$\mathbb{Q}$-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 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. Using Hecke characters we prove that a twist of the elliptic curve representation descends to $\mathbb{Q}$ hence (by Serre's conjectures) corresponds to a newform in $S_2(n, \varepsilon)$ for explicit values of n and ε. This gives a systematic procedure to study solutions of the above equations and allows us to prove non-existence of solutions 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. Of particular interest is the problem of determining all solutions of a generalized Fermat equation

$$AX^p + BY^q = CZ^r,$$

mostly when $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$, as in this case solutions correspond to points on curves of genus greater than 1 (see [DG95]). Using $\mathbb{Q}$-curves, solutions of the equation

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

were studied in [Ell04] for $d = 1$ and in [DU09] for $d = 2, 3$. Both articles prove an asymptotic result, namely there exists N_d such that (1) has no non-trivial solutions for $p > N_d$. The constant N_d obtained equals $211, 349, 131$ for $d = 1, 2, 3$ respectively. Furthermore, by a detailed study of the small primes, it is possible to extend the result to all primes in the cases $d = 1, 2$. ([BEN10]).

A solution (A, B, C) to (1) is called *primitive* if $\gcd(A, B, C) = 1$. As explained in [DM97], it is mostly interesting to understand primitive solutions, as otherwise there might be infinitely many of them. There are some *trivial* solutions to (1), namely $(\pm 1, 0, 1)$ and $(0, \pm d, d)$ for $p = 3$.

The general strategy for finding primitive solutions of Diophantine equations consist on attaching a Frey curve to a solution. The Frey curve has the property that modulo p, the residual Galois image has small level, hence using modularity of rational irreducible representations (Serre's conjectures) and Ribet's lowering the level theorem, one concludes that the solution is related to a newform in a specific level and weight space. In many instances, after computing such space, one deduces that no such form can exist.

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

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

where $r^2 = -d$. To easy notation, we denote $E = E_{(A,B)}$ when there is no confusion. The existence of trivial solutions sometimes imposes a big issue in the aforementioned strategy! The advantage of equation (1) is that the trivial solutions $(\pm 1, 0, 1)$ and $(0, \pm d, d)$ for $p = 3$ correspond to elliptic curves with complex multiplication while others do not.

The curve E is not defined over $\mathbb{Q}$, but is what is called in the literature a $\mathbb{Q}$-curve, i.e. an elliptic curve whose Galois conjugates are isogenous to E. As will be explained in detail, $\overline{E}$ is 2-isogenous to the quadratic twist of E by (the quadratic character associated to the field) $\mathbb{Q}(\sqrt{-2})$. Over the compose field $\mathbb{Q}(\sqrt{-d}, \sqrt{-2})$, E is a (completely defined) $\mathbb{Q}$-curve. By a result of Ribet ([Rib04]) a twist of E gives a Galois representation that descends to $\mathbb{Q}$. However, Ribet's result is not explicit, as it depends on finding a map trivializing some cocycle and there is not much control of it.

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

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

AP and LVT are partially supported by Proyecto Consolidar 2018-2021 33620180100781CB.

The strategy used in the literature follows a strategy of Quer ([Que00]) which gives an ad-hoc element (via Hilbert's 90 theorem) after a tedious search for it. In particular, it gives no control on the ramification of the character so determining the level and the Nebentypus of (one) weight 2 modular form attached to E (after twisting) is not straightforward. In the present article, we give a solution different from Ribet's one. We define a Hecke character χ such that the ℓ-adic Galois representation (for any ℓ) attached to E twisted by χ descends to $\mathbb{Q}$. In this way, we have complete control on the level and the Nebentypus of the resulting newform. We also compare our approach to Ribet's classical solution (which implies trivializing a cocycle).

The advantage of our approach is that it can be applied to other Diophantine problems where the $\mathbb{Q}$-curve is defined over an imaginary quadratic field. For example in [BC12], the Diophantine equation

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

is considered, for $d = 1$. The Frey curve attached to a primitive solution (A, B, C) is given by the equation

$$\widetilde{E}_{(A,B)} : y^2 = x^3 - 3(5B^3 + 4Ai)Bx + 2(11B^6 + 14iB^3A - 2A^2). \tag{4}$$

The curve $\widetilde{E}$ is also a $\mathbb{Q}$-curve as its Galois conjugate is 3-isogenous to the quadratic twist of E by $\mathbb{Q}(\sqrt{-3})$. In Section 5 we attach a Frey curve to a solution of equation (3) for a general d, and prove that such curve is a $\mathbb{Q}$-curve; in particular its Galois conjugate is a twist by $\mathbb{Q}(\sqrt{-3})$ of an isogenous curve (our equation is different from that of [BC12] where the 3-isogeny is not explicit). Our Frey curve comes from the description of curves with a 3-torsion point given by Kubert ([Kub76]). We apply the same strategy, namely we construct a Hecke character such that the twisted representation descends to $\mathbb{Q}$, to give an explicit formula for the level and Nebentypus of the newform attached to a solution of it.

The restriction to imaginary quadratic twists is to avoid fundamental units, a case in which Hecke characters are harder to construct. Nevertheless, our construction of the Hecke character works when the fundamental unit of $\mathbb{Q}(\sqrt{d})$ (for d positive) has norm -1. Applications of such result to Diophantine problems will be considered in a sequel (as the techniques are completely different than the ones used for imaginary quadratic fields).

As an application, in the present article we study equations (1) and (3) for $d = 1, 2, 3, 5, 6$ and 7 (the cases that were not considered before), but our approach allows to study any other value of d. 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). It would be an interesting problem to study if the so called "multi-Frey"method can be used in such cases (although it implies working over other number fields).

The article is organized as follows: in section 1 the main properties of the curve (2) are given. In particular, we recall the proof that E is a $\mathbb{Q}$-curve and compute its reduction type and conductor at all primes (for any value of d). This result is needed to give an explicit formula for the level n and the Nebentypus ε of the newform attached to a primitive solution. Section 2 gives the general strategy to construct the Hecke character, and describes it explicitly for equation (1). Since the conjugate Galois representation is isomorphic to its twist by $\sqrt{-2}$, the prime 2 plays a special role in the construction (this is why we give one construction of the character needed to solve (1) first and another construction to solve (3)). The way to define the character χ is to split the set of primes ramifying in $K/\mathbb{Q}$ depending on their congruence modulo 8. If q is such an odd prime, the ramification of the local component of χ at $\mathfrak{q}$ (the unique prime of K dividing q) has order $1, 2$ or 4 and depends only on $q \pmod 8$. Special care needs to be taken for primes dividing 2 (which is the more technical part of the construction). The main application (Theorem 2.3) gives the recipe for n and ε using the control on the conductor of $\rho_{E,p} \otimes \chi$ and standard techniques.

In Section 3 we relate our construction to that of Ribet. This includes an explicit description of the field extension N where the cocycle attached to our $\mathbb{Q}$-curve is trivialized (in terms of the character χ), a description of the Galois group $\mathrm{Gal}(N/\mathbb{Q})$ and a trivialization map.

Section 4 recalls the general strategy (and the results needed) to prove non-existence of primitive solutions of equation (1). The main idea is to use Ribet's lowering the level result. For doing that, we need the residual image (modulo p) of the residual representation $\rho_{E,p}$ to be absolutely irreducible. To assure the big residual image hypothesis, we consider two different cases. Either the solution (A, B, C) satisfies that C is divisible by a prime greater than 3 or it does not. In the first case, the curve E has a prime of multiplicative reduction, hence cannot be a curve with complex multiplication. Then a result of Ellenberg implies that there exists

a bound N_K (depending only on the base field K) such that the curve has big residual image at all primes greater than N_K. In the second case, we adapt a stratedy used in [DU09]: namely if C is supported only at the primes $\{2,3\}$ and the residual image is not absolutely irreducible, then there exists a congruence with an Eisenstein series. For p large enough this violates Hasse's bound on $|a_p(E)|$. With all tools in hand, we prove non-existence of solutions for $d=5$ (Theorem 4.5), $d=6$ (Theorem 4.6) and $d=7$ (Theorem 4.7). In some cases, we exploit the relation to Bianchi modular forms (using an algorithm due to Cremona to compute such space for imaginary quadratic fields of class number 1) which improves the computational effort.

Section 5 is devoted to study equation (3). Based on Kubert's description of elliptic curves with a 3-rational point ([Kub76]), we attached to a non-primitive solution of it a general Frey curve $\tilde{E}$ (for any value of d). We prove that the curve $\tilde{E}$ is a $\mathbb{Q}$-curve by proving that its Galois conjugate is isogenous to its quadratic twist by $\sqrt{-3}$. Contrary to what happened for the curve E, the primes ramifying in the quadratic extension $K/\mathbb{Q}$ are primes of additive reduction for $\tilde{E}$. We study the ramification type of $\tilde{E}$ at all primes, including primes dividing 2, 3 and the ones ramifying in $K/\mathbb{Q}$. For the latter ones, we also describe the local type of the Weil-Deligne representation attached to $\tilde{E}$ (such information is sometimes useful to discard newforms which are candidates to come from solutions). In Section 6 we study the problem of how to descend the Galois representation attached to a $\mathbb{Q}$-curve $\tilde{E}$ over an imaginary quadratic field K satisfying that its conjugate curve is isogenous to the twist of $\tilde{E}$ by a quadratic character ramified at a unique prime $t \equiv 3 \pmod 4$ (the case of interest being $t=3$). The general strategy follows the case $t=2$ given in Section 2, but turns out to be more interesting. The set of primes ramifying in $K/\mathbb{Q}$ need to be separated into four different sets depending on properties modulo $4t$ (more concretely depending on whether an odd prime q is a square modulo 4 or not, and whether it is a square modulo t or not). Once the local definition of the Hecke character is given, the proof that the global character satisfies the desired properties is similar to the case $t=2$ (with some extra technicalities).

At last, in Section 7 we apply our results to solve new instances of equation (3). In particular, we succeed to solve the case $d=2$ (Theorem 7.1) and $d=6$ (Theorem 7.2), while did not succeed to prove the cases $d=5$ and $d=7$ due to the existence of newforms matching all conditions of curves coming from real solutions.

To easy notation during the exposition, if K is a number field or a local field, Gal_K will denote the Galois group $\mathrm{Gal}(\overline{K}/K)$.

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. The equation (1): properties of the curve E

The curve E satisfies: $\Delta(E) = 512(A^2+rB)C^p$ and $j(E) = \frac{64(5A^2-3rB)^3}{C^p(A^2+rB)}$. There are two important facts on primitive solutions: if (A,B,C) is a primitive solution of (1), then $\gcd(A,d)=1$ and also the following elementary property holds.

Lemma 1.1. *Let (A,B,C) be a primitive solution with $p>3$, then*

- *If d is even, A is odd.*
- *If $d \equiv 1,3,5 \pmod 8$ only one of $\{A,B\}$ is even and the other one is odd.*

The trivial solution $(\pm 1, 0, 1)$ corresponds to a curve curve with complex multiplication by $\mathbb{Z}[\sqrt{-2}]$ (with j-invariant 8000) and the solution $(0, \pm d, d)$ for $p=3$ corresponds to a curve with complex multiplication by $\mathbb{Z}[\sqrt{-1}]$ (with j-invariant 1728). Note that $j(E)$ is not in $\mathbb{Q}$ unless $B=0$ (corresponding to a trivial solution) or $(A,B,d)=(3,5,7)$ (corresponding to an elliptic curve with complex multiplication by $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ and j-invariant -3375)). In particular, if (A,B,C) is a non-trivial solution, the curve E is not defined over $\mathbb{Q}$. Let $K = \mathbb{Q}(\sqrt{-d})$.

