ASYMPTOTIC RESULTS FOR THE EQUATIONS
$x^4 + dy^2 = z^p$ **AND** $x^2 + dy^6 = z^p$

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 a congruence between the Galois representations attached to f and to g for a large prime p implies an isomorphism between the endomorphism algebras of the abelian varieties A_f and A_g attached to f and g by the Eichler-Shimura construction. 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 $x^2 + dy^6 = z^p$.

INTRODUCTION

Let $f \in S_2(\Gamma_1(N))$ and $g \in S_2(\Gamma_1(\tilde{N}))$ be two newforms satisfying the following two conditions:

(1) The coefficient field K_f of f matches the coefficient field K_g of g.
(2) There exists a large prime p such that the Galois representations $\overline{\rho_{f,\mathfrak{p}}}$ and $\overline{\rho_{g,\mathfrak{p}}}$ are isomorphic.

By Eichler-Shimura's 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

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

and a similar relation for g. Let $L/\mathbb{Q}$ be a finite extension.

Question 1: is there a relation between $\text{End}_L(A_f) \otimes \mathbb{Q}$ and $\text{End}_L(A_g) \otimes \mathbb{Q}$?

One of the main results of the present article (Theorem 1.2) is a positive answer to the question when the forms f and g do not have complex multiplication. The ideas used to prove such a result 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.

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 [14, 15, 16]). 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. A key fact here is that a congruence between two newforms for a large prime p gives equality of their first Fourier coefficients.

By a result of Hecke, if two modular forms f and g satisfy that $a_n(f) = a_n(g)$ for sufficiently many values of n, then they must coincide. Applying these two facts in a clever way allows us to give an isomorphism between the algebra of endomorphisms of A_f and that of A_g. Furthermore, our results states that $\mathrm{End}_L(A_f) \otimes \mathbb{Q}$ is isomorphic to $\mathrm{End}_L(A_g) \otimes \mathbb{Q}$ not just as $\mathbb{Q}$-algebras, but also as $\mathrm{Gal}(L/\mathbb{Q})$-modules. This in particular implies that the splitting (up to isogeny) of the abelian variety A_f matches that of A_g over any field extension $L/\mathbb{Q}$.

Here is a very 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

$$
(1) \qquad\qquad\qquad\qquad x^4 + dy^2 = z^p,
$$

for a fixed positive integer d. A solution (a, b, c) of a Fermat-type equation such as (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

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

The curve $E_{(a,b,c)}$ turns out to be a $\mathbb{Q}$-curve hence in particular (by a result of Ribet in [17]), there exist a character $\varkappa$ 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 $\mathrm{Gal}_{\mathbb{Q}}$. By Serre's conjectures and some Taylor-Wiles result, $\tilde{\rho}$ is modular, i.e. there exist a modular form $f \in S_2(N, \varepsilon)$ and a prime $\mathfrak{p}$ in the coefficient field K_f dividing p such that $\tilde{\rho} \simeq \rho_{f,\mathfrak{p}}$. By Eichler-Shimura, f has associated an abelian variety A_f of dimension $[K_f : \mathbb{Q}]$.

The curve $E_{(a,b,c)}$ has multiplicative reduction at all odd primes dividing c (since the solution is primitive, if a prime divides c, it cannot divide d), so by a result of Hellegouarch 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 $S_2(\tilde{N}, \varepsilon)$ and prove that no newform can be related to a non-trivial primitive solution of (1). By an idea due to Mazur, one can discard all forms g whose coefficient field K_g does not match that of f, which justifies our hypothesis in Question 1. However, the newforms g whose coefficient field K_g matches K_f in general 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 might have dimension two (i.e. is related to a "fake elliptic curve", namely an abelian surface with quaternionic multiplication). While studying Fermat's original equation over number fields, the way to discard this unpleasant situation is to use the existence of a prime of potentially multiplicative reduction (see for example [3]), which unfortunately we do not have.

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

Question 2: Is it true that the newform g also has a building block E_g of dimension 1? If so, what is the minimum field of definition of the building block?

The answer to this second question is also positive when p is large enough (see Theorem 2.4), and we will furthermore prove that the building block E_g can be defined over the

quadratic field K (see Theorem 2.4). A non-trivial consequence is that actually there exists a building block E_g defined over K such that the residual Galois representations $\overline{\rho_{E_{(a,b,c)},p}}$ and $\overline{\rho_{E_g,p}}$ are isomorphic (see Theorem 2.11).

For proving non-existence of non-trivial primitive solutions of (1), we are led to prove that there are no 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 3.1. *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 Corollary we can prove the following asymptotic result.

Theorem 3.4. *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

$$(3) \qquad\qquad\qquad x^2 + dy^6 = z^p.$$

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

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

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 [11]. 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) 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 [11, Lemmas 2.13, 2.14 and 2.15]), while the curve $E_{(a,b,c)}$ had only bad reduction at primes dividing 2. We will prove the following result.

Theorem 3.5. *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: the first section recalls the definition and main properties of inner twists as developed by Ribet in [14]. It also contains the proof of Theorem 1.2 providing an answer to the first posed question. In Section 2 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). In particular, we compute explicitly the group of inner twists of A_f and use this information to answer the second aforementioned question (and its consequences). The last section is devoted to prove Theorem 3.1 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 3.4 and of Theorem 3.5. The code used to prove Theorem 3.5 is available at https://github.com/lucasvillagra/Asymptotic-results.

