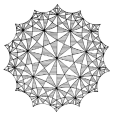
Rev. Mat. Iberoam. (Online first)
DOI 10.4171/RMI/1556



On endomorphism algebras of GL_2-type abelian varieties and Diophantine applications

Franco Golfieri Madriaga, Ariel Pacetti and Lucas Villagra Torcomian

Abstract. Let f and g be two different newforms without complex multiplication having the same coefficient field. The main result of the present article proves that an isomorphism between the residual Galois representations attached to f and to g for a large prime p (depending only on g) implies that the endomorphism algebra of the abelian variety A_f, attached to f by the Eichler–Shimura construction (after tensoring with $\mathbb{Q}$), is a subalgebra of the endomorphism algebra of the abelian variety A_g attached to g. This implies important relations between their building blocks. A non-trivial application of our result is that for all prime numbers d congruent to 3 modulo 8 satisfying that the class number of $\mathbb{Q}(\sqrt{-d})$ is prime to 3, the equation $x^4 + dy^2 = z^p$ has no non-trivial primitive solutions when p is large enough. We prove a similar result for the equation $x^2 + dy^6 = z^p$.

1. Introduction

Let $\tilde{N}$ be a positive integer and let ε be a Dirichlet character of conductor dividing $\tilde{N}$. Let $g \in S_2(\Gamma_0(\tilde{N}), \varepsilon)$ be a newform of weight 2, level $\tilde{N}$ and Nebentypus ε. Let K_g denote the coefficient field of the newform g (i.e., the minimum number field containing all the Fourier coefficients $a_n(g)$ of g). For $\mathfrak{p}$ a prime ideal of K_g, we denote $\rho_{g,\mathfrak{p}}$ the Galois representation attached to g (by Eichler and Shimura). After choosing an appropriate basis for the underlying vector space, one can always assume that the representation has coefficients in the ring of integers of the completion of K_g at $\mathfrak{p}$, so it makes sense to consider its reduction $\bar{\rho}_{g,\mathfrak{p}}$.

Let N be a divisor of $\tilde{N}$ and let $f \in S_2(\Gamma_0(N), \varepsilon)$ be another newform satisfying the following conditions:

(1) The coefficient field K_f of f matches the coefficient field K_g of g.

(2) There exists a prime p such that the semisimplification of the residual Galois representations $\bar{\rho}_{f,\mathfrak{p}}$ and $\bar{\rho}_{g,\mathfrak{p}}$ are isomorphic for some prime ideal $\mathfrak{p}$ of K_g dividing p.

Mathematics Subject Classification 2020: 11D41 (primary); 11F80 (secondary).
Keywords: endomorphisms of GL_2-type abelian varieties, Diophantine equations, modular method.

By the Eichler–Shimura construction, there exist abelian varieties A_f and A_g defined over $\mathbb{Q}$ of dimension $[K_f : \mathbb{Q}]$ attached to each of the eigenforms with the property that

$$L(A_f, s) = \prod_{\sigma \in \mathrm{Hom}(K_f, \mathbb{C})} L(\sigma(f), s),$$

and a similar relation for g. Let $L/\mathbb{Q}$ be a field extension, and denote by $\mathrm{End}_L(A_f)$ the ring of endomorphisms of A_f defined over L.

Question 1. *Is there a relation between* $\mathrm{End}_L(A_f) \otimes \mathbb{Q}$ *and* $\mathrm{End}_L(A_g) \otimes \mathbb{Q}$*?*

By a result of Hecke (see [9], p. 811, Satz 1 and Satz 2), if the Fourier coefficients $a_n(f) = a_n(g)$ for sufficiently many small values of n, then the two forms coincide. A congruence between f and g modulo a large prime ideal $\mathfrak{p}$ implies (as will be explained in the proof of Theorem 2.5) that their first Fourier coefficients must be equal (due to the Ramanujan–Petersson bound), proving the existence of a constant M (depending on the level of f and the level of g) such that if $\mathfrak{p}$ is a prime ideal whose norm is larger than M, then an isomorphism (of the semisimplifications of) $\bar{\rho}_{f,\mathfrak{p}} \simeq \bar{\rho}_{g,\mathfrak{p}}$ implies that $f = g$. In particular, their endomorphism algebras are isomorphic. The non-trivial problem is whether given the form g, there exists a constant M_g (depending either on the form g or on its level) such that if $p > M_g$ then the endomorphism algebras of both varieties are related for any form f.

One of the main results of the present article (Theorem 2.5) is to provide a positive answer to this second problem when g does not have complex multiplication and $\tilde{N}/N$ is square-free, namely, we prove the existence of a constant M_g such that if $p > M_g$, then for any newform f without complex multiplication and satisfying conditions (1) and (2), there exists an injective morphism $\psi\colon \mathrm{End}_L(A_f) \otimes \mathbb{Q} \to \mathrm{End}_L(A_g) \otimes \mathbb{Q}$.

Our method could be used to prove a similar result for modular forms with complex multiplication; however, because of the applications we have in mind, in the present article we restrict to the case of modular forms without complex multiplication. Similarly, the hypothesis $\tilde{N}/N$ square-free can be removed if one makes a more detailed study of local types, but it simplifies some proofs and is satisfied in our applications.

The proof is based on results of Ribet on the splitting of a modular GL_2-type abelian variety A_f over a number field L (as developed in [22–24]). In such articles, the author constructs endomorphisms of A_f in terms of properties of Fourier coefficients of the form f. Then to provide an answer to Question 1, it is enough to relate the Fourier coefficients of f to those of g.

The proof of Theorem 2.5 consists on proving that the congruence between the newforms f and g implies that all inner twists of g are also inner twists of f. The constructed morphism is not just a morphism of $\mathbb{Q}$-algebras, but also a morphism of $\mathrm{Gal}(L/\mathbb{Q})$-modules. This provides a relation between the splitting (up to isogeny) of the abelian variety A_f and that of A_g over any field extension $L/\mathbb{Q}$.

Here is, in our opinion, an interesting application of our main result to the study of Diophantine equations (the original motivation for this article) following the modular approach. Consider the equation

$$x^4 + dy^2 = z^p, \tag{1.1}$$

for a fixed positive square-free integer d. A solution (a, b, c) of a Fermat-type equation such as (1.1) is called *primitive* if $\gcd(a, b, c) = 1$, and is also said to be *trivial* if $abc = 0$. To a putative primitive solution (a, b, c), one attaches an elliptic curve $E_{(a,b,c)}$ defined over the imaginary quadratic field $K := \mathbb{Q}(\sqrt{-d})$ given by the equation

$$E_{(a,b,c)} : y^2 = x^3 + 4ax^2 + 2(a^2 + \sqrt{-d}\,b)\,x, \tag{1.2}$$

whose discriminant equals $512(a^2 + b\sqrt{-d})\,c^p$. The curve $E_{(a,b,c)}$ has additive/multiplicative reduction at the primes dividing 2, multiplicative reduction at all odd primes dividing c and good reduction at all other primes (our primitivity assumption implies that $\gcd(c, d) = 1$). The curve $E_{(a,b,c)}$ turns out to be a $\mathbb{Q}$-curve, hence in particular (by a result of Ribet in [25], see the paragraph after Theorem 6.3), there exists a Hecke character $\varkappa\colon \mathrm{Gal}_K \to \overline{\mathbb{Q}}^\times$, where Gal_K denotes the absolute Galois group of K, such that the twisted representation

$$\rho := \rho_{E_{(a,b,c)},p} \otimes \varkappa : \mathrm{Gal}_K \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$$

extends to a representation $\tilde{\rho}$ of the whole absolute Galois group $\mathrm{Gal}_{\mathbb{Q}}$. If the residual representation of $\tilde{\rho}$ is reducible, then $\tilde{\rho}$ is modular by Theorem 1.0.2 in [19]. Otherwise, the residual representation of $\tilde{\rho}$ is modular by Serre's conjecture (proven in [13, 14]). Then $\tilde{\rho}$ itself is modular by [15] (theorem in the second page), i.e., there exist a modular form $f \in S_2(\Gamma_0(N), \varepsilon)$, where N is the conductor of the representation $\tilde{\rho}$ and ε its Nebentypus (an explicit formula for N and ε is given in Theorem 4.2 of [18]), and a prime ideal $\mathfrak{p}$ in the coefficient field K_f of f such that $\tilde{\rho} \simeq \rho_{f,\mathfrak{p}}$.

The curve $E_{(a,b,c)}$ has multiplicative reduction at all odd primes dividing c (since the solution is primitive, if a prime q divides c, it cannot divide d), so by a result of Hellegouarch (Theorem 6.5.1 in [10]), together with Ribet's lowering the level result, there exists a newform g of level $\tilde{N}$ (only divisible by primes dividing $2d$) congruent to f modulo p. Then one is led to compute the space $S_2(\Gamma_0(\tilde{N}), \varepsilon)$ and to prove that no newform can be related to a non-trivial primitive solution of (1.1). By an idea due to Mazur (see [30]), one can discard all forms g whose coefficient field K_g does not match that of f when the prime p is large enough. This justifies the first hypothesis in Question 1. However, the newforms g whose coefficient field K_g matches K_f could pass this elimination procedure. There is a plausible situation that might appear (because K is an imaginary quadratic field) which is that the building block of A_g (see Section 3.1 for a quick review of building blocks) might have dimension two (i.e., is related to a "fake elliptic curve", namely an abelian surface with quaternionic multiplication).

The abelian variety A_f has a 1-dimensional building block, namely the elliptic curve $E_{(a,b,c)}$ itself. Suppose once again that the newform g does not have complex multiplication.

Question 2. *Is it true that the building block E_g of A_g has dimension 1? If so, what is the minimum field of definition of the elliptic curve E_g?*

To our knowledge, no general method was developed before to provide an answer to Question 2 (i.e., an unpleasant type of congruence between an elliptic curve and a fake elliptic curve). A key result used in the pioneering article [26] is that fake elliptic curves have potentially good reduction at all primes. In particular, if the elliptic curve attached to a

putative solution of our favorite Diophantine equation has a prime of multiplicative reduction, the building block E_g must have dimension 1. This is the case for Fermat's original equation, as exploited in [26] while proving asymptotic results for general number fields. Unfortunately, this is not the case for many Diophantine equations, like equation (1.1), which motivated the results of the present article. A possible workaround (to get partial results) is to impose some constraints on the solutions in order to ensure a prime of potentially multiplicative reduction for the attached elliptic curve. For instance, this idea was used in [11, 17] while studying equations $x^p + y^p = z^2$ and $x^p + y^p = z^3$.

One of the main contributions of the present article is to provide a positive answer to Question 2 when p is large enough (see Proposition 3.5 and Theorem 3.6). Furthermore, we prove that the elliptic curve E_g can be defined over the quadratic field K (see Theorem 3.6) and the building block is totally defined over $K(\sqrt{-2})$. A non-trivial strengthening of our solution to this problem (required while studying equation (1.1)) is that the curve E_g can be chosen so that the residual Galois representations $\bar{\rho}_{E_{(a,b,c)},p}$ and $\bar{\rho}_{E_g,p}$ are isomorphic (see Theorem 3.16).

The method used to answer Question 2 could be used to prove non-existence of solutions of other Diophantine equations over number fields (like imaginary quadratic ones).

For proving non-existence of non-trivial primitive solutions of (1.1), the last missing ingredient is a result on non-existence of elliptic curves with the same properties as E_g defined over K. The key property that E_g satisfies is that it has conductor supported on primes dividing 2 and it has a K-rational point of order 2. Some quite recent results on Diophantine equations depend on results of non-existence of elliptic curves over number fields whose conductor is supported at a unique prime (see for example [7]). Here is an instance of such a result that we prove in the present article.

Theorem 3.17. *Let $d \neq 3$ be a prime number such that $d \equiv 3 \pmod 8$, and 3 does not divide the class number of $K = \mathbb{Q}(\sqrt{-d})$. Then the only elliptic curves defined over K having a K-rational point of order 2 and conductor supported at 2 are those that are base change of $\mathbb{Q}$.*

As a consequence, we can prove the following asymptotic result.

Theorem 3.23. *Let d be a prime number congruent to 3 modulo 8 and such that the class number of $\mathbb{Q}(\sqrt{-d})$ is not divisible by 3. Then there are no non-trivial primitive solutions of the equation*

$$x^4 + dy^2 = z^p,$$

for p large enough.

A similar approach works while studying the Diophantine equation

$$x^2 + dy^6 = z^p.$$

To a putative solution (a, b, c) one can attach the elliptic curve

$$\widetilde{E}_{(a,b,c)} : y^2 + 6b\sqrt{-d}xy - 4d(a + b^3\sqrt{-d})y = x^3, \tag{1.3}$$

over the quadratic field $K = \mathbb{Q}(\sqrt{-d})$. The curve $\widetilde{E}_{(a,b,c)}$ is again a $\mathbb{Q}$-curve with a K-rational point of order 3 (namely the point $(0, 0)$). Such equation was also studied in [18].

Once again, there is a character $\varkappa$ such that the twisted representation $\rho_{\widetilde{E}_{(a,b,c)},p} \otimes \varkappa$ extends to an odd representation of $\mathrm{Gal}_{\mathbb{Q}}$. The main difference with equation (1.1) is that the elliptic curve $\widetilde{E}_{(a,b,c)}$ has bad additive reduction at all primes of K dividing d (extra care must be taken at primes dividing 6, see Lemmas 2.13, 2.14 and 2.15 in [18]), while the curve $E_{(a,b,c)}$ had only bad reduction (either additive or multiplicative, depending on d modulo 8, see Lemma 2.8 in [18]) at primes dividing 2. We will prove the following result.