Lemma 1.2. *Let $\mathfrak{q}$ be an odd prime of K. Then $v_{\mathfrak{q}}(\Delta(E)) \equiv 0 \pmod p$.*

Proof. Clearly if $\mathfrak{q} \mid \gcd(A^2+rB, A^2-rB)$ then $\mathfrak{q} \mid 2$ (because (A,B,C) is primitive). Then, since $C^p = A^4 + dB^2 = (A^2+rB)(A^2-rB)$,

$$v_{\mathfrak{q}}(A^2+rB) = \begin{cases} 0 & \text{if } \mathfrak{q} \nmid (A^2+rB), \\ v_{\mathfrak{q}}(C^p) & \text{otherwise.} \end{cases}$$

□

Lemma 1.3. *Suppose that p is an odd rational prime ramified at $K/\mathbb{Q}$ and let $\mathfrak{p}$ denote the (unique) prime in K dividing p. Then $\mathfrak{p} \nmid \Delta(E)$.*

Proof. Since p is ramified, $\mathfrak{p} \mid r$, and since (A,B,C) is a primitive solution, $\mathfrak{p} \nmid A$. Then $\mathfrak{p} \nmid C^p(A^2+rB)$. □

Let N_E denote the conductor of E. Assume that $p \geq 11$ to avoid extra computations when 2 splits in K.

Lemma 1.4. *Let $\mathfrak{q}$ be a prime ideal of K dividing 2.*

(1) If 2 is inert in K then $v_2(N_E) = 8$.
(2) If 2 ramifies in K then $v_{\mathfrak{q}}(N_E) \in \{10, 12\}$.
(3) If $(2) = \mathfrak{p}_2\bar{\mathfrak{p}}_2$ then either $v_{\mathfrak{p}_2}(N_E) = v_{\bar{\mathfrak{p}}_2}(N_E) = 8$ or $v_{\mathfrak{p}_2}(N_E) = 6$ and $v_{\bar{\mathfrak{p}}_2}(N_E) \in \{1, 4\}$.

Proof. Apply Tate's algorithm ([Tat75]). The invariants of E are: $a_6 = 0$, $b_2 = 16A$, $b_6 = 0$ and $b_8 = -4(A^2+rB)^2$. Let $\mathcal{O}_K$ denote the ring of integers of K.

(1) The hypothesis implies that $d \equiv 3 \pmod 8$ and 2 is prime in $\mathcal{O}_K$. Notice that, by Lemma 1.1, $2 \nmid A^2+rB$ hence $v_2(\Delta(E)) = 9$. Since: $2 \mid b_2$, $2^2 \mid a_6$, $2^3 \nmid b_8$, the curve has reduction type III and $v_2(N_E) = v_2(\Delta(E)) - 1 = 8$.

(2) Let $\mathfrak{q}$ be the unique prime in $\mathcal{O}_K$ dividing 2 and let π be a local uniformizer. By Lemma 1.1, $\mathfrak{q} \nmid (A^2+rB)$, hence $v_{\mathfrak{q}}(\Delta(E)) = 18$. To easy notation, consider the curve

$$y^2 = x^3 + 4\alpha x^2 + 2\beta x, \tag{5}$$

where $\mathfrak{q} \nmid \beta$. Clearly $\mathfrak{q} \mid b_2$, $\mathfrak{q}^2 \mid a_6$, $\mathfrak{q}^3 \mid b_8$ and $\mathfrak{q}^3 \mid b_6$. 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 (5), to get the new equation

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

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), $v_{\mathfrak{q}}(\pi^2 + 2\beta) = 3$ hence $v_{\mathfrak{q}}(\tilde{a_4}) = 4$ 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 $v_{\mathfrak{q}}(N_E) = v_{\mathfrak{q}}(\Delta(E)) - 6 = 12$.

Suppose that d is even and B is even. If $\frac{d}{2} \equiv 1 \pmod 4$ then $v_{\mathfrak{q}}(\tilde{a}_6) \geq 6$ and $v_{\mathfrak{q}}(\tilde{a}_4) = 4$, so we do not need to make any translation and the type is I_4^* and $v_{\mathfrak{q}}(N_2) = 18 - 8 = 10$. If $\frac{d}{2} \equiv 3 \pmod 4$ then $v_{\mathfrak{q}}(\tilde{a}_6) = 4$ and $v_{\mathfrak{q}}(\tilde{a}_4) \geq 5$ 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, $v_{\mathfrak{q}}(\tilde{a}_6) \geq 5$ and $v_{\mathfrak{q}}(\tilde{a}_4) = 4$, hence again the type is I_4^* and $v_{\mathfrak{q}}(N_2) = 18 - 8 = 10$.

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

- If either A or B is even (hence the other one is odd) then $v_{\mathfrak{p}}(A^2+rB) = 0$ and $v_{\mathfrak{p}}(\Delta) = 9$ (for both primes). Clearly $v_{\mathfrak{p}}(b_2) \geq 4$ and $v_{\mathfrak{p}}(b_8) = 2$ hence the reduction type is III and $v_{\mathfrak{p}}(N_E) = 9 - 1 = 8$ (at both primes).
- If both A, B are odd, we can assume that $v_{\mathfrak{p}}(A^2+rB) > 1$ while $v_{\bar{\mathfrak{p}}}(A^2+rB) = 1$ (since $\frac{A^2+rB}{2}$ is an integer, and $v_{\bar{\mathfrak{p}}}(A^2+rB) = v_{\mathfrak{p}}(A^2-rB) = v_{\mathfrak{p}}(A^2+rB-2rB)$). Furthermore, our assumption $p \geq 11$ implies that $v_{\mathfrak{p}}(A^2+rB) \geq 11$ so $v_{\mathfrak{p}}(j(E)) < 0$. In particular E has

potentially multiplicative reduction. Furthermore, the equation is not minimal at $\mathfrak{p}$, under a change of variables, it equals

$$y^2 = Ax^2 + \frac{(A^2 + rB)}{2^5}x,$$

which already has multiplicative reduction. Hence its conductor equals $\mathfrak{p}$ or $\mathfrak{p}^4$. To compute the type at $\bar{\mathfrak{p}}$, the hypothesis also implies that $v_{\bar{\mathfrak{p}}}(j) < 0$ 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 $\bar{\mathfrak{p}}^6$.

□

Lemma 1.5. *Let $\mathfrak{p}$ be an odd prime dividing $\Delta(E)$. Then E has multiplicative reduction at $\mathfrak{p}$.*

Proof. By Lemma 1.3 we know that primes dividing $\Delta(E)$ are not ramified in $K/\mathbb{Q}$; in particular, if $\mathfrak{p}$ is an odd prime dividing $\Delta(E)$, $\mathfrak{p} \nmid 4A$, hence clearly the reduction of (2) modulo $\mathfrak{p}$ is multiplicative. □

Recall (as explained in [DU09]) that the curve E is a $\mathbb{Q}$-curve. The 2-isogenous curve of E (corresponding to the quotient by the 2-torsion point $(0,0)$) is the curve

$$y^2 = x^3 - 8Ax^2 + 8(A^2 - rB)x.$$

Such curve equals the quadratic twist by -2 of $\tau(E)$ (the Galois conjugate of E). In particular, if we look at E over $L = \mathbb{Q}(\sqrt{-d}, \sqrt{-2})$ then it is a $\mathbb{Q}$-curve in the sense that the curve is isogenous to all of its Galois conjugates. In particular, for any prime number p, there exists a twists of the Galois representation $\rho_{E,p} : \mathrm{Gal}_L \to \mathrm{GL}_2(\mathbb{Z}_p)$ which extends to the whole Galois group $\mathrm{Gal}_{\mathbb{Q}}$ (see [Rib04]). Methods to describe the twist are explained in [Que01, Que00], and a detailed concrete example is given in [Pyl04] (page 47). The problem is that in such approaches no control on the ramification of the twist is given. Our main contribution is to give an alternative solution in terms of Hecke characters.

Recall that a representation $\rho : \mathrm{Gal}_K \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$ descends to $\mathrm{Gal}_{\mathbb{Q}}$ if and only of ${}^{\tau}\rho = \rho$, where $\tau \in \mathrm{Gal}_{\mathbb{Q}}$ is an element whose restriction is non-trivial, and ${}^{\tau}\rho(\sigma) = \rho(\tau\sigma\tau^{-1})$ (we will present a proof of this fact in Theorem 2.3).

If t is an integer, let ψ_t denote the character of $\mathrm{Gal}_{\mathbb{Q}}$ corresponding to the extension $\mathbb{Q}(\sqrt{t})/\mathbb{Q}$. The hypothesis of E being a $\mathbb{Q}$-curve whose Galois conjugate equals its quadratic twist by ψ_{-2} implies that ${}^{\tau}\rho_{E,p} = \rho_{E,p} \otimes \psi_{-2}$. In section 2 we construct a Hecke character $\chi : \mathrm{Gal}_K \to \overline{\mathbb{Q}}^{\times}$ satisfying that ${}^{\tau}\chi = \chi \cdot \psi_{-2}$ (as characters of Gal_K). Then the twisted representation $\rho_{E,p} \otimes \chi$ does descend to a representation of $\mathrm{Gal}_{\mathbb{Q}}$. Knowing the conductor of χ allows us (in Theorem 2.3) to specify the level and Nebentypus of the rational representation.

2. Construction of the Hecke character

Let $\mathbb{I}_K$ denote the idèle group of K and $\mathrm{Cl}(K)$ the class group of K. Fix for each prime p an embedding $\mathrm{Gal}_{\mathbb{Q}_p} \hookrightarrow \mathrm{Gal}_{\mathbb{Q}}$. Class field theory relates characters of Gal_K with characters on the idèle group $\mathbb{I}_K$ (our characters will always be finite), hence we will denote by the same letter both incarnations of the same object (and hope there is no confusion on doing that).

If N is a local field, local class field theory relates abelian extensions of N with continuous characters ϕ of $N^{\times}$. Furthermore, the ramification information is encoded in the restriction of ϕ to $\mathcal{O}^{\times}$ (the ring of integers of N). Let L be a global field. From the short exact sequence

$$0 \longrightarrow L^{\times} \cdot (\textstyle\prod_{\mathfrak{q}} \mathcal{O}_{\mathfrak{q}}^{\times} \times (L \otimes \mathbb{R})^{\times}) \longrightarrow \mathbb{I}_L \longrightarrow \mathrm{Cl}(L) \longrightarrow 0, \tag{6}$$

we deduce that to define a character of $\mathbb{I}_L$ it is enough to give its values on $(\prod_{\mathfrak{q}} \mathcal{O}_{\mathfrak{q}}^{\times} \times (L \otimes \mathbb{R})^{\times})$, on $L^{\times}$ (where the character is trivial) and on idèles representing the class group of K. Note that $(\prod_{\mathfrak{q}} \mathcal{O}_{\mathfrak{q}}^{\times} \times (L \otimes \mathbb{R})^{\times}) \cap L^{\times} = \mathcal{O}_L^{\times}$, hence the compatibility condition is that the product of the local components evaluated at a unit equals 1.

For $L=\mathbb{Q}$, since the class group is trivial, a Hecke character is determined by its values on $\prod_p \mathbb{Z}_p^\times \times \mathbb{R}^\times$. i.e. give for each prime p a character $\phi_p : \mathbb{Z}_p^\times \to \mathbb{C}^\times$ and an infinite character $\phi_\infty : \mathbb{R}^\times \to \mathbb{C}^\times$ satisfying

$$\prod_p \phi_p(-1)\phi_\infty(-1) = 1. \tag{7}$$

Such information determines a unique Hecke character ψ, and if ψ has finite order, we can take its image to take values in $\overline{\mathbb{Q}}^\times$.

