}_{\mathbb{Q}}(A) \otimes \mathbb{Q}$. Let $K$ be the minimal field over which all endomorphisms of $A \otimes \bar{\mathbb{Q}}$ are defined. Assume $\mathcal{O} = \operatorname{End}_K(A)$ is an order in a division totally indefinite quaternion algebra $B$ over a totally real number field $F$.

For any prime $N$, the action of $G_{\mathbb{Q}}$ on the Tate module $V_N(A)$ of $A$ induces a Galois representation

$$\mathcal{R}_N : G_{\mathbb{Q}} \longrightarrow \operatorname{GL}_{2g}(\mathbb{Q}_N),$$

which in fact takes values in $\operatorname{GL}_2(R_E)$, independently of $\mathfrak{N}$.

For any prime ideal $\mathfrak{N}$ of $E$ over $N$, let $E_{\mathfrak{N}}$ stand for the completion of $E$ along $\mathfrak{N}$ and write $V_{\mathfrak{N}}(A) = V_N(A) \otimes_{\mathbb{Q}_N} E_{\mathfrak{N}}$. Since the representation $\mathcal{R}_N$ is compatible with the action of $E$, it induces a Galois representation

$$r_{\mathfrak{N}} : G_{\mathbb{Q}} \longrightarrow \operatorname{GL}_2(E_{\mathfrak{N}}).$$

**Lemma 2.1.** *Let $\ell$ be a prime number. There exists a finite extension $L_\ell/\mathbb{Q}_\ell$ such that the closed fibre of the Néron model of $A \otimes_{\mathbb{Q}} L_\ell$ over the ring of integers of $L_\ell$ is an abelian variety $\tilde{A}$ over $\mathbb{F}_\ell$.*

*Proof.* By [Ri1, Theorem 3], $A$ has potential good reduction at $\ell$. Under this assumption, Serre and Tate explicitly construct $L_\ell$ and $\tilde{A}/\mathbb{F}_\ell$ at the end of p. 498 of [SeTa]. □

**Remark 2.2.** Let $A/\mathbb{Q}_\ell$ be an abelian variety with potential good reduction. By definition, there exist finite extensions $L/\mathbb{Q}_\ell$ over which $A$ acquires good reduction. Lemma above claims that $L$ can be chosen to have residue field $\mathbb{F}_\ell$. Note that in general there does not exist a *minimal* extension $L/\mathbb{Q}_\ell$ over which $A$ has good reduction (cf. [SeTa, p. 498] for a proof of this fact when the residue field is algebraically closed). Hence, there may exist good reduction extensions $L/\mathbb{Q}_\ell$ for $A$ with non trivial residual degree such that $A \times M$ has bad reduction for any subextension $M \subsetneq L$.

Let $\ell$ be a prime and let $\tilde{A}/\mathbb{F}_\ell$ denote the closed fibre of the Néron model of $A \otimes L_\ell$ as in the lemma above.

Let $\operatorname{Fr}_\ell \in \operatorname{Gal}(\bar{\mathbb{F}}_\ell/\mathbb{F}_\ell)$ be the Frobenius automorphism. Let $\varphi_\ell$ be an element of $\operatorname{Gal}(\bar{\mathbb{Q}}_\ell/L_\ell)$ whose image in $\operatorname{Gal}(\bar{\mathbb{F}}_\ell/\mathbb{F}_\ell)$ under the canonical reduction map is $\operatorname{Fr}_\ell$. By Serre-Tate's criterion [SeTa, Thm. 1], $r_{\mathfrak{N}}(\varphi_\ell)$ is a well-defined element of $\operatorname{GL}_2(R_E)$ up to conjugation.

Let $P_\ell(T) := P_{\varphi_\ell}(T) \in R_E[T]$ denote the characteristic polynomial of $r_{\mathfrak{N}}(\varphi_\ell)$. We shall write $a_\ell = \mathrm{Tr}(r_{\mathfrak{N}}(\varphi_\ell)) \in R_E$. By the work of Weil, $|\tau(a_\ell)| \leq 2\sqrt{\ell}$ for any embedding $\tau : E \to \mathbb{C}$. By [Ri2, Prop. 3.5], $E = \mathbb{Q}(\{a_\ell\}_{\ell \nmid N_A})$, where $N_A$ stands for the conductor of $A$.

There is a natural action of $G_{\mathbb{Q}}$ on the ring of endomorphisms $\mathcal{O} = \mathrm{End}_{\bar{\mathbb{Q}}}(A)$ of $A \otimes \bar{\mathbb{Q}}$. By the Skolem-Noether theorem, for any $\sigma \in G_{\mathbb{Q}}$ the automorphism $B \to B$, $\beta \mapsto \beta^\sigma$ is inner: there exists $\omega_\sigma \in \mathcal{O}$ such that $\beta^\sigma = \omega_\sigma \beta \omega_\sigma^{-1}$. Thus, $\omega_\sigma$ belongs to the normalizer $\mathrm{Norm}_B(\mathcal{O})$ of $\mathcal{O}$ in $B$, because $\beta^\sigma \in \mathcal{O}$ for any $\beta \in \mathcal{O}$.

Since the endomorphisms of $R \subset \mathcal{O}$ are defined over $\mathbb{Q}$, it follows that $\omega_\sigma$ belongs to the commutator of $E$ in $B$, which is $E$ itself because it is a maximal subfield of $B$. Hence, $\omega_\sigma \in R = E \cap \mathcal{O}$. This induces a continuous homomorphism

$$\psi : G_{\mathbb{Q}} \longrightarrow E^*/F^*, \quad \sigma \mapsto \omega_\sigma.$$

**Lemma 2.3.**     (i) $K$ *is imaginary quadratic, say* $K = \mathbb{Q}(\sqrt{-d})$, $d > 0$.
   (ii) $E = F(\omega)$ *for an element* $\omega \in \mathcal{O} \cap \mathrm{Norm}_B(\mathcal{O})$, $\omega^2 = m$, *where* $m \in R_F$ *is square-free and totally positive.*

*Proof.*     By [Ri2, Lemma 3.1], $\det(r_{\mathfrak{N}}) = \epsilon \cdot \chi_N : G_{\mathbb{Q}} \longrightarrow E^*$, where $\chi_N$ is the $N$-adic cyclotomic character and $\epsilon : G_{\mathbb{Q}} \to E^*$ is a character of finite order.

