Publ. Mat. **67** (2023), 569–599
DOI: 10.5565/PUBLMAT6722304

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

Ariel Pacetti and Lucas Villagra Torcomian

Abstract: In the article [**25**] 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 prescribed local conditions. We also extend some "large image" results due to Ellenberg regarding images of Galois representations coming from $\mathbb{Q}$-curves from imaginary to real quadratic fields.

2020 Mathematics Subject Classification: 11D41, 11F80.

Key words: $\mathbb{Q}$-curves, Diophantine equations.

Introduction

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

$$Ax^p + By^q = Cz^r, \tag{1}$$

for $\frac{1}{p}+\frac{1}{q}+\frac{1}{r} < 1$. As was already observed in [**9**], if no condition on the solutions is imposed, then the equation might have infinitely many solutions. To overcome this subtlety we restrict to what in the literature is called *primitive solutions*. A solution (a,b,c) to (1) is called *primitive* if the numbers $\{aA, bB, cC\}$ are pairwise coprime.

A particularly interesting example of (1) occurs for exponents $(p,q,r) = (4,2,r)$ and $(A,B,C)=(1,1,1)$, studied by Darmon and Ellenberg independently (see [**13**]). The Frey curve attached to a solution of it happens to be a $\mathbb{Q}$-curve (i.e. an elliptic curve defined over a number field, which is isogenous to all its Galois conjugates). $\mathbb{Q}$-curves have the special property that a twist of their Galois representation extends to a Galois representation of the whole Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and by [**30**, Theorem 4.4] and Serre's modularity conjecture ([**32**], [**17**], and [**18**]) it equals the Galois representation of a classical modular form. Then, one can follow the modular method to compute (via a lowering-the-level argument) a fixed space of level N and weight 2 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). Using this method, in [**25**] the equation

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

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?

To a primitive solution (a,b,c) of (2) (or equivalently a solution (a,b,c) satisfying that the values $\{a, b, c\}$ are pairwise coprime), one associates (as explained in [**12**]) the elliptic curve

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

defined 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 (see [**14**]) hence one can follow the modular approach working with Hilbert modular forms. It turns out that such an approach becomes impractical very soon, due to the huge dimension of the corresponding spaces (see Table 5.1). However, the $\mathbb{Q}$-curves approach is still practical in many circumstances, which motivates the present article. This article should be regarded as a continuation of our previous work [**25**], 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 how it can be used to discard modular forms with complex multiplication.
- Explain why the case d positive is harder due to potential existence of non-trivial primitive solutions for all exponents p.

Section 5 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 (2) with $c = \pm 1$, which are valid for all exponents p, making the modular approach fail. Finally, we explain why when there are modular forms with complex multiplication to be discarded, 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: Section 1 contains a brief review of the strategy developed in [**25**] as well as a review of the modular method. In Section 2 (Theorem 2.1) we solve 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: 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 (this 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 by class field theory it corresponds to a genus character (see for example Chapter 2 of [**6**]). Is there a natural description for such a character? Can the extension $K(\sqrt{\epsilon})$ be described in terms of d?

We give a positive answer to this problem (Theorem 2.2), which plays a crucial role in the proof of the good definition of our Hecke character. The third section (Theorem 3.2) settles the second issue, i.e. it gives a precise recipe for N and ε. A proof of this statement was given in [**25**] 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 fourth section gives an explicit version of Ellenberg's large image result for real quadratic fields where the prime 2 splits. The proof follows from an "explicit" version of the main result of [**20**], our little contribution being making the constants explicit. The last section contains the examples, where the cases $d = 6$ and $d = 129$ are specially considered along with other values of d between 1 and 20 (see Table 5.1). Here are two instances of the results proved in the present article:

Theorem 5.1. *Let $p > 19$ be a prime number such that $p \neq 97$ and $p \equiv 1, 3 \pmod 8$. Then, $(\pm 7, \pm 20, 1)$ are the only non-trivial primitive solutions of the equation*

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

Theorem 5.5. *Let $p > 19$ be a prime number satisfying that either $p > 900$ or $p \equiv 1, 3 \pmod 8$ and $p \neq 43$. Then there are no non-trivial primitive 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 [**25**]. The code in `PARI/GP` ([**27**]) and Magma ([**2**]) used in the examples (and the outputs), as well the one used to verify Tables 2.3, 2.4, and 2.5, are available on the web page `https://github.com/lucasvillagra/Q-curves2.git`.

Acknowledgments. We would like to thank Yingkun Li for sharing with us a proof of Theorem 2.2 and Harald Helfgott for providing some bounds used in Section 4. We also want to thank Nuno Freitas for some useful comments on the proofs of Section 3. Lastly, we want to thank the referees for their suggestions, which improved the quality of the present article. 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. Brief review of the modular method

Let us recall briefly how the modular method works. To a putative primitive solution (a, b, c) of (2), attach the elliptic curve $E_{(a,b,c)}$ given by the equation

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

defined over the quadratic field $K = \mathbb{Q}(\sqrt{d})$. Let Gal_K denote an absolute Galois group of K, i.e. $\mathrm{Gal}_K := \mathrm{Gal}(\overline{\mathbb{Q}}/K)$, and for p a prime number, let $\rho_{E_{(a,b,c)},p} \colon \mathrm{Gal}_K \to \mathrm{GL}_2(\mathbb{Z}_p)$ denote the 2-dimensional p-adic Galois representation attached to $E_{(a,b,c)}$ (obtained by looking at the action of the Galois group on the p-adic Tate module of the curve $E_{(a,b,c)}$). The curve $E_{(a,b,c)}$ is what is called a $\mathbb{Q}$-curve, that is, its Galois conjugate is isogenous (via the order 2 isogeny whose kernel is the point $(0, 0)$) to itself (see for example [**25**, Proposition 2.2]). The problem is that the isogeny is not defined over K but over $K(\sqrt{-2})$, so the Galois representation $\rho_{E_{(a,b,c)},p}$ does not extend to a 2-dimensional representation of the whole Galois group $\mathrm{Gal}_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. However, there exists a character χ (that will be constructed in the next section) such that the twisted representation $\rho_{E_{(a,b,c)},p} \otimes \chi$ does extend to an odd 2-dimensional Galois representation of the whole Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Let $\tilde{\rho}_p$ denote such an extension.

It is well known that modularity of the representation $\tilde{\rho}_p$ follows from Serre's modularity conjecture (see [**30**, Theorem 4.4]). As a side remark, Ribet's proof uses the fact that our representation is related to an abelian variety of GL_2-type. Modularity of odd 2-dimensional abstract representations (satisfying the usual geometric hypothesis) is also known if $p \geq 5$ (see [**26**, Theorem 1.0.4]). In particular, $\tilde{\rho}_p$ matches the Galois representation of a weight 2, level $\tilde{N}$, and nebentypus ε newform $f_{(a,b,c)}$ (the level and nebentypus are described explicitly in Theorem 3.2).

The classical Hellegouarch result implies that our residual representation $\overline{\rho_{E_{(a,b,c)},p} \otimes \chi}$ is unramified at all primes not dividing $2d$, and the same holds for $\bar{\tilde{\rho}}$. Suppose that p is a prime number such that the residual representation of $\tilde{\rho}_p$ is absolutely irreducible. Then Ribet's lowering-the-level result ([**29**]) implies that we have a congruence modulo p between our newform $f_{(a,b,c)}$ and a newform $g_{(a,b,c)}$ whose level N is only divisible by primes dividing $2d$ and with the same nebentypus. We are now led to "discard" the newforms $g \in S_2(N, \varepsilon)$ that do not come from real solutions.

The first elimination process consists in applying the so called "Mazur's trick", in other words, checking whether the eigenvalues are consistent with a "local" solution of the original equation. More concretely, suppose we intend to discard a form g. Let q be a prime number such that $q \nmid 2pd$, and let

$$C(q,g) = \prod_{(a,b,c)\in\mathbb{F}_q^3} B(q,g;a,b,c),$$

where the product is over non-zero triples (a,b,c) satisfying (2) modulo q, and where the number $B(q,g;a,b,c)$ is defined by

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

If (a,b,c) is a solution of (2) and $g \in S_2(N,\varepsilon)$ is congruent modulo p to $f_{(a,b,c)}$, it must be the case that $p \mid C(q,g)$ for all prime numbers q (see [**25**, Proposition 6.1]). We say that the form g passes the test if $C(q,g) \neq 0$ for some small prime q. If all the newforms pass the test, we can conclude that no such solution exists (which never happens, due to the existence of a trivial solution).

If (a,b,c) is a solution of equation (2) for all primes p, and $g \in S_2(N,\varepsilon)$ is the modular form congruent modulo p to $f_{(a,b,c)}$, then $C(q,g) = 0$ for all primes q, so the above method fails. This occurs precisely when $c = \pm 1$. When $d < 0$, the only solutions with $c = \pm 1$ are the trivial ones, but the Frey curves $E_{(\pm 1,0,1)}$ have complex multiplication. To discard forms with complex multiplication Ellenberg's result ([**13**, Theorem 3.14]) is needed. Modular forms with complex multiplication have the property that the image of their Galois representations is not as large as expected (their image lies in the normalizer of a Cartan group), while for $\mathbb{Q}$-curves without complex multiplication Ellenberg's result implies that their projective residual image contains $\mathrm{PSL}_2(\mathbb{F}_p)$, hence they cannot be congruent. This is the reason why we were able to prove non-existence of non-trivial primitive solutions of (2) for different negative values of d in [**25**].

There are two unfortunate situations where the previous approach cannot be applied. One of them is when [**13**, Theorem 3.14] 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, i.e. its residual image is contained in the normalizer of a split Cartan subgroup). The second one (which only occurs when $d > 0$) is when the curve

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

admits non-trivial solutions. For $1 < d < 20$, the non-trivial solutions of such an equation are precisely the following:

$$\begin{aligned}(a,b,c,d) \in \{&(\pm1,\pm1,-1,2),(\pm3,\pm4,1,5),(\pm7,\pm20,1,6),\\ &(\pm2,\pm1,1,15),(\pm2,\pm1,-1,17)\}.\end{aligned} \tag{5}$$

Equation (4) was studied in several articles (see for example [**33**]). It is known that the equation with $+1$ on the right-hand side has at most one non-trivial solution (see [**21**]) except when $d = 1785$. Furthermore, in [**5**] all solutions for $1 \leq d \leq 150000$ are computed. The equation with -1 on the right-hand side was studied in [**22**], 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 of (4) (although we will soon prove it does work for $d = 6$).

