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

ARIEL PACETTI AND LUCAS VILLAGRA TORCOMIAN

Abstract. In this article we study the equations $x^4 + dy^2 = z^p$ and $x^2 + dy^6 = z^p$ for positive square-free values of d. A Frey curve over $\mathbb{Q}(\sqrt{-d})$ is attached to each primitive solution, which happens to be a $\mathbb{Q}$-curve. Our main result is the construction of a Hecke character χ satisfying that the Frey elliptic curve representation twisted by χ extends to $\mathrm{Gal}_{\mathbb{Q}}$, therefore (by Serre's conjectures) corresponds to a newform in $S_2(\Gamma_0(n), \varepsilon)$ for explicit values of n and ε. Following some well known results and elimination techniques (together with some improvements) our result provides a systematic procedure to study solutions of the above equations and allows us to prove non-existence of non-trivial primitive solutions for large values of p of both equations for new values of d.

Introduction

Since Wiles' proof of Fermat's last theorem, there has been an increasing interest in solving different Diophantine equations. An open challenging problem is to understand solutions of a generalized Fermat type equation of the form

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

In [DG95] it was proven that for each triple of exponents (p, q, r) satisfying $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$, the set of integral primitive solutions is finite (i.e. the surface has finitely many integral points). Recall that a solution (a, b, c) to (1) is called *primitive* if the numbers $\{aA, bB, cC\}$ are pairwise coprime. As explained in [DM97], there are many instances where equation (1) posses infinitely many non-primitive solutions, one of the reason to restrict to primitive ones.

Nowadays there exists a sort of "guideline" to study solutions of equation (1). A short version of the procedure (more details will be given in Section 1) is the following: firstly attach to a non-trivial primitive solution an odd, two-dimensional Galois representations with values in $\overline{\mathbb{F}_p}$ (or in $\overline{\mathbb{Q}_p}$) with very special properties, for example that its conductor is only divisible by the primes dividing ABC (or its reduction does). The next step is to prove modularity of the representation (which in the case of rational representations follows mostly by Serre's conjectures), i.e. prove that such representation matches that of a newforms of "known" level and Nebentypus, independent of the solution (in many circumstances this goal is achieved using some result like Ribet's level lowering one). At last, one computes the particular spaces of modular forms and use different elimination techniques (some will be explained in Section 6) aiming to prove that all computed newforms are not related to solutions, hence solutions cannot exist.

The present article started as an attempt to study particular cases of equation (1), namely equation

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

and equation

$$x^2 + dy^6 = z^p, \tag{3}$$

for positive square-free values of d. For such equations, a solution is called *trivial* if one of its coordinate is zero, for example the solutions $(\pm 1, 0, 1)$ are trivial solutions of both (2) and (3) for all values of p. The first equation was studied in [Ell04] for $d = 1$ and in [DU09] for $d = 2, 3$. The articles [Ell04] and [DU09] proved what might be called "asymptotic results", namely the existence of a constant N_d such that all non-trivial primitive solutions of equation (2) have exponent $p \leq N_d$. Explicitly, the constants are $N_d = 211,349,131$

2010 *Mathematics Subject Classification.* 11D41,11F80.

Key words and phrases. $\mathbb{Q}$-curves, Fermat equations.

AP 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). LVT was supported by a CONICET grant.

for $d = 1, 2, 3$ respectively. The main contribution of [BEN10] was to extend the result for small values of p, proving non-existence of non-trivial primitive solutions for exponents $n \geq 4$ (not necessarily prime) when $d = 1$ and the existence of a unique non-trivial primitive solution for exponents $n \geq 4$ when $d = 2$.

Equation (3) was studied in [BC12] for $d = 1$ and in [Kou20] for $d = 3$, where non-existence of primitive non-trivial solutions was proved for all exponents $n \geq 3$ when $d = 1$, while there exist a unique primitive solution for exponents $n \geq 4$ when $d = 3$. The crucial connection between equations (2) and (3) is that in both cases, to a putative primitive non-trivial solution (a, b, c) one attaches an elliptic curve over the quadratic extension $K = \mathbb{Q}(\sqrt{-d})$ that has the property of being a $\mathbb{Q}$-curve (i.e. an elliptic curve E whose Galois conjugates are isogenous to E), fulfilling the first step of the general strategy shortly described before. In the case of equation (2), the representation comes from the elliptic curve (proposed in [DU09]) given by the equation

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

In the case of equation (3), in [BC12] and [Kou20] the authors attach to a solution (a, b, c) a $\mathbb{Q}$-curve with a 3-torsion point. Generalizing their ideas (and using the description of curves with a 3-torsion point given by Kubert [Kub76] we attach to a solution (a, b, c) of (3) the $\mathbb{Q}$-curve

$$\widetilde{E}_{(a,b,c)} : y^2 + 6b\sqrt{-d}xy - 4d(a + b^3\sqrt{-d})y = x^3, \tag{5}$$

where $(0, 0)$ is its natural rational point of order 3. Part of our contribution to study solutions of (3) lies in the fact that such an elliptic curve has a Galois representation fulfilling the requirements of the general strategy (as will be proved in Section 2).

A key property of $\mathbb{Q}$-curves is that their Galois representations can be "extended" to the whole Galois group, providing the second result of the general strategy. More concretely, a result of Ribet [Rib04] implies that if E/K is a $\mathbb{Q}$-curve then there exists a character χ such that the twisted Galois representation $\rho_{E,p} \otimes \chi$ extends to the whole Galois group $\mathrm{Gal}_{\mathbb{Q}}$. Ribet's result is not explicit, as it depends on trivializing a cocycle naturally attached to the $\mathbb{Q}$-curve E. In the aforementioned articles, the way the cocycle was trivialized was using an algorithm due to Quer [Que00] which gives an ad-hoc element (via Hilbert's 90 theorem) after a tedious search for it. The disadvantage of such an approach is that a priori there is no control on the ramification of the character nor a clear description of the character itself.

One of the main contributions of the present article is to provide a (computable) alternative to Ribet's approach. Namely, we give an explicit description of a Hecke character χ such that the Galois representation $\rho_{E_{(a,b,c)},p} \otimes \chi$ extends to the whole Galois group $\mathrm{Gal}_{\mathbb{Q}}$ (and a respective result for the representation $\rho_{\widetilde{E}_{(a,b,c)},p}$). To explain our approach, let us introduce some notation that will be used (and recalled) during the article. If t is an integer, let ψ_t denote the quadratic character corresponding to the quadratic extension $\mathbb{Q}(\sqrt{t})/\mathbb{Q}$. Let $L/\mathbb{Q}$ be a Galois extension, let $\rho : \mathrm{Gal}_L \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$ be a Galois representation and let $\tau \in \mathrm{Gal}_{\mathbb{Q}}$. By ${}^{\tau}\rho$ we denote the Galois representation of Gal_L given by ${}^{\tau}\rho(\sigma) = \rho(\tau\sigma\tau^{-1})$.

A key property satisfied by the curve $E_{(a,b,c)}$ is that if τ denotes any element of $\mathrm{Gal}_{\mathbb{Q}}$ not trivial on K, then ${}^{\tau}\rho_{E_{(a,b,c)},p} \simeq \rho_{E,p} \otimes \psi_{-2}$ (see Proposition 2.2). Analogously, under the same hypothesis, ${}^{\tau}\rho_{\widetilde{E}_{(a,b,c)},p} \simeq \rho_{\widetilde{E}_{(a,b,c)},p} \otimes \psi_{-3}$ (see Proposition 2.3). Recall that a representation of Gal_K extends to $\mathrm{Gal}_{\mathbb{Q}}$ if and only if ${}^{\tau}\rho \simeq \rho$, for τ as before. Although this result is well known to experts, a proof of it will be provided in Theorems 4.2 and 4.5, as we need control on the extension conductor. Note that if we can construct a finite order Hecke character $\chi_t : \mathrm{Gal}_K \to \overline{\mathbb{Q}}^{\times}$ satisfying

$${}^{\tau}\chi_t = \chi_t \cdot \psi_{-t},$$

for $t = 2, 3$, then the twisted representation $\rho_{E_{(a,b,c)},p} \otimes \chi_2$ (respectively $\rho_{\widetilde{E}_{(a,b,c)},p} \otimes \chi_3$) does extend to $\mathrm{Gal}_{\mathbb{Q}}$. The main contribution of the present article (as developed in Section 3) is to give a general strategy to construct the Hecke character χ_t. More precisely, we give a concrete explicit construction of it in the cases $t = 2$ and t a prime number which is congruent to 3 modulo 4. This result might be of independent interest, as it could be applied to other Diophantine problems involving $\mathbb{Q}$-curves.

While constructing the Hecke character, we restrict to positive values of d, since one of the steps of the construction involves verifying a compatibility condition at units of the base field. This technical problem is in general hard to verify for real quadratic fields due to the existence of fundamental units. Nevertheless, we are able to prove that our construction works when the fundamental unit of $\mathbb{Q}(\sqrt{d})$ (for d positive) has

norm -1. The case of general real quadratic fields (and applications to Diophantine problems) can be found in the sequel [PV22].

By construction, the Hecke character χ_t is ramified only at primes ramifying in $K/\mathbb{Q}$ and at t. Going back to the problem of extending the representation $\rho_{E_{(a,b,c)},p}$ (respectively $\rho_{\widetilde{E}_{(a,b,c)},p}$), this fact allows us to prove that the extended representation has residual image of conductor divisible only by primes dividing $6d$. In particular, we construct a rational representation (whose modularity follows from Serre's conjectures) with small conductor, fulfilling the first two steps of the general strategy. Moreover, in Corollaries 4.3 and 4.6 we give an explicit description of the conductor and Nebentypus of such residual representations.

To apply the last steps of the general strategy, one needs a result on the image of the residual Galois representation (needed in Ribet's lowering the level result) and an elimination procedure. For our purpose, the main result regarding residual images of Galois representations coming from $\mathbb{Q}$-curves is due to Ellenberg ([Ell04, Theorem 3.14]), which states that if a $\mathbb{Q}$-curve E over a quadratic field K happens to have a prime of multiplicative reduction larger than 3, then for all large enough primes p (say $p > N_K$), the residual image is "large" (i.e. its projective image contains $\mathrm{SL}_2(\mathbb{F}_p)$). Moreover, Elleberg's article contains bounds that allows to compute explicitly the constant N_K, which depends only on the base field K and the degree of the isogenies between E and its Galois conjugates. We included some improvements from the literature to Ellenberg's original result, and we wrote a `PARI/GP` script to compute the bound needed for the examples.

After explaining how Ellenberg's result is important to eliminate newforms with complex multiplication, we recall a strategy due to Mazur that we learned from [Sik12]. It is the main tool used in the present article to discard newforms as not coming from solutions of our equation. All the previous techniques/constructions are used to study solutions of equations (2) and (3) for the values $d = 1, 2, 3, 5, 6$ and 7 not studied before. The choice of the values for d is arbitrary, since in principle our method could be applied to other values of d, within the computational limitations of the algorithms used to construct newforms.

We succeed to prove non-existence of solutions in all cases but $d = 5$ and $d = 7$ for equation (3) (where the existence of newforms satisfying all the required properties makes the classical approach to fail). In [GPV21] more advanced elimination techniques are used to get partial results for these two cases as well.

The article is organized as follows: in Section 1 we give details of a general strategy due to Darmon for studying solutions of equation (1). In Section 2 we study the main properties of the curves (4) and (5). In particular, we prove that they are $\mathbb{Q}$-curves, compute their complete field of definition, and their local type at primes of bad reduction (getting in particular a formula for their conductor). Section 3 is devoted to the construction of the Hecke character χ_t. It starts with a general idea of its construction and main properties, while the proper construction and proofs are given in Subsection 3.1 for $t = 2$ and in Subsection 3.2 for t any prime number congruent to 3 modulo 4. The proofs are a little tedious, so we suggest the reader to avoid reading them on a first read of the article. The way to define the character χ_t is to first give its local ramification (i.e. the value of the restriction of the local components to the local ring of integers) and then extend it to the whole idèle group. Although it is not clear how the local definitions were obtained, they are the result of many computational experiments done with a script wrote in `PARI/GP` ([PAR19]) for that purpose, and a meticulous task of finding patterns on the outputs. Such experiments allowed us to give a very clean statement; once the character definition is given, one is only left to check that it satisfies the expected properties.

Section 4 contains a proof of the extension result. As mentioned before, although it is well known to experts, we included its proof for two reasons: on the one hand, we could not find a clear reference to its proof, but also because we need the explicit result on the conductor of the extended representation. The section is split into two parts: one for the representation $\rho_{E_{(a,b,c)},p}$ and another one for the representation $\rho_{\widetilde{E}_{(a,b,c)},p}$. In both cases, a formula for the conductor of the residual extended representation is given.

Section 5 is devoted to study conditions to assure absolutely irreducible image of the residual representation. As explained before, the main result is due to Ellenberg. The same section contains a strategy to be used when the curve E does not have the prime of multiplicative reduction needed to apply Ellenberg's result. Section 6 contains a description of Mazur's method, the main tool used to discard newforms. It also contains some remarks on how to handle newforms with complex multiplication, and the role of the trivial solutions in the elimination procedure.

At last, Section 7 contains results on equation (2) for $d = 5$ (Theorem 7.1), $d = 6$ (Theorem 7.2) and $d = 7$ (Theorem 7.3), while Section 8 contains solutions and attempts to study primitive solutions of equation (3)

for $d = 2, 5, 6$ and 7. We do get non-existence results for $d = 2$ (Theorem 8.1) and for $d = 6$ (Theorem 8.2) but the elimination procedure fails in the cases $d = 5, 7$ due to the existence of newforms (without complex multiplication) that systematically pass Mazur's test. In [GPV21] some partials results are presented for both such equations.

The present article depends on different scripts that can be downloaded from the web page `http://sweet.ua.pt/apacetti/research.html`. There are mainly two different scripts used. One of them (written in `PARI/GP` [PAR19]) is the one used to give an explicit bound for Ellenberg's result (as explained in the proof of Theorem 5.2), called *"Ellenberg.gp"*. The second ones are used to eliminate newforms (mostly an implementation of Mazur's trick) in `Magma` ([BCP97]). There is one script for each equation (as it includes the definition of the character χ_t); the scripts used for equation (2) are *"Eq1d5.mg"*, *"Eq1d6.mg"* and *"Eq1d7.mg"* which depend on the file *"Mazur26p.mg"*. The scripts used for equation (3) are *"Eq2d5.mg"*, *"Eq2d6.mg"* and *"Eq2d7.mg"*. The outputs of the scripts are available in the files *"OutputsEq1.txt"* and *"OutputsEq2.txt"*.

Acknowledgments. We would like to thank John Cremona for many useful conversations regarding computing with Bianchi modular forms, and for explaining us how to use his code to compute them.

1. General strategy

Based on Frey-Hellegouarch's approach of relating a solution to Fermat's equation with a "special" elliptic curve, Darmon in [Dar00] proposed a generalization of the strategy to study a general Fermat-type equation of the form (1). The strategy consists roughly in the following three steps:

(1) **Construct a Galois representation:** to a putative solution (a, b, c) of equation (1), attach an odd residual Galois representation $\overline{\rho}_{(a,b,c)} : \mathrm{Gal}_K \to \mathrm{GL}_2(\mathbb{F})$ that is unramified at primes not dividing ABC and ℓ, where $\mathbb{F}$ is a finite field of characteristic ℓ and K is a finite extension of $\mathbb{Q}$ depending on the exponents (p, q, r).
(2) **Prove Modularity of $\overline{\rho}_{(a,b,c)}$:** prove that $\overline{\rho}_{(a,b,c)}$ matches the reduction of a Galois representation attached to an automorphic representation of $\mathrm{GL}_2(\mathbb{A}_K)$ whose level is only divisible by primes dividing the Artin conductor of $\overline{\rho}_{(a,b,c)}$.
(3) **Reach a Contradiction:** compute the space of automorphic representations of the last item, and prove that none is related to a possible solution.

The way the representation $\overline{\rho}_{(a,b,c)}$ is constructed in [Dar00] (that covers most possible exponents (p, q, r) but not all) is via the specialization of a parametric family $\overline{\rho}(t)$ at the point $t = \frac{Aa^p}{Cc^r}$. Furthermore, in the aforementioned article, Darmon gives an equation of a curve $C(a, b, c)$ whose natural residual Galois representation (via the action of the Galois group $\mathrm{Gal}_{\mathbb{Q}}$ on the p-torsion points of its Jacobian) gives raise to $\overline{\rho}_{(a,b,c)}$. In our case of interest, as mentioned in the introduction, to study solutions of (2), in [DU09] the authors attach to a solution the elliptic curve

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

defined over the field $K = \mathbb{Q}(\sqrt{-d})$. For studying the equation (3), we propose as a natural object attached to a solution (a, b, c) the elliptic curve

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

defined again over the quadratic field $K = \mathbb{Q}(\sqrt{-d})$ (generalizing the construction in [BC12]). Note that if $d > 0$, then both curves are defined over an imaginary quadratic field. For that purpose, let us explain in more detail what the second step "prove modularity" means. There should exist an automorphic representation Π of $\mathrm{GL}_2(\mathbb{A}_K)$ with the following properties:

- Let $\mathcal{O}$ denote the ring of integers of the coefficient field of the automorphic form Π. Then for each prime ideal λ of $\mathcal{O}$, there exists a Galois representation $\rho_{\Pi,\lambda} : \mathrm{Gal}_K \to \mathrm{GL}_2(\mathcal{O}_\lambda)$ such that $L(\Pi, s) = L(\rho_{\Pi,\lambda}, s)$.
- There exists a prime λ dividing ℓ such that the residual representation $\overline{\rho_{\Pi,\lambda}}$ is isomorphic to $\overline{\rho}_{(a,b,c)}$.

The curves $C(a, b, c)$ given in [Dar00] are all defined over $\mathbb{Q}$ and attain their full endomorphism ring over a totally real field, hence the relation between automorphic representations, Hilbert modular forms and Galois

representations is well known in this case. Although our curves are defined over imaginary quadratic fields, they are what is called a "$\mathbb{Q}$-curve" (as will be explained in Section 2), which implies that their Galois representations are related to classical weight 2 modular forms. The existence of a Bianchi modular form whose L-series matches the one of our elliptic curve then follows from Langlands results on cyclic base change. While solving equation (3) for $d = 2$ this fact will be extremely useful, as computing Bianchi modular forms is more effective in this case (all other computations will involve classical modular forms).

2. $\mathbb{Q}$-curves and properties of $E_{(a,b,c)}$ and $\widetilde{E}_{(a,b,c)}$

Definition 2.1. Let L be a number field and E/L an elliptic curve. The curve E is called a $\mathbb{Q}$-*curve* if for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$, the curve $\sigma(E)$ is isogenous to E.

The isogeny between E and $\sigma(E)$ needs not be defined over L. The minimum field where the curve and all the isogenies are defined is usually called the field of total definition. Let $\tau \in \mathrm{Gal}_{\mathbb{Q}}$ be any element whose restriction to $\mathbb{Q}(\sqrt{-d})$ is not the identity and let ψ_{-2} denote the quadratic character corresponding to the quadratic extension $\mathbb{Q}(\sqrt{-2})/\mathbb{Q}$.

Proposition 2.2. *The elliptic curve $E_{(a,b,c)}$ is a $\mathbb{Q}$-curve which is totally defined over the field $\mathbb{Q}(\sqrt{-d}, \sqrt{-2})$. Furthermore, $\tau(E_{(a,b,c)})$ is isogenous to the quadratic twist $E_{(a,b,c)} \otimes \psi_{-2}$.*

Proof. This result is explained in [DU09]. Let τ be a non-trivial generator of $\mathrm{Gal}(\mathbb{Q}(\sqrt{-d})/\mathbb{Q})$. The point $(0,0)$ has order two, and (as explained in [Sil09, Example 4.5]) the quotient has equation

$$y^2 = x^3 - 8ax^2 + 8(a^2 - \sqrt{-d}b)x.$$

An easy change of variables proves that it equals the quadratic twist by -2 of $\tau(E_{(a,b,c)})$. In particular, the curve and the isogenies are all defined over the field $\mathbb{Q}(\sqrt{-d}, \sqrt{-2})$ as claimed. □

Let ψ_{-3} denote the quadratic character corresponding to the quadratic extension $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$.

Proposition 2.3. *The elliptic curve $\widetilde{E}_{(a,b,c)}$ is a $\mathbb{Q}$-curve which is totally defined over the field $\mathbb{Q}(\sqrt{-d}, \sqrt{-3})$. Furthermore, $\tau(\widetilde{E}_{(a,b,c)})$ is isogenous to the quadratic twist $\widetilde{E}_{(a,b,c)} \otimes \psi_{-3}$.*

Proof. As explained in [Kub76, Table 1], all elliptic curves having a 3-torsion point have a minimal model of the form:

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

where $P = (0,0)$ is a point of order 3. Its 3-isogenous curve (obtained as the quotient of the curve by the order 3 group generated by P) has equation

$$y^2 + a_1xy + a_3y = x^3 - 5a_1a_3x - a_1^3a_3 - 7a_3^2.$$

Our curve $\widetilde{E}_{(a,b,c)}$ corresponds to the values $a_1 = 6b\sqrt{-d}$, $a_3 = -4d(a + b^3\sqrt{-d})$. The previous formula implies that the quotient $\widetilde{E}_{(a,b,c)}$ by $\langle(0,0)\rangle$ has equation

$$y^2 + 6b\sqrt{-d}xy - 4d(a + b^3\sqrt{-d})y = x^3 + (-120b^4d^2 + 120abd\sqrt{-d})x + 976b^6d^3 - 1088ab^3d^2\sqrt{-d} - 112a^2d^2. \tag{6}$$

On the other hand, if τ generates the Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt{-d})/\mathbb{Q})$, clearly $\tau(\widetilde{E}_{(a,b,c)}) = \widetilde{E}_{(a,-b,c)}$. The quadratic twist of $\widetilde{E}_{(a,-b,c)}$ by $\sqrt{-3}$ (which can be computed for example using [PAR19]) corresponds to the equation

$$y^2 + 6b\sqrt{-d}xy + 12d(-a + b^3\sqrt{-d})y = x^3 + 36b^2dx^2 + (144abd\sqrt{-d} + 144b^4d^2)x + 288ab^3d^2\sqrt{-d} + 144b^6d^3 - 144a^2d^2. \tag{7}$$

Via the usual change of variables (making $a_1 = a_3 = a_2 = 0$) it is easy to check that both (7) and (6) translate to the curve

$$y^2 = x^3 + (108abd\sqrt{-d} - 135b^4d^2)x - 756ab^3d^2\sqrt{-d} + 594b^6d^3 - 108a^2d^2.$$

In particular, $\tau(\widetilde{E}_{(a,b,c)})$ is isogenous to the quadratic twist of $\widetilde{E}_{(a,b,c)}$ by $\sqrt{-3}$. Hence $\widetilde{E}_{(a,b,c)}$ is a $\mathbb{Q}$-curve and its complete field of definition equals $\mathbb{Q}(\sqrt{-d},\sqrt{-3})$ as claimed. □

Let $K=\mathbb{Q}(\sqrt{-d})$ and $\mathcal{O}_K$ its ring of integers. The following trivial result will be useful later.

Lemma 2.4. *Let (a,b,c) be a primitive solution of either equation (2) or equation (3) with $p>3$. Then*

- $\gcd(ac,d)=1$.
- *If $d\equiv 1,3,5 \pmod 8$ only one of $\{a,b\}$ is even and the other one is odd.*
- *If 2 does not split in K (i.e. $d\not\equiv 7 \pmod 8$), then c is odd.*
- *If 3 does not split in K (i.e. $d\not\equiv 2 \pmod 3$), then c is not divisible by 3.*

2.1. **Properties of $E_{(a,b,c)}$.** Recall the defining equation:

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

Its discriminant equals $\Delta(E_{(a,b,c)})=512(a^2+b\sqrt{-d})c^p$ and its j-invariant equals $j(E_{(a,b,c)})=\frac{64(5a^2-3b\sqrt{-d})^3}{c^p(a^2+b\sqrt{-d})}$.