Let us first show that $E$ is totally real. Indeed, if it were not, $E$ would be a CM-field. Let $\mathfrak{L}$ be the set of primes $\ell \nmid N_A$ such that $a_\ell \neq 0$. If $\epsilon(\varphi_\ell) = 1$ then $a_\ell \in F^*$ by [Ri2, Proposition 3.4] and the fact that $E$ is a totally imaginary quadratic extension of $F$. Since $\psi(\varphi_\ell) \in a_\ell \cdot F^*$ by [Ri2, Theorem 5.5], we deduce in turn that $\psi(\varphi_\ell) \in F^*$, thus $\varphi_\ell \in \mathrm{Ker}(\psi)$. Čebotarev Density Theorem together with the fact that $\mathfrak{L}$ has density 1 within the set of all primes (cf. [Se2]) would imply that $\mathrm{Ker}(\epsilon) \subseteq \mathrm{Ker}(\psi)$, whence $K \subseteq \bar{\mathbb{Q}}^{\mathrm{Ker}(\epsilon)}$. By [Ri2, Lemma 3.2], $\epsilon(c) = 1$ for any complex conjugation $c \in G_{\mathbb{Q}}$ on $\bar{\mathbb{Q}}$ and we deduce that $K$ would be totally real. Theorem 2 in [Ri1] would apply to say that $B$ is not division, which contradicts our assumptions.

Since $E$ is totally real, it contains no roots of unity $\zeta \neq \pm 1$ and any non-trivial finite subgroup of $E^*/F^*$ has order 2. As $\psi$ embeds $\mathrm{Gal}(K/\mathbb{Q})$ in $E^*/F^*$, we obtain that $K$ is quadratic. Theorem 2 of [Ri1] implies that it is imaginary and $(i)$ follows.

Write $\mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma\}$ and let $\omega \in R$ such that $\psi(\sigma) \in \omega \cdot F^*$. As we argued above, $\omega \in \mathcal{O} \cap \mathrm{Norm}_B(\mathcal{O})$. Since $\sigma^2 = 1$, $\omega^2 = m \in R_F$ and we can assume $m$ is square-free. This shows $(ii)$. $\square$

Recall that an order $\mathcal{O}$ in $B$ is an *Eichler order* if it is the intersection of two maximal orders (cf. [Vi, p. 39, 84]). All orders with *square-free* discriminant $\mathrm{disc}(\mathcal{O})$ are Eichler orders by [Vi, p. 84 and p. 98, Ex. 5.3].

**Corollary 2.4.** *Assume* $\mathcal{O}$ *is an Eichler order. Then* $m \cdot R_F = \mathfrak{m}_0^2 \cdot \mathfrak{m}$, *where* $\mathfrak{m}_0$ *and* $\mathfrak{m}$ *are integral ideals of* $F$ *and* $\mathfrak{m} \mid \mathrm{disc}(\mathcal{O})$. *If the class number of* $F$ *is* $h(F) = 1$, *then* $m \mid \mathrm{disc}(\mathcal{O})$.

*Proof.*     Let $\omega \in \mathcal{O} \cap \mathrm{Norm}_B(\mathcal{O})$ as in the above proof. By [Vi, p. 99, Ex. 5.4], $\omega$ normalizes $\mathcal{O}_\wp$ in $B_\wp$ for any prime ideal $\wp$ of $F$. By [Vi, p. 34 and 40], there are no restrictions on $m = \mathrm{n}(\omega)$ at any $\wp \mid \mathrm{disc}(\mathcal{O})$. By [Vi, p. 40], $m \cdot R_{F_\wp}$ is an even power of $\wp R_{F_\wp}$ for any $\wp \nmid \mathrm{disc}(\mathcal{O})$. This shows the first part. If $h(F) = 1$, all ideals of $R_F$ are principal. Since $m$ is square-free, $\mathfrak{m}_0 = (1)$. $\square$

Since $E$ is totally real, the character $\epsilon$ mentioned in the proof above is trivial (cf. [Ri2, p. 244]) and [Ri2, Theorem 5.3] asserts that $F = \mathbb{Q}(\{a_\ell^2\}_{\ell \nmid N_A})$. Also, by [Ri2, Lemma 3.1] $\det(r_{\mathfrak{N}}(\varphi_\ell)) = \ell$ and $P_\ell(T) = T^2 - a_\ell T + \ell$ for any prime $\ell$.

For primes $\ell \nmid N_A$ such that $a_\ell \neq 0$ we have by [Ri2, Theorem 5.5] that if $\ell$ remains inert in $K$, then $a_\ell \in F^* \cdot \omega$. Otherwise, $a_\ell \in F^*$ and $P_\ell \in R_F[T]$.

In the terminology of modular forms, this is equivalent to saying that $A$ is the abelian variety attached (up to isogeny) to a normalized newform $f = \sum a_n q^n \in S_2(\Gamma_0(L))$ with an *extra-twist* by $\psi$. As we have seen, $F = \mathbb{Q}(\{a_\ell^2\})$, $E = F(\sqrt{m}) = \mathbb{Q}(\{a_\ell\})$, $K = \mathbb{Q}(\sqrt{-d}) = \text{Ker}\psi$ and $B = (\frac{-d,m}{F})$ are completely determined by the coefficients $a_\ell$. With this perspective in mind, the conjecture addressed in this note claims that the Fourier coefficients of a normalized newform for $\Gamma_0(L)$, $L \geq 1$, generate only finitely many endomorphism algebras $E$, $B$ of given degree over $\mathbb{Q}$.

## 3. The case $\mathfrak{N}$ inert in $E$

Keep the notation of Section 2. In addition, for the rest of the article we shall assume the following

**Assumption.** *There exists a prime ideal $\mathfrak{N}_0 \mid \text{disc}(B)$, $\mathfrak{N}_0 \nmid 2m$, at which $\mathcal{O}$ is locally maximal.*

Fix such a prime $\mathfrak{N}_0$ and let $R_0 = R \cap F$, a suborder of the ring of integers $R_F$ of $F$. By saying that $\mathcal{O}$ is locally maximal at $\mathfrak{N}_0$ we mean that $R_{0,\mathfrak{N}_0}$, the localization of $R_0$ at $\mathfrak{N}_0$, is the ring of integers of $F_{\mathfrak{N}_0}$ and that $\mathcal{O}_{\mathfrak{N}_0}$ is the (single) maximal order of $B_{\mathfrak{N}_0}$. Let $k_0$ be the residue field of $R_0$ at $\mathfrak{N}_0$, say of $\nu := N^f$ elements for $f = f_{\mathfrak{N}_0/N} \geq 1$.

Having this, the condition on $\mathfrak{N}_0$ not to ramify in $E$ actually implies that $\mathfrak{N}_0$ remains inert in $R$. This follows from the fact that $R$ embeds optimally in $\mathcal{O}$, as by construction $R = E \cap \mathcal{O}$ (cf. [Vi, Ch. II, §3] for details on Eichler's theory of optimal embeddings). Let $k$ be the residue field of $\mathfrak{N} = \mathfrak{N}_0 \cdot R$, which is a quadratic extension of $k_0$. Reducing mod $\mathfrak{N}$ we obtain the residual representation

$$\bar{r}_{\mathfrak{N}} : G_{\mathbb{Q}} \longrightarrow \text{GL}_2(k),$$

that is, the representation of $G_{\mathbb{Q}}$ on $A[\mathfrak{N}] = \{x \in A : \beta \cdot x = 0 \quad \forall \beta \in \mathfrak{N}\}$ of $A$.