Theorem 3.24. *Let d be a prime number congruent to 19 modulo 24 and such that the class number of $\mathbb{Q}(\sqrt{-d})$ is not divisible by 3. Then there are no non-trivial primitive solutions of the equation*

$$x^2 + dy^6 = z^p,$$

for p large enough.

The article is organized as follows. Section 2 recalls the definition and main properties of inner twists as developed by Ribet in [22]. It also contains the proof of Theorem 2.5 providing an answer to Question 1. In Section 3.1, after recalling the basic definitions of building blocks and fields of definition, we apply the theory of inner twists to the abelian variety A_f attached to the (non-quadratic twist of the) elliptic curve $E_{(a,b,c)}$ coming from a putative solution (a, b, c) of (1.1). In particular, we compute explicitly the group of inner twists of A_f and use this information to answer Question 2 (and its consequences). The last part of the article is devoted to prove Theorem 3.17 on non-existence of elliptic curves over K with a 2-torsion point and bad reduction only at the prime 2. It also contains the proof of Theorem 3.23 and of Theorem 3.24. The code used to prove Theorem 3.24 is available at https://github.com/lucasvillagra/Asymptotic-results.

2. Inner twists

Let $f \in S_k(\Gamma_0(N), \varepsilon)$ be a modular form and let χ be a Dirichlet character. The *twist* of f by χ (denoted $f \otimes \chi$) is the newform attached to the modular form with Fourier expansion

$$\sum_{n \geq 1} a_n(f)\chi(n)\, q^n.$$

Definition. A modular form $f \in S_k(\Gamma_0(N), \varepsilon)$, with $k \geq 2$, has *complex multiplication* (CM for short) if there exists a non-trivial Dirichlet character χ such that $f = f \otimes \chi$.

As mentioned in the introduction, due to the applications we have in mind, during this article we will restrict to modular forms without complex multiplication. Recall the following definition of [22].

Definition. Let $f \in S_2(\Gamma_0(N), \varepsilon)$ be a newform without complex multiplication, and let K_f denote its coefficient field. The *set of inner twists* of f is defined as

$$\Gamma_f := \{\gamma \in \mathrm{Hom}_{\mathbb{Q}}(K_f, \mathbb{C}) : \exists\, \chi_\gamma \text{ a Dirichlet character with } \gamma(a_p(f)) = \chi_\gamma(p) a_p(f) \text{ for almost all } p\}. \tag{2.1}$$

Remark 2.1. Although it is not explicitly stated in Ribet's article, it is the case that we can replace the condition "for almost all p" in (2.1) by "for all p not dividing the conductor of χ_γ nor N".

Here are some facts about Γ_f and its elements:

(1) For $\gamma \in \Gamma_f$, $\gamma(K_f) \subset K_f$ (see Proposition 3.2 in [22]). In particular, Γ_f is a subset of $\mathrm{Aut}_{\mathbb{Q}}(K_f)$ and the values of χ_γ belong to K_f.

(2) The set Γ_f is in fact an abelian group (see Proposition 3.3 in [22]).

(3) Given $\gamma \in \Gamma_f$, the character χ_γ is unique (see [22], page 48).

(4) The conductor of χ_γ is supported at primes dividing N (see [22], page 48).

The third property implies that we can (and will) denote elements of Γ_f by pairs (γ, χ).

Example. If f is a newform in $S_2(\Gamma_0(N), \varepsilon)$, and the Nebentypus ε is not trivial, then the coefficient field K_f is a CM extension of $\mathbb{Q}$, and the pair (c, ε^{-1}), where c denotes complex conjugation, is an element of Γ_f (see Example 3.7 in [22]).

Lemma 2.2. *If $(\gamma, \chi) \in \Gamma_f$, then the conductor of χ divides $8N$.*

Proof. Comparing the Nebentypus of $\gamma(f)$ and $f \otimes \chi$, we get the well-known relation

$$\chi^2 = \gamma(\varepsilon)/\varepsilon. \tag{2.2}$$

In particular, the conductor of χ^2 divides N. If p is an odd prime, the valuation at p of the conductor of χ^2 is either 0 (so the valuation at p of the conductor of χ is at most 1), or it equals the valuation at p of the conductor of χ. But the conductor of χ is supported at primes dividing N (because $f \otimes \chi$ has the same level N as f), so we conclude that the p-valuation of its conductor is at most $v_p(N)$. At the prime 2, if χ^2 is unramified at 2, then the conductor of χ has valuation at most 3 at 2; otherwise, the valuation at 2 of the conductor of χ^2 is one less than that of χ. ∎

Let $\mathrm{End}^0(A_f) := \mathrm{End}(A_f) \otimes \mathbb{Q}$ denote the algebra of endomorphisms defined over the algebraic closure of $\mathbb{Q}$. If L is an extension of $\mathbb{Q}$, let $\mathrm{End}^0_L(A_f) := \mathrm{End}_L(A_f) \otimes \mathbb{Q}$, where $\mathrm{End}_L(A_f)$ denotes the ring of endomorphisms of A_f defined over L. An important consequence of the main results of [22] is that the endomorphism algebra $\mathrm{End}^0(A_f)$ can be computed in terms of the group of inner twists Γ_f. Concretely, in the proof of Theorem 5.1 in [22], Ribet constructs for each inner twist $(\gamma, \chi) \in \Gamma_f$ an endomorphism η_γ, and proves that the algebra generated by K_f and the endomorphisms η_γ (for all $\gamma \in \Gamma_f$) equals $\mathrm{End}^0(A_f)$ (see page 59 of [22]).

The construction of η_γ given by Ribet is as follows: let $(\gamma, \chi) \in \Gamma_f$ be an inner twist. Let t be the order of χ and let r be its conductor. As mentioned in Ribet's article, without loss of generality, we can assume that $r^2 \mid N$. Otherwise, let h be the modular form

$$h = \sum_{(n,r)=1} a_n(f)\, q^n.$$

Then h is a modular form of level $r^2 N$ (as proved for example in Proposition 17 in Section 3 of [16]). In [22], Ribet proves (see Proposition 2.2 and page 57) that the abelian variety A_f is isogenous over $\mathbb{Q}$ to the abelian variety A_h, hence it is enough to define the endomorphism η_γ on A_h (see Section 5 of [22] for extra details).

The first stated property at the beginning of the section implies that K_f contains the t-th roots of unity, so for any integer u, the value $\chi^{-1}(u)$ is an endomorphism of A_f (defined over $\mathbb{Q}$). Then (as in page 57 of [22]) let

$$\eta_\gamma := \sum_{u \pmod r} \chi^{-1}(u) \circ \alpha_{u/r}, \tag{2.3}$$

where $\alpha_{u/r}$ is the endomorphism corresponding to slashing by the matrix $\left(\begin{smallmatrix} 1 & u/r \\ 0 & 1 \end{smallmatrix}\right)$ in the space $S_2(\Gamma(N))$ (see Section 2 of [22] and also Section 4 of [28]). The hypothesis $r^2 \mid N$ is needed for the slashing operator to preserve the space.

As explained in Ribet's article, the endomorphism η_γ is defined over the field of r-th roots of unity (because the map $\alpha_{u/r}$ is defined over such a field, as explained in nSection 4 of [28]; see also Section 6 of [29]). The following result is well known to experts, but we did not find a proper reference for its proof. Let $\mathbb{Q}(\zeta_r)$ be the field of r-th roots of unity. Identify χ with a character of $\mathrm{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q})$ and let $\overline{\mathbb{Q}}^\chi$ be the field fixed by the kernel of χ.

Lemma 2.3. *The endomorphism η_γ is defined over $\overline{\mathbb{Q}}^\chi$.*

Proof. We know that η_γ is defined at least over $\mathbb{Q}(\zeta_r)$. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q})$, say $\sigma(\zeta_r) = \zeta_r^i$. If $f \in S_2(\Gamma_1(N))$, then $\sigma(\alpha_{u/r}(f)) = \alpha_{iu/r}(\sigma(f))$ (by looking at the q-expansion). This relation implies the relation $\sigma(\alpha_{u/r}) = \alpha_{iu/r}$ as endomorphisms of A_f. Since the endomorphism $\chi(u)$ is defined over $\mathbb{Q}$,

$$\sigma(\eta_\gamma) = \sum_{u \pmod r} \chi^{-1}(u) \circ \sigma(\alpha_{u/r}) = \chi(i) \sum_{v \pmod r} \chi^{-1}(v) \circ \alpha_{v/r},$$

where the second equality comes from the change of variables $v = iu$. The result follows from the fact that $\chi(i) = 1$ if and only if σ restricted to $\overline{\mathbb{Q}}^\chi$ is the identity. ∎

It was already known to Hecke (see [9], p. 811, Satz 1 and Satz 2) that two modular forms of weight k whose first coefficients coincide (up to an explicit bound C depending on the level and the weight of the two forms) must be equal. For later purposes, we need a little variant of Hecke's result, whose elegant proof was communicated to us by Professor Gabor Wiese.

Lemma 2.4. *Let $f \in S_k(\Gamma_1(N))$ and $g \in S_k(\Gamma_1(\tilde{N}))$ be newforms. Let S be a finite set of primes. There exists a constant C depending only on N, $\tilde{N}$, k and S, such that if $a_q(f) = a_q(g)$ for all primes $q \le C$, $q \notin S$, then $f = g$.*

Proof. Let χ be a character whose conductor is divisible by all primes in S. Applying Hecke's result to $f \otimes \chi$ and $g \otimes \chi$, there exists a constant C (depending only on k, N, $\tilde{N}$ and the primes in S) such that if $a_n(f)\chi(n) = a_n(g)\chi(n)$ for all $n \le C$, then $f \otimes \chi = g \otimes \chi$. We claim that the constant C suffices for our purposes.

If $a_q(f) = a_q(g)$ for all primes $q \le C$, $q \notin S$, then (since f and g are newforms) $a_n(f) = a_n(g)$ for all positive integers $n \le C$ not divisible by primes in S, so $a_n(f)\chi(n) = a_n(g)\chi(n)$ for all $n \le C$ and $f \otimes \chi = g \otimes \chi$. Since f (respectively g) is a newform, $f = (f \otimes \chi) \otimes \chi^{-1} = (g \otimes \chi) \otimes \chi^{-1} = g$. ∎

The following result provides a partial answer to Question 1.

Theorem 2.5. *Let $g \in S_2(\Gamma_0(\tilde{N}), \varepsilon)$ be a newform without complex multiplication. There exists a constant M_g (depending only on g) such that if $f \in S_2(\Gamma_0(N), \varepsilon)$ is any newform without complex multiplication, satisfying the conditions*:

(1) *the coefficient field K_f of f equals the coefficient field K_g of g,*

(2) *$\tilde{N} \mid N$ and $N/\tilde{N}$ is square-free,*

(3) *there exists a prime $p > M_g$ and a prime ideal $\mathfrak{p}$ of K_g dividing p such that the Galois representations $\bar{\rho}_{f,\mathfrak{p}}$ and $\bar{\rho}_{g,\mathfrak{p}}$ are isomorphic,*

then, for any field extension $L/\mathbb{Q}$, there exists an injective morphism between the $\mathbb{Q}$-algebras

$$\psi : \mathrm{End}^0_L(A_f) \to \mathrm{End}^0_L(A_g).$$

Moreover, if $L/\mathbb{Q}$ is Galois, then the morphism ψ is also a morphism of $\mathrm{Gal}(L/\mathbb{Q})$-modules.

Proof. The endomorphism algebra $\mathrm{End}^0(A_f)$ is generated by K_f and by the endomorphisms η_γ for $(\gamma, \chi) \in \Gamma_f$ (the latter defined over the field $\overline{\mathbb{Q}}^\chi$ by Lemma 2.3). If we prove that the set Γ_f is contained in the set Γ_g, then the morphism ψ we seek for sends the endomorphism η_γ of A_f to the endomorphism η_γ of A_g; this morphism is clearly injective and Galois equivariant. The key point to prove the inclusion of the inner twists groups is the fact that the group Γ_f is defined in terms of a property of Fourier coefficients.

Let S be the set of primes dividing $2\tilde{N}$ and let M be the set of characters θ whose conductor is supported at primes dividing $\tilde{N}$ with the property that there exists $\gamma \in \Gamma_f$ satisfying (2.2). Lemma 2.2 implies that the set M is finite. If $\theta \in M$ and $\gamma \in \mathrm{Hom}_{\mathbb{Q}}(K_g, \mathbb{C})$, Lemma 2.4 implies the existence of a constant C_θ (depending only on $\tilde{N}$, θ and S) such that if

$$a_q(\gamma(g)) = \theta(q)\, a_q(g), \quad \forall q \le C_\theta,\ q \notin S, \tag{2.4}$$

then $\gamma(g) = g \otimes \theta$. Define the constant

$$M_g := \max_{\theta \in M} \{C_\theta^2\}.$$

Let f be a newform satisfying the stated hypotheses, so in particular there exists a prime $p > M_g$ such that the residual Galois representations $\bar{\rho}_{f,\mathfrak{p}}$ and $\bar{\rho}_{g,\mathfrak{p}}$ are isomorphic for some prime ideal $\mathfrak{p}$ of K_g dividing p. Let $(\gamma, \chi) \in \Gamma_f$, so for all primes q not dividing $2N$,

$$\gamma(a_q(f)) = \chi(q)\, a_q(f). \tag{2.5}$$

Let p be a prime dividing N but not dividing $\tilde{N}$. Since ε (the Nebentypus of f) is unramified at p, (2.2) implies that either χ is unramified at p, or it is ramified at p but its square is not. We claim that the second hypothesis implies that the latter case cannot occur.