Let $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be such that its restriction to K is not trivial. If $\chi : \mathbb{I}_K \to \mathbb{C}^\times$ is a Hecke character on K, let ${}^\tau\chi$ denote the character given by

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

Looking at characters of the Galois group, the character ${}^\tau\chi$ is given by ${}^\tau\chi(\sigma) = \chi(\tau\sigma\tau^{-1})$.

Problem: Given ψ_t a quadratic character of $\mathrm{Gal}_\mathbb{Q}$ corresponding to an imaginary quadratic extension ramified at a unique prime, find a Hecke character χ of Gal_K such that ${}^\tau\chi = \chi \cdot \psi_{-t}$.

We solve the previous problem for $t=2$ and for t a prime number congruent to 3 modulo 4 (so ψ_t corresponds to an imaginary quadratic extension ramified at a unique prime). Furthermore, we construct a character $\varepsilon : \mathbb{I}_\mathbb{Q} \to \overline{\mathbb{Q}}^\times$ such that $\chi^2 = \varepsilon \circ \mathcal{N}$. Once the existence of the character χ is proven, a well known result (see Theorem 2.3) implies that the Galois representation attached to the elliptic curve E (respectively $\tilde{E}$) descends to $\mathbb{Q}$ and ε will be its Nebentypus.

The characters ε and χ ramify only on primes ramifying in $K/\mathbb{Q}$ and on primes dividing $2t$. The general strategy is to split the odd primes $\{p \ : \ p \text{ ramifies in } K/\mathbb{Q}\}$ into four sets depending on the values of $\psi_{-t}(p)$ (more concretely: for $t=2$ depending on the congruence of p modulo 8 while for t an odd prime, depending whether p is a square modulo t or not and on whether p is a square modulo 4 or not). For primes in each set, define the local characters ε_p and $\chi_\mathfrak{p}$ restricted to the integers $\mathbb{Z}_p^\times$ and $\mathcal{O}_\mathfrak{p}^\times$ respectively (where $\mathfrak{p}$ is the unique prime in K dividing p). Then we define global characters ε and χ as a product of the local parts on the set $(\prod_\mathfrak{q} \mathcal{O}_\mathfrak{q}^\times \times \mathbb{C}^\times)$. The definitions are given so that both characters satisfy:

(1) The local character $\chi_\mathfrak{p}$ satisfies that ${}^\tau\chi_\mathfrak{p} = \chi_\mathfrak{p} \cdot ((\psi_{-t})_p \circ \mathcal{N})$.
(2) For q an odd prime, let δ_q denote the quadratic character in $(\mathbb{Z}/q)^\times$, then for all odd primes p ramified in $K/\mathbb{Q}$, $\chi_\mathfrak{p} = \varepsilon_p\delta_p$ (identifying $(\mathcal{O}_\mathfrak{p}/\mathfrak{p})^\times$ with $(\mathbb{Z}/p)^\times$).
(3) An extra condition at primes dividing 2 so that a compatibility conditions on units holds (a condition similar to (7) for the units of K).

The first condition is needed for χ to solve the problem. If $\mathfrak{p}$ is an odd prime not dividing t, the second condition implies that then $\chi_\mathfrak{p} = \varepsilon_p \circ \mathcal{N}$. The proof of this fact is the following: for primes $\mathfrak{p} \nmid 2td$, both characters are trivial, hence the statement trivially holds. For odd primes that $\mathfrak{p} \nmid t$ and $\mathfrak{p} \mid d$ (of norm p), recall that the restriction of ε_p to $\mathrm{Gal}_{K_\mathfrak{p}}$ equals (as Hecke characters) $\varepsilon_p \circ \mathcal{N}$, 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 $x \to x^2$, so the equality

$$\chi_\mathfrak{p}^2(x) = \varepsilon_p \circ \mathcal{N}(x) = \varepsilon_p^2(x)$$

holds. The last condition is the key for the existence of χ and ε as it will imply that χ can be defined in the first term of (6) (so we are only led to define it on idèles representing the class group of K).

2.1. **The case $t=2$.** Since our applications involve imaginary quadratic fields, let $K = \mathbb{Q}(\sqrt{-d})$ with d a positive square-free integer and split the odd prime divisors of d in 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 $\varepsilon : \mathbb{I}_\mathbb{Q} \to \mathbb{C}^\times$ ramified at the primes in $Q_3 \cup Q_5$ and sometimes in $\{2\}$, with local component ε_p as follows:

- For primes $p \in Q_1 \cup Q_7$, the character $\varepsilon_p : \mathbb{Z}_p^\times \to \mathbb{C}^\times$ is trivial.
- For primes $p \in Q_3$, the character $\varepsilon_p = \delta_p$, the quadratic character $\delta_p(n) = \left(\frac{n}{p}\right)$.
- 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} their local component at the prime 2 (see Table 2.1).

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

TABLE 2.1. Table

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

By construction, the first hypothesis is satisfied for ε, 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 $\varepsilon : G_\mathbb{Q} \to \overline{\mathbb{Q}}$. Let N_ε denote its conductor, given by $N_\varepsilon = 2^e \prod_{p\in Q_3\cup Q_5} p$, where $e = 0$ if $\#Q_5 + \#Q_7$ even and 2 otherwise.

Remark 1. The dependence on d of the parity of $Q_3 + Q_5$ (and Q_7) is given on Table 2.2. In particular, if d is odd, ε_2 depends only on $d \pmod 8$ (not the sets Q_3, 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 2.2. Table

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

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

Proof. Following the strategy described above, let $\chi_p : \mathcal{O}_\mathfrak{p}^\times \to \mathbb{C}^\times$ (where $\mathcal{O}_\mathfrak{p}$ denotes the completion of $\mathcal{O}_K$ at $\mathfrak{p}$) be the character given by

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

In particular, the second property of the general strategy is satisfied. Furthermore, the local component of the character satisfies the stated properties, namely:

(1) Is proven in the general strategy.
(2) The ramification statement is clear from the definition of $\chi_\mathfrak{p}$.

(3) At primes not dividing elements of $Q_1 \cup Q_5 \cup Q_7$ all characters are trivial, hence the equality. For primes ramifying in K, τ acts as the identity in the quotient $\mathcal{O}_\mathfrak{p}/\mathfrak{p}$ and ψ_{-2} is trivial.

The archimidean component of χ is trivial, while its local component at places dividing 2 depends on K and ε. 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 $(\mathcal{O}_{\mathfrak{p}_2}/2^3)^\times$ and its generators are given in Table 2.3 (where the order of the generators match the group structure, and the norms are modulo 8). Define χ_2 on the set of

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	$\mathbb{F}_3 \times \mathbb{Z}/4 \times \mathbb{Z}/2 \times \mathbb{Z}/2$	$\{\zeta_3, \sqrt{-d}, 3+2\sqrt{-d}, -1\}$	$\{1,3,5,1\}$
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 2.3. Table

generators as follows:

- If $d \equiv 1 \pmod 8$, $\chi_2(\sqrt{-d}) = 1$, $\chi_2(1+2\sqrt{-d}) = 1$, $\chi_2(5) = -1$.
- If $d \equiv 3 \pmod 8$, $\chi_2(\zeta_3) = 1$, $\chi_2(\sqrt{-d}) = i$, $\chi_2(3+2\sqrt{-d}) = 1$, $\chi_2(-1) = 1$.
- If $d \equiv 5 \pmod 8$, $\chi_2(\sqrt{-d}) = 1$, $\chi_2(1+2\sqrt{-d}) = 1$, $\chi_2(-1) = -1$.
- If $d \equiv 2 \pmod 8$ and $\#Q_3 + \#Q_5$ is even, $\chi_2(1+\sqrt{-d}) = 1$, $\chi_2(-1) = 1$, $\chi_2(5) = 1$.
- If $d \equiv 2 \pmod 8$ and $\#Q_3 + \#Q_5$ is odd, $\chi_2(1+\sqrt{-d}) = i$, $\chi_2(-1) = -1$, $\chi_2(5) = 1$.
- If $d \equiv 6 \pmod 8$ and $\#Q_3 + \#Q_5$ is even, $\chi_2(1+\sqrt{-d}) = 1$, $\chi_2(-1) = -1$, $\chi_2(5) = 1$.
- If $d \equiv 6 \pmod 8$ and $\#Q_3 + \#Q_5$ is odd, $\chi_2(1+\sqrt{-d}) = i$, $\chi_2(-1) = 1$, $\chi_2(5) = 1$.
- 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 by $\chi_2 = \chi_{\mathfrak{p}_2}\chi_{\overline{\mathfrak{p}_2}} = \delta_{-2}$.

With the above definitions, it is easy to check that $\chi_2^2 = \varepsilon_2 \circ \mathcal{N}$, using the character values in Table 2.1, the parity of Table 2.2 and the norm of the generators given in Table 2.3.

To check the second property, clearly ${}^\tau\chi_2 \cdot \chi_2 = \chi_2 \circ \mathcal{N}$, hence ${}^\tau\chi_2 = \chi_2^{-1} \cdot \chi_2 \circ \mathcal{N}$. An easy case by case computation on the generators shows that ${}^\tau\chi_2 = \chi_2 \cdot (\delta_{-2} \circ \mathcal{N})$.

It is important to notice that

$$\chi_2|_{\mathbb{Z}_2^\times} = \delta_2^{v_2(d)+1}\delta_{-1}^{\#Q_5+\#Q_7}. \tag{8}$$

Extend χ to $K^\times \cdot (\prod_\mathfrak{q} \mathcal{O}_\mathfrak{q}^\times \times \mathbb{C}^\times)$ by making it trivial in $K^\times$, so all the above properties continue to hold.

Compatibility: the subgroup of units in K is generated by roots of order 2, 3 and 4 (for $\mathbb{Q}(\sqrt{-1})$). Since all 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, $i = 1,3,5,7$ are empty and the compatibility at $\sqrt{-1}$ follows from the fact that $\chi_2(\sqrt{-1}) = 1$ in such case.

To check the compatibility at -1, abusing notation, let $\mathfrak{p} \in Q_i$ denote the fact that the norm of $\mathfrak{p}$ is in such set, then

$$\chi(-1) = \prod_\mathfrak{p} \chi_\mathfrak{p}(-1) = \prod_{\mathfrak{p} \in Q_1 \cup Q_5 \cup Q_7} \chi_\mathfrak{p}(-1)\chi_2(-1) = (-1)^{\#Q_5+\#Q_7}\delta_{-1}(-1)^{\#Q_5+\#Q_7} = 1. \tag{9}$$

Extension: To extend χ to $\mathbb{I}_K$, it is enough to define it on idèles that generate the class group of K. Let $\{\mathfrak{q}_1, \cdots, \mathfrak{q}_\mathfrak{h}\}$ be prime ideals of K generating $\mathrm{Cl}(K)$ (we can and do assume they are not ramified in $K/\mathbb{Q}$). Since $\mathfrak{q}_i$ is not principal, it must split in $K/\mathbb{Q}$, so if $q_i = \mathcal{N}(\mathfrak{q}_i)$, we can take as representatives the idèle a_i in $\mathbb{I}_K$ with trivial infinite component and finite components:

$$(a_i)_\mathfrak{p} = \begin{cases} q_i & \text{if } \mathfrak{p} = \mathfrak{q}_\mathfrak{i}, \\ 1 & \text{otherwise.} \end{cases}$$

Suppose that $\mathfrak{q}_i$ has odd order in the class group, hence there exists $\alpha \in K^\times$ and $u \in \prod_\mathfrak{q} \mathcal{O}_\mathfrak{q}^\times \times \mathbb{C}^\times$ such that $a_i = \alpha u b_i^2$. Then it must hold that

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

If on the contrary, $\mathfrak{q}_\mathfrak{i}$ has order a power of 2, define $\chi(a_i) = \sqrt{\varepsilon(\mathcal{N}(a_i))}$ (any of the two ones works) and extend it multiplicatively. Recall that both 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: 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. Let $\tilde{\chi}$ denote the extension and χ the character on $K^\times\cdot(\prod_\mathfrak{q}\mathcal{O}_\mathfrak{q}^\times\times\mathbb{C}^\times)$; if the idèle a_i corresponds to an ideal of order t in the class group, the consistency relation translates into $\tilde{\chi}(a_i^t) = \chi(a_i^t)$.