2. Construction of the Hecke character

Given $\tau \in \mathrm{Gal}_{\mathbb{Q}}$ and ρ a representation of Gal_K, by ${}^{\tau}\rho$ we denote the representation of Gal_K whose value at $\sigma \in \mathrm{Gal}_K$ equals

$${}^{\tau}\rho(\sigma) = \rho(\tau\sigma\tau^{-1}).$$

Fix an element $\tau \in \mathrm{Gal}_{\mathbb{Q}}$ which is not the identity on K. Then the curve $\tau(E_{(a,b,c)})$ is isogenous to $E_{(a,b,c)} \otimes \delta_{-2}$ (the quadratic twist of the curve by -2) as proved in [**25**, Proposition 2.2]. This implies that

$${}^{\tau}\rho_{E_{(a,b,c)},p} \simeq \rho_{E_{(a,b,c)},p} \otimes \delta_{-2}, \tag{6}$$

where we interpret δ_{-2} as the quadratic character of Gal_K corresponding (via class field theory) to the quadratic extension $K(\sqrt{-2})/K$. Note that δ_{-2} is actually a quadratic character of $\mathrm{Gal}_{\mathbb{Q}}$ restricted to Gal_K.

Remark 1. All the previous stated properties hold for any pair of rational numbers (a, b) (independently of whether they are part of a solution of (2) or not). The fact that they are a solution is needed while studying the Kodaira type at bad primes, and also (together with the extra hypothesis that the solution is primitive) to assure that the residual representation $\overline{\rho_{E_{(a,b,c)},p}}$ is unramified at all prime ideals not dividing 2.

The main idea of [**25**] is to construct a finite order Hecke character χ satisfying also property (6) (using class field theory, we will denote indistinctly Hecke characters and their Galois character counterparts). If $\chi\colon \mathrm{Gal}_K \to \overline{\mathbb{Q}}^\times$ is a Hecke character satisfying ${}^\tau\chi(\sigma) := \chi(\tau\sigma\tau^{-1}) = \chi(\sigma)\delta_{-2}(\sigma)$ for all $\sigma \in \mathrm{Gal}_K$, then the twisted representation $\rho_{E_{(a,b,c)},p} \otimes \chi$ is invariant under the action of τ and hence extends to a 2-dimensional representation of $\mathrm{Gal}_\mathbb{Q}$. How can we construct a Hecke character χ on the idèle group of K (which we denote by $\mathbb{I}_K$) satisfying that ${}^\tau\chi = \chi \cdot \delta_{-2}$?

Let $\mathcal{O}_K$ denote the ring of integers of K, and given $\mathfrak{q}$ a prime ideal of $\mathcal{O}_K$, let $\mathcal{O}_\mathfrak{q}$ denote the completion of $\mathcal{O}_K$ at $\mathfrak{q}$. Let $\mathrm{Cl}(K)$ denote the class group of K. From the short exact sequence

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

it is enough to define the character χ 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 (i.e. elements of $\mathbb{I}_K$ that are in bijection with representatives for the class group $\mathrm{Cl}(K)$ under the map Id). The intersection of these two subgroups $\left(\prod_\mathfrak{q} \mathcal{O}_\mathfrak{q}^\times \times (\mathbb{R}^\times)^2\right) \cap K^\times = \mathcal{O}_K^\times$ imposes a *compatibility* condition on its definition, namely that 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 proved in [**25**, Theorem 3.4] when the fundamental unit has norm -1, so, after replacing ϵ by $-\epsilon$ if needed, we assume that ϵ is totally positive.

Let us briefly recall the construction given in [**25**] (there is a discrepancy with the definitions used in [**25**], namely that d needs to be changed to $-d$ in that 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 $\varepsilon\colon \mathbb{I}_{\mathbb{Q}} \to \overline{\mathbb{Q}}^{\times}$ (which will be the nebentypus of the extended Galois representation) as follows:

- For primes $p \nmid d$ and also for primes $p \in Q_1 \cup Q_7$, the character $\varepsilon_p\colon \mathbb{Z}_p^{\times} \to \overline{\mathbb{Q}}^{\times}$ 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 archimedean component) is trivial.
- Define $\varepsilon_2 = \delta_{-1}^{\#Q_3+\#Q_5}$.

Since $\mathbb{Q}$ has class number 1, the rational idèle $\mathbb{I}_{\mathbb{Q}}$ is isomorphic to $\mathbb{Q}^{\times} \cdot \left(\prod_p \mathbb{Z}_p^{\times} \times \mathbb{R}^{\times}\right)$, hence our local definitions give rise to a unique Hecke character ε once the compatibility condition is checked. But

$$\prod_p \varepsilon_p(-1)\varepsilon_\infty(-1) = \prod_{p\in Q_3\cup Q_5} \varepsilon_p(-1)\varepsilon_2(-1) = (-1)^{\#Q_3+\#Q_5}\varepsilon_2(-1) = 1.$$

By class field theory, ε gets identified with a character $\varepsilon\colon \mathrm{Gal}_{\mathbb{Q}} \to \overline{\mathbb{Q}}^{\times}$ whose kernel fixes 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. 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 $\#Q_3 + \#Q_5$ is even and 2 otherwise. If p is an odd prime dividing d, we denote by $\mathfrak{p}$ the unique prime in K dividing it.

Theorem 2.1. *There exists a Hecke character $\chi\colon \mathrm{Gal}_K \to \overline{\mathbb{Q}}^{\times}$ such that:*

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

Furthermore, if d denotes the discriminant of K and $\mathfrak{p}_2$ is a prime of K dividing 2, then its conductor equals $\mathfrak{p}_2^e \cdot \prod_{p\in Q_1\cup Q_5\cup Q_7} \mathfrak{p}$, where

$$e = \begin{cases} 5 & \text{if } d/4 \equiv 7 \pmod 8, \\ 3 & \text{if } d \equiv 1 \pmod 4, \\ 3 & \text{if } d/4 \equiv 2,3 \pmod 8, \\ 3 & \text{if } d/4 \equiv 6 \pmod{16}, \\ 0 & \text{if } d/4 \equiv 14 \pmod{16}. \end{cases}$$

The theorem was proved in [**25**, Theorem 3.2] 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 of 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 (i.e. equals the discriminant of the extension $K/\mathbb{Q}$). 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

$$\mathcal{P}_{\pm} = \{p \mid d,\, p \text{ odd} : \epsilon \equiv \pm 1 \pmod{\mathfrak{p}}\}.$$

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

Theorem 2.2. *Let* $\omega := \prod_{p \in \mathcal{P}_-} p$. *Then:*

1. *if 2 is unramified in* $K/\mathbb{Q}$, *we have* $K(\sqrt{\epsilon}) = K(\sqrt{\omega})$,
2. *if 2 is ramified in* $K/\mathbb{Q}$, *we have* $K(\sqrt{\epsilon}) = K(\sqrt{2\omega})$ *or* $K(\sqrt{\epsilon}) = K(\sqrt{\omega})$.

Furthermore, when $8 \mid d$, *the latter case occurs precisely when* $\epsilon \equiv -1 \pmod{\mathfrak{p}_2^3}$.

Proof: Let us recall some well-known results on the narrow class group of a real quadratic field. The result is due mostly to Gauss [**16**] (see also [**3**] for a more modern presentation), although Gauss' approach was via the study of indefinite binary quadratic forms. Among such forms, there are some special ones called "ambiguous forms" (see [**3**, Chapter 1, p. 7, and Chapter 3, p. 24]), which are precisely the elements of order 2 under Gauss' composition law. 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 [**3**, Proposition 4.7] and its proof).

Recall that 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. Under this correspondence, the ambiguous forms map to ideals of order 2 in the narrow class group. But such ideals correspond precisely to the ramified prime ideals of K (indexed by divisors of d), by [**3**, Corollary 4.9]. In particular, there exists a unique non-trivial and square-free principal ideal $\mathfrak{d}$ (generated by a totally positive element α) dividing the different $\mathcal{D}$ of K. Let $\omega := \mathcal{N}\mathfrak{d} = \mathcal{N}(\alpha) = \alpha\overline{\alpha}$ so that $\omega \mid d$.

Since all ramified primes are invariant under conjugation, and $\mathfrak{d}$ is divisible only by ramified primes, $\overline{\mathfrak{d}} = \mathfrak{d}$. Then the quotient $\frac{\alpha}{\overline{\alpha}} \in \mathcal{O}_K$ is a totally positive unit which cannot be trivial (as otherwise $\alpha \in \mathbb{Q}_{>0}$, but it must divide the different of K and also generate a square-free ideal of $\mathcal{O}_K$, hence equals 1). Substituting α by $\epsilon^k\alpha$ changes the quotient $\frac{\alpha}{\overline{\alpha}}$ by a factor of ϵ^{2k}, so we can assume that

$$\frac{\alpha}{\overline{\alpha}} = \epsilon.$$

Then $\sqrt{\epsilon} = \frac{\sqrt{\alpha\overline{\alpha}}}{\overline{\alpha}}$ and hence $K(\sqrt{\epsilon}) = K(\sqrt{\omega})$. We are led to determine the set of primes dividing ω. Let $\mathfrak{p}$ be a prime ideal dividing $\mathcal{D}$ and assume that $\mathfrak{p} \nmid 2$.

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

If $2 \nmid d$, then $\omega = \prod_{p \in \mathcal{P}_-} p$ and the statement follows. If d is even, the only ambiguity is whether ω is even or not. Suppose that $8 \mid d$. Let $\mathfrak{p}_2$ denote the prime ideal dividing 2 ($\mathfrak{p}_2 = \langle 2, \sqrt{d/4}\rangle$). Clearly $v_{\mathfrak{p}_2}(\alpha) = v_{\mathfrak{p}_2}(\bar{\alpha}) = v_2(\omega)$. An elementary case by case analysis shows that $v_{\mathfrak{p}_2}(\alpha) \in \{0, 2\}$ if and only if $v_{\mathfrak{p}_2}(\epsilon - 1) \geq 3$ and $v_{\mathfrak{p}_2}(\epsilon + 1) = 2$. Similarly, $v_{\mathfrak{p}_2}(\alpha) \in \{1, 3\}$ if and only if $v_{\mathfrak{p}_2}(\epsilon + 1) \geq 3$ and $v_{\mathfrak{p}_2}(\epsilon - 1) = 2$ as stated. $\square$

Proof of Theorem 2.1: Keeping the previous notation, let d denote the discriminant of K. Let $\chi_{\mathfrak{p}} \colon \mathcal{O}_{\mathfrak{p}}^{\times} \to \overline{\mathbb{Q}}^{\times}$ be the character given by the following.