1. Inner Twists

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 [14].

Definition. Let f be a newform without complex multiplication, and let $K_f = \mathbb{Q}(a_p(f))$ denote its coefficient field. The *group of inner twists* of f is defined as

(5) $\Gamma_f := \{\gamma \in \mathrm{Hom}_{\mathbb{Q}}(K_f, \mathbb{C}) : \exists \, \chi_\gamma$ a Dirichlet character with

$$\gamma(a_p(f)) = \chi_\gamma(p)a_p(f) \text{ for almost all } p\}.$$

By assumption f does not have complex multiplication, so given γ there exists a unique character χ_γ. For this reason, we denote the elements of Γ_f by pairs (γ, χ).

Example. If f is a newform in $S_2(N, \varepsilon)$, 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 [14, Example 3.7]).

Let us recall some properties of the group Γ_f.
- For $\gamma \in \Gamma_f$, $\gamma(K_f) \subset K_f$ (by [14, Proposition 3.2]). In particular, Γ_f is a subset of $\mathrm{Aut}_{\mathbb{Q}}(K_f)$.
- The set Γ_f is in fact an abelian group (by [14, Proposition 3.3]).

By $\mathrm{End}^0(A_f) := \mathrm{End}(A_f) \otimes \mathbb{Q}$ we denote the algebra of endomorphisms defined over the algebraic closure of $\mathbb{Q}$. If L is an extension of K, we denote by $\mathrm{End}_L^0(A_f)$ the endomorphisms defined over L. One of the main results of [14] is that the endomorphism algebra $\mathrm{End}^0(A_f)$ can be computed in terms of the inner twists of f. More concretely, in the proof of [14, Theorem 5.1], Ribet constructs for each inner twist (γ, χ) an endomorphism (denoted by η_γ in [14]) via the following formula

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

where r is the conductor of χ, $\chi(u)$ is viewed as an element of the endomorphism algebra of A_f, and $\alpha_{u/r}$ is the endomorphism given by slashing by the matrix $\left(\begin{smallmatrix} 1 & \frac{u}{r} \\ 0 & 1 \end{smallmatrix}\right)$.

As explained in Ribet's article, if χ has conductor r, then 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). The

following result is well known to experts, but we did not find a proper reference for its proof. 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 1.1. *The endomorphism η_γ is defined over $\overline{\mathbb{Q}}^\chi$.*

Proof. We know that η_γ is defined at least over $\mathbb{Q}(\zeta_r)$ (the field of r-th roots of unity). Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q})$, say $\sigma(\zeta_r) = \zeta_r^i$, so the endomorphism $\sigma(\alpha_{u/r}) = \alpha_{iu/r}$. Then

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

The result follows from the fact that $\chi(i) = 1$ if and only if σ restricted to $\overline{\mathbb{Q}}^\chi$ is the identity. $\square$

Theorem 1.2. *Let $f \in S_2(\Gamma_1(N))$ and $g \in S_2(\Gamma_1(\tilde{N}))$ be newforms without complex multiplication, such that:*

> *(1) The coefficient field K_f of f equals the coefficient field K_g of g.*
> *(2) There exists a large prime p such that the Galois representations $\overline{\rho_{f,\mathfrak{p}}}$ and $\overline{\rho_{g,\mathfrak{p}}}$ are isomorphic.*

Let A_f and A_g be the abelian varieties attached to f and g by the Eichler-Shimura construction. Then for any field extension L/K the $\mathbb{Q}$-algebras $\mathrm{End}_L^0(A_f)$ and $\mathrm{End}_L^0(A_g)$ are isomorphic. Moreover, if L/K is Galois, then the algebras are isomorphic as $\mathrm{Gal}(L/K)$-modules as well.

Proof. By Ribet's result, the endomorphisms of the abelian variety A_f over $\overline{\mathbb{Q}}$ is the algebra generated by the endomorphisms η_γ, where $\gamma \in \Gamma_f$, and by Lemma 1.1 the endomorphism attached to the pair (γ, χ) is defined over the field $\overline{\mathbb{Q}}^\chi$. If we prove that the sets Γ_f and Γ_g are the same, then the stated isomorphism sends the endomorphism η_γ of A_f to the endomorphism η_γ of A_g, which is clearly Galois equivariant. The key point to prove that the inner twists groups are the same is the fact that the group Γ_f is defined in terms of a property of Fourier coefficients.

Let $(\gamma, \chi) \in \Gamma_f$ and let's prove that it also belongs to Γ_g. By definition, for almost all primes q,

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

The second hypothesis then implies that there exists a prime ideal $\mathfrak{p}$ in $\mathcal{O}_f$ (the ring of integers of K_f) such that for all primes q (but finitely many),

$$\gamma(a_q(g)) \equiv \chi(q)a_q(g) \pmod{\mathfrak{p}}. \tag{7}$$

By the Ramanujan-Petersson conjecture (see [4]), for all embeddings $\sigma : K_f \to \mathbb{C}$, $|\sigma(a_q(g))| \leq 2\sqrt{q}$. Then, if p is large enough (with respect to q), the congruence (7) implies that both numbers are in fact equal, i.e. taking p large enough, $\gamma(a_q(g)) = \chi(q)a_q(g)$ for all small primes q.

