$\mathbb{Q}$-CURVES, HECKE CHARACTERS AND SOME DIOPHANTINE EQUATIONS II.

ARIEL PACETTI AND LUCAS VILLAGRA TORCOMIAN

ABSTRACT. In the article [PT20] a general procedure to study solutions of the equations $x^4 - dy^2 = z^p$ was presented for negative values of d. The purpose of the present article is to extend our previous results to positive values of d. On doing so, we give a description of the extension $\mathbb{Q}(\sqrt{d}, \sqrt{\epsilon})/\mathbb{Q}(\sqrt{d})$ (where ϵ is a fundamental unit) needed to prove the existence of a Hecke character over $\mathbb{Q}(\sqrt{d})$ with fixed local conditions. We also extend some "large image" results regarding images of Galois representations coming from $\mathbb{Q}$-curves (due to Ellenberg in [Ell04]) from imaginary to real quadratic fields.

INTRODUCTION

The study of solutions of Diophantine equations has been a very active research field since Wile's proof of Fermat's last theorem. There are still many open conjectures on understanding solutions of a generalized equation

$$Ax^p + By^q = Cz^r,$$

for $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$. A particular interesting example occurs for exponents $(p, q, r) = (4, 2, r)$ and $(A, B, C) = (1, 1, 1)$ studied by Darmon and Ellenberg independently (see [Ell04]). The Frey curve attached to a solution of such an equation happens to be a so called $\mathbb{Q}$-curve, having the special property that (a twist of) its Galois representation descends to $\mathbb{Q}$. Then one can follow the classical approach to compute (via a lowering the level argument) a fixed space of level N and weight two modular forms (with a Nebentypus ε) and try to discard the ones that cannot match a possible solution (due to a so called "local" obstruction). In [PT20] the generalized curve

$$x^4 - dy^2 = z^p \tag{1}$$

was studied for different negative values of d. The novelty was to use the theory of Hecke characters over imaginary quadratic fields to give a precise formula for the value of N and the character ε. A natural question is the following: what happens if we take positive values of d?

As explained in [DU09], to a primitive solution (A, B, C) of (1) one associates the elliptic curve

$$E_{(A,B)} : y^2 = x^3 + 4Ax^2 + 2(A^2 + rB)x, \tag{2}$$

where $r^2 = d$ over the field $K = \mathbb{Q}(\sqrt{d})$. When d is positive (and not a square) K is a real quadratic field. It is known that all elliptic curves over real quadratic fields are modular ([FLHS15]) hence one can follow the classical approach working with Hilbert modular forms. It turns out that such approach becomes impractical very soon, due to the huge dimension of the corresponding spaces. However, the $\mathbb{Q}$-curves approach is still practical in many circumstances, which motivates the present article. This article should be thought as a continuation of our previous one, where we settle the following problems:

- Prove the existence of Hecke characters over real quadratic fields with prescribed local behavior.
- Give a precise recipe for the level N and the Nebentypus ε.
- Show how Ellenberg's "large image" result can be adapted (under some hypothesis) to real quadratic fields and discard modular forms with complex multiplication.
- Explain why the case d positive is harder due to potential existence of non-trivial solutions for all exponents p.

2010 *Mathematics Subject Classification.* 11D41,11F80.
Key words and phrases. $\mathbb{Q}$-curves, Diophantine equations.

Section 4 contains different examples aiming to explain the difference between the Hilbert/$\mathbb{Q}$-curves computational effort. We also explain why in some cases there exist non-trivial solutions of (1) with $C = \pm 1$, which are valid for all exponents p, making the modular approach to fail. At last, we explain why when there are modular forms with complex multiplication, classical results give a partial result for all primes satisfying some congruence. We provide an example ($d = 3 \cdot 43$) where Ellenberg's large image result applies, and a non-existence result for all large enough primes can be obtained.

The article is organized as follows: after a quick review of the strategy developed in [PT20], Section 1 solves the first problem described above, namely the existence of a Hecke character with the desired properties. The good definition of the character is related to a very interesting problem of class field theory, namely suppose that $K = \mathbb{Q}(\sqrt{d})$ is a real quadratic field, and ϵ is a totally positive fundamental unit congruent to 1 modulo 8 (such assumption is for expository purposes only, we consider the general case in the article). Then the extension $K(\sqrt{\epsilon})$ is a quadratic unramified extension of K, hence it corresponds to a genus character. Is there a natural description for such character? Can the extension $K(\sqrt{\epsilon})$ be described in terms of d?

We give a positive answer to this problem, which plays a crucial role in the proof of the good definition of our Hecke character. The second section settles the second issue, namely it gives a precise recipe for N and ε. A proof of such statement was given in [PT20] when K is imaginary quadratic, since the Nebentypus had a unique candidate due to the fact that it was odd. For real quadratic fields, the hard part is to prove the formula for the Nebentypus! We do so by computing explicitly an action on 3-torsion points. The proof might be of independent interest.

The third section gives an explicit version of Ellenberg's result for real quadratic fields where the prime 2 splits. The proof follows from an "explicit" version of the main result of [LF17]; our little contribution being making the constants explicit. The last section contains the examples, were the cases $d = 6$ and $d = 129$ are specially considered along with other values of d between 1 and 20. We prove the following results:

Theorem 4.1. *Let $p > 19$ such that $p \neq 97$ and $p \equiv 1, 3 \pmod 8$. Then, $(\pm 7, \pm 20, 1)$ are the only non-trivial solutions of the equation*

$$x^4 - 6y^2 = z^p.$$

Theorem 4.2. *Let $p > 19$ be a prime number satisfying that either $p > 64690$ or $p \equiv 1, 3 \pmod 8$. Then there are no non-trivial solutions of the equation*

$$x^4 - 129y^2 = z^p.$$

We want to remark that the techniques and methods developed in the present article can be used to study the equation $x^2 - dy^6 = z^p$ for positive values of d following the results of [PT20].

Acknowledgments. We would like to thank Yingkun Li for sharing with us a proof of Theorem 1.2 and to Harald Helfgott for providing some bounds used in Section 3. This research was partially supported by FonCyT BID-PICT 2018-02073 and by the Portuguese Foundation for Science and Technology (FCT) within project UIDB/04106/2020 (CIDMA).

1. Construction of the Hecke character

The elliptic curve $E_{(A,B)}$ is what is called a $\mathbb{Q}$-curve, namely its Galois conjugate is isogenous (via the order 2 isogeny whose kernel is the point $(0, 0)$) to itself. The problem is that the isogeny is not defined over K but over $K(\sqrt{-2})$, hence the Galois representation $\rho_{E,p}$ does not extend to a 2-dimensional representation of $\mathrm{Gal}_{\mathbb{Q}}$. Let τ be an element of $\mathrm{Gal}_{\mathbb{Q}}$ whose restriction to K is not the identity and let δ_{-2} denote the quadratic character of $\mathrm{Gal}_{\mathbb{Q}}$ corresponding to the extension $\mathbb{Q}(\sqrt{-2})/\mathbb{Q}$. If $\chi : \mathrm{Gal}_K \to \mathbb{C}^\times$ is a Hecke character satisfying ${}^\tau\chi(\sigma) := \chi(\tau\sigma\tau^{-1}) = \chi(\sigma)\delta_{-2}(\sigma)$ then the twisted representation $\rho_{E,p} \otimes \chi$ does extend to a 2-dimensional representation of $\mathrm{Gal}_{\mathbb{Q}}$. The main strategy of [PT20] was to give an explicit construction for such a character. From the short exact sequence

$$0 \longrightarrow K^\times \cdot (\textstyle\prod_{\mathfrak{q}} \mathcal{O}_{\mathfrak{q}}^\times \times (\mathbb{R}^\times)^2) \longrightarrow \mathbb{I}_K \longrightarrow \mathrm{Cl}(K) \longrightarrow 0, \tag{3}$$

it is enough to define the character on $\prod_{\mathfrak{q}} \mathcal{O}_{\mathfrak{q}}^\times \times (\mathbb{R}^\times)^2$, on $K^\times$ (where the character is trivial) and on idèles representing the class group of K. The intersection of these two subgroups $(\prod_{\mathfrak{q}} \mathcal{O}_{\mathfrak{q}}^\times \times (\mathbb{R}^\times)^2) \cap K^\times = \mathcal{O}_K^\times$ imposes a *compatibility* condition on its definition, namely the product of the local components evaluated at

a unit equals 1. When $d>0$ the ring $\mathcal{O}_K^\times = \langle -1, \epsilon\rangle$, where ϵ denotes a fundamental unit, hence it is enough to check compatibility at both such elements (the compatibility was proven in [PT20, Theorem 2.2] when the fundamental unit has norm -1, so we assume that ϵ is totally positive).