Start supposing that the idèle a_i satisfies that the ideal attached to it has odd order t in the class group, in particular 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 $a_i = \alpha u b_i^2$, and the ideal attached to b_i also has order t in the class group. Then

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

because $\chi^2 = \varepsilon\circ\mathcal{N}$ on $K^\times\cdot(\prod_\mathfrak{q}\mathcal{O}_\mathfrak{q}^\times\times\mathbb{C}^\times)$. In particular, this proves compatibility for idèles whose attached ideal have odd order in the class group.

Suppose that a_i is not a square, and has order 2^t, with $t\geq 2$, in the class group of K. By definition, $\tilde{\chi}(a_i^{2^t}) = \tilde{\chi}^2(a_i^{2^{t-1}})$. The idèle $a_i^{2^{t-1}}$ corresponds to an ideal of order 2 in the class group; if we prove compatibility for such idèles, we are done. It is well known that the ideals $\mathfrak{b} = \langle q, \sqrt{-d}\rangle$, where q is an odd prime dividing d, form a set of representatives for the elements of order two in the class group of K. Such ideal can be represented by the idèle b_i' with $\sqrt{-d}$ at the place $\mathfrak{b}$ and 1 at all other places. Then $\tilde{\chi}(b_i^2) = \tilde{\chi}^2(b_i) = \varepsilon(\mathcal{N}(b_i)) = \varepsilon_q(d)$. Furthermore,

$$\varepsilon_q(d) = \varepsilon_q(d/q)\varepsilon_2(q)^{-1}\prod_{p\in Q_3\cup Q_5}\varepsilon_p(q)^{-1}, \tag{10}$$

where the product runs over primes different from q. On the other hand,

$$\chi(b_i^2) = \chi_\mathfrak{q}(-d) = \chi_\mathfrak{q}\left(\frac{-d}{q}\right)\chi_2\left(\frac{1}{q}\right)\prod_{\mathfrak{p}\in Q_1\cup Q_5\cup Q_7}\chi_\mathfrak{p}\left(\frac{1}{q}\right), \tag{11}$$

where the product again runs over primes $p\neq q$. Recall our second hypothesis of the strategy, that states that $\chi_\mathfrak{p} = \varepsilon_p\delta_p$ at odd primes, so we can replace in (11) to get

$$\chi(b_i^2) = \varepsilon_q(d)\left(\chi_2^{-1}(q)\varepsilon_q(-1)\varepsilon_2(q)\delta_q(2)^{v_2(d)}\right)\cdot\left(\delta_q(2)^{v_2(d)}\delta_q\left(\frac{-d}{q}\right)\prod_{\substack{p\in Q_1\cup Q_3\cup Q_5\cup Q_7\\ p\neq q}}\delta_p(q)\right). \tag{12}$$

If $q\equiv 1 \pmod 4$, the product involving the quadratic character δ_* is 1 by quadratic reciprocity, while if $q\equiv 3 \pmod 4$ it equals $(-1)^{\#Q_3+\#Q_7}$. We can write this as $\delta_{-1}(q)^{\#Q_3+\#Q_7}$. Note that $\delta_q(2) = \delta_2(q)$. The following identity holds from the definition of ε_2 and (8):

$$\chi_2^{-1}\cdot\varepsilon_2\cdot\delta_2^{v_2(d)}\cdot\delta_{-1}^{\#Q_3+\#Q_7} = \delta_2. \tag{13}$$

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

At last, we need to prove that ${}^\tau\chi = \chi\cdot\psi_{-2}\circ\mathcal{N}$ on $\mathbb{I}_k$, and by the previous results, it is enough to prove it for the idèles a_i. Note that $\tau(a_i)$ is the idéle of K with value q_i at $\overline{\mathfrak{q}_\mathfrak{i}}$ and 1 at the other places. Then

$${}^\tau\chi(a_i) = \chi(\tau(a_i)) = \chi(a_i)^{-1}\chi(a_i\tau(a_i)) = \chi(a_i)^{-1}\chi\left(\frac{a_i\tau(a_i)}{q_i}\right), \tag{14}$$

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

$$\chi\left(\frac{a_i\tau(a_i)}{q_i}\right) = \chi_2(q_i)^{-1}\prod_{\mathfrak{p}\in Q_1\cup Q_5\cup Q_7}\chi_\mathfrak{p}(q_i)^{-1} \tag{15}$$

By the product formula,

$$1 = \varepsilon(q_i) = \varepsilon_{q_i}(q_i)\varepsilon_2(q_i) \prod_{p \in Q_3 \cup Q_5} \varepsilon_p(q_i). \tag{16}$$

Since $\varepsilon_{q_i}(q_i) = \varepsilon(\mathcal{N}(a_i)) = \chi^2(a_i)$, multiplying (15) and (16) and using the second property of our general strategy, we get that

$$\chi\left(\frac{a_i\tau(a_i)}{q_i}\right) = \chi^2(a_i)\chi_2(q_i)^{-1}\varepsilon_2(q_i) \prod_{p \in Q_1 \cup Q_3 \cup Q_5 \cup Q_7} \delta_p(q_i). \tag{17}$$

Recall that q_i splits in K, hence $\left(\frac{-d}{q_i}\right) = 1$ so by reciprocity

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

From a similar computation, $\psi_{-2}(\mathcal{N}(a_i)) = \delta_{-2}(q_i)$, and the result follows from (13),

□

Remark 2. The character χ is not unique, but the last condition implies that the quotient of two such characters is a character of $\mathrm{Gal}_{\mathbb{Q}}$, hence all of them differ from χ by a character of $\mathrm{Gal}_{\mathbb{Q}}$.

Remark 3. Let p be an odd prime ramified in $K/\mathbb{Q}$. The equality ${}^{\tau}\chi = \chi \cdot \psi_{-2} \circ \mathcal{N}$ at the idèle whose p-th component is $\sqrt{-d}$ (a local uniformizer) implies that $\chi_{\mathfrak{p}}(-1) = \delta_2(p)$. This implies that any χ must ramify at primes in Q_5 and Q_7. This is also clear from the previous remark, as in our construction χ is ramified at primes of $Q_1 \cup Q_5 \cup Q_7$, where its local component at primes of $Q_5 \cup Q_7$ is not a square, hence multiplying χ by a character of $\mathbb{Q}$ cannot kill the ramification in such sets. Note also that any character ε must ramify at primes in $Q_3 \cup Q_5$ by a similar argument.

Remark 4. If $p \in Q_1$, we can twist χ by an order 4 character, and make it unramified at primes in Q_1 at the cost of adding a quadratic contribution to ε. So we can make χ ramify in $Q_5 \cup Q_7$ and ε ramify in $Q_1 \cup Q_3 \cup Q_5$; the ramification at primes in Q_1 and Q_3 being given by a quadratic character.

Remark 5. The conductor $\mathfrak{f}$ of $\chi_{\mathfrak{p}}$ for $\mathfrak{q} \mid 2$ has valuation:

$$v(\mathfrak{f}) = \begin{cases} 5 & \text{if } d \equiv 1 \pmod 8, \\ 3 & \text{if } d \equiv 3 \pmod 8, \\ 3 & \text{if } d \equiv 5 \pmod 8, \\ 0 & \text{if } d \equiv 2 \pmod 8 \text{ and } 2 \mid \#Q_3 + \#Q_5, \\ 4 & \text{if } d \equiv 2 \pmod 8 \text{ and } 2 \nmid \#Q_3 + \#Q_5, \\ 3 & \text{if } d \equiv 6 \pmod 8 \text{ and } 2 \mid \#Q_3 + \#Q_5, \\ 4 & \text{if } d \equiv 6 \pmod 8 \text{ and } 2 \nmid \#Q_3 + \#Q_5, \end{cases}$$

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

A result similar to Theorem 2.1 holds for real quadratic fields, where an extra condition at the archimedean places needs to be imposed.

Theorem 2.2. *Suppose that $K = \mathbb{Q}(\sqrt{d})$ is a real quadratic field, whose fundamental unit has norm -1. Then the same results of the last theorem hold.*

Proof. Since we prioritize the imaginary quadratic field, to take advantage of the previous cases, write $d = -(-d)$ (so $d < 0$ in the above notations/definitions) and take precisely the same local definitions for both ε and χ.

There are two important facts to consider: while proving (9), we get a -1 factor coming from the fact that we change $d \leftrightarrow -d$, hence we need to add ramification at one of the archimedean places (we will later specify which one).

Let ϵ be a fundamental unit (fixed). The proof works mutatis mutandis once we checked the compatibility of χ at ϵ. The advantage of assuming ϵ has norm -1, is that $Q_3 = Q_7 = \emptyset$ (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 for 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 2.3) $\#Q_5$ is odd, 2 is inert and 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 2.3, 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 positive 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 the imaginary quadratic case applies. □

For general real quadratic fields, the computation is more subtle, and it involves studying many different cases. For example, if $K = \mathbb{Q}(\sqrt{195})$, the positive fundamental unit equals $\epsilon = 14 - \sqrt{195}$. It reduces to 1 modulo (the prime in K dividing) 13, while to -1 modulo 3 and 5. Its reduction modulo 8 (although $d \equiv 3 \pmod 8$ in the previous computations it corresponds to the value $d = 5$) equals $\sqrt{195}^3(1 + 2\sqrt{195})^3$ then the previous definitions give that $\chi_{13}(\epsilon) = 1$, $\chi_5(\epsilon) = -1$, $\chi_3(\epsilon) = 1$ and $\chi_2(\epsilon) = 1$ hence the compatibility condition is not fulfilled independently of our definition at the archimedean places.

It is important to remark that we run some numerical experiments with real quadratic fields (a couple of hundreds) and in all cases, a character of the expected conductor is found. In a sequel we will explain how to compute the Hecke character for real quadratic fields and use them to solve our equations for some negative values of d.

Theorem 2.3. *Suppose that $K/\mathbb{Q}$ is imaginary quadratic. Then the twisted representation $\rho_{E,p}\otimes\chi$ descends to a 2-dimensional representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ attached to a newform of weight 2, Nebentypus ε, level N given by*

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

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

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

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

Proof. As was mentioned before, the result follows mostly by Ribet's theorem, but we give an alternative proof based on Galois representations (which is well known to experts) to get the full statement.

Let ρ denote $\rho_{E,p}\otimes\chi$. Its conductor equals $\mathrm{lcm}\{N_E, \mathrm{cond}(\chi)^2\}$ and its Nebentypus matches ε restricted to Gal_K (by the first claim of Theorem 2.1). Let τ be as in Theorem 2.1 (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.