It was already known to Hecke (see [9], p. 811, Satz 1 and Satz 2) that two modular forms whose first coefficients coincide (up to an explicit bound B depending on the level and the weight) must be equal. In particular, the forms $\gamma(g)$ and $g \otimes \chi$ (the twist of g by the character χ) are the same, so $\gamma \in \Gamma_g$ as claimed. The other containment follows by replacing f with g and vice-versa. $\square$

Remark 1. Note that the prime p in the previous result depends on both N and $\tilde{N}$, since we need to use Hecke's bound twice. However, the same proof gives that if we fix $\tilde{N}$, then there exists a bound B (depending only on $\tilde{N}$) such that $\text{End}_L^0(A_f) \subset \text{End}_L^0(A_g)$ if p is larger than B. We will make use of this fact later.

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

Let (a, b, c) be a non-trivial primitive solution of (1) for $d \neq 1$ and let $E_{(a,b,c)}$ be the elliptic curve over $K = \mathbb{Q}(\sqrt{-d})$ defined in (2).

Lemma 2.1. *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 them gives the relation

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

hence $\frac{a^2}{b} = \pm\frac{9}{5}\sqrt{d/7}$. 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 $c = \pm 16$. $\square$

As explained in the introduction, there exists a finite order Hecke character $\varkappa$ (whose description is given in [11]) of K such that the twisted representation $\rho_{E_{(a,b,c)},p} \otimes \varkappa$ extends to a representation $\tilde{\rho} : \text{Gal}_\mathbb{Q} \to \text{GL}_2(\overline{\mathbb{Q}_p})$. Let $f \in S_2(N, \varepsilon)$ be the newform attached to such a representation (see [11] for a description of the Nebentypus ε) and 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, $A_f \sim B_1 \times \cdots \times B_r$. Each variety B_i is called a *building block* of A_f. In the particular case of abelian varieties coming from newforms, all building blocks are isogenous to each other, so in particular $A_f \sim B^r$ (see [13]).

In our particular case, the building block of A_f is clearly the elliptic curve $E_{(a,b,c)}$ defined over the quadratic field K.

Lemma 2.2. *Let $r = [K_f : \mathbb{Q}]$. Then the endomorphism algebra $\text{End}^0(A_f)$ is isomorphic to $M_r(\mathbb{Q})$.*

Proof. Follows from the fact that the building block of A_f is the elliptic curve $E_{(a,b,c)}$, of dimension 1 and which does not have complex multiplication. $\square$

Remark 2. Since the center of $\text{End}^0(A_f)$ is the field of rational numbers $\mathbb{Q}$, Ribet's result ([14, Theorem 5.1]) 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's just verify that this is indeed the case (because a similar computation will be needed later).

A key property of the character $\varkappa$ and ε is that as characters of the respective idèle group, they satisfy the relation $\varkappa^2 = \varepsilon \circ \mathcal{N}$. Consider the following two cases:

- If the prime p splits, say $p = \mathfrak{p}\overline{\mathfrak{p}}$, then the previous relation translates into $\varkappa(\mathfrak{p})^2 = \varepsilon(p)$. Then
$$a_p(f)^2 \varepsilon(p)^{-1} = \left(a_{\mathfrak{p}}(E)\varkappa(\mathfrak{p})\right)^2 \varepsilon(p)^{-1} = a_{\mathfrak{p}}(E)^2 \in \mathbb{Q}.$$

- If the prime p is inert, $\varkappa(p)^2 = \varepsilon(p^2) = \varepsilon(p)^2$. Then using the relation between $a_p(f)$ and $a_p(E)$ we get that
$$a_p(f)^2 \varepsilon(p)^{-1} = a_p(E)\varkappa(p)\varepsilon(p)^{-1} + 2p = \pm a_p(E) - 2p \in \mathbb{Q}.$$

The elliptic curve $E_{(a,b,c)}$ has discriminant $\Delta(E_{(a,b,c)}) = 512(a^2 + b\sqrt{-d})c^p$, which is a p-th power outside 2. In particular, if $q \mid c$, then the curve $E_{(a,b,c)}$ has multiplicative reduction at the primes dividing q (in K), and the residual representation $\overline{\rho_{E_{(a,b,c)},p}}$ is unramified at (the primes dividing) q by a result due to Hellegouarch.

There exists an explicit bound N_K such that the residual Galois representation $\overline{\rho_{E_{(a,b,c)},p}}$ is absolutely irreducible for all primes $p > N_K$ (see [11, Theorem 5.1] and [6, Proposition 3.2]). Then by Ribet's lowering the level result, there exists a newform $g \in S_2(\tilde{N}, \varepsilon)$, where $\tilde{N}$ is a positive integer only divisible by 2 and by the primes dividing d, such that $\overline{\rho_{f,\mathfrak{p}}} \simeq \overline{\rho_{g,\mathfrak{p}}}$. Note in particular that the value of $\tilde{N}$ is independent of the solution (a, b, c) we started with.

Assume from now on that the newform 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 1.2 is the following result.

Proposition 2.3. *Suppose that $K_f = K_g$. Then there exists B (depending only on $\tilde{N}$) such that if $p > B$, $\mathrm{End}^0(A_g) \simeq \mathrm{End}^0(A_f)$. In particular, the building block of the abelian variety A_g has dimension 1.*

Proof. Theorem 1.2 and Remark 1 imply that $\mathrm{End}^0(A_f) \subset \mathrm{End}^0(A_g)$ (over $\overline{\mathbb{Q}}$), so $M_r(\mathbb{Q}) \subset \mathrm{End}^0(A_g)$, where $r = [K_f : \mathbb{Q}] = \dim(A_g)$. Since the form g does not have complex multiplication, the previous inclusion is actually an equality. In particular, the building block of A_g has dimension 1. $\square$

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 that of A_f (namely K).