Lemma 2.5. *Suppose that q is an odd rational prime ramified at $K/\mathbb{Q}$ and let $\mathfrak{q}$ denote the (unique) prime ideal in $\mathcal{O}_K$ dividing q. Then $\mathfrak{q}\nmid\Delta(E_{(a,b,c)})$.*

Proof. Since q is ramified, $\mathfrak{q}\mid\sqrt{-d}$, and since (a,b,c) is a primitive solution, $\mathfrak{q}\nmid a$. Then $\mathfrak{q}\nmid c^p(a^2+\sqrt{-d}b)$. □

Lemma 2.6. *Let $\mathfrak{q}$ be an odd prime ideal of $\mathcal{O}_K$ such that $\mathfrak{q}\mid\Delta(E_{(a,b,c)})$. Then $E_{(a,b,c)}$ has multiplicative reduction at $\mathfrak{q}$.*

Proof. By Lemma 2.5 we know that primes dividing $\Delta(E_{(a,b,c)})$ are not ramified in $K/\mathbb{Q}$; in particular, if $\mathfrak{q}$ is an odd prime dividing $\Delta(E_{(a,b,c)})$, $\mathfrak{q}\nmid 4a$, hence clearly the reduction of (4) modulo $\mathfrak{q}$ is multiplicative. □

Lemma 2.7. *Let $\mathfrak{q}$ be an odd prime ideal of $\mathcal{O}_K$. Then $v_{\mathfrak{q}}(\Delta(E_{(a,b,c)}))\equiv 0 \pmod p$.*

Proof. From the discriminant formula, clearly $v_{\mathfrak{q}}(\Delta(E_{(a,b,c)}))=pv_{\mathfrak{q}}(c)+v_{\mathfrak{q}}(a^2+b\sqrt{-d})$. If $\mathfrak{q}\mid\gcd(a^2+\sqrt{-d}b,a^2-\sqrt{-d}b)$ then $\mathfrak{q}\mid 2$ (because (a,b,c) is primitive), hence the equality $c^p=a^4+db^2=(a^2+\sqrt{-d}b)(a^2-\sqrt{-d}b)$ implies that

$$v_{\mathfrak{q}}(a^2+\sqrt{-d}b)=\begin{cases}0 & \text{if } \mathfrak{q}\nmid(a^2+\sqrt{-d}b),\\ v_{\mathfrak{q}}(c^p) & \text{otherwise.}\end{cases}$$

□

The last two results are the ones needed for removing the primes dividing c from the conductor of the residual representation (via a theorem of Ribet). Let $N(E_{(a,b,c)})$ denote the conductor of $E_{(a,b,c)}$. Assume that $p\geq 11$ to avoid extra computations when 2 splits in K.

Lemma 2.8. *Let $\mathfrak{p}_2$ be a prime ideal of $\mathcal{O}_K$ dividing 2.*

(1) If 2 is inert in K then $E_{(a,b,c)}$ has reduction type III *at 2, with $v_2(N(E_{(a,b,c)}))=8$.*
(2) If 2 ramifies in K then $E_{(a,b,c)}$ has reduction type I_2^* or I_4^* at $\mathfrak{p}_2$, with $v_{\mathfrak{p}_2}(N(E_{(a,b,c)}))\in\{10,12\}$.
(3) If $(2)=\mathfrak{p}_2\bar{\mathfrak{p}}_2$ then either $E_{(a,b,c)}$ has reduction type III *at both primes, with $v_{\mathfrak{p}_2}(N(E_{(a,b,c)}))=v_{\bar{\mathfrak{p}}_2}(N(E_{(a,b,c)}))=8$, or $E_{(a,b,c)}$ is a twist of a curve with multiplicative reduction, so the primes can be chosen so that $v_{\mathfrak{p}_2}(N(E_{(a,b,c)}))=6$ and $v_{\bar{\mathfrak{p}}_2}(N(E_{(a,b,c)}))\in\{1,4\}$.*

Proof. The proof is a straight application of Tate's algorithm ([Tat75]). The invariants of $E_{(a,b,c)}$ are: $a_6=0$, $b_2=16a$, $b_6=0$ and $b_8=-4(a^2+\sqrt{-d}b)^2$.

(1) The hypothesis implies that $d\equiv 3 \pmod 8$ and 2 is prime in $\mathcal{O}_K$. Notice that, by Lemma 2.4, $2\nmid a^2+\sqrt{-d}b$ hence $v_2(\Delta(E_{(a,b,c)}))=9$. Since: $2\mid b_2$, $2^2\mid a_6$, $2^3\nmid b_8$, the curve has reduction type $\mathring{\mathrm{I}}\mathrm{I}\mathrm{I}$ and $v_2(N(E_{(a,b,c)}))=v_2(\Delta(E_{(a,b,c)}))-1=8$.

(2) Let $\mathfrak{p}_2$ be the unique prime in $\mathcal{O}_K$ dividing 2 and let π be a local uniformizer. By Lemma 2.4, $\mathfrak{p}_2 \nmid (a^2+\sqrt{-d}b)$, hence $v_{\mathfrak{p}_2}(\Delta(E_{(a,b,c)})) = 18$. To easy notation, consider the curve

$$y^2 = x^3 + 4\alpha x^2 + 2\beta x, \tag{8}$$

where $\mathfrak{p}_2 \nmid \beta$. Clearly $\mathfrak{p}_2 \mid b_2$, $\mathfrak{p}_2^2 \mid a_6$, $\mathfrak{p}_2^3 \mid b_8$ and $\mathfrak{p}_2^3 \mid b_6$. Following Tate's notation, let $a_{n,m} = \frac{a_n}{\pi^m}$. The polynomial $P = x^3 + a_{2,1}x^2 + a_{4,2}x + a_{6,3}$ has a double root at $x = 1$, hence we make the translation $x \to x + \pi$ in (8), to get the new equation

$$y^2 = x^3 + (4\alpha + 3\pi)x^2 + (8\pi\alpha + 3\pi^2 + 2\beta)x + 4\pi^2\alpha + \pi^3 + 2\beta\pi. \tag{9}$$

Write $\tilde{a}_i$ for the new coefficients. If either d is even (so we can take $\pi = \sqrt{-d}$) and b is odd, or d is odd (so $\pi = 1 + \sqrt{-d}$) and b is even (hence a is odd), $v_{\mathfrak{p}_2}(\pi^2 + 2\beta) = 3$ hence $v_{\mathfrak{p}_2}(\tilde{a_6}) = 4$ and the polynomial $Y^2 + \tilde{a}_{3,2}Y - \tilde{a}_{6,4}$ has a double non-zero root. Although we need to make a translation (to take the double root to zero), such procedure will not change $\tilde{a}_{4,3}$, which has valuation 3, so the type equals I_2^* and $v_{\mathfrak{p}_2}(N(E_{(a,b,c)})) = v_{\mathfrak{p}_2}(\Delta(E_{(a,b,c)})) - 6 = 12$.

Suppose that d is even and b is even. If $\frac{d}{2} \equiv 1 \pmod 4$ then $v_{\mathfrak{p}_2}(\tilde{a}_6) \geq 6$ and $v_{\mathfrak{p}_2}(\tilde{a}_4) = 4$, so we do not need to make any translation and the type is I_4^* and $v_{\mathfrak{p}_2}(N(E_{(a,b,c)})) = 18 - 8 = 10$. If $\frac{d}{2} \equiv 3 \pmod 4$ then $v_{\mathfrak{p}_2}(\tilde{a}_6) = 4$ and $v_{\mathfrak{p}_2}(\tilde{a}_4) \geq 5$ hence the polynomial $Y^2 + \tilde{a}_{3,2}Y - \tilde{a}_{6,4}$ has a non-zero double root, and after sending the root to 0, we get that the new a_4 has valuation 4, so the same computation works.

At last, if $d \equiv 1 \pmod 4$ and b is odd, $v_{\mathfrak{p}_2}(\tilde{a}_6) \geq 5$ and $v_{\mathfrak{p}_2}(\tilde{a}_4) = 4$, hence again the type is I_4^* and $v_{\mathfrak{p}_2}(N(E_{(a,b,c)})) = 18 - 8 = 10$.

(3) Let $\mathfrak{p}_2$ be a prime dividing 2. Consider the different cases:

- If either a or b is even (hence the other one is odd) then $v_{\mathfrak{p}_2}(a^2+\sqrt{-d}b) = 0$ and $v_{\mathfrak{p}_2}(\Delta(E_{(a,b,c)})) = 9$ (for both primes). Clearly $v_{\mathfrak{p}_2}(b_2) \geq 4$ and $v_{\mathfrak{p}_2}(b_8) = 2$ hence the reduction type is III and $v_{\mathfrak{p}_2}(N(E_{(a,b,c)})) = 9 - 1 = 8$ (at both primes).
- If both a, b are odd, we can assume that $v_{\mathfrak{p}_2}(a^2 + \sqrt{-d}b) > 1$ while $v_{\overline{\mathfrak{p}}_2}(a^2 + \sqrt{-d}b) = 1$ (since $\frac{a^2+\sqrt{-d}b}{2}$ is an integer, and $v_{\overline{\mathfrak{p}}_2}(a^2 + \sqrt{-d}b) = v_{\mathfrak{p}_2}(a^2 - \sqrt{-d}b) = v_{\mathfrak{p}_2}(a^2 + \sqrt{-d}b - 2\sqrt{-d}b)$). Furthermore, our assumption $p \geq 11$ implies that $v_{\mathfrak{p}_2}(a^2 + \sqrt{-d}b) \geq 11$, so $v_{\mathfrak{p}_2}(j(E_{(a,b,c)})) < 0$. In particular $E_{(a,b,c)}$ has potentially multiplicative reduction. The equation is not minimal at $\mathfrak{p}_2$; under a change of variables, it equals

$$y^2 = x^3 + ax^2 + \frac{(a^2 + \sqrt{-d}b)}{2^5}x,$$

which already has multiplicative reduction. Hence its conductor equals $\mathfrak{p}_2$ or $\mathfrak{p}_2^4$. To compute the type at $\overline{\mathfrak{p}}_2$, the hypothesis also implies that $v_{\overline{\mathfrak{p}}_2}(j(E_{(a,b,c)})) < 0$ so the curve has potentially multiplicative reduction, but it equals a quadratic twist (by the character of conductor 8) of a curve with multiplicative reduction, hence its conductor equals $\overline{\mathfrak{p}}_2^6$.

□

The following technical Lemma is needed only to compute the conductor of the extended Galois representation when $d \equiv 1 \pmod 8$, so we recommend the reader to skip it on a first reading.

Lemma 2.9. *Suppose that $d \equiv 1 \pmod 8$ and b is odd. Let $\mathfrak{p}_2$ the prime dividing 2, $\pi = 1 + \sqrt{-d}$ and ϵ be any unit. Then, at $\mathfrak{p}_2$, the elliptic curve $E_{(a,b,c)}$ twisted by $\epsilon\pi$ with equation*

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

has conductor exponent 8 if $b \equiv 1 \pmod 4$ and 6 if $b \equiv 3 \pmod 4$.

Proof. The proof also follows Tate's algorithm. The effect of twisting our elliptic curve in equation (9) is that the coefficient a_i becomes $a_i(\pi\varepsilon)^{-i}$, hence the discriminant valuation decreases by 6 and the coefficients a_i decrease their valuation by i. Then if $b \equiv 1 \pmod 4$, the valuations are $v_{\mathfrak{p}_2}(\tilde{a}_2) = 0$, $v_{\mathfrak{p}_2}(\tilde{a}_4) \geq 4$ while $v_{\mathfrak{p}_2}(\tilde{a}_6) = 2$ (because $\frac{\pi^2}{2} + b\sqrt{-d}$ is divisible by π but not by π^3). Following Step 6 of Tate's algorithm, we make the change of variables $y \to y + x + \pi$ and the new even coefficients become $\tilde{a}_2 - 1$, $\tilde{a}_4 - 2\pi$ and $\tilde{a}_6 - \pi^2$, with valuations 2, 3 and 3 respectively, so the reduction type is I_0^* and the conductor equals $18 - 6 - 4 = 8$.

On the other hand, if $b \equiv 3 \pmod 4$ then $v_{\mathfrak{p}_2}(\tilde{a}_2) = 0$, $v_{\mathfrak{p}_2}(\tilde{a}_4) = 2$ (because $2 \mid \frac{3\pi^2}{2} + b\sqrt{-d}$ but π^3 does not) while $v_{\mathfrak{p}_2}(\tilde{a}_6) \geq 4$. Following Tate's algorithm, apply the change of variables $y \to y+x$ to get coefficients $\alpha_1 = 2$, $\alpha_2 = \tilde{a}_2 - 1$, $\alpha_3 = 0$, $\alpha_4 = \tilde{a}_4$ and $\alpha_6 = \tilde{a}_6$ with $v_{\mathfrak{p}_2}(\alpha_2) = 2$, $v_{\mathfrak{p}_2}(\alpha_4) = 2$ and $v_{\mathfrak{p}_2}(\alpha_6) \geq 4$. Since the reduction of the polynomial $t^3 + \frac{\alpha_2}{\pi}t^2 + \frac{\alpha_4}{\pi^2}t + \frac{\alpha_6}{\pi^3}$ has a double root and one simple one, the reduction type is I_n^*. Making the change of variables $x \to x + \pi$ the new a_4 equals $3\pi^2 + \frac{2}{\pi^2}\beta + 3$, which has valuation 3 at $\mathfrak{p}_2$, so the type is I_2^* and the conductor valuation equals $18 - 6 - 6 = 6$ as claimed. □

All primitive trivial solutions correspond to very special curves.

Lemma 2.10. *The trivial solution $(0,0,0)$ gives rise to a singular curve. All other trivial primitive solutions of (2) are the following:*

- *The solution $(1,0,1)$, corresponding to the curve with lmfdb label 256-a2 and complex multiplication by $\mathbb{Z}[\sqrt{-2}]$.*
- *The solution $(-1,0,1)$, corresponding to the curve with lmfdb label 256-d2 and complex multiplication by $\mathbb{Z}[\sqrt{-2}]$.*
- *The solution $(0,\pm 1,1)$ (when $d = 1$), corresponding to the curve with lmfdb label 256-c2 and complex multiplication by $\mathbb{Z}[\sqrt{-1}]$.*

Proof. The solution $(0,0,0)$ clearly gives a singular curve. Any other trivial solution must have $b = 0$ or $a = 0$. In the first case, the primitive hypothesis implies that the solution equals $(\pm 1, 0, 1)$. If $a = 0$, and q is a prime dividing d, it must divide c but since the solution is primitive, q cannot divide b. This implies that no such prime can exist, and the later is a solution precisely $d = 1$, with trivial solution $(0, \pm 1, 1)$. □

Remark 1. The conductor of the curve $E_{(\pm 1,0,1)}$ over K has valuation 8 at primes dividing 2 when 2 is unramified in $K/\mathbb{Q}$, valuation 10 when $2 \mid d$ and valuation 12 when 2 ramifies in $K/\mathbb{Q}$ but $2 \nmid d$ (equivalently when $d \equiv 1 \pmod 4$).

2.2. **Properties of $\widetilde{E}_{(a,b,c)}$.** Recall once again the defining equation

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

Its discriminant equals $\Delta(\widetilde{E}_{(a,b,c)}) = -2^8 3^3 d^4 c^p (a + b^3\sqrt{-d})^2$; note that the discriminant is divisible by d (unlike the previous case). Its j-invariant is $j(\widetilde{E}_{(a,b,c)}) = \frac{2^4 3^3 b^3 \sqrt{-d}(4a - 5b^3\sqrt{-d})^3}{c^p(a+b^3\sqrt{-d})^2}$.

Lemma 2.11. *Let $\mathfrak{q}$ be a prime ideal of $\mathcal{O}_K$ such that $\mathfrak{q} \mid \Delta(\widetilde{E}_{(a,b,c)})$ and $\mathfrak{q} \nmid 6d$. Then $\widetilde{E}_{(a,b,c)}$ has multiplicative reduction at $\mathfrak{q}$.*

Proof. Mimics the proof of Lemma 2.6. □

Lemma 2.12. *Let $\mathfrak{q}$ be a prime of $\mathcal{O}_K$ such that $\mathfrak{q} \nmid 6d$. Then $v_{\mathfrak{q}}(\Delta(\widetilde{E}_{(a,b,c)})) \equiv 0 \pmod p$.*

Proof. Mimics the proof of Lemma 2.7. □

One important difference between equation (2) and equation (3) is that we will not be able to remove (via a lowering the level result) the ramified odd primes from the conductor of the residual representation.

Lemma 2.13. *Suppose that q is an odd rational prime ramified at $K/\mathbb{Q}$ and let $\mathfrak{q}$ denote the (unique) prime ideal in $\mathcal{O}_K$ dividing q. Then $v_{\mathfrak{q}}(\Delta(\widetilde{E}_{(a,b,c)})) = 8 + 3v_{\mathfrak{q}}(3)$.*

Proof. Since q is ramified, $\mathfrak{q} \mid \sqrt{-d}$, and since (a,b,c) is a primitive solution, $\mathfrak{q} \nmid a$. Then, using that $\mathfrak{q} \nmid c^p(a + b^3\sqrt{-d})$ and that $v_{\mathfrak{q}}(d) = 2$ the result follows. □

Remark 2. The curve $\widetilde{E}_{(a,b,c)}$ has bad additive reduction at all odd primes different from 3 ramifying in $K/\mathbb{Q}$. However, over the extension $K(\sqrt[6]{-d})$ it attains good reduction (via the usual change of coordinates $(x,y) \to (\sqrt[3]{(-d)^2}x, dy)$). If $q \mid d$ is such an odd prime, let $\mathfrak{q} = \langle q, \sqrt{-d}\rangle$ denote the ideal in K dividing it. If $q \equiv 1 \pmod 3$, the extension $K_{\mathfrak{q}}(\sqrt[6]{-d})/K_{\mathfrak{q}}$ is an abelian extension, hence the local type of the Weil-Deligne representation at $\mathfrak{q}$ is that of a principal series (given by an order 3 character), while if $q \equiv 2 \pmod 3$ the curve attains good reduction over a non-abelian extension, hence its local type matches that of a supercuspidal representation (obtained inducing an order 3 character from the quadratic unramified extension $K_{\mathfrak{q}}(\zeta_3)/K_{\mathfrak{q}}$).

Let $N(\widetilde{E}_{(a,b,c)})$ denote the conductor of $\widetilde{E}_{(a,b,c)}$ and suppose that $p > 3$.

Lemma 2.14. *Let $\mathfrak{p}_2$ be a prime ideal of $\mathcal{O}_K$ dividing 2. Then:*

(1) If 2 is inert in K then $\widetilde{E}_{(a,b,c)}$ has reduction type IV* *at 2, with $v_2(N(\widetilde{E}_{(a,b,c)})) = 2$.*

(2) If 2 is split in K then $\widetilde{E}_{(a,b,c)}$ has reduction type IV* *or* $\mathrm{I_n}$ *at $\mathfrak{p}_2$, with $v_{\mathfrak{p}_2}(N(\widetilde{E}_{(a,b,c)})) = 1, 2$ at both primes above 2.*

(3) If 2 ramified in K but $2 \nmid d$ then $\widetilde{E}_{(a,b,c)}$ has reduction type IV *at $\mathfrak{p}_2$, with $v_{\mathfrak{p}_2}(N(\widetilde{E}_{(a,b,c)})) = 2$.*

(4) If $2 \mid d$ then $\widetilde{E}_{(a,b,c)}$ has good reduction at $\mathfrak{p}_2$.

Proof. Consider each case separately:

(1) If 2 is inert then $2 \nmid c$, by Lemma 2.4. Clearly $2 \mid b_2$, $4 \mid a_6$ and $8 \mid b_8$, but since $2 \nmid (a + b^3\sqrt{-d})$, the polynomial $y^2 + \frac{a_3}{4}y - a_6$ has distinct roots, so Step 8 of Tate's algorithm implies the reduction is of type IV* and the conductor equals $v_2(\Delta(\widetilde{E}_{(a,b,c)})) - 6 = 2$.

(2) Suppose that 2 splits and let $\mathfrak{p}_2$ be a prime dividing 2. The primitive hypothesis implies that either one of a, b is even and the other is odd or both are odd. In the first case, $v_{\mathfrak{p}_2}(a_1) \geq 1$ and $v_{\mathfrak{p}_2}(a_3) = 2$ hence we are again in Step 8 of Tate's algorithm (type IV*), therefore the conductor exponent is 2. On the other hand, if both a and b are odd, the model is not minimal, as $v_{\mathfrak{p}_2}(a_1) = 1$ and $v_{\mathfrak{p}}(a_3) \geq 3$; its minimal model has $\tilde{a_1}$ a unit (hence $\tilde{b_2}$ a unit) and the curve has type $\mathrm{I_n}$. In particular, its conductor exponent equals 1.

(3) Suppose 2 ramifies but $2 \nmid d$ and let π be a local uniformizer. The hypothesis (a, b, c) primitive implies that $v_\pi(a + b^3\sqrt{-d}) = 0$ (i.e. one of a or b is even but not both). The model is not minimal; the change of variables $y \to \pi^3 y$, $x \to \pi^2 x$ gives a minimal model with valuations $v_\pi(\tilde{a_1}) \geq 1$ and $v_\pi(\tilde{a_3}) = 1$. In particular, $v_\pi(\tilde{b_6}) = 2$ so we are in Step 5 of Tate's algorithm which implies that the reduction has type IV and its conductor equals $v_\pi(\Delta(\widetilde{E}_{(a,b,c)})) - 2 = 2$.

(4) If $2 \mid d$ then $2 \nmid a$ (as the solution is primitive), so the change of variables $x \to 2^2 x$, $y \to 2^3 y$ gives a non-singular curve.

□

At last, we need information on primes dividing 3.

Lemma 2.15. *Let $\mathfrak{p}_3$ be a prime ideal of $\mathcal{O}_K$ dividing 3.*

(1) If 3 is inert in K then $\widetilde{E}_{(a,b,c)}$ has reduction type II or III at 3, with $v_3(N(\widetilde{E}_{(a,b,c)})) \in \{2, 3\}$.

(2) If $3 = \mathfrak{p}_3\overline{\mathfrak{p}}_3$ in K then $\widetilde{E}_{(a,b,c)}$ has reduction type II or III at $\mathfrak{p}_3$, with $v_{\mathfrak{p}_3}(N(\widetilde{E}_{(a,b,c)})) = v_{\overline{\mathfrak{p}}_3}(N(\widetilde{E}_{(a,b,c)})) \in \{2, 3\}$, or the primes can be chosen so that $v_{\mathfrak{p}_3}(N(\widetilde{E}_{(a,b,c)})) = 2$ and $v_{\overline{\mathfrak{p}}_3}(N(\widetilde{E}_{(a,b,c)})) = 1$.

(3) If 3 ramifies in K then $\widetilde{E}_{(a,b,c)}$ has reduction type IV* at $\mathfrak{p}_3$, with $v_{\mathfrak{p}_3}(N(\widetilde{E}_{(a,b,c)})) = 8$.