Let us briefly recall the construction given in [PT20] (there is a discrepancy with the definitions used in [PT20], namely d needs to be changed to $-d$ in such article). Split the odd prime divisors of d into four different sets, namely:

$$Q_i = \{p \text{ prime } : \ p \mid d, \quad p \equiv i \pmod 8\},$$

for $i = 1, 3, 5, 7$. Let δ_{-1}, δ_2, δ_{-2} be the characters of $\mathbb{Z}$ corresponding to the quadratic extensions $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$ respectively and (abusing notation) let δ_{-1}, δ_2, δ_{-2} also denote their local component at the prime 2. Define a character $\varepsilon : \mathbb{I}_\mathbb{Q} \to \overline{\mathbb{Q}}^\times$ (that will be the Nebentypus of the Galois representation extension) as follows:

- For primes $p \in Q_1 \cup Q_7$, the character $\varepsilon_p : \mathbb{Z}_p^\times \to \mathbb{C}^\times$ is trivial.
- For primes $p \in Q_3$, the character $\varepsilon_p(n) = \left(\frac{n}{p}\right)$ (quadratic).
- For $p \in Q_5$, let ε_p be a character of order 4 and conductor p.
- The character ε_∞ (the archimidean component) is trivial.
- Define $\varepsilon_2 = \delta_{-1}^{\#Q_3+\#Q_5}$.

This gives a well defined Hecke character ε of $\mathbb{I}_\mathbb{Q}$ corresponding to a totally real field L whose degree equals 1 if $Q_3 = Q_5 = \emptyset$, 2 if $Q_3 \neq Q_5 = \emptyset$ and 4 otherwise. By class field theory, ε gets identified with a character $\varepsilon : G_\mathbb{Q} \to \overline{\mathbb{Q}}$. Let N_ε denote its conductor, given by $N_\varepsilon = 2^e \prod_{p\in Q_3\cup Q_5} p$, where $e = 0$ if $\#Q_5 + \#Q_7$ is even and 2 otherwise.

Theorem 1.1. *There exists a Hecke character $\chi : \mathrm{Gal}_K \to \overline{\mathbb{Q}}$ such that:*

(1) $\chi^2 = \varepsilon$ as characters of Gal_K,
(2) χ is unramified at primes not dividing $2\prod_{p\in Q_1\cup Q_5\cup Q_7} p$,
(3) for τ in the above hypothesis, ${}^\tau\chi = \chi\cdot\psi_{-2}$ as characters of Gal_K.

Furthermore, its conductor equals $2^a \prod_{p\in Q_1\cup Q_5\cup Q_7} \mathfrak{p}$, where

$$a = \begin{cases} 3 & \text{if } d \equiv 5 \pmod 8, \\ 5 & \text{if } d/4 \equiv 3 \pmod 4, \\ 0 & \text{if } d/4 \equiv 14 \pmod{16}, \\ 4 & \text{if } d/4 \equiv 6 \pmod{16}, \\ 3 & \text{if } d/4 \equiv 2 \pmod{16}, \\ 4 & \text{if } d/4 \equiv 10 \pmod{16}, \end{cases}$$

The theorem was proved in [PT20] (Theorem 2.1) for $d<0$ and for $d>0$ when the fundamental unit ϵ has norm -1. The main obstacle in the remaining case is to have some understanding on the reduction of a positive fundamental unit modulo ramified primes of K. Let us state the following related natural problem.

Problem: Let $K/\mathbb{Q}$ be a real quadratic field, and let ϵ be a totally positive fundamental unit. What can be said of the extension $K(\sqrt{\epsilon})/K$?

Suppose that $K = \mathbb{Q}(\sqrt{d})$ with d a positive fundamental discriminant. Let $p \mid d$ be an odd prime and let $\mathfrak{p}$ denote the unique prime ideal of K dividing it. The hypothesis $\mathcal{N}(\epsilon) = 1$ implies that $\epsilon \equiv \pm 1 \pmod{\mathfrak{p}}$. Let

$$\mathcal{P}_\delta = \{p \mid d, \ p \text{ odd} \ : \ \epsilon \equiv \delta \pmod{\mathfrak{p}}\},$$

where $\delta = \pm 1$. If 2 ramifies in $K/\mathbb{Q}$, let $\mathfrak{p}_2$ denote the unique prime of K dividing it.

Theorem 1.2. *Let $d_0 := \prod_{p\in\mathcal{P}_-} p$. Then if 2 is unramified in $K/\mathbb{Q}$, $K(\sqrt{\epsilon}) = K(\sqrt{d_0})$ while if 2 is ramified in $K/\mathbb{Q}$, $K(\sqrt{\epsilon}) = K(\sqrt{2d_0})$ or $K(\sqrt{\epsilon}) = K(\sqrt{d_0})$. Furthermore, when $8 \mid d$, the later case occurs precisely when $\epsilon \equiv -1 \pmod{\mathfrak{p}_2^3}$.*

Proof. Let us recall some well known results on quadratic fields and binary quadratic forms (due mostly to Gauss [Gau86]; see also [Bue89] for a more modern presentation). There is a correspondence between strict

equivalence classes of indefinite binary quadratic forms of discriminant d and ideal classes for the narrow class group of K. The ramified prime ideals of K (indexed by divisors of d) are precisely the ideals of order 2 [Bue89, Corollary 4.9]. Under the correspondence, they match the so called "ambiguous forms" (see [Bue89] page 7 Chapter 1 and page 24 Chapter 3) The total number of ambiguous classes (including the trivial one) equals 2^{t-1}, where t is the number of prime divisors of d (by [Bue89, Proposition 4.7] and its proof). Equivalently, the number of order two ideals in the narrow class group equals 2^{t-1}. In particular, there exists a unique principal ideal $\mathcal{D}_0$ (generated by a totally positive element α) dividing the different $\mathcal{D}$ of K. Let $\mathcal{N}\mathcal{D}_0 = \mathcal{N}(\alpha) = \alpha\overline{\alpha} = d_0 \mid d$.

Since $\overline{\mathcal{D}_0} = \mathcal{D}_0$, the quotient $\frac{\alpha}{\overline{\alpha}} \in \mathcal{O}_K$ is a totally positive unit hence equals ϵ^k for some integer k. Substituting α by $\epsilon^k\alpha$ changes the quotient $\frac{\alpha}{\overline{\alpha}}$ by a factor of ϵ^{2k}, hence we can assume that

$$\frac{\alpha}{\overline{\alpha}} = \epsilon \tag{4}$$

(clearly such quotient cannot be trivial). Then $\sqrt{\epsilon} = \frac{\sqrt{\alpha\overline{\alpha}}}{\overline{\alpha}}$ and hence $K(\sqrt{\epsilon}) = K(\sqrt{d_0})$. We are led to determine the set of primes dividing d_0. Let $\mathfrak{p}$ be a prime ideal dividing $\mathcal{D}$ and assume that $\mathfrak{p} \nmid 2$.

- The fact that $\alpha + \overline{\alpha} \in \mathcal{D}_0 \cap \mathbb{Z} = (d_0)$ implies that $\alpha + \overline{\alpha} \in \mathcal{D}_0^2$, hence $\epsilon + 1 = \frac{\alpha}{\overline{\alpha}} + 1 = \frac{\alpha+\overline{\alpha}}{\alpha} \in \mathcal{D}_0$ hence $\epsilon \equiv -1 \pmod{\mathcal{D}_0}$. In particular, $\epsilon \equiv -1 \pmod{\mathfrak{p}}$ for all odd prime ideals $\mathfrak{p} \mid \mathcal{D}_0$.
- On the other hand, if $\mathfrak{p} \mid \mathcal{D}$ but $\mathfrak{p} \nmid \mathcal{D}_0$ (in particular $\mathfrak{p} \nmid \alpha$), $\epsilon - 1 = \frac{\alpha-\overline{\alpha}}{\alpha} \equiv 0 \pmod{\mathfrak{p}}$ hence $\epsilon \equiv 1 \pmod{\mathfrak{p}}$.