The eigenform f has associated an automorphic representation π_f of the adelic group $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})$, where $\mathbb{A}_{\mathbb{Q}}$ denotes the adèle ring of $\mathbb{Q}$. The representation π_f factors as a restricted tensor product of components $\pi_{f,v}$ over places v of $\mathbb{Q}$. The second hypothesis

implies that if $p \mid N$ and $p \nmid \tilde{N}$, then the local component $\pi_{f,p}$ is a Steinberg representation. Then the level of the twisted modular form $f \otimes \chi$ has valuation 1 at p if χ is unramified at p, or 2 if χ is ramified at p when p is odd. When $p = 2$ and χ is ramified at 2, the valuation at 2 of the level of $f \otimes \chi$ equals 2 or 6. Since $\gamma(f)$ has the same level as f, χ must be unramified at p, proving the claim. Then $\chi \in M$, and it is enough to prove the equality

$$\gamma(a_q(g)) = \chi(q)\, a_q(g), \quad \forall q \leq \sqrt{M_g},\ q \notin S, \tag{2.6}$$

to deduce that $(\gamma, \chi) \in \Gamma_g$. Let $q \leq \sqrt{M_g}$ be a prime number not in S. There are two possibilities: either q divides N or it does not. If $q \nmid N$, Remark 2.1 implies that

$$\gamma(a_q(f)) = \chi(q)\, a_q(f).$$

The third hypothesis implies that

$$a_q(g)\chi(q) \equiv a_q(f)\,\chi(q) \pmod{\mathfrak{p}} \quad \text{and} \quad \gamma(a_q(g)) \equiv \gamma(a_q(f)) \pmod{\gamma(\mathfrak{p})}. \tag{2.7}$$

By the Ramanujan–Petersson conjecture (proved in [3]), for all embeddings $\sigma\colon K_g \to \mathbb{C}$, $|\sigma(a_q(g))| \leq 2\sqrt{q}$. Then, since

$$\mathrm{Norm}(\mathfrak{p}), \mathrm{Norm}(\gamma(\mathfrak{p})) \geq p > M_g \geq 4\sqrt{q},$$

both sides of each congruence of (2.7) are in fact equal, so (2.6) follows from (2.5).

Suppose then that $q \mid N$ but $q \nmid 2\tilde{N}$ (since $q \notin S$). Then hypotheses (2) and (3) imply that q is a prime of "level lowering" for f modulo $\mathfrak{p}$, so

$$a_q(g)^2 \equiv \varepsilon(q)\,(q+1)^2 \pmod{\mathfrak{p}}.$$

Since the absolute value of the left-hand side is bounded by $4q$, both sides of the congruence are not equal. Then p must divide their difference, which is bounded by $(\sqrt{q}+1)^2$, giving a contradiction, since $\mathrm{Norm}(\mathfrak{p}) \geq p > M_g \geq q^2 > (\sqrt{q}+1)^2$ (since q is odd). Then this last case cannot happen. ∎

3. Applications to the equations $x^4 + dy^2 = z^p$ and $x^2 + dy^6 = z^p$

3.1. Decomposing the abelian variety attached to $E_{(a,b,c)}$

Let us start this section recalling some general basic definitions (see for example the second chapter of [20]). Let A be an abelian variety of GL_2-type and let B be a simple component (over $\overline{\mathbb{Q}}$) of A.

Definition. The simple abelian variety B is a *building block* of A if it satisfies:

- the variety B is a $\mathbb{Q}$-variety, i.e., it is isogenous to all of its Galois conjugates,
- the endomorphism algebra $\mathrm{End}^0(B)$ is either a totally real field F of degree $[F : \mathbb{Q}] = \dim B$ or a totally indefinite quaternion algebra over a totally real field F of degree $[F : \mathbb{Q}] = \frac{1}{2}\dim B$.

Definition. Let L be a number field. A building block B of the variety A is *totally defined* over L if the abelian variety B is defined over L, all the isogenies between B and its Galois conjugates are defined over L and all of its endomorphisms are defined over L as well.

Let (a, b, c) be a non-trivial primitive solution of (1.1) for $d \neq 1$, and let $E_{(a,b,c)}$ be the elliptic curve over $K = \mathbb{Q}(\sqrt{-d})$ defined in (1.2).

As explained in the introduction, there exists a finite order Hecke character $\varkappa$ (whose construction is given in Section 3 of [18]) of K unramified outside 2 and primes ramifying in $K/\mathbb{Q}$ such that the twisted representation $\rho_{E_{(a,b,c)},p} \otimes \varkappa$ extends to a representation $\tilde{\rho}\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$. Let $f \in S_2(\Gamma_0(N), \varepsilon)$ be the newform attached to $\tilde{\rho}$ (see [18] for a description of the Nebentypus ε) and let A_f be the GL_2-type abelian variety constructed via the Eichler–Shimura map.

Over $\overline{\mathbb{Q}}$, the variety A_f is isogenous to a product of simple abelian varieties, $A_f \sim B_1 \times \cdots \times B_k$, each variety B_i being a building block of A_f as defined before. In the particular case of abelian varieties coming from newforms, all building blocks are isogenous to each other, so in particular $A_f \sim B^k$ (see [21]).

Lemma 3.1. *The curve $E_{(a,b,c)}$ does not have complex multiplication if $p > 2$.*

Proof. Since K is an imaginary quadratic field, if $E_{(a,b,c)}$ has complex multiplication, then its j-invariant must be a rational number (in particular, a real one).

The j-invariant of the elliptic curve $E_{(a,b,c)}$ equals

$$j = \frac{64(5a^2 - 3b\sqrt{-d})^3}{c^p(a^2 + b\sqrt{-d})}.$$

Since (a, b, c) is a non-trivial solution, a and b are non-zero, so j is a real number if and only if

$$\begin{cases} jc^p = 8000a^4 - 8640db^2, \\ jc^p = -14400a^4 + 1728db^2. \end{cases}$$

Subtracting both equations gives the relation

$$175a^4 = 81db^2,$$

hence $a^2/b = \pm\frac{9}{5}\sqrt{d/7}$. Since d is square-free, and both a, b are integers, $d = 7$ and $(a, b) = (\pm 3, \pm 5)$. Since $c^p = a^4 + db^2 = 256 = 2^8$, we get that $p = 2$ and $c = \pm 16$. ∎

Lemma 3.2. *Let $r = [K_f : \mathbb{Q}]$. Then the endomorphism algebra $\mathrm{End}^0(A_f)$ is isomorphic to $M_r(\mathbb{Q})$.*

Proof. Let $L = \overline{K}^{\varkappa}$. Then there are isomorphisms of Galois representations $\rho_{A_f,p}|_{\mathrm{Gal}_L} \simeq (\rho_{f,p}|_{\mathrm{Gal}_L})^r \simeq (\rho_{E_{(a,b,c)},p}|_{\mathrm{Gal}_L})^r$, so Faltings' isogeny theorem (see Corollary 1 in page 21 of [6]) implies that A_f is isogenous to $(E_{(a,b,c)})^r$, hence the elliptic curve $E_{(a,b,c)}$ is a building block of A_f which does not have complex multiplication. ∎

Remark 3.3. The elliptic curve $E_{(a,b,c)}$ is a building block of A_f defined over K, but it is totally defined over $K(\sqrt{-2})$.

Remark 3.4. Since the center of $\mathrm{End}^0(A_f)$ is the field of rational numbers $\mathbb{Q}$, Ribet's result (Theorem 5.1 and the remark before Proposition 3.5 of [22]) implies that the field generated by the numbers $a_p(f)^2\varepsilon(p)^{-1}$ for p not dividing the level of f is the rational one. Let us just verify that this is indeed the case (because a similar computation will be needed later).

If K is a number field, we denote by $\mathbb{I}_K$ its idèle ring. A key property of the characters $\varkappa$ and ε is that as characters of the respective idèle group, they satisfy the relation

$$\varkappa^2 = \varepsilon \circ \mathcal{N}, \tag{3.1}$$

where $\mathcal{N}\colon \mathbb{I}_K \to \mathbb{I}_{\mathbb{Q}}$ is the norm map (see [18], page 2831). Consider the following two cases:

- If the prime p splits, say $p = \mathfrak{p}_1\mathfrak{p}_2$, then relation (3.1) translates into $\varkappa(\mathfrak{p}_1)^2 = \varepsilon(p)$. Then
$$a_p(f)^2\varepsilon(p)^{-1} = \big(a_{\mathfrak{p}_1}(E)\varkappa(\mathfrak{p}_1)\big)^2\varepsilon(p)^{-1} = a_{\mathfrak{p}_1}(E)^2 \in \mathbb{Q}.$$
- If the prime p is inert, relation (3.1) implies that $\varkappa(p)^2 = \varepsilon(p^2) = \varepsilon(p)^2$. Then using the relation between $a_p(f)$ and $a_p(E)$,
$$a_p(f)^2\varepsilon(p)^{-1} = a_p(E)\varkappa(p)\varepsilon(p)^{-1} + 2p = \pm a_p(E) + 2p \in \mathbb{Q}.$$

The elliptic curve $E_{(a,b,c)}$ has discriminant $\Delta(E_{(a,b,c)}) = 512\,(a^2 + b\sqrt{-d})\,c^p$. From the equality
$$(a^2 + b\sqrt{-d}\,)(a^2 - b\sqrt{-d}\,) = a^4 + db^2 = c^p$$
and the hypothesis that (a, b, c) is a primitive solution (so any prime ideal dividing both $a^2 + b\sqrt{-d}$ and $a^2 - b\sqrt{-d}\,$) must divide 2), it follows that $(a^2 + b\sqrt{-d}\,)$ is a p-th power outside 2, and the same holds for $\Delta(E_{(a,b,c)})$. Let $q \nmid 2d$ be a prime number. If $q \mid c$ and $q \neq p$, then the curve $E_{(a,b,c)}$ has multiplicative reduction at the primes dividing q (in K), and the residual representation $\bar{\rho}_{E_{(a,b,c)},p}$ is unramified at (the primes dividing) q. Since $\varkappa$ is unramified at q (by construction), the same holds for $\overline{\rho_{E_{(a,b,c)},p} \otimes \varkappa}$. If $q = p$, then the residual representation corresponds to a finite flat group scheme (or equivalently, its Serre's weight equals 2) by a result due to Hellegouarch, and since $\varkappa$ is unramified at (primes dividing) p, the same holds for the twisted representation. Since the extension $K/\mathbb{Q}$ is unramified at primes not dividing $2d$, the residual representation of $\tilde{\rho} = \rho_f$ is also unramified at all primes q not dividing $2d$.

There is an explicit bound N_K such that the residual Galois representation $\bar{\rho}_{E_{(a,b,c)},p}$ is absolutely irreducible for all primes $p > N_K$ (see Theorem 5.1 in [18] and Proposition 3.2 in [5]). Then by Ribet's lowering the level result applied to f, there exists a newform $g \in S_2(\Gamma_0(\tilde{N}), \varepsilon)$, where $\tilde{N}$ is a positive integer only divisible by 2 and by the primes dividing d, such that $\bar{\rho}_{f,\mathfrak{p}} \simeq \bar{\rho}_{g,\mathfrak{P}}$, where $\mathfrak{p}$ and $\mathfrak{P}$ are some primes in K_f and K_g (respectively) dividing p. As explained in the introduction, it will be sufficient to consider the case when $K_f = K_g$ and $\mathfrak{p} = \mathfrak{P}$. Note in particular that the value of $\tilde{N}$ is independent of the solution (a, b, c) we started with.

Suppose that the form g does not have complex multiplication. Let A_g be the abelian variety attached to the newform g by Eichler–Shimura's construction. An immediate consequence of Theorem 2.5 is the following result.

Proposition 3.5. *Suppose that $K_f = K_g$. There exists a constant B (depending only on $\tilde{N}$) such that if $p > B$, then we have $\mathrm{End}^0(A_g) \simeq \mathrm{End}^0(A_f) \simeq M_r(\mathbb{Q})$. In particular, the building block of the abelian variety A_g has dimension* 1.

Proof. From the theory of building blocks, we know that there exists a simple abelian variety E such that $A_g \sim E^t$, hence $\mathrm{End}^0(A_g) \simeq M_t(\mathrm{End}^0(E))$. Theorem 2.5 implies that $\mathrm{End}^0(A_f) \subset \mathrm{End}^0(A_g)$ (over $\overline{\mathbb{Q}}$ under the map ψ), so $M_r(\mathbb{Q}) \subset M_t(\mathrm{End}^0(E))$, where $r = [K_f : \mathbb{Q}] = \dim(A_g) = t \dim(E)$, implying that $r \leq t$ (since $\mathrm{End}^0(E)$ does not have zero divisors). Then $r = t$ and $\dim(E) = 1$, i.e., E is an elliptic curve. Since the form g does not have complex multiplication, neither does E, hence $M_r(\mathbb{Q}) = \mathrm{End}^0(A_g)$. ∎

It is a natural problem to determine the minimal field of definition (if it exists) of a building block of A_g and whether it matches a building block of A_f (namely K).