Theorem 2.4. *There exists a 1-dimensional building block E_g for A_g defined over the quadratic field K.*

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 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 μ_σ denote such an isogeny. Abusing notation (as in Ribet's article [14]) we can attach to E_g a map $c: \mathrm{Gal}_{\mathbb{Q}} \times \mathrm{Gal}_{\mathbb{Q}} \to \mathbb{Q}^\times$ given by

$$(8) \qquad\qquad c(\sigma, \tau) = \mu_\sigma \circ \sigma(\mu_\tau) \circ \mu_{\sigma\tau}^{-1},$$

which is an element of $\mathrm{End}^0(E_g) \simeq \mathbb{Q}^\times$. The map c is actually a cocycle (by [14] (5.7)). 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 [14, Remark 5.8] and [16, Proposition 3.2]). Then by [12, Proposition 5.2] the building block E_g is isogenous (over $\overline{\mathbb{Q}}$) to a building block 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 ([16, Corollary 4.5]) the curve E_g does have a minimum field of definition. Furthermore, it can be explicitly described (as done in the proof of [16, Theorem 3.3]): 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) $(\overline{c}, c_\pm)$, where $\overline{c} \in \mathrm{H}^2(\mathrm{Gal}_\mathbb{Q}, \mathbb{Q}_+^\times)[2]$ and $c_\pm \in \mathrm{H}^2(\mathrm{Gal}_\mathbb{Q}, \{\pm 1\})$. The minimum field of definition $K_{\min}$ for a building block equals the fixed field of $\overline{c}$.

There is a second way to define the cocycle $[c]$ in terms of the $\mathbb{Q}$-algebra $\mathrm{End}^0(A_g)$ (see [12, Chapter 1]). Let K_g, as before, denote the coefficient field of g (which also equals $\mathrm{End}_\mathbb{Q}^0(A_g)$) and let $\psi \in \mathrm{End}^0(A_g)$. If $\sigma \in \mathrm{Gal}_\mathbb{Q}$, it acts on the set $\mathrm{End}^0(A_g)$. Let us denote by $^\sigma \psi$ the action of σ 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 [12, Theorem 4.6], both definitions coincide. But by Proposition 2.3, 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 definition of both building blocks coincide. $\qquad\square$

Remark 3. Even when the building block E_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 2.11). Here is an example (that will be explained in detail while proving such theorem): let $L = K \cdot \overline{\mathbb{Q}}^\varepsilon$. 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 isogeny 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 [17, Theorem 8.2], 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 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.

Lemma 2.5. *Following the previous notation, let M be the order of the character $\varkappa$. Then $\mathbb{Q}(\zeta_M) \subset K_f$, where ζ_M denotes a primitive M-th root of unity.*

Proof. The set of unramified primes $\mathfrak{p}$ of K with inertial degree 1 over $\mathbb{Q}$ have density one, 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 $a_{\mathfrak{p}}(E) \neq 0$. 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. $\square$

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

Lemma 2.6. *With the previous notations, $K \cdot \overline{\mathbb{Q}}^{\varepsilon} \subset \overline{K}^{\varkappa}$ with index 2. Moreover, we have the following field diagram.*
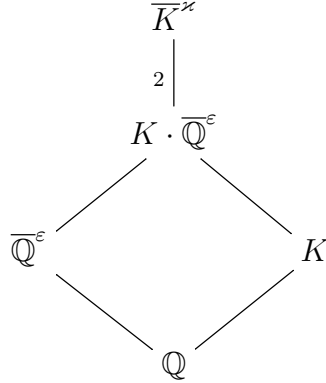
Proof. Follows from the fact that as a Galois character, $\varepsilon|_{\mathrm{Gal}_K} = \varkappa^2$. $\square$

Proposition 2.7. *Let M be the order of the character $\varkappa$. Then 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 $K/\mathbb{Q}$, not dividing the level of f, for which $a_p(f) \neq 0$.

Proof. By Lemma 2.5, $\mathbb{Q}(\zeta_M) \subseteq K_f$. If p is a rational prime which is split in K, say $p = \mathfrak{p}\overline{\mathfrak{p}}$, then

$$(9) \qquad a_p(f) = a_{\mathfrak{p}}(E_{(a,b,c)})\varkappa(\mathfrak{p}) \in \mathbb{Q}(\zeta_M).$$

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

$$(10) \qquad a_p(f)^2 = a_p(E_{(a,b,c)})\varkappa(p) + 2p\varepsilon(p).$$

Recall that $\varkappa^2 = \varepsilon \circ \mathcal{N}$, so $\varkappa(p) = \pm\varepsilon(p)$. Thus $a_p(f)^2 \in \mathbb{Q}(\varkappa)$, the field obtained by adding to $\mathbb{Q}$ the values of $\varkappa$. Formula (10) 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.