If $2 \nmid d$ then d_0 is odd and the statement follows, while if d is even the only ambiguity is whether d_0 is even or not. Suppose that $8 \mid d$, so $\alpha = a + b\sqrt{d/4}$ with $a, b \in \mathbb{Z}$. Let $\mathfrak{p}$ denote the prime ideal dividing 2 ($\mathfrak{p} = \langle 2, \sqrt{d/4}\rangle$). Clearly $v_\mathfrak{p}(\alpha) = v_\mathfrak{p}(\bar{\alpha}) = v_2(d_0)$. An elementary case by case analysis shows that $v_\mathfrak{p}(\alpha) \in \{0, 2\}$ if and only if $v_\mathfrak{p}(\epsilon - 1) \geq 3$ and $v_\mathfrak{p}(\epsilon + 1) = 2$. Similarly, $v_\mathfrak{p}(\alpha) \in \{1, 3\}$ if and only if $v_\mathfrak{p}(\epsilon + 1) \geq 3$ and $v_\mathfrak{p}(\epsilon - 1) = 2$ as stated. □

Proof of Theorem 1.1. If $\mathfrak{p}$ is a prime ideal of K, let $\mathcal{O}_\mathfrak{p}$ denote the completion of $\mathcal{O}_K$ at $\mathfrak{p}$. Let $\chi_p : \mathcal{O}_\mathfrak{p}^\times \to \mathbb{C}^\times$ be the character given by

- If $\mathfrak{p}$ is an odd (i.e. $\mathfrak{p} \nmid 2$) unramified prime, $\chi_\mathfrak{p}$ is the trivial character. The same applies to primes in K dividing the primes in Q_3.
- If p is an odd prime ramifying in $K/\mathbb{Q}$ and $\mathfrak{p} \mid p$, clearly $(\mathcal{O}_\mathfrak{p}/\mathfrak{p})^\times \simeq (\mathbb{Z}/p)^\times$. If $p \in Q_1 \cup Q_7$, let $\chi_\mathfrak{p}$ correspond to the quadratic character δ_p of $(\mathbb{Z}/p)^\times$.
- If $p \in Q_5$, using the previous item isomorphism, let $\chi_\mathfrak{p} = \varepsilon_p \cdot \delta_p$.

At the archimidean places $\{v_1, v_2\}$, let χ_{v_1} be the trivial character and χ_{v_2} be the sign function (the order of the archimidean places does not matter, both choices work). At a prime $\mathfrak{p}$ dividing 2, the character $\chi_\mathfrak{p}$ has conductor at most 2^3; its definition on a set of generators of $\mathcal{O}_K/2^3$ is the following:

- If $d \equiv 1 \pmod 8$, the prime 2 splits as $2 = \mathfrak{p}_2\overline{\mathfrak{p}_2}$. Let $\chi_{\mathfrak{p}_2} := \delta_{-2}$ and $\chi_{\overline{\mathfrak{p}_2}} := 1$ (trivial) or take $\chi_{\mathfrak{p}_2} := \delta_2$ and $\chi_{\overline{\mathfrak{p}_2}} := \delta_{-1}$. To make the proofs consistent, we denote by $\chi_2 = \chi_{\mathfrak{p}_2}\chi_{\overline{\mathfrak{p}_2}} = \delta_{-2}$.
- If $d \equiv 5 \pmod 8$, $\chi_\mathfrak{p}(\zeta_3) = 1$, $\chi_\mathfrak{p}(\sqrt{d}) = i$, $\chi_\mathfrak{p}(3 + 2\sqrt{d}) = 1$, $\chi_\mathfrak{p}(-1) = 1$.
- If $d/4 \equiv 7 \pmod{16}$, $\chi_\mathfrak{p}(\sqrt{d/4}) = -1$, $\chi_\mathfrak{p}(1 + 2\sqrt{d/4}) = 1$, $\chi_\mathfrak{p}(5) = -1$.
- If $d/4 \equiv 15 \pmod{16}$, $\chi_\mathfrak{p}(\sqrt{d/4}) = 1$, $\chi_\mathfrak{p}(1 + 2\sqrt{d/4}) = 1$, $\chi_\mathfrak{p}(5) = -1$.
- If $d/4 \equiv 3 \pmod{16}$, $\chi_\mathfrak{p}(\sqrt{d/4}) = -1$, $\chi_\mathfrak{p}(1 + 2\sqrt{d/4}) = 1$, $\chi_\mathfrak{p}(-1) = -1$.
- If $d/4 \equiv 11 \pmod{16}$, $\chi_\mathfrak{p}(\sqrt{d/4}) = 1$, $\chi_\mathfrak{p}(1 + 2\sqrt{d/4}) = 1$, $\chi_\mathfrak{p}(-1) = -1$.
- If $d/4 \equiv 6 \pmod 8$ and $\#Q_3 + \#Q_5$ is even, $\chi_\mathfrak{p}(1 + \sqrt{d/4}) = 1$, $\chi_\mathfrak{p}(-1) = 1$.
- If $d/4 \equiv 6 \pmod 8$ and $\#Q_3 + \#Q_5$ is odd, $\chi_\mathfrak{p}(1 + \sqrt{d/4}) = i$, $\chi_\mathfrak{p}(-1) = -1$
- If $d/4 \equiv 2 \pmod 8$ and $\#Q_3 + \#Q_5$ is even, $\chi_\mathfrak{p}(1 + \sqrt{d/4}) = 1$, $\chi_\mathfrak{p}(-1) = -1$.
- If $d/4 \equiv 2 \pmod 8$ and $\#Q_3 + \#Q_5$ is odd, $\chi_\mathfrak{p}(1 + \sqrt{d/4}) = i$, $\chi_\mathfrak{p}(-1) = 1$.

It is important to notice that in all cases

$$\chi_2|_{\mathbb{Z}_2^\times} = \delta_2^{v_2(d)+1}\delta_{-1}^{\#Q_5+\#Q_7+1}. \tag{5}$$

Extend χ to $K^\times \cdot (\prod_\mathfrak{q} \mathcal{O}_\mathfrak{q}^\times \times \mathbb{C}^\times)$ by making it trivial on $K^\times$. It is easy to verify that $\chi^2 = \varepsilon \circ \mathcal{N}$.

Compatibility: the subgroup of units in K is generated by $\{-1, \epsilon\}$ hence it is enough to prove the compatibility at both elements. Replacing d by $-d$ we interchange real quadratic fields with imaginary quadratic ones. The local part of the character χ is invariant under such transformation for all odd primes, but not at primes dividing 2. For such places, the restriction of the local character to $\mathbb{Z}_2^\times$ differs by δ_{-1}. In [PT20, Theorem 2.1] we proved the compatibility at -1 for imaginary quadratic fields K; since $\delta_{-1}(-1) = -1$, the compatibility relation for real quadratic fields at -1 follows from the extra sign coming from the archimedean contribution.

Proving the compatibility for ϵ takes more effort. The character $\chi_p(\epsilon) = 1$ for all unramified primes and for primes in $\mathcal{P}_- \cap (Q_1 \cup Q_3)$. Its value at primes in $\mathcal{P}_- \cap (Q_5 \cup Q_7)$ equals -1 hence we need to prove the following identity

$$\chi_2(\epsilon) \cdot (-1)^{\#(\mathcal{P}_- \cap (Q_5 \cup Q_7))} = \chi_2(\epsilon)\delta_{-2}(d_0) = 1, \tag{6}$$

where $d_0 = \prod_{p \in \mathcal{P}_-} p$ as before. The proof of Theorem 1.2 implies that there exists $\alpha \in \mathcal{O}_K$ such that $d_0 = \epsilon\overline{\alpha}^2$ or $2d_0 = \epsilon\overline{\alpha}^2$. In the first case,

$$\chi_2(\overline{\alpha}^2) = \chi_2^2(\overline{\alpha}) = \varepsilon_2(\mathcal{N}(\alpha)) = \varepsilon_2(d_0).$$

Since ε_2 is at most quadratic, it equals its inverse hence $\chi_2(\epsilon) = \chi_2(d_0)\varepsilon_2(d_0)$, then equation (6) is equivalent to the statement

$$\chi_2(d_0)\varepsilon_2(d_0)\delta_{-2}(d_0) = 1. \tag{7}$$

A key fact is that the hypothesis $\mathcal{N}(\alpha) = d_0$ imposes a constrain on its possible values. Using equation (5), the proof follows from the following case by case study:

- If $d \equiv 1 \pmod 8$, then $\chi_2 = \delta_{-2}$ and ε_2 is trivial hence (7) holds.
- If $d/4 \equiv 3 \pmod 8$, the norm condition implies that d_0 is congruent to 1 or 5 modulo 8. By definition $\chi_2|_{\mathbb{Z}_2^\times} = \delta_{-2}$ and $\varepsilon_2 = \delta_{-1}$, which is trivial on both $1, 5$ hence (7) holds.
- If $d \equiv 5 \pmod 8$, by definition $\chi_2|_{\mathbb{Z}_2^\times} = \delta_2$ and $\varepsilon_2 = \delta_{-1}$ hence (7) holds.
- If $d/4 \equiv 7 \pmod 8$, the norm condition implies that d_0 is congruent to 1 or 5 modulo 8. By definition $\chi_2|_{\mathbb{Z}_2^\times} = \delta_2$ and $\varepsilon_2 = 1$. But $\delta_2 = \delta_{-2}$ take the same values at $\{1, 5\}$ hence (7) holds.
- If $d/4 \equiv 2 \pmod 8$, the norm condition implies that d_0 is congruent to 1 or 7 modulo 8. By definition $\chi_2|_{\mathbb{Z}_2^\times} \cdot \varepsilon_2 = \delta_{-1}$, which coincides with δ_{-2} on $\{1, 7\}$ hence (7) holds.
- If $d/4 \equiv 6 \pmod 8$, the norm condition implies that d_0 is congruent to 1 or 3 modulo 8. By definition $\chi_2|_{\mathbb{Z}_2^\times} \cdot \varepsilon_2 = 1$ but δ_{-2} is trivial on $\{1, 3\}$ hence (7) holds.