Theorem 3.6. *There exists a* 1*-dimensional building block E_g for A_g defined over the quadratic field K and totally defined over $K(\sqrt{-2})$.*

Proof. Let E_g denote any building block of A_g (which is 1-dimensional by the last proposition). Recall that E_g is a $\mathbb{Q}$-curve, i.e., the curve E_g is totally defined over a Galois number field L satisfying that for all $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, the curve $\sigma(E_g)$ is isogenous to E_g. Let $\mu_\sigma : \sigma(E_g) \to E_g$ denote such an isogeny. Abusing notation (as in Ribet's article [22]), we can attach to E_g a map $c : \mathrm{Gal}_\mathbb{Q} \times \mathrm{Gal}_\mathbb{Q} \to \mathbb{Q}^\times$ given by

$$c(\sigma, \tau) = \mu_\sigma \circ \sigma(\mu_\tau) \circ \mu_{\sigma\tau}^{-1}, \tag{3.2}$$

which is an element of $\mathrm{End}^0(E_g) \simeq \mathbb{Q}^\times$. The map c is actually a cocycle (by (5.7) in [22]). In particular, its class is an element of $\mathrm{H}^2(\mathrm{Gal}_\mathbb{Q}, \mathbb{Q}^\times)$, whose order is at most 2 (see Remark 5.8 in [22] and Proposition 3.2 in [24]). Then, by Proposition 5.2 in [20], the building block E_g is isogenous (over $\overline{\mathbb{Q}}$) to a building block totally defined over a field F if and only if $[c]$ lies in the kernel of the restriction map $\mathrm{Res} : \mathrm{H}^2(\mathrm{Gal}_\mathbb{Q}, \mathbb{Q}^\times) \to \mathrm{H}^2(\mathrm{Gal}_F, \mathbb{Q}^\times)$.

By a result of Ribet (Corollary 4.5 in [24]), the curve E_g does have a minimum field of totally definition. Furthermore, it can be explicitly described (as done in the proof of Theorem 3.3 in [24]): consider the natural isomorphism

$$\mathbb{Q}^\times \simeq \{\pm 1\} \times \mathbb{Q}^\times / \{\pm 1\},$$

where now the second factor is a free group that can be identified with the group of positive rational numbers $\mathbb{Q}_+^\times$. This induces an isomorphism

$$\mathrm{H}^2(\mathrm{Gal}_\mathbb{Q}, \mathbb{Q}^\times)[2] \simeq \mathrm{H}^2(\mathrm{Gal}_\mathbb{Q}, \mathbb{Q}_+^\times)[2] \times \mathrm{H}^2(\mathrm{Gal}_\mathbb{Q}, \{\pm 1\}).$$

The short exact sequence

$$1 \longrightarrow \mathbb{Q}_+^\times \xrightarrow{x \mapsto x^2} \mathbb{Q}_+^\times \longrightarrow \mathbb{Q}_+^\times / (\mathbb{Q}_+^\times)^2 \longrightarrow 1$$

induces an isomorphism of the cohomology groups

$$\mathrm{H}^2(\mathrm{Gal}_\mathbb{Q}, \mathbb{Q}_+^\times)[2] \simeq \mathrm{Hom}(\mathrm{Gal}_\mathbb{Q}, \mathbb{Q}_+^\times / (\mathbb{Q}_+^\times)^2).$$

Our cocycle class $[c]$ then decomposes as a product (following Ribet's notation) $(\bar{c}, c_{\pm})$, where $\bar{c} \in \mathrm{H}^2(\mathrm{Gal}_{\mathbb{Q}}, \mathbb{Q}_+^{\times})[2]$ and $c_{\pm} \in \mathrm{H}^2(\mathrm{Gal}_{\mathbb{Q}}, \{\pm 1\})$. The minimum field of totally definition $K_{\min}$ for a building block equals the fixed field of $\bar{c}$.

There is a second way to define the cocycle $[c]$ in terms of the $\mathbb{Q}$-algebra $\mathrm{End}^0(A_g)$ (see Chapter 1 of [20]). Let K_g, as before, denote the coefficient field of g (which also equals $\mathrm{End}^0_{\mathbb{Q}}(A_g)$) and let $\psi \in \mathrm{End}^0(A_g)$. The group $\mathrm{Gal}_{\mathbb{Q}}$ acts on the set $\mathrm{End}^0(A_g)$. Let us denote by ${}^{\sigma}\psi$ the action of $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$ on an endomorphism ψ. Skolem–Noether's theorem implies the existence of an element $\alpha(\sigma) \in K_g^{\times}$ such that

$$ {}^{\sigma}\psi = \alpha(\sigma) \circ \psi \circ \alpha(\sigma)^{-1} $$

for every $\psi \in \mathrm{End}^0(A_g)$. We can then define a second cocycle

$$ c(\sigma, \tau) = \alpha(\sigma)\alpha(\tau)\alpha(\sigma\tau)^{-1}. $$

Then by Theorem 4.6 in [20], both definitions coincide. But by Proposition 3.5, the $\mathbb{Q}$-algebras $\mathrm{End}^0(A_f)$ and $\mathrm{End}^0(A_g)$ are isomorphic as $\mathrm{Gal}_{\mathbb{Q}}$-modules, hence with this second definition it is clear that the cocycle attached to A_f matches the one attached to A_g, and in particular the minimum field of totally definition of both building blocks coincide, so the building block E_g of A_g can be totally defined over the field $\mathbb{Q}(\sqrt{-d}, \sqrt{-2}) = K(\sqrt{-2})$ (see Remark 3.3). We need to prove that the elliptic curve E_g can furthermore be defined over K.

Let $\sigma_2 \in \mathrm{Gal}(\mathbb{Q}(\sqrt{-d}, \sqrt{-2})/\mathbb{Q})$ be the map given by

$$ \sigma_2(\sqrt{-d}) = -\sqrt{-d} \quad \text{and} \quad \sigma_2(\sqrt{-2}) = \sqrt{-2}. $$

Denote by $\mathbb{1}$ the identity element in such a Galois group. Since the elliptic curve $E_{(a,b,c)}$ is defined over K, we can take the isogeny $\mu_{\sigma_2} = 1$ (the identity) and $\mu_{\mathbb{1}} = 1$ (i.e., the isogeny corresponding to the identity element to be the identity map on $E_{(a,b,c)}$), the corresponding map $\widetilde{\mu_{\sigma_2}}$ on E_g satisfies that

$$ 1 = c(\sigma_2, \sigma_2) = \widetilde{\mu_{\sigma_2}} \circ \sigma_2(\widetilde{\mu_{\sigma_2}}). $$

In particular, $\widetilde{\mu_{\sigma_2}}$ has degree one, hence is an isomorphism (so E_g is isomorphic to $\sigma_2(E_g)$). Then the j-invariant of E_g lies in K, so we can take the curve E_g defined over such a field. ∎

Remark 3.7. Even when the building block E_g of A_g is defined over K, it is not true (in general) that if L/K is a field extension where the abelian variety A_g has a 1-dimensional building block E, then E is isogenous to E_g (this will become clear while proving Theorem 3.16). Here is an example (that will be explained in detail while proving such theorem): let $L = K \cdot \overline{\mathbb{Q}}^{\varepsilon}$, where $\overline{\mathbb{Q}}^{\varepsilon}$ denotes the field fixed by the kernel of ε. Then there exists an elliptic curve E defined over L (actually $E = E_{(a,b,c)} \otimes \varkappa$) such that the abelian variety A_f is isogenous over L to E^r (where $r = \dim(A_f)$). However, the building block E is not defined over K and is not isomorphic (nor isogenous) to E_g over L (although they clearly are isomorphic over $\overline{\mathbb{Q}}$).

A natural question (whose answer will be needed later) is the following:

Question 3. *Suppose that L is a number field, and suppose that an abelian variety A is isogenous over L to E^r for some building block E. When is E the base change of a variety (up to isogeny) that is defined over a smaller field K?*

Note that if E is defined over K, then the cocycle c attached to E in the proof of the last theorem is trivial while restricted to Gal_K (not just cohomologically trivial). In Theorem 8.2 of [25], Ribet proves that the converse is also true, i.e., he proves that if the cocycle c is trivial on Gal_K then there exists an abelian variety $\tilde{E}$ defined over K such that E is isogenous to $\tilde{E}$ over L.

To relate the residual Galois representation of E_g to that of our original elliptic curve $E_{(a,b,c)}$, we need some understanding on the coefficient field K_f. Let M be the order of the character $\varkappa$ and let ζ_M be a primitive M-th root of unity. Let $\mathbb{Q}(\varkappa) = \mathbb{Q}(\zeta_M)$ denote the field obtained by adding to $\mathbb{Q}$ the values of $\varkappa$.

Lemma 3.8. *Following the previous notation, we have that $\mathbb{Q}(\zeta_M) \subset K_f$.*

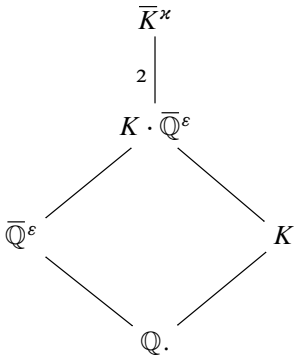
Proof. The set of prime ideals $\mathfrak{p}$ of K which are unramified in $K/\mathbb{Q}$ and with inertial degree 1 over $\mathbb{Q}$ (i.e., $f(\mathfrak{p}|p) = 1$) have density one in K, so by Chebotarev's density theorem, there exists a set S of primes with inertial degree 1 of positive density (in the set of all primes of K) such that $\varkappa(\mathfrak{p})$ is a primitive M-th root of unity for all prime ideals $\mathfrak{p} \in S$. Our assumption that the curve $E_{(a,b,c)}$ does not have complex multiplication implies that for some prime $\mathfrak{p} \in S$, the value $a_{\mathfrak{p}}(E_{(a,b,c)}) \neq 0$ (as the set of primes $\mathfrak{p}$ of good reduction where $a_{\mathfrak{p}}(E_{(a,b,c)}) = 0$ has density zero by [27], page IV-13). In particular, for such a prime (of norm p), it holds that

$$a_p(f) = \varkappa(\mathfrak{p})\, a_{\mathfrak{p}}(E_{(a,b,c)})$$

is non-zero. The result follows from the fact that $\varkappa(\mathfrak{p})$ is a primitive M-th root of unity. ∎

Let $\overline{K}^{\varkappa}$ denote the abelian extension of K fixed by the kernel of the character $\varkappa\colon \mathrm{Gal}_K \to \mathbb{C}^{\times}$, and similarly, let $\overline{\mathbb{Q}}^{\varepsilon}$ be the field fixed by the kernel of the character ε.

Lemma 3.9. *With the previous notation, $K \cdot \overline{\mathbb{Q}}^{\varepsilon} \subset \overline{K}^{\varkappa}$ with index 2. Moreover, we have the following field diagram*:



Proof. Follows from the fact that as a Galois character, $\varepsilon|_{\mathrm{Gal}_K} = \varkappa^2$. ∎

Proposition 3.10. *The coefficient field K_f is either*

(1) *the field $\mathbb{Q}(\zeta_M)$, or*

(2) *a quadratic extension of $\mathbb{Q}(\zeta_M)$.*

Moreover, $K_f = \mathbb{Q}(\zeta_M, a_p(f))$, where p is any prime inert in $K/\mathbb{Q}$ that does not divide the level of f, of ordinary reduction for $E_{(a,b,c)}$ and such that $a_p(f) \neq 0$.

Proof. By Lemma 3.8, we have $\mathbb{Q}(\zeta_M) \subseteq K_f$. Let p be a rational prime not dividing the level of f which is split in K, say $p = \mathfrak{p}\bar{\mathfrak{p}}$. Then

$$a_p(f) = a_{\mathfrak{p}}(E_{(a,b,c)})\,\varkappa(\mathfrak{p}) \in \mathbb{Q}(\zeta_M). \tag{3.3}$$

On the other hand, if p is an inert prime, we have the formula

$$a_p(f)^2 = a_p(E_{(a,b,c)})\,\varkappa(p) + 2p\varepsilon(p). \tag{3.4}$$

Recall that $\varkappa^2 = \varepsilon \circ \mathcal{N}$, so $\varkappa(p) = \pm\varepsilon(p)$. Thus $a_p(f)^2 \in \mathbb{Q}(\zeta_M)$. Formula (3.4) also implies that for a fixed inert prime p, the extension $L = \mathbb{Q}(\zeta_M)(a_p(f))$ has degree at most two over $\mathbb{Q}(\zeta_M)$, and clearly $L \subset K_f$.

Let ℓ be a rational prime, and let λ be a prime in L dividing it and let $\mathfrak{l} = \lambda \cap \mathbb{Q}(\zeta_M)$. In the usual basis, the twisted representation $\rho_{E_{(a,b,c)},\ell} \otimes \varkappa$ takes values in $\mathrm{GL}_2(\mathbb{Q}(\zeta_M)_{\mathfrak{l}})$. To extend it to a representation $\tilde{\rho}$ of $\mathrm{Gal}_{\mathbb{Q}}$, it is enough to define it on an element $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$ which is not in Gal_K, for example a Frobenius element Frob_p at a prime p inert in K.