- 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 archimedean 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 archimedean places does not matter; both choices work). At a prime $\mathfrak{p}_2$ dividing 2, the character $\chi_{\mathfrak{p}_2}$ has conductor at most 2^3. The group structure of $(\mathcal{O}_{\mathfrak{p}_2}/2^n)^{\times}$ and its generators when 2 does not split are given in Table 2.1 (see [**28**]). The generators are ordered so that the order of the generator i matches the i-th factor of the group structure, while the element norms are modulo 8.

Condition	n	Structure	Generators	Norms
$d \equiv 5 \pmod 8$	3	$\mathbb{Z}/3 \times \mathbb{Z}/4 \times \mathbb{Z}/2 \times \mathbb{Z}/2$	$\{\zeta_3, \sqrt{d}, 3 + 2\sqrt{d}, -1\}$	$\{1, 3, 5, 1\}$
$d/4 \equiv 7 \pmod 8$	3	$\mathbb{Z}/4 \times \mathbb{Z}/4 \times \mathbb{Z}/2$	$\{\sqrt{d/4}, 1 + 2\sqrt{d/4}, 5\}$	$\{1, 5, 1\}$
$d/4 \equiv 3 \pmod 8$	3	$\mathbb{Z}/4 \times \mathbb{Z}/4 \times \mathbb{Z}/2$	$\{\sqrt{d/4}, 1 + 2\sqrt{d/4}, -1\}$	$\{5, 5, 1\}$
$8 \mid d$	2	$\mathbb{Z}/4 \times \mathbb{Z}/2$	$\{1 + \sqrt{d/4}, -1\}$	$\{3, 1\}$

TABLE 2.1.

The definition of $\chi_{\mathfrak{p}_2}$ on this set of generators for $(\mathcal{O}_{\mathfrak{p}_2}/2^3)^\times$ is the following:

- If $d \equiv 5 \pmod 8$, $\chi_{\mathfrak{p}_2}(\zeta_3) = 1$, $\chi_{\mathfrak{p}_2}(\sqrt{d}) = i$, $\chi_{\mathfrak{p}_2}(3 + 2\sqrt{d}) = 1$, $\chi_{\mathfrak{p}_2}(-1) = 1$.
- If $d/4 \equiv 7 \pmod{16}$, $\chi_{\mathfrak{p}_2}(\sqrt{d/4}) = -1$, $\chi_{\mathfrak{p}_2}(1 + 2\sqrt{d/4}) = 1$, $\chi_{\mathfrak{p}_2}(5) = -1$.
- If $d/4 \equiv 15 \pmod{16}$, $\chi_{\mathfrak{p}_2}(\sqrt{d/4}) = 1$, $\chi_{\mathfrak{p}_2}(1 + 2\sqrt{d/4}) = 1$, $\chi_{\mathfrak{p}_2}(5) = -1$.
- If $d/4 \equiv 3 \pmod{16}$, $\chi_{\mathfrak{p}_2}(\sqrt{d/4}) = -1$, $\chi_{\mathfrak{p}_2}(1 + 2\sqrt{d/4}) = 1$, $\chi_{\mathfrak{p}_2}(-1) = -1$.
- If $d/4 \equiv 11 \pmod{16}$, $\chi_{\mathfrak{p}_2}(\sqrt{d/4}) = 1$, $\chi_{\mathfrak{p}_2}(1 + 2\sqrt{d/4}) = 1$, $\chi_{\mathfrak{p}_2}(-1) = -1$.
- If $d/4 \equiv 6 \pmod 8$ and $\#Q_3 + \#Q_5$ is even, $\chi_{\mathfrak{p}_2}(1 + \sqrt{d/4}) = 1$, $\chi_{\mathfrak{p}_2}(-1) = 1$, $\chi_{\mathfrak{p}_2}(5) = 1$.
- If $d/4 \equiv 6 \pmod 8$ and $\#Q_3 + \#Q_5$ is odd, $\chi_{\mathfrak{p}_2}(1 + \sqrt{d/4}) = i$, $\chi_{\mathfrak{p}_2}(-1) = -1$, $\chi_{\mathfrak{p}_2}(5) = 1$.
- If $d/4 \equiv 2 \pmod 8$ and $\#Q_3 + \#Q_5$ is even, $\chi_{\mathfrak{p}_2}(1 + \sqrt{d/4}) = 1$, $\chi_{\mathfrak{p}_2}(-1) = -1$, $\chi_{\mathfrak{p}}(5) = 1$.
- If $d/4 \equiv 2 \pmod 8$ and $\#Q_3 + \#Q_5$ is odd, $\chi_{\mathfrak{p}_2}(1 + \sqrt{d/4}) = i$, $\chi_{\mathfrak{p}_2}(-1) = 1$, $\chi_{\mathfrak{p}_2}(5) = 1$.

Lastly,

- 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).

Following the notation of [**25**], we denote $\chi_2 = \prod_{\mathfrak{p}_2 | 2} \chi_{\mathfrak{p}_2}$.

There are some constraints on the values of $\#Q_3$, $\#Q_5$, and $\#Q_7$ depending on the congruence of d (or $d/4$) modulo 8; they are given in Table 2.2.

Condition	$\#Q_3$	$\#Q_5$	$\#Q_7$	Condition	$\#Q_3$	$\#Q_5$	$\#Q_7$
$d \equiv 1 \pmod 8$	0	0	1	$d \equiv 5 \pmod 8$	0	1	1
	1	1	0		1	0	0
$d/4 \equiv 3 \pmod 8$	0	1	0	$d/4 \equiv 7 \pmod 8$	0	0	0
	1	0	1		1	1	1
$d/4 \equiv 2 \pmod 8$	0	0	1	$d/4 \equiv 6 \pmod 8$	0	0	0
	0	1	1		0	1	0
	1	0	0		1	0	1
	1	1	0		1	1	1

TABLE 2.2.

Using such relations and the previous definitions, it is not hard to verify that in all cases

$$\chi_2|_{\mathbb{Z}_2^\times} = \delta_2^{v_2(d)+1}\delta_{-1}^{\#Q_5+\#Q_7+1}. \tag{7}$$

Extend χ to $K^\times \cdot \left(\prod_{\mathfrak{q}} \mathcal{O}_{\mathfrak{q}}^\times \times (\mathbb{R}^\times)^2\right)$ by making it trivial on $K^\times$. With these definitions, the same proof given in [**25**, Theorem 3.2, p. 14] proves that the equality $\chi^2 = \varepsilon \circ \mathcal{N}$ holds.

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 [**25**, Theorem 3.2] 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 χ satisfies $\chi_{\mathfrak{p}}(\epsilon) = 1$ for all unramified primes and for primes in $\mathcal{P}_- \cap (Q_1 \cup Q_3)$ (recall that the character $\chi_{\mathfrak{p}}$ has order 2 at primes in Q_1 and is trivial at primes in Q_3). Its value at primes in $\mathcal{P}_- \cap (Q_5 \cup Q_7)$ equals -1. Since the character δ_{-2} also satisfies that it takes the value -1 at primes in $Q_5 \cup Q_7$ and $+1$ at the other ones, we need to prove the following identity

$$\chi_2(\epsilon) \cdot (-1)^{\#(\mathcal{P}_- \cap (Q_5 \cup Q_7))} = \chi_2(\epsilon)\delta_{-2}(\omega) = 1, \tag{8}$$

where $\omega = \prod_{p \in \mathcal{P}_-} p$ as before. The proof of Theorem 2.2 implies that there exists $\alpha \in \mathcal{O}_K$ such that $\omega = \epsilon\overline{\alpha}^2$ or $2\omega = \epsilon\overline{\alpha}^2$. In the first case,

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

Since ε_2 is at most quadratic, it equals its inverse. Hence $\chi_2(\epsilon) = \chi_2(\omega)\varepsilon_2(\omega)$ and then equation (8) is equivalent to the statement

$$\chi_2(\omega)\varepsilon_2(\omega)\delta_{-2}(\omega) = 1. \tag{9}$$

A key fact is that the hypothesis $\mathcal{N}(\alpha) = \omega$ imposes a constraint on its possible values. Using equation (7), 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 (9) holds.
- If $d/4 \equiv 3 \pmod 8$, the norm condition implies that ω 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 and 5 hence (9) holds.

- If $d \equiv 5 \pmod 8$, by definition $\chi_2|_{\mathbb{Z}_2^\times} = \delta_2$ and $\varepsilon_2 = \delta_{-1}$ hence (9) holds.
- If $d/4 \equiv 7 \pmod 8$, the norm condition implies that ω is congruent to 1 or 5 modulo 8. By definition $\chi_2|_{\mathbb{Z}_2^\times} = \delta_2$ and $\varepsilon_2 = 1$. But δ_2 and δ_{-2} take the same values at $\{1, 5\}$ hence (9) holds.
- If $d/4 \equiv 2 \pmod 8$, the norm condition implies that ω 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 (9) holds.
- If $d/4 \equiv 6 \pmod 8$, the norm condition implies that ω 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 (9) holds.

If d is odd, the equality $\omega = \epsilon\bar{\alpha}^2$ always holds hence the result follows. Assume then that 2 ramifies in $K/\mathbb{Q}$ and that $2\omega = \epsilon\bar{\alpha}^2$. Let $\mathfrak{p}_2$ denote the unique prime of K dividing 2. To ease notation, let $\tilde{d} = d/4$. Recall that $K(\sqrt{\epsilon})$ is unramified at $\mathfrak{p}_2$ if and only if ϵ is a square mod 4 (see for example [**7**, Lemma 3.4]). The equality $2\omega = \epsilon\overline{\alpha}^2$ implies that

$$\left(\frac{2}{\overline{\alpha}}\right)^2 \omega = 2\epsilon. \tag{10}$$

Note that $\frac{2}{\overline{\alpha}}$ has positive valuation at $\mathfrak{p}_2$, hence we can reduce equality (10) modulo 16 to compute for each possible value of ϵ the corresponding value of ω (up to squares) via a finite computation. 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 (10) proves that the value ω attached to a fundamental unit of the form $a + b\sqrt{d_1}$ equals that attached to $a + b\sqrt{d_2}$. In particular, it is enough to perform the finite computation for $\tilde{d}$ modulo 16.