If d is odd, the equality $d_0 = \epsilon\bar{\alpha}^2$ always holds hence the result follows. Assume then that 2 ramifies in $K/\mathbb{Q}$ and that $2d_0 = \epsilon\bar{\alpha}^2$. Let $\mathfrak{p}_2$ denote the unique prime of K dividing 2. To easy notation, let $\tilde{d} = d/4$. Recall that $K(\sqrt{\epsilon})$ is unramified at $\mathfrak{p}_2$ if and only if $\epsilon \equiv \square \pmod 4$ (see for example [CP19, Lemma 3.4]). The equality $2d_0 = \epsilon\overline{\alpha}^2$ implies that

$$\left(\frac{2}{\overline{\alpha}}\right)^2 d_0 = 2\epsilon. \tag{8}$$

Note that $\frac{2}{\overline{\alpha}}$ has positive valuation at $\mathfrak{p}_2$, hence we can reduce equality (8) modulo 16 to compute for each possible value of ϵ the corresponding value of d_0 (up to squares) via a finite computation. Not all elements of $(\mathcal{O}_K/8)^\times$ do correspond to a possible value of ϵ, since the fact that $K(\sqrt{\epsilon})/\mathbb{Q}$ is biquadratic imposes a big constrain. Before presenting the results of the finite computation, note the following: if $d_1 \equiv d_2 \pmod{16}$, then $\mathbb{Z}[\sqrt{d_1}]/2^4 \simeq \mathbb{Z}[\sqrt{d_2}]/2^4$ (as rings) via the natural map sending $\sqrt{d_1}$ to $\sqrt{d_2}$. Applying it to equality (8) proves that the value d_0 attached to a fundamental unit of the form $a + b\sqrt{d_1}$ equals that of $a + b\sqrt{d_2}$. In particular, it is enough to perform the finite computation for $\tilde{d}$ modulo 16.

If $\tilde{d} \equiv 3 \pmod 4$ and $t \mid d$ the extension $K(\sqrt{t})$ is ramified at $\mathfrak{p}_2$ precisely when t is even (and not divisible by 4). Then under our hypothesis, the extension $K(\sqrt{\epsilon})/K$ is ramified at $\mathfrak{p}_2$. Take $\{\sqrt{d}/2, 1 + \sqrt{d}, -1\}$ as generators for the group of invertible elements modulo 16. Consider the different cases:

- If $\tilde{d} \equiv 3, 7 \pmod{16}$, the possible values for ϵ (given as generators' exponents) and the values of d_0 are given in Table 1.1. Since $\chi_2((a, b, c)) = (-1)^{a+c}$ (again as exponents) the equality $\chi_2(\epsilon) = \delta_{-2}(d_0)$ follows recalling that $\delta_{-2}(1) = \delta_{-2}(3) = 1$ and $\delta_{-2}(5) = \delta_{-2}(7) = -1$.

$\tilde{d} \pmod{16}$	Exp.	d_0	Exp.	d_0	Exp.	d_0	Exp.	d_0
3	$(1,1,0)$	$\{5,7\}$	$(1,1,1)$	$\{1,3\}$	$(1,3,0)$	$\{5,7\}$	$(1,3,1)$	$\{1,3\}$
3	$(3,1,0)$	$\{5,7\}$	$(3,1,1)$	$\{1,3\}$	$(3,3,0)$	$\{5,7\}$	$(3,3,1)$	$\{1,3\}$
7	$(1,0,0)$	5	$(1,0,1)$	1	$(1,2,0)$	5	$(1,2,1)$	1
7	$(3,0,0)$	5	$(3,0,1)$	1	$(3,2,0)$	5	$(3,2,1)$	1

TABLE 1.1. Relation ϵ and d_0 for $\tilde{d} \equiv 3, 7 \pmod{16}$

- If $\tilde{d} \equiv 11, 15 \pmod{16}$ the possible values for ϵ and the values of d_0 are given in Table 1.2. Since $\chi_2((a,b,c)) = (-1)^c$ in this case, the equality $\chi_2(\epsilon) = \delta_{-2}(d_0)$ holds.

$\tilde{d} \pmod{16}$	Exp.	d_0	Exp.	d_0	Exp.	d_0	Exp.	d_0
11	$(1,1,0)$	$\{1,3\}$	$(1,1,1)$	$\{5,7\}$	$(1,3,0)$	$\{1,3\}$	$(1,3,1)$	$\{5,7\}$
11	$(3,1,0)$	$\{1,3\}$	$(3,1,1)$	$\{5,7\}$	$(3,3,0)$	$\{1,3\}$	$(3,3,1)$	$\{5,7\}$
15	$(1,0,0)$	1	$(1,0,1)$	5	$(1,2,0)$	1	$(1,2,1)$	5
15	$(3,0,0)$	1	$(3,0,1)$	5	$(3,2,0)$	1	$(3,2,1)$	5

TABLE 1.2. Relation ϵ and d_0 for $\tilde{d} \equiv 11, 15 \pmod{16}$

When $8 \mid d$, Theorem 1.2 implies that the case $2d_0 = \epsilon\bar{\alpha}^2$ occurs precisely for $\epsilon \equiv -1 \pmod{\mathfrak{p}_2^3}$. Recall that $(\mathcal{O}_K/2^3)^\times$ is generated by the elements $\{-1, 5, 1+\sqrt{d/4}\}$ (of order $2, 2, 8$). Using the congruence of ϵ modulo $\mathfrak{p}_2^3$, the condition (8) and the fact that $2d_0$ is the norm of an element, we search for all possible values of ϵ and d_0.

- If $\tilde{d} \equiv 2 \pmod{16}$ (respectively $d \equiv 10 \pmod{16}$) then $\#Q_3 + \#Q_5$ even (respectively odd). The assumption that $2d_0$ is a norm implies that $d_0 \equiv 1, 7 \pmod 8$ (respectively $d_0 \equiv 3, 5 \pmod 8$). All the possibles values of ϵ for each d_0 are given in Table (1.3) from which it follows that (6) holds.

$\tilde{d} \pmod{16}$	ϵ	d_0	ϵ	d_0	ϵ	d_0	ϵ	d_0
2	-1	7	$(1+\sqrt{d})^2$	1	$-(1+\sqrt{d})^4$	7	$(1+\sqrt{d})^6$	1
10	-1	3	$(1+\sqrt{d})^2$	5	$-(1+\sqrt{d})^4$	3	$(1+\sqrt{d})^6$	5
6	-1	5	$5(1+\sqrt{d})^2$	7	$-(1+\sqrt{d})^4$	5	$5(1+\sqrt{d})^6$	7

TABLE 1.3. Relation ϵ and d_0 for $\tilde{d} \equiv 2, 6, 10 \pmod{16}$

- If $\tilde{d} \equiv 6 \pmod{16}$ then $\#Q_3 + \#Q_5$ is odd. The norm condition implies that $d_0 \equiv 1, 7 \pmod 8$. The possibles values of ϵ and d_0 are given in Table (1.3).
- If $\tilde{d} \equiv 14 \pmod{16}$ then $\#Q_3 + \#Q_5$ is even, hence χ_2 is trivial. The norm condition implies that $d_0 \equiv 1, 3 \pmod 8$ so formula (6) holds.

Once the compatibility is verified, the proof of Theorem 2.1 in [PT20] works mutatis mutandis. □

2. The conductor and Nebentypus of the extended representation

The properties imposed on χ imply that the twisted representation $\rho_{E,\ell} \otimes \chi$ extends to a 2-dimensional representation of $\mathrm{Gal}_{\mathbb{Q}}$.