Let ρ^τ denote the Galois representation $\rho^\tau(\sigma) = \rho(\tau\sigma\tau^{-1})$. Our hypothesis implies that ρ and ρ^τ are isomorphic (as they have the same trace at Frobenius elements). In particular, there exists $A \in \mathrm{GL}_2(\mathbb{Q}_p)$ such that $\rho = A\rho^\tau A^{-1}$. Furthermore, since ρ is irreducible (as E does not have complex conjugation) the matrix A is unique up to a scalar. The equality $\rho(\sigma) = \rho^{\tau^2}(\sigma) = A^2\rho(\sigma)A^{-2}$ implies that $A^2 = \lambda$ (a scalar).

If such an extension exists, say $\tilde\rho : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$, then $\tilde\rho(\tau\sigma\tau^{-1}) = \tilde\rho(\tau)\tilde\rho(\sigma)\tilde\rho(\tau)^{-1}$. In particular, if $\sigma \in \mathrm{Gal}_K$, $\rho^\tau(\sigma) = \tilde\rho(\tau\sigma\tau^{-1}) = \tilde\rho(\tau)\rho(\sigma)\tilde\rho(\tau)^{-1}$, so $\tilde\rho(\tau) = \mu A$. Since $\tilde\rho^2(\tau) = \rho(\tau^2) = 1$, $\mu^2 = \frac{1}{\lambda}$. It is easy to verify that defining $\tilde\rho(\tau) = \frac{1}{\sqrt{\lambda}}A$ gives an extension (the two choices of the square root give the two possible extensions, namely one and its twist by the quadratic character attached to the extension $K/\mathbb{Q}$).

Since any extension is odd, $\det(\tilde\rho)(\tau) = -1 = \varepsilon(\tau)\chi_p(\tau)$ (where χ_p denotes the cyclotomic character) giving the Nebentypus claim. Modularity of the representation follows from Serre's conjectures ([KW10][KW09]).

The conductor exponent of the representation $\tilde{\rho}$, at primes q which are unramified in $K/\mathbb{Q}$ equals that of $\rho_{E,p} \otimes \chi$. Let us postpone the case $q = 2$ and consider primes ramifying in $K/\mathbb{Q}$. Let $\mathfrak{q}$ be such a prime, and consider the local representation $\mathrm{Ind}_{G_{K_\mathfrak{q}}}^{G_{\mathbb{Q}_q}}(\rho_{E,p}|_{G_{K_\mathfrak{q}}} \otimes \chi_\mathfrak{q}) = \tilde{\rho}|_{G_{K_\mathfrak{q}}} \oplus (\tilde{\rho}|_{G_{K_\mathfrak{q}}} \otimes \mu_{K_\mathfrak{q}})$, where $\mu_{K_\mathfrak{q}}$ is the quadratic character giving the extension $K_\mathfrak{q}/\mathbb{Q}_q$. Recall the well known formula (see for example Theorem 8.2 of [Hen79])

$$v_q(\mathrm{Ind}_{G_{K_\mathfrak{q}}}^{G_{\mathbb{Q}_q}}(\rho_{E,p}|_{G_{K_\mathfrak{q}}} \otimes \chi_\mathfrak{q})) = f(K_\mathfrak{p}/\mathbb{Q}_p)(2\delta(K_\mathfrak{q}/\mathbb{Q}_q) + v_\mathfrak{q}(\rho_{E,p}|_{G_{K_\mathfrak{q}}} \otimes \chi_\mathfrak{q})), \tag{18}$$

where $\delta(K_\mathfrak{q}/\mathbb{Q}_q)$ denotes the $\mathfrak{q}$-valuation of the different. Recall that $\chi_\mathfrak{q}$ is unramified for $q \in Q_3$ and of conductor $\mathfrak{q}$ for $q \in Q_1 \cup Q_5 \cup Q_7$. The conductor of $\tilde{\rho}|_{G_{K_\mathfrak{q}}}$ equals that of its twist (which is clear for primes not in Q_3 and for primes in Q_3 follow from the fact that its Nebentypus equals $\varepsilon_\mathfrak{q} = \mu_{K_\mathfrak{q}}$, so both parts are ramified) proving the level formula.

The value of e follows from Lemma 1.4 and the formula (18). Note that the conductor of χ_2 (see Remark 5) has valuation too small to affect the conductor of the twisted representation when 2 is inert or ramified. In the split case, say $2 = \mathfrak{p}\bar{\mathfrak{p}}$ we chose the local character $\chi_{\mathfrak{p}_2}$ so that the twist of E by $\chi_\mathfrak{p}$ has split multiplicative reduction of conductor $\mathfrak{p}$ (recall that there were two possible definitions for $\chi_\mathfrak{p}$) to get the result. □

Remark 6. The coefficient field can be computed from the following observation: if p is a prime inert in $K/\mathbb{Q}$ then $\mathrm{Tr}(\tilde{\rho}(\mathrm{Frob}_p))^2 = a_p(E)\chi(\mathrm{Frob}_p) + 2\varepsilon(\mathrm{Frob}_p)p$.

Remark 7. If K is real quadratic the same proof gives an extension, but we cannot prove whether the Nebentypus equals ε or $\varepsilon\mu_K$. For imaginary quadratic fields, knowing that $\tilde{\rho}$ is odd allows us to distinguish the character (which is why we define ε to be even), but we do not know how to distinguish between the two ones for real quadratic fields.

3. Relation with Ribet's approach

Suppose $K/\mathbb{Q}$ is imaginary quadratic (so $d > 0$). Let $L = \mathbb{Q}(\sqrt{-d}, \sqrt{-2})$. The curve E, its Galois conjugates and the isogenies are all defined over L. Let $\{\sigma_d, \sigma_2\}$ be the generators for $\mathrm{Gal}(L/\mathbb{Q})$ given by $\sigma_d(\sqrt{-d}) = -\sqrt{-d}$, $\sigma_d(\sqrt{-2}) = \sqrt{-2}$ and $\sigma_2(\sqrt{-d}) = \sqrt{-d}$, $\sigma_2(\sqrt{-2}) = -\sqrt{-2}$.

Since E does not have complex multiplication, one can attach to E a 2-cocycle. For each $\tau \in \mathrm{Gal}(L/\mathbb{Q})$ let $\phi_\tau : E^\tau \to E$ be an isogeny, and define $c(\tau, \tau') = \phi_\tau \circ {}^\tau\phi_{\tau'} \circ \phi_{\tau\tau'}^{-1}$, where ${}^\tau\phi_{\tau'} : (E^{\tau'})^\tau \to E^\tau$ is the isogeny obtained by applying τ to $\phi_{\tau'}$. All the endomorphisms considered are in $\mathrm{End}(E) \otimes \mathbb{Q}$ (hence the inverse means the dual isogeny divided by its degree).

The cocycle c does not depend on the choice of isogenies (up to a coboundary). In our case, taking ϕ_1, ϕ_{σ_2} as the identity, and $\phi_{\sigma_d}, \phi_{\sigma_d\sigma_2}$ as the 2-isogeny described before, the values of c are given in Table 3.1 (which matches Pyla's example in page 49 of her Ph.D. thesis). Let $\mathrm{Inf}(c) \in H^2(\mathrm{Gal}_\mathbb{Q}, \mathbb{Q}^\times)$ be the image

$c(\tau,\tau')$	1	σ_2	σ_d	$\sigma_2\sigma_d$
1	1	1	1	1
σ_2	1	1	−1	−1
σ_d	1	1	−2	−2
$\sigma_2\sigma_d$	1	1	2	2

Table 3.1. Table

of c under the inflation morphism. By a result of Quer (Proposition 2.1 of ([Que01]) $\mathrm{Inf}(c)$ belongs to the 2-torsion subgroup and has trivial image in $H^2(\mathrm{Gal}_\mathbb{Q}, \overline{\mathbb{Q}}^\times)$ (as the latter group is trivial by a result of Tate). In particular, to trivialize the cocycle, we need to enlarge the coefficient field (and our field L).

The cocycle $\mathrm{Inf}(c)$ can be decomposed into a sign part, and a "positive part" (see Section 3 of [Que00]). The sign part corresponds to the quaternion algebra $(-d, 2)$ (see Theorem 3.1 of [Que01]). The splitting character is then ramified at all primes where such algebra ramifies, namely the primes in $Q_3 \cup Q_5$ (as our character ε).

Let M be the extension of K corresponding (via class field theory) to χ. Then a splitting map is obtained over the Galois closure of $M/\mathbb{Q}$. Note that such Galois closure is obtained by composing M with the extension

corresponding to the character ${}^{\tau}\chi$, which equals $N = M(\sqrt{-2})$. Consider the following three cases (were in all of them N denotes the total extension).

3.1. **Case $Q_5 = Q_7 = \emptyset$.** Following Remark 4, we can take the quadratic character ε to correspond precisely to the real quadratic field $\mathbb{Q}(\sqrt{2d})$. The character χ has order 4 corresponding to a degree 4 extension M of K (which equals N). The third condition of Theorem 2.1 implies that the character ${}^{\tau}\chi$ is contained in the compositum of M and $\mathbb{Q}(\sqrt{-2})$. But $K(\sqrt{-2})$ equals the fixed field of χ^2, so $M/\mathbb{Q}$ is a Galois extension with Galois group isomorphic to D_4 (the dihedral group with 8 elements). In this case, we can even give an explicit construction of M. For each odd prime p dividing d, the hypothesis implies that p splits in $\mathbb{Q}(\sqrt{-2})$ (which has class number one).

Let $\mathfrak{p}$ be one of the two ideals appearing in the factorization of p over $\mathbb{Q}(\sqrt{-2})$ and let α_p be a generator. Let $\alpha_2 = \sqrt{-2}$ and let T be the quadratic extension of $\mathbb{Q}(\sqrt{-2})$ obtained by adding the element $\gamma = \sqrt{\prod_{p|d} \alpha_p \cdot \alpha_2}$. The Galois closure of T is the compositum of T with the quadratic extension $\tilde{T}$ of $\mathbb{Q}(\sqrt{-2})$ obtained by adding the element $\tilde{\gamma} = \sqrt{\prod_{p|d} \overline{\alpha_p} \cdot \overline{\alpha_2}}$ (see Figure 1). Such field contains the subextension

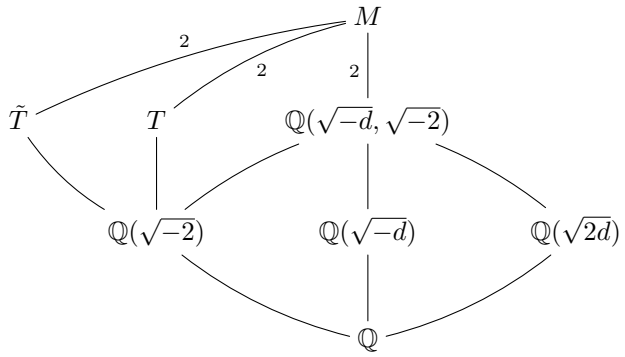

FIGURE 1. Field extension diagram

$\mathbb{Q}(\gamma\tilde{\gamma}) = \mathbb{Q}(\sqrt{2d})$ (recall that in this case the two different choices of ε correspond to the quadratic fields $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-2d})$). The Galois group $\mathrm{Gal}(M/\mathbb{Q}) \simeq D_4 = \langle \sigma, \tau \ : \ \sigma^4 = \tau^2 = 1, \tau\sigma = \sigma^3\tau \rangle$. The quadratic extension $\mathbb{Q}(\sqrt{-d})$ corresponds to the fixed field of σ (a normal subgroup of order 4). As explained in [Pyl04], in this case σ and τ restrict to our σ_2 and σ_d respectively, and a trivializing cocycle is given by the map $\beta : D_4 \to \bar{\mathbb{Q}}^{\times}$ given in Table 3.2. Note that the ambiguity in the choice of M (the choice of an ideal

g	1	σ	σ^2	σ^3	τ	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$
$\beta(g)$	1	$\sqrt{-1}$	-1	$-\sqrt{-1}$	$\sqrt{-2}$	$\sqrt{2}$	$-\sqrt{-2}$	$-\sqrt{2}$

TABLE 3.2. Trivializing cocycle case 3.1

above p for each $p \mid d$) corresponds to the fact that while constructing the character χ we took square roots. Different choices of the root give different fields M, and they differ by quadratic twists corresponding to the quadratic unramified extensions of K.