To ease notation, let $t = a_p(f) = \mathrm{Tr}(\tilde{\rho}(\mathrm{Frob}_p))$ and $s = p\varepsilon(p) = \det(\tilde{\rho}(\mathrm{Frob}_p))$. Assume that $a_p(f) = t \neq 0$ and that p is a prime of ordinary reduction for $E_{(a,b,c)}$. The ordinary hypothesis on p implies that $t \neq 2\sqrt{s}$ (otherwise (3.4) gives that $a_p(f) = \pm 2p$, so p is not ordinary for $E_{(a,b,c)}$). The matrices $\rho_{E_{(a,b,c)},\ell}(\mathrm{Frob}_p^2)\,\varkappa(\mathrm{Frob}_p^2)$ and $\left(\begin{smallmatrix} -s & -st \\ t & t^2 - s \end{smallmatrix}\right)$ are diagonalizable, have the same trace and the same determinant, hence there exists a matrix $W \in \mathrm{GL}_2(L_\lambda)$ such that

$$W(\rho_{E_{(a,b,c)},\ell}(\mathrm{Frob}_p^2)\,\varkappa(\mathrm{Frob}_p^2))\,W^{-1} = \begin{pmatrix} -s & -st \\ t & t^2 - s \end{pmatrix}.$$

Conjugating the representation $\rho_{E_{(a,b,c)},\ell} \otimes \varkappa$ by W, we can assume, without loss of generality, that this twisted representation takes values in $\mathrm{GL}_2(L_\lambda)$ and that

$$\rho_{E_{(a,b,c)},\ell}(\mathrm{Frob}_p^2)\,\varkappa(\mathrm{Frob}_p^2) = \begin{pmatrix} -s & -st \\ t & t^2 - s \end{pmatrix}. \tag{3.5}$$

We claim that then (since $t = a_p(f) \neq 0$),

$$\tilde{\rho}(\mathrm{Frob}_p) = \begin{pmatrix} 0 & -s \\ 1 & t \end{pmatrix}.$$

The reason is that if A is any 2×2 matrix with different eigenvalues, and B is another 2×2 matrix satisfying that

$$A^2 = B^2, \quad \mathrm{Tr}(A) = \mathrm{Tr}(B) \neq 0,$$

then $A = B$ (which follows from an elementary computation, assuming that A is diagonal). This implies that the representation $\tilde{\rho}$ can be chosen to take values in $\mathrm{GL}_2(L_\lambda)$. In particular, for any prime q not dividing the level of f, $\mathrm{Tr}(\tilde{\rho}(\mathrm{Frob}_q)) = a_q(f) \in L_\lambda$ for all

primes $\lambda \in L$, hence $a_q(f) \in L$ (by Lemma 3.12), and the same is true for primes dividing the level of f (by Chebotarev's density theorem). Since K_f is the smallest field containing $a_q(f)$, we conclude that $K_f \subset L$. ∎

Remark 3.11. The first case of the last result can occur. For example, let E be a rational elliptic curve attached to a rational modular form f, and let $\varkappa$ be any quadratic character of K which does not come from $\mathbb{Q}$. Let $\tilde{E} := E \otimes \varkappa$ be the twist of E by $\varkappa$. Then the coefficient field of $\tilde{E}$ equals $K_f = \mathbb{Q}$, which is the trivial extension of $\mathbb{Q}(\zeta_2) = \mathbb{Q}$.

Lemma 3.12. *Let $\alpha \in \overline{\mathbb{Q}}$ and let L be a number field. Suppose that for all prime ideals $\mathfrak{p}$ of L, $\alpha \in L_{\mathfrak{p}}$. Then $\alpha \in L$.*

Proof. Suppose that $\alpha \notin L$, so $L(\alpha)/L$ is a non trivial extension. Let $\mathfrak{p}$ be a prime ideal of L and let $\mathfrak{q}$ be a prime ideal of $L(\alpha)$ dividing $\mathfrak{p}$ satisfying that the inertial degree $f(\mathfrak{q} \mid \mathfrak{p})$ is not 1 (such an ideal always exists by applying Chebotarev's density theorem to the Galois closure of $L(\alpha)$ over L). Then $\alpha \notin L_{\mathfrak{p}}$, contradicting the hypothesis. ∎

An important fact of the character $\varkappa$ (and also of ε) is that by construction it has order a power of two (although this is not explicitly stated in [18], it follows from its construction given in the proof of Theorem 3.2 in loc. cit).

Lemma 3.13. *Suppose that $\mathbb{Q}(\zeta_M) \subsetneq K_f$. Then the extension $K_f/\mathbb{Q}$ is an abelian Galois extension. Furthermore, the field K_f is the compositum of a quadratic extension of $\mathbb{Q}$ with $\mathbb{Q}(\zeta_M)$.*

Proof. As proved in the last proposition, the quadratic extension $K_f/\mathbb{Q}(\zeta_M)$ is obtained by adding the coefficient $a_p(f)$ for p a prime that is inert in K and of ordinary reduction for $E_{(a,b,c)}$ satisfying that $a_p(f) \neq 0$. Recall that if p is an inert prime, then $\varkappa^2(p) = \varepsilon(p^2)$, so $\varkappa(p) = \pm\varepsilon(p)$. Replacing this equality in (3.4), we get that

$$a_p(f)^2 = \varepsilon(p)(\pm a_p(E_{(a,b,c)}) + 2p). \tag{3.6}$$

Keeping the previous notation, let M be the order of $\varkappa$ (a power of 2). The order of ε equals the degree of the extension $[\overline{\mathbb{Q}}^{\varepsilon} : \mathbb{Q}]$. Since the character ε is even (as proven in Section 3.1 of [18]), its fixed field is a totally real number field, so $\overline{\mathbb{Q}}^{\varepsilon} \cap K = \mathbb{Q}$. In particular, $[\overline{\mathbb{Q}}^{\varepsilon} : \mathbb{Q}] = [K \cdot \overline{\mathbb{Q}}^{\varepsilon} : K] = M/2$ by Lemma 3.9. Then $\varepsilon(p)$ is a root of unity of order a divisor of $M/2$, hence a square in $\mathbb{Q}(\zeta_M)$, so $K_f = \mathbb{Q}(\zeta_M)[\sqrt{(\pm a_p(E_{(a,b,c)}) + 2p}]$ as claimed. ∎

The last lemma implies that if $\mathbb{Q}(\zeta_M) \subsetneq K_f$, then the Galois group $\mathrm{Gal}(K_f/\mathbb{Q})$ is isomorphic to $\mathbb{Z}/2 \times (\mathbb{Z}/M)^{\times}$. It turns out that (in our situation) each element of such a Galois group gives an inner twists.

Theorem 3.14. *Let M be the order of the character $\varkappa$ and let δ_K denote the quadratic Dirichlet character corresponding to the extension $K/\mathbb{Q}$. Write $K_f = \mathbb{Q}(\zeta_M) \cdot F$, where $F/\mathbb{Q}$ is at most a quadratic extension, as in the previous lemma. Let $j \in (\mathbb{Z}/M)^{\times}$ and let $\sigma_j \in \mathrm{Gal}(\mathbb{Q}(\zeta_M)/\mathbb{Q})$ be the map given by $\sigma_j(\zeta_M) = \zeta_M^j$. Then all inner twists of A_f are the following*:

- *if σ_j acts trivially on F, then $(\sigma_j, \varepsilon^{(j-1)/2})$ is an inner twist*;
- *if σ_j does not act trivially on F, then $(\sigma_j, \delta_K\varepsilon^{(j-1)/2})$ is an inner twist.*

Proof. Let p be a rational prime not dividing the level of f. If p splits in $K/\mathbb{Q}$, let $\mathfrak{p}$ a prime ideal of K dividing p. Then $a_p(f) = \varkappa(\mathfrak{p})a_{\mathfrak{p}}(E_{(a,b,c)})$, so

$$\sigma_j(a_p(f)) = \varkappa^j(\mathfrak{p})a_{\mathfrak{p}}(E_{(a,b,c)}) = \varkappa^{j-1}(\mathfrak{p})(\varkappa(\mathfrak{p})a_{\mathfrak{p}}(E_{(a,b,c)})) = \varepsilon^{(j-1)/2}(p)a_p(f), \tag{3.7}$$

where the last equality comes from the fact that $\varkappa^{(j-1)}(\mathfrak{p}) = (\varkappa^2(\mathfrak{p}))^{(j-1)/2}$, because j is odd (recall that M is a power of 2). On the other hand, if p is inert in K, it is enough to study the case when $a_p(f) \neq 0$. By (3.6), we have

$$a_p(f)^2 = \varepsilon(p)(\pm a_p(E_{(a,b,c)}) + 2p).$$

To ease notation, let $\eta = \pm a_p(E_{(a,b,c)}) + 2p$. Note that $\varepsilon(p) = \zeta_M^{2r}$ for some r (see the proof of the last lemma), so $a_p(f) = \zeta_M^r\sqrt{\eta}$ (for the right choice of the square root). Applying σ_j to it we get

$$\sigma_j(a_p(f)) = \zeta_M^{jr}\sigma_j(\sqrt{\eta}) = a_p(f)\zeta_M^{(j-1)r}\frac{\sigma_j(\sqrt{\eta})}{\sqrt{\eta}} = a_p(f)\varepsilon(p)^{(j-1)/2}\frac{\sigma_j(\sqrt{\eta})}{\sqrt{\eta}}. \tag{3.8}$$

If $\sigma_j(\sqrt{\eta}) = \sqrt{\eta}$ (i.e., if σ_j acts trivially on F), then equations (3.7) and (3.8) imply that $(\sigma_j, \varepsilon^{(j-1)/2})$ is an inner twist, while if $\sigma_j(\sqrt{\eta}) = -\sqrt{\eta}$ (i.e., if σ_j does not act trivially on F), then both equations imply that $(\sigma_j, \delta_K\varepsilon^{(j-1)/2})$ is an inner twist. ∎

As an immediate application, using Lemma 2.3, we get the following result.

Corollary 3.15. *All the endomorphisms of A_f are defined over the field $K \cdot \overline{\mathbb{Q}}^{\varepsilon}$.*

Let M_g be the constant coming from Theorem 2.5.

Theorem 3.16. *In the previous notation, and under the assumption that $K_f = K_g$ and that $p > M_g$, there exists a building block E_g defined over the quadratic field K such that*

$$\bar{\rho}_{E_{(a,b,c)},p} \simeq \bar{\rho}_{E_g,p}.$$

Proof. Since all endomorphisms of A_f are defined over $L := K \cdot \overline{\mathbb{Q}}^{\varepsilon}$ (by Corollary 3.15), Theorem 2.5 jointly with Proposition 3.5 implies that $\mathrm{End}_L^0(A_g) \simeq M_r(\mathbb{Q})$, where $r = \dim(A_f) = \dim(A_g)$. Then, over L, both varieties are isogenous to r-copies of an elliptic curve. Let us explain in more detail the situation for A_f. The extension L/K is an abelian extension of order $M/2$, a power of 2. Over $\overline{\mathbb{Q}}$, $E_{(a,b,c)}$ is a building block of A_f, but it is not a factor of its splitting over L as we now explain. By Eichler–Shimura's construction,

$$\rho_{A_f,p} \simeq \bigoplus_{\sigma \in \mathrm{Gal}(K_f/\mathbb{Q})} \rho_{\sigma(f),\mathfrak{p}},$$

hence a similar decomposition holds while restricted to Gal_K. For σ the identity, we have that $\rho_{f,\mathfrak{p}}|_{\mathrm{Gal}_K} \simeq \rho_{E_{(a,b,c)}} \otimes \varkappa$, hence for any $\sigma \in \mathrm{Gal}(K_f/\mathbb{Q})$, we get

$$\rho_{\sigma(f),\mathfrak{p}} \simeq \rho_{E_{(a,b,c)},\mathfrak{p}} \otimes \sigma(\varkappa).$$

Recall that $\varkappa$ has order M and $\zeta_M \in K_f$, hence while σ ranges over all elements of $\mathrm{Gal}(K_f/\mathbb{Q})$, $\sigma(\varkappa)$ ranges over all conjugates of $\varkappa$, which equals all its odd powers.

Let M' be the order of $\mathrm{Gal}(K_f/\mathbb{Q})$. By Proposition 3.10, M' equals M or $M/2$, depending on whether K_f is a quadratic extension of $\mathbb{Q}(\zeta_M)$ or not. Then we get the following decomposition:

$$\rho_{A_f,p}|_{\mathrm{Gal}_K} \simeq \Big(\bigoplus_{i=1}^{M/2} \rho_{E_{(a,b,c)},p} \otimes \varkappa^{2i-1}\Big)^{2M'/M}. \tag{3.9}$$

The key point is that $\varkappa$ restricted to Gal_L is a quadratic character (by Lemma 3.9), so while restricted to Gal_L, the representation is isomorphic to r-copies of $\rho_{E_{(a,b,c)},p} \otimes \varkappa$. In particular, the variety A_f over L is isogenous to $(E_{(a,b,c)} \otimes \varkappa)^r$. The problem is that the elliptic curve $E_{(a,b,c)} \otimes \varkappa$ is not defined over K. For that purpose, we look at the variety A_f over $\overline{K}^{\varkappa}$, and it is true that over such a field, A_f is isogenous to $(E_{(a,b,c)})^r$ (the base change of a curve defined over K). In particular, the cocycle c attached to $E_{(a,b,c)}$ (in the proof of Theorem 3.6) over $\overline{K}^{\varkappa}$ is trivial while restricted to Gal_K.

By Theorem 3.6 (and Remark 3.7), there exists a building block E_g of A_g defined over K such that A_g is isogenous (over $\overline{K}^{\varkappa}$) to E_g^r. In particular, the semisimplification of the residual Galois representations $\bar{\rho}_{E_{(a,b,c)},p}$ and $\bar{\rho}_{E_g,p}$ are isomorphic while restricted to $\mathrm{Gal}_{\overline{K}^{\varkappa}}$.