Proof. Let's consider the different cases:

(1) If 3 is inert, the primitive hypothesis implies that c is not divisible by 3 and $v_3(a_3) = 0$ hence the singular point is not at the origin but it goes to the origin under the translation $(x, y) \to (x - a_3^6, y + a_3)$ (we are using that in the residue field raising to the eight power is the constant map). Let a_1 and a_3 denote the corresponding coefficients of $\widetilde{E}_{(a,b,c)}$ (to easy notation). Then the model becomes

$$y^2 + a_1xy + (3a_3 - a_1a_3^6)y = x^3 - 3a_3^6x^2 - a_1a_3x + (a_1a_3^7 - a_3^{18} - 2a_3^2). \tag{10}$$

Let $\tilde{a_i}$ denote such coefficients. If $3 \mid b$ then $v_3(a_1) \geq 2$ so $v_3(\tilde{a_6}) = 1$ hence we are in Step 3 of Tate's algorithm, hence the curve has type II and the conductor exponent is 3. If $3 \nmid b$, $v_3(a_1) = 1$. If $9 \nmid a_1a_3^7 - a_3^{18} - 2a_3^2$ we are again in case II (with exponent 3). Otherwise the following equality holds:

$$\frac{a_1}{3} \equiv a_3^3 \left(\frac{a_3^{16} + 2}{3} \right) \pmod 3.$$

The coefficient $\tilde{b_2}$ equals $-4a_1^2a_3^{18} + 6a_1a_3^{13} + 12a_3^{24} - 3a_3^8$. Using the above equation a simple computation shows its valuation at 3 equals 2 hence the reduction type is III and the conductor exponent equals 2.

(2) If 3 splits in K, let $\mathfrak{p}_3$ be a prime dividing it. If $3 \mid a$ then $3 \nmid b$ hence $v_{\mathfrak{p}_3}(a_1) = 1$ and $v_{\mathfrak{p}_3}(a_3) = 0$. This situation matches the previous case and a similar computation proves that the type is II or III and the exponent valuation 3 or 2 at both $\mathfrak{p}_3$ and $\bar{\mathfrak{p}}_3$. If $3 \mid b$ then $3 \nmid a$, hence $v_{\mathfrak{p}_3}(a_1) \geq 2$ and $v_{\mathfrak{p}_3}(a_3) = 0$; as in the previous case this corresponds to type II with conductor exponent 3.

Suppose then that $3 \nmid ab$. Then one of the primes (say $\mathfrak{p}_3$) divides $a + b^3\sqrt{-d}$ while the other does not. Since $c^p = (a + b^3\sqrt{-d})(a - b^3\sqrt{-d})$ the assumption $p \geq 5$ implies that (without loss of generality) $v_{\mathfrak{p}_3}(a + b^3\sqrt{-d}) > 3$ so $\mathfrak{p}_3$ divides the denominator of the j-invariant. Furthermore, the model is not minimal, and under the usual change of variables (sending $(x, y) \to (3^2x, 3^3y)$ we get a curve with multiplicative reduction, hence the discriminant exponent equals 1. At the prime $\bar{\mathfrak{p}}_3$ the curve is a quadratic twist (by the character of conductor 3) of a curve with multiplicative reduction, hence the statement.

(3) If 3 ramifies in K then $3 \mid d$ and the primitive hypothesis implies that $3 \nmid a$. Let $\mathfrak{p}$ denote the prime ideal dividing 3 in K. Then $v_{\mathfrak{p}_3}(a_1) \geq 2$ and $v_{\mathfrak{p}_3}(a_3) = 2$ hence we are in Step 8 of Tate's algorithm, the reduction type is IV^* and the conductor exponent equals $14 - 6 = 8$.

□

Remark 3. If 3 is inert in $K/\mathbb{Q}$ and the curve has type III reduction (the case of conductor valuation 2), the change of variables $(x, y) \to (\sqrt[4]{3}x, \sqrt{3}y)$ in equation (10) gives a curve with good reduction. Since the fourth roots of unity are in K_3, the local type of the Weil-Deligne representation is that of a principal series (whose inertia is given by an order 4 character).

Lemma 2.16. *Suppose that q is a rational prime ramified at $K/\mathbb{Q}$ such that $q \nmid 6$ and let $\mathfrak{q}$ denote the (unique) prime ideal in $\mathcal{O}_K$ dividing q. Then $\widetilde{E}_{(a,b,c)}$ has reduction type IV^* at $\mathfrak{q}$ and $v_{\mathfrak{q}}(N(\tilde{E}_{(a,b,c)})) = 2$.*

Proof. Since (a, b, c) is a primitive solution, then $q \nmid a$ so $v_{\mathfrak{q}}(a_3) = 2$ and $v_{\mathfrak{q}}(b_6) = 4$. Also, $v_{\mathfrak{q}}(b_2) \geq 2$ which implies that we are in Step 8 of Tate's algorithm so the result follows from Lemma 2.13. □

Once again, all trivial solutions correspond to special curves.

Lemma 2.17. *The trivial solution $(0, 0, 0)$ gives rise to a singular curve. All other trivial primitive solutions of (3) are the following:*

- *The solution $(0, \pm 1, 1)$ (when $d = 1$), corresponding to the elliptic curve with lmfdb label 2.0.4.1-324.1-a3 and complex multiplication by $\mathbb{Z}[\sqrt{-1}]$.*
- *The solution $(\pm 1, 0, 1)$, corresponding to a cubic twists by $\sqrt[3]{d}$ of the elliptic curve with lmfdb label 108-a2. Such a twist has complex multiplication by $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$.*

Proof. The solution $(0, 0, 0)$ clearly gives a singular curve. The other trivial primitive solutions must be of the form $(\pm 1, 0, 1)$ or $(0, \pm 1, 1)$. The later case can only occur when $d = 1$ (since d is assumed to be square-free) giving the first equation. The solution $(\pm 1, 0, 1)$ corresponds to the elliptic curve

$$\tilde{E}_{(\pm 1,0,1)} : y^2 \pm 4dy = x^3.$$

When $d = 1$, it corresponds to the elliptic curve with lmfdb label 108-a2, which has complex multiplication by $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. The fact that the cubic roots of unity act on the curve allows to define cubic twists of the curve, and the general case is precisely the cubic twist by $\sqrt[3]{d}$ of the case $d = 1$. □

Remark 4. The trivial solution $(\pm 1, 0, 1)$ corresponds to an elliptic curve over K with complex multiplication whose conductor has valuation:

- 2 for all odd primes $\mathfrak{q}$ dividing d but not 3,
- 2 if $\mathfrak{p}_2 \mid 2$ and $2 \nmid d$,
- 0 if $\mathfrak{p}_2 \mid 2$ and $2 \mid d$,
- 3 if $\mathfrak{p}_3 \mid 3$ and $3 \nmid d$,
- 8 if $\mathfrak{p}_3 \mid 3$ and $3 \mid d$.

3. Construction of the Hecke character

For a number field L, let $\mathbb{I}_L$ denote its idèle group and $\mathrm{Cl}(L)$ denote its class group. Class field theory relates finite characters of Gal_L with finite characters of the idèle group $\mathbb{I}_L$. We will make constant use of this relation, and will denote by the same letter both incarnations of the same object (and hope there is no confusion on doing that).

Let $\tau \in \mathrm{Gal}_{\mathbb{Q}}$ and $\chi : \mathbb{I}_L \to \overline{\mathbb{Q}}^{\times}$ be a finite order Hecke character. Denote by ${}^{\tau}\chi$ the Hecke character given on an element $\alpha \in \mathbb{I}_L$ by

$$ {}^{\tau}\chi(\alpha) = \chi(\tau(\alpha)).$$

Via class field theory, the character ${}^{\tau}\chi$ corresponds to the character on Gal_L given by ${}^{\tau}\chi(\sigma) = \chi(\tau\sigma\tau^{-1})$. In general, if $\rho : \mathrm{Gal}_L \to \mathrm{GL}_n(\overline{\mathbb{Q}_p})$ is a Galois representation, and $\tau \in \mathrm{Gal}_{\mathbb{Q}}$, we denote by ${}^{\tau}\rho$ the Galois representation whose value at $\sigma \in \mathrm{Gal}_L$ equals ${}^{\tau}\rho(\sigma) = \rho(\tau\sigma\tau^{-1})$.

For K a quadratic extension of $\mathbb{Q}$, a representation $\rho : \mathrm{Gal}_K \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$ extends to a 2-dimensional representation of $\mathrm{Gal}_{\mathbb{Q}}$ if and only if ${}^{\tau}\rho \simeq \rho$, where $\tau \in \mathrm{Gal}_{\mathbb{Q}}$ is any element whose restriction to Gal_K is not the identity (although this result is well known for experts, a proof will be given in Theorem 4.2).

Let t be an integer, and let ψ_t denote the character of $\mathrm{Gal}_{\mathbb{Q}}$ corresponding to the quadratic extension $\mathbb{Q}(\sqrt{t})/\mathbb{Q}$. Proposition 2.2 implies that for any prime p, ${}^{\tau}\rho_{E_{(a,b,c)},p}$ is isomorphic to $\rho_{E_{(a,b,c)},p} \otimes \psi_{-2}$, while Proposition 2.3 implies that for any prime p, ${}^{\tau}\rho_{\widetilde{E}_{(a,b,c)},p}$ is isomorphic to $\rho_{\widetilde{E}_{(a,b,c)},p} \otimes \psi_{-3}$. If we construct a Hecke character $\chi_t : \mathrm{Gal}_K \to \overline{\mathbb{Q}}^{\times}$ satisfying that ${}^{\tau}\chi_t = \chi_t \cdot \psi_{-t}$ (as characters of Gal_K) then the twisted representations $\rho_{E_{(a,b,c)},p} \otimes \chi_2$ (respectively $\rho_{\widetilde{E}_{(a,b,c)},p} \otimes \chi_3$) is isomorphic to ${}^{\tau}(\rho_{E_{(a,b,c)},p} \otimes \chi_2)$ (respectively to ${}^{\tau}(\rho_{\widetilde{E}_{(a,b,c)},p} \otimes \chi_3)$) and so as explained in the introduction (see also Theorems 4.2 and 4.5) it does extend to a two dimensional representations of $\mathrm{Gal}_{\mathbb{Q}}$. Furthermore, an explicit description of χ and of its conductor allows to give a formula for the level and Nebentypus of the extended rational representation. This leads to the following problem.

Problem 1: Let ψ_t be the quadratic character of $\mathrm{Gal}_{\mathbb{Q}}$ corresponding to the extension $\mathbb{Q}(\sqrt{t})/\mathbb{Q}$. Find a Hecke character χ_t of Gal_K such that ${}^{\tau}\chi_t = \chi_t \cdot \psi_{-t}$.

Our main result is to give a solution the previous problem for $t = 2$ (corresponding to equation (2)) and for t a prime number congruent to 3 modulo 4 (corresponding to equation (3)). To explain how our construction works, consider the natural short exact sequence

$$0 \longrightarrow L^{\times} \cdot (\textstyle\prod_{\mathfrak{q}} \mathcal{O}_{\mathfrak{q}}^{\times} \times (L \otimes \mathbb{R})^{\times}) \longrightarrow \mathbb{I}_L \xrightarrow{\mathrm{Id}} \mathrm{Cl}(L) \longrightarrow 0. \tag{11}$$

We start defining the Hecke character χ_t at elements of the first term of the short exact sequence and then extend it to elements of $\mathbb{I}_L$ that map via Id to representatives of the class group. Let us make one important remark, as the picture might be a little misleading: our character χ_t will not be trivial at units (the first term of the sequence), hence it will not be a character of the whole class group! (it will be a character of a suitable ray class group though).

Recall that Hecke characters are trivial at elements of $L^{\times}$, hence we are only left to define our character on local units (which determines the ramification behavior of the abelian extension cut out by the kernel of the character χ_t). Note that $(\prod_{\mathfrak{q}} \mathcal{O}_{\mathfrak{q}}^{\times} \times (L \otimes \mathbb{R})^{\times}) \cap L^{\times} = \mathcal{O}_L^{\times}$, hence there is a compatibility condition that always needs to be checked:

Compatibility condition: the product of the local components evaluated at a unit equals 1, i.e.

$$\prod_v \chi_{t,v}(\epsilon) = 1 \tag{12}$$

for all $\epsilon \in \mathcal{O}_L^{\times}$. Verifying this property is what makes construction of Hecke characters quite hard in general.

In our case, the field L is the imaginary quadratic field K, so its set of units is well known. Our character χ_t will be ramified at most at the odd primes ramifying in $K/\mathbb{Q}$ (with conductor exponent one), at primes dividing 2 and at primes dividing t.

Let $\mathcal{N} : \mathbb{I}_K \to \mathbb{I}_{\mathbb{Q}}$ be the norm map. The way we verify the compatibility condition of our defined character (and other properties it satisfies) is via the construction of an auxiliary rational Hecke character ε_t (that will

end up being the Nebentypus of the extended representation) unramified outside $2td$ with the following key properties relating ε_t to χ_t:

(1) The local character $\chi_{t,\mathfrak{p}}$ satisfies that ${}^{\tau}\chi_{t,\mathfrak{p}} = \chi_{t,\mathfrak{p}} \cdot ((\psi_{-t})_p \circ \mathcal{N})$.
(2) Let p be an odd prime ramified in $K/\mathbb{Q}$, and let $\mathfrak{p}$ the unique prime of $\mathcal{O}_K$ dividing it. Then under the field isomorphism $\mathcal{O}_K/\mathfrak{p} \to \mathbb{Z}/p$, the local character $\chi_{t,\mathfrak{p}}$ equals $\varepsilon_{t,p}\delta_p$, where δ_p is the quadratic character of $(\mathbb{Z}/p)^\times$.
(3) An extra condition at primes dividing 2 so that a compatibility conditions on units holds (a condition similar to (12) for the units of K).
(4) For all $\sigma \in \mathrm{Gal}_K$, $\chi_t(\sigma)^2 = \varepsilon_t(\sigma)$ (or in terms of idèles, $\chi_t^2 = \varepsilon_t \circ \mathcal{N}$).

Let us explain the role of each property we imposed. The first condition is needed for χ_t to locally solve the problem. The second condition will play a crucial role while proving the compatibility condition (via quadratic reciprocity). It is a local version of the last one.

Lemma 3.1. *Let $p \nmid t$ be an odd rational prime and $\mathfrak{p}$ a prime of $\mathcal{O}_K$ dividing it. Then the second condition implies that the fourth condition holds locally, namely $\chi_{t,\mathfrak{p}}^2 = \varepsilon_{t,p} \circ \mathcal{N}$.*

Proof. For primes $\mathfrak{p} \nmid 2td$, both characters are trivial, hence the statement trivially holds. For odd primes $\mathfrak{p}$ (of norm p) such that $\mathfrak{p} \nmid t$ and $\mathfrak{p} \mid d$, recall that the restriction of $\varepsilon_{t,p}$ to $\mathrm{Gal}_{K_\mathfrak{p}}$ equals (as Hecke characters) $\varepsilon_{t,p} \circ \mathcal{N}$, where $\mathcal{N} : K_\mathfrak{p} \to \mathbb{Q}_p$ is the norm map. Since p ramifies in $K/\mathbb{Q}$ the local norm map (modulo $\mathfrak{p}$) is given by $x \mapsto x^2$, so we get the equality

$$\chi_{t,\mathfrak{p}}^2(x) = \varepsilon_{t,p}^2(x) = \varepsilon_{t,p}(x^2) = \varepsilon_{t,p} \circ \mathcal{N}(x).$$

□

The third condition is needed to prove the compatibility condition. The first three conditions will be enough to define the character χ_t at elements of the first term of (11). The last condition will be used to extend the character to idèles that are representatives of the class group of K.

The general strategy to prove existence of the characters ε_t and χ_t with the above properties, is to split the set of odd primes $\{p : p \text{ ramifies in } K/\mathbb{Q}\}$ into four sets. More concretely, for $t = 2$ they will be divided depending on their congruence modulo 8, while for t an odd prime, they will be divided depending on whether p is a square modulo t or not and on whether p is a square modulo 4 or not. Then for primes p in each set we give an explicit definition of the local character $\varepsilon_{t,p}$ and $\chi_{t,\mathfrak{p}}$ satisfying the previous four properties. The description (and proof) depends on whether $t = 2$ or t is an odd prime congruent to 3 modulo 4, so each case will be considered in a different section. To ease notation, in each subsection the subscript t will be removed.

3.1. **The case $t = 2$.** Let $K = \mathbb{Q}(\sqrt{-d})$ with d a positive square-free integer. 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 $i = 1, 3, 5, 7$.

The character ε: Define an even character $\varepsilon : \mathbb{I}_\mathbb{Q} \to \overline{\mathbb{Q}}^\times$ ramified at the set of primes of $Q_3 \cup Q_5$ and sometimes in $\{2\}$, with local component ε_p given by:

- For primes $p \in Q_1 \cup Q_7$, the character $\varepsilon_p : \mathbb{Z}_p^\times \to \overline{\mathbb{Q}}^\times$ is trivial.
- For primes $p \in Q_3$, the character $\varepsilon_p = \delta_p$, the quadratic character defined by $\delta_p(n) = \left(\frac{n}{p}\right)$.
- 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.

Before defining the character at the prime 2, let us introduce some notation. Let ψ_{-1}, ψ_2, ψ_{-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 let δ_{-1}, δ_2, δ_{-2} be their local component at the prime 2 (see Table 3.1 for their values).

- Define $\varepsilon_2 = \delta_{-1}^{\#Q_3+\#Q_5}$.

Char	1	3	5	7
δ_{-1}	1	-1	1	-1
δ_{-2}	1	1	-1	-1
δ_2	1	-1	-1	1

TABLE 3.1.

By construction, the character ε satisfies the compatibility condition, namely

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

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 $\varepsilon : G_\mathbb{Q} \to \overline{\mathbb{Q}}^\times$. 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 $\#Q_3 + \#Q_5$ even and 2 otherwise.

Remark 5. The possible values for $\#Q_3$, $\#Q_5$ and $\#Q_7$ depending on the congruence of d modulo 8 are given on Table 3.2. Note in particular that when d is odd, the definition of ε_2 depends only on the value of $d \pmod 8$ and not on the parity of $\#Q_3$ and $\#Q_5$.

d	$\#Q_3$	$\#Q_5$	$\#Q_7$	d	$\#Q_3$	$\#Q_5$	$\#Q_7$
1	0	0	0	5	0	1	0
	1	1	1		1	0	1
3	0	1	1	7	0	0	1
	1	0	0		1	1	0
2	0	0	0	6	0	0	1
	0	1	0		0	1	1
	1	0	1		1	0	0
	1	1	1		1	1	0

TABLE 3.2.

Theorem 3.2. *There exists a Hecke character $\chi : \mathrm{Gal}_K \to \overline{\mathbb{Q}}^\times$ such that:*

(1) $\chi^2(\sigma) = \varepsilon(\sigma)$ for all $\sigma \in \mathrm{Gal}_K$,

(2) χ is unramified at primes not dividing $2\prod_{p\in Q_1\cup Q_5\cup Q_7} p$,

(3) If $\tau \in \mathrm{Gal}_\mathbb{Q}$ is not the identity on K, ${}^\tau\chi = \chi\cdot\psi_{-2}$ as characters of Gal_K.

Proof. Recall that for each ramified prime p in K there is a natural group isomorphism $(\mathcal{O}_\mathfrak{p}/\mathfrak{p})^\times \simeq (\mathbb{Z}/p)^\times$ (where $\mathcal{O}_\mathfrak{p}$ denotes the completion of $\mathcal{O}_K$ at $\mathfrak{p}$). By an abuse of notation, we will also denote by δ_p or ε_p the character of $(\mathcal{O}_\mathfrak{p}/\mathfrak{p})^\times$ obtained under the previous isomorphism. Following the strategy described above, define $\chi_\mathfrak{p} : \mathcal{O}_\mathfrak{p}^\times \to \overline{\mathbb{Q}}^\times$ by:

- If $\mathfrak{p}$ is an odd (i.e. $\mathfrak{p} \nmid 2$) unramified prime, $\chi_\mathfrak{p}$ is the trivial character.
- If $\mathfrak{p}$ is an odd ramified prime,

$$\chi_\mathfrak{p} = \varepsilon_p\delta_p. \tag{13}$$

- The archimidean component of χ is trivial.

Its local definition at places dividing 2 is more involved. Suppose that 2 does not split in K, and let $\mathfrak{p}_2$ denote the unique ideal dividing 2. The character $\chi_{\mathfrak{p}_2}$ has conductor dividing 2^3; the group structure of $(\mathcal{O}_{\mathfrak{p}_2}/2^n)^\times$ and its generators are given in Table 3.3. The generators are ordered so that the order of the generator i matches the i-th factor of the group structure, while the elements norms are modulo 8. Define $\chi_{\mathfrak{p}_2}$ on the set of generators as follows:

- If $d \equiv 1 \pmod{16}$, $\chi_{\mathfrak{p}_2}(\sqrt{-d}) = 1$, $\chi_{\mathfrak{p}_2}(1+2\sqrt{-d}) = 1$, $\chi_{\mathfrak{p}_2}(5) = -1$.
- If $d \equiv 9 \pmod{16}$, $\chi_{\mathfrak{p}_2}(\sqrt{-d}) = -1$, $\chi_{\mathfrak{p}_2}(1+2\sqrt{-d}) = 1$, $\chi_{\mathfrak{p}_2}(5) = -1$.

d	n	Structure	Generators	Norms
1	3	$\mathbb{Z}/4\times\mathbb{Z}/4\times\mathbb{Z}/2$	$\{\sqrt{-d}, 1+2\sqrt{-d}, 5\}$	$\{1,5,1\}$
3	3	$\mathbb{Z}/3\times\mathbb{Z}/4\times\mathbb{Z}/2\times\mathbb{Z}/2$	$\{\zeta_3, \sqrt{-d}, 3+2\sqrt{-d}, -1\}$	$\{1,3,5,1\}$
5	3	$\mathbb{Z}/4\times\mathbb{Z}/4\times\mathbb{Z}/2$	$\{\sqrt{-d}, 1+2\sqrt{-d}, -1\}$	$\{5,5,1\}$
even	2	$\mathbb{Z}/4\times\mathbb{Z}/2$	$\{1+\sqrt{-d}, -1\}$	$\{3,1\}$

TABLE 3.3.

- If $d\equiv 3 \pmod 8$, $\chi_{\mathfrak{p}_2}(\zeta_3)=1$, $\chi_{\mathfrak{p}_2}(\sqrt{-d})=i$, $\chi_{\mathfrak{p}_2}(3+2\sqrt{-d})=1$, $\chi_{\mathfrak{p}_2}(-1)=1$.
- If $d\equiv 5 \pmod{16}$, $\chi_{\mathfrak{p}_2}(\sqrt{-d})=1$, $\chi_{\mathfrak{p}_2}(1+2\sqrt{-d})=1$, $\chi_{\mathfrak{p}_2}(-1)=-1$.
- If $d\equiv 13 \pmod{16}$, $\chi_{\mathfrak{p}_2}(\sqrt{-d})=-1$, $\chi_{\mathfrak{p}_2}(1+2\sqrt{-d})=1$, $\chi_{\mathfrak{p}_2}(-1)=-1$.
- If $d\equiv 2 \pmod 8$ and $\#Q_3+\#Q_5$ is even, $\chi_{\mathfrak{p}_2}(1+\sqrt{-d})=1$, $\chi_{\mathfrak{p}_2}(-1)=1$.
- If $d\equiv 2 \pmod 8$ and $\#Q_3+\#Q_5$ is odd, $\chi_{\mathfrak{p}_2}(1+\sqrt{-d})=i$, $\chi_{\mathfrak{p}_2}(-1)=-1$.
- If $d\equiv 6 \pmod 8$ and $\#Q_3+\#Q_5$ is even, $\chi_{\mathfrak{p}_2}(1+\sqrt{-d})=1$, $\chi_{\mathfrak{p}_2}(-1)=-1$.
- If $d\equiv 6 \pmod 8$ and $\#Q_3+\#Q_5$ is odd, $\chi_{\mathfrak{p}_2}(1+\sqrt{-d})=i$, $\chi_{\mathfrak{p}_2}(-1)=1$.

At last,

- If $d\equiv 7 \pmod 8$, 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 $\chi_2=\prod_{\mathfrak{p}_2\mid 2}\chi_{\mathfrak{p}_2}$.