An easy computation proves that the Nebentypus attached to β matches $\varepsilon(\sigma)$ (see [Pyl04] page 52 for the details).

3.2. **Case $Q_5 = \emptyset$ but $Q_7 \neq \emptyset$.** As in the previous case, the character χ corresponds to a degree 4 extension M of K and ε to a real quadratic extension of $\mathbb{Q}$; let $\sqrt{n}$ denote a generator for it.

The third condition of Theorem 2.1 implies that $N = M(\sqrt{-2})$, so $N/\mathbb{Q}$ is a Galois extension of degree 16. Furthermore, N contains the fields $\mathbb{Q}(\sqrt{-d})$, $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{n})$. This implies that $\mathrm{Gal}(N/\mathbb{Q})$ is isomorphic to the central product of $D_4 \times \mathbb{Z}/4$ (also called the Pauli group url), equal to the direct product

of the two groups, identifying the order two rotation with the order two element of $\mathbb{Z}/4$, i.e. it can be given by $\mathrm{Gal}(N/\mathbb{Q}) \simeq \langle \sigma, \tau\, \mu \ : \ \sigma^4 = \tau^2 = 1, \tau\sigma = \sigma^3\tau, \sigma^2 = \mu^2, \sigma\mu = \mu\sigma, \tau\mu = \mu\tau \rangle$.

The group $D_4 \bowtie \mathbb{Z}/4$ has many automorphisms, hence we can make some choices on the presentation to identify fixed fields with subgroups. The extension $N/K \simeq \mathbb{Z}/2 \times \mathbb{Z}/4$, and we can assume it corresponds to the fixed field by $\langle \sigma, \mu \rangle$ (all other ones are related by outer automorphisms to it). Then $M = N^{\langle \sigma\mu \rangle}$, $K = N^{\langle \sigma, \mu \rangle}$, and $\mathbb{Q}(\sqrt{-d}, \sqrt{n}) = N^{\langle \sigma\mu, \sigma^2 \rangle}$. Figure 2 shows the field diagram extensions.

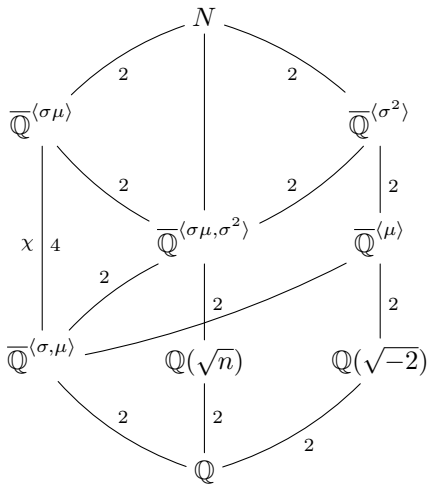

FIGURE 2. Field extension diagram

In particular, the following holds:

- $\sigma(\sqrt{-d}) = \sqrt{-d} = \mu(\sqrt{-d})$ and $\tau(\sqrt{-d}) = -\sqrt{-d}$ (hence τ can be taken as the generator for $\mathrm{Gal}(K/\mathbb{Q})$),
- The condition ${}^{\tau}\chi = \chi\psi_{-2}$ implies that ${}^{\tau}\chi(\sigma) = \chi(\tau\sigma\tau) = \chi(\sigma^3) = \chi(\sigma)\psi_{-2}(\sigma)$ hence $\psi_{-2}(\sigma) = -1$. In particular, $\sigma(\sqrt{-2}) = -\sqrt{-2}$ hence $\mu(\sqrt{-2}) = \sqrt{-2}$. Since the choice of the reflection is not unique, we can (and will) assume that $\tau(\sqrt{-2}) = -\sqrt{-2}$.

Then σ and τ restrict to our σ_2 and σ_d while μ restricts to the identity element in L. A map $\beta : \mathrm{Gal}(N/\mathbb{Q}) \to \bar{\mathbb{Q}}^{\times}$ trivializing the cocycle $\mathrm{Inf}(c)$ is given in Table 3.3. In fact, the map β satisfies that

g	1	σ	σ^2	σ^3	τ	μ	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$	$\sigma\mu$	$\sigma^2\mu$	$\sigma^3\mu$	$\mu\tau$	$\sigma\mu\tau$	$\sigma^2\mu\tau$	$\sigma^3\mu\tau$
$\beta(g)$	1	$\sqrt{-1}$	-1	$-\sqrt{-1}$	$\sqrt{-2}$	$\sqrt{-1}$	$\sqrt{2}$	$-\sqrt{-2}$	$-\sqrt{2}$	-1	$-\sqrt{-1}$	1	$-\sqrt{2}$	$\sqrt{-2}$	$\sqrt{2}$	$-\sqrt{-2}$

TABLE 3.3. Trivializing cocycle case 3.2

$$\beta(\sigma^i\tau^j\mu^k) = \tilde{\beta}(\sigma^i\tau^j)(\sqrt{-1})^k,$$

where $\tilde{\beta}$ equals the trivializing cocycle of the previous case.

3.3. **Case $Q_5 \neq \emptyset$.** The character ε has order 4 in this case, and χ order 8, so the extension $N/\mathbb{Q}$ order 32. The group $\mathrm{Gal}(N/\mathbb{Q})$ contains a quotient isomorphic to $\mathbb{Z}/4 \times \mathbb{Z}/2 \times \mathbb{Z}/2$ hence a little inspection between all groups of order 32 with such quotient shows that $\mathrm{Gal}(N/\mathbb{Q})$ is isomorphic to the central product of $D_4 \times \mathbb{Z}/8$ (url), which can be presented as $\langle \sigma, \tau, \mu \ : \ \sigma^4 = \tau^2 = \mu^8 = 1, \sigma\tau = \tau\sigma^3, \mu\sigma = \sigma\mu, \tau\mu = \mu\tau \rangle$.

The following facts hold: $N^{\langle \sigma\mu^2 \rangle} = M$, $N^{\langle \mu, \sigma \rangle} = K$ and $\mathrm{Gal}(N/K) = \langle \sigma, \mu \rangle \simeq \mathbb{Z}/8 \times \mathbb{Z}/2$. $N^{\langle \sigma^2 \rangle} = \overline{\mathbb{Q}}^{\varepsilon}(\sqrt{-d}, \sqrt{-2})$ and $N^{\langle \mu^2 \rangle}$ corresponds to the compositum of the three quadratic extensions. Figure 2 shows the field diagram extensions. Regarding restrictions to L, we have the following:

- $\sigma(\sqrt{-d}) = \sqrt{-d}$, $\mu(\sqrt{-d}) = \sqrt{-d}$ and $\tau(\sqrt{-d}) = -\sqrt{-d}$.

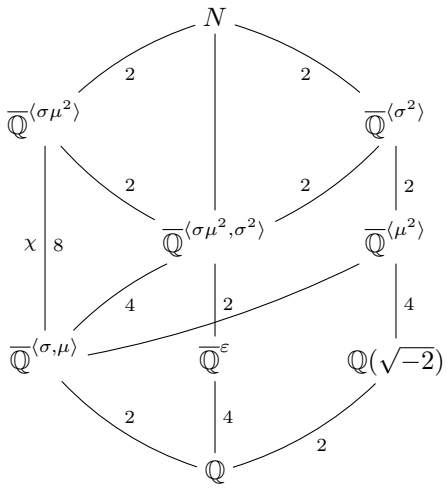

FIGURE 3. Field extension diagram

- $\sigma\mu^2(\sqrt{-2}) = -\sqrt{-2}$ hence $\sigma(\sqrt{-2}) = -\sqrt{-2}$ and the equality ${}^{\tau}\chi = \chi\psi_{-2}$ implies that $\mu(\sqrt{-2}) = \sqrt{-2}$ as in the previous case. Note that the choice of the reflection is not unique, hence we can assume that $\tau(\sqrt{-2}) = -\sqrt{-2}$.

With these choices, the restriction of σ and τ to L match σ_2 and σ_d respectively, while μ restricts to the identity. A map $\beta : \mathrm{Gal}(N/\mathbb{Q}) \to \overline{\mathbb{Q}}^{\times}$ that trivializes the cocycle $\mathrm{Inf}(c)$ is given by the formula:

$$\beta(\sigma^i\tau^j\mu^k) = \tilde{\beta}(\sigma^i\tau^j)\zeta_8^k,$$

for ζ_8 an primitive eighth root of unity, $0 \leq i \leq 3$, $0 \leq j \leq 1$, $0 \leq k \leq 3$ and $\tilde{\beta}$ as in Table 3.2.

4. Solving equation (1)

During this section we will assume that $K/\mathbb{Q}$ is imaginary quadratic. Theorem 2.3 implies that the representation $\tilde{\rho}_p$ equals that of a newform f in $S_2(N, \varepsilon)$ for a precise level N. Suppose that $p \nmid d$ (so that it does not ramify in $K/\mathbb{Q}$). If we can assure that $\tilde{\rho}_p$ has absolutely irreducible residual image, Lemma 1.2 implies that the form f satisfies the lowering the level hypothesis at primes $\mathfrak{q}$ dividing N_E but not dividing p. The *finite* hypothesis (to remove p also from the level) at $\mathfrak{p}$ for primes $\mathfrak{p} \mid p$ follows from the same argument given in [Ell04] (page 783) under our assumption that p does not ramify in $K/\mathbb{Q}$. Then by Ribet's lowering the level result (see [Rib91]) there exists an eigenform $g \in S_2(n, \varepsilon)$ where

$$n = 2^e \cdot \prod_{q \in Q_3} q \cdot \prod_{q \in Q_1 \cup Q_5 \cup Q_7} q^2, \tag{19}$$

where e is one of:

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

such that $\rho_{E,p} \equiv \rho_{g,K,p} \otimes \chi^{-1} \pmod{p}$, where $\rho_{g,K,p}$ is the restriction of the representation $\rho_{g,p}$ to the Galois group $\mathrm{Gal}_{\mathbb{Q}}$. Let us state two results on the big image hypothesis needed in Ribet's lowering the level result.

Theorem 4.1. *If (A, B, C) is a non-primitive solution such that C is supported at primes dividing 2 and 3 then there exists a bound N_K such that if $p > N_K$ the representation $\rho_{E_{A,B},p}$ has absolutely irreducible image.*

Proof. The proof is similar to [DU09] (case (ii)). Recall that E has at most multiplicative reduction at primes dividing 3. The case $C = \pm 1$ (a unit) corresponds to the trivial solutions $(\pm 1, 0, \pm 1)$. Suppose then that $C = 2^\alpha 3^\beta$. Recall that if 3 is ramified in $K/\mathbb{Q}$ then $\beta = 0$ by Lemma 1.3. The curve E has conductor $2^a \cdot 3^b$, where $a \leq 12$, $b \leq 1$ and $N_{\tilde{\rho}} = 2^s \cdot 3 \cdot \prod_{q \in Q_3} q \cdot \prod_{q \in Q_1 \cup Q_5 \cup Q_7} q^2$, where $s \leq 9$ by Theorem 2.3. Suppose that the residual image of $\tilde{\rho}_p$ is reducible, i.e.

$$\overline{\tilde{\rho}_p}^{s.s} \simeq \nu \oplus \varepsilon \nu^{-1} \overline{\chi}_{\text{cyc}}, \tag{20}$$

where χ_{cyc} denotes the cyclotomic character. If $3 \mid C$, it is unramified in $K/\mathbb{Q}$ hence it does not divide the conductor of ε and it cannot divide the conductor of ν either.