If $\tilde{d} \equiv 3 \pmod 4$ and $t \mid d$, then 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 when $\tilde{d} \equiv 3 \pmod 8$ and $\{\sqrt{d}/2, 1 + \sqrt{d}, 5\}$ when $\tilde{d} \equiv 7 \pmod 8$. Consider the different cases, taking into account once again that the condition 2ω being a norm implies that $\omega \equiv 3, 7 \pmod 8$ when $\tilde{d} \equiv 3 \pmod 8$ and $\omega \equiv 1, 5 \pmod 8$ when $\tilde{d} \equiv 7 \pmod 8$. Then:

- If $\tilde{d} \equiv 3, 7 \pmod{16}$, the possible values for ϵ (given as generators' exponents) and the values of ω are given in Table 2.3. Since $\chi_2((a, b, c)) = (-1)^{a+c}$ (again as exponents) the equality $\chi_2(\epsilon) =$

$\delta_{-2}(\omega)$ follows, recalling that $\delta_{-2}(1) = \delta_{-2}(3) = 1$ and $\delta_{-2}(5) = \delta_{-2}(7) = -1$.

$\tilde{d} \pmod{16}$	Exp.	ω	Exp.	ω	Exp.	ω	Exp.	ω
3	$(1,1,0)$	7	$(1,1,1)$	3	$(1,3,0)$	7	$(1,3,1)$	3
3	$(3,1,0)$	7	$(3,1,1)$	3	$(3,3,0)$	7	$(3,3,1)$	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 2.3. Relation between ϵ and ω 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 ω are given in Table 2.4. Since $\chi_2((a,b,c)) = (-1)^c$ in this case, the equality $\chi_2(\epsilon) = \delta_{-2}(\omega)$ holds.

$\tilde{d} \pmod{16}$	Exp.	ω	Exp.	ω	Exp.	ω	Exp.	ω
11	$(1,1,0)$	3	$(1,1,1)$	7	$(1,3,0)$	3	$(1,3,1)$	7
11	$(3,1,0)$	3	$(3,1,1)$	7	$(3,3,0)$	3	$(3,3,1)$	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 2.4. Relation between ϵ and ω for $\tilde{d} \equiv 11, 15 \pmod{16}$.

When $8 \mid d$, Theorem 2.2 implies that the case $2\omega = \epsilon\bar{\alpha}^2$ occurs precisely for $\epsilon \equiv -1 \pmod{\mathfrak{p}_2^3}$. Recall that $(\mathcal{O}_{\mathfrak{p}_2}/2^3)^\times$ 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 (10) and the fact that 2ω is the norm of an element, we search for all possible values of ϵ and ω.

- If $\tilde{d} \equiv 2 \pmod{16}$ (respectively $\tilde{d} \equiv 10 \pmod{16}$), then $\#Q_3 + \#Q_5$ is even (respectively odd). The assumption that 2ω is a norm implies that $\omega \equiv 1, 7 \pmod 8$ (respectively $\omega \equiv 3, 5 \pmod 8$). All the possible values of ϵ for each ω are given in Table 2.5, from which it follows (using the definition of χ_2) that (8) holds.
- If $\tilde{d} \equiv 6 \pmod{16}$, then $\#Q_3 + \#Q_5$ is odd. The norm condition implies that $\omega \equiv 5, 7 \pmod 8$. The possible values of ϵ and ω are given in Table 2.5, from which it follows that (8) holds.

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

TABLE 2.5. Relation between ϵ and ω for $\tilde{d} \equiv 2, 6, 10 \pmod{16}$.

- If $\tilde{d} \equiv 14 \pmod{16}$, then $\#Q_3 + \#Q_5$ is even, hence χ_2 is trivial. The norm condition implies that $\omega \equiv 1, 3 \pmod 8$ so formula (8) holds.

Once the compatibility is verified, the proof of Theorem 3.2 in [**25**] works mutatis mutandis. $\square$

3. The conductor and nebentypus of the extended representation

Let (a, b, c) be a primitive solution of (2) and let $E_{(a,b,c)}$ be the elliptic curve attached to it, with defining equation (3). The properties imposed on χ imply that the twisted representation $\rho_{E_{(a,b,c)},p} \otimes \chi$ extends to a 2-dimensional representation of $\mathrm{Gal}_{\mathbb{Q}}$.

Lemma 3.1. *Suppose that there exists an odd prime p ramifying in $K/\mathbb{Q}$. Let $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$ and let δ_K denote the quadratic character corresponding to the real quadratic extension $K/\mathbb{Q}$. Then,*

$$\chi(\sigma^2) = \varepsilon(\sigma)\delta_K(\sigma).$$

Proof: If $\sigma \in \mathrm{Gal}_K$, then the first property of Theorem 2.1 implies that $\chi(\sigma^2) = \chi(\sigma)^2 = \varepsilon(\sigma)$, so the statement is clearly true for all elements of Gal_K (since $\delta_K(\sigma) = 1$). Since Gal_K has index 2 in $\mathrm{Gal}_{\mathbb{Q}}$, it is enough to prove that the equality holds at one element of $\mathrm{Gal}_{\mathbb{Q}} \setminus \mathrm{Gal}_K$. Let p be an odd prime ramifying in the extension $K/\mathbb{Q}$, and let $L = \mathbb{Q}(\zeta_p)$ be the cyclotomic extension. The Galois group $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to the cyclic group $(\mathbb{Z}/p)^\times$. Let g be a generator. By class field theory, $\mathrm{Gal}(L/\mathbb{Q})$ is also isomorphic to the quotient $\mathbb{I}_{\mathbb{Q}}/\mathcal{N}_{L/\mathbb{Q}}(\mathbb{I}_L)$. Let σ_p be the element of $\mathrm{Gal}(L/\mathbb{Q})$ corresponding to the idèle ι_p with local coordinates

$$(\iota_p)_v = \begin{cases} g & \text{if } v = p, \\ 1 & \text{otherwise.} \end{cases}$$

Also denote by σ_p any extension of it to the whole Galois group $\mathrm{Gal}_{\mathbb{Q}}$, which is not the identity on K. As explained before, it is then enough to prove the equality at the element σ_p. Clearly $\sigma_p^2 \in \mathrm{Gal}_K$, and furthermore, it matches the transfer map from $\mathrm{Gal}_{\mathbb{Q}}^{\mathrm{ab}}$ to $\mathrm{Gal}_K^{\mathrm{ab}}$ (see for example [**31**, Chapter 8] for the definition of the transfer map). On the idèle side, the transfer map matches the natural map $\mathbb{I}_{\mathbb{Q}} \to \mathbb{I}_K$, so the element ι_p corresponds to the idèle ι_p^K of $\mathbb{I}_K$ with local components

$$(\iota_p^K)_v = \begin{cases} g & \text{if } v = \mathfrak{p}, \\ 1 & \text{otherwise.} \end{cases}$$

The value $\chi(\sigma_p^2)$ then equals $\chi(\iota_p^K) = \chi_{\mathfrak{p}}(g)$, and one of the key properties imposed on χ and ε in [**25**] is that at all odd ramified primes $\chi_{\mathfrak{p}} = \varepsilon_p \delta_{K,p}$, via the natural identification of $(\mathbb{Z}/p)^\times$ with $(\mathcal{O}_K/\mathfrak{p})^\times$. Hence the statement. $\square$

Theorem 3.2. *Suppose there exists a prime $q > 3$ ramifying in K. Then the twisted representation $\rho_{E_{(a,b,c)},p} \otimes \chi$ 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*

$$N = 2^e \cdot \prod_q q^{v_{\mathfrak{q}}(N(E_{(a,b,c)}))} \cdot \prod_{q \in Q_3} q \cdot \prod_{q \in Q_1 \cup Q_5 \cup Q_7} q^2,$$

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

$$e = \begin{cases} 1, 8 & \text{if } 2 \text{ splits}, \\ 8 & \text{if } 2 \text{ is inert}, \\ 7, 8 & \text{if } d \equiv 3 \pmod 8, \\ 5, 8 & \text{if } d \equiv 7 \pmod 8, \\ 8, 9 & \text{if } 2 \mid d. \end{cases}$$

Proof: The extension result is well known although a proof was recalled in [**25**, Theorem 4.2]. To ease notation let $\rho'_p = \rho_{E_{(a,b,c)},p} \otimes \chi$ and $\tilde{\rho}_p$ denote its extension to $\mathrm{Gal}_{\mathbb{Q}}$. The nebentypus assertion was only proved under the hypothesis that $K/\mathbb{Q}$ is imaginary quadratic. The reason is the following: we know that ρ'_p has determinant the cyclotomic character (denoted by χ_{cyc}) times ε (by Theorem 2.1), hence the determinant of $\tilde{\rho}_p$ equals $\varepsilon\chi_{\mathrm{cyc}}$ or $\varepsilon\delta_K\chi_{\mathrm{cyc}}$ (where δ_K denotes the quadratic character corresponding to the extension $K/\mathbb{Q}$). But Ribet's result (see [**30**, Theorem 4.4]) implies that the determinant of $\tilde{\rho}_p$ is odd hence the statement. When $K/\mathbb{Q}$ is real both characters take the same value at complex conjugation! How can we distinguish which one is the nebentypus of the representation $\tilde{\rho}_p$ when our extension is real? The solution is to work with another element of an inertia subgroup of $K/\mathbb{Q}$.

Fix a basis for the Tate module of the elliptic curve $E_{(a,b,c)}$ (so we can assume that the image of our representation lies in $\mathrm{GL}_2(\mathbb{Q}_p)$). Since our field K is real quadratic, we know that the Galois representation $\rho_{E_{(a,b,c)},p}$ is absolutely irreducible. In particular, any matrix commuting with its image must be a scalar matrix by Schur's lemma.