Define χ on $K^\times\cdot(\prod_{\mathfrak{q}}\mathcal{O}_{\mathfrak{q}}^\times\times\mathbb{C}^\times)$ to be trivial at elements of $K^\times$ and as the product of the local components at elements of the second factor. Let us start proving that even when we do not know that that our character χ satisfies the compatibility condition, nor have extended it to the whole idèle group, it satisfies the three properties of the Theorem at elements of $K^\times\cdot(\prod_{\mathfrak{q}}\mathcal{O}_{\mathfrak{q}}^\times\times\mathbb{C}^\times)$.

(1) We need to verify that the equality
$$\chi^2=\varepsilon\circ\mathcal{N}$$
holds for all elements of $K^\times\cdot(\prod_{\mathfrak{q}}\mathcal{O}_{\mathfrak{q}}^\times\times\mathbb{C}^\times)$. The statement is clear for elements of $K^\times$ (as both terms are trivial) and at $\mathbb{C}^\times$ for the same reason, so we are left to verify it for each local component. The proof for odd prime ideals $\mathfrak{p}$ is the following: if $\mathfrak{p}$ is unramified in $K/\mathbb{Q}$, then the result is clear (as all characters are trivial), while at ramified primes, it follows from (13) together with Lemma 3.1.

At last, it is easy to verify that $\chi_2^2=\varepsilon_2\circ\mathcal{N}$ using the character values in Table 3.1, the parity of Table 3.2 and the norm of the generators given in Table 3.3.

(2) From the definition of ε and χ it is clear that the ramification hypothesis is fulfilled.

(3) From its definition it is clear that for all odd primes ${}^\tau\chi_{\mathfrak{p}}=\chi_{\mathfrak{p}}$, so the third condition is also locally fulfilled. The reason it holds for primes $\mathfrak{p}_2$ dividing 2 is that ${}^\tau\chi_{\mathfrak{p}_2}\cdot\chi_{\mathfrak{p}_2}=\chi_{\mathfrak{p}_2}\circ\mathcal{N}$, hence ${}^\tau\chi_{\mathfrak{p}_2}=\chi_{\mathfrak{p}_2}^{-1}\cdot(\chi_{\mathfrak{p}_2}\circ\mathcal{N})$. An easy case by case computation on the generators shows that ${}^\tau\chi_{\mathfrak{p}_2}=\chi_{\mathfrak{p}_2}\cdot(\delta_{-2}\circ\mathcal{N})$.

An important property of our character at 2 is that its restriction to the 2-adic integers always satisfies

$$\chi_2|_{\mathbb{Z}_2^\times}=\delta_2^{v_2(d)+1}\delta_{-1}^{\#Q_5+\#Q_7}. \tag{14}$$

Compatibility: the subgroup of units in K is generated by roots of unity of order 2, 6 and 4 (for $\mathbb{Q}(\sqrt{-1})$). Since our characters have order a power of 2, the compatibility relation at roots of order 3 (if K has one) is trivial. If $K=\mathbb{Q}(\sqrt{-1})$, all sets Q_i for $i=1,3,5,7$ are empty and the compatibility at $\sqrt{-1}$ follows from the fact that $\chi_2(\sqrt{-1})=1$ in such case.

Let us make the following abuse of notation: for $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$ let us denote by $\mathfrak{p}\in Q_i$ the fact that $\mathfrak{p}\cap\mathbb{Z}$ is in such set. Then compatibility at -1 follows from

$$\chi(-1)=\prod_{\mathfrak{p}}\chi_{\mathfrak{p}}(-1)=\prod_{\mathfrak{p}\in Q_1\cup Q_5\cup Q_7}\chi_{\mathfrak{p}}(-1)\chi_2(-1)=(-1)^{\#Q_5+\#Q_7}\delta_{-1}(-1)^{\#Q_5+\#Q_7}=1. \tag{15}$$

Extension: As explained before, to extend χ to the whole idèle group $\mathbb{I}_K$, it is enough to define it on idèles whose image via Id (in (11)) generate the class group of K. For that purpose, consider the p-primary decomposition $(\mathbb{Z}/p_1)^{r_1}\times(\mathbb{Z}/p_h)^{r_h}$ of the class group $\mathrm{Cl}(K)$, and let $\{\mathfrak{r}_1,\cdots,\mathfrak{r}_h\}$ be prime ideals of K

generating each part (we can and do assume they are not ramified in $K/\mathbb{Q}$). Since $\mathfrak{r}_i$ is not principal, it must split in $K/\mathbb{Q}$, so if $r_i = \mathcal{N}(\mathfrak{r}_i)$, then the element a_i in $\mathbb{I}_K$ with trivial infinite component and finite components:

$$(a_i)_{\mathfrak{p}} = \begin{cases} r_i & \text{if } \mathfrak{p} = \mathfrak{r}_i, \\ 1 & \text{otherwise.} \end{cases}$$

is a preimage of $\mathfrak{r}_i$ under Id. The value $\chi(a_i)$ cannot be arbitrary. For example, suppose that $\mathfrak{r}_i$ has odd order in the class group, so there exists an ideal $\mathfrak{t}$ such that $\mathfrak{t}^2$ lies in the same class as $\mathfrak{r}_i$. In particular, if b_i denotes an idèle in the preimage of $\mathfrak{t}$ by Id, there must exist $\alpha \in K^\times$, $u \in \prod_{\mathfrak{q}} \mathcal{O}_{\mathfrak{q}}^\times \times \mathbb{C}^\times$ such that $a_i = \alpha u b_i^2$. Since we want χ to be a character, it must hold that

$$\chi(a_i) = \chi(u)\chi(b_i^2) = \chi(u)\chi(b_i)^2 = \chi(u)\varepsilon(\mathcal{N}(b_i)), \tag{16}$$

so there is a unique possible value for $\chi(a_i)$.

Since $\mathrm{Cl}(K)$ is a finite abelian group, and χ is multiplicative, we only need to understand how to define χ for ideal classes $\mathfrak{r}_i$ whose order is a power of 2, so let us suppose that this is the case. Let

$$\chi(a_i) = \sqrt{\varepsilon(\mathcal{N}(a_i))} \tag{17}$$

(it does not really matter which square root one takes). Then we just extend χ multiplicatively to the whole idèle group. Recall that we already proved that χ^2 and $\varepsilon \circ \mathcal{N}$ coincide on $K^\times \cdot (\prod_{\mathfrak{q}} \mathcal{O}_{\mathfrak{q}}^\times \times \mathbb{C}^\times)$ so with this definition they coincide on the whole idèle group $\mathbb{I}_K$.

There is a caveat here: it is not clear at all why the multiplicative function that we defined is well defined! Once again, a power of the idèle a_i lies in $K^\times \cdot (\prod_{\mathfrak{q}} \mathcal{O}_{\mathfrak{q}}^\times \times \mathbb{C}^\times)$ hence we need to prove that our definition really extends the previous one. To avoid confusions, for the time being let $\tilde{\chi}$ denote the function whose value at the idèles a_i is given by (17) and (16) and χ the character on $K^\times \cdot (\prod_{\mathfrak{q}} \mathcal{O}_{\mathfrak{q}}^\times \times \mathbb{C}^\times)$ defined before; if the idèle a_i corresponds to an ideal of order s in the class group, the consistency relation translates into the equality $\tilde{\chi}(a_i)^s = \chi(a_i^s)$. It is enough to prove it in the following two cases:

• The ideal $\mathfrak{r}_i$ has odd order s in the class group. Then as explained before, there exists $b_i \in \mathbb{I}_K$, $\alpha \in K^\times$ and $u \in \prod_{\mathfrak{q}} \mathcal{O}_{\mathfrak{q}}^\times \times \mathbb{C}^\times$ such that $a_i = \alpha u b_i^2$. Note that $\mathrm{Id}(b_i^s)$ is also a principal ideal, hence b_i^s lies in $K^\times \cdot (\prod_{\mathfrak{q}} \mathcal{O}_{\mathfrak{q}}^\times \times \mathbb{C}^\times)$. Then by (16) and the fact that $\chi^2 = \varepsilon \circ \mathcal{N}$ on $K^\times \cdot (\prod_{\mathfrak{q}} \mathcal{O}_{\mathfrak{q}}^\times \times \mathbb{C}^\times)$, we get that

$$\tilde{\chi}(a_i)^s = \chi(u)^s \varepsilon(\mathcal{N}(b_i))^s = \chi(u)^s \varepsilon(\mathcal{N}(b_i^s)) = \chi(u)^s \chi^2(b_i^s) = \chi(u^s b_i^{2s}) = \chi(a_i^s).$$

• The ideal $\mathfrak{r}_i$ has order a power of 2, say 2^s and is not a square (since it generates the class group). By definition we want to prove the equality

$$\chi(a_i^{2^s}) = \tilde{\chi}(a_i)^{2^s} = \varepsilon(\mathcal{N}(a_i))^{2^{s-1}} = \varepsilon(\mathcal{N}(a_i^{2^{s-1}})).$$

Let $b_i = a_i^{2^{s-1}}$, an idèle whose square satisfies that $\mathrm{Id}(b_i^2)$ is principal. It is enough to prove that for any such idèle, the following equality holds:

$$\chi(b_i^2) = \varepsilon(\mathcal{N}(b_i)). \tag{18}$$

It is well known that the two torsion subgroup of the class group is generated by the prime ideals $\mathfrak{q} = \langle q, \sqrt{-d} \rangle$, where q is an odd prime dividing d, and also the prime $\mathfrak{p}_2 = \langle 2, 1 + \sqrt{-d} \rangle$ when $d \equiv 1 \pmod 4$. Let q be an odd prime dividing d and let b_q be the idèle of K defined by

$$(b_q)_{\mathfrak{p}} = \begin{cases} 1 & \text{if } \mathfrak{p} \neq \mathfrak{q}, \\ \sqrt{-d} & \text{if } \mathfrak{p} = \mathfrak{q}. \end{cases}$$

Then $\mathrm{Id}(b_q) = \mathfrak{q}$. Similarly, if $d \equiv 1 \pmod 4$, let b_2 be the idèle define by

$$(b_2)_{\mathfrak{p}} = \begin{cases} 1 & \text{if } \mathfrak{p} \neq \mathfrak{p}_2, \\ 1 + \sqrt{-d} & \text{if } \mathfrak{p} = \mathfrak{p}_2. \end{cases}$$

Claim: it is enough to prove (18) for the elements b_q.

Suppose that equality (18) holds for them. Let b be an idèle satisfying that $\mathrm{Id}(b)^2$ is principal. Then

$$\mathrm{Id}(b) = \prod_{q \mid 2d} \mathrm{Id}(b_q)^{\epsilon_q},$$

for some $\epsilon_q \in \{0,1\}$, so there exists $\alpha \in K^\times$, and $u \in \prod_{\mathfrak{q}} \mathcal{O}_{\mathfrak{q}}^\times \times \mathbb{C}^\times$ such that $b = \alpha u \prod_{q|2d} b_q^{\epsilon_q}$. By the multiplicative property of the character χ,

$$\chi(b^2) = \chi(u)^2 \prod_{q|2d} \chi(b_q^2)^{\epsilon_q} = \varepsilon(\mathcal{N}(u)) \prod_{q|2d} \varepsilon(\mathcal{N}(b_q))^{\epsilon_q} = \varepsilon(\mathcal{N}(b)).$$

Let q be an odd prime dividing d. To prove (18) for the elements b_q, we compute both sides of the equality and prove that they coincide. Note that $b_q^2 = qc_q$, where $q \in K^\times$ and $c_q = b_q^2/q$ has the property that it is a unit at all finite places. Then

$$\chi(b_q^2) = \chi_{\mathfrak{q}}\left(\frac{-d}{q}\right) \chi_2\left(\frac{1}{q}\right) \prod_{\mathfrak{p} \in Q_1 \cup Q_5 \cup Q_7} \chi_{\mathfrak{p}}\left(\frac{1}{q}\right), \tag{19}$$

where the product runs over primes $\mathfrak{p} \neq \mathfrak{q}$. On the other hand, the right hand side of (18) equals

$$\varepsilon(\mathcal{N}(b_q)) = \varepsilon_q(d) = \varepsilon_q(d/q)\varepsilon_2(q)^{-1} \prod_{p \in Q_3 \cup Q_5} \varepsilon_p(q)^{-1}, \tag{20}$$

where the product runs over primes different from q. Recall that for each ramified prime, under the isomorphism $(\mathcal{O}_K/\mathfrak{p})^\times \simeq (\mathbb{Z}/p)^\times$, we have the equality $\chi_{\mathfrak{p}} = \varepsilon_p \delta_p$. In particular, both sides evaluate the same at elements of $\mathbb{Z}_p^\times$. Using such a relation in (19) for all odd ramified primes and gathering together the terms involving ε gives

$$\begin{aligned} \chi(b_q^2) = \chi_2^{-1}(q)\varepsilon_q\left(\frac{-d}{q}\right) \prod_{\substack{p \in Q_1 \cup Q_3 \cup Q_5 \cup Q_7 \\ p \neq q}} \varepsilon_p^{-1}(q) \cdot \delta_q\left(\frac{-d}{q}\right) \prod_{\substack{p \in Q_1 \cup Q_3 \cup Q_5 \cup Q_7 \\ p \neq q}} \delta_p(q) = \\ = \varepsilon_q(d)\left(\chi_2^{-1}(q)\varepsilon_q(-1)\varepsilon_2(q)\delta_q(2)^{v_2(d)}\right) \cdot \left(\delta_q(2)^{v_2(d)}\delta_q\left(\frac{-d}{q}\right) \prod_{\substack{p \in Q_1 \cup Q_3 \cup Q_5 \cup Q_7 \\ p \neq q}} \delta_p(q)\right). \end{aligned} \tag{21}$$

Our goal is to prove that the product of all the factors of the last expression except the first one is 1 for the result to hold. When $q \equiv 1 \pmod 4$, quadratic reciprocity implies that $\delta_q(p) = \delta_p(q)$ and $\delta_q(-1) = 1$, so the last factor (between round brackets) in (21) equals 1. On the other hand, for $q \equiv 3 \pmod 4$ quadratic reciprocity implies that $\delta_q(p) = \delta_p(q)\delta_p(-1)$. Note that q is one of the elements in $Q_3 \cup Q_7$, so the last factor in (21) equals $(-1)^{\#Q_3+\#Q_7}$. In both cases, the last factor equals $\delta_{-1}(q)^{\#Q_3+\#Q_7}$.

Regarding the second factor, quadratic reciprocity again implies that $\delta_q(2) = \delta_2(q)$ (recall the definition of δ_2 from Table 3.1). By definition $\varepsilon_2 = \delta_{-1}^{\#Q_3+\#Q_5}$ and on elements of $\mathbb{Z}_2^\times$, $\chi_2 = \delta_2^{v_2(d)+1}\delta_{-1}^{\#Q_5+\#Q_7}$ (see (14)) then the right hand side of (21) equals

$$\varepsilon_q(d)\delta_2(q)\varepsilon_q(-1)\delta_{-1}(q)^{2\#Q_3+2\#Q_5+2\#Q_7} = \varepsilon_q(d)\delta_2(q)\varepsilon_q(-1).$$

Then we are led to prove that $\varepsilon_q(-1)\delta_2(q) = 1$, which follows from the definitions, since:

- If $q \equiv \pm 1 \pmod 8$, $\varepsilon_q(-1) = 1 = \delta_2(q)$.
- If $q \equiv \pm 3 \pmod 8$, $\varepsilon_q(-1) = -1 = \delta_2(q)$.

Suppose now that $d \equiv 1 \pmod 4$, when we also need to check the compatibility for b_2. A similar computation as the previous one gives that:

$$\varepsilon_2(1+d) = \varepsilon_2\left(\frac{1+d}{2}\right) \cdot \prod_{p \in Q_3 \cup Q_5} \varepsilon_p(2)^{-1},$$

while

$$\chi(b_i^2) = \chi_2\left(\frac{(1+\sqrt{-d})^2}{2}\right) \cdot \prod_{p \in Q_3 \cup Q_5} \varepsilon_p(2)^{-1} \cdot \prod_{p \in Q_1 \cup Q_3 \cup Q_5 \cup Q_7} \delta_p(2).$$

By quadratic reciprocity, $\prod_{p \in Q_1 \cup Q_3 \cup Q_5 \cup Q_7} \delta_p(2) = (-1)^{\#Q_3+\#Q_5}$, so the statement follows from the following easy to verify (from its definitions) facts:

- If $d \equiv 1 \pmod 8$, then $\varepsilon_2\left(\frac{1+d}{2}\right) = 1$, $\chi_2\left(\frac{(1+\sqrt{-d})^2}{2}\right) = 1$ and $\#Q_3 + \#Q_5$ is even.

- If $d \equiv 5 \pmod{16}$, then $\varepsilon_2\left(\frac{1+d}{2}\right) = -1$, $\chi_2\left(\frac{(1+\sqrt{-d})^2}{2}\right) = 1$ and $\#Q_3 + \#Q_5$ is odd.
- If $d \equiv 13 \pmod{16}$, then $\varepsilon_2\left(\frac{1+d}{2}\right) = 1$, $\chi_2\left(\frac{(1+\sqrt{-d})^2}{2}\right) = -1$ and $\#Q_3 + \#Q_5$ is odd.

Now that we defined the character χ on the whole idèle group and proved that it is well defined, we only need to verify that our extension also satisfies

$$^{\tau}\chi = \chi \cdot (\psi_{-2} \circ \mathcal{N})$$

for all elements of $\mathbb{I}_K$. Since we already proved this is the case for elements of $K^\times \cdot (\prod_{\mathfrak{q}} \mathcal{O}_{\mathfrak{q}}^\times \times \mathbb{C}^\times)$, it is enough to prove it for the idèles a_i (as defined before) with local finite components

$$(a_i)_{\mathfrak{p}} = \begin{cases} r_i & \text{if } \mathfrak{p} = \mathfrak{r}_i, \\ 1 & \text{otherwise.} \end{cases}$$

Note that $\tau(a_i)$ is the idèle of K with value r_i at $\overline{\mathfrak{r}_i}$ and 1 at the other places. Then

$$^{\tau}\chi(a_i) = \chi(\tau(a_i)) = \chi(a_i)^{-1}\chi(a_i\tau(a_i)) = \chi(a_i)^{-1}\chi\left(\frac{a_i\tau(a_i)}{r_i}\right), \tag{22}$$

where $\frac{1}{r_i}$ denotes the image by $K^\times \hookrightarrow \mathbb{I}_K$. Note that $\frac{a_i\tau(a_i)}{r_i}$ is a unit at all places, so

$$\chi\left(\frac{a_i\tau(a_i)}{r_i}\right) = \chi_2(r_i)^{-1} \prod_{\mathfrak{p}\in Q_1\cup Q_5\cup Q_7} \chi_{\mathfrak{p}}(r_i)^{-1}. \tag{23}$$

By the product formula,

$$1 = \varepsilon(r_i) = \varepsilon_{r_i}(r_i)\varepsilon_2(r_i) \prod_{p\in Q_3\cup Q_5} \varepsilon_p(r_i). \tag{24}$$

Since $\varepsilon_{r_i}(r_i) = \varepsilon(\mathcal{N}(a_i)) = \chi^2(a_i)$, multiplying (23) and (24) and using that $\chi_{\mathfrak{p}}(r_i) = \varepsilon_p(r_i)\delta_p(r_i)$ we get that

$$\chi\left(\frac{a_i\tau(a_i)}{r_i}\right) = \chi^2(a_i)\chi_2(r_i)^{-1}\varepsilon_2(r_i) \prod_{p\in Q_1\cup Q_3\cup Q_5\cup Q_7} \delta_p(r_i). \tag{25}$$

Recall that r_i splits in K, hence $\left(\frac{-d}{r_i}\right) = 1$ and quadratic reciprocity implies that

$$1 = \left(\frac{2}{r_i}\right)^{v_2(d)} \left(\frac{-1}{r_i}\right)^{\#Q_3+\#Q_7+1} \prod_{p\in Q_1\cup Q_3\cup Q_5\cup Q_7} \delta_p(r_i).$$

In particular, the right hand side of (22) equals

$$\chi(a_i)\chi_2(r_i)^{-1}\varepsilon_2(r_i)\delta_2(r_i)^{v_2(d)}\delta_{-1}(r_i)^{\#Q_3+\#Q_7+1} = \chi(a_i)\cdot\left(\delta_2(r_i)\delta_{-1}(r_i)^{\#Q_5+\#Q_7}\varepsilon_2(r_i)\delta_{-1}(r_i)^{\#Q_3+\#Q_7+1}\right).$$

A similar (but easier) computation shows that $\psi_{-2}(\mathcal{N}(a_i)) = \delta_{-2}(r_i)$, so the result follows from the equality

$$\delta_2(r_i)\varepsilon_2(r_i)\delta_{-1}(r_i)^{\#Q_3+\#Q_5+1} = \delta_2(r_i)\delta_{-1}(r_i) = \delta_{-2}(r_i).$$

□

Remark 6. The precise conductor $\mathfrak{f}$ of $\chi_{\mathfrak{p}_2}$ has valuation:

$$v(\mathfrak{f}) = \begin{cases} 5 & \text{if } d \equiv 1 \pmod 8, \\ 3 & \text{if } d \equiv 3,5,6 \pmod 8, \\ 3 & \text{if } d \equiv 2 \pmod 8 \text{ and } 2 \nmid \#Q_3 + \#Q_5, \\ 0 & \text{if } d \equiv 2 \pmod 8 \text{ and } 2 \mid \#Q_3 + \#Q_5. \end{cases}$$

When $d \equiv 7 \pmod 8$ it is either $0, 2, 3$ depending on its choice.

Although we constructed one Hecke character satisfying that

$$^{\tau}\chi = \chi \cdot \psi_{-2},$$

it is a natural problem to understand all such possible finite order Hecke characters. Note that if χ is such a character, and ν is a character of $\mathrm{Gal}_{\mathbb{Q}}$, then $\chi \cdot \nu$ also satisfies the same condition.

Theorem 3.3. *Let χ_1 and χ_2 be finite order Hecke characters such that ${}^\tau\chi_i = \chi_i \cdot \psi_{-2}$ for $i = 1, 2$. Then there exists a rational character $\nu : \mathrm{Gal}_{\mathbb{Q}} \to \overline{\mathbb{Q}}^\times$ such that $\chi_2 = \chi_1 \cdot \nu$.*

Proof. Let $\tilde{\nu}$ denote the quotient $\frac{\chi_1}{\chi_2}$, a character on $\mathbb{I}_K$. The hypothesis ${}^\tau\chi_i = \chi_i \cdot \psi_{-2}$ implies that ${}^\tau\tilde{\nu} = \tilde{\nu}$. Let $\mathbb{I}_K^1$ be the kernel of the norm map $\mathcal{N} : \mathbb{I}_K \to \mathbb{I}_{\mathbb{Q}}$.

Claim: the character $\tilde{\nu}$ is trivial on $\mathbb{I}_K^1$.

To prove the claim, let v be a place of $\mathbb{Q}$ which does not split in K, and let w be the place of K dividing it. In particular $K_w/\mathbb{Q}_v$ is a Galois quadratic extension. If $k \in K_w$ has norm one, Hilbert's theorem 90 implies that there exists $t \in K_w$ such that $k = \frac{t}{\sigma(t)}$ for $\sigma \in \mathrm{Gal}(K_w/\mathbb{Q}_v)$ non-trivial. The hypothesis ${}^\tau\tilde{\nu} = \tilde{\nu}$ then implies that $\tilde{\nu}(k) = 1$. If the place v happens to split, let w_1, w_2 be the two places of K above it and let $(k_1, k_2) \in K_{w_1} \times K_{w_2}$ be an element of norm one, i.e. $k_1 \cdot k_2 = 1$. The hypothesis ${}^\tau\tilde{\nu} = \tilde{\nu}$ implies that $\tilde{\nu}_{w_1} = \tilde{\nu}_{w_2}$, so $\tilde{\nu}_{w_1}(k_1)\tilde{\nu}_{w_2}(k_2) = \tilde{\nu}_{w_1}(k_1 \cdot k_2) = 1$ as claimed.