Theorem 2.1. *Suppose there exists a prime $p > 3$ ramifying in K. Then the twisted representation $\rho_{E,\ell} \otimes \chi$ descends to a 2-dimensional representation of $\mathrm{Gal}_{\mathbb{Q}}$ attached to a newform of weight 2, Nebentypus ε and level N given by*

$$N = 2^e \prod_q q^{v_q(N_E)} \cdot \prod_{q \in Q_3} q \cdot \prod_{q \in Q_1 \cup Q_5 \cup Q_7} q^2,$$

where the product is over odd primes, and $\mathfrak{q}$ *denotes a prime of* K *dividing* q*. The value of* e *is one of:*

$$e = \begin{cases} 1, 8 & \text{if } 2 \text{ splits}, \\ 8 & \text{if } 2 \text{ is inert}, \\ 6, 7 & \text{if } 2 \text{ ramifies but } 2 \nmid d, \\ 8, 9 & \text{if } 2 \mid d. \end{cases}$$

Proof. The extension result is well known although a proof was recalled in [PT20, Theorem 2.3]. To easy notation let $\rho'_\ell = \rho_{E,\ell} \otimes \chi$ and $\tilde{\rho}_\ell$ denote its extension to $\mathrm{Gal}_{\mathbb{Q}}$. The Nebentypus assertion was only proved under the hypothesis that $K/\mathbb{Q}$ is quadratic imaginary. The reason is the following: we know that ρ' has determinant the cyclotomic character times ε, hence the determinant of $\tilde{\rho}_\ell$ equals (up to the cyclotomic factor) ε or $\varepsilon \cdot \delta_K$ (where δ_K denotes the quadratic character corresponding to the extension $K/\mathbb{Q}$). But Ribet's result ([Rib04]) implies that the determinant of $\tilde{\rho}$ is even hence the statement. When $K/\mathbb{Q}$ is real quadratic both characters take the same value at complex conjugation! The solution is to work with other element of the inertia group of $K/\mathbb{Q}$.

Let S denote the set of primes ramifying in $K/\mathbb{Q}$, and for each odd $p \in S$ let $\mathfrak{p}$ denote the prime of K dividing it. Take ℓ an odd prime that does not belong to S. Let $I_p \subset \mathrm{Gal}_{\mathbb{Q}}$ denote an inertia subgroup at p and $I_{\mathfrak{p}}$ its index two subgroup. By [PT20, Lemma 1.3] the curve $E_{(A,B)}$ has good reduction at $\mathfrak{p}$ hence (by the Néron-Ogg-Shafarevich criterion) $\rho'|_{I_{\mathfrak{p}}}$ is a scalar matrix. Let $\sigma_p \in I_p \setminus I_{\mathfrak{p}}$ and let ${}^{\sigma_p}\rho'(\tau) := \rho'(\sigma_p^{-1}\tau\sigma_p)$. The character χ was constructed so that ${}^{\sigma_p}\rho' \simeq \rho'$, hence both representations are conjugate under a matrix of $\mathrm{GL}_2(\mathbb{Q}_\ell)$. Since $\tilde{\rho}$ extends ρ', $\tilde{\rho}(\sigma_p)$ is such a matrix. Consider the following two different cases:

- If ${}^{\sigma_p}\rho' = \rho'$, then $\tilde{\rho}(\sigma_p)$ is a scalar matrix. In particular, $\det(\tilde{\rho}(\sigma_p))$ equals the value of the scalar matrix $\tilde{\rho}(\sigma_p)^2 = \rho'(\sigma_p^2) = \chi(\sigma_p^2) = (\delta_K \cdot \varepsilon)(\sigma_p)$ (the last statement can easily be verified using the fact that σ_p is not a square). Then $\det(\tilde{\rho}) = \delta_K \cdot \varepsilon \cdot \chi_\ell$.
- If ${}^{\sigma_p}\rho' \neq \rho'$, $\tilde{\rho}(\sigma_p)^2 = \rho'(\sigma_p^2)$ is a scalar matrix, hence we can assume that $\tilde{\rho}(\sigma_p)$ equals a scalar matrix times $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and the same proof as before gives that $\det(\tilde{\rho}) = \varepsilon \cdot \chi_\ell$.

Then we are left to prove that ${}^{\sigma_p}\rho' \neq \rho'$ (a result independent of the prime $p \in S$). Recall that $\rho' = \rho \otimes \chi$, hence the statement is equivalent to prove that ${}^{\sigma_p}\rho \neq \rho \cdot \delta_{-2}$ (since ${}^{\sigma_p}\chi = \chi\delta_{-2}$). The isogeny $\phi : E_{(A,B)} \to \overline{E_{(A,B)}}$ is given by

$$\phi(x, y) = \left(\frac{-y^2}{2x^2}, \frac{y(2A^2 + 2\sqrt{d}B - x^2)}{2\sqrt{-2}x^2} \right), \tag{9}$$

hence $\tau \circ \phi = \phi \circ \tau \cdot \delta_{-2}(\tau)$ for all $\tau \in \mathrm{Gal}_K$.

Abusing notation, we will denote by ϕ the map it induces on the Galois group $\mathrm{Gal}(K(E[\ell^n])/K)$. In particular, it makes sense to talk about ϕ^{-1}, which (under our assumption ℓ odd) coincides with the map $\frac{\phi^*}{2}$ (where ϕ^* denotes the dual isogeny). Take $\ell = 3$ and n large so that the 3-adic representation modulo 3^n is absolutely irreducible. Let $\tau \in \mathrm{Gal}(K(E[3^n])/K)$, then

$$\sigma_p^{-1}\tau\sigma_p = (\phi^{-1}\sigma_p)^{-1}(\phi^{-1}\tau\phi)(\phi^{-1}\sigma_p) = \delta_{-2}(\tau)(\phi^{-1}\sigma_p)^{-1}\tau(\phi^{-1}\sigma_p). \tag{10}$$

Its action matches $\delta_{-2}(\tau)\tau$ if and only if $\phi^{-1}\sigma_p$ acts as a scalar matrix (by our absolutely irreducible hypothesis). But $\det(\phi^{-1}\sigma_p)^2 = \det(\phi^{-1}\phi\delta_{-2}\sigma_p^2) = 1$, hence $\det(\phi^{-1}\sigma_p) = \pm 1$ and since $\phi^{-1}\sigma_p$ is a scalar matrix its determinant equals 1 so $\phi^{-1}\sigma_p = \pm 1$.

Let $L = K(x(E_{(A,B)}[3]))$ denote the extension of K obtained by adding all the x-coordinates of the 3-torsion points of $E_{(A,B)}$. It is a degree 2-subextension of $K(E[3])$ invariant under ϕ (from its definition (9)) hence $L/\mathbb{Q}$ is a Galois extension. Note that multiplication by -1 acts as the identity on $\mathrm{Gal}(L/K)$, hence it is enough to prove that $\phi \neq \sigma_p$ as elements of $\mathrm{Gal}(L/\mathbb{Q})$. For a generic curve $y^2 = x^3 + ax^2 + bx$, the 3-division polynomial (whose roots generate the extension L/K) is given by

$$\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 - b^2. \tag{11}$$

An easy study of $\mathrm{PGL}_2(\mathbb{F}_3)$ shows that L contains precisely 3 degree two extensions of $\mathbb{Q}$, namely $K, \mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{-3d})$. Since the ramification degree of p in $L/\mathbb{Q}$ is two, if we prove that ϕ fixes $\sqrt{-3d}$, then L/L^ϕ is unramified at primes dividing p hence $\phi \neq \sigma_p$ as desired.

Let $\theta_1, \dots, \theta_4$ be the roots of ψ_3 and let $\bar{b} = \frac{a^2-4b}{4}$ (in our case $\bar{b}$ matches the conjugate of b). Then

$$\frac{\Delta(\psi_3)}{2^8 \cdot 3^2 \cdot b^4 \cdot \bar{b}^2} = \left(\frac{\prod_{i<j}(\theta_i - \theta_j)}{2^4 \cdot 3 \cdot b^2 \cdot \bar{b}} \right)^2 = -3. \tag{12}$$

Note that $\phi_1(\theta_i - \theta_j) = \frac{1}{2} \cdot (\theta_i - \theta_j) \cdot \left(\frac{b - \theta_i\theta_j}{\theta_i\theta_j} \right)$. Then, since ϕ_1 acts as conjugation on K,

$$\phi_1 \left(\frac{\prod_{i<j}(\theta_i - \theta_j)}{2^4 \cdot 3 \cdot b^2 \cdot \bar{b}} \right) = \frac{\prod_{i<j}(\theta_i - \theta_j)}{2^4 \cdot 3 \cdot b^2 \cdot \bar{b}} \cdot \left(\frac{-3^3}{b^6} \cdot \frac{b \prod_{i<j}(b - \theta_i\theta_j)}{2^6 \bar{b}} \right).$$

An easy computation using elementary symmetric polynomials (and their relation with the coefficients of (11)) prove that the last term equals -1, hence $\phi(\sqrt{-3}) = -\sqrt{-3}$ so $\sqrt{-3d} \in L^\phi$ and the claim follows. □

Remark 1. The same result holds for $K = \mathbb{Q}(\sqrt{3})$ or $\mathbb{Q}(\sqrt{6})$ replacing the 3-torsion points computation with the 5-torsion ones (for the prime $p = 3 \in S$). While working with 5-torsion points, formula (12) becomes

$$\frac{\Delta(\psi_5)}{2^{88} \cdot 5^{10} \cdot b^{44} \cdot (a^2 - 4b)^{22}} = 5.$$

The case $K = \mathbb{Q}(\sqrt{2})$ is more subtle as there is no clear choice of an order two element in the Galois group $\mathrm{Gal}(K(E[\ell])/\mathbb{Q})$. In particular computed examples the result holds (but we do not have a general proof).