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 $a_p(f) = t \neq 0$. 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

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

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

$$(11) \qquad \rho_{E_{(a,b,c)},\ell}(\mathrm{Frob}_p^2)\varkappa(\mathrm{Frob}_p^2) = \begin{pmatrix} -s & -st \\ t & t^2 - s \end{pmatrix}.$$

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, $\mathrm{Tr}(\tilde{\rho}(\mathrm{Frob}_q)) = a_q(f) \in L_\lambda$ for all primes $\lambda \in L$, hence $a_q(f) \in L$ for all primes q so $K_f \subseteq L$. $\qquad\square$

Remark 4. 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 coefficient field of E equals $K_f = \mathbb{Q}$, which is the trivial extension of $\mathbb{Q}(\zeta_2) = \mathbb{Q}$.

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 [11], it follows from its construction given in the proof of Theorem 3.2).

Lemma 2.8. *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 taking the square root of the coefficient $a_p(f)$ for an inert prime p 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 (10), we get that

$$(12) \qquad a_p(f)^2 = \varepsilon(p)(\pm a_p(E_{(a,b,c)}) + 2p).$$

The order of ε is a power of two which equals the degree of the extension $[\overline{\mathbb{Q}}^{\varepsilon} : \mathbb{Q}]$. Since the character ε is even, its fixed field is a totally real number field, so $\overline{\mathbb{Q}}^{\varepsilon} \cap K = \mathbb{Q}$. In particular, $[\overline{\mathbb{Q}}^{\varepsilon} : \mathbb{Q}] = [K \cdot \overline{\mathbb{Q}}^{\varepsilon} : K]$, which by Lemma 2.6 is a proper divisor of M, the order of $\varkappa$. Since M is also a power of two, $\varepsilon(p)$ is a square in $\mathbb{Q}(\zeta_M)$, hence $K_f = \mathbb{Q}(\zeta_M)[\sqrt{(\pm a_p(E_{(a,b,c)}) + 2p}]$ as claimed. $\qquad \square$

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 $\mathbb{Z}/2 \times (\mathbb{Z}/M)^{\times}$. An interesting phenomena in our situation is that all elements of such Galois group correspond to an inner twist.

Theorem 2.9. *Let M be the order of the character $\varkappa$ and let δ_K denote the quadratic Dirichlet character giving 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. Then all inner twists of A_f are the following:*

- *If $\sigma_j \in \mathrm{Gal}(K_f/\mathbb{Q})$ satisfies that $\sigma_j(\zeta_M) = \zeta_M^j$ and σ_j acts trivially on F, then $(\sigma_j, \varepsilon^{(j-1)/2})$ is an inner twist.*
- *If $\sigma_j \in \mathrm{Gal}(K_f/\mathbb{Q})$ satisfies that $\sigma_j(\zeta_M) = \zeta_M^j$ and 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 $K/\mathbb{Q}$, then $a_p(f) = \varkappa(\mathfrak{p}) a_{\mathfrak{p}}(E_{(a,b,c)})$, so

$$(13) \qquad \sigma_j(a_p(f)) = \varkappa^j(\mathfrak{p}) a_{\mathfrak{p}}(E_{(a,b,c)}) = \varkappa^{j-1}(\mathfrak{p})(\varkappa(\mathfrak{p}) a_{\mathfrak{p}}(E_{(a,b,c)})) = \varepsilon^{(j-1)/2}(p) a_p(f),$$

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. On the other hand, if p is inert in K, it is enough to study the case when $a_p(f) \neq 0$. By (12)

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

where $\varepsilon(p)$ is a square in $\mathbb{Q}(\zeta_M)$, say $\varepsilon(p) = \zeta_M^{2r}$. To ease notation, let $\eta = \pm a_p(E_{(a,b,c)}) + 2p$. Then $a_p(f) = \zeta_M^r \sqrt{\eta}$ (for the right choice of the square root), so applying σ_j we get

$$(14) \qquad \sigma_j(a_p(f)) = \zeta_M^{jr} \sigma_j(\sqrt{\eta}) = a_p(f) \zeta_M^{(j-1)r} \frac{\sigma_j(\sqrt{\eta})}{\sqrt{\eta}} = a_p(f) \varepsilon(p)^{(j-1)/2} \frac{\sigma_j(\sqrt{\eta})}{\sqrt{\eta}}.$$

If $\sigma_j(\sqrt{\eta}) = \sqrt{\eta}$ (i.e. σ_j acts trivially on F), then equations (13) and (14) imply that $(\sigma_j, \varepsilon^{(j-1)/2})$ is an inner twist, while if $\sigma_j(\sqrt{\eta}) = -\sqrt{\eta}$ (i.e. 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. $\qquad \square$

As an immediate application, using Lemma 1.1, we get the following result.

Corollary 2.10. *All the endomorphisms of A_f are defined over the field $K \cdot \overline{\mathbb{Q}}^{\varepsilon}$.*