Let $\tilde{d} = \frac{d}{2^{v_2(d)}}$ (i.e. the prime to 2 part of d), hence $\text{cond}(\nu) \mid 2^4 \cdot \tilde{d}$ and if a prime q in Q_3 divides the conductor of ν, $\nu_q = \varepsilon_q$ (quadratic). Let ℓ be a prime such that $\ell \equiv 1 \pmod{16\tilde{d}}$; in particular, ℓ splits in $K/\mathbb{Q}$, say $\ell = \mathfrak{l}\bar{\mathfrak{l}}$. Then $\tilde{\rho}_p(\text{Frob}_\ell) = a_\mathfrak{l}\chi(\mathfrak{l})$ is an integer (as the form has an inner twist) and satisfies $|a_\mathfrak{l}| \leq 2\sqrt{\ell}$, but (20) and our assumption on ℓ implies that it is congruent to $\ell + 1$, so $p \mid \ell + 1 - a_\mathfrak{l}\chi(\mathfrak{l})$ (which is non-zero), hence for $p > 2\sqrt{\ell} + \ell + 1$ no such reducible representation can exist. □

Remark 8. The constant N_K depends on the first prime 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.

The previous result is needed to discard solutions that might correspond to elliptic curves with complex multiplication.

Remark 9. While working with equation (1), the value C of a primitive solution could be even only when $d \equiv 7 \pmod 8$ (if $p > 3$). In such a case, the proof of Lemma 1.4 implies that the level valuation of the newform g at the prime 2 equals 1 and ε is unramified at 2, hence the form g has a prime of multiplicative reduction. In particular, it cannot correspond to a form with complex multiplication and we are led to consider the case when C happens to be divisible only by the prime 3. The newform g obtained after applying Ribet's lowering the level result to the curve E must be in the raising the level hypothesis, so $N(\varepsilon^{-1}(3)(3+1)^2 - a_3(g)^2)$ must be divisible by p.

Assume on the contrary that there exists an odd prime $\mathfrak{p}$ dividing C and not dividing 3. By Lemma 1.3 we know that primes dividing $\Delta(E)$ are not ramified in $K/\mathbb{Q}$ and by Lemma 1.5 they have multiplicative reduction. In particular E does not have complex multiplication and we are in the hypothesis of Ellenberg's big image result ([Ell04, Theorem 3.14]).

Theorem 4.2 (Ellenberg)**.** *Given d, if the curve E is a $\mathbb{Q}$-curve and does not have complex multiplication, there exists an integer N_d such that the projective image of the residual representation of $\rho_{E,p}$ is surjective for all primes $\mathfrak{p}$ of norm greater than N_d.*

In [Ell04] it is explained how to get an explicit bound for N_d. Concretely, let N be a 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 Ellenberg's result states that for any prime p for which

$$(a_1, L_\chi)_{p^2}^{p-\text{new}} = (a_1, L_\chi)_{p^2} - p(p^2-1)^{-1}(a_1 - p^{-1}\chi(p)a_p, L_\chi)_p \tag{21}$$

is non-zero, the residual image is large for p. Then one is left to bound the previous contributions. The main term comes from the first term. In [Ell05] (Theorem 1) a formula to compute $(a_1, L_\chi)_{p^2}$ is given, written as

$$(a_1, L_\chi)_{p^2} = 4\pi e^{-2\pi/\sigma N log(N)} - E^{(3)} + E_3 - E_2 - E_1 + (a_1, B(\sigma N \log(N))),$$

where σ is taken to be $\frac{q^2}{2\pi}$ (as in [DU09]) and $N = p^2$. The main contribution comes from the first term (close to 4π) and in Ellenberg's article a bound for all other terms is given. In [DU09] (see the proof of Lemma 8, which we followed closely) is shown how to use the bounds to compute an explicit value of N_d. In particular (following their notation) to bound $E^{(3)}$ one splits the sum depending on whether $c \leq p^4$ or

$c > p^4$ (we remark this as there is a typo in such article since c should be p^2c). All given bounds decrease with p, hence evaluating them at a good candidate is enough to get the result (for all greater values). Taking the bounds corresponding to the contributions of the other terms of (21) exactly as in Lemma 3.13 [Ell04] allows to make N_d explicit.

Our examples cover only the cases $d = 1, 2, 3, 5, 6, 7$ of conductors $4, 8, 3, 20, 24, 7$ respectively.

Proposition 4.3. *The bound N_d in Ellenberg's result can be taken as: $N_2 = 353$, $N_3 = 137$, $N_5 = 439$, $N_6 = 569$ and $N_7 = 137$.*

Proof. Follows from the previous discussion and an implementation of the bounds in [DU09] for a general value of $\mathfrak{f}$ (implemented in Pari/GP [PAR19]). □

Remark 10. The previous bound can be improved by a finite computation for the smaller values of p as follows: if there exists a newform $f \in S_2(\Gamma_0(d'p^2))$, where $d' \mid d$ (recall that $K = \mathbb{Q}(\sqrt{-d})$) satisfying one of

- $d' = d$, $w_p f = f$ and $w_d f = -d$ or
- $d' < d$, $w_p f = f$,

and such that $L(f, \chi)$ is non-zero then Theorem 4.2 holds for p. In [Kou20, Proposition 5.4] it is proven that $N_3 = 11$ via searching for such an f for all small values of p. Running the same script for the other fields proves that $N_d = 11$ in all other cases as well.

If $p > \max\{N_d, N_K\}$, we can apply Ribet's lowering the level result, and the curve E will be congruent modulo p to a form $g \in S_2(n, \varepsilon)$ with n as in (19). We compute the space of such forms and try to discard all forms in such space. First we discard all forms with complex multiplication (Theorem 4.1 implies the curve has a multiplicative prime and then Ellenberg's result implies the projective image is surjective, hence it cannot be congruent to a form with complex multiplication, whose image is contained in the normalizer of a non-split Cartan group) and we try to discard the remaining ones using Mazur's trick (see Lemma 7.2 of [cS18]).

Proposition 4.4 (Mazur's trick)**.** *Let $g \in S(n, \varepsilon)$ be such that $\rho_{E,p} \otimes \chi \equiv \rho_{g,K,p} \pmod{p}$. Let $q \neq p$ be a rational prime with $q \nmid n$. Let*

$$B(q,g) = \begin{cases} N(a_q(E)\chi(q) - a_q(g)) & \text{if } A^4 + dB^2 \not\equiv 0 \pmod q \text{ and } \left(\frac{-d}{q}\right) = 1, \\ N(a_q(g)^2 - a_q(E)\chi(q) - 2q\varepsilon(q)) & \text{if } A^4 + dB^2 \not\equiv 0 \pmod q \text{ and } \left(\frac{-d}{q}\right) = -1, \\ N(\varepsilon^{-1}(q)(q+1)^2 - a_q(g)^2) & \text{if } A^4 + dB^2 \equiv 0 \pmod q. \end{cases}$$

Then $p \mid B(q, f)$.

Proof. The first case corresponds to a split prime (in such case the decomposition groups over $\mathbb{Q}$ and over K are the same), the second corresponds to an inert prime (where the formula is well known) and the last one corresponds to a case of "lowering the level", were the formula corresponds to Ribet's condition. □

Then we compute some values of

$$C(q,g) = \prod_{\substack{(A,B)\in\mathbb{F}_q^2 \\ (A,B)\neq(0,0)}} B(q,g),$$

and compute the set of common prime divisors, obtaining a bound for p. At last, if some form passes both checks, we compare the "local type" of it and that of the representation $\rho_{E,p}$, knowing that two congruent forms must have the same restriction to inertia (modulo p). In most cases this "tests" are enough to discard all candidates g.

4.1. **Some cases of (1).** In this section we apply the previous results to solve some cases of equation (1) (and provide references to the cases studied before).

4.1.1. *The equation $x^4 + dy^2 = z^p$, with $d = 1, 2, 3$.* These cases were considered in the articles [Ell04], [BEN10] and [DU09].

4.1.2. *The equation* $x^4 + 5y^2 = z^p$. In this case ε is a character of order 4 and conductor $4 \cdot 5$, hence χ has order 8. The form g attached to a solution lies in one of the spaces $S_2(2^6 \cdot 5^2, \varepsilon)$ or $S_2(2^7 \cdot 5^2, \varepsilon)$.

The space $S_2(2^6 \cdot 5^2, \varepsilon)$ has 22 conjugacy classes, five of them with CM while the space $S_2(2^7 \cdot 5^2, \varepsilon)$ has 12 conjugacy classes, none of them with CM. Computing $C(q, g)$ for $q = 7, 11, 13$ we can discard all forms without CM in both spaces for $p > 17$. If C is divisible by a prime greater than 3 then Ellenberg's result implies that our form cannot have CM (discarding the remaining ones). Clearly C cannot be odd, as otherwise looking modulo 8, $C \equiv 6 \pmod 8$ (hence is not a p-th power). If C is a power of 3, then the CM forms should satisfy the raising the level hypothesis, in particular $p \mid N(16\varepsilon^{-1}(3) - a_3(g)^2)$, which does not occur if $p > 13$.

Theorem 4.5. *Let $p > 273$ be a prime number. Then there are no non-trivial solutions of the equation*

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

Proof. The prime $\ell = 241$ can be used in the proof of Theorem 4.1, giving the bound $N_K = 273$. Since $N_5 = 11$ (by Proposition 4.3 and Remark 10) the above argument gives the result. □

4.1.3. *The equation* $x^4 + 6y^2 = z^p$. In this case ε is a character of conductor $4 \cdot 3$ and order 2 whereas χ has order 4. The form g attached to a non-trivial solution lies in one of $S_2(2^8 \cdot 3, \varepsilon)$ or $S_2(2^9 \cdot 3, \varepsilon)$. Note that if (A, B, C) is a primitive solution, C is prime to 6 hence we are always in Ellenberg's hypothesis (namely C is divisible by a prime greater than 3).

The space $S_2(2^8 \cdot 3, \varepsilon)$ has 10 conjugacy classes. Six of them have CM. An easy computation of $C(5, g)$ shows that we can discard the four forms without CM for $p > 7$.

The space $S_2(2^9 \cdot 3, \varepsilon)$ has 13 conjugacy classes and three of them have CM. Mazur's trick for $q = 13$ allows us to discard all the non-CM forms for $p > 383$. Computing also $C(23, g)$, $C(29, g)$ and $C(31, g)$ we can decrease the bound so the result still works for $p > 19$. Notice that in this case there exists a near solution, like

$$11^4 + 6 \cdot 19^2 = 7^5$$

hence a strong version would at most hold for $p \geq 7$ (although we did not try to reach such a small bound).