3. Ellenberg's result

Let $K/\mathbb{Q}$ be a quadratic extension, and let E/K be a $\mathbb{Q}$-curve with a prime $\ell > 3$ of potentially multiplicative reduction. Then following ideas of Darmon-Merel, Ellenberg proved ([Ell04, Theorem 3.14]) that the residual p-representation of E has large image (i.e. not contained in the normalizer of a non-split cartan group) if either:

- there exists $f \in S_2(\Gamma_0(p^2))$ such that $w_p f = f$, or
- there exists $f \in S_2(\Gamma_0(2p^2)$ such that $w_p f = f$ and $w_2 f = -f$,

with $L(f \otimes \delta_K, 1) \neq 0$. An important result of Ellenberg ([Ell04, Proposition 3.9]) proves that if K is an imaginary quadratic field then there is always a modular form satisfying the first hypothesis for p large enough.

Proposition 3.1. *If $K/\mathbb{Q}$ is a real quadratic field in which p is unramified, there does not exist a newform satisfying any of the two previous conditions unless 2 splits in $K/\mathbb{Q}$.*

Proof. For a newform f, let $\epsilon(f)$ denote its root number (i.e. the sign of the functional equation). Recall from [Bum97] (§I.5) that if $f \in S_2(\Gamma_0(N))$ is a newform and χ is a Dirichlet character whose conductor is prime to N then $\epsilon(f \otimes \chi) = \epsilon(f)\chi(-N)$. Under the assumption p unramified in $K/\mathbb{Q}$, this result rules out the existence of a newform of level p^2 such that $L(f, \otimes\delta_K, 1) \neq 0$ (since $\delta_K(-1) = 1$ for K real quadratic).

Suppose that f is a newform of level $2p^2$. The Atkin-Lehner eigenvalues hypotheses imply that $\epsilon(f) = 1$. Suppose that 2 is unramified in $K/\mathbb{Q}$, hence $\epsilon(f \otimes \delta_K) = \delta_K(-2p^2) = \delta_K(2) = 1$ if and only if 2 splits in $K/\mathbb{Q}$. When 2 ramifies in $K/\mathbb{Q}$, we can write $d_K = d_1 \cdot d_2$, where $d_1 \in \{-4, \pm 8\}$ and d_2 is an odd fundamental discriminant. Suppose $d_1 = -4$; writing $f \otimes \delta_K = (f \otimes \delta_{d_1}) \otimes \delta_{d_2}$, it is enough to understand the sign change for the first twist (the form $f \otimes \delta_{-4}$ being a form of level $16p^2$). By a result of Atkin-Lehner (see [AL70, Theorem 7]) $w_2(f \otimes \delta_{-4}) = -1$ while $w_p(f \otimes \delta_{-4}) = w_p(f)$, hence $\epsilon(f \otimes \delta_{-4}) = \epsilon(f) = 1$ and since d_2 is negative (hence $\delta_{d_2}(-1) = -1$) $\epsilon(f \otimes \delta_K) = -1$. A similar computation (using that $w_2(f \otimes \delta_8) = 1$ and $w_2(f \otimes \delta_{-8}) = -1$) proves the remaining cases. □

Suppose then that 2 splits in $K/\mathbb{Q}$. Ellenberg's proof of the existence of a newform with prescribed properties consists on bounding an average of twisted central values in the whole space of level p^2 modular forms (since the forms with the wrong Atkin-Lehner involution sign in such space have zero central value). While considering the space $S_2(\Gamma_0(2p^2))^{\mathrm{new}}$ the computations are harder, as one needs to compute an average not over the whole space, but over the subspace with a chosen Atkin-Lehner sign at p (therefore imposing also a condition to the Atkin-Lehner sign at 2). Such computation was carried out in [LF17] (see the proof of Corollary 4). Unfortunately, explicit constants are not presented in Le Fourn's article, hence we need to

add some (minor) extra details to its proof (we suggest the reader to have a copy of such article in hand for the rest of this section as we follow its notations and definitions; specially Section 6).

The inequality $J_1(x) \leq \frac{|x|}{2}$ and $|S(1,n;c)| < \sqrt{c}\tau(c)$ (used in Ellenberg's article) turns inequality (30) of [LF17] into

$$|A_{N,Q,c}(x)| \leq \frac{\pi}{3} \cdot \frac{xe^{-2\pi/x}\tau(c)}{Qc^{3/2}}, \tag{13}$$

for $x \geq 71$ (using that $(1-e^{-2\pi/x})^{-1} \leq \frac{x}{6}$ when $x \geq 71$). The same bound for J_1 gives the explicit inequality for equation (31)

$$|A_{N,Q,c}(x)| \leq \frac{12}{\pi} \frac{(\log(Dc)+1)\sqrt{D}}{cQ} e^{-2\pi/x}. \tag{14}$$

To get a bound for $A_{N,Q}(x) = 2\pi \sum_{c>0,(N/Q)|c,(c,Q)=1} A_{N,Q,c}(x)$ we split the sum as in [LF17]:

$$|A_{N,Q}(x)| \leq \frac{12}{\pi} \frac{\sqrt{D}e^{-2\pi/x}}{Q} \sum_{\substack{c<x^2 \\ (N/Q)|c}} \frac{(\log(Dc)+1)}{c} + \frac{\pi}{3} \sum_{\substack{c>x^2 \\ (N/Q)|c}} \frac{xe^{-2\pi/x}\tau(c)}{Qc^{3/2}}.$$

For the first inner sum, writing $c = (N/Q)b$, we get the inequality

$$\sum_{\substack{c<x^2 \\ (N/Q)|c}} \frac{(\log(Dc)+1)}{c} \leq \frac{Q}{N} \left((\log(\frac{DN}{Q})+1)\log(\frac{x^2N}{Q}) + \frac{\log^2(\frac{x^2N}{Q})}{2} \right). \tag{15}$$

To bound the sum $\sum_{c>X^2} \frac{\tau(c)}{c^{3/2}}$, recall the following inequalities:

$$\sum_{n\geq X} \frac{1}{n^s} \leq -\frac{X^{1-s}}{1-s} + \frac{X^{-s}}{2}, \text{ and } \sum_{d\leq X} \frac{1}{d} \leq \log(X) + \gamma + \frac{7}{12X},$$

where γ is the Euler-Mascheroni constant ($\gamma \leq 0.58$). If $s > 1$,

$$\sum_{n\geq X} \frac{\tau(n)}{n^s} = \sum_{n\geq X} \left(\sum_{d|n} \frac{1}{n^s} \right) = \sum_d \frac{1}{d^s} \sum_{m\geq X/d} \frac{1}{m^s} \leq \zeta(s) \sum_{d>X} \frac{1}{d^s} + \sum_{d\leq X} \frac{1}{d^s} \left(-\frac{(X/d)^{1-s}}{(1-s)} + \frac{(X/d)^{-s}}{2} \right) \leq$$
$$\zeta(s) \left(-\frac{X^{1-s}}{(1-s)} + \frac{X^{-s}}{2} \right) - \frac{X^{1-s}}{(1-s)} \sum_{d\leq X} \frac{1}{d} + \frac{X^{1-s}}{2} \leq$$
$$\zeta(s) \left(-\frac{X^{1-s}}{(1-s)} + \frac{X^{-s}}{2} \right) - \frac{X^{1-s}}{(1-s)} (\log(X) + \gamma + \frac{7}{12X}) + \frac{X^{1-s}}{2}.$$

Substituting at $s = 3/2$, X by X^2 and assuming $X \geq 32$, we obtain

$$\sum_{n\geq X^2} \frac{\tau(n)}{n^{3/2}} \leq \frac{6\log(X)}{X}. \tag{16}$$

Using both inequalities, we get (for $N \neq Q$)

$$|A_{N,Q}(x)| \leq \frac{12\sqrt{D}e^{-2\pi/x}}{N\pi} \left((\log(\frac{DN}{Q})+1)\log(\frac{x^2N}{Q}) + \frac{\log^2(\frac{x^2N}{Q})}{2} \right) + \tag{17}$$
$$+ \frac{2\pi}{N} \sqrt{Q/N}\tau(N/Q)\log(x)e^{-2\pi/x}.$$

Using the fact that $B_{N,Q}(x) = A_{N,Q}(D^2N/x)$, we get the bound

$$|B_{N,Q}(x)| \leq |A_{N,Q}(D^2N/x)| + \delta_{Q=N} \frac{\pi}{3} \frac{\sqrt{D}}{x} \tau(D) e^{\frac{-2\pi x}{ND^2}}. \tag{18}$$

Recall that $(a_1, L_\chi)_{2p^2}^{+_{p^2},\text{new}} = (a_1, L_\chi)_{2p^2}^{+_{p^2}} - \frac{1}{p-1}(a_1, L_\chi)_{2p}^{\chi(p)_p}$ ([LF17, Lemma 7]), hence formulas (28), (29) of [LF17] give

$$\frac{1}{2\pi}(a_1, L_\chi)_{2p^2}^{+_{p^2},\text{new}} \geq \frac{(p-2)}{(p-1)}e^{-2\pi/x} - (|A_{2p^2,1}(x)| + |A_{2p^2,p^2}(x)| + |A_{2p,1}(x)| + |A_{2p,p}(x)| + \\ + |B_{2p^2,2p^2}(x)| + |B_{2p^2,2}(x)| + |B_{2p,2p}(x)| + |B_{2p,2}(x)|). \tag{19}$$

Taking x of the same magnitude of p^2 (in our applications we will take $x = p^2 \cdot \kappa$ for a numerical computed constant κ), the right hand side is an increasing function of p, hence as soon as we find a positive value for it, we get an explicit bound.