Theorem 2.11. *In the previous notation, and under the assumption that $K_f = K_g$ and that p is large enough, there exists a building block E_g defined over the quadratic field K such that*

$$\overline{\rho_{E_{(a,b,c)}, p}} \simeq \overline{\rho_{E_g, p}}.$$

Proof. Since all endomorphisms of A_f are defined over $L := K \cdot \overline{\mathbb{Q}}^{\varepsilon}$ (by Corollary 2.10), $\mathrm{End}_L^0(A_g)$ contains $M_r(\mathbb{Q})$ by Theorem 1.2 and Remark 1, where $r = \dim(A_f)$. Then, over L both varieties are isgenous to r-copies of an elliptic curve. Let us explain in more detail the situation for A_f. Over $\overline{\mathbb{Q}}$, $E_{(a,b,c)}$ is a building block, but it is not a factor of its splitting

over L. The reason is that by construction, the Galois representation of A_f restricted to Gal_K is isomorphic either to the direct sum

$$(15) \qquad \rho_{A_f,p}|_{\mathrm{Gal}_K} \simeq \bigoplus_{i=1}^{M/2} \rho_{E_{(a,b,c)},p} \otimes \varkappa^{2i-1},$$

or to twice such a sum (depending on whether $\mathbb{Q}(\zeta_M)$ equals K_f or not). The key point is that $\varkappa$ restricted to Gal_L is a quadratic character (by Lemma 2.6), 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 $E_{(a,b,c)}$ over $\overline{K}^\varkappa$ is trivial while restricted to Gal_K.

By Theorem 2.4 (and Remark 3), 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 residual Galois representations $\overline{\rho_{E_{(a,b,c)},p}}$ and $\overline{\rho_{E_g,p}}$ 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

$$(16) \qquad \mathrm{Ind}_{\mathrm{Gal}_{\overline{K}^\varkappa}}^{\mathrm{Gal}_K}(\rho_{E_g,p}|_{\mathrm{Gal}_{\overline{K}^\varkappa}}) \simeq \bigoplus_{i=1}^{M} \rho_{E_g,p} \otimes \varkappa^i.$$

Since the curve $E_{(a,b,c)}$ is also defined over K, a similar splitting holds for $\mathrm{Ind}_{\mathrm{Gal}_{\overline{K}^\varkappa}}^{\mathrm{Gal}_K}(\rho_{E_{(a,b,c)},p}|_{\mathrm{Gal}_L})$. Then

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

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

$$\overline{\rho_{E_{(a,b,c)},p}} \simeq \overline{\rho_{E_g,p}} \otimes \overline{\varkappa}^i,$$

for some exponent i. Taking determinants on both sides, it follows that either $\overline{\varkappa}^i = 1$, or $\overline{\varkappa}^i$ is a quadratic character. Note that since p is odd, and $\varkappa$ has order a power of two, $\varkappa$ and $\overline{\varkappa}$ 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. $\qquad\square$

3. Applications

3.1. **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 3.1. *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 hypothesis. 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 at most one extra prime $\mathfrak{p}$ (which we assume is odd), and the discriminant valuation at $\mathfrak{p}$ equals 12. 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
    Since E/K has a K-rational point of order 2, we can take a model (which might not be minimal at 2 but is minimal at all other prime ideals) 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 $\Delta(E) = 2^4 b^2(a^2 - 4b)$ 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

(17)
$$b^2(a^2 - 4b) = \pm 2^{r-4}.$$

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 $b \in \mathbb{Z}$ (and since $\Delta(E)$ is an algebraic integer, $2t + 4 \leq r$). Substituting in (17) we get that

(18)
$$a^2 = \pm 2^{r-4-2t} \pm 2^{t+2} \in \mathbb{Z}.$$

Suppose that $a = \frac{a_1 + a_2\sqrt{-d}}{2}$, with $a_1, a_2 \in \mathbb{Z}$ (and $a_1 \equiv a_2 \pmod{2}$). Since a^2 is a rational number, $a_1 a_2 = 0$. If $a_2 = 0$ then both a, 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 (18) 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 $d > 3$. $\qquad\square$

13

Remark 5. 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 6. The last result is similar to [7, Theorem 1], 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 7. 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 [2, §6]). The Cohen-Lenstra heuristics ([1, (C2)] and also page 58 of such an article) 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 3.2. *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 $\overline{\rho_{E_1,p}} \simeq \overline{\rho_{E_2,p}}$. 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 [8, Theorem 1.4]. Since $p > 3$, the curve E_2 must have either good or multiplicative reduction at $\mathfrak{q}$ (by [8, Remark 6]). If the reduction is multiplicative, we are in a "lowering the level" case, hence

$$(19) \qquad a_{\mathfrak{q}}(E_1) \equiv \pm(\mathcal{N}(\mathfrak{q}) + 1) \pmod p.$$

But Hasse's bound implies that $|a_{\mathfrak{q}}(E_1)| \leq 2\sqrt{\mathcal{N}(\mathfrak{q})}$. Since the difference of the right and the left-hand side of (19) 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. $\qquad\square$

Lemma 3.3. *Let (a, b, c) a primitive solution of (1), where p is large enough so that $\overline{\rho_{E_{(a,b,c)},p}}$ is absolutely irreducible. Let q an odd prime, then there exists a bound B (depending only on d) 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 $\overline{\rho_{E_{(a,b,c)},p}}$. 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 "lowering the level case". In particular,

$$(20) \qquad p \mid \mathcal{N}(\varepsilon^{-1}(q)(q+1)^2 - a_q(g)^2).$$

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 $S_2(\tilde{N}, \varepsilon)$ which does not depend on (a, b, c)), so it is enough to prove that the right-hand side of (20) 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. $\qquad\square$

Theorem 3.4. *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.

Proof. The case $d = 3$ was proven in [5], so we can restrict to values $d > 3$. Let (a, b, c) be a non-trivial primitive solution and consider the elliptic curve

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

as in the introduction. The assumption (a, b, c) being non-trivial and primitive implies that $E_{(a,b,c)}$ does not have complex multiplication (by Lemma 2.1).