Let S denote the set of primes ramifying in $K/\mathbb{Q}$, and for each odd prime $q \in S$ let $\mathfrak{q}$ denote the prime of K dividing it. Fix one odd prime $q > 3$ in S different from p. Let $I_q \subset \mathrm{Gal}_{\mathbb{Q}}$ denote an inertia subgroup at q and $I_{\mathfrak{q}}$ its index 2 subgroup. By [**25**, Lemma 2.5] the curve $E_{(a,b,c)}$ has good reduction at $\mathfrak{q}$ hence (by the Néron–Ogg–Shafarevich criterion) $\rho'_p|_{I_{\mathfrak{q}}}$ is a scalar matrix. Let $\sigma_q \in I_q \setminus I_{\mathfrak{q}}$ and let ${}^{\sigma_q}\rho'_p(\tau) := \rho'_p(\sigma_q \tau \sigma_q^{-1})$. The character χ was constructed so that ${}^{\sigma_q}\rho'_p \simeq \rho'_p$, hence both representations are conjugate under a matrix of $\mathrm{GL}_2(\mathbb{Q}_p)$. Since $\tilde{\rho}_p$ extends ρ'_p, $\tilde{\rho}_p(\sigma_q)$ is such a matrix. Consider the following two different cases:

- If ${}^{\sigma_q}\rho'_p = \rho'_p$, then $\tilde{\rho}_p(\sigma_q)$ is a scalar matrix (by Schur's lemma), say $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda \end{smallmatrix}\right)$. In particular, $\det(\tilde{\rho}_p(\sigma_q)) = \lambda^2$. On the other hand, $\tilde{\rho}_p(\sigma_q)^2 = \rho'_p(\sigma_q^2) = \left(\begin{smallmatrix} \chi(\sigma_q^2) & 0 \\ 0 & \chi(\sigma_q^2) \end{smallmatrix}\right)$ hence in particular $\lambda^2 = \chi(\sigma_q^2) = \varepsilon(\sigma_q)\delta_K(\sigma_q)$ from Lemma 3.1, so $\det(\tilde{\rho}_p) = \varepsilon\delta_K\chi_{\mathrm{cyc}}$.
- If ${}^{\sigma_q}\rho'_p \neq \rho'_p$, $\tilde{\rho}_p(\sigma_q)^2 = \rho'_p(\sigma_q^2)$ is a scalar matrix, then we can choose another basis of the Tate module so that the matrix $\tilde{\rho}_p(\sigma_q)$ equals the matrix $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & -\lambda \end{smallmatrix}\right)$. Then $\det(\tilde{\rho}_p(\sigma_q)) = -\lambda^2$. Once again, $\tilde{\rho}_p(\sigma_q)^2 = \rho'_p(\sigma_q^2) = \left(\begin{smallmatrix} \chi(\sigma_q^2) & 0 \\ 0 & \chi(\sigma_q^2) \end{smallmatrix}\right)$ hence in particular Lemma 3.1 (and the fact that $\delta_K(\sigma_q) = -1$) implies that $\det(\tilde{\rho}_p(\sigma_q)) = -\lambda^2 = -\chi(\sigma_q^2) = -\varepsilon(\sigma_q)\delta_K(\sigma_q) = \varepsilon(\sigma_q)$ so $\det(\tilde{\rho}_p) = \varepsilon\chi_{\mathrm{cyc}}$.

Then we are left to prove that ${}^{\sigma_q}\rho'_p \neq \rho'_p$ (a result independent of the prime $q \in S$). Recall that $\rho'_p = \rho_{E_{(a,b,c)},p} \otimes \chi$, hence the statement is equivalent to proving that ${}^{\sigma_q}\rho_{E_{(a,b,c)},p} \neq \rho_{E_{(a,b,c)},p} \cdot \delta_{-2}$ (since ${}^{\sigma_q}\chi = \chi\delta_{-2}$). Consider both actions for $\tau \in \mathrm{Gal}_K$ on points of $E_{(a,b,c)}$ of order p^n: the left-hand side equals $\sigma_q \cdot \tau \cdot \sigma_q^{-1}(P)$, while the right-hand side equals $\delta_{-2}(\tau)\tau(P)$.

Consider the 2-isogeny $\phi\colon E_{(a,b,c)} \to \overline{E_{(a,b,c)}}$ explicitly given by

$$\phi(x,y) = (\phi_1(x,y), \phi_2(x,y)) = \left(\frac{-y^2}{2x^2}, \frac{y(2a^2 + 2\sqrt{d}b - x^2)}{2\sqrt{-2}x^2}\right).$$

Note in particular that

$$\delta_{-2}(\tau) \cdot \tau \circ \phi = \phi \circ \tau \text{ for all } \tau \in \mathrm{Gal}_K, \tag{11}$$

where we consider $\delta_{-2}(\tau)$ as an endomorphism of $E_{(a,b,c)}$. The hypothesis on p being odd implies that for all positive integers n, the map $\phi\colon E_{(a,b,c)}[p^n] \to \overline{E_{(a,b,c)}}[p^n]$ is bijective. Then if $P \in E_{(a,b,c)}[p^n]$, we have

$$\begin{aligned}\sigma_q \cdot \tau \cdot \sigma_q^{-1}(P) &= (\sigma_q \cdot \phi^{-1})(\phi\tau\phi^{-1})(\sigma_q \cdot \phi^{-1})^{-1}(P)\\ &= \delta_{-2}(\tau)(\sigma_q \cdot \phi^{-1})\tau(\sigma_q \cdot \phi^{-1})^{-1}(P),\end{aligned}$$

where the last equality follows from (11). Take n large enough so that the representation on p^n-torsion points (which we denote by ρ_n) is absolutely irreducible. Then, by Schur's lemma, ${}^{\sigma_q}\rho_n = \rho_n \cdot \delta_{-2}$ if and only if the endomorphism $\sigma_q\phi^{-1}$ acts as a scalar matrix on $E_{(a,b,c)}[p^n]$. Since the Galois representation of an elliptic curve is a part of a compatible family (and the nebentypus does not depend on the choice of the prime p), it is enough to consider the case $p = 3$ and prove that $\sigma_q\phi^{-1}$ acting on the 3-torsion points is not equal to multiplication by ± 1 (then it cannot act as multiplication by an integer on points of order 3^n).

Note that -1 acts trivially on the x-coordinates of torsion points, hence it is enough to prove that on the x-coordinate of the 3-torsion points the elements σ_q and ϕ do not coincide. Let $M = K(x(E_{(a,b,c)}[3]))$ denote the extension of K obtained by adding to K the x-coordinates of all points in $E_{(a,b,c)}[3]$ (a degree 2 subextension of $K(E_{(a,b,c)}[3])$). Note on the one hand that ϕ maps x-coordinates of 3-torsion points of $E_{(a,b,c)}$ to x-coordinates of 3-torsion points of $\overline{E_{(a,b,c)}}$, but also, the map ϕ_1 is given by a polynomial in x with coordinates in K. More concretely,

$$\phi_1(x) = -\frac{x^3 + 4ax^2 + 2(a^2 + \sqrt{d}b)x}{2x^2}. \tag{12}$$

This implies that M is a Galois extension of $\mathbb{Q}$. Clearly, both K and $\mathbb{Q}(\sqrt{-3})$ are subfields of M (since the determinant of our representation is the cyclotomic character modulo 3). In particular, $\mathbb{Q}(\sqrt{-3d})$ is contained in M. Since the ramification degree of q in $M/\mathbb{Q}$ is 2 (because $E_{(a,b,c)}$ has good reduction at the prime dividing q), it must be the case that $\mathbb{Q}(\sqrt{-3}) \subset M^{\sigma_q}$ (since σ_q fix neither $\sqrt{d}$ nor $\sqrt{-3d}$).

For a generic curve $y^2 = x^3 + \alpha x^2 + \beta x$, its 3-division polynomial (whose roots generate the extension M/K) is given by

$$\psi_3(x) = 3x^4 + 4\alpha x^3 + 6\beta x^2 - \beta^2$$

(recall that in our case $\alpha = 4a$ while $\beta = 2(a^2 + \sqrt{d}b)$). Let $\theta_1, \dots, \theta_4$ be the roots of ψ_3 and let $\bar{\beta} = \frac{\alpha^2 - 4\beta}{4}$ (in our case $\bar{\beta}$ matches the conjugate of β). Then

$$\frac{\Delta(\psi_3)}{2^{12} \cdot 3^2 \cdot \beta^4 \cdot \bar{\beta}^2} = \left(\frac{\prod_{i<j}(\theta_i - \theta_j)}{2^6 \cdot 3 \cdot \beta^2 \cdot \bar{\beta}}\right)^2 = -3. \tag{13}$$

In particular, since σ_q fixes $\sqrt{-3}$, it must fix the quotient $\frac{\prod_{i<j}(\theta_i - \theta_j)}{2^6 \cdot 3 \cdot \beta^2 \cdot \bar{\beta}}$, and since σ_q is not the identity in K, it must send β to $\bar{\beta}$ and vice versa. In particular,

$$\sigma_p\left(\prod_{i<j}(\theta_i - \theta_j)\right) = \prod_{i<j}(\sigma_p(\theta_i) - \sigma_p(\theta_j)) = \prod_{i<j}(\theta_i - \theta_j) \cdot \frac{\bar{\beta}}{\beta}.$$

On the other hand, for $i \neq j$, using (12) we get

$$\phi_1(\theta_i)-\phi_1(\theta_j)=-\frac{\theta_i^2+\alpha\theta_i+\beta}{2\theta_i}+\frac{\theta_j^2+\alpha\theta_j+\beta}{2\theta_j}=(-1)(\theta_i-\theta_j)\frac{(\theta_i\theta_j-\beta)}{2\theta_i\theta_j}.$$

It is not hard to verify that if $\{\theta_1,\dots,\theta_4\}$ are roots of a monic polynomial $x^4+A_1x^3+A_2x^2+A_3x+A_4$, then

$$\prod_{i<j}(\theta_i\theta_j-\beta)=\beta^6-A_2\beta^5+(A_1A_3-A_4)\beta^4+(2A_4A_2-A_4A_1^2-A_3^2)\beta^3 + (A_4A_3A_1-A_4^2)\beta^2-A_4^2A_2\beta+A_4^3.$$

Using this formula for ψ_3, we obtain

$$\prod_{i<j}(\theta_i\theta_j-\beta)=\frac{16\beta^5}{27}(\alpha^2-4\beta)=\frac{64\beta^5\bar{\beta}}{27}.$$

Then

$$\prod_{i<j}(\phi_1(\theta_i)-\phi_1(\theta_j))=(-1)^6\prod_{i<j}(\theta_i-\theta_j)\left(\frac{-\bar{\beta}}{\beta}\right).$$

In particular, the action of ϕ_1 and σ_q do not match in the roots θ_i so the claim follows. $\square$

Remark 2. 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 $q = 3 \in S$). While working with 5-torsion points, formula (13) 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 2 element in the Galois group $\mathrm{Gal}(K(E_{(a,b,c)}[p])/\mathbb{Q})$. In particular computed examples the result holds (but we do not have a general proof).