4. Examples

Let us recall briefly how the modular method works: attach to a primitive solution (A, B, C) of (1) the Frey curve $E_{(A,B)}$. It has the property that all odd primes dividing its conductor have exponent divisible by p. Since $E_{(A,B)}$ is a $\mathbb{Q}$-curve, there exists a weight 2, level N and Nebentypus ε newform attached to its extension to $\text{Gal}_{\mathbb{Q}}$ (by Serre's conjectures). Suppose that p is a prime number such that the residual representation of $\tilde{\rho}$ is absolutely irreducible, then Ribet's lowering the level result ([Rib91]) implies that all primes but 2 and the ones ramifying in $K/\mathbb{Q}$ can be removed from the level. In particular we have a congruence modulo p between the Galois representation attached to $E_{(A,B)}$ and a newform in a concrete space. Discard each newform in the given space via the so called "Maruz's trick", namely check whether the eigenvalues are consistent with a "local" solution of the original equation. If no newform passes the test, we can conclude that no such solution exists.

If there exists a solution of equation (1) for all primes p, then the above method fails. This is the case for solutions with $C = \pm 1$. When $d < 0$ this only happens when $B = 0$, namely for the trivial solution $(\pm 1, 0, 1)$. The Frey curve attached to it has the particular property that it corresponds to a $\mathbb{Q}$-curve with complex multiplication. Here is where Ellenberg's large image result is useful! The Frey curve attached to a non-trivial solution does not have complex multiplication, hence it cannot be congruent to a trivial solution! This is the reason why we could prove non-existence of non-trivial solutions of (1) for some negative values of d (in [PT20]).

There are two unfortunate situations when the previous approach cannot be applied. On of them is when Ellenberg's result cannot be applied. Then we can only hope to prove non-existence of solutions for primes satisfying certain congruence properties (the ones where the curve coming from the trivial solution has small image, namely its projectivization is contained in the normalizer of a non-split Cartan subgroup). The second one (which only occurs when $d > 0$) is when the curve

$$x^4 - dy^2 = \pm 1 \tag{20}$$

admits non-trivial solutions. For $1 < d < 20$, a non-trivial solution for such equation exists precisely for

$$(A, B, C, d) \in \{(\pm 1, \pm 1, -1, 2), (\pm 3, \pm 4, 1, 5), (\pm 7, \pm 20, 1, 6), (\pm 2, \pm 1, 1, 15), (\pm 2, \pm 1, -1, 17)\}.$$

Equation (20) was studied in several articles (see for example [Wal00]). It is known that the equation with $+1$ on the right hand side has at most one non-trivial solution ([Lju42]) except when $d = 1785$. Furthermore, in ([Coh97]) all solutions for $1 \leq d \leq 150000$ are computed. The equation with -1 on the right hand side was studied in [Lju54], where it is also shown that in all cases there is at most one non-trivial solution, and a condition for the existence is presented. A priori, the modular method should not work in cases when there exists a solution from solutions of (20) (although we will soon prove it does work for $d = 6$).

Before giving a detailed study of equation (1) for $d = 6$ and $d = 129$ (for computational reasons, while describing the fields we do not assume that d is a discriminant, but that it is square-free), let us explain why we chose such values. The field $\mathbb{Q}(\sqrt{6})$ is the first one where the fundamental unit has norm 1 (and also it contains a non-trivial solution for all primes p). The case $d = 129$ is the first field where 2 splits (so Ellenberg's result can be applied) and we could discard all newforms using Mazur's trick. For $d \in \{3, 5, 7, 14\}$ there are modular forms without CM that cannot be discarded with the aforementioned strategy (so the modular method fails). For the other square-free values of d, the modular method does give a positive answer for primes $p > M$ (an explicit constant) with a prescribed congruence condition. The results are

d	M	Condition on p	$\dim(S_2(N,\varepsilon))$	Hilbert space
6	19	$p \neq 97$; $p \equiv 1,3 \pmod 8$	28, 64	96, 384
10	19	$p \neq 41, 89$; $p \equiv 1,3 \pmod 8$	140, 288	448, 1792
11	19	$p \equiv 1,3 \pmod 8$	22, 92	224, 896
19	19	$p \neq 41, 43$; $p \equiv 1,3 \pmod 8$	38, 156	608, 2432
129	19	$p > 64690$ or $p \equiv 1,3 \pmod 8$	16, 1400	100, 600, 38400

TABLE 4.1.

shown in Table 4.1. The table contains also the dimension of the weight two newform space (computed to discard possible solutions) as well as the dimension of the Hilbert parallel weight 2 modular forms space (if one would follow the classical approach over K). Note the dimension of the Hilbert space becomes almost infeasible from a computational point of view very soon.

4.1. **The case $d = 6$.** As mentioned before, although the case $d = 6$ seems to be out of reach of the modular method, it turns out that the Frey curve attached to the solution $(\pm 7, \pm 20, 1)$ does also have complex multiplication! (this seems like a very fortunate coincidence, but will not occur for other values). The trivial solution gives an elliptic curve with j-invariant 8000 (with CM by $\mathbb{Z}[\sqrt{-2}]$). Over $\mathbb{Q}(\sqrt{6})$ there are only two extra isomorphism classes of elliptic curves with CM whose j-invariant is not rational (see [DLR15]), with j-invariant $188837384000 \pm 77092288000\sqrt{6}$. The Frey curve $E_{(\pm 7,\pm 20)}$ has precisely such a j-invariant!

Theorem 4.1. *Let $p > 19$ such that $p \neq 97$ and $p \equiv 1,3 \pmod 8$. Then, $(\pm 7, \pm 20, 1)$ are the only non-trivial solutions of the equation*

$$x^4 - 6y^2 = z^p.$$

Proof. Suppose that (A, B, C) is a solution with $C \neq \pm 1$ (in particular C is divisible by a prime number greater than 3). In order to apply Ribet's lowering the level result, we need to probe that the residual representation of $E_{(A,B)}$ modulo p is absolutely irreducible. For that purpose we apply Theorem 1 of [FS15]. Let $\epsilon = 5 + 2\sqrt{6}$ be a fundamental unit. The value $\operatorname{lcm}(\mathcal{N}(\epsilon^{12} - 1), \mathcal{N}(\bar{\epsilon}^{12} - 1)) = 2^7 \cdot 3^5 \cdot 5^2 \cdot 11^2 \cdot 97^2$. Next we need to compute the characteristic polynomial at a prime of good reduction. Since $E_{(A,B)}$ has good reduction at primes ramifying in $K/\mathbb{Q}$, $q = 3$ is a good candidate so let $\mathfrak{q} = \langle 3 + \sqrt{6} \rangle$. The curve $E_{(A,B)}$ modulo $\mathfrak{p}$ is one of $y^2 = x^3 \pm x^2 + 2x$, hence $a_{\mathfrak{q}}(E) = \pm 2$. The resultant between $x^2 \pm 2x + 3$ and $x^{12} - 1$ is only divisible by the primes $\{2, 3, 19, 97\}$, hence the residual image is absolutely irreducible for all primes except the ones in one of these two sets. Using Theorem 2.1 (and Remark 1) and Ribet's lowering the level result, we have to compute the spaces $S_2(2^8 \cdot 3, \varepsilon)$ and $S_2(2^9 \cdot 3, \varepsilon)$, where ϵ is the character corresponding to the quadratic field $\mathbb{Q}(\sqrt{3})$. Such spaces have 10 and 13 conjugacy classes respectively. Mazur's trick for $q = 5, 7, 17$ discards all classes in both spaces except from three in the first space coming from the solutions $(\pm 1, 0, 1)$ and $(\pm 7, \pm 20, 1)$ with CM by $\mathbb{Z}[\sqrt{-2}]$. If $p \equiv 1,3 \pmod 8$, it splits in $\mathbb{Q}(\sqrt{-2})$ hence the residual representation of the forms with CM modulo p have projective image lying in the normalizer of a split Cartan subgroup. This contradicts [Ell04, Proposition 3.4] (as C is divisible by a prime greater than 3). □

Remark 2. While proving big image, [FS15, Theorem 1] was used with $q = 3$, since we know that the curve has good reduction for odd primes ramifying in K. Although we do not know a priori other primes of good reduction, if the obtained bound is large not everything is lost. Let $q > 5$ be a prime inert in K and suppose $p > 71$. If q divides C, the curve has multiplicative reduction at q hence [NT20, Theorem 1.2] implies that the residual representation is irreducible. Otherwise, the curve has good reduction at q hence we can apply the above strategy to the prime q. This method was used for $d \in \{10, 11, 19\}$.