Let $\pi_0$ be an uniformizer of $F_{\mathfrak{N}_0}$. By [Vi, Ch. II, §1], locally at $\mathfrak{N}_0$ the division quaternion algebra $B_{\mathfrak{N}_0}$ can be described as $B_{\mathfrak{N}_0} = E_{\mathfrak{N}} + E_{\mathfrak{N}}\pi$, where $\pi^2 = \pi_0$ and $\beta \cdot \pi = \pi \cdot \beta^\tau$ for any $\beta \in E_{\mathfrak{N}}$. Here, $\tau$ denotes the non-trivial automorphism of $\text{Gal}(E_{\mathfrak{N}}/F_{\mathfrak{N}_0})$. Moreover, $\mathcal{O}_{\mathfrak{N}_0} = R_{\mathfrak{N}} + \cdot R_{\mathfrak{N}} \cdot \pi$.

Let $I = \{\beta \in \mathcal{O} : n(\beta) \in \mathfrak{N}_0\}$. This is an ideal of $\mathcal{O}$ which locally at $\mathfrak{N}_0$ is $I_{\mathfrak{N}_0} = \mathfrak{N} \cdot R_{\mathfrak{N}} + R_{\mathfrak{N}} \cdot \pi$, whereas $I_{\mathfrak{M}_0} = \mathcal{O}_{\mathfrak{M}_0}$ at the remaining primes $\mathfrak{M}_0 \neq \mathfrak{N}_0$ of $F$. Let $C = \text{Ker}(I : A \to A) = \bigcap_{\beta \in I} \text{Ker}(\beta : A \to A)$, a subgroup of $A[\mathfrak{N}]$.

The action of $B$ on $A(\bar{\mathbb{Q}})$ makes $V_{\mathfrak{N}}(A)$ a $B_{\mathfrak{N}_0}$-module, which must be free because $B_{\mathfrak{N}_0}$ is simple. In fact, since $\dim_{F_{\mathfrak{N}_0}}(B_{\mathfrak{N}_0}) = \dim(V_{\mathfrak{N}}(A)) = 4$, we have $V_{\mathfrak{N}}(A) \simeq B_{\mathfrak{N}_0}$.

In the same fashion, $T_{\mathfrak{N}}(A)$ is naturally a module over $\mathcal{O}_{\mathfrak{N}_0}$. In fact, one can identify $T_{\mathfrak{N}}(A)$ as a left ideal of $\mathcal{O}_{\mathfrak{N}_0}$ by choosing an isomorphism $V_{\mathfrak{N}}(A) \simeq B_{\mathfrak{N}_0}$.

Since $\mathcal{O}_{\mathfrak{N}_0}$ is a maximal order, all its ideals are principal by [Vi, p. 34] and we may write $T_{\mathfrak{N}}(A) = \mathcal{O}_{\mathfrak{N}_0} \cdot x$ for some $x \in A[\mathfrak{N}]$.

Note that $A[\mathfrak{N}] = T_{\mathfrak{N}}(A)/\mathfrak{N} \cdot T_{\mathfrak{N}}(A) \simeq \mathcal{O}_{\mathfrak{N}_0}/\mathfrak{N} \cdot \mathcal{O}_{\mathfrak{N}_0}$. Also, we have $C = \mathcal{O}_{\mathfrak{N}_0}/I_{\mathfrak{N}} \simeq R_{\mathfrak{N}}/\mathfrak{N} \cdot R_{\mathfrak{N}} \simeq k$. As a $R$-module, $\text{Aut}_R(C) \simeq k^*$.

The action of $G_{\mathbb{Q}}$ on $\mathcal{O}$ leaves $I$ invariant because it is the single two-sided ideal of $\mathcal{O}$ of reduced norm $\mathfrak{N}_0$. Since $R = \operatorname{End}_{\mathbb{Q}}(A)$, $G_{\mathbb{Q}}$ acts $R$-linearly on $C$. It thus induces a Galois representation

$$\alpha_{\mathfrak{N}} : G_{\mathbb{Q}} \longrightarrow \operatorname{Aut}_R(C) = k^*.$$

As in [Jo], the character $\alpha_{\mathfrak{N}}$ shall play a key role in what follows, since it encodes many of the arithmetic properties of the Galois representation of $G_{\mathbb{Q}}$ on the torsion of $A$. Recall that $\nu = \sharp k_0$ and that $\psi$ is a character of $G_{\mathbb{Q}}$ with values in $\{\pm 1\}$.

**Lemma 3.1.** *There exists a $k$-basis of $A[\mathfrak{N}]$ with respect to which*

$$\bar{r}_{\mathfrak{N}} : \begin{array}{ccc} G_{\mathbb{Q}} & \longrightarrow & \operatorname{GL}_2(k) \\ \sigma & \rightarrow & \begin{pmatrix} \psi(\sigma)\alpha_{\mathfrak{N}}(\sigma)^{\nu} & 0 \\ \beta_{\sigma} & \alpha_{\mathfrak{N}}(\sigma) \end{pmatrix} \end{array}$$

*for some $\beta_{\sigma} \in k$.*

*Proof.* Write $\mathcal{O}_{\mathfrak{N}_0} = R_{\mathfrak{N}} + R_{\mathfrak{N}} \cdot \pi$ as above and let $x \in A[\mathfrak{N}]$ such that $A[\mathfrak{N}] = \mathcal{O}_{\mathfrak{N}_0}/\mathfrak{N}\mathcal{O}_{\mathfrak{N}_0} \cdot x = R_{\mathfrak{N}}/\mathfrak{N}R_{\mathfrak{N}} \cdot x + R_{\mathfrak{N}}/\mathfrak{N}R_{\mathfrak{N}} \cdot \pi(x)$. We shall compute $r_{\mathfrak{N}}(\sigma)$ for $\sigma \in G_{\mathbb{Q}}$ with respect to the $k$-basis $\{x, \pi(x)\}$ of $A[\mathfrak{N}]$.

Let $\sigma \in G_K$. Since all endomorphisms of $A$ are defined over $K$ it follows that $\pi^{\sigma} = \pi$. Let $x^{\sigma} = \alpha_{\sigma} \cdot x + \beta_{\sigma} \cdot \pi(x)$ for some $\alpha_{\sigma}, \beta_{\sigma} \in R_{\mathfrak{N}}$. Then $(\pi(x))^{\sigma} = \pi^{\sigma}(x^{\sigma}) = \pi(\alpha_{\sigma} \cdot x + \beta_{\sigma} \cdot \pi(x)) = \alpha_{\sigma}^{\tau}\pi(x) + \beta_{\sigma}^{\tau}\pi^2(x) = \alpha_{\sigma}^{\tau}\pi(x)$, because $\pi^2 = \pi_0$ and $\pi_0 \cdot x = 0$. Switching $\alpha_{\sigma}$ by $\alpha_{\sigma}^{\tau}$ and reducing mod $\mathfrak{N}$ it follows that $r_{\mathfrak{N}}(\sigma) = \begin{pmatrix} \alpha_{\sigma}^{\nu} & 0 \\ \beta_{\sigma} & \alpha_{\sigma} \end{pmatrix}$. In particular we recover the canonical character $\alpha_{\mathfrak{N}} : G_{\mathbb{Q}} \to k^*$ as $\alpha_{\mathfrak{N}}(\sigma) = \alpha_{\sigma}$.