4. Ellenberg's result

Let $K/\mathbb{Q}$ be a quadratic extension, and let E/K be a $\mathbb{Q}$-curve 2-isogenous to its Galois conjugate with a prime $\ell > 3$ of potentially multiplicative reduction. Then, following ideas of Darmon and Merel, Ellenberg proved (in Propositions 3.2, 3.4, 3.14, and Section 4 of [**13**]) that the projective modulo p representation of E is surjective if either:

- there exists $f \in S_2(2p^2)$ such that $w_pf = f$ and $w_2f=-f$, or
- there exists $f \in S_2(p^2)$ such that $w_pf = f$,

with $L(f \otimes \delta_K, 1) \neq 0$. Recall here that if $f = \sum_n a_n q^n$ is a modular form and ψ is a Dirichlet character, then $f \otimes \psi$ denotes the newform attached to the modular form $\sum_n a_n \psi(n) q^n$.

An important result of Ellenberg (see [**13**, Proposition 3.9]) proves that if K is an imaginary quadratic field, then there is always a modular form satisfying the second hypothesis for p large enough.

Proposition 4.1. *If $K/\mathbb{Q}$ is a real quadratic field in which p is unramified, then 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 [**4**, §I.5] that if $f \in S_2(N)$ is a newform and ψ is a Dirichlet character whose conductor is prime to N, then $\epsilon(f \otimes \psi) = \epsilon(f)\psi(-N)$. Suppose that $f \in S_2(p^2)$ satisfies that $w_p f = f$, so its root number equals -1 (recall that the root number equals minus the sign of the canonical involution). Then if p is unramified in $K/\mathbb{Q}$, the twisted form $f \otimes \delta_K$ also has root number -1 (since $\delta_K(-p^2) = 1$ for K real quadratic), so $L(f \otimes \delta_K, 1) = 0$.

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 and Lehner (see [**1**, 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. $\square$

Suppose then that 2 splits in $K/\mathbb{Q}$. Ellenberg's proof of the existence of a newform with prescribed properties consists in 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 this space have zero central value). While considering the space $S_2(2p^2)^{\mathrm{new}}$ 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 also imposing a condition to the Atkin–Lehner sign at 2). This computation was carried out in [**20**] (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 recommend the reader to have a copy of [**20**] at hand for the rest of this section as we follow its notations and definitions, specially Section 6 of said article).

The inequality $J_1(x) \le \frac{|x|}{2}$ and $|S(1,n;c)| < \sqrt{c}\tau(c)$ (used in Ellenberg's article) turns inequality (6.3) of [**20**] into

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

for $x \ge 71$ (using that $(1-e^{-2\pi/x})^{-1} \le \frac{x}{6}$ when $x \ge 71$). The same bound for J_1 gives the explicit inequality for equation (6.4) of [**20**]:

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

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 [**20**]. Suppose that $N \ne Q$, so in the following sum there is no term for $c = D$:

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

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

$$\begin{aligned}\sum_{\substack{c<x^2\\(N/Q)|c}}\frac{(\log(Dc)+1)}{c} &= \frac{Q}{N}\left(\left(1+\log\left(\frac{DN}{Q}\right)\right)\sum_{b=1}^{\frac{x^2Q}{N}}\frac{1}{b} + \sum_{b=1}^{\frac{x^2Q}{N}}\frac{\log(b)}{b}\right)\\ &\le \frac{Q}{N}\left(\left(1+\log\left(\frac{DN}{Q}\right)\right)\left(1+\log\left(\frac{x^2N}{Q}\right)\right) + \frac{\log^2\left(\frac{x^2N}{Q}\right)}{2}\right),\end{aligned}$$

where the last inequality comes from the usual comparison between the series and the integral. To bound the sum $\sum_{c>X^2}\frac{\tau(c)}{c^{3/2}}$, recall the following inequalities:

- For all real $s > 1$, $\sum_{n\ge X}\frac{1}{n^s} \le -\frac{X^{1-s}}{1-s} + \frac{X^{-s}}{2}$ (see for example [**34**, Lemma 3.1]).
- For $X > 1$ a real number, $\sum_{d\le X}\frac{1}{d} \le \log(X) + \gamma + \frac{7}{12X}$, where γ is the Euler–Mascheroni constant, $\gamma \le 0.58$ (see equation (3.1) of [**11**]).

Then, if $s > 1$,

$$
\begin{aligned}
\sum_{n\geq X}\frac{\tau(n)}{n^s} &= \sum_{n\geq X}\Big(\sum_{d\mid n}\frac{1}{n^s}\Big) = \sum_{d}\frac{1}{d^s}\sum_{m\geq X/d}\frac{1}{m^s}\\
&\leq \zeta(s)\sum_{d>X}\frac{1}{d^s} + \sum_{d\leq X}\frac{1}{d^s}\Big(-\frac{(X/d)^{1-s}}{(1-s)} + \frac{(X/d)^{-s}}{2}\Big)\\
&\leq \zeta(s)\Big(-\frac{X^{1-s}}{(1-s)} + \frac{X^{-s}}{2}\Big) - \frac{X^{1-s}}{(1-s)}\sum_{d\leq X}\frac{1}{d} + \frac{X^{1-s}}{2}\\
&\leq \zeta(s)\Big(-\frac{X^{1-s}}{(1-s)} + \frac{X^{-s}}{2}\Big)\\
&\quad - \frac{X^{1-s}}{(1-s)}\Big(\log(X) + \gamma + \frac{7}{12X}\Big) + \frac{X^{1-s}}{2}.
\end{aligned}
$$

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

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

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

$$
\begin{aligned}
\frac{|A_{N,Q}(x)|}{2\pi} \leq{}& \frac{12\sqrt{D}e^{-2\pi/x}}{N\pi}\\
&\times\left(\left(\log\left(\frac{DN}{Q}\right)+1\right)\left(1+\log\left(\frac{x^2N}{Q}\right)\right)+\frac{\log^2\left(\frac{x^2N}{Q}\right)}{2}\right)\\
&+\frac{2\pi}{N}\sqrt{Q/N}\,\tau(N/Q)\log(x)e^{-2\pi/x}.
\end{aligned}
\tag{14}
$$

When $N = Q$, there is an extra term $\frac{\pi}{3}\frac{xe^{\frac{-2\pi}{x}}\tau(D)}{ND^{3/2}}$ corresponding to the value $c = D$. Using the fact that $B_{N,Q}(x) = A_{N,Q}(D^2N/x)$, we get the bound

$$\frac{|B_{N,Q}(x)|}{2\pi} \leq \frac{|A_{N,Q}(D^2N/x)|}{2\pi} + \delta_{Q=N}\frac{\pi}{3}\frac{\sqrt{D}}{x}\tau(D)e^{\frac{-2\pi x}{ND^2}}. \tag{15}$$

Recall that $(a_1, L_\chi)_{2p^2}^{+_{p^2},\text{new}} = (a_1, L_\chi)_{2p^2}^{+_{p^2}} - \frac{1}{p-1}(a_1, L_\chi)_{2p}^{\chi(p)_p}$ (see [**20**, Lemma 4.1]), hence formulas (6.1), (6.2) of [**20**] give

$$\begin{aligned} \frac{1}{2\pi}(a_1, L_\chi)_{2p^2}^{+_{p^2},\text{new}} &\geq \frac{(p-2)}{(p-1)}e^{-2\pi/x} \\ &- \left(|A_{2p^2,1}(x)| + |A_{2p^2,p^2}(x)| + \frac{|A_{2p,1}(x)|}{p-1} + \frac{|A_{2p,p}(x)|}{p-1}\right. \\ &\left. + |B_{2p^2,2p^2}(x)| + |B_{2p^2,2}(x)| + \frac{|B_{2p,2p}(x)|}{p-1} + \frac{|B_{2p,2}(x)|}{p-1}\right). \end{aligned} \tag{16}$$

Taking x of the same magnitude as p (in our applications we will take $x = p \cdot \kappa$ 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.

5. Examples

In this section, instead of working with fundamental discriminants, we take values of d which are square-free. We applied the method to study solutions of (2) for square-free values $1 \leq d \leq 20$ and $d = 129$. The field $\mathbb{Q}(\sqrt{6})$ is the first one where the fundamental unit has norm 1 and also 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 also where all the newforms could be discarded using Mazur's trick. For $d \in \{3, 5, 7, 14\}$ there are modular forms without complex multiplication 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 but only for primes $p > M$ (an explicit constant) with a prescribed congruence condition. A summary of the results is presented in Table 5.1. The table also contains the dimension of the weight 2 newform space (computed to discard possible solutions) as well as the dimension of the Hilbert parallel weight 2 modular form space (if one followed the classical modular approach over K). Note the dimension of the Hilbert space becomes almost infeasible from a computational point of view very soon.

d	Theorem	M	Condition on p	$\dim(S_2(N,\varepsilon))$	Hilbert space
6	5.1	19	$p \neq 97$; $p \equiv 1, 3 \pmod 8$	28, 64	96, 384
10	5.2	19	$p \neq 139$; $p \equiv 1, 3 \pmod 8$	140, 288	448, 1792
11	5.3	19	$p \neq 73$; $p \equiv 1, 3 \pmod 8$	48, 92	224, 896
19	5.4	19	$p \neq 43, 113$; $p \equiv 1, 3 \pmod 8$	80, 156	608, 2432
129	5.5	19	$p > 900$ or $p \equiv 1, 3 \pmod 8$ and $p \neq 43$	16, 1400	100, 600, 38400

TABLE 5.1.

5.1. 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 to be a very fortunate coincidence, unlikely to occur for other values.) Trivial solutions give elliptic curves with j-invariant 8000 (with complex multiplication by $\mathbb{Z}[\sqrt{-2}]$). Over $\mathbb{Q}(\sqrt{6})$ there are only two extra isomorphism classes of elliptic curves with complex multiplication whose j-invariant is not rational (see [**8**]), with j-invariants $188837384000 \pm 77092288000\sqrt{6}$. The Frey curves $E_{(\pm 7, \pm 20, 1)}$ have precisely such j-invariants!

Theorem 5.1. *Let $p > 19$ be a prime number such that $p \neq 97$ and $p \equiv 1, 3 \pmod 8$. Then, $(\pm 7, \pm 20, 1)$ are the only non-trivial primitive solutions of the equation*

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

Proof: Suppose that (a, b, c) is a non-trivial primitive solution. If $c = \pm 1$, then, by (5), $(a, b, c) = (\pm 7, \pm 20, 1)$. Hence, we are led to consider the case $c \neq \pm 1$ (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 prove that the residual representation of $E_{(a,b,c)}$ modulo p is absolutely irreducible. For that purpose we apply Theorem 1 of [**15**]. Let $\epsilon = 5+2\sqrt{6}$ be a fundamental unit. The primes dividing $\operatorname{lcm}(\mathcal{N}(\epsilon^{12} - 1), \mathcal{N}(\overline{\epsilon}^{12} - 1))$ live in $\{2, 3, 5, 11, 97\}$. Next we need to compute the characteristic polynomial at a prime of good reduction. Since $E_{(a,b,c)}$ 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 $E_{(a,b,c)}$ modulo $\mathfrak{q}$ 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 the set $\{2, 3, 5, 11, 19, 97\}$. Using Theorem 3.2 (and Remark 2) 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 $\mathbb{Q}(\sqrt{3})$.