The extension $\overline{K}^{\varkappa}/K$ is abelian, and the characters of $\mathrm{Gal}(\overline{K}^{\varkappa}/K)$ are precisely powers of $\varkappa$. Since E_g is defined over K, we have that

$$\mathrm{Ind}_{\mathrm{Gal}_{\overline{K}^{\varkappa}}}^{\mathrm{Gal}_K}(\rho_{E_g,p}|_{\mathrm{Gal}_{\overline{K}^{\varkappa}}}) \simeq \bigoplus_{i=1}^{M} \rho_{E_g,p} \otimes \varkappa^i. \tag{3.10}$$

Since the curve $E_{(a,b,c)}$ is also defined over K, a similar splitting holds for

$$\mathrm{Ind}_{\mathrm{Gal}_{\overline{K}^{\varkappa}}}^{\mathrm{Gal}_K}(\rho_{E_{(a,b,c)},p}|_{\mathrm{Gal}_{\overline{K}^{\varkappa}}}).$$

Then

$$\bigoplus_{i=1}^{M} \bar{\rho}_{E_g,p} \otimes \bar{\varkappa}^i \simeq \bigoplus_{i=1}^{M} \bar{\rho}_{E_{(a,b,c)},p} \otimes \bar{\varkappa}^i.$$

Note that since $\bar{\rho}_{E_{(a,b,c)},p}$ is absolutely irreducible, the same must hold for $\bar{\rho}_{E_g,p}$. In particular, $\bar{\rho}_{E_{(a,b,c)},p}$ must be a summand of the left-hand side, i.e.,

$$\bar{\rho}_{E_{(a,b,c)},p} \simeq \bar{\rho}_{E_g,p} \otimes \bar{\varkappa}^i,$$

for some exponent i. Taking determinants on both sides, it follows that either $\bar{\varkappa}^i = 1$, or $\bar{\varkappa}^i$ is a quadratic character. Note that since p is odd, and $\varkappa$ has order a power of two, $\varkappa$ and $\bar{\varkappa}$ have the same order, so either $\varkappa^i$ is trivial, or it is a quadratic character. If $\varkappa^i = 1$ then the result follows, while if $\varkappa^i \neq 1$, then the elliptic curve $E_g \otimes \varkappa^i$ is another building block defined over K satisfying the required property. ∎

3.2. The Diophantine equation $x^4 + dy^2 = z^p$

Let us start with a general result on non-existence of elliptic curves over quadratic fields with a 2-torsion point.

Theorem 3.17. *Let d be a positive integer larger than 3 such that the field $K = \mathbb{Q}(\sqrt{-d})$ satisfies the following properties*:

- *the prime 2 is inert in $K/\mathbb{Q}$ (i.e., $d \equiv 3 \pmod 8$),*
- *the class number of K is prime to 6.*

Then the only elliptic curves defined over $K = \mathbb{Q}(\sqrt{-d})$ having a K-rational point of order 2 and conductor supported at the prime ideal 2 are those that are base change of $\mathbb{Q}$.

Proof. Let E/K be an elliptic curve satisfying the hypotheses. Since K does not have (in general) trivial class group, there is no reason for the curve E to have a global minimal model. However, it always has what is called a "semi-global" minimal model, i.e., a model which is minimal at all primes dividing the conductor of the curve, but is not minimal at most one extra prime $\mathfrak{p}$ (which we assume is odd), and the discriminant valuation at $\mathfrak{p}$ equals 12 (see Exercise 8.14 in [32]). Our assumption that E has only bad reduction at the prime ideal (2) implies that $\Delta(E) = 2^r\mathfrak{p}^{12}$. In particular, $\mathfrak{p}^{12}$ is a principal ideal. Our assumption that the class number of K is prime to 6 then implies that $\mathfrak{p}$ is principal, hence E does have a global minimal model.

Take a global minimal model for the curve E. Doing the usual change of variables $y \to y - (a_1x + a_3)/2$ and clearing denominators, we can assume that our curve E is given by a model (which might not be minimal at 2 but is minimal at all other prime ideals) with $a_1 = a_3 = 0$. Furthermore, we can assume (after a translation, which preserves minimality of the model at all odd primes) that our 2-torsion point corresponds to the point $(0, 0)$. Then the curve E is given by an equation of the form

$$E : y^2 = x^3 + ax^2 + bx,$$

where $a, b \in \mathbb{Z}[\frac{1+\sqrt{-d}}{2}]$. Minimality at all odd primes implies in particular that its discriminant $\Delta(E) = 2^4b^2(a^2 - 4b)$ is a power of the prime ideal (2), i.e., $\Delta(E) = (2)^r$, for some $r \geq 0$. The hypothesis $K \neq \mathbb{Q}(\sqrt{-3})$ implies that the only roots of unity in K are ± 1. Then

$$b^2(a^2 - 4b) = \pm 2^{r-4}. \tag{3.11}$$

Since K is a Dedekind domain, it has unique factorization in prime ideals, so in particular

$$b = \pm 2^t,$$

for some $t \geq 0$, and in particular, $b \in \mathbb{Z}$; since $\Delta(E)$ is an algebraic integer, $2t + 4 \leq r$. Substituting in (3.11), we get that

$$a^2 = \pm 2^{r-4-2t} \pm 2^{t+2} \in \mathbb{Z}. \tag{3.12}$$

Suppose that $a = (a_1 + a_2\sqrt{-d})/2$, with $a_1, a_2 \in \mathbb{Z}$ (and $a_1 \equiv a_2 \pmod 2$). Since a^2 is a rational number, $a_1a_2 = 0$. If $a_2 = 0$ then both a and b are rational numbers, and hence E is a rational elliptic curve as claimed.

Suppose then that $a_2 \neq 0$ and $a_1 = 0$, i.e., $a = a_2\sqrt{-d}$ for some integer a_2. Write a_2 in the form

$$a_2 = 2^s\tilde{a},$$

where $s \geq 0$ and $2 \nmid \tilde{a}$. Substituting in (3.12), we obtain the equation

$$-d\tilde{a}^2 = \pm 2^{r-4-2t-2s} \pm 2^{t+2-2s},$$

where the exponents are non-negative integers and at least one of them must be zero (as the left-hand side is odd). The left-hand side is a negative integer which is congruent to 5 mod 8. All solutions of the equation $\pm 1 \pm 2^m \equiv 5 \pmod 8$ are

$$\begin{cases} 1 \pm 2^2 \equiv 5 \pmod 8, \\ -1 - 2 \equiv 5 \pmod 8. \end{cases}$$

Note that in both cases, the non-zero exponent is at most 2, so d is at most 3, which contradicts our assumption $d > 3$. ∎

Remark 3.18. The result is not true over $\mathbb{Q}(\sqrt{-3})$, since for example the curve 2.0.3.1-4096.1-a1 has conductor 2^6, a 2-torsion point, but is not defined over the rationals (nor is isogenous to a rational elliptic curve). It is, however, a $\mathbb{Q}$-curve.

Remark 3.19. The last result is similar to Theorem 1 in [7], in the case $\ell = 2$, although in such an article the authors impose to the curve the condition that it has multiplicative reduction at ℓ (while our curve has additive reduction). In particular the condition on the class group being odd is the natural one (which matches theirs). The method of proof is completely different though.

Remark 3.20. The hypothesis on the class group being odd is equivalent to d being a prime number (under the assumption $d \equiv 3 \pmod 8$). This was already discovered by Gauss (see for example Section 6 of [2]). The Cohen–Lenstra heuristics (see (C2) in [1] and also page 58 of loc. cit.) imply that the number of imaginary quadratic fields of prime discriminant, where 2 is inert, and whose class group is not divisible by 3, should have density 56.013% (so there should be many of them).

Lemma 3.21. *Let E_1 and E_2 be two elliptic curves over a number field K. Let $\mathfrak{q}$ be a prime of K of good reduction for E_1. Let $p > \max\{\mathcal{N}(\mathfrak{q}) + 1 + 2\sqrt{\mathcal{N}(\mathfrak{q})}, 4\,\mathcal{N}(\mathfrak{q})\}$ be a prime number such that $\bar{\rho}_{E_1,p} \simeq \bar{\rho}_{E_2,p}$. Then E_2 also has good reduction at $\mathfrak{q}$ and $a_{\mathfrak{q}}(E_1) = a_{\mathfrak{q}}(E_2)$.*

Proof. The proof is similar to that of Theorem 1.4 in [8]. Since $p > 3$, the curve E_2 must have either good or multiplicative reduction at $\mathfrak{q}$ (by Remark 7 in [8]). The reason is that if E_2 has additive reduction, then its local type is either: a principal series, a ramified quadratic twist of an elliptic curve with multiplicative reduction or supercuspidal. A ramified quadratic character reduces modulo an odd prime to a ramified quadratic character, so the second case cannot occur. Since the coefficient field of an elliptic curve is the rational one, any character (in both the principal series or the supercuspidal type) appearing at a prime of bad reduction has order n with $\phi(n) \leq 2$ (where $\phi(n)$ denotes Euler's totient function), so $n \in \{1, 2, 3, 4, 6\}$. Then for $p > 3$, the local type of ρ is preserved by congruences.

If the reduction is multiplicative, we are in a "lower the level" case, hence

$$a_{\mathfrak{q}}(E_1) \equiv \pm(\mathcal{N}(\mathfrak{q}) + 1) \pmod p. \tag{3.13}$$

But Hasse's bound implies that $\left|a_{\mathfrak{q}}(E_1)\right| \leq 2\sqrt{\mathcal{N}(\mathfrak{q})}$. Since the difference of the right and the left-hand side of (3.13) is non-zero, then p must be smaller than their difference, which contradicts the hypothesis $p > 1 + 2\sqrt{\mathcal{N}(\mathfrak{q})} + \mathcal{N}(\mathfrak{q})$.

Once we know that both curves have good reduction at $\mathfrak{q}$, we get the congruence

$$a_{\mathfrak{q}}(E_1) \equiv a_{\mathfrak{q}}(E_2) \pmod{p}.$$

If both numbers are different, p must divide their difference, which by Hasse's bound is at most $4\,\mathcal{N}(\mathfrak{q})$, giving the result. ∎

Lemma 3.22. *Let (a, b, c) a primitive solution of (1.1), where p is large enough so that $\bar{\rho}_{E_{(a,b,c)},p}$ is absolutely irreducible and let q an odd prime. There exists a bound B (depending only on d and on q) such that if $p > B$, then $q \nmid c$.*

Proof. If $q \mid c$, then the curve $E_{(a,b,c)}$ has multiplicative reduction at q, but it does not divide the conductor of the residual representation $\bar{\rho}_{E_{(a,b,c)},p}$. In particular, the form f has level divisible by q, but the form g does not, i.e., we are in what is called the "lower the level case". In particular,

$$p \mid \mathcal{N}(\varepsilon^{-1}(q)(q+1)^2 - a_q(g)^2). \tag{3.14}$$

Note that ε depends only on d and there are finitely many possibilities for the value $a_q(g)$ (since the form g is a newform in the space $S_2(\Gamma_0(\tilde{N}), \varepsilon)$, which does not depend on (a, b, c)), so it is enough to prove that the right-hand side of (3.14) is non-zero for any newform g. But by the Ramanujan–Petersson conjecture, $|a_q(g)|^2 \leq 4q < (q+1)^2$, so the difference cannot be zero. ∎

Theorem 3.23. *Let d be a prime number congruent to 3 modulo 8 and such that the class number of $K = \mathbb{Q}(\sqrt{-d})$ is not divisible by 3. Then there are no non-trivial primitive solutions of the equation*

$$x^4 + dy^2 = z^p,$$

for p large enough.

Proof. The case $d = 3$ was proven in [4], so we can restrict to values $d > 3$. Let (a, b, c) be a non-trivial primitive solution and consider the elliptic curve $E_{(a,b,c)}$ as in (1.2). The assumption (a, b, c) being non-trivial and primitive implies that $E_{(a,b,c)}$ does not have complex multiplication (by Lemma 3.1).

The discriminant of $E_{(a,b,c)}$ equals $512(a^2 + b\sqrt{-d})c^p$, which is a perfect p-power except at the prime 2. Furthermore, all odd primes dividing the conductor of $E_{(a,b,c)}$ are of multiplicative reduction, so the residual representation $\bar{\rho}_{E_{(a,b,c)},p}$ is unramified outside 2.

Recall that there exists a Hecke character $\varkappa$ and a newform $f \in S_2(\Gamma_0(N), \varepsilon)$ (where N depends on (a, b, c), but the conductor of ε is supported only at primes dividing $2d$) such that the twisted representation $\rho_{E_{(a,b,c)},p} \otimes \varkappa$ extends to $\rho_{f,\mathfrak{p}}$.

Note that if (a, b, c) is a non-trivial solution of (1.1), clearly $c \neq 1$. Looking at (1.1) modulo 8, it follows that c is not divisible by 2, and by Lemma 3.22, we can assume that c is not divisible by 3. Then there exists a prime number q larger than 3 such that c is divisible by q. In particular, the curve $E_{(a,b,c)}$ has a prime of multiplicative reduction not

dividing 6. Ellenberg's large image result (Theorem 3.14 in [5]) implies that there exists a bound B (depending only on K) such that if $p > B$, then the projective residual image of $\rho_{E_{(a,b,c)},p}$ is surjective.