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 $\overline{\rho_{E_{(a,b,c)},p}}$ is unramified outside 2.

The elliptic curve $E_{(a,b,c)}$ is a $\mathbb{Q}$-curve, hence there exists a Hecke character $\varkappa$ (unramified outside primes dividing $2d$) such that the twisted representation $\rho_{E_{(a,b,c)},p} \otimes \varkappa$ extends to a representation $\tilde{\rho}$ of the whole Galois group $\mathrm{Gal}_{\mathbb{Q}}$. By Serre's conjecture together with an appropriate Taylor-Wiles result, the representation $\tilde{\rho}$ is modular, i.e. there exists a modular form $f \in S_2(N, \varepsilon)$ such that $\rho_{f,\mathfrak{p}} \simeq \tilde{\rho}$. The level N depends on (a, b, c), but the conductor of the Nebetypus ε is supported only at primes dividing $2d$ by construction of the Hecke character $\varkappa$ (see [11, Theorem 4.2]).

By [11, Theorem 5.1] and [6], there exists a bound B_1 (depending only on K) such that if $p > B_1$ the residual representation $\overline{\rho_{E_{(a,b,c)},p}}$ is absolutely irreducible. In particular, for such primes p we are in the hypothesis of Ribet's lowering the level result. Then there exists a newform $g \in S_2(\tilde{N}, \varepsilon)$ 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 $2d$. Furthermore, by Lemma 3.3, we can assume that c is not divisible by 3. Looking at (1) modulo 8 it follows that c is not divisible by 2 either, hence it is divisible by some prime number q larger than 3. By Ellenberg's large image result ([6, Theorem 3.14]) the projective residual image of $\rho_{E_{(a,b,c)},p}$ is surjective, so it cannot be congruent to a modular form with complex multiplication. In particular, the form g does not have complex multiplication either so we can apply our previous results.

Let g be any newform in the space $S_2(\tilde{N}, \varepsilon)$ without complex multiplication and suppose that it is related to a solution (a, b, c) of (1). Let g^{BC} denote its base change to K. Let ℓ be an odd 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, either:

(1) 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

$$\varkappa(\mathfrak{l})a_{\mathfrak{l}}(E_{(\tilde{a},\tilde{b},\tilde{c})}) \equiv a_{\mathfrak{l}}(g^{\mathrm{BC}}) \pmod{p},$$

or

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

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 $p \mid B(\ell, g; \tilde{a}, \tilde{b}, \tilde{c})$. 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, imply 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

$$(21) \qquad\qquad p \mid \prod_{(\tilde{a},\tilde{b},\tilde{c})\in S_\ell} B(\ell, g; \tilde{a}, \tilde{b}, \tilde{c}),$$

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 (21) 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 2.11, if p is large enough, there exists an elliptic curve E_g defined over K, whose conductor divides $\tilde{N}$ such that $\overline{\rho_{E_g,p}} \simeq \overline{\rho_{E_{(a,b,c)},p}}$. 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 [8, Proposition 1.1] and also Remark 7).

The residual representation $\overline{\rho_{E_g,2}}$ 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 $\overline{\rho_{E_g,2}}$, 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 [20] 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 3.2 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 $\overline{\rho_{E_g, 2}}$ has image in a Borel subgroup, so the curve E_g also has a K-rational 2-torsion point.

Theorem 3.1 then implies that the elliptic curve E_g is in fact defined over $\mathbb{Q}$, so in particular $a_{\mathfrak{q}}(E_g) = a_{\overline{\mathfrak{q}}}(E_g)$ for all primes q splitting in $K/\mathbb{Q}$, a property that the curve $E_{(a,b,c)}$ does not satisfy, giving a contradiction. $\qquad\square$

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

Theorem 3.5. *Let d be a prime number congruent to 19 modulo 24 and such that the class number of $\mathbb{Q}(\sqrt{-d})$ 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 3.4, in particular all results of Section 2 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 [8, Lemma 3.2].

(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 [11, Remark 2]). 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 2.11), 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, $a_{\mathfrak{p}}(\widetilde{E}_{(a,b,c)})$ is divisible by 3. Using Lemma 3.2 we know that $a_{\mathfrak{p}}(\widetilde{E}_{(a,b,c)}) = a_{\mathfrak{p}}(\tilde{E}_g)$ for all small prime ideals $\mathfrak{q}$. In particular, $a_{\mathfrak{q}}(\tilde{E}_g) \equiv 0 \pmod 3$ for all small prime ideals, hence by the so called "Sturm" bound (see for example Corollary 9.20 of [19]), the congruence holds for all prime ideals of good reduction. Then by [10, Theorem 2] there exists a curve E' over K which is isogenous to $\tilde{E}_g$ over K which has a rational point.

Under our hypothesis ($d \equiv 19 \pmod{24}$), the primes 2 and 3 are inert in $K/\mathbb{Q}$. The hypothesis on the class number of K being odd implies in particular that d is a prime number. Then there must 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 a E' has even valuation at $(\sqrt{-d})$.
- The curve E' has a K-rational 3-torsion point.