- The space $S_2(2^8 \cdot 3, \varepsilon)$ has 10 Galois conjugacy classes, 6 of them having complex multiplication. Running Mazur's trick (see [**25**, Proposition 6.1]) for primes $5 \leq q \leq 10$ we can discard all the newforms except 3 with complex multiplication, if $p \notin \{2, 5, 7\}$. The only newforms that cannot be discarded in this space are the 3 newforms corresponding to the solutions $(\pm 1, 0, 1)$ and $(\pm 7, \pm 20, 1)$ with complex multiplication by $\mathbb{Z}[\sqrt{-2}]$.

- The space $S_2(2^9 \cdot 3, \varepsilon)$ has 13 Galois conjugacy classes, 3 of them having complex multiplication. Again, running Mazur's trick for primes $5 \le q \le 20$ allows us to discard all such newforms if $p \notin \{2, 3, 5, 7, 17\}$.

Then, assuming $p > 19$ and $p \neq 97$, we are able to lower the level and discard all the possible newforms except 3 with complex multiplication by $\mathbb{Z}[\sqrt{-2}]$. To discard the remaining ones we need to impose a congruence condition on p. If $p \equiv 1, 3 \pmod 8$, then it splits in $\mathbb{Q}(\sqrt{-2})$ and then the residual representations of the newforms with complex multiplication modulo p have image lying in the normalizer of a split Cartan subgroup. This contradicts [**13**, Proposition 3.4] (as c is divisible by a prime greater than 3). $\square$

Remark 3. While proving large image, [**15**, 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 [**24**, 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 $d \in \{10, 11, 19\}$.

5.2. The case $d = 10$. In this case we have the following result.

Theorem 5.2. *Let $p > 19$ be a prime number such that $p \neq 139$ and $p \equiv 1, 3 \pmod 8$. Then, there are no non-trivial primitive solutions of the equation*

$$x^4 - 10y^2 = z^p.$$

Proof: Let (a, b, c) be a putative non-trivial primitive solution. In this case, Theorem 2.1 implies that ε is a character of order 4 and conductor $4 \cdot 5$, while χ has order 8. As in the previous case, applying [**15**, Theorem 1] and Remark 3 for primes $q = 5, 7$, we get that $\overline{\rho_{E_{(a,b,c)},p}}$ is irreducible if p does not belong to $\{2, 3, 5, 7, 13, 31, 37\}$. Hence, by Theorem 3.2 and Ribet's lowering-the-level result, we have that there exists a newform g in $S_2(2^8 \cdot 5^2, \varepsilon)$ or in $S_2(2^9 \cdot 5^2, \varepsilon)$ whose Galois representation is congruent modulo p to $\rho_{E_{(a,b,c)},p} \otimes \chi$.

- The space $S_2(2^8 \cdot 5^2, \varepsilon)$ has 55 Galois conjugacy classes, 22 of them having complex multiplication. Running Mazur's trick for all the newforms g and primes $3 \le q \le 37$ such that $q \neq 5, 31$, we obtain that all the newforms can be discarded if $p \notin \{2, 3, 5, 7, 11, 17, 19, 23\}$ except for the 2 newforms coming from the trivial solutions, with complex multiplication by $\mathbb{Z}[\sqrt{-2}]$.

- The space $S_2(2^9\cdot 5^2,\varepsilon)$ has 40 newforms, 10 of them having complex multiplication. In this case Mazur's trick for primes $q \neq 5$ such that $3 \le q \le 20$ discards all the newforms in the space if $p \notin \{2,3,5,7,11,13,17,23\}$.

Hence, assuming $p \notin \{2,5,7,11,13,17,19,23,31,37\}$, it only remains to discard the 2 newforms with complex multiplication belonging to the first space. Since the solution is primitive, c is odd (see [**25**, Lemma 2.4]). If c is divisible by 3, then we can use Mazur's trick with $q = 3$, getting that $p \mid \mathcal{N}(16\varepsilon^{-1}(3) - a_3(g)^2)$ (see the last line of the definition of $B(g,q;a,b,c)$), so $p \in \{2,5\}$. Hence c is not divisible by 3 and we are in the hypothesis of [**13**, Proposition 3.4]. Then, once again, we can discard the remaining 2 newforms when $p \equiv 1,3 \pmod 8$. □

5.3. The case $d = 11$. In this case we have the following result.

Theorem 5.3. *Let $p > 19$ be a prime number such that $p \neq 73$ and $p \equiv 1,3 \pmod 8$. Then, there are no non-trivial primitive solutions of the equation*

$$x^4 - 11y^2 = z^p.$$

Proof: Let (a,b,c) be a non-trivial primitive solution. By Theorem 2.1 we have that ε is of order 2 and conductor $4\cdot 11$, and χ is of order 4. Applying [**15**, Theorem 1] (and using again the strategy of Remark 3) for primes $q = 11, 13$ we get that if p does not belong to $\{2,3,5,7,11,17,19,73,397\}$, then $\overline{\rho_{E_{(a,b,c)},p}}$ is absolutely irreducible and we can apply Ribet's lowering-the-level result, so Theorem 3.2 implies the existence of a newform g in $S_2(2^7\cdot 11,\varepsilon)$ or in $S_2(2^8\cdot 11,\varepsilon)$ congruent modulo p to $\rho_{E_{(a,b,c)},p}\otimes\chi$.

- The space $S_2(2^7\cdot 11,\varepsilon)$ has 4 Galois conjugacy classes, none of them with complex multiplication. Running Mazur's trick for primes $3 \le q \le 10$ we can discard all the newforms if $p > 7$.
- The space $S_2(2^8\cdot 11,\varepsilon)$ has 15 Galois conjugacy classes, 7 of them having complex multiplication. 2 of the newforms with complex multiplication correspond to the trivial solutions $(\pm1,0,1)$. Running Mazur's trick for the other 13 newforms, for primes $q \neq 11$ such that $3 \le q \le 43$, we can discard them if $p > 19$. To discard the remaining 2 newforms we need the hypothesis $p \equiv 1,3 \pmod 8$ and use [**13**, Proposition 3.4]. □

5.4. The case $d = 19$. In this case we have the following result.

Theorem 5.4. *Let $p > 19$ be a prime number such that $p \neq 43, 113$ and $p \equiv 1, 3 \pmod 8$. Then, there are no non-trivial primitive solutions of the equation*

$$x^4 - 19y^2 = z^p.$$

Proof: Let (a, b, c) be a non-trivial primitive solution. To prove that the residual representation of $E_{(a,b,c)}$ modulo p is absolutely irreducible we apply [**15**, Theorem 1] for $q = 19$ and follow Remark 3 for the prime $q = 7$, obtaining that $\rho_{E_{(a,b,c)},p}$ has absolutely irreducible reduction if $p \notin \{2, 3, 5, 11, 13, 17, 19, 31, 43, 113, 115597\}$, so we are going to assume this hypothesis from now on.

The character ε has order 2 and conductor $4 \cdot 19$, while χ is of order 4. Then Ribet's lowering-the-level result together with Theorem 3.2 imply that we have to search for a newform g in one of the spaces $S_2(2^7 \cdot 19, \varepsilon)$ or $S_2(2^8 \cdot 19, \varepsilon)$.

- The space $S_2(2^7 \cdot 19, \varepsilon)$ has 4 Galois conjugacy classes, none of them with complex multiplication. Using Mazur's trick with primes $3 \leq q \leq 17$ we are able to discard all the newforms (in fact we just need $p > 2$).
- The space $S_2(2^8 \cdot 19, \varepsilon)$ has 18 Galois conjugacy classes, 7 of them having complex multiplication. With the above assumption on p (and in fact just assuming $p > 19$), we can use Mazur's trick with primes $3 \leq q \leq 17$ and discard all the newforms but 2 of them, corresponding to the trivial solutions (and having complex multiplication by $\mathbb{Z}[\sqrt{-2}]$).

To discard these 2 newforms with complex multiplication, we proceed as before. Since the solution is primitive, c must be odd. Suppose that c is divisible by 3. Then, the fact that $p \mid \mathcal{N}(16\varepsilon(3)^{-1} - a_3(g)^2)$ implies that $p \in \{2, 3\}$, which gives a contradiction. Hence c is not divisible by 3 and then we are in the hypothesis of [**13**, Proposition 3.4], so we can discard the newforms attached to the trivial solutions under the assumption $p \equiv 1, 3 \pmod 8$. $\square$

5.5. The case $d = 129$. The prime 2 splits in $\mathbb{Q}(\sqrt{129})$, hence Ellenberg's result (as described in Section 4) can be applied to discard the trivial solutions as well.

Theorem 5.5. *Let $p > 19$ be a prime number satisfying that either $p > 900$ or $p \equiv 1, 3 \pmod 8$ and $p \neq 43$. Then, there are no non-trivial primitive solutions of the equation*

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

Proof: As before, let (a, b, c) be a non-trivial primitive solution, and $E_{(a,b,c)}$ the Frey curve attached to it. [**15**, 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 [**23**, Lemma 3.2]. Suppose that the residual extended representation $\tilde{\rho}_p$ at a prime p is reducible; say its semisimplification is given by $\theta_1 \oplus \theta_2$. Then the residual representation of $\rho_{E_{(a,b,c)},p}$ is isomorphic to $\chi^{-1}\theta_1|_{\mathrm{Gal}_K} \oplus \chi^{-1}\theta_2|_{\mathrm{Gal}_K}$. To ease notation, let $\psi_i = \chi^{-1}\theta_i|_{\mathrm{Gal}_K}$. Since the curve $E_{(a,b,c)}$ has additive reduction only at primes dividing 2, both ψ_1 and ψ_2 are unramified outside primes dividing 2 and p. Furthermore, by [**19**, Lemma 1], one of the characters is unramified outside p (say ψ_1).