Theorem 4.6. *Let $p > 19$ be a prime number. Then there are no non-trivial solutions of the equation*

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

Proof. Note that we do not have to use Theorem 4.1 because d is already divisible by 6 hence $\gcd(6, C) = 1$. Since $N_6 = 11$ (by Proposition 4.3 and Remark 10) the result follows. □

4.1.4. *The equation* $x^4 + 7y^2 = z^p$. The character ε is trivial while the character χ is the quadratic even character of conductor $7 \cdot 8$. The newform g attached to a solution has trivial Nebentypus and (by Theorem 2.3) level $2 \cdot 7^2$ or $2^8 \cdot 7^2$. Before discarding forms, note that any primitive solution corresponds to a value of C prime to 3 (as $3 \mid x^4 + 7y^2$ if and only if $3 \mid x$ and $3 \mid y$). Remark 9 imples that C cannot be even, hence the curve E contains a prime of multiplicative reduction (so Ellenberg's result applies).

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 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. 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 solution of our equation.

The space $S_2(\Gamma_0(2 \cdot 7^2))$ has 2 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 $x^2 - 2x - 7$. Mazur's trick with $q = 3$ discards the rational form for $p > 2$. The second form cannot be discarded using Mazur's trick, as it corresponds to an elliptic curve matching our requirements. 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 $\sqrt{-7}$). If we compute it with magma, it shows that the local component is supercuspidal, but induced from an order 8 character of the unramified quadratic extension of $\mathbb{Q}_7$, hence it does not match that of our elliptic curve (induced from an order 4 character of the same extension).

The space $S_2(\Gamma_0(2^8 \cdot 7^2))$ has 98 conjugacy classes, 17 of them being rational. After eliminating the 30 forms with CM, we can discard all of the rational forms using the Mazur's trick with $q = 3$. The remainders forms are harder to eliminate but it can be done for $p > 53$ by computing $C(q, g)$ for $q = 3, 5, 17, 31$.

Theorem 4.7. *Let $p > 137$ be a prime number. Then there are no non-trivial solutions of the equation*

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

Proof. The result follows taking $\ell = 113$ in Theorem 4.1, using the bound $N_7 = 11$ (by Proposition 4.3) and the previous analysis. □

5. The equation (3): properties of the curve $\widetilde{E}$

The construction of the Frey curve in [BC12] does not show explicitly the 3-isogeny. Knowing that our curve will have a 3-torsion point, it makes sense to start with the parametrized family of elliptic curves having a 3-torsion point as given by Kubert in [Kub76, Table 1]: such curves 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. The curve E has discriminant $a_3^3(a_1^3 - 27a_3)$. Its 3-isogenous curve has equation

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

with discriminant $a_3(a_1^3 - 27a_3)^3$. To a solution (A, B, C) of (3), we attach the elliptic curve:

$$\widetilde{E}_{(A,B)} : y^2 + 6B\sqrt{-d}xy - 4d(A + B^3\sqrt{-d})y = x^3. \tag{22}$$

The discriminant of $\widetilde{E}$ equals $-2^8 3^3 d^4 C^p (A + B^3\sqrt{-d})^2$ and its j-invariant $\frac{2^4 3^3 B^3\sqrt{-d}(4A-5B^3\sqrt{-d})^3}{C^p(A+B^3\sqrt{-d})^2}$.

The quadratic twist by $\sqrt{-3}$ of $\widetilde{E}_{(A,B)}$ corresponds to the equation

$$\begin{aligned} y^2 + 6B\sqrt{-d}xy + 12d(-A + B^3\sqrt{-d})y = x^3 + 36B^2dx^2 + \\ (144ABd\sqrt{-d} + 144B^4d^2)x + 288AB^3d^2\sqrt{-d} + 144B^6d^3 - 144A^2d^2. \end{aligned} \tag{23}$$

The quotient $\widetilde{E}_{(A,B)}$ by $\langle(0, 0)\rangle$ (a curve 3-isogenous to $\widetilde{E}_{(A,B)}$) has equation

$$\begin{aligned} y^2 + 6B\sqrt{-d}xy - 4d(A + B^3\sqrt{-d})y = x^3 + \\ (-120B^4d^2 + 120ABd\sqrt{-d})x + 976B^6d^3 - 1088AB^3d^2\sqrt{-d} - 112A^2d^2. \end{aligned} \tag{24}$$

Via the usual change of variables (making $a_1 = a_3 = a_2 = 0$) it is easy to check that both (23) and (24) 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, the Galois conjugate of $\widetilde{E}_{(A,B)}$ is isomorphic to the quadratic twist by $\sqrt{-3}$ of the quotient $\widetilde{E}_{(A,B))}/\langle(0, 0)\rangle$, hence a $\mathbb{Q}$-curve.

As in section (1), there are some basic results that $\widetilde{E}_{(A,B)}$ must satisfy. Again, we will denote $\widetilde{E} = \widetilde{E}_{(A,B)}$. Lemma (1.1) holds exactly the same, while we have to modified a little the others, namely:

Lemma 5.1. *Let $\mathfrak{q}$ be a prime of K such that $\mathfrak{q} \nmid 6d$. Then $v_{\mathfrak{q}}(\Delta(\widetilde{E})) \equiv 0 \pmod{p}$.*

Proof. Clear from the value of $\Delta(\widetilde{E})$. □

It is also clear that if $\mathfrak{q} \mid \Delta(\tilde{E})$ and $\mathfrak{q} \nmid 6d$ then $\tilde{E}$ has multiplicative reduction at $\mathfrak{q}$.

Lemma 5.2. *Suppose that p is an odd rational prime ramified at $K/\mathbb{Q}$ and let $\mathfrak{p}$ denote the (unique) prime in K dividing p. Then $v_{\mathfrak{p}}(\Delta(\widetilde{E})) = 8 + 3v_{\mathfrak{p}}(3)$.*

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

Remark 11. The curve $\tilde{E}$ has bad additive reduction at all odd primes 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 it 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 $N_{\widetilde{E}}$ denote the conductor of $\widetilde{E}$ and suppose that $p > 3$.

Lemma 5.3. *Let $\mathfrak{q}$ be a prime ideal of K dividing 2. Then:*

(1) If 2 is inert in $K/\mathbb{Q}$ then $\tilde{E}$ has type IV* *at $\mathfrak{q}$ with $v_{\mathfrak{q}}(N_{\widetilde{E}}) = 2$.*
(2) If 2 is split in $K/\mathbb{Q}$ then $v_{\mathfrak{q}}(N_{\widetilde{E}}) = 1, 2$ at both primes above 2.
(3) If 2 ramified in $K/\mathbb{Q}$ but $2 \nmid d$ then $\tilde{E}$ has reduction type IV *at $\mathfrak{q}$ with $v_{\mathfrak{q}}(N_{\widetilde{E}}) = 2$.*
(4) If $2 \mid d$ then $\widetilde{E}$ has good reduction at $\mathfrak{q}$.

Proof. Consider each case separately:

- If 2 is inert, $2 \nmid C$ (since $C \equiv A^2 + 3B^6$ which is never divisible by 8 which contradicts our assumption $p > 3$). Clearly $2 \mid b_2$, $4 \mid a_6$, $8 \mid b_8$ 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 $v_2(\Delta) - 6 = 2$.
- Suppose that 2 splits and let $\mathfrak{q}$ 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, $v_{\mathfrak{p}}(a_1) \geq 1$ and $v_{\mathfrak{p}}(a_3) = 2$ hence we are again in Step 8 of Tate's algorithm (type IV*) hence the conductor exponent is 2. On the other hand, if both A and B are odd, the model is not minimal, as $v_{\mathfrak{p}}(a_1) = 1$ 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 I_n. In particular, its conductor exponent equals 1.
- 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 $v_\pi(\tilde{\Delta}) - 2 = 2$.
- 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.

□

In particular, C can be even only if 2 splits in $K/\mathbb{Q}$. Suppose that $p \geq 5$.

Lemma 5.4. *Let $\mathfrak{q}$ be a prime ideal of K dividing 3.*

(1) If 3 is inert in K then $v_3(N_{\widetilde{E}}) \in \{2, 3\}$.
(2) If $3 = \mathfrak{q}_3\bar{\mathfrak{q}}_3$ in K then $v_{\mathfrak{q}_3}(N_{\widetilde{E}}) = v_{\bar{\mathfrak{q}}_3}(N_{\widetilde{E}}) \in \{2, 3\}$ or $v_{\mathfrak{q}_3}(N_{\widetilde{E}}) = 2$ and $v_{\bar{\mathfrak{q}}_3}(N_{\widetilde{E}}) = 1$.
(3) If 3 ramifies in K then $v_{\mathfrak{q}}(N_{\widetilde{E}}) = 8$.

Proof. Let's consider the different cases:

- 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 $\tilde{E}$ (to easy notation). Then the model becomes

$$y^2 + a_1xy + (3a_3 - a_1a_3^6)y = x^3 - 3a_3^6x^2 - a_1a_3x + (a_1a_3^7 - a_3^{18} - 2a_3^2). \tag{25}$$

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 $9 \nmid a_1 a_3^7 - a_3^{18} - 2a_3^2$ 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 $-4a_1^2 a_3^{18} + 6a_1 a_3^{13} + 12a_3^{24} - 3a_3^8$. 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.

- If 3 splits in K, let $\mathfrak{q}_3$ be a prime dividing it. If $3 \mid A$ then $3 \nmid B$ hence $v_{\mathfrak{q}_3}(a_1) = 1$ and $v_{\mathfrak{q}_3}(a_3) = 0$. 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 $\mathfrak{q}$ and $\bar{\mathfrak{q}}$. If $3 \mid B$ then $3 \nmid A$ hence $v_{\mathfrak{q}_3}(a_1) \geq 2$ and $v_{\mathfrak{q}_3}(a_3) = 0$ and 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 $\mathfrak{q}_3$) 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) $v_{\mathfrak{q}}(A + B^3\sqrt{-d}) > 3$ so $\mathfrak{q}$ divides the denominator of the j-invariant. Furthermore, the model is not minimal, and under the usual change of variables (sending $(x, y) \to (3^2 x, 3^3 y)$ we get a curve with multiplicative reduction, hence the discriminant exponent equals 1. At the prime $\overline{\mathfrak{q}_3}$ the curve is a quadratic twist (by the character of conductor 3) of a curve with multiplicative reduction, hence the statement.
- 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 $v_{\mathfrak{p}}(a_1) \geq 2$ and $v_{\mathfrak{p}}(a_3) = 2$ hence we are in Step 8 of Tate's algorithm, the reduction type is IV^* and the conductor exponent equals $14 - 6 = 8$.

□

Remark 12. 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 (25) 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 5.5. *Let $\mathfrak{q}$ be an odd prime ramified in $K/\mathbb{Q}$ and not dividing 3. Then E has reduction type IV^* at $\mathfrak{q}$ and $v_{\mathfrak{q}}(N_{\tilde{E}}) = 2$.*

Proof. Since (A, B, C) is a primitive solution, if q denotes the norm of $\mathfrak{q}$, 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 5.2. □

6. Constructing the Hecke character for a prime $t \equiv 3 \pmod 4$

Let $K = \mathbb{Q}(\sqrt{-d})$ with $d > 0$ (square-free). The computation is 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 6.1. *The prime t splits in K when one of the following two conditions are satisfied:*

- *the value $\#Q_{+-} + \#Q_{--} + v_2(d)$ is odd and $t \equiv 3 \pmod 8$ or,*
- *the value $\#Q_{+-} + \#Q_{--}$ is odd and $t \equiv 7 \pmod 8$.*

Similarly, it is inert when the opposite parity holds.

Proof. Follows easily from quadratic reciprocity. □

The character ε: Define an even character $\varepsilon : \mathbb{I}_{\mathbb{Q}} \to \mathbb{C}