Then the character $\tilde{\nu}$ gives a well defined character on $\mathcal{N}(\mathbb{I}_K)$, a subgroup of $\mathbb{I}_{\mathbb{Q}}$ and we can extend it to $\mathbb{Q}^\times \mathcal{N}(\mathbb{I}_K)$ by making it trivial at elements of $\mathbb{Q}^\times$. Recall that $\mathbb{Q}^\times \mathcal{N}(\mathbb{I}_K)$ has finite index in $\mathbb{I}_{\mathbb{Q}}$ so let ν be any extension of $\tilde{\nu}$ to the whole idèle group $\mathbb{I}_{\mathbb{Q}}$. Then by construction $\tilde{\nu}$ coincides with $\nu \circ \mathcal{N}$ on $\mathbb{I}_K$, so in particular $\chi_1 = \chi_2 \cdot (\nu \circ \mathcal{N})$. □

It is also natural to study whether our construction can be extended to negative values of d, i.e. to real quadratic fields. The problem now is that we need some control on the fundamental unit. In this case, we have a partial answer.

Theorem 3.4. *Suppose that $K = \mathbb{Q}(\sqrt{d})$ is a real quadratic field, whose fundamental unit has norm -1. Then the same statement of Theorem 3.2 holds.*

Proof. To use the previous results, write $d = -(-d)$ (so $d < 0$ in the above notations/definitions) and make precisely the same local definitions for both ε and χ at finite places. There are two important facts to consider: while proving (15), we get an extra -1 factor coming from the fact that we changed $d \leftrightarrow -d$. This forces us to add ramification at one of the archimedean places (we will latter specify which one).

Let ϵ be a fundamental unit (fixed). The proof works mutatis mutandis once we checked the compatibility of χ at ϵ. Our assuming ϵ of norm -1, implies that $Q_3 = Q_7 = \emptyset$, the reason being that if $\epsilon = a + b\sqrt{d}$, with $2a, 2b \in \mathbb{Z}$, the condition $a^2 - db^2 = -1$ implies that -1 is a square modulo all odd primes dividing d. Furthermore, for all such primes, the reduction of ϵ has order 4, so that $\chi_p(\epsilon) = \pm 1$ if $p \in Q_1$ and a primitive fourth root of unity if $p \in Q_5$. We claim that $\chi_2(\epsilon) \prod_{p \in Q_5} \chi_p(\epsilon) = \pm 1$ (and therefore $\chi_2(\epsilon) \prod_{p \in Q_1 \cup Q_5} \chi_p(\epsilon) = \pm 1$).

- If $d \equiv 1 \pmod 8$ then $\#Q_5$ is even and χ_2 is quadratic, hence the statement.
- If $d \equiv 5 \pmod 8$ (the case $d = 3$ in Table 3.3) $\#Q_5$ is odd, 2 is inert, χ_2 has order 4 and evaluated at any element of order 4 gives a primitive fourth root of unity.
- If $d \equiv 2 \pmod 8$ and $\#Q_5$ is even, χ_2 has order 2, while if $\#Q_5$ is odd, χ_2 has order 4 and ϵ has order 8 (which follows from Table 3.3, as its norm equals -1) so $\chi_2(\epsilon)$ is a fourth root of unity.

Then if the product $\chi_2(\epsilon) \prod_{p \in Q_1 \cup Q_5} \chi_p(\epsilon) = 1$, define χ to be trivial at the archimedean component where ϵ is negative and the sign character at the other, while if the product equals -1, take the opposite choice. Since $\mathcal{N}(\epsilon) = -1$, the compatibility is satisfied and the same proof of Theorem 3.2 applies. □

For general real quadratic fields we run some numerical experiments (a couple of hundreds) and in all cases, a character of the expected conductor is found. The result will be explained (and proved) in a sequel (see [PV22]).

3.2. **The case $t \equiv 3 \pmod 4$.** Let $K = \mathbb{Q}(\sqrt{-d})$ with $d > 0$ (square-free). The method is very similar to the previous case. Define the following sets:

- $Q_{++} = \{p \mid d,\ p \nmid 2t,\ p \equiv \square \pmod 4,\ p \equiv \square \pmod t\}$.
- $Q_{+-} = \{p \mid d,\ p \nmid 2t,\ p \equiv \square \pmod 4,\ p \not\equiv \square \pmod t\}$.
- $Q_{-+} = \{p \mid d,\ p \nmid 2t,\ p \not\equiv \square \pmod 4,\ p \equiv \square \pmod t\}$.
- $Q_{--} = \{p \mid d,\ p \nmid 2t,\ p \not\equiv \square \pmod 4,\ p \not\equiv \square \pmod t\}$.

We have the following elementary result (that will clarify later computations).

Lemma 3.5. *Suppose that t is unramified in K. Then the prime t splits in K precisely when the following equality holds:*

$$(-1)^{\#Q_{+-}+\#Q_{--}}\delta_t(2)^{v_2(d)} = -1.$$

Similarly, it is inert when $(-1)^{\#Q_{+-}+\#Q_{--}}\delta_t(2)^{v_2(d)} = 1$.

Proof. Follows easily from the well known fact that t splits in $\mathbb{Q}(\sqrt{-d})$ if and only if $-d$ is a square modulo t. □

The character ε: Define an even character $\varepsilon : \mathbb{I}_{\mathbb{Q}} \to \overline{\mathbb{Q}}^{\times}$ ramified at the primes in Q_{++}, Q_{-+}, Q_{+-} and eventually at 2 and t. Its local components ε_p are defined as follows:

- For primes $p \in Q_{++} \cup Q_{-+}$, the character $\varepsilon_p : \mathbb{Z}_p^{\times} \to \overline{\mathbb{Q}}^{\times}$ is quadratic, i.e, $\varepsilon_p = \delta_p$.
- For primes $p \in Q_{+-}$, the character $\varepsilon_p : \mathbb{Z}_p^{\times} \to \overline{\mathbb{Q}}^{\times}$ is any character of order $2^{v_2(p-1)}$.
- For $p = t$ define $\varepsilon_t = \begin{cases} \delta_t^{\#Q_{+-}+\#Q_{--}+v_t(d)+v_2(d)+1} & \text{if } t \equiv 3 \pmod 8, \\ \delta_t^{\#Q_{+-}+\#Q_{--}+v_t(d)+1} & \text{if } t \equiv 7 \pmod 8. \end{cases}$
- For $p = 2$ define $\varepsilon_2 = \begin{cases} \delta_{-1}^{\#Q_{-+}+\#Q_{--}+v_t(d)+v_2(d)+1} & \text{if } t \equiv 3 \pmod 8, \\ \delta_{-1}^{\#Q_{-+}+\#Q_{--}+v_t(d)+1} & \text{if } t \equiv 7 \pmod 8. \end{cases}$
- At all other primes, ε_p is trivial.
- The character ε_∞ (the archimidean component) is trivial.

By Lemma 3.5, ε_t is trivial if t splits in K and equals δ_t if t is inert in K. A similar result for ε_2 is the following.

Lemma 3.6. *The previous defined character ε_2 satisfies that*

$$\varepsilon_2 = \begin{cases} 1 & \text{if } d \equiv 3 \pmod 4, \\ \delta_{-1} & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Proof. Since $2 \nmid d$, the prime 2 is ramified in K if and only if $-d \equiv 3 \pmod 4$. Recall that the prime t is not an element of $Q_{\pm\pm}$, so the prime divisors of d congruent to 3 modulo 4 are precisely the ones in $Q_{-+} \cup Q_{--}$ and possibly t. Then the prime 2 is ramified in K precisely when $\#Q_{-+} + \#Q_{--} + v_t(d)$ is even. Since $2 \nmid d$, ε_2 equals δ_{-1} when 2 is ramified and 1 when it is unramified, as claimed. □

With the above definitions, and using that $\varepsilon_2(-1)\varepsilon_t(-1) = (-1)^{\#Q_{+-}+\#Q_{-+}}$, it is not hard to verify that

$$\prod_p \varepsilon_p(-1)\varepsilon_\infty(-1) = (-1)^{\#Q_{-+}+\#Q_{+-}}\varepsilon_2(-1)\varepsilon_t(-1) = 1.$$

The main result of the present section is the following.

Theorem 3.7. *There exists a Hecke character $\chi : \mathrm{Gal}_K \to \overline{\mathbb{Q}}^{\times}$ such that:*

(1) $\chi^2(\sigma) = \varepsilon(\sigma)$ for all $\sigma \in \mathrm{Gal}_K$,
(2) χ is unramified at primes not dividing $2t\prod_{p \in Q_{+-} \cup Q_{--}} p$,
(3) If $\tau \in \mathrm{Gal}_{\mathbb{Q}}$ is not the identity on K, ${}^{\tau}\chi = \chi \cdot \psi_{-t}$ as characters of Gal_K.

Proof. Following the strategy described at the beginning of the section, define $\chi_p : \mathcal{O}_{\mathfrak{p}}^{\times} \to \overline{\mathbb{Q}}^{\times}$ by:

- If $\mathfrak{p}$ is an odd (i.e. $\mathfrak{p} \nmid 2$) unramified prime, $\chi_{\mathfrak{p}}$ is the trivial character.
- If $p \in Q_{\pm\pm}$ and $\mathfrak{p} \mid p$,

$$\chi_{\mathfrak{p}} = \varepsilon_p\delta_p. \tag{26}$$

- At primes $\mathfrak{t}$ dividing t, define the character $\chi_{\mathfrak{t}}$ by
  - If t ramifies in K, $\chi_{\mathfrak{t}} = \varepsilon_t$.
  - If t splits in K, say $t = \mathfrak{t}\bar{\mathfrak{t}}$, let $\chi_{\mathfrak{t}} = \delta_t$ and $\chi_{\bar{\mathfrak{t}}} = 1$.
  - If t is inert in K, $\chi_{\mathfrak{t}}$ is an order 4 character (hence its restriction to $\mathbb{F}_t^{\times}$ is trivial).

  We will denote in all cases $\chi_t = \prod_{\mathfrak{t}|t} \chi_{\mathfrak{t}}$.
- At a prime $\mathfrak{p}_2$ dividing 2, define the character $\chi_{\mathfrak{p}_2}$ as follows:
  - If 2 is not ramified in $K/\mathbb{Q}$, it is trivial.

– If 2 ramifies in $K/\mathbb{Q}$ but $2 \nmid d$, then define $\chi_{\mathfrak{p}_2}$ as:
  * if $t \equiv 3 \pmod 8$, the character of conductor 2 sending $\sqrt{-d}$ to -1.
  * if $t \equiv 7 \pmod 8$, the trivial character.
– If $2 \mid d$ then $\chi_{\mathfrak{p}_2}$ is the character of conductor $\mathfrak{p}_2^5$ whose value at the generators 5, -1 and $1+\sqrt{-d}$ equals: $\chi_{\mathfrak{p}_2}(5) = -1$, $\chi_{\mathfrak{p}_2}(-1) = \delta_2(t)$ and
  * If $d \equiv 2 \pmod 8$, $\chi_{\mathfrak{p}_2}(1+\sqrt{-d}) = \begin{cases} 1 & \text{if } t \equiv 3 \pmod 8, \\ \sqrt{-1} & \text{if } t \equiv 7 \pmod 8. \end{cases}$
  * If $d \equiv 6 \pmod 8$, $\chi_{\mathfrak{p}_2}(1+\sqrt{-d}) = \begin{cases} \sqrt{-1} & \text{if } t \equiv 3 \pmod 8, \\ -1 & \text{if } t \equiv 7 \pmod 8. \end{cases}$

  Abusing notation, we will write $\chi_2 = \chi_{\mathfrak{p}_2}$.
- The archimidean component of χ is trivial.

Let us recall some properties of the local characters just defined (which motivate their definition) that will play a crucial role.

(P1) The product $\varepsilon_t\chi_t$ on elements of $\mathbb{Z}_t^\times$ equals

$$\varepsilon_t\chi_t = \begin{cases} \delta_t & \text{if } t \nmid d, \\ 1 & \text{if } t \mid d. \end{cases}$$

(P2) If $d \equiv 1 \pmod 4$ then $\chi_2(\sqrt{-d}) = \delta_t(2)$.
(P3) If $2 \mid d$, then $\chi_2^2(1+\sqrt{-d}) = \chi_2(1+d)$.
(P4) If $2 \mid d$ then $\chi_2|_{\mathbb{Z}_2^\times} = \delta_{-2}$ if $t \equiv 3 \pmod 8$ and $\chi_2|_{\mathbb{Z}_2^\times} = \delta_2$ if $t \equiv 7 \pmod 8$.
(P5) In all cases $\chi_2(-1) = \delta_2(t)^{v_2(d)}$ and $\chi_2(t) = 1$.

As in the previous case, define χ on $K^\times \cdot (\prod_{\mathfrak{q}} \mathcal{O}_{\mathfrak{q}}^\times \times \mathbb{C}^\times)$ to be trivial at elements of $K^\times$ and as the product of the local component at elements of the second factor. We claim that χ satisfies the expected three properties.

(1) We need to verify that the equality

$$\chi^2 = \varepsilon \circ \mathcal{N}$$

holds for all elements of $K^\times \cdot (\prod_{\mathfrak{q}} \mathcal{O}_{\mathfrak{q}}^\times \times \mathbb{C}^\times)$. As before, it is enough to prove it componentwise, and the result for all primes not dividing $2t$ follows from (26) together with Lemma 3.1.

For primes dividing t, the case t split and t ramified follows from the fact that both χ_t^2 and $\varepsilon_t \circ \mathcal{N}$ are trivial. In the inert case, it is enough to check the condition at a generator g of $\mathbb{F}_{t^2}^\times$: $\chi_t^2(g) = -1$ (as χ_t has order 4), and $\varepsilon_t(\mathcal{N}(g)) = -1$ because $\mathcal{N}(g)$ generates $\mathbb{F}_t^\times$.

If $2 \nmid d$, the statement is also clear as χ_2^2 is trivial and ε_2 is trivial if 2 is unramified (by Lemma 3.6) and δ_{-1} when 2 is ramified. But the norm map in the ramified case only takes the values $\{0,1,2\}$ modulo 4, hence $\delta_{-1} \circ \mathcal{N}$ is trivial as well. At last, if $2 \mid d$, both χ_2^2 and $\varepsilon_2 \circ \mathcal{N}$ are trivial at elements of $\mathbb{Z}_2^\times$ and agree at $1+\sqrt{-d}$ by (P3).

(2) The ramification statement is clear from the definition.

(3) For odd primes $\mathfrak{p}$ not dividing t the local character $(\psi_{-t})_p \circ \mathcal{N}$ is trivial while ${}^\tau\chi_{\mathfrak{p}} = \chi_{\mathfrak{p}}$, hence the statement. For primes dividing 2, since $(\psi_{-t})_2 \circ \mathcal{N}$ is also trivial, we need to verify that ${}^\tau\chi_2 = \chi_2$ (remember the notation $\chi_2 = \chi_{\mathfrak{p}_2}$, where $\mathfrak{p}_2$ is any prime dividing 2). This follows easily from its definition when $2 \nmid d$. When $2 \mid d$, we only need to verify the property at the element $1+\sqrt{-d}$, but ${}^\tau\chi_2(1+\sqrt{-d}) = \chi_2(1-\sqrt{-d}) = \chi_2(1+\sqrt{-d})^{-1}\chi_2(1+d) = \chi_2(1+\sqrt{d})$ by (P3).
Let $\mathfrak{t}$ be a prime dividing t. If t ramifies in K, $(\psi_{-t})_t \circ \mathcal{N}$ is trivial while ${}^\tau\chi_{\mathfrak{t}} = \chi_{\mathfrak{t}}$, hence the statement. If t splits, without loss of generality we can assume that $\chi_{\mathfrak{t}}$ matches $(\psi_{-t})_t \circ \mathcal{N}$ and $\chi_{\bar{\mathfrak{t}}}$ is trivial, so the result holds. At last, suppose that t is inert in K. Let g be a generator of $\mathbb{F}_{t^2}^\times$; then ${}^\tau\chi_t(g)\chi_t(g) = \chi_t(\mathcal{N}(g)) = 1$ (since χ_t is trivial on elements of $\mathbb{F}_t^\times$) so ${}^\tau\chi_t = \chi_t^{-1}$. On the other hand, $\delta_t(\mathcal{N}(g)) = -1$ because $\mathcal{N}(g)$ is a generator of $\mathbb{F}_t^\times$, hence (since $\chi_t(g)$ is a fourth root of unity) ${}^\tau\chi_t(g) = \chi_t(g)^{-1} = -\chi_t(g) = \chi_t(g) \cdot \psi_{-t}(\mathcal{N}(g))$ as claimed.

Compatibility: since all characters have order a power of 2, the compatibility relation at roots of unity of order 3 (if K happens to have one) is trivial. The only case when K contains roots of unity of order 4 is for $K = \mathbb{Q}(\sqrt{-1})$. In such a case, all sets $Q_{\pm,\pm}$ are empty. By definition:

(1) $\chi_2(\sqrt{-1}) = -1$ if $t \equiv 3 \pmod 8$ and 1 if $t \equiv 7 \pmod 8$.
(2) χ_t is an order 4 character (since t is inert in $\mathbb{Q}(\sqrt{-1})$) whose restriction to $\mathbb{F}_t^\times$ is trivial.

Since $t \equiv 3 \pmod 4$, -1 is not a square in $\mathbb{F}_t$, hence $\sqrt{-1}$ is an element of $\mathbb{F}_{t^2}^\times$ so $\chi_t(\sqrt{-1}) \in \{\pm 1\}$. Let g be a generator of $\mathbb{F}_{t^2}$, and let $\sqrt{-1} = g^e$. Recall that the minimum power of g in $\mathbb{F}_t^\times$ is $t+1$, hence if $t \equiv 3 \pmod 8$, e has valuation one at 2 so $\chi_t(\sqrt{-1}) = -1$, while if $t \equiv 7 \pmod 8$, $4 \mid e$ and $\chi_t(\sqrt{-1}) = 1$ as needed.

For all other fields (abusing a little notation) we have

$$\chi(-1) = \prod_{\mathfrak{p} \in Q_{+-} \cup Q_{--}} \chi_{\mathfrak{p}}(-1)\chi_2(-1)\chi_t(-1) = (-1)^{\#Q_{+-}+\#Q_{--}}\chi_2(-1)\chi_t(-1).$$

Recall from property (P5) that $\chi_2(-1) = \delta_t(2)^{v_2(d)}$. Consider the different cases:

- If t is unramified in K, quadratic reciprocity (Lemma 3.5) implies that t splits in K (respectively is inert in K) if and only if $(-1)^{\#Q_{+-}+\#Q_{--}}\delta_t(2)^{v_2(d)} = -1$ (respectively 1). In the first case $\chi_t(-1) = -1$ while in the second it equals 1. In both cases, $(-1)^{\#Q_{+-}+\#Q_{--}}\chi_2(-1)\chi_t(-1) = 1$ as expected.
- If t ramifies in K, by definition $\chi_t = \varepsilon_t$, its value at -1 equals
$$\varepsilon_t(-1) = (-1)^{\#Q_{+-}+\#Q_{--}}\delta_t(2)^{v_2(d)}.$$

Extension: we extend our character χ to idèles whose image generates the class group $\mathrm{Cl}(K)$ exactly as in the previous case, namely via (16) for ideals of odd order in the class group and via (17) for those whose order is a power of 2. Then we are led to prove that if for each odd prime number q dividing d (and also for $q = 2$ if $d \equiv 1 \pmod 4$), b_q denotes the idèle

$$(b_q)_{\mathfrak{p}} = \begin{cases} 1 & \text{if } \mathfrak{p} \neq \mathfrak{q}, \\ \sqrt{-d} & \text{if } \mathfrak{p} = \mathfrak{q}. \end{cases}$$

then

$$\chi(b_q^2) = \varepsilon(\mathcal{N}(b_i)). \tag{27}$$

Once again, we compute both sides of the equation to verify that they do match. Start supposing that $q \neq t$, then the left hand side equals

$$\chi(b_q^2) = \chi_{\mathfrak{q}}\left(\frac{-d}{q}\right)\chi_2\left(\frac{1}{q}\right)\chi_t\left(\frac{1}{q}\right)\prod_{\mathfrak{p} \in Q_{\pm\pm}}\chi_{\mathfrak{p}}\left(\frac{1}{q}\right), \tag{28}$$

where the product is over primes which do not divide q. On the other hand, the right hand side equals

$$\varepsilon(\mathcal{N}(b_q)) = \varepsilon(d) = \varepsilon_q(d/q)\varepsilon_2(q)^{-1}\varepsilon_t(q)\prod_{p \in Q_{\pm\pm}}\varepsilon_p(q)^{-1}, \tag{29}$$

where the product runs over primes different from q. Recall that for all ramified primes different from t, $\chi_{\mathfrak{p}} = \varepsilon_p\delta_p$. In particular, both sides evaluate the same at elements of $\mathbb{Z}_p^\times$. Using such a relation in (28) for all odd ramified primes different from t we get

$$\chi(b_q^2) = \chi_2(q)^{-1}\chi_t(q)^{-1}\varepsilon_q\left(\frac{-d}{q}\right)\prod_{\substack{p \in Q_{\pm\pm} \\ p \neq q}}\varepsilon_p(q)^{-1} \cdot \delta_q\left(\frac{-d}{q}\right)\prod_{\substack{p \in Q_{\pm\pm} \\ p \neq q}}\delta_p(q) = \tag{30}$$

$$= \varepsilon_q(d)\left(\chi_2(q)^{-1}\chi_t(q)^{-1}\varepsilon_q(-1)\varepsilon_2(q)\varepsilon_t(q)^{-1}\delta_q(2)^{v_2(d)}\delta_q(t)^{v_t(d)}\right) \cdot \left(\delta_q(2)^{v_2(d)}\delta_q(t)^{v_t(d)}\delta_q\left(\frac{-d}{q}\right)\prod_{\substack{p \in Q_{\pm\pm} \\ p \neq q}}\delta_p(q)\right).$$

Our goal is to prove that the product of all the factors except the first one is 1 for the result to hold. By quadratic reciprocity, if p, q are odd primes, then

$$\delta_p(q)\delta_q(p) = \begin{cases} 1 & \text{if } p \in Q_{+\pm}, \\ \delta_{-1}(q) & \text{if } p \in Q_{-\pm}. \end{cases}$$

Then the last term of (30) equals $\delta_{-1}(q)^{\#Q_{-+}+\#Q_{--}}$. Regarding the middle factor, we claim that the following equality holds (note that it does not involve the factor $\varepsilon_q(-1)$):

$$\left(\chi_2(q)^{-1}\chi_t(q)^{-1}\varepsilon_2(q)\varepsilon_t(q)\delta_q(2)^{v_2(d)}\delta_q(t)^{v_t(d)}\right)\delta_{-1}(q)^{\#Q_{-+}+\#Q_{--}} = \delta_q(t). \tag{31}$$

Since all the above values belong to $\{\pm 1\}$ we can remove the inverses. By property (P1), $\chi_t(q)\varepsilon_t(q) = \delta_t(q)^{1+v_t(d)}$, so quadratic reciprocity implies that $\chi_t(q)\varepsilon_t(q)\delta_q(t)^{v_t(d)} = \delta_q(t)\delta_{-1}(q)^{1+v_t(d)}$, and the claim is equivalent to the equality

$$\left(\chi_2(q)\varepsilon_2(q)\delta_q(2)^{v_2(d)}\right)\delta_{-1}(q)^{\#Q_{-+}+\#Q_{--}+1+v_t(d)} = 1.$$

The last term equals $\varepsilon_2(q)$ when $t \equiv 7 \pmod 8$ and it equals $\varepsilon_2(q)\delta_{-1}(q)^{v_2(d)}$ when $t \equiv 3 \pmod 8$. But recall that χ_2 on elements of $\mathbb{Z}_2^\times$ is trivial when $2 \nmid d$ and when $2 \mid d$, it equals δ_{-2} if $t \equiv 3 \pmod 8$ and δ_2 if $t \equiv 7 \pmod 8$ by property (P4). Then the claim follows from the observation that $\delta_q(2) = \delta_2(q)$.