Let $c \in G_{\mathbb{Q}}$ denote a complex conjugation. As in Lemma 2.3 and its proof, for all $\beta \in \mathcal{O}$ we have $\beta^c = \omega\beta\omega^{-1}$, $\omega \in R$, $\omega^2 = m \in F^*$.

It follows that $\pi^c = \omega\pi\omega^{-1} = \pi\omega^{\tau}\omega^{-1} = -\pi$. Write $x^c = \alpha_c x + \beta_c \pi(x)$ for some $\alpha_c, \beta_c \in R_{\mathfrak{N}}$. Then $(\pi(x))^c = \pi^c(x^c) = -\pi(\alpha_c x + \beta_c \pi(x)) = -\pi_0\beta_c^{\tau}x - \alpha_c^{\tau}\pi(x) = -\alpha_c^{\tau}\pi(x)$. In particular $\alpha_{\mathfrak{N}}(c) = -\alpha_c^{\tau}$. Since $c^2 = \operatorname{Id}$, $\alpha_c^{\tau} = \pm 1$ and $\bar{r}_{\mathfrak{N}}(c) = \begin{pmatrix} \pm 1 & 0 \\ \beta_c & \mp 1 \end{pmatrix}$. Either value takes $\bar{r}_{\mathfrak{N}}(c)$, the lemma follows. $\square$

Let $G_{\mathbb{Q}}^{ab} = \operatorname{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$ denote the Galois group of the maximal abelian extension $\mathbb{Q}^{ab}$ of $\mathbb{Q}$. For every prime $\ell$, let $\mathbb{Q}_{\ell}^{ab}$ denote the maximal abelian extension of $\mathbb{Q}_{\ell}$ and let $G_{\ell}^{ab} = \operatorname{Gal}(\mathbb{Q}_{\ell}^{ab}/\mathbb{Q}_{\ell})$. Let $I_{\ell}^{ab}$ denote the inertia subgroup of $G_{\ell}^{ab}$, which we regard as a subgroup of $G_{\mathbb{Q}}^{ab}$. Local class field theory establishes a canonical isomorphism

$$\omega_{\ell} : \mathbb{Z}_{\ell}^* \stackrel{\sim}{\longrightarrow} I_{\ell}^{ab},$$

the local Artin reciprocity map. Global class field theory yields a surjective map

$$\omega : \prod_{\ell} \mathbb{Z}_{\ell}^* \stackrel{\prod \omega_{\ell}}{\twoheadrightarrow} G_{\mathbb{Q}}^{ab}.$$

We shall denote

$$\varrho_{\ell} : \mathbb{Z}_{\ell}^* \stackrel{\omega_{\ell}}{\simeq} I_{\ell}^{ab} \subset G_{\mathbb{Q}}^{ab} \stackrel{\alpha_{\mathfrak{N}}}{\longrightarrow} k^*$$

the composition of the local Artin reciprocity map together with the character $\alpha_{\mathfrak{N}}$ acting on the canonical torsion subgroup $C$. In particular, since $\varrho_N : \mathbb{Z}_N^* \longrightarrow k^*$ is a continuous homomorphism, $\varrho_N(\mathbb{Z}_N^*) \subseteq \mathbb{F}_N^* \subset k^*$.

**Definition 3.2.** *Let $\kappa(A, \mathfrak{N})$ be the least common multiple of 4 and the orders of $\alpha_{\mathfrak{N}}(I_\ell)$ as $\ell$ runs over all prime integers $\ell \neq N$.*

Since $A$ has good reduction outside a finite set of primes, and potential good reduction at those, $\kappa(A, \mathfrak{N})$ is a well-defined integer.

For a prime $\ell$, let $\mathfrak{a}_\ell = \prod \mathfrak{L}$, where $\mathfrak{L}$ runs over the prime ideals of $F$ above $\ell$ such that $[F_\mathfrak{L} : \mathbb{Q}_\ell]$ is odd. Let $B(\ell)$ be the totally definite quaternion algebra over $F$ of discriminant $\frac{\mathfrak{D} \cdot \mathfrak{a}_\ell}{(\mathfrak{D}, \mathfrak{a}_\ell)^2}$.

**Definition 3.3.** *Let $\kappa(B)$ be the least common multiple of 2 and the positive integers $n \geq 3$ such that*

    (i) $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) \subseteq F$, and
    (ii) *For all $\ell \mid N_{F/\mathbb{Q}}(\mathfrak{D})$, no prime ideal $\wp \mid \frac{\mathfrak{D}}{(\mathfrak{D}, \mathfrak{a}_\ell)}$ splits in $F(\zeta_n)$.*

For instance, when $F = \mathbb{Q}$ or $F$ quadratic, $F \neq \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{5})$, we have $\kappa(B) \mid 12$. If $F = \mathbb{Q}(\sqrt{2})$, $\kappa(B) \mid 24$. If $F = \mathbb{Q}(\sqrt{5})$, $\kappa(B) \mid 60$.

For arbitrary $F$, we have $\kappa(B) \mid \mathrm{lcm}_{\varphi(n)|g}(n)$, since $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) = \sharp(\mathbb{Z}/n\mathbb{Z})^*$. Also, $8 \nmid \kappa(B)$ provided $\sqrt{2} \notin F$, because $\mathbb{Q}(\zeta_8 + \zeta_8^{-1}) = \mathbb{Q}(\sqrt{2})$.

**Lemma 3.4.** $\kappa(A, \mathfrak{N}) \mid 2 \cdot \kappa(B)$.

*Proof.* Let $\ell$ be a prime and $v$ a place of $K$ over $\ell$. Since $[I_\ell : I_v] \leq 2$, it suffices to show that $\alpha_{\mathfrak{N}}^{\kappa(B)}(I_v) = \{1\}$ for all places $v \nmid N$ of $K$.

Let $L_\ell/\mathbb{Q}_\ell$ be as in Lemma 2.1 the extension constructed by Serre and Tate over which $A$ acquires good reduction. Let $\tilde{A}/\mathbb{F}_\ell$ denote the closed fibre of the Néron model $\mathcal{A}$ of the abelian variety $A \otimes L_\ell$.

Let $\bar{\mathbb{F}}_\ell$ be a fixed algebraic closure of $\mathbb{F}_\ell$. Let $\tilde{B} = \mathrm{End}_{\bar{\mathbb{F}}_\ell}(\tilde{A}) \otimes \mathbb{Q}$ be the algebra of endomorphisms of $\tilde{A} \otimes \bar{\mathbb{F}}_\ell$, in which $B$ is embedded.

The group $I_v$ acts on $\mathcal{A} \times K_v$ via the Galois action on $L_\ell \cdot K_v$ over $K_v$. Since $B = \mathrm{End}_K^0(A)$, the action of $I_v$ commutes with that of $B$.