The prime 2 splits in $\mathbb{Q}(\sqrt{129})/\mathbb{Q}$; say $(2) = \mathfrak{p}_2\bar{\mathfrak{p}}_2$. By [**25**, Lemma 2.8], the conductor of $E_{(a,b,c)}$ at $(\mathfrak{p}_2, \bar{\mathfrak{p}}_2)$ equals one of $(8, 8)$, $(1, 6)$, or $(4, 6)$, hence the character ψ_1 has conductor at most 2^4, $\mathfrak{p}_2^3$, or $4 \cdot \mathfrak{p}_2$ (or their conjugates). The ray class group for such conductors has exponent 4 in the first case and 2 in the other two cases (computed using [**27**]). 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 [**10**, Theorem 1.2].

Theorem 3.2, Ribet's lowering-the-level result, and the proof of [**25**, Lemma 2.8] imply that $\rho_{E_{(a,b,c)},p} \otimes \chi$ is congruent modulo p to the Galois representation of a newform in $S_2(2\cdot 3\cdot 43, \varepsilon)$ (when c is even) or in $S_2(2^8 \cdot 3 \cdot 43, \varepsilon)$ (when c is odd), where ε corresponds to $\mathbb{Q}(\sqrt{129})$.

- The space $S_2(2 \cdot 3 \cdot 43, \varepsilon)$ has 4 Galois conjugacy classes, none of them having complex multiplication. Using Mazur's trick for primes $5 \leq q \leq 20$, all the newforms in the first space can be discarded assuming $p > 5$.
- The space $S_2(2^8 \cdot 3 \cdot 43, \varepsilon)$ has 36 Galois conjugacy classes, 18 of them having complex multiplication. Using Mazur's trick for primes $5 \leq q \leq 20$, the first 33 newforms (in `Magma`'s order) can be discarded assuming $p \notin \{2, 5, 7, 11, 13, 17, 23, 43\}$, but 4 newforms have complex multiplication by $\mathbb{Z}[\sqrt{-2}]$. The last 3 newforms do not have complex multiplication, but they do have a large coefficient field and `Magma` is unable to compute norms over these fields, so we used `Magma` to compute the coefficients a_5 and a_7 of each of these newforms and apply Mazur's trick in `PARI/GP` for $q = 5, 7$ by hand (where the norms are computed in a few seconds). It follows that they can be discarded if $p \notin \{2, 5, 7, 37\}$.

Since in this case 2 splits over K, then we can use the results of Section 4 to discard the newforms having complex multiplication. After a computer search for the minimum x we obtained that taking $x = 49885$ in (16) (using the inequalities (14) and (15)) makes the right-hand side positive for $p > 900$. This can be checked with the following command (in `PARI/GP`):

```
? read("RemoveCM");
? Bound(129,907,49885)
%2 = 0.039412707010082109791157365950637933812
```

For small primes, the same argument as in the previous examples works; note that c is divisible by an odd prime larger than 3 because it cannot be divisible by 3 (as the solution is primitive) and it is not divisible by 2 because the modular forms with complex multiplication appear in the space $S_2(2^8 \cdot 3 \cdot 43, \varepsilon)$. Then we are again in the hypothesis of [**13**, Proposition 3.4], which discards newforms with complex multiplication by $\mathbb{Z}[\sqrt{-2}]$ for primes $p \equiv 1, 3 \pmod 8$. $\square$

Remark 4. Ellenberg's bound obtained in the last example could probably be slightly improved if better bounds were given in the computations of Section 4. If the final value is not too large, a newform $f \in S_2(2p^2)$ with the desired properties could be found in the intermediate range via a computer search.

References

[1] A. O. L. Atkin and J. Lehner, Hecke operators on $\Gamma_0(m)$, *Math. Ann.* **185** (1970), 134–160. DOI: 10.1007/BF01359701.

[2] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I: The user language, *J. Symbolic Comput.* **24(3-4)** (1997), 235–265. DOI: 10.1006/jsco.1996.0125.

[3] D. A. Buell, *"Binary Quadratic Forms. Classical Theory and Modern Computations"*, Springer-Verlag, New York, 1989. DOI: 10.1007/978-1-4612-4542-1.

[4] D. Bump, *"Automorphic Forms and Representations"*, Cambridge Studies in Advanced Mathematics **55**, Cambridge University Press, Cambridge, 1997. DOI: 10.1017/CBO9780511609572.

[5] J. H. E. Cohn, The Diophantine equation $x^4 - Dy^2 = 1$, II, *Acta Arith.* **78(4)** (1997), 401–403. DOI: 10.4064/aa-78-4-401-403.

[6] D. A. Cox, *"Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication"*, Second edition, Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013. DOI: 10.1002/9781118400722.

[7] J. Cremona and A. Pacetti, On elliptic curves of prime power conductor over imaginary quadratic fields with class number 1, *Proc. Lond. Math. Soc. (3)* **118(5)** (2019), 1245–1276. DOI: 10.1112/plms.12214.

[8] H. B. Daniels and Á. Lozano-Robledo, On the number of isomorphism classes of CM elliptic curves defined over a number field, *J. Number Theory* **157** (2015), 367–396. DOI: 10.1016/j.jnt.2015.05.009.

[9] H. Darmon and A. Granville, On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$, *Bull. London Math. Soc.* **27(6)** (1995), 513–543. DOI: 10.1112/blms/27.6.513.

[10] M. Derickx, S. Kamienny, W. Stein, and M. Stoll, Torsion points on elliptic curves over number fields of small degree, Preprint (2017). arXiv:1707.00364.

[11] J.-M. Deshouillers and F. Dress, Sommes de diviseurs et structure multiplicative des entiers, *Acta Arith.* **49(4)** (1988), 341–375. DOI: 10.4064/aa-49-4-341-375.

[12] L. Dieulefait and J. Jiménez Urroz, Solving Fermat-type equations via modular $\mathbb{Q}$-curves over polyquadratic fields, *J. Reine Angew. Math.* **2009(633)** (2009), 183–195. DOI: 10.1515/CRELLE.2009.064.

[13] J. 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)** (2004), 763–787. DOI: 10.1353/AJM.2004.0027.

[14] N. Freitas, B. V. Le Hung, and S. Siksek, Elliptic curves over real quadratic fields are modular, *Invent. Math.* **201(1)** (2015), 159–206. DOI: 10.1007/s00222-014-0550-z.

[15] N. Freitas and S. Siksek, Criteria for irreducibility of mod p representations of Frey curves, *J. Théor. Nombres Bordeaux* **27(1)** (2015), 67–76. DOI: 10.5802/jtnb.894.

[16] C. F. Gauss, *"Disquisitiones arithmeticae"*, 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, Springer-Verlag, New York, 1986.

[17] C. Khare and J.-P. Wintenberger, Serre's modularity conjecture (II), *Invent. Math.* **178(3)** (2009), 505–586. DOI: 10.1007/s00222-009-0206-6.

[18] C. Khare and J.-P. Wintenberger, Serre's modularity conjecture, in: *"Proceedings of the International Congress of Mathematicians"*, Vol. II, Hindustan Book Agency, New Delhi, 2010, pp. 280–293. DOI: 10.1142/9789814324359_0051.

[19] A. Kraus, Courbes elliptiques semi-stables sur les corps de nombres, *Int. J. Number Theory* **3(4)** (2007), 611–633. DOI: 10.1142/S1793042107001127.

[20] S. 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)** (2017), 329–349. DOI: 10.4153/CMB-2016-085-6.

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

[22] W. Ljunggren, Ein Satz über die diophantische Gleichung $Ax^2 - By^4 = C$ ($C = 1, 2, 4$), in: *"Tolfte Skandinaviska Matematikerkongressen, Lund, 1953"*, Lunds Universitets Matematiska Institution, Lund, 1954, pp. 188–194.

[23] P. Michaud-Jacobs, Fermat's Last Theorem and modular curves over real quadratic fields, *Acta Arith.* **203(4)** (2022), 319–351. DOI: 10.4064/aa210812-2-4.

[24] F. Najman and G. C. Ţurcaş, Irreducibility of mod p Galois representations of elliptic curves with multiplicative reduction over number fields, *Int. J. Number Theory* **17(8)** (2021), 1729–1738. DOI: 10.1142/S1793042121500585.

[25] A. PACETTI AND L. VILLAGRA TORCOMIAN, $\mathbb{Q}$-curves, Hecke characters and some Diophantine equations, *Math. Comp.* **91(338)** (2022), 2817–2865. DOI: 10.1090/mcom/3759.

[26] L. PAN, The Fontaine–Mazur conjecture in the residually reducible case, *J. Amer. Math. Soc.* **35(4)** (2022), 1031–1169. DOI: 10.1090/jams/991.

[27] THE PARI GROUP, PARI/GP version 2.12.2 (2019). Available at http://pari.math.u-bordeaux.fr/.

[28] A. RANUM, The group of classes of congruent quadratic integers with respect to a composite ideal modulus, *Trans. Amer. Math. Soc.* **11(2)** (1910), 172–198. DOI: 10.2307/1988676.

[29] K. A. RIBET, Lowering the levels of modular representations without multiplicity one, *Internat. Math. Res. Notices* **1991(2)** (1991), 15–19. DOI: 10.1155/S107379289100003X.

[30] K. A. RIBET, Abelian varieties over $\mathbf{Q}$ and modular forms, in: *"Modular Curves and Abelian Varieties"*, Progr. Math. **224**, Birkhäuser, Basel, 2004, pp. 241–261. DOI: 10.1007/978-3-0348-7919-4_15.

[31] J.-P. SERRE, *"Local Fields"*, Translated from the French by Marvin Jay Greenberg, Graduate Texts in Mathematics **67**, Springer-Verlag, New York-Berlin, 1979. DOI: 10.1007/978-1-4757-5673-9.

[32] J.-P. SERRE, Sur les représentations modulaires de degré 2 de Gal$(\overline{\mathbf{Q}}/\mathbf{Q})$, *Duke Math. J.* **54(1)** (1987), 179–230. DOI: 10.1215/S0012-7094-87-05413-5.

[33] P. G. WALSH, Diophantine equations of the form $aX^4-bY^2=\pm1$, in: *"Algebraic Number Theory and Diophantine Analysis"* (Graz, 1998), de Gruyter, Berlin, 2000, pp. 531–554. DOI: 10.1515/9783110801958.531.

[34] S. ZUNIGA ALTERMAN, Explicit averages of square-free supported functions: to the edge of the convolution method, *Colloq. Math.* **168(1)** (2022), 1–23. DOI: 10.4064/cm8337-11-2020.

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

Lucas Villagra Torcomian
FAMAF-CIEM, Universidad Nacional de Córdoba, C.P:5000, Córdoba, Argentina
E-mail address: lucas.villagra@unc.edu.ar

Received on March 22, 2021.
Accepted on March 25, 2022.