To finish the compatibility proof when $q \neq t$, we need to verify that $\delta_q(t)\varepsilon_q(-1) = 1$, an equality that follows from the definitions (that are collected in Table 3.4).

$q \pmod 4$	$q \pmod t$	$\varepsilon_q(-1)$	$\delta_q(t)$	$q \pmod 4$	$q \pmod t$	$\varepsilon_q(-1)$	$\delta_q(t)$
1	$\square$	1	1	3	$\square$	-1	-1
1	$\not\square$	-1	-1	3	$\not\square$	1	1

TABLE 3.4.

If $q = t$ (so in particular $t \mid d$) the computation is similar, replacing q by t in (28) and in (29) but omitting the factor with subscript t. Note that in this case property (P1) states that $\chi_t\varepsilon_t = 1$ so the analogue of (30) becomes

$$\chi(b_t^2) = \chi_2(t)\varepsilon_t\left(\frac{-d}{t}\right)\prod_{p\in Q_{\pm\pm}}\varepsilon_p(q)^{-1}\cdot\prod_{p\in Q_{\pm\pm}}\delta_p(q) = \varepsilon_t(d)\left(\chi_2(t)\varepsilon_t(-1)\varepsilon_2(t)\right)\cdot\left(\prod_{p\in Q_{\pm\pm}}\delta_p(t)\right). \tag{32}$$

Quadratic reciprocity implies that $\delta_p(t) = 1$ if $p \in Q_{++} \cup Q_{--}$ and -1 if $p \in Q_{+-} \cup Q_{-+}$. Then the last factor equals $(-1)^{\#Q_{+-}+\#Q_{-+}} = \varepsilon_t(-1)\varepsilon_2(t)$ (since $\delta_t(-1) = -1$ and $\delta_{-1}(t) = -1$) and the validity of (32) follows from the fact that $\chi_2(t) = 1$ (by property (P5)).

At last, when $d \equiv 1 \pmod 4$ we also need to prove the same result for the idèle b_2 whose local component equals $1 + \sqrt{-d}$ at the place $\mathfrak{p}_2$ and 1 at all other places. Then

$$\varepsilon_2(1+d) = \varepsilon_2\left(\frac{1+d}{2}\right)\cdot\prod_{p\in Q_{\pm\pm}}\varepsilon_p(2)^{-1}\cdot\varepsilon_t(2)^{-1}, \tag{33}$$

while

$$\chi(b_i^2) = \chi_2\left(\frac{(1+\sqrt{-d})^2}{2}\right)\prod_{p\in Q_{\pm\pm}}\varepsilon_p(2)^{-1}\delta_p(2)\cdot\chi_t(2)^{-1}. \tag{34}$$

Then we are led to prove that

$$\varepsilon_2\left(\frac{1+d}{2}\right)\varepsilon_t(2)^{-1} = \chi_2\left(\frac{(1+\sqrt{-d})^2}{2}\right)\prod_{p\in Q_{\pm\pm}}\delta_p(2)\cdot\chi_t(2)^{-1}.$$

Recall by Property (P1) that $\varepsilon_t(2)\chi_t(2) = \delta_t(2)^{1+v_t(d)}$. Also, the equality $\frac{(1+\sqrt{-d})^2}{2} = \frac{1-d}{2} + \sqrt{-d}$ implies that $\chi_2\left(\frac{(1+\sqrt{-d})^2}{2}\right) = \chi_2(\sqrt{-d}) = \delta_t(2)$ (by definition), so

$$\varepsilon_t(2)\chi_t(2)^{-1}\chi_2\left(\frac{(1+\sqrt{-d})^2}{2}\right) = \delta_t(2)^{v_t(d)}.$$

Regarding the other terms:

- If $d \equiv 1 \pmod 8$ then $\varepsilon_2\left(\frac{1+d}{2}\right) = 1$ and $\prod_{p\in Q_{\pm\pm}} \delta_p(2)\delta_t(2)^{v_t(d)} = 1$, hence the statement.
- If $d \equiv 5 \pmod 8$ then $\varepsilon_2\left(\frac{1+d}{2}\right) = -1$ and $\prod_{p\in Q_{\pm\pm}} \delta_p(2)\delta_t(2)^{v_t(d)} = -1$, hence the statement.

Now that we have a well defined character on the whole idèle group $\mathbb{I}_K$, we need to verify that the condition

$${}^\tau\chi = \chi \cdot (\psi_{-t} \circ \mathcal{N})$$

holds for the extension. Once again, it is enough to check the property at the idèles a_i in $\mathbb{I}_K$ with trivial infinite component and finite components:

$$(a_i)_{\mathfrak{p}} = \begin{cases} r_i & \text{if } \mathfrak{p} = \mathfrak{r}_i, \\ 1 & \text{otherwise.} \end{cases}$$

where the unramified prime ideals $\{\mathfrak{r}_i\}$ generate the class group and where r_i is the norm of $\mathfrak{r}_i$. The same computation of (22), (23) and (24) makes equation (25) becomes

$${}^\tau\chi(a_i) = \chi(a_i)^{-1}\chi\left(\frac{a_i\tau(a_i)}{r_i}\right) = \chi(a_i)\chi_2(r_i)^{-1}\chi_t(r_i)^{-1}\varepsilon_2(r_i)\varepsilon_t(r_i)\prod_{p\in Q_{\pm\pm}}\delta_p(r_i).$$

The fact that r_i splits in K implies that $\left(\frac{-d}{r_i}\right) = 1$ so quadratic reciprocity gives

$$1 = \left(\frac{2}{r_i}\right)^{v_2(d)}\left(\frac{t}{r_i}\right)^{v_t(d)}\left(\frac{-1}{r_i}\right)^{\#Q_{-+}+\#Q_{--}+1}\prod_{p\in Q_{\pm\pm}}\delta_p(r_i).$$

Since $\psi_{-t}(\mathcal{N}(a_i)) = \delta_t(r_i)$, we are left to verify that

$$\chi_2(r_i)^{-1}\chi_t(r_i)^{-1}\varepsilon_2(r_i)\varepsilon_t(r_i)\delta_{r_i}(2)^{v_2(d)}\delta_{r_i}(t)^{v_t(d)}\delta_{-1}(r_i)^{\#Q_{-+}+\#Q_{--}+1} = \delta_t(r_i),$$

which follows directly from (31) . □

Theorem 3.3 and its proof translates mutatis mutandis to the case $t \equiv 3 \pmod 4$ studied in this section, so in particular χ is unique up to a character of $\mathrm{Gal}_{\mathbb{Q}}$.

Remark 7. The precise conductor $\mathfrak{f}$ of $\chi_{\mathfrak{p}_2}$ has valuation:

$$v(\mathfrak{f}) = \begin{cases} 0 & \text{if } d \equiv 3 \pmod 4, \\ 2 & \text{if } d \equiv 1 \pmod 4 \text{ and } t \equiv 3 \pmod 8, \\ 0 & \text{if } d \equiv 1 \pmod 4 \text{ and } t \equiv 7 \pmod 8, \\ 5 & \text{if } 2 \mid d. \end{cases}$$

4. Extension and lowering the level

Recall that by Proposition 2.2 (respectively Proposition 2.3) the Galois conjugate of the elliptic curve $E_{(a,b,c)}$ (respectively $\widetilde{E}_{(a,b,c)}$) is isogenous to its quadratic twist by ψ_{-2} (respectively to its quadratic twist by ψ_{-3}). In particular if χ denotes the character constructed in Theorem 3.2 (respectively Theorem 3.7) then the twisted representation $\rho_{E_{(a,b,c)},p}\otimes\chi$ (respectively $\rho_{\widetilde{E}_{(a,b,c)},p}\otimes\chi$) is invariant under the action of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ so it should extend to a 2-dimensional Galois representation of $\mathrm{Gal}_{\mathbb{Q}}$. In this section we will prove that this is indeed the case and furthermore, compute the determinant and conductor of the extension. Let us state an important result on induced representations.

Theorem 4.1. *Let E/F be a finite extension of local fields, and let ρ be an n-dimensional representation of W_E. Then the conductor of the induced representation $\mathrm{Ind}_{W_E}^{W_F}$ equals*

$$v(\mathrm{cond}(\mathrm{Ind}_{W_E}^{W_F}\rho)) = n\delta(E/F) + f(E/F)v(\mathrm{cond}(\rho)), \tag{35}$$

where $\delta(E/F)$ denotes the valuation of the different of the extension and $f(E/F)$ the inertial degree.

Proof. See for example [Ser68], page 105 (after Proposition 4). □

4.1. **The case $\rho_{E_{(a,b,c)},p}$.** Let ε be the real character constructed in Section 3.1 and let $S(E_{(a,b,c)})$ be the set of odd primes of bad reduction of $E_{(a,b,c)}$ (where the curve has multiplicative reduction by Lemma 2.6). Abusing notation, we will say that a rational prime $q \in S(E_{(a,b,c)})$ if there exists a prime element of $S(E_{(a,b,c)})$ dividing q.

Theorem 4.2. *Suppose that $K/\mathbb{Q}$ is imaginary quadratic. Then the twisted representation $\rho_{E_{(a,b,c)},p} \otimes \chi$ extends to a 2-dimensional representation of $\mathrm{Gal}_{\mathbb{Q}}$ attached to a newform of weight 2, Nebentypus ε and level N given by*

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

The value of e is one of:

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

Furthermore, the coefficient field is a quadratic extension of $\mathbb{Q}(\chi)$.

Proof. As mentioned before, the existence of the extension was proved by Ribet in ([Rib04]). We give an alternative proof based on Galois representations (which is well known to experts) to get control on the level and conductor. If the elliptic curve $E_{(a,b,c)}$ has complex multiplication, then its j-invariant is a real number in K, hence rational. This implies that the curve is a quadratic twist of a rational elliptic curve, hence the existence of the extension is automatic. Assume then that $E_{(a,b,c)}$ does not have complex multiplication.

To ease notation, let ρ denote $\rho_{E_{(a,b,c)},p} \otimes \chi$. Its conductor divides $\mathrm{lcm}\{N(E_{(a,b,c)}), \mathrm{cond}(\chi)^2\}$ and its Nebentypus matches ε restricted to Gal_K (by the first claim of Theorem 3.2). Let τ be as in Theorem 3.2 (i.e. an element of $\mathrm{Gal}_{\mathbb{Q}}$ whose restriction to $\mathrm{Gal}(K/\mathbb{Q})$ is non-trivial) and suppose furthermore that it corresponds to complex conjugation (although this is not really necessary). It is enough to define the extension of ρ at τ and check the Nebentypus statement on it.

Recall that ${}^{\tau}\rho$ denotes the Galois representation defined on σ by ${}^{\tau}\rho(\sigma) = \rho(\tau\sigma\tau^{-1})$. By the third property of χ, ρ and ${}^{\tau}\rho$ are isomorphic (as they have the same trace at Frobenius elements). In particular, there exists $A \in \mathrm{GL}_2(\overline{\mathbb{Q}_p})$ such that ${}^{\tau}\rho = A\rho A^{-1}$. Furthermore, since ρ is irreducible (because $E_{(a,b,c)}$ does not have complex multiplication), Schur's lemma implies that the matrix A is unique up to a scalar. Since τ has order 2, the equality $\rho(\sigma) = {}^{\tau^2}\rho(\sigma) = A^2\rho(\sigma)A^{-2}$ implies that $A^2 = \lambda$ (a scalar matrix).

Suppose that there exists an extension $\tilde{\rho} : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$. Then for $\sigma \in \mathrm{Gal}_K$, $\tilde{\rho}(\tau\sigma\tau^{-1}) = \tilde{\rho}(\tau)\tilde{\rho}(\sigma)\tilde{\rho}(\tau)^{-1} = \tilde{\rho}(\tau)\rho(\sigma)\tilde{\rho}(\tau)^{-1}$ and the uniqueness of the matrix A implies that there exists a constant μ such that $\tilde{\rho}(\tau) = \mu A$. Since $\tilde{\rho}^2(\tau) = \rho(\tau^2) = 1$, $\mu^2 = \frac{1}{\lambda}$.

This suggests that we should define $\tilde{\rho}(\tau) = \frac{1}{\sqrt{\lambda}}A$ and it is easy to verify that this definition indeed gives an extension (the other choice of a square root gives the second possible extension; they differ by the twist by the character attached to the quadratic extension $K/\mathbb{Q}$). To determine the determinant of the extended representation $\tilde{\rho}$, note that $\det(\rho) = \varepsilon\chi_{\mathrm{cyc}}$ (where χ_{cyc} denotes the cyclotomic p-adic character) as a character of Gal_K, hence it is enough to check that they coincide in an element of $\mathrm{Gal}_{\mathbb{Q}}$ which is not in Gal_K (like τ). By Ribet's result, we know that any extension is odd, i.e. $\det(\tilde{\rho})(\tau) = -1$. But also $\varepsilon(\tau)\chi_{\mathrm{cyc}}(\tau) = -1$ (since ε is even) hence $\det(\tilde{\rho}) = \varepsilon\chi_{\mathrm{cyc}}$.

Modularity of the representation $\tilde{\rho}$ follows from Serre's conjectures ([KW09] and [KW10]), so we know it is attached to a modular form of weight 2 and Nebentypus ε; we need to compute the conductor of $\tilde{\rho}$ to

finish the proof. Let $\mathfrak{q}$ be an odd prime unramified in $K/\mathbb{Q}$. Then χ is unramified at $\mathfrak{q}$, so the conductor valuation of $\rho_{E_{(a,b,c)},p} \otimes \chi$ equals one for primes in $S(E_{(a,b,c)})$ and zero for the other ones. The validity of the second factor in the formula for N then follows from the fact that the conductor of a representation does not change while restricting it to the absolute Galois group of an unramified extension.

Let $\mathfrak{q}$ be an odd prime ramifying in $K/\mathbb{Q}$ and q be the rational prime it divides (which does not equal p). The local induced representation $\mathrm{Ind}_{\mathrm{Gal}_{K_\mathfrak{q}}}^{\mathrm{Gal}_{\mathbb{Q}_q}}(\rho_{E_{(a,b,c)},p}|_{\mathrm{Gal}_{K_\mathfrak{q}}} \otimes \chi_\mathfrak{q}) = \tilde{\rho}|_{\mathrm{Gal}_{K_\mathfrak{q}}} \oplus (\tilde{\rho}|_{\mathrm{Gal}_{K_\mathfrak{q}}} \otimes \mu_{K_\mathfrak{q}})$, where $\mu_{K_\mathfrak{q}}$ is the quadratic character of the local the extension $K_\mathfrak{q}/\mathbb{Q}_q$. Now we apply Theorem 4.1. By construction $\chi_\mathfrak{q}$ is unramified for $q \in Q_3$ and of conductor $\mathfrak{q}$ for $q \in Q_1 \cup Q_5 \cup Q_7$, hence the right hand side of (35) equals 2 for primes in Q_3 and 4 for primes in $Q_1 \cup Q_5 \cup Q_7$. Note that both $\tilde{\rho}$ and $\tilde{\rho} \otimes \mu$ have the same Nebentypus, hence they both must ramify at primes in Q_3 with conductor exponent 1. Since μ has conductor exponent 1 at q, twisting $\tilde{\rho}$ by μ cannot vary the conductor exponent from 1 to 3 (or from 0 to 4), hence at primes in $Q_1 \cup Q_5 \cup Q_7$ both $\tilde{\rho}$ and $\tilde{\rho} \otimes \mu$ have conductor exponent 2 as claimed.

The value of e equals the value of the conductor exponent of $\rho_{E_{(a,b,c)},p}$ when 2 is unramified; this gives the inert case result. Furthermore, in the split case (say $2 = \mathfrak{p}_2\overline{\mathfrak{p}}_2$) we can chose the local character $\chi_{\mathfrak{p}_2}$ so that the twist of $E_{(a,b,c)}$ by $\chi_{\mathfrak{p}_2}$ has split multiplicative reduction of conductor $\mathfrak{p}_2$ to get the statement.

If 2 ramifies in $K/\mathbb{Q}$ we use again formula (35). Note that if $d \not\equiv 1 \pmod 8$ then the value of the conductor of $\rho_{E_{(a,b,c)},p}$ at $\mathfrak{p}_2$ is larger than twice the value of the conductor of χ at $\mathfrak{p}_2$ (see Remark 6) so the formula follows easily from Lemma 2.8 noting that once again the conductor at 2 of $\tilde{\rho}$ matches that of $\tilde{\rho} \otimes \mu$. When $d \equiv 1 \pmod 8$, the local character $\chi_{\mathfrak{p}_2}$ corresponds to a tame extension (generated by the square root of $1 + \sqrt{-d}$ times a unit), so Lemma 2.9 implies that the twisted representation has conductor valuation 8 (when $b \equiv 1 \pmod 4$) or 6 (when $b \equiv 3 \pmod 4$) when b is odd and 12 when b is even. Since we can assume (changing b by $-b$) that $b \equiv 3 \pmod 4$ the result follows. □

Remark 8. The coefficient field can be computed as follows: if p is a prime inert in $K/\mathbb{Q}$ then $\mathrm{Tr}(\tilde{\rho}(\mathrm{Frob}_p))^2 = a_p(E_{(a,b,c)})\chi(\mathrm{Frob}_p) + 2\varepsilon(\mathrm{Frob}_p)p$, so it is enough to perform such computation for one inert prime of $K/\mathbb{Q}$.

Remark 9. If K is real quadratic the same proof gives an extension, but we cannot distinguish whether the Nebentypus equals ε or $\varepsilon\mu_K$. Our proof deeply used the fact that by Ribet's result, the extension is odd, but we do not get any information for real quadratic fields K, as complex conjugation is an element of Gal_K. In the forthcoming article ([PV22]) a completely different approach will be presented to solve this issue.

Let $\tilde{\rho}_p$ denote the extension of $\rho_{E_{(a,b,c)},p} \otimes \chi$, a modular representation of $\mathrm{Gal}_\mathbb{Q}$.

Corollary 4.3. *Suppose that $p \nmid 2d$ and suppose that the residual Galois representation $\overline{\tilde{\rho}_p}$ is absolutely irreducible. Then there exists a newform $g \in S_2(\Gamma_0(n), \varepsilon)$, where*

$$n = 2^e \cdot \prod_{q \in Q_3} q \cdot \prod_{q \in Q_1 \cup Q_5 \cup Q_7} q^2,$$

for e as in Theorem 4.2, such that $\rho_{E_{(a,b,c)},p} \equiv \rho_{g,K,p} \otimes \chi^{-1} \pmod{\mathfrak{p}}$, where $\rho_{g,K,p}$ is the restriction of the representation $\rho_{g,p}$ to the Galois group Gal_K and $\mathfrak{p}$ is a prime ideal of $\overline{\mathbb{Q}}$ dividing p.

Proof. Let $\mathfrak{q}$ be a prime ideal of $\mathcal{O}_K$ dividing $N(E_{(a,b,c)})$ but not dividing p. By Lemma 2.7 and by the well known Hellegouarch's result the residual representation $\overline{\rho_{E_{(a,b,c)},p}}$ is unramified at $\mathfrak{q}$. Since χ is unramified at $\mathfrak{q}$, the same holds for $\overline{\rho_{E_{(a,b,c)},p} \otimes \chi}$, and since $K/\mathbb{Q}$ is unramified at $\mathfrak{q}$, the image of inertia of $\overline{\tilde{\rho}_p}$ matches that of $\overline{\rho_{E_{(a,b,c)},p}}$. In particular, $\overline{\tilde{\rho}_p}$ is unramified at all primes not dividing $2dp$. The *finite* hypothesis (to remove p also from the level) at $\mathfrak{p}$ for primes $\mathfrak{p}$ dividing p follows from the same argument given in [Ell04] (page 783) under our assumption that p does not ramify in $K/\mathbb{Q}$. Our absolutely irreducible assumption implies that we are in the hypothesis of Ribet's lowering the level result (see [Rib90]) so there exists an eigenform $g \in S_2(\Gamma_0(n), \varepsilon)$ with n only divisible by ramified primes and probably by the prime two which is congruent to our representation $\tilde{\rho}_p$ modulo $\mathfrak{p}$ for some prime ideal $\mathfrak{p}$ dividing p. □

It is important to remark that the level, weight and Nebentypus of the newform g does not depend neither on the particular solution (a, b, c) nor on the prime p.

Proposition 4.4. *The extension of the trivial solutions $(\pm 1, 0, 1)$ corresponds to forms $g_\pm$ with complex multiplication in the space $S_2(\Gamma_0(n), \varepsilon)$ where $n = 2^8 \cdot \prod_{q \in Q_3} q \cdot \prod_{q \in Q_1 \cup Q_5 \cup Q_7} q^2$.*

Proof. By Lemma 2.10 and Remark 1 the conductor exponent of the elliptic curve with complex multiplication attached to the trivial solution $(\pm 1, 0, 1)$ equals 8 when 2 does not ramify in $K/\mathbb{Q}$, it equals 12 if $d \equiv 1 \pmod 4$ and 10 if $2 \mid 10$. In all cases, formula (35) implies that the extension has exponent valuation 8 at 2. □

4.2. **The case $\rho_{\widetilde{E}_{(a,b,c)},p}$.** As in the previous section, let ε be the real character constructed in Section 3.2 and let $S(\widetilde{E}_{(a,b,c)})$ be the set of odd primes different from 3 of bad reduction of $\widetilde{E}_{(a,b,c)}$. Abusing notation, if q is a rational prime, by $q \in S(\widetilde{E}_{(a,b,c)})$ we will mean that there exists a prime ideal of $\mathcal{O}_K$ dividing q in the set $S(\widetilde{E}_{(a,b,c)})$.

Before stating the result, let us make some remarks regarding the conductor of the twisted representation $\rho_{\widetilde{E}_{(a,b,c)},p} \otimes \chi$. Let $\mathfrak{q}$ be an odd prime ramifying in $K/\mathbb{Q}$ not dividing 3. The curve $\tilde{E}_{(a,b,c)}$ has additive reduction at all such primes and its local type (by Remark 2) is that of a principal series (given by a character whose inertial part has order 3) or a supercuspidal representation. Since the inertial part of $\chi_{\mathfrak{q}}$ has order a power of two, it cannot cancel the inertial contribution of $\rho_{\widetilde{E}_{(a,b,c)},p}$, hence the conductor of the twisted representation at $\mathfrak{q}$ has still valuation 2.

At primes dividing 2, the conductor valuation of $N(\widetilde{E}_{(a,b,c)})$ never matches the square of the conductor of $\chi_{\mathfrak{p}_2}$ (see Lemma 2.14 and Remark 7) hence the twisted representation has conductor the least common multiple of both quantities. At primes dividing 3 there is a situation where the twisted representation has smaller conductor than the elliptic curve. It happens precisely when 3 is inert in $K/\mathbb{Q}$ and $\tilde{E}_{(a,b,c)}$ has conductor valuation 2. In such case, the local type of the Weil-Deligne representation is that of a principal series whose inertia is given by an order 4 character (by Remark 3). Then twisting by χ_3 (also a character of order 4 while restricted to the inertia subgroup) cancels one of the characters and the twisted representation has conductor valuation 1.

Theorem 4.5. *Suppose that $K/\mathbb{Q}$ is imaginary quadratic. Then the twisted representation $\rho_{\tilde{E},p} \otimes \chi$ descends to a 2-dimensional representation of $\mathrm{Gal}_{\mathbb{Q}}$ attached to a newform g of weight 2, Nebentypus ε and level N given by*

$$N = 2^a \cdot 3^b \cdot \prod_{q \in S(\widetilde{E}_{(a,b,c)})} q \cdot \prod_{q \in Q_{\pm\pm}} q^2.$$

The value of a is one of:

$$a = \begin{cases} 2 & \text{if } 2 \text{ is inert,} \\ 1, 2 & \text{if } 2 \text{ splits,} \\ 4 & \text{if } 2 \text{ ramifies but } 2 \nmid d, \\ 8 & \text{if } 2 \mid d. \end{cases}$$

and the value of b is one of

$$b = \begin{cases} 2, 3 & \text{if } 3 \text{ is split,} \\ 1, 3 & \text{if } 3 \text{ is inert,} \\ 5 & \text{if } 3 \text{ ramifies.} \end{cases}$$

Furthermore, the coefficient field is some quadratic extension of $\mathbb{Q}(\chi)$.