In addition, $I_v$ acts trivially on the residue field of $L_\ell \cdot K_v$ and thus specializes to an action on the closed fibre of $\mathcal{A}$ by algebraic automorphisms (cf. [SeTa, p. 497]). By considering the action both of $I_v$ and $\tilde{B}$ on $V_{\mathfrak{N}}(A \times L_\ell \cdot K_v) = V_{\mathfrak{N}}(\tilde{A})$ we obtain that $r_{\mathfrak{N}}(I_v)$ is a finite subgroup of the group $G$ of units of an order in $C_{\tilde{B}}(B)$, the centralizer of $B$ in $\tilde{B}$.

As in the proof of Proposition 5.2 in [Mi], $C_{\tilde{B}}(B)$ is either $(i)$ a totally imaginary quadratic extension of $F$ which splits $B$ or $(ii)$ $B(\ell)$.

In $(i)$, $A$ is isogenous over $\bar{\mathbb{F}}_\ell$ to $A_0^2$, where $A_0/\bar{\mathbb{F}}_\ell$ is an abelian variety of dimension $g/2$ with $\mathrm{End}_{\bar{\mathbb{F}}_\ell}(A_0) \supseteq C_{\tilde{B}}(B)$. In $(ii)$ $A/\bar{\mathbb{F}}_\ell$ is supersingular: it is isogenous to $g$ copies of a supersingular elliptic curve.

If $(i)$ holds, $G$ is the cyclic group of $n$-th roots of unity in the CM-field $C_{\tilde{B}}(B)$ for some $n \geq 1$. As soon as $n > 2$, $C_{\tilde{B}}(B) = F(\zeta_n)$. Since it splits $B$, no prime $\wp \mid \mathfrak{D}$ splits in $F(\zeta_n)$.

Assume now that $(ii)$ holds. If $G \supseteq \langle \zeta_n \rangle$ for some $n > 2$, then $F(\zeta_n)$ is a quadratic extension of $F$ which embeds in $B(\ell)$. We again deduce that no $\wp \mid \mathrm{disc}(B(\ell))$ splits in $F(\zeta_n)$. If $\ell \nmid N_{F/\mathbb{Q}}(\mathfrak{D})$, this implies that no $\wp \mid \mathfrak{D} \cdot \mathfrak{a}_\ell$ splits in $F(\zeta_n)$. If $\ell \mid N_{F/\mathbb{Q}}(\mathfrak{D})$, we obtain that no $\wp \mid \frac{\mathfrak{D}}{(\mathfrak{D}, \mathfrak{a}_\ell)}$ splits in $F(\zeta_n)$.

By Lemma 3.1, there exists a surjective homomorphism from $r_{\mathfrak{N}}(I_v)$ onto $\alpha_{\mathfrak{N}}(I_v)$. Since $\alpha_{\mathfrak{N}}(I_v) \subseteq k^*$, this is a cyclic group. The discussion above yields that $\alpha_{\mathfrak{N}}(I_v)^n = \{1\}$ for some $n$ as in the statement. $\square$

The above proof shows a slightly stronger fact: If $\ell \nmid N_{F/\mathbb{Q}}(\mathfrak{D})$ is a *supersingular prime* for $A$, then no $\wp \mid \mathfrak{D} \cdot \mathfrak{a}_\ell$ splits in $F(\zeta_n)$. We did not include this in the statement of Lemma 3.4 because we shall apply it to *any* modular abelian variety $A/\mathbb{Q}$ with multiplication by $B$. One can not expect to find a prime $\ell \nmid N_{F/\mathbb{Q}}(\mathfrak{D})$ which is supersingular for all such $A$ simultaneously.

**Corollary 3.5.** *Assume $K = \mathbb{Q}(\sqrt{-N})$ and $4 \mid \kappa(B)$. Then $\kappa(A, \mathfrak{N}) \mid \kappa(B)$.*

*Proof.* In the above proof we showed that $\alpha_{\mathfrak{N}}^{\kappa(B)}(I_v) = \{1\}$ for all places $v \nmid N$ of $K$. Since $K = \mathbb{Q}(\sqrt{-N})$, we have $I_v = I_\ell$ for all these places of $K$. As $4 \mid \kappa(B)$, it follows from the definition of $\kappa(A, \mathfrak{N})$ that it divides $\kappa(B)$. $\square$

**Proposition 3.6.** *For any prime $\ell \neq N$, $\alpha_{\mathfrak{N}}(\varphi_\ell^{\kappa(A,\mathfrak{N})}) = \ell^{\kappa(A,\mathfrak{N})/2}$.*

*Proof.* Let $\kappa = \kappa(A, \mathfrak{N})$. Let us first show that $\alpha_{\mathfrak{N}}(\varphi_\ell^\kappa) = \varrho_N^\kappa(\frac{1}{\ell}) \in \mathbb{F}_N^*$. The image by $\omega$ of the tuple

$$(\frac{1}{\ell}, ..., \frac{1}{\ell}, \overset{\ell}{\overset{\smile}{1}}, \frac{1}{\ell}, ..., \frac{1}{\ell}) \in \prod_p \mathbb{Z}_p^*$$

is an element $\tilde{\varphi}_\ell \in G_{\mathbb{Q}}^{ab}$ which reduces to the Frobenius automorphism $\mathrm{Fr}_\ell \in \mathrm{Gal}(\bar{\mathbb{F}}_\ell/\mathbb{F}_\ell)$. Hence $\varphi_\ell \circ \tilde{\varphi}_\ell^{-1} \in I_\ell$ and $\alpha_{\mathfrak{N}}(\varphi_\ell^\kappa) = \alpha_{\mathfrak{N}}(\tilde{\varphi}_\ell^\kappa)$ because $\alpha_{\mathfrak{N}}^\kappa(I_\ell) = \{1\}$. It follows that $\alpha_{\mathfrak{N}}^\kappa(\varphi_\ell) = \varrho_\ell^\kappa(1) \cdot \varrho_N^\kappa(\frac{1}{\ell}) \cdot \prod_{p \neq N, \ell} \varrho_p^\kappa(\frac{1}{\ell}) = \varrho_N^\kappa(\frac{1}{\ell})$.

Let $\bar{\chi}_N : G_{\mathbb{Q}} \longrightarrow \mathbb{F}_N^*$ be the reduction of the cyclotomic character mod $N$. By [Se1, Prop. 3, 8] we have $\bar{\chi}_{N|I_N^{ab}} \cdot \omega_N(x) = \frac{1}{x} \bmod N$ for all $x \in \mathbb{Z}_N^*$.

Since $\mathbb{F}_N^*$ has order $N - 1$, we have

$$\varrho_N(x) = x^{-c} \bmod N \text{ for some } 0 \leq c < N - 1.$$

By Lemma 3.1, since $\det(r_{\mathfrak{N}}) = \chi_N$ we have $\frac{1}{x} = \bar{\chi}_N(\omega_N(x)) = \det \bar{r}_{\mathfrak{N}}(\omega_N(x)) = \psi(\omega_N(x)) \cdot N_{k/k_0}(\alpha_{\mathfrak{N}}(\omega_N(x))) = \psi(\omega_N(x))N_{k/k_0}(\varrho_N(x))$.