In particular, for such primes p we are in the hypothesis of Ribet's lowering the level result, so there exists a newform $g \in S_2(\Gamma_0(\tilde{N}), \varepsilon)$ such that the residual representation of $\rho_{g,\mathfrak{p}}$ is isomorphic to that of $\tilde{\rho}$, where $\tilde{N}$ is only divisible by primes dividing $2d$. The surjectivity of the residual representation of $\rho_{E_{(a,b,c)},p}$ implies that the form g cannot have complex multiplication either (which justifies such an hypothesis made in the present article), so we can apply our previous results.

Let g be any newform in the space $S_2(\Gamma_0(\tilde{N}), \varepsilon)$ without complex multiplication and suppose that it is related to a solution (a, b, c) of (1.1). Let g^{BC} denote its base change to K. Let ℓ be a prime not dividing $2d$ and define

$$S_\ell = \{(\tilde{a}, \tilde{b}, \tilde{c}) \in \mathbb{F}_\ell^3 \setminus \{(0,0,0)\} : \tilde{a}^4 + d\tilde{b}^2 = \tilde{c}^p\}.$$

In practice, since p will be a larger prime (compared to ℓ), raising to the p-th power is a bijection of $\mathbb{F}_\ell$. For each point $(\tilde{a}, \tilde{b}, \tilde{c}) \in S_\ell$, consider the curve $E_{(\tilde{a},\tilde{b},\tilde{c})}$ over $\mathbb{F}_\ell$. Let $\mathfrak{l}$ be a prime of K dividing ℓ. Then,

(1) either the curve $E_{(\tilde{a},\tilde{b},\tilde{c})}$ is non-singular, in which case if (a, b, c) is an integral solution reducing to $(\tilde{a}, \tilde{b}, \tilde{c})$, we must have that $a_{\mathfrak{l}}(E_{(a,b,c)}) = a_{\mathfrak{l}}(E_{(\tilde{a},\tilde{b},\tilde{c})})$ and furthermore
$$\varkappa(\mathfrak{l}) a_{\mathfrak{l}}(E_{(\tilde{a},\tilde{b},\tilde{c})}) \equiv a_{\mathfrak{l}}(g^{\mathrm{BC}}) \pmod{p},$$

(2) or the curve $E_{(a,b,c)}$ has bad reduction at $\mathfrak{l}$, in which case we are in the lowering the level hypothesis, and
$$a_\ell(g) \equiv \pm \varkappa^{-1}(\mathfrak{l})(\ell + 1) \pmod{p}.$$

Given $(\tilde{a}, \tilde{b}, \tilde{c}) \in S_\ell$, let $B(\ell, g; \tilde{a}, \tilde{b}, \tilde{c})$ be given by

$$B(\ell, g; \tilde{a}, \tilde{b}, \tilde{c}) = \begin{cases} \mathcal{N}(a_{\mathfrak{l}}(E_{(a,b,c)})\varkappa(\mathfrak{l}) - a_\ell(g)) & \text{if } \ell \nmid \tilde{c} \text{ and } \ell \text{ splits in } K, \\ \mathcal{N}(a_\ell(g)^2 - a_\ell(E_{(a,b,c)})\varkappa(\ell) - 2\ell\varepsilon(\ell)) & \text{if } \ell \nmid \tilde{c} \text{ and } \ell \text{ is inert in } K, \\ \mathcal{N}(\varepsilon^{-1}(\ell)(\ell+1)^2 - a_\ell(g)^2) & \text{if } \ell \mid \tilde{c}. \end{cases}$$

If $(\tilde{a}, \tilde{b}, \tilde{c})$ belongs to case (2), then clearly $p \mid B(\ell, g; \tilde{a}, \tilde{b}, \tilde{c})$ (since $\varkappa(\mathfrak{l})^2 = \varepsilon(\ell)$). If $(\tilde{a}, \tilde{b}, \tilde{c})$ belongs to case (1), the well-known formula for the Fourier coefficients of g^{BC} in terms of those of g implies that

$$\begin{cases} \varkappa(\mathfrak{l})\, a_{\mathfrak{l}}(E_{(\tilde{a},\tilde{b},\tilde{c})}) \equiv a_\ell(g) \pmod{p} & \text{if } \ell \text{ splits}, \\ \varkappa(\mathfrak{l})\, a_{\mathfrak{l}}(E_{(\tilde{a},\tilde{b},\tilde{c})}) \equiv a_\ell(g)^2 - 2\ell\varepsilon(\ell) \pmod{p} & \text{if } \ell \text{ is inert}. \end{cases}$$

In all cases, it holds that

$$p \mid \prod_{(\tilde{a},\tilde{b},\tilde{c}) \in S_\ell} B(\ell, g; \tilde{a}, \tilde{b}, \tilde{c}). \tag{3.15}$$

As previously explained, the Ramanujan–Petersson conjecture implies that the third row value in the definition of $B(\ell, g; \tilde{a}, \tilde{b}, \tilde{c})$ is never zero. If the coefficient field K_g does

not match the coefficient field K_f, then there exists some prime ℓ for which the first or the second row (depending on whether ℓ is split or inert) is non-zero, so the right-hand side of (3.15) is non-zero, giving finitely many possibilities for the value of the prime p (this is an idea of Mazur). Then to finish the proof we are left to discard the newforms g whose coefficient field K_g matches the coefficient field K_f of f.

By Theorem 3.16, if p is large enough, there exists an elliptic curve E_g, defined over K, whose conductor divides $\tilde{N}$ such that $\bar{\rho}_{E_g,p} \simeq \bar{\rho}_{E_{(a,b,c)},p}$. A priori, the curve E_g has bad reduction at primes dividing $\tilde{N}$ (i.e., at primes dividing $2d$), but the curve $E_{(a,b,c)}$ has good reduction at all odd primes dividing d, so in particular the same must be true for the curve E_g if $p > 3$ (see Proposition 1.1 in [8] and also Remark 7).

The residual representation $\bar{\rho}_{E_g,2}$ has image lying in S_3. Under the isomorphism $\mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$, the elements of order 1 or 2 are precisely the ones of trace 0, while the ones of order 3 have trace 1. In particular, the image of the residual representation (is isomorphic to one that) lies in the Borel subgroup (i.e., the curve E_g has a K-rational point of order 2) if and only if the trace of any Frobenius element is even if and only if the image does not have elements of order 3. Let T denote the fixed field of the kernel of $\bar{\rho}_{E_g,2}$, so the extension T/K is unramified outside 2 (by the Nerón–Ogg–Shafarevich criterion) and is of degree at most 6. A well-known result of Hermite and Minkowski states that there are finitely many field extensions of a given degree and bounded discriminant. In particular, our field T is one of a finite list, say $\{T_1, \ldots, T_n\}$, of at most degree 6 extensions of K unramified outside $\{2\}$. Suppose that $[T_i : K]$ is divisible by 3 for some index i. Then an explicit version of Chebotarev's density theorem (see for example [34] and the references therein) proves the existence of a bound B and a prime $\mathfrak{q} \in \mathcal{O}_K$ (the ring of integers of K) of norm at most B such that $\mathrm{Frob}_{\mathfrak{q}}$ has order 3 in $\mathrm{Gal}(T_i/K)$. In particular, if $[T : K]$ is divisible by 3, there exists a prime whose norm is bounded by B (independently of the original solution (a, b, c)) such that

$$a_{\mathfrak{q}}(E_g) = \mathrm{Tr}(\rho_{E_g,2}(\mathrm{Frob}_{\mathfrak{q}})) \equiv 1 \pmod 2.$$

But Lemma 3.21 implies that if p is large enough (where the bound depends on the norm of the prime $\mathfrak{q}$, which is bounded by B), then $E_{(a,b,c)}$ has good reduction at $\mathfrak{q}$ and furthermore $a_{\mathfrak{q}}(E_g) = a_{\mathfrak{q}}(E_{(a,b,c)})$. Recall that $E_{(a,b,c)}$ has a 2-torsion point, so $a_{\mathfrak{q}}(E_{(a,b,c)})$ is even, giving a contradiction. Then T/K has degree 1 or 2 and the residual representation $\bar{\rho}_{E_g,2}$ has image in a Borel subgroup, so the curve E_g also has a K-rational 2-torsion point.

Theorem 3.17 then implies that the elliptic curve E_g is in fact defined over $\mathbb{Q}$. In particular, if q is a prime integer that splits in K as $(q) = \mathfrak{q}\bar{\mathfrak{q}}$, then

$$a_{\mathfrak{q}}(E_g) = a_{\bar{\mathfrak{q}}}(E_g).$$

However, the curve $E_{(a,b,c)}$ satisfies the property (proved in Proposition 2.2 of [18])

$$a_{\mathfrak{q}}(E_{(a,b,c)}) = \left(\frac{-2}{q}\right) a_{\bar{\mathfrak{q}}}(E_{(a,b,c)}).$$

Recall that by Ellenberg's result (Theorem 3.14 in [5]), we are assuming that the projective residual image of $\rho_{E_{(a,b,c)},p}$ equals $\mathrm{PGL}_2(\mathbb{F}_p)$. Its fixed field is an extension of K disjoint from $K(\sqrt{-2})$ if q is odd. Then by Chebotarev's theorem, there exists a prime ideal $\mathfrak{q}$ of K

of prime norm q of good reduction for both E_g and $E_{(a,b,c)}$ such that $a_{\mathfrak{q}}(E_{(a,b,c)})$ is not divisible by p (if for example $\bar{\rho}_{E_{(a,b,c)},p}(\mathrm{Frob}_{\mathfrak{q}})$ is the identity matrix in $\mathrm{PGL}_2(\mathbb{F}_q)$) and $(\frac{-2}{q}) = -1$. This contradicts the fact that E_g and $E_{(a,b,c)}$ are congruent modulo p. ∎

3.3. The Diophantine equation $x^2 + dy^6 = z^p$

Theorem 3.24. *Let d be a prime number congruent to 19 modulo 24 and such that the class number of $K = \mathbb{Q}(\sqrt{-d})$ is prime to 6. Then there are no non-trivial primitive solutions of the equation*

$$x^2 + dy^6 = z^p,$$

for p large enough.

Proof. The proof mimics that of Theorem 3.23, in particular all results of Section 3.1 hold for $\widetilde{E}_{(a,b,c)}$, with the following important observation:

(1) The curve $\widetilde{E}_{(a,b,c)}$ does not have complex multiplication if $p > 3$ by Lemma 3.2 in [8].

(2) The curve $\widetilde{E}_{(a,b,c)}$ has additive reduction at the prime $\sqrt{-d}$, and acquires good reduction over the extension $K(\sqrt[6]{-d})$ (see Remark 2 in [18]). In particular, if $\tilde{E}_g$ denotes the elliptic curve defined over K that is obtained after applying the lowering the level result to $\widetilde{E}_{(a,b,c)}$ (whose existence is warranted by Theorem 3.16), then it also acquires good reduction over the extension $K(\sqrt[6]{-d})$, hence its minimal discriminant valuation at the prime $\sqrt{-d}$ must be even.

(3) The curve $\widetilde{E}_{(a,b,c)}$ has a K-rational 3-torsion point, so we would like to know that the same is true for $\tilde{E}_g$. Since the curve $\widetilde{E}_{(a,b,c)}$ has a point of order 3, for all prime ideals $\mathfrak{p}$ of good reduction, $a_{\mathfrak{p}}(\widetilde{E}_{(a,b,c)}) \equiv \mathcal{N}(\mathfrak{p}) + 1 \pmod 3$. Using Lemma 3.21, we know that $a_{\mathfrak{p}}(\widetilde{E}_{(a,b,c)}) = a_{\mathfrak{p}}(\tilde{E}_g)$ for all small prime ideals $\mathfrak{p}$. In particular, $a_{\mathfrak{p}}(\tilde{E}_g) \equiv \mathcal{N}(\mathfrak{p}) + 1 \pmod 3$ for all small prime ideals, hence by the so called "Sturm" bound (see for example Corollary 9.20 of [33]), the congruence holds for all prime ideals of good reduction. Then by Theorem 2 in [12], there exists a curve E' over K which is isogenous to $\tilde{E}_g$ over K which has a rational point of order 3.

(4) The hypothesis $d \equiv 19 \pmod{24}$ implies that the primes 2 and 3 are inert in $K/\mathbb{Q}$. Then the curve $\widetilde{E}_{(a,b,c)}$ has reduction type IV* at the prime ideal (2) (by Lemma 22.14 in [18]), so it has additive but potentially good reduction. Then its local type is preserved by a congruence modulo any prime larger than 3 (as explained in the proof of Lemma 3.21), so $\tilde{E}_g$ has also additive but potentially good reduction at the prime ideal (2). The same is true for the prime ideal (3), the curve $\widetilde{E}_{(a,b,c)}$ has reduction type II or III (by Lemma 2.15 in [18]).

Then there exists an elliptic curve E' defined over K with the following properties:

- The conductor of E' is supported at the prime ideals dividing $6d$.
- If the model E' is minimal at the prime ideal $(\sqrt{-d})$, then the discriminant $\Delta(E')$ of E' has even valuation at $(\sqrt{-d})$.
- The curve E' has a K-rational 3-torsion point P.
- The curve E' has potentially good reduction at (2) and at (3).