4.2. **The case $d = 129$.** The prime 2 splits in $\mathbb{Q}(\sqrt{129})$, hence Ellenberg's result can be applied to discard the trivial solutions as well.

Theorem 4.2. *Let $p > 19$ be a prime number satisfying that either $p > 64690$ or $p \equiv 1,3 \pmod 8$. Then there are no non-trivial solutions of the equation*

$$x^4 - 129y^2 = z^p.$$

Proof. As before, let (A, B, C) be a non-trivial solution, and $E_{(A,B)}$ the Frey curve attached to it. [FS15, Theorem 1] proves that the residual image is absolutely irreducible for primes not in $\{2, 3, 5, 7, 11, 13, 17, 43, 53, 251, 313, 661, 2593, 3371, 411577\}$. As this bound is a little large, we follow the strategy described in [MR21, Lemma 3.2]. Suppose that the residual representation at a prime p is reducible, say its semisimplification is given by $\theta_1 \oplus \theta_2$. The curve $E_{(A,B)}$ has additive reduction only at primes dividing 2, hence a priori the characters θ_i are only ramified at such primes and probably at primes dividing p. The fact that $E \otimes \chi$ descends to a rational representation, and that χ is only ramified at $3, 43$, imply that if $p \neq 3, 43$ the characters θ_i cannot be ramified at primes dividing p. The prime 2 splits in $\mathbb{Q}(\sqrt{129}/\mathbb{Q})$, say $2 = \mathfrak{p}\bar{\mathfrak{p}}$. The conductor of $E_{(A,B)}$ at $(\mathfrak{p}, \bar{\mathfrak{p}})$ equals one of $(8, 8), (1, 6)$ or $(4, 6)$, hence the character θ_1 has conductor $2^4, \mathfrak{p}^3$ or $4 \cdot \mathfrak{p}$. The ray class group for such conductors have exponent 4 (in the first case) and 2 (in the other two ones) (computed using [PAR19]). In particular the curve (or a quadratic twist of it) has a rational point over an extension of degree 2 or 4 over $\mathbb{Q}$, hence $p \leq 17$ by [DKSS17, Theorem 1.2].

Theorem 2.1 and Ribet's lowering the level imply our solution gives a newform in $S_2(\Gamma_0(2 \cdot 3 \cdot 43), \varepsilon)$ (when C is even) and $S_2(\Gamma_0(2^8 \cdot 3 \cdot 43), \varepsilon)$ (when C is odd), where ε corresponds to $\mathbb{Q}(\sqrt{129})$. The first space has 4 conjugacy classes while the second one has 36. Using Mazur's trick all forms in the first space and all forms in the second space without CM can be discarded (using primes up to 19). Clearly we cannot discard the remaining forms with complex multiplication by $\mathbb{Z}[\sqrt{-2}]$. To discard them, we use the results of Section 3. In this case, we know that C is odd, not divisible by 3 (since 3 ramifies in $K/\mathbb{Q}$) and since there are no other solutions with $C = \pm 1$ than the trivial ones, C is divisible by an odd prime greater than 3. After a computer search for the minimum x of the form $x = p^2 \cdot \kappa$ we obtained that taking $x = \frac{p^2}{90000}$ in (19) makes the right hand side positive for $p > 64690$. For small primes, the same argument as in the previous example proves that the CM forms can be discarded for primes $p \equiv 1, 3 \pmod 8$. □

Remark 3. Ellenberg's bound obtained in the last example could probably be slightly improved if better bounds are given in the computations of Section 3. If the final value is not too large, a newform $f \in S_2(\Gamma_0(2p^2))$ with the desired properties could be found in the intermediate range via a computer search.

References

[AL70] A. O. L. Atkin and J. Lehner. Hecke operators on $\Gamma_0(m)$. *Math. Ann.*, 185:134–160, 1970.

[Bue89] Duncan A. Buell. *Binary quadratic forms*. Springer-Verlag, New York, 1989. Classical theory and modern computations.

[Bum97] Daniel Bump. *Automorphic forms and representations*, volume 55 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1997.

[Coh97] J. H. E. Cohn. The Diophantine equation $x^4 - Dy^2 = 1$. II. *Acta Arith.*, 78(4):401–403, 1997.

[CP19] John Cremona and Ariel Pacetti. On elliptic curves of prime power conductor over imaginary quadratic fields with class number 1. *Proc. Lond. Math. Soc. (3)*, 118(5):1245–1276, 2019.

[DKSS17] Maarten Derickx, Sheldon Kamienny, William Stein, and Michael Stoll. Torsion points on elliptic curves over number fields of small degree, 2017.

[DLR15] Harris B. Daniels and Álvaro Lozano-Robledo. On the number of isomorphism classes of CM elliptic curves defined over a number field. *J. Number Theory*, 157:367–396, 2015.

[DU09] Luis Dieulefait and Jorge Jiménez Urroz. Solving Fermat-type equations via modular Q-curves over polyquadratic fields. *J. Reine Angew. Math.*, 633:183–195, 2009.

[Ell04] Jordan S. Ellenberg. Galois representations attached to Q-curves and the generalized Fermat equation $A^4 + B^2 = C^p$. *Amer. J. Math.*, 126(4):763–787, 2004.

[FLHS15] Nuno Freitas, Bao V. Le Hung, and Samir Siksek. Elliptic curves over real quadratic fields are modular. *Invent. Math.*, 201(1):159–206, 2015.

[FS15] Nuno Freitas and Samir Siksek. Criteria for irreducibility of mod p representations of Frey curves. *J. Théor. Nombres Bordeaux*, 27(1):67–76, 2015.

[Gau86] Carl Friedrich Gauss. *Disquisitiones arithmeticae*. Springer-Verlag, New York, 1986. Translated and with a preface by Arthur A. Clarke, Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse.

[LF17] Samuel Le Fourn. Nonvanishing of central values of L-functions of newforms in $S_2(\Gamma_0(dp^2))$ twisted by quadratic characters. *Canad. Math. Bull.*, 60(2):329–349, 2017.

[Lju42] Wilhelm Ljunggren. Über die Gleichung $x^4 - Dy^2 = 1$. *Arch. Math. Naturvid.*, 45(5):61–70, 1942.

[Lju54] Wilhelm Ljunggren. Ein Satz über die diophantische Gleichung $Ax^2 - By^4 = C$ $(C = 1, 2, 4)$. In *Tolfte Skandinaviska Matematikerkongressen, Lund, 1953*, pages 188–194. Lunds Universitets Matematiska Inst., Lund, 1954.

[MR21] Philippe Michaud-Rodgers. Fermat's last theorem and modular curves over real quadratic fields, 2021.

[NT20] Filip Najman and George C. Turcas. Irreducibility of mod p galois representations of elliptic curves with multiplicative reduction over number fields, 2020.
[PAR19] PARI Group, Univ. Bordeaux. *PARI/GP version 2.12.2*, 2019. available from http://pari.math.u-bordeaux.fr/.
[PT20] Ariel Pacetti and Lucas Villagra Torcomian. $\mathbb{Q}$-curves, hecke characters and some diophantine equations, 2020.
[Rib91] Kenneth A. Ribet. Lowering the levels of modular representations without multiplicity one. *Internat. Math. Res. Notices*, (2):15–19, 1991.
[Rib04] Kenneth A. Ribet. Abelian varieties over $\mathbf{Q}$ and modular forms. In *Modular curves and abelian varieties*, volume 224 of *Progr. Math.*, pages 241–261. Birkhäuser, Basel, 2004.
[Wal00] P. G. Walsh. Diophantine equations of the form $aX^4 - bY^2 = \pm 1$. In *Algebraic number theory and Diophantine analysis (Graz, 1998)*, pages 531–554. de Gruyter, Berlin, 2000.

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

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