Since $\varrho_N(x) \in \mathbb{F}_N^*$, $N_{k/k_0}(\varrho_N(x)) = \varrho_N^2(x)$ and it follows that $\varrho_N^2(x) = x^{-2c} = \pm x^{-1}$. Hence $2c \equiv 1$ or $\frac{N+1}{2} \bmod N - 1$. Since $N - 1$ is even, we deduce that $N \equiv 3 \bmod 4$ and $c = \frac{N+1}{4}$ or $\frac{3N-1}{4} \bmod N - 1$. Thus $\varrho_N^\kappa(x) \equiv x^{-\frac{(N+1)\kappa}{4}}$ or $x^{-\frac{(3N-1)\kappa}{4}} \bmod N$. Since $4 \mid \kappa$, $\frac{(N+1)\kappa}{4} \equiv \frac{(3N-1)\kappa}{4} \equiv \kappa/2 \bmod N - 1$ and $\alpha_{\mathfrak{N}}(\varphi_\ell^\kappa) = \ell^{\kappa/2} \in \mathbb{F}_N^*$. Consequently, $\alpha_{\mathfrak{N}}(\varphi_\ell^\kappa) = \ell^{\kappa/2}$. $\square$

During the proof of the above proposition we proved in passing the following.

**Corollary 3.7.** *$N \equiv 3 \bmod 4$.*

**Corollary 3.8.** *If $\mathrm{ord}_2(\kappa(A, \mathfrak{N})) \leq \mathrm{ord}_2(\nu + 1)$ then $K = \mathbb{Q}(\sqrt{-N})$.*

*Proof.* Let $\kappa = \kappa(A, \mathfrak{N})$. For each $\ell \neq N$ we have $\ell \equiv \psi(\mathrm{Fr}_\ell)\alpha_{\mathfrak{N}}(\mathrm{Fr}_\ell)^{\nu+1} \bmod \mathfrak{N}$. Set $t = \kappa/2^{\mathrm{ord}_2(\kappa)}$. Then $\kappa \mid t(\nu + 1)$ and $\ell^t \equiv \psi^t(\mathrm{Fr}_\ell)\alpha_{\mathfrak{N}}^{t(\nu+1)}(\mathrm{Fr}_\ell)$. Since $t$ is odd and $\psi$ is a quadratic character, it follows from Proposition 3.6 that $\psi(\mathrm{Fr}_\ell) \equiv \ell^{t(\nu-1)/2}$

mod $\mathfrak{N}$. As $\psi(\mathrm{Fr}_\ell), \ell \in \mathbb{Z}$ and $\mathfrak{N} = \mathfrak{N}_0 \cdot R$, this is equivalent to the congruence $\psi(\mathrm{Fr}_\ell) \equiv \ell^{t(\nu-1)/2} \bmod \mathfrak{N}_0$.

Since the residue field of $\mathfrak{N}_0$ is $k_0$, we obtain that $\psi(\mathrm{Fr}_\ell) = (\frac{\ell}{k_0})$ for all $\ell \neq N$. If $f$ is even, then $(\frac{\ell}{k_0}) = 1$ for all $\ell$ and $\psi$ is trivial, a contradiction. Hence $f$ is odd and $(\frac{\ell}{k_0}) = (\frac{\ell}{N}) = (\frac{-N}{\ell})$. It follows that $\psi = (\frac{-N}{\cdot})$ and $K = \mathbb{Q}(\sqrt{-N})$. $\square$

One application of Corollary 3.8 is in Theorem 1.4 $(ii)$. It can also be used to show in many instances that an analogue of (3) in the Introduction holds for higher degree fields $F$.

Let for example $(\mathcal{O}_\mathfrak{D}, R_{F(\sqrt{m})}, K)$ be a modular triplet such that $\sqrt{2} \notin F$ and $m \mid \mathfrak{D} = \mathfrak{N}_1 \cdot \ldots \cdot \mathfrak{N}_{2r}$, above integer primes $N_i$. Order them in some way that $\mathfrak{N}_i \mid 2m$ for $1 \leq i \leq s$ and $\mathfrak{N}_i \nmid 2m$ for $i > s$. Assume $\mathfrak{N}_{2r-1}$ and $\mathfrak{N}_{2r}$ can be chosen such that $N_{2r-1}, N_{2r}$ are odd, $N_{2r-1} \neq N_{2r}$ and $f(\mathfrak{N}_{2r}/N_{2r})$ is odd.

If either $(a)$ $N_i, N_j \equiv 1 \bmod 4$ for some $1 \leq i \neq j \leq s$ or $(b)$ $N_{2r} \equiv 7 \bmod 8$, then $s \geq 2r - 1$.

Indeed, if $s \leq 2r - 2$, it would follow from (2) in the Introduction that $N_{2r-1}N_{2r} \mid \mathrm{disc}(K)$. By Definition 3.3, $4 \nmid \kappa(B)$ in $(a)$, $8 \nmid \kappa(B)$ in $(b)$. By Lemma 3.4, $8 \nmid \kappa(A, \mathfrak{N}_{2r})$ in $(a)$, $16 \nmid \kappa(A, \mathfrak{N}_{2r})$ in $(b)$. Corollary 3.8 applied to $\mathfrak{N}_{2r}$ would imply $K = \mathbb{Q}(\sqrt{-N_{2r}})$, a contradiction.

**Lemma 3.9.** *The characteristic polynomial of $\varphi_\ell$ satisfies* $P_\ell(T) \equiv T^2 - (\alpha_\mathfrak{N}(\varphi_\ell) + \ell\alpha_\mathfrak{N}(\varphi_\ell^{-1})) \cdot T + \ell \in k[T]$.

*Proof.* It follows from Lemma 3.1 that for any $\sigma \in G_\mathbb{Q}$, the characteristic polynomial $P_\sigma(T) \in R[T]$ satisfies

$$P_\sigma \bmod \mathfrak{N} \equiv T^2 - (\alpha_\mathfrak{N}(\sigma) + \psi(\varphi_\ell)\alpha_\mathfrak{N}(\sigma)^\nu) \cdot T + \psi(\varphi_\ell)\mathrm{Nm}(\alpha_\mathfrak{N}(\sigma)).$$

Besides, as we mentioned at the end of Section 2, we have $P_\ell = P_{\varphi_\ell} = T^2 - a_\ell T + \ell$. Hence $\psi(\varphi_\ell)\alpha_\mathfrak{N}(\varphi_\ell)^\nu\alpha_\mathfrak{N}(\varphi_\ell) = \ell \in k$ and we deduce that $a_\ell \equiv \alpha_\mathfrak{N}(\varphi_\ell) + \psi(\varphi_\ell)\alpha_\mathfrak{N}(\varphi_\ell)^\nu \equiv \alpha_\mathfrak{N}(\varphi_\ell) + \ell\alpha_\mathfrak{N}(\varphi_\ell^{-1}) \bmod \mathfrak{N}$. $\square$

## 4. Proof of the main results

Keep the notations of the previous section. Let $\lambda_\pm = \sqrt{2\ell \pm \sqrt{3}}$.