Take a semi-global minimal model for E', i.e., a model which is minimal at all primes except one extra prime ideal $\mathfrak{p}$, which we can assume that does not divide $6d$. The coordinates of the point P are algebraic integers (by Theorem 3.4 in Chapter VII of [32]), so after a translation (a transformation which preserves the discriminant of the equation), we can assume that the rational 3-torsion point is the origin $(0, 0)$, so the model is of the form

$$E' : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x, \tag{3.16}$$

where a_1, a_2, a_3 and a_4 are algebraic integers. Let $y = \alpha x$ be the tangent line of E' at P (for some number α). The fact that $P = (0, 0)$ is an inflection point of E' implies that the substitution $y = \alpha x$ on equation (3.16) (and substracting the left-hand side with the right-hand side) gives the polynomial $-x^3$.

Then $\alpha^2 + a_1\alpha - a_2 = 0$, so α is an algebraic integer. The change of variables $y' = y - \alpha x$, $x' = x$ (which preserves the discriminant and the properties of the model) sends the tangent line to the line $y' = 0$. In particular, we can (and do) assume that our semi-global minimal model is of the form

$$E' : y^2 + a_1xy + a_3y = x^3,$$

where $a_1, a_3 \in \mathbb{Z}[\frac{1+\sqrt{-d}}{2}]$. In particular,

$$\Delta(E') = a_3^3(a_1^3 - 27a_3) = 2^r\,3^q\,(\sqrt{-d})^{2s}\,\mathfrak{p}^{12}.$$

The even exponent at $(\sqrt{-d})$ comes from the fact that the model is minimal at $(\sqrt{-d})$ and the second condition. In particular, the ideal $\mathfrak{p}^{12}$ is a principal ideal, so under our assumption on the class number of K being prime to 6, $\mathfrak{p}$ is principal and hence E' does have a global minimal model (of the same form). In particular, since the only roots of unity in K are ± 1, for the minimal model it holds that

$$\Delta(E') = a_3^3(a_1^3 - 27a_3) = \pm 2^r\,3^q\,d^s. \tag{3.17}$$

If $(\sqrt{-d})$ does not divide the gcd of the two middle factors (as elements of K), a_3 must be a rational number. Then a_1^3 is also a rational number and hence a_1 is rational. On the other hand, if $(\sqrt{-d})$ divides the gcd of the two middle factors, then the minimality condition of the model E' implies that $v_{(\sqrt{-d})}(a_3) \leq 2$, so it is either 1 or 2. If it happens to be 2, then a_3 is once again a rational number, and the same proof as before implies that a_1 is rational as well.

Suppose then that $a_3 = \sqrt{-d} \cdot \beta$ for some algebraic integer β not divisible by $(\sqrt{-d})$, and that $a_1 = \sqrt{-d} \cdot \alpha$ for some algebraic integer α. Then the valuation at $(\sqrt{-d})$ of the middle term in (3.17) is 4, hence $s = 2$ and we get the equation

$$\beta^3(d\alpha^3 + 27\beta) = \pm 2^r\,3^q. \tag{3.18}$$

Once again, α and β must be integers. Since the curve E' has potentially good reduction at the prime ideals (2) and (3), there is a bound for r and q that we recall. By Theorem 10.4 in [31], the exponent conductor of E/K at the prime ideal (2) is bounded by 8 and at the prime ideal (3) is bounded by 5. By Table 4.1 on page 365 of [31], the number of

irreducible components of the special fiber of Neron's model is at most 9. Then Ogg's formula (Theorem 11.1 in [31]) implies that $r \leq 16$ and $s \leq 13$. Then we can run over all possible exponents on the right-hand side within this bound, and verify for which values we get a divisor β such that $\pm 2^r 3^q/\beta^3 - 27\beta$ is a prime times a perfect cube. Furthermore, we discard the solutions for which the curve E' does not have additive reduction at both primes 2 and 3 (since the curve $\widetilde{E}_{(a,b,c)}$ has this property). We get only four non-rational candidates, all of them defined over the quadratic field $K = \mathbb{Q}(\sqrt{-547})$, corresponding to the values

$$(\alpha, \beta) \in \{(-6, 2), (-12, 16), (6, -2), (12, -16)\}.$$

Clearly, there are only two non-isomorphic pairs (the map $(x, y) \to (x, -y)$ gives an isomorphism between a pair (a_1, a_3) and a pair $(-a_1, -a_3)$). It is easy to verify that for the two isomorphism classes of curves, the quotient by the 3-torsion point is a rational elliptic curve, hence the curve E' is isogenous to a base change. As in Theorem 3.23, this contradicts the fact that $\widetilde{E}_{(a,b,c)}$ satisfies

$$a_{\mathfrak{q}}(\widetilde{E}_{(a,b,c)}) = \left(\frac{-3}{\mathcal{N}(\mathfrak{q})}\right) a_{\bar{\mathfrak{q}}}(\widetilde{E}_{(a,b,c)}),$$

for all prime ideals $\mathfrak{q} \nmid 3$ of good reduction (as proven in Proposition 2.3 of [18]). ∎

Acknowledgements. We thank Nuno Freitas for many useful comments and remarks, as well as the anonymous referees for their many suggestions that improved the quality of the present article.

Funding. A. Pacetti was partially supported by the Portuguese Foundation for Science and Technology (FCT) Individual Call to Scientific Employment Stimulus (https://doi.org/10.54499/2020.02775.CEECIND/CP1589/CT0032) and by CIDMA under the FCT Multi-Annual Financing Program for R&D Units. L. Villagra Torcomian was supported by a CONICET grant and a PIMS-Simons postdocotal fellowship. F. Golfieri Madariaga was supported by an FCT grant UI/BD/152573/2022.

References

[1] Cohen, H. and Lenstra, H. W., Jr.: Heuristics on class groups of number fields. In *Number theory (Noordwijkerhout, 1983)*, pp. 33–62. Lecture Notes in Math. 1068, Springer, Berlin, 1984. Zbl 0558.12002 MR 0756082

[2] Cox, D. A.: *Primes of the form $x^2 + ny^2$. Fermat, class field theory, and complex multiplication*. Second edition. Pure Appl. Math. (Hoboken), John Wiley & Sons, Hoboken, NJ, 2013. Zbl 1275.11002 MR 3236783

[3] Deligne, P.: La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.* (1974), no. 43, 273–307. Zbl 0287.14001 MR 0340258

[4] Dieulefait, L. and Jiménez Urroz, J.: Solving Fermat-type equations via modular $\mathbb{Q}$-curves over polyquadratic fields. *J. Reine Angew. Math.* **633** (2009), 183–195. Zbl 1250.11033 MR 2561200

[5] Ellenberg, J. S.: Galois representations attached to $\mathbb{Q}$-curves and the generalized Fermat equation $A^4 + B^2 = C^p$. *Amer. J. Math.* **126** (2004), no. 4, 763–787. Zbl 1059.11041 MR 2075481

[6] Faltings, G.: Finiteness theorems for abelian varieties over number fields. In *Arithmetic geometry (Storrs, Conn., 1984)*, 9–27. Springer, New York, 1986. Zbl 0602.14044 MR 0861971

[7] Freitas, N., Kraus, A. and Siksek, S.: Class field theory, Diophantine analysis and the asymptotic Fermat's last theorem. *Adv. Math.* **363** (2020), article no. 106964, 37 pp. Zbl 1450.11023 MR 4054049

[8] Golfieri Madriaga, F. G., Pacetti, A. and Torcomian, Villlagra Torcomian, L.: On the equation $x^2 + dy^6 = z^p$ for square-free $1 \leq d \leq 20$. *Int. J. Number Theory* **19** (2023), no. 5, 1129–1165. Zbl 1523.11060 MR 4583916

[9] Hecke, E.: *Mathematische Werke*. Vandenhoeck & Ruprecht, Göttingen, 1970. Zbl 0205.28902 MR 0371577

[10] Hellegouarch, Y.: *Invitation to the mathematics of Fermat–Wiles*. Academic Press, San Diego, CA, 2002. Zbl 1036.11001 MR 1858559

[11] Işik, E., Kara, Y. and Ozman, E.: On ternary Diophantine equations of signature $(p, p, 2)$ over number fields. *Turkish J. Math.* **44** (2020), no. 4, 1197–1211. Zbl 1478.11041 MR 4122899

[12] Katz, N. M.: Galois properties of torsion points on abelian varieties. *Invent. Math.* **62** (1981), no. 3, 481–502. Zbl 0471.14023 MR 0604840

[13] Khare, C. and Wintenberger, J.-P.: Serre's modularity conjecture. I. *Invent. Math.* **178** (2009), no. 3, 485–504. Zbl 1304.11041 MR 2551763

[14] Khare, C. and Wintenberger, J.-P.: Serre's modularity conjecture. II. *Invent. Math.* **178** (2009), no. 3, 505–586. Zbl 1304.11042 MR 2551764

[15] Kisin, M.: Moduli of finite flat group schemes, and modularity. *Ann. of Math. (2)* **170** (2009), no. 3, 1085–1180. Zbl 1201.14034 MR 2600871

[16] Koblitz, N.: *Introduction to elliptic curves and modular forms*. Second edition. Grad. Texts in Math. 97, Springer, New York, 1993. Zbl 0804.11039 MR 1216136

[17] Mocanu, D.: Asymptotic Fermat for signatures $(p, p, 2)$ and $(p, p, 3)$ over totally real fields. *Mathematika* **68** (2022), no. 4, 1233–1257. Zbl 1534.11041 MR 4490710

[18] Pacetti, A. and Villagra Torcomian, L.: $\mathbb{Q}$-Curves, Hecke characters and some Diophantine equations. *Math. Comp.* **91** (2022), no. 338, 2817–2865. Zbl 1503.11072 MR 4473105

[19] Pan, L.: The Fontaine–Mazur conjecture in the residually reducible case. *J. Amer. Math. Soc.* **35** (2022), no. 4, 1031–1169. Zbl 1502.11062 MR 4467307

[20] Pyle, E. E.: *Abelian varieties over the set of rational numbers with large endomorphism algebras and their simple components over the set of irrational numbers*. Ph.D. Thesis, University of California, Berkeley, 1995. MR 2693262

[21] Quer, J.: Fields of definition of building blocks. *Math. Comp.* **78** (2009), no. 265, 537–554. Zbl 1204.11091 MR 2448720

[22] Ribet, K. A.: Twists of modular forms and endomorphisms of abelian varieties. *Math. Ann.* **253** (1980), no. 1, 43–62. Zbl 0421.14008 MR 0594532

[23] Ribet, K. A.: Abelian varieties over $\mathbb{Q}$ and modular forms. In *Algebra and topology 1992 (Taejŏn)*, pp. 53–79. Korea Adv. Inst. Sci. Tech., Taejŏn, 1992. Zbl 1092.11029 MR 1212980

[24] Ribet, K. A.: Fields of definition of abelian varieties with real multiplication. In *Arithmetic geometry (Tempe, AZ, 1993)*, pp. 107–118. Contemp. Math. 174, American Mathematical Society, Providence, RI, 1994. Zbl 0877.14030 MR 1299737

[25] Ribet, K. A.: Abelian varieties over $\mathbb{Q}$ and modular forms. In *Modular curves and abelian varieties*, pp. 241–261. Progr. Math. 224, Birkhäuser, Basel, 2004. Zbl 1092.11029 MR 2058653

[26] Şengün, M. H. and Siksek, S.: On the asymptotic Fermat's last theorem over number fields. *Comment. Math. Helv.* **93** (2018), no. 2, 359–375. Zbl 1430.11045 MR 3811755

[27] Serre, J.-P.: *Abelian l-adic representations and elliptic curves*. Res. Not. Math. 7, A K Peters, Wellesley, MA, 1998. MR 1484415

[28] Shimura, G.: On the factors of the Jacobian variety of a modular function field. *J. Math. Soc. Japan* **25** (1973), 523–544. Zbl 0266.14017 MR 0318162

[29] Shimura, G.: *Introduction to the arithmetic theory of automorphic functions*. Pub. Math. Soc. Japan 11, Princeton University Press, Princeton, NJ, 1994. Zbl 0872.11023 MR 1291394

[30] Siksek, S.: The modular approach to Diophantine equations. In *Explicit methods in number theory*, pp. 151–179. Panor. Synthèses 36, Société Mathématique de France, Paris, 2012. Zbl 1343.11042 MR 3098134

[31] Silverman, J. H.: *Advanced topics in the arithmetic of elliptic curves*. Grad. Texts in Math. 151, Springer, New York, 1994. Zbl 0911.14015 MR 1312368

[32] Silverman, J. H.: *The arithmetic of elliptic curves*. Second edition. Grad. Texts in Math. 106, Springer, Dordrecht, 2009. Zbl 1194.11005 MR 2514094

[33] Stein, W.: *Modular forms, a computational approach*. Grad. Stud. Math. 79, American Mathematical Society, Providence, RI, 2007. Zbl 1110.11015 MR 2289048

[34] Thorner, J. and Zaman, A.: An explicit bound for the least prime ideal in the Chebotarev density theorem. *Algebra Number Theory* **11** (2017), no. 5, 1135–1197. Zbl 1432.11167 MR 3671433

Received May 13, 2024; revised March 12, 2025.

Franco Golfieri Madriaga
Department of Mathematics, Center for Research and Development in Mathematics and Applications (CIDMA), University of Aveiro
Campus Universitário de Santiago, 3810-193 Aveiro, Portugal;
francogolfieri@ua.pt

Ariel Pacetti
Department of Mathematics, Center for Research and Development in Mathematics and Applications (CIDMA), University of Aveiro
Campus Universitário de Santiago, 3810-193 Aveiro, Portugal;
apacetti@ua.pt

Lucas Villagra Torcomian
Department of Mathematics, Simon Fraser University
8888 University Drive, Burnaby, V5A 1S6, Canada;
lvillagr@sfu.ca