Proof. The extension existence result and its Nebentypus description is proven exactly in the same way as in Theorem 4.2. The conductor result is clear for all odd unramified primes, since the curve has semistable reduction (by Lemma 2.11) and χ is unramified at such primes.

If $\mathfrak{q} \mid q$ is an odd ramified prime ideal not dividing 3, Lemma 2.16 implies that $v_{\mathfrak{q}}(\rho_{\widetilde{E}_{(a,b,c)},p}) = 2$. The same holds for $\rho_{\widetilde{E}_{(a,b,c)},p} \otimes \chi$ (as explained before). Then the conductor formula of the induced representation (35) implies that the four dimensional representation has conductor valuation 4 at such primes, so the extended representation has conductor valuation 2.

At the prime 2 the character χ_2 is unramified when 2 is unramified in $K/\mathbb{Q}$, hence the twisted representation (and its extension) has the same conductor as $\widetilde{E}_{(a,b,c)}$. If $d \equiv 1 \pmod 4$ then χ_2 has conductor 2, so the twisted representation has conductor valuation 4 and its induction conductor valuation 8, so $\tilde{\rho}_p$

has conductor valuation 4 at the prime 2. When $2 \mid d$, χ_2 has conductor 5, so the twisted representation valuation 10, the induced one 16 and $\tilde{\rho}_p$ has conductor valuation 8 as claimed.

At last we need to prove the exponent for the prime 3. If 3 ramifies in $K/\mathbb{Q}$, $v_{\mathfrak{p}_3}(N(\widetilde{E}_{(a,b,c)})) = 8$ (by Lemma 2.15) and the character has conductor valuation at most 1, so the induced representation has valuation 10 and $\tilde{\rho}_p$ has valuation 5. If 3 splits, the twisted representation has conductor exponent 2 or 3 (so does $\tilde{\rho}_p$), while in the inert case, as explained before, the twisted representation has conductor valuation 1 or 3. □

Let $\tilde{\rho}_p$ denote the extension of $\rho_{\widetilde{E}_{(a,b,c)},p} \otimes \chi$.

Corollary 4.6. *Suppose that $p \nmid 6d$ and suppose that the residual Galois representation $\overline{\tilde{\rho}_p}$ is absolutely irreducible. Then there exists a newform $g \in S_2(\Gamma_0(n), \varepsilon)$, where*

$$n = 2^a \cdot 3^b \cdot \prod_{q \in Q_{\pm\pm}} q^2,$$

for a and b as in Theorem 4.5 such that $\rho_{\widetilde{E}_{(a,b,c)},p} \equiv \rho_{g,K,p} \otimes \chi^{-1} \pmod{\mathfrak{p}}$, where $\rho_{g,K,p}$ is the restriction of the representation $\rho_{g,p}$ to the Galois group Gal_K and $\mathfrak{p}$ is a prime ideal of $\overline{\mathbb{Q}}$ dividing p.

Proof. Mimics the one of Corollary 4.3. □

We can give a precise formula for the level of the form attached to the trivial solution $(\pm 1, 0, 1)$.

Proposition 4.7. *The extension of the trivial solutions $(\pm 1, 0, 1)$ correspond to forms $g_\pm$ with complex multiplication in the space $S_2(\Gamma_0(n), \varepsilon)$ where $n = 2^a \cdot 3^b \cdot \prod_{q \in Q_{\pm\pm}} q^2$, with*

$$a = \begin{cases} 2 & \text{if } d \equiv 3 \pmod 4, \\ 4 & \text{if } d \equiv 1 \pmod 4, \\ 8 & \text{if } 2 \mid d. \end{cases}$$

and with

$$b = \begin{cases} 3 & \text{if } 3 \nmid d, \\ 5 & \text{if } 3 \mid d. \end{cases}$$

Proof. Follows the same proof of Theorem 4.5 with the precise formula for the conductor exponent of $\tilde{E}_{(\pm 1,0,1)}$ given in Remark 4. □

5. Irreducibility of the residual representations of $\rho_{E_{(a,b,c)},p}$ and of $\rho_{\widetilde{E}_{(a,b,c)},p}$

To use Ribet's level lowering result we need to assure that the residual representation $\overline{\tilde{\rho}_p}$ is absolutely irreducible. Ellenberg's result on the image of Galois representations attached to $\mathbb{Q}$-curves ([Ell04]) is very useful for this purpose as it not only provides irreducibility but also implies large image of the residual representation (i.e. $\mathrm{SL}_2(\mathbb{F}_p)$ is contained in the image of the residual projective representation). This plays a crucial role while trying to discard forms with complex multiplication (a major problem that will be addressed later). Ellenberg's theorem holds under the hypothesis that there exists of a prime $\mathfrak{q}$, not dividing 6, where the $\mathbb{Q}$-curve has multiplicative reduction. Recall from Lemma 2.6 (respectively Lemma 2.11) that $E_{(a,b,c)}$ (respectively $\widetilde{E}_{(a,b,c)}$) has multiplicative reduction at all primes q larger than 2 (respectively 3) dividing c.

Then we are led to distinguish between two different cases: namely when c is supported only at the primes $\{2, 3\}$ (i.e. 2 and 3 are the unique primes in its factorization) where Ellenberg's result does not apply, and when c is divisible by a prime larger than 3.

When c is only supported at $\{2, 3\}$, the value of the level N belongs to a finite list, hence we can compute all such spaces and try to discard their forms for not being related to putative solutions. This is precisely the strategy we follow while studying equation (3). However, the prime 3 does not play any special role while studying solutions of (2), hence if (a, b, c) is a non-trivial primitive solution of it, and $3 \mid c$, then we are in the hypothesis of Ribet's lowering the level result. A crucial hypothesis in Ribet's theorem is that the residual image is absolutely irreducible, hence we need a different approach to achieve such a goal.

5.1. **The case c supported in $\{2,3\}$.** The results of the present subsection will only be applied while studying solutions of equation (2). Suppose that the unique possible primes dividing c are 2 and 3. Recall that c being divisible by 2 (respectively by 3) implies that $d \equiv 7 \pmod 8$ (respectively $d \equiv 2 \pmod 3$) by Lemma 2.4.

Theorem 5.1. *There exists an explicit bound N_K such that if $p > N_K$ and (a,b,c) is a primitive solution of (2) where c is only supported in $\{2,3\}$, then the representation $\rho_{E_{(a,b,c)},p}$ has absolutely irreducible image.*

Proof. The proof mimics the one presented in [DU09] (case (ii)). Suppose that $c = 2^\alpha 3^\beta$ so the curve $E_{(a,b,c)}$ has conductor $2^a \cdot 3^b$, where $a \leq 12$, $b \leq 1$ (by Lemma 2.8). Let $\epsilon_3 = 1$ if $3 \mid c$ and 0 otherwise. Then $N(\tilde{\rho}) = 2^s 3^{\epsilon_3} \cdot \prod_{q \in Q_3} q \cdot \prod_{q \in Q_1 \cup Q_5 \cup Q_7} q^2$, where $s \leq 9$ by Theorem 4.2. Suppose that the residual image of $\tilde{\rho}_p$ is reducible, i.e.

$$\overline{\tilde{\rho}_p}^{s.s} \simeq \nu \oplus \varepsilon \nu^{-1} \overline{\chi_{\text{cyc}}}, \tag{36}$$

where as before χ_{cyc} denotes the p-adic cyclotomic character. In particular, since the conductor of the reduced representation divides the conductor of $\tilde{\rho}$, $\text{cond}(\nu) \mid N(\tilde{\rho})$. Let ℓ be a prime number such that $\ell \equiv 1 \pmod{\text{lcm}(4d, \text{cond}(\nu))}$. In particular, ℓ splits in $K/\mathbb{Q}$, say $\ell = \mathfrak{l}\bar{\mathfrak{l}}$. Then on the one hand $\text{Tr}(\tilde{\rho}_p(\text{Frob}_\ell)) = a_\mathfrak{l}(E_{(a,b,c)})\chi(\mathfrak{l})$ is an integer (as the form has an inner twist) and by Hasse's bound it satisfies that $|a_\mathfrak{l}(E_{(a,b,c)})| \leq 2\sqrt{\ell}$. On the other hand, (36) and our assumption on ℓ implies that $\text{Tr}(\overline{\tilde{\rho}_p}^{s.s}(\text{Frob}_\ell)) = \ell + 1$. In particular, $p \mid \ell + 1 - a_\mathfrak{l}(E_{(a,b,c)})\chi(\mathfrak{l})$ (which is non-zero), which cannot occur if $p > 2\sqrt{\ell} + \ell + 1$. □

Remark 10. The constant N_K depends on the first prime congruent to 1 modulo $\text{lcm}(4d, N(\tilde{\rho}))$. We can improve the bound for the conductor of ν in the previous theorem. From (36) it follows that actually $\text{cond}(\nu) \cdot \text{cond}(\nu^{-1}\varepsilon) \mid N(\tilde{\rho})$. If $3 \mid c$ then ε is unramified at 3, and $\tilde{\rho}$ has conductor exponent one at 3, then $3 \nmid \text{cond}(\nu)$. For odd ramified primes q, since the conductor of ε is square-free, $v_q(\text{cond}(\nu)) \leq 1$. Then if $\tilde{d} = \frac{d}{2^{v_2(d)}}$ (i.e. the prime to 2 part of d) actually $\text{cond}(\nu) \mid 2^4 \cdot \tilde{d}$, so we can replace the least common multiple by $16\tilde{d}$.

Regarding the least minimum prime number ℓ congruent to 1 modulo $16\tilde{d}$, according to Dirichlet's theorem, $1/\varphi(16\tilde{d})$-th of the primes are congruent to 1 modulo $16\tilde{d}$, but giving a precise bound on the first such prime is very ineffective for computational purposes.

5.2. **The case c not supported in $\{2,3\}$.** Assume on the contrary that there exists an odd prime q dividing c and not dividing 3 (so in particular $q \nmid d$). Then we are in the hypothesis of Ellenberg's big image result ([Ell04, Theorem 3.14]).

Theorem 5.2 (Ellenberg)**.** *Given d a positive integer, suppose that $E/\mathbb{Q}(\sqrt{-d})$ is a $\mathbb{Q}$-curve with square-free degree which has multiplicative reduction at an odd prime $\mathfrak{q}$ not dividing 3. Then, there exists an integer N_d such that the projective image of the residual representation of $\rho_{E,p}$ is surjective for all primes $p > N_d$ not dividing the degree of E. Furthermore, some explicit values of N_d are the following: $N_1 = 149$, $N_2 = 257$, $N_3 = 7$, $N_5 = 547$, $N_6 = 599$ and $N_7 = 283$.*

Proof. This result was proved in [Ell04], where a method to bound N_d was given. The explicit value of N_d was given in: [BEN10] for $d = 1$ and $d = 2$ and in [DU09] for all values of d whose field conductor is at most 8 (with an improvement via a finite computation given in [Kou20] for $d = 3$).

Let N be any positive integer, and χ the character corresponding to $K/\mathbb{Q}$ (of conductor $\mathfrak{f}$). Let $\mathcal{F}$ be a Petersson-orthogonal basis for $S_2(\Gamma_0(N))$. Define

$$(a_m, L_\chi)_N = \sum_{f \in \mathcal{F}} a_m(f) L(f \otimes \chi, 1).$$

If $M \mid N$, define $(a_m, L_\chi)_N^M$ as the contribution from the old forms of level M. Then one of the main results of Ellenberg in [Ell04] is that if for some prime p the value

$$(a_1, L_\chi)_{p^2}^{p-\text{new}} = (a_1, L_\chi)_{p^2} - p(p^2-1)^{-1}(a_1 - p^{-1}\chi(p)a_p, L_\chi)_p \tag{37}$$

is non-zero, the residual image for the prime p is large. Also in the aforementioned article, lower bounds for $(a_1, L_\chi)_{p^2}^{p-\text{new}}$ are presented, where the main contribution comes from the first term. In [Ell05] (Theorem 1) the following formula is proven

$$(a_m, L_\chi)_{p^2} = 4\pi\chi(m)e^{-2\pi m/\sigma N log(N)} - E^{(3)} + E_3 - E_2 - E_1 + (a_m, B(\sigma N \log(N))),$$

where σ is taken to be $\frac{q^2}{2\pi}$ and $N = p^2$. Theorem 1 of [Ell05] provides the following bounds (note that the first bound is not the one given in Ellenberg's article due to a mistake, whose errata is given in Appendix A):

- $|(a_m, B(\sigma N \log(N)))| \leq 2(4\pi\zeta^2(3/2)+1)(400/399)^3 exp(2\pi) q^2 m^{3/2} N^{-1/2} d(N) N^{-2\pi\sigma/q^2}$, where $d(N)$ denote the number of divisors of N.
- $|E_1| \leq (16/3)\pi^3 m^{3/2}\sigma \log(N) \exp(-N/2\pi m\sigma \log(N))$.
- $|E_3| \leq (8/3)\zeta(3/2)^2\pi^3\sigma m^{3/2} N^{-1/2} \log(N) d(N) \exp(-N/2\pi m\sigma \log(N))$.
- $|E^{(3)}| \leq 16\pi^3 m \sum_{c>0, N|c} \min\{\frac{2}{\pi}\phi(q)c^{-1}\log(c), \frac{1}{6}\sigma N \log(N) m^{1/2} c^{-3/2} d(c)\}$, where ϕ is Euler's function.

Also the following bounds hold:

- If the field discriminant is even, then by Proposition 10 of [BEN10]

$$|E_2| \leq 64q\phi(q)\pi^5 m^2 \left(\frac{\zeta(2)}{6}/N^2 + \frac{1}{\pi}\left(\zeta(3) log\left(\frac{eN}{2}\right)\right) - \zeta'(3)N^{-3}\right)$$
$$+ 32\pi^5\zeta(7/2)^2 m^{5/2} d(N) N^{-7/2}\left((\frac{N^2}{4\pi^2 m}+1)(1-\theta)^{-1} + (1-\theta)^{-2}\right)\exp(-\frac{N}{2\pi\sigma m\log(N)})$$
$$+ \frac{512}{3}\zeta(11/2)^2\pi^7 m^{7/2} d(N) N^{-11/2}(1-\theta^2)^{-3},$$

  where $x = \sigma N \log(N)$ and $\theta = \exp(-2\pi/x)$. Otherwise, by [Ell05, Theorem 1],

$$|E_2| \leq \frac{8}{9}\pi^5\zeta(7/2)^2 m^{5/2}\sigma^2 N^{-3/2}\log^2(N).$$

- By Lemma 3.13 of [Ell04], for $t = 1$ or $t = p$,

$$(a_{mt}, L_\chi)_p \leq 2\sqrt{3} m^{1/2} d(m)(1 - \exp(-2\pi/q\sqrt{p}))^{-1}(4\pi + 16\zeta^2(3/2)\pi^2 p^{-3/2}).$$

We wrote a script in `PARI/GP` to compute the bound for $(a_1, L_\chi)_{p^2}^{p-\text{new}}$ using the previous bounds. The function depends on a parameter M which is used to compute the bound for $E^{(3)}$. Its role is to take the first function of the minimum for all values of c up to MN and the second one for the rest of them. We want to stress that the cited bounds for $d = 1, 2, 3$ depend on Ellenberg's bound, so a priori need to be modified to include the correct bound for $|(a_m, B(\sigma N \log(N)))|$. The correct value for the constants is proved by our script:

```
? EllenbergBound(151,4,151^2*100)
% 1 = 0.032478298538855530962882830523012352630

? EllenbergBound(263,8,263^2*100)
% 2 = 0.351802535488606812024212716661688659 21

? EllenbergBound(137,3,137^2*8)
%3 = 0.509627960014380441051639880970309645 46

? EllenbergBound(557,20,557^2*800)
% 4 = 0.817022044815589750153045114815004510 44

? EllenbergBound(601,24,601^2*1000)

% 5 = 0.009930957916559737365975635414997018 7577
```

```
? EllenbergBound(293,7,293^2*20)
% 6 = 0.47805180308864650586682498409454832948
```

Since the output is positive, we can take $N_1 = 149$, $N_2 = 257$, $N_3 = 131$, $N_5 = 547$, $N_6 = 599$ and $N_7 = 283$. With our bound for N_3, the proof given in [Kou20] to reduce the bound N_3 to 7 (via a finite computation) holds. □

Remark 11. In [BEN10] a better bound for N_1 and N_2 was obtained via a delicate improvement of [Ell05]. The proof relies on the bound for $|(a_m, B(\sigma N \log(N)))|$. It is quite plausible that the same result holds, but we did not verify how the new bound affects their computations.

6. Strategies to discard newforms

We need to prove that the newforms in the space $S_2(\Gamma_0(n), \varepsilon)$ obtained from Corollary 4.3, while studying equation (2), and Corollary 4.6, while studying equation (3), are not related to non-trivial primitive solutions. To discard newforms we will mostly use a strategy due to Mazur (which in practice works better for forms without complex multiplication).

Proposition 6.1 (Mazur's trick)**.** *Let (a, b, c) be a non-trivial primitive solution, and $g \in S_2(\Gamma_0(n), \varepsilon)$ be such that $\overline{\rho_{E_{(a,b,c)},p} \otimes \chi} \simeq \overline{\rho_{g,K,p}}$. Let q be a rational prime with $q \nmid pn$. Let $\mathfrak{q}$ be a prime of $\mathcal{O}_K$ dividing q and define*

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

Then $p \mid B(q, g; a, b)$.

Proof. If h is a rational newform in $S_2(\Gamma_0(n), \varepsilon)$ and K is a quadratic field, recall the well known formula for the Fourier coefficients of the modular form H obtained as the automorphic base change of h to K: if $q = \mathfrak{q}\overline{\mathfrak{q}}$ (is split) then $a_{\mathfrak{q}}(H) = a_q(h)$, while if q is inert in K then $a_q(H) = a_q(g)^2 - 2q\varepsilon(q)$.

Taking $h = g$ gives the first two statements. The last one corresponds to "Ribet's lowering the level" condition. The proof of this fact (well known to experts) mimics the one given in [BC12, Lemma 24]. □

The way we apply the last proposition is as follows: take an odd prime q not dividing d, and define

$$C(q, g) = \prod_{(a,b) \in \mathbb{F}_q^2} B(q, g; a, b),$$

where the product is over non-zero elements satisfying equation (2) modulo q. Then the prime p must divide all the values $C(q, g)$, so we compute a couple of them and compute their gcd obtaining in some cases a bound for p. However, it happens sometimes that the value $C(q, g)$ is always zero, in which case we cannot discard the newform g for any prime p. A similar strategy holds while studying solutions of (3), using the curve $\widetilde{E}_{(a,b,c)}$.

Recall that the trivial solutions $(\pm 1, 0, 1)$ correspond to newforms $g_\pm$ with complex multiplication. Since they are solutions for all values of p, Proposition 6.1 implies that $p \mid C(q, g_\pm)$ for all primes p, so $C(q, g_\pm) = 0$. In particular, a safe check of any implementation of Mazur's trick should fail to discard such forms with complex multiplication.

Modular forms with complex multiplication however have the property that the image of their Galois representations are not as large as expected (their image lies in the normalizer of a Cartan group, since they are the induction of a one dimensional representation from an index two subgroup of $\mathrm{Gal}_{\mathbb{Q}}$). In particular, if we can prove that given a non-trivial primitive solution (a, b, c) there exists a prime $q > 3$ dividing c then Ellenberg's large image result (Theorem 5.2) implies that our representation $\tilde{\rho}_p$ has surjective projective image for p large enough, hence cannot be congruent to a newform with complex multiplication and we have good chances to prove non-existence of non-trivial primitive solutions.

Problem 2: how can we discard newforms with complex multiplication when c is supported at $\{2, 3\}$?

This is a very delicate problem, and at the time, we do not know of a general answer to it. However, for the examples of the present article some naive ideas are enough to get results.

By Lemma 2.4, if $d \not\equiv 7 \pmod 8$ then c cannot be even. If $d \equiv 7 \pmod 8$ then either $2 \mid ab$, in which case c is odd, or $2 \nmid ab$, in which case c is even. Recall that when $d \equiv 7 \pmod 8$, there are two possible conductor exponent values at the prime 2 (depending on the parity of ab). Then in the space corresponding to solutions where ab is even (where our trivial solution lies), we know that c is odd, so we have good chances that it is divisible by a prime larger than 3 (as c cannot be 1) and we can discard the newforms with complex multiplication as they are not related to non-trivial primitive solutions by Ellenberg's result. In the other space, there is a priori no reason for Mazur's trick to fail. This is precisely the case when we study equation (2) for $d = 7$. The same phenomena occurs while studying non-trivial primitive solutions (a, b, c) of equation (3) with c divisible by 3.

For this strategy to work completely while studying equation (2), we need to rule out the possibility of c being a power of 3 (so in particular $d \equiv 2 \pmod 3$). Suppose then that (a, b, c) is a non-trivial primitive solution of (2) with c divisible by 3. Then the modular form f (attached to the extension of $\rho_{E_{(a,b,c)},p} \otimes \chi$ by Theorem 4.2) has level divisible by 3 and is congruent to a form g whose level is not. In particular, we are in the "lowering the level" hypothesis at 3, hence

$$N(\varepsilon^{-1}(3)(3+1)^2 - a_3(g)^2) \equiv 0 \pmod p. \tag{38}$$

In practice, this gives a bound for the possible exponents p where a solution supported at $\{3\}$ can exist.

7. Solutions of equation $x^4 + dy^2 = z^p$ for small values of d

In the present section we study solutions of (2) for square-free values of d up to ten. For that purpose we follow the general strategy described in Section 1. The algorithms used for the following examples are available at the web page http://sweet.ua.pt/apacetti/research.html as well as the outputs of the computations (in a file labeled *"OutputsEq1.txt"*).

7.0.1. *The equation $x^4 + dy^2 = z^p$, for $d = 1, 2, 3$.* For $d = 1, 2$ the equation was completely solved in [BEN10], where the authors proved that there are no non-trivial primitive solutions for $p > 2$. For $d = 3$, in [DU09, Theorem 3] it was proved the non existence of non-trivial primitive solutions for $p > 131$. The bound 131 comes from Ellemberg's bound (see Lemma 8 of *loc.cit*), but applying [Kou20, Proposition 5.4] it can be lowered to 7, proving non existence of non-trivial primitive solutions for $p > 17$.

7.0.2. *The equation $x^4 + 5y^2 = z^p$.* This equation was not considered before, and our method gives the following result.

Theorem 7.1. *Let $p > 499$ be a prime number. Then there are no non-trivial primitive solutions of the equation*

$$x^4 + 5y^2 = z^p.$$

Proof. Theorem 4.2 implies that ε is a character of order 4 and conductor $4 \cdot 5$ while χ has order 8. Let (a, b, c) be a non-trivial primitive solution. Since $d \not\equiv 7 \pmod 8$, c cannot be even, so either c is a power of 3, or it is divisible by a prime larger than 3. In the later case, Theorem 5.2 implies that $N_d = 499$ so if $p > 499$ the image is large (in particular absolutely irreducible). If c is a power of three, we can use Theorem 5.1 (and Remark 10) with the prime $\ell = 241$ giving the bound $N_K = 273$. In particular, if $p > 499$ we are in the lowering the level hypothesis, hence by Corollary 4.3 there exists a newform g in $S_2(\Gamma_0(2^7 \cdot 5^2), \varepsilon)$ or in $S_2(\Gamma_0(2^8 \cdot 5^2), \varepsilon)$. whose Galois representation is congruent modulo p to $E_{(a,b,c)} \otimes \chi$.