**Theorem 4.1.** *Let $(\mathcal{O}, R, K)$ be a modular triplet. Assume $\zeta_n + \zeta_n^{-1} \notin F$ for any $n$-th primitive root of 1, $n \neq 1, 2, 3, 4, 6$, and that $\mathcal{O}$ is locally maximal at some ideal $\mathfrak{N}_0 \mid \mathrm{disc}(B)$, $\mathfrak{N}_0 \nmid 2m$. Then, for any prime $\ell$ which splits or ramifies in $K$, either $\mathfrak{N}_0 \in \mathcal{N}_\ell$ or*

- $(\frac{-\ell}{\wp}) \neq 1$ *for all $\wp \mid \mathfrak{D}$, or*
- $\sqrt{2\ell} \in F$ *and $(\frac{-1}{\wp}) \neq 1$ for all $\wp \mid \mathfrak{D}$, $\wp \nmid \ell$, or*
- $\sqrt{\ell}$ *or $\sqrt{3\ell} \in F$ and $(\frac{-3}{\wp}) \neq 1$ for all $\wp \mid \mathfrak{D}$, $\wp \nmid \ell$, or*
- $\lambda_\pm\sqrt{\ell} \in F$ *and $(\frac{-1\mp4\sqrt{3}/7}{\wp}) \neq 1$ for all $\wp \mid \mathfrak{D}$, $\wp \nmid \ell$.*

*Proof.* Let $A$ be a modular abelian variety over $\mathbb{Q}$ such that $\mathrm{End}_\mathbb{Q}(A) = R$ and $\mathrm{End}_K(A) \simeq \mathcal{O}$.

By our assumption on $\mathfrak{N}_0$, it remains inert in $R$ and we let $\mathfrak{N} = \mathfrak{N}_0 R$ (cf. Section 3). Let $\bar{\mathfrak{N}}$ be an ideal of $\bar{\mathbb{Q}}$ above $\mathfrak{N}_0$. Choose a prime $\ell$ such that $\mathfrak{N}_0 \notin \mathcal{N}_\ell$ and $(\frac{K}{\ell}) \neq -1$. Then $\mathfrak{N}_0 \nmid \ell$, $\varphi_\ell \in G_K$ and $a_\ell \in R_F$.

By Lemma 3.9, $\alpha_{\mathfrak{N}}(\varphi_\ell) + \ell\alpha_{\mathfrak{N}}(\varphi_\ell^{-1}) = \sqrt{\ell} \cdot (\frac{\alpha_{\mathfrak{N}}(\varphi_\ell)}{\sqrt{\ell}} + (\frac{\alpha_{\mathfrak{N}}(\varphi_\ell)}{\sqrt{\ell}})^{-1}) \equiv a_\ell \bmod \bar{\mathfrak{N}}$. Here, $\zeta = \frac{\alpha_{\mathfrak{N}}(\varphi_\ell)}{\sqrt{\ell}}$ is a $\kappa(A, \mathfrak{N})$-th root of 1 by Proposition 3.6.

Since $\zeta_n + \zeta_n^{-1} \notin F$ for any $n \neq 1, 2, 3, 4, 6$, we have $\kappa(B) \mid 12$. Hence $\kappa(A, \mathfrak{N}) \mid 24$ by Lemma 3.4.

Computing the possible values of $\sqrt{\ell}(\zeta + \zeta^{-1})$ for all 24-th roots of 1, we obtain that $a_\ell \equiv 0, \sqrt{\ell}, \sqrt{2\ell}, \sqrt{3\ell}, 2\sqrt{\ell}$ or $\lambda_\pm \cdot \sqrt{\ell} \bmod \bar{\mathfrak{N}}$. In other words, $\mathfrak{N}_0 \mid a_\ell^2 - s\ell$ for some $s = 0, 1, 2, 3, 4$ or $\mathfrak{N}_0 \mid a_\ell^4 - 4a_\ell^2\ell + \ell^2$.

As we already mentioned, $|\tau(a_\ell)| \leq 2\sqrt{\ell}$ for any $\tau : F \hookrightarrow \mathbb{R}$. It follows from the very definition of $\mathcal{N}_\ell$ that the above congruence is in fact an identity: $a_\ell = 0, \sqrt{\ell}, \sqrt{2\ell}, \sqrt{3\ell}, 2\sqrt{\ell}$ or $\lambda_\pm \cdot \sqrt{\ell}$.

Since $(\frac{K}{\ell}) \neq -1$, the residue field of $K$ at $\ell$ is $\mathbb{F}_\ell$. By reducing the endomorphisms of $A$ mod $\ell$ it follows that $B = \mathrm{End}_K(A) \otimes \mathbb{Q}$ embeds in $\mathrm{End}_{\mathbb{F}_\ell}(\tilde{A}) \otimes \mathbb{Q}$.

According to [Ta1, Theorem 2 (a)], [Ta2, Theorem 1 (1)], $\mathrm{End}_{\mathbb{F}_\ell}(\tilde{A}) \otimes \mathbb{Q}$ is isomorphic to $\mathrm{M}_{2r}(\tilde{F})$, where $\tilde{F}$ is the splitting field of $\prod_{\tau:F\hookrightarrow\mathbb{R}}(T^2 - a_\ell^\tau T + \ell)$. Here, $r \mid g = \dim(A)$ and $[\tilde{F} : \mathbb{Q}] = g/r$.

From the above values for $a_\ell$ we have (in the same order) $\tilde{F} = \mathbb{Q}(\sqrt{-\ell})$, $\mathbb{Q}(\sqrt{\ell}, \sqrt{-3})$, $\mathbb{Q}(\sqrt{2\ell}, \sqrt{-1})$, $\mathbb{Q}(\sqrt{3\ell}, \sqrt{-3})$, $\mathbb{Q}(\sqrt{\ell})$ or $\mathbb{Q}(\lambda_\pm \cdot \sqrt{\ell}, \sqrt{-1 \mp 4\sqrt{3}/7})$.

Case $\tilde{F} = \mathbb{Q}(\sqrt{\ell})$ can not arise: we would have $\mathrm{End}_{\mathbb{F}_\ell}(A) \otimes \mathbb{Q} \simeq \mathrm{M}_g(\mathbb{Q}(\sqrt{\ell}))$ and this would say that $A$ is isogenous to $g$ copies of an elliptic curve $E/\mathbb{F}_\ell$ with $\mathrm{End}_{\mathbb{F}_\ell}(E) \otimes \mathbb{Q} \simeq \mathbb{Q}(\sqrt{\ell})$, which is not possible.

Let us show that $F \cdot \tilde{F}$ splits $B$ locally at all places $\wp \nmid \ell$, or equivalently, no prime $\wp \mid \mathfrak{D}$, $\wp \nmid \ell$, splits in the quadratic extension $F \cdot \tilde{F}$ of $F$.