17

Take a semi-global minimal model for E' which is minimal at all primes except one extra prime ideal $\mathfrak{p}$ which does not divide $6d$. After a translation (a transformation which preserves the discriminant of the equation) we can assume that the rational 3-torsion point is the origin $(0,0)$. The fact that $(0,0)$ is now an inflection point of the cubic implies that the tangent line is of the form $y = \alpha x$ for some integral element α, so the change of variables $y' = y - \alpha x$, $x' = x$ (which preserves the discriminant) 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

$$E' : y^2 + a_1 xy + a_3 y = x^3,$$

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

(22) $$\Delta(E') = a_3^3(a_1^3 - 27a_3) = \pm 2^r 3^q d^s.$$

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 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 (22) is 4, hence $s = 2$ and we get the equation

(23) $$\beta^3(d\alpha^3 + 27\beta) = \pm 2^r 3^q.$$

Once again, α and β must be integers. Recall that by Ogg's formula, because the primes 2 and 3 are unramified at $K/\mathbb{Q}$, $r \leq 16$ and $q \leq 13$ (see [18] Theorem 10.4, Theorem 11.1 and Table 4.1 in page 365). 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, which (as in Theorem 3.4) contradicts the fact that $\widetilde{E}_{(a,b,c)}$ is a $\mathbb{Q}$-curve (not isogenous to a rational one, since (a,b,c) is non-trivial). $\qquad\square$

References

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

[2] David A. Cox. *Primes of the form $x^2 + ny^2$*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication.

[3] Mehmet Haluk Şengün and Samir Siksek. On the asymptotic Fermat's last theorem over number fields. *Comment. Math. Helv.*, 93(2):359–375, 2018.

[4] Pierre Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, (43):273–307, 1974.

[5] Luis Dieulefait and Jorge Jiménez Urroz. Solving Fermat-type equations via modular $\mathbb{Q}$-curves over polyquadratic fields. *J. Reine Angew. Math.*, 633:183–195, 2009.

[6] Jordan S. Ellenberg. Galois representations attached to $\mathbb{Q}$-curves and the generalized Fermat equation $A^4 + B^2 = C^p$. *Amer. J. Math.*, 126(4):763–787, 2004.

[7] Nuno Freitas, Alain Kraus, and Samir Siksek. Class field theory, Diophantine analysis and the asymptotic Fermat's last theorem. *Adv. Math.*, 363:106964, 37, 2020.

[8] Franco Golfieri, Ariel Pacetti, and Lucas Villagra Torcomian. On the equation $x^2 + dy^6 = z^p$ for square-free $1 \leq d \leq 20$, 2021. arXiv:2109.07291, to appear in the International Journal of Number Theory.

[9] Erich Hecke. *Mathematische Werke*. Vandenhoeck & Ruprecht, Göttingen, 1970. Mit einer Vorbemerkung von B. Schoenberg, einer Anmerkung von Carl Ludwig Siegel, und einer Todesanzeige von Jakob Nielsen, Zweite durchgesehene Auflage.

[10] Nicholas M. Katz. Galois properties of torsion points on abelian varieties. *Invent. Math.*, 62(3):481–502, 1981.

[11] Ariel Pacetti and Lucas Villagra Torcomian. $\mathbb{Q}$-curves, Hecke characters and some Diophantine equations. *Math. Comp.*, 91(338):2817–2865, 2022.

[12] Elisabeth Eve Pyle. *Abelian varieties over the set of rational numbers with large endomorphism algebras and their simple components over the set of irrational numbers*. ProQuest LLC, Ann Arbor, MI, 1995. Thesis (Ph.D.)–University of California, Berkeley.

[13] Jordi Quer. Fields of definition of building blocks. *Math. Comp.*, 78(265):537–554, 2009.

[14] Kenneth A Ribet. Twists of modular forms and endomorphisms of abelian varieties. *Mathematische Annalen*, 253(1):43–62, 1980.

[15] Kenneth A. Ribet. Abelian varieties over $\mathbb{Q}$ and modular forms. In *Algebra and topology 1992 (Taejŏn)*, pages 53–79. Korea Adv. Inst. Sci. Tech., Taejŏn, 1992.

[16] Kenneth A. Ribet. Fields of definition of abelian varieties with real multiplication. In *Arithmetic geometry (Tempe, AZ, 1993)*, volume 174 of *Contemp. Math.*, pages 107–118. Amer. Math. Soc., Providence, RI, 1994.

[17] Kenneth A. Ribet. Abelian varieties over $\mathbb{Q}$ and modular forms. In *Modular curves and abelian varieties*, volume 224 of *Progr. Math.*, pages 241–261. Birkhäuser, Basel, 2004.

[18] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Grad. Texts Math.* New York, NY: Springer-Verlag, 1994.

[19] William Stein. *Modular forms, a computational approach*, volume 79 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2007. With an appendix by Paul E. Gunnells.

[20] Jesse Thorner and Asif Zaman. An explicit bound for the least prime ideal in the Chebotarev density theorem. *Algebra Number Theory*, 11(5):1135–1197, 2017.

Center for Research and Development in Mathematics and Applications (CIDMA), Department of Mathematics, University of Aveiro, 3810-193 Aveiro, Portugal
Email address: francogolfieri@ua.pt

Center for Research and Development in Mathematics and Applications (CIDMA), Department of Mathematics, University of Aveiro, 3810-193 Aveiro, Portugal
Email address: apacetti@ua.pt

FAMAF-CIEM, Universidad Nacional de Córdoba. C.P:5000, Córdoba, Argentina.
Email address: lucas.villagra@unc.edu.ar