- The space $S_2(\Gamma_0(2^7 \cdot 5^2), \varepsilon)$ has 12 Galois conjugacy classes (of newforms), none of them with complex multiplication. Using Mazur's trick for primes $3 \leq q \leq 30$ different from 5 and every g in the space we conclude that $p \in \{2, 7, 13\}$.
- The space $S_2(\Gamma_0(2^8 \cdot 5^2), \varepsilon)$ has 55 Galois conjugacy classes, 24 of them with complex multiplication (one of them corresponding to the trivial solution by Proposition 4.4). Applying Mazur's trick for primes $3 \leq q \leq 20$ different from 5 to forms without complex multiplication we conclude that $p \in \{2, 3, 5, 7, 11\}$. If c is divisible by a prime larger than 3 then Ellenberg's result implies that our form cannot be congruent to a newform with complex multiplication. If c is a power of 3, then the forms with complex multiplication should satisfy the raising the level hypothesis, i.e. that $p \mid N(16\varepsilon^{-1}(3) - a_3(g)^2)$. This implies that $p \in \{2, 3, 5, 29, 101, 139\}$. □

Here is how our script works: in Magma just load the file "*Eq1d5.mg*" to get the previous statements.

```
> load "Eq1d5.mg";
Loading "Eq1d5.mg"
Loading "Mazur42p.mg"
Forms in Space 2^7*5^2:
Forms with CM:
[]
Primes obtained via Mazur's trick for non-CM forms:
{@ 2 @}
{@ 2 @}
{@ 2 @}
{@ 2 @}
{@ 2, 7 @}
{@ 2, 7 @}
{@ 2, 7 @}
{@ 2, 7 @}
{@ 13 @}
{@ 13 @}
{@ 13 @}
{@ 13 @}
Forms in Space 2^8*5^2:
Forms with CM:
[ 1, 2, 3, 4, 5, 6, 7, 8, 13, 14, 17, 18, 21, 22, 23, 24, 29, 30, 31, 32, 33,
34, 44, 45 ]
Primes obtained via Mazur's trick for non-CM forms:
{@ 11, 2, 7 @}
{@ 11, 2, 7 @}
{@ 11, 2, 7 @}
{@ 11, 2, 7 @}
{@ 2, 7 @}
{@ 2, 7 @}
{@ 2, 7 @}
{@ 2, 7 @}
{@ 7 @}
{@ 7 @}
{@ 7 @}
{@ 7 @}
{@ 3 @}
{@ 3 @}
{@ 2, 3 @}
{@ 2, 3 @}
{@ 3, 7 @}
{@ 3, 7 @}
{@ @}
{@ @}
{@ 2, 3, 5, 7 @}
{@ 2 @}
{@ 2 @}
{@ 2 @}
{@ 2 @}
{@ 3 @}
{@ 3 @}
{@ 3 @}
{@ 3 @}
{@ 2, 5 @}
{@ 2, 5 @}
Primes obtained via Mazur's trick for CM forms:
{@ 2 @}
{@ 2 @}
{@ 2 @}
{@ 2 @}
{@ 2 @}
{@ 2 @}
```

```
{@ 2 @}
{@ 2 @}
{@ 2, 3 @}
{@ 2, 3 @}
{@ 2, 3 @}
{@ 2, 3 @}
{@ 2, 5 @}
{@ 2, 5 @}
{@ 2 @}
{@ 2 @}
{@ 3, 139 @}
{@ 3, 139 @}
{@ 3, 139 @}
{@ 3, 139 @}
{@ 2, 29 @}
{@ 2, 29 @}
{@ 5, 101 @}
{@ 5, 101 @}
```

7.0.3. *The equation $x^4 + 6y^2 = z^p$.* In this case we can prove the following result.

Theorem 7.2. *Let $p > 563$ be a prime number. Then there are no non-trivial primitive solutions of the equation*

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

Proof. Note that since $6 \mid d$, the c-value of a non-trivial primitive solution (a, b, c) cannot be supported in $\{2, 3\}$, so in this case we always get large image for $p > 563$ (by Theorem 5.2). Theorem 4.2 implies that ε is a character of conductor $4 \cdot 3$ and order 2 whereas χ has order 4. Corollary 4.3 implies the existence of a newform g attached to a non-trivial primitive solution (a, b, c) lying in one of $S_2(\Gamma_0(2^8 \cdot 3), \varepsilon)$ or $S_2(\Gamma_0(2^9 \cdot 3), \varepsilon)$ congruent modulo p to $\rho_{E_{(a,b,c)},p} \otimes \chi$.

• The space $S_2(\Gamma_0(2^8 \cdot 3), \varepsilon)$ has 10 Galois conjugacy classes. Six of them have complex multiplication (one of them corresponding to the trivial solution by Proposition 4.4). Running Mazur's trick for $q = 5$ and $q = 7$ for each non-CM form we conclude that $p \in \{2, 7\}$.

• The space $S_2(\Gamma_0(2^9 \cdot 3), \varepsilon)$ has 13 Galois conjugacy classes, three of them with complex multiplication. Applying Mazur's trick for primes $5 \leq q \leq 20$ to each non-CM form we conclude that $p \in \{2, 5, 7\}$. □

Remark 12. If Ellenberg's constant in Theorem 5.2 could be improved to 11 (as we expect), the previous result would hold for $p > 11$ as well.

7.0.4. *The equation $x^4 + 7y^2 = z^p$.* Our method allows to prove the following result.

Theorem 7.3. *Let $p > 349$ be a prime number. Then there are no non-trivial primitive solutions of the equation*

$$x^4 + 7y^2 = z^p.$$

Proof. Let (a, b, c) be a non-trivial primitive solution. Since $7 \equiv 1 \pmod 3$ we deduce that c cannot be divisible by 3, but it could be a power of 2, so to get absolutely irreducible image we need to use Theorem 5.1. Remark 10 implies we can use Theorem 5.1 with $\ell = 113$ getting absolutely irreducible image for all primes $p \geq 127$. If c is divisible by a prime larger than 3 then the image is large for all primes $p > 349$ (by Theorem 5.2).

Theorem 4.2 implies that ε is trivial while the character χ is the quadratic even character of conductor $7 \cdot 8$. Corollary 4.3 implies the existence of a newform g in $S_2(\Gamma_0(2 \cdot 7^2))$ or $S_2(\Gamma_0(2^8 \cdot 7^2))$ congruent to $\rho_{E_{(a,b,c)},p} \otimes \chi$ modulo p.

Let us give two different ways to discard the forms in the first space. If $g \in S_2(\Gamma_0(2 \cdot 7^2))$ is a newform (candidate for a primitive solution) its base change to K gives a Bianchi modular form whose twist by χ^{-1} must correspond to a Bianchi modular form of level $(\frac{1+\sqrt{-7}}{2})^6 \cdot (\frac{1-\sqrt{-7}}{2})$. Such space can easily be computed (using

Cremona's algorithm [Cre84], available at https://github.com/JohnCremona/bianchi-progs/releases/tag/v20200713) the result being also available at the lmfdb ([LMF22]). There are two forms whose level has norm 128, given by 2.0.7.1-128.4 and 2.0.7.1-128.5, whose level equals $(\frac{1+\sqrt{-7}}{2})^3(\frac{1-\sqrt{-7}}{2})^4$ and its Galois conjugate, so none comes from a primitive solution of our equation.

• The space $S_2(\Gamma_0(2\cdot 7^2))$ has 2 Galois conjugacy classes, one of them has rational coefficients (corresponding to an elliptic curve) and the other with coefficients in the quadratic extension corresponding to the polynomial x^2-2x-7. None of them have complex multiplication. Mazur's trick for primes $3\leq q\leq 50$ different from 7 discards the rational form if p is not in $\{2,7,17\}$. The second form cannot be discarded using Mazur's trick. Since it does not appear in the space of Bianchi modular forms, its local type at 7 must not be the correct one (so the twist by χ^{-1} of its base change to K is ramified at $\sqrt{-7}$). Actually, `Magma` can compute such local type, giving that the local component is indeed supercuspidal, induced from an order 8 character of the unramified quadratic extension of $\mathbb{Q}_7$. Such local type does not match the one of our elliptic curve (induced from an order 4 character of the same extension), hence they cannot be congruent.

• The space $S_2(\Gamma_0(2^8\cdot 7^2))$ has 98 Galois conjugacy classes, 17 of them with rational coefficients and 30 forms with complex multiplication (one of them corresponding to the trivial solution by Proposition 4.4). Mazur's trick (for primes $3\leq q\leq 20$ different from 7) allows us to eliminate the for forms without complex multiplication when p is not in the set $\{2,3,5,7,11,17,23,27,31\}$. □

8. Solutions of equation $x^2+dy^6=z^p$ for small values of d

As in the last section, we apply the general strategy to study solutions of the equation $x^4+dy^2=z^p$ for square-free values of d up to ten. To avoid false expectations, we want to point out that our approach does not provide any result for $d=5,7$, and we will explain what goes wrong in these particular cases (see [GPV21] for partial solutions). The outputs can be founded in *"OutputsEq2.txt"*.

8.0.1. *The equation $x^2+y^6=z^p$.* This case was considered in [BC12].

8.0.2. *The equation $x^2+2y^6=z^p$.* This case is very interesting, as working with Bianchi modular forms is enough to get the following result.

Theorem 8.1. *Let $p>5$ be a prime number. Then there are no non-trivial primitive solutions of the equation*

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

Proof. Following the notation of Section 3.2, the sets $Q_{\pm,\pm}$ are all empty; ε is the trivial character (i.e. the form g does not have Nebentypus) while the character χ corresponds to the quadratic character δ_3 at one of the primes dividing 3 in $\mathbb{Q}(\sqrt{-2})$ and does not ramify at any other prime. This is a very interesting example, as the curve $\tilde{E}_{(a,b,c)}$ has always good reduction at 2 and the 3-part of the conductor equals $3(1+\sqrt{-2})$, $3(1-\sqrt{-2})$, 9 or 27. In particular, it is more efficient to work with Bianchi modular forms than with rational ones (to avoid high powers of 2 in the level). The newform g attached to a primitive solution satisfies that its base extension to K and its twist by χ^{-1} (which equals χ as it is quadratic) gets only bad reduction at primes dividing 3. Computing the respective spaces (using Cremona's algorithm, although such spaces are also available at [LMF22]) it turns out that there are no Bianchi modular forms at any level but 3^3.

Let (a,b,c) be a non-trivial primitive solution. If c is divisible by 3, then the proof of Lemma 2.15 implies that our curve has conductor exponent 2 at one prime dividing 3 and 1 at the other. However the space of Bianchi modular forms of such a level is the zero space, hence 3 cannot divide c and c must be divisible by a prime larger than 3, so we are in the hypothesis of Ellenberg's large image result.

The space of Bianchi modular forms of weight 2 and level 3^3 contains three newforms corresponding to the elliptic curves 2.0.8.1-729.4-a1, 2.0.8.1-729.4-b1 and 2.0.8.1-729.4-c1. The second curve has complex multiplication and is the base change of a rational elliptic curve (it corresponds to the trivial solution, and cannot be congruent to $\tilde{E}_{(a,b,c)}$ if $p>5$ by Theorem 5.2). The other two ones (complex conjugate of each other) satisfy that $a_5=-1$. It is easy to compute for each possible value of (a,b) modulo 5 the value of $a_5(\tilde{E}_{(a,b,c)})$ and verify it belongs to the set $\{2,-7,-10\}$ hence both elliptic curves cannot be congruent to an elliptic curve coming from a non-trivial primitive solution if $p>5$. □

8.0.3. *The equation* $x^2+3y^6=z^p$. This case was considered in [Kou20].

8.0.4. *The equation* $x^2+5y^6=z^p$. Following our general strategy, the only non-empty set is $Q_{+-}=\{5\}$ so the character ε has conductor $4\cdot 5$, and its local component at 5 has order 4. In particular χ has order 8. Corollary 4.6 implies that we need to compute the spaces $S_2(\Gamma_0(2^4\cdot 3^2\cdot 5^2),\varepsilon)$ and $S_2(\Gamma_0(2^4\cdot 3^3\cdot 5^2),\varepsilon)$. By Remark 8 the coefficient field of $\tilde{\rho}$ is a degree eight extension of $\mathbb{Q}$.

• The space $S_2(\Gamma_0(2^4\cdot 3^2\cdot 5^2),\varepsilon)$ has 15 conjugacy classes, three of them with coefficient field $\mathbb{Q}(\sqrt{-1})$, another three of them with coefficient field a quadratic extension of it, and the last nine newforms with coefficient field a degree 4 extension of $\mathbb{Q}(\sqrt{-1})$ (so of degree eight over $\mathbb{Q}$). There are seven forms with complex multiplication. Mazur's trick allows to discard all newforms whose coefficient field does not have the right degree and some extra ones, but there are four newforms without complex multiplication which pass systematically Mazur's test, so we cannot reach a contradiction in this particular case.

• The space $S_2(\Gamma_0(2^4\cdot 3^3\cdot 5^2),\varepsilon)$ has 24 conjugacy classes, six of them with complex multiplication (one of them corresponding to the trivial solution by Proposition 4.7). Once again, some newforms without complex multiplication pass systematically Mazur's test.

Some partial results can still be obtained using more advanced elimination techniques (see [GPV21]).

8.0.5. *The equation* $x^2+6y^6=z^p$. In this case we can prove the following result.

Theorem 8.2. *Let $p>563$ be a prime number. Then there are no non-trivial primitive solutions of the equation*

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

Proof. Let (a,b,c) be a non-trivial primitive solution. Since d is divisible by 6, c is prime to 6 so in particular c is divisible by a prime larger than 3 and we are in the hypothesis of Ellenberg's large image result. In particular, Theorem 5.2 implies that the residual image is absolutely irreducible for all primes $p>N_6=563$.

Since d is only divisible by the primes 2 and 3, all sets $Q_{\pm,\pm}$ are empty, so the character ε equals the quadratic character of conductor 12. Theorem 4.5 implies the existence of a quadratic character χ of conductor $3\cdot\langle 2,\sqrt{-6}\rangle^5$ and Corollary 4.6 implies that we need to compute the space $S_2(\Gamma_0(2^8\cdot 3^5),\varepsilon)$. Such space has dimension 1152 and splits into 58 Galois conjugacy classes of newforms, eight of them having complex multiplication so Ellenberg's result implies that we can discard them. We discard the remaining newforms as follows:

• We run Mazur's trick for primes $5\leq q\leq 13$ for the first (in `Magma`'s order) 43 newforms without complex multiplication and it follows that $p\in\{2,3,5,11,7,37\}$.

• The last 7 newforms have a large coefficient field (of degrees 48, 72 and 144) and for some unclear reason `Magma` is unable to compute norms of elements in such large fields. To overcome this problem, we used `Magma` to compute the coefficients a_5 and a_{11} of each of these forms and apply Mazur's trick in `PARI/GP` for $q=5,11$ by hand (where the norms are computed within a few seconds). It follows that $p\in\{2,11,13\}$.

□

Remark 13. If Ellenberg's constant in Theorem 5.2 could be improved to 11 (as we expect), the previous result would hold for $p>37$. It is probably the case that the result can even be improved to $p>17$ via adding extra primes q into Mazur's test, but we did not pursue this objective because all involved computations are very time consuming (due to the fact that the coefficient fields have huge dimension).

8.0.6. *The equation* $x^2+7y^6=z^p$. The set $Q_{-+}=\{7\}$ while all other ones are empty. The character ε has order 2 and conductor 21, while χ has order 4. Let (a,b,c) be a non-trivial primitive solution. Corollary 4.6 implies the existence of a newform in one of the spaces $S_2(\Gamma_0(2^t\cdot 3^s\cdot 7^2),\varepsilon)$, for $t=1,2$ and $s=1,3$.

Note that the level valuation at 2 equals 1 when c is even and 2 when c is odd, by Lemma 2.14. In particular, Ellenberg's large image result applies to all newforms in $S_2(\Gamma_0(2^2\cdot 3^s\cdot 7^2),\varepsilon)$ (so we can discard the newforms with complex multiplication in such spaces).

• The space $S_2(\Gamma_0(2\cdot 3\cdot 7^2),\varepsilon)$ has 2 Galois conjugacy classes of newforms, but Mazur's trick only allows us to discard the second one (in `Magma`'s order).

• The space $S_2(\Gamma_0(2^2\cdot 3\cdot 7^2),\varepsilon)$ has 4 Galois conjugacy classes, one of them with complex multiplication (which can be discarded). Applying Mazur's trick with primes $1\leq q\leq 20$ to the forms without complex multiplication we can discard the three newforms if p does not belong to the set $\{2,3,7\}$.

• The space $S_2(\Gamma_0(2\cdot 3^3\cdot 7^2),\varepsilon)$ has 6 Galois conjugacy classes but only three of them can be proved to be not related to primitive solutions using Mazur's trick. We cannot discard the remaining three ones.

• The space $S_2(\Gamma_0(2^2\cdot 3^3\cdot 7^2),\varepsilon)$ has 7 Galois conjugacy classes, three of them having complex multiplication (one coming from the trivial solution by Proposition 4.7). All forms having complex multiplication can be discarded using Ellenberg's large image result. Applying Mazur's trick for primes $1\leq q\leq 20$ we can discard the remaining ones if $p>7$.

Still, some partial results can also be obtained for this particular equation using more advances elimination techniques (see [GPV21]).

Appendix A. Errata to [Ell05] (by Franco Golfieri, Ariel Pacetti and Lucas Villagra Torcomian)

This is an errata for the article [Ell05]. As pointed out by John Duncan, the proof of Lemma 4 missed an extra 2π (obtained from the equality of Lemma 3). The correct statement is the following.

Lemma 4. *We have the bound*

$$|(a_m,a_n)-4\pi\sqrt{mn}\delta_{mn}|\leq 16\pi^3\zeta^2(3/2)(m,n)^{1/2}mnN^{-3/2}d(N).$$

This is the precise statement proven in Ellenberg's Lemma 4. In page 4, when the Lemma is used, the bound for $|a_n(g)|$ has to be modified by adding and extra 2π factor.

In page 5, to compute the bound of $|(a_m,B(x)|$, one needs to add the extra factor 2π to the constant c (and the first result holds the same). The middle bound then reads

$$cM(2\pi)^{-2}+4\pi mM^{-1}=4\pi\zeta^2(3/2)q^2m^{3/2}N^{-1/2}d(N)+4\pi mq^{-2}N^{-1}.$$

Note that the last term is easily bounded by $q^2m^{3/2}N^{-1/2}d(N)$ (as implied in Ellenberg's article), giving the bound

$$cM(2\pi)^{-2}+4\pi mM^{-1}\leq(4\pi\zeta^2(3/2)+1)m^{3/2}q^2N^{-1/2}d(N).$$

The next line in Ellenberg's article has the wrong inequalities (but the needed ones), namely

$$1-\exp(-2\pi x/M)=1-\exp(-2\pi\sigma\log N/q^2)\geq 1-400^{-2\pi\sigma/q^2}\geq 399/400.$$

However, one needs to bound the inverse of the left expression (to the third power), so the final bound is correct (or a missing inverse must be included in Ellenberg's article). Then Proposition 5 reads.

Proposition 5. *Suppose $N\geq 400$ and $\sigma\geq q^2/2\pi$. Then*

$$|(a_m,B(\sigma N\log N)|\leq 2(4\pi\zeta^2(3/2)+1)(400/399)^3\exp(2\pi)q^2m^{3/2}N^{-1/2}d(N)N^{-2\pi\sigma/q^2}.$$

The previous bound was used in [Ell04] to prove Proposition 4.6. Playing a little bit with how the sum given in [Ell05, Theorem 1] to bound $E^{(3)}$ is split, on can still prove that the statement is correct; furthermore, one can replace the value 211 by 151. For that purpose, one can use the script described in Section 5.2 to check that splitting the sum at the value $c=151^2\cdot 100$ gives the value

```
? EllenbergBound(151,4,151^2*100)
%1 = 0.032478298538855530962882830523012352630
```

Since the value is positive, the result follows.

References

[BC12] Michael A. Bennett and Imin Chen. Multi-Frey $\mathbb{Q}$-curves and the Diophantine equation $a^2+b^6=c^n$. *Algebra Number Theory*, 6(4):707–730, 2012.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BEN10] Michael A. Bennett, Jordan S. Ellenberg, and Nathan C. Ng. The Diophantine equation $A^4+2^\delta B^2=C^n$. *Int. J. Number Theory*, 6(2):311–338, 2010.

[Cre84] J. E. Cremona. Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields. *Compositio Math.*, 51(3):275–324, 1984.

[Dar00] Henri Darmon. Rigid local systems, Hilbert modular forms, and Fermat's last theorem. *Duke Math. J.*, 102(3):413–449, 2000.

[DG95] Henri Darmon and Andrew Granville. On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. *Bull. London Math. Soc.*, 27(6):513–543, 1995.

[DM97] Henri Darmon and Loïc Merel. Winding quotients and some variants of Fermat's last theorem. *J. Reine Angew. Math.*, 490:81–100, 1997.

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

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

[Ell05] Jordan S. Ellenberg. On the error term in Duke's estimate for the average special value of L-functions. *Canad. Math. Bull.*, 48(4):535–546, 2005.

[GPV21] Franco Golfieri, Ariel Pacetti, and Lucas Villagra Torcomian. On the equation $x^2+dy^6 = z^p$ for square-free $1 \leq d \leq 20$, 2021.

[Kou20] Angelos Koutsianas. On the generalized fermat equation $a^2+3b^6 = c^n$. *Bulletin of the Hellenic Mathematical Society*, 64:56–68, 2020.

[Kub76] Daniel Sion Kubert. Universal bounds on the torsion of elliptic curves. *Proc. London Math. Soc. (3)*, 33(2):193–237, 1976.

[KW09] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture. II. *Invent. Math.*, 178(3):505–586, 2009.

[KW10] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture. In *Proceedings of the International Congress of Mathematicians. Volume II*, pages 280–293. Hindustan Book Agency, New Delhi, 2010.

[LMF22] The LMFDB Collaboration. The L-functions and modular forms database. http://www.lmfdb.org, 2022. [Online; accessed 4 January 2022].

[PAR19] PARI Group, Univ. Bordeaux. *PARI/GP version 2.12.2*, 2019. available from http://pari.math.u-bordeaux.fr/.

[PV22] Ariel Pacetti and Lucas Villagra Torcomian. $\mathbb{Q}$-curves, hecke characters and some diophantine equations ii. *Publicacions Matemàtiques*, to appear, 2022.

[Que00] Jordi Quer. $\mathbb{Q}$-curves and abelian varieties of GL_2-type. *Proc. London Math. Soc. (3)*, 81(2):285–317, 2000.

[Rib90] K. A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.

[Rib04] Kenneth A. Ribet. Abelian varieties over $\mathbb{Q}$ and modular forms. In *Modular curves and abelian varieties*, volume 224 of *Progr. Math.*, pages 241–261. Birkhäuser, Basel, 2004.

[Ser68] Jean-Pierre Serre. *Corps locaux*. Publications de l'Université de Nancago, No. VIII. Hermann, Paris, 1968. Deuxième édition.

[Sik12] Samir Siksek. The modular approach to Diophantine equations. In *Explicit methods in number theory*, volume 36 of *Panor. Synthèses*, pages 151–179. Soc. Math. France, Paris, 2012.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Tat75] J. Tate. Algorithm for determining the type of a singular fiber in an elliptic pencil. In *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 33–52. Lecture Notes in Math., Vol. 476, 1975.

Center for Research and Development in Mathematics and Applications (CIDMA), Department of Mathematics, University of Aveiro, 3810-193 Aveiro, Portugal

Email address: apacetti@ua.pt

FAMAF-CIEM, Universidad Nacional de Córdoba. C.P:5000, Córdoba, Argentina.

Email address: lucas.villagra@unc.edu.ar