The Tate module $V_p(\tilde{A})$ is a $F \cdot \tilde{F} \otimes \mathbb{Q}_p$-vector space of rank 2. Since $B \subset \mathrm{End}_{\mathbb{F}_\ell}(\tilde{A}) \otimes \mathbb{Q}$ and $\tilde{F}$ is the center of $\mathrm{End}_{\mathbb{F}_\ell}(\tilde{A}) \otimes \mathbb{Q}$, we conclude that $B$ acts $F \cdot \tilde{F} \otimes \mathbb{Q}_p$-linearly on $V_p(\tilde{A})$.

Thus $B \subset \mathrm{M}_2(F \cdot \tilde{F} \otimes \mathbb{Q}_p)$, which says that $F \cdot \tilde{F}$ splits $B$ locally at $\wp$.

Finally, when $\tilde{F} = \mathbb{Q}(\sqrt{-\ell})$, it is also clear that $F \cdot \tilde{F} = F(\sqrt{-\ell})$ also splits $B$ at the places $\wp \mid \ell$, because these prime ideals ramify in $F \cdot \tilde{F}$. This finishes the proof of the theorem. □

Theorem 1.2 $(iii)$ now follows automatically by applying Theorem 4.1 to each prime ideal $\mathfrak{N} \mid \mathfrak{D}$, $\mathfrak{N} \nmid 2m$. Note that, in this case, since we assume that $\sqrt{\ell}, \sqrt{2\ell}, \sqrt{3\ell}, \sqrt{2\ell} \pm \sqrt{3\ell} \notin F$, it follows that $a_\ell = 0$ and $\tilde{F} = \mathbb{Q}(\sqrt{-\ell})$.

**Remark 4.2.** As we saw in Proposition 1.3, Theorem 1.4 and Corollary 3.8, we can often claim that $K = \mathbb{Q}(\sqrt{-N})$. When this is the case, last item in the statement of Theorem 4.1 can be removed and one can replace the sets $\mathcal{N}_\ell$ by the smaller sets $\mathcal{N}_\ell^0 = \{\mathfrak{N}_0 \mid \ell \text{ or } a^2 - s\ell\}$, with $a$ and $s$ as in Definition 1.1. This is because in the above proof we have $\kappa(A, \mathfrak{N}) \mid 12$, thanks to Corollary 3.5.

*Proof of Theorem 1.4.* Since the hypothesis of Theorem 1.2 $(ii)$ are satisfied, we obtain that $N \equiv 3 \bmod 4$.

Assume first that $M \equiv 3 \bmod 4$. Proposition 1.3 applies and asserts that $K \simeq \mathbb{Q}(\sqrt{-d})$, where $d = M$ or $N$. Since $B \simeq (\frac{-d,M}{\mathbb{Q}})$ we deduce that $d = N$ and $(\frac{-N}{M}) = -1$. Finally, for any odd prime $\ell$ such that $(\frac{\ell}{N}) = 1$ and $N \notin \mathcal{N}_\ell$, Theorem 4.1 together with Gauss' reciprocity law asserts that $(\frac{-\ell}{M}) = -1$.

Assume now that $M \equiv 1 \bmod 4$. Proposition 1.3 now implies that $K \simeq \mathbb{Q}(\sqrt{-d})$ for $d = MN$ or $N$. In any case, it again follows as above that $(\frac{-N}{M}) = -1$.

If $d = N$, we similarly have $(\frac{-\ell}{M}) = -1$ for any prime $\ell$ such that $(\frac{\ell}{N}) = 1$ and $N \notin \mathcal{N}_\ell$, even for $\ell = 2$.

If $d = MN$, $N \equiv 3 \bmod 8$ by Lemma 3.4 and Corollary 3.8. Let $\ell \neq 2$ be a prime such that $N \notin N_\ell$ and $(\frac{-MN}{\ell}) = 1$. Theorem 4.1 produces the congruences $(\frac{-\ell}{N}) = (\frac{-\ell}{M}) = -1$, which Gauss' reciprocity law shows to be incompatible with $(\frac{-MN}{\ell}) = 1$. $\square$

## References

[BFGR]  N. Bruin, V. Flynn, J. Gonzàlez, and V. Rotger, *On finiteness conjectures for endomorphism algebras of abelian surfaces*, Math. Proc. Camb. Phil. Soc. **141:3** (2006), 383-408.

[Di]  L. V. Dieulefait, *Remarks on Serre's modularity conjecture*, Preprint 2006.

[Ha]  Y. Hasegawa, *On some examples of modular QM-abelian surfaces*, Proc. Japan Acad., Ser. A **72** (1996), 23-27.

[Jo]  B.W. Jordan, *Points on Shimura curves rational over number fields*, J. Reine Angew. Math. **371** (1986), 92-114.

[KaWi]  C. Khare and J.-P. Wintenberger, *Serre's Modularity Conjecture (I), (II)*, Preprints 2006.

[Ki]  M. Kisin, *Modularity of 2-adic Barsotti-Tate representations*, Preprint.

[Mi]  J. S. Milne, *Points on Shimura varieties mod p*, Proc. Symp. Pure Math. **33** (1979), 165-184.

[PY]  P. Parent and A. Yafaev, *Proving the triviality of rational points on Atkin-Lehner quotients of Shimura curves*, Math. Annalen **339:4** (2007), 915-935.

[Ri1]  K. A. Ribet, *Endomorphism algebras of abelian varieties attached to newforms of weight 2*, Progress in Math. **12** (1981), 263-276.

[Ri2]  ———, *Abelian varieties over $\mathbb{Q}$ and modular forms*, in Modular curves and abelian varieties, J. Cremona, J.-C. Lario, J. Quer, K. Ribet (eds.), Progress in Mathematics **224**, Birkhäuser (2004), 241-261.

[Ro]  V. Rotger, *Rational points on Atkin-Lehner quotients of Shimura varieties*, in preparation.

[RSY]  V. Rotger, A. Skorobogatov, and A. Yafaev, *Failure of the Hasse principle for Atkin-Lehner quotients of Shimura curves over $\mathbb{Q}$*, Moscow Math. J. **5:2**, (2005) 463-476.

[Se1]  J.-P. Serre, *Propriétés galoisiennes des points d'ordre finit des coubes elliptiques*, Invent. Math. **15** (1972), 259-331.

[Se2]  ———, *Quelques applications du théorème de densité de Chebotarev*, Publ. I. H. É. S. **54** (1981), 123-201.

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

[Ta1]  J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134-144.

[Ta2]  ———, *Classes d'isogénie des variétés abéliennes sur un corps fini*, Séminaire Bourbaki, **352** (1968-69), 95-110.

[Vi]  M.F. Vignéras, *Arithmétique des algèbres de quaternions*, Lect. Notes Math. **800**, 1980.

Universitat Politècnica de Catalunya, Departament de Matemàtica Aplicada IV (EPSEVG), Av. Victor Balaguer s/n, 08800 Vilanova i la Geltrú (Barcelona), Spain.

*E-mail address*: `vrotger@ma4.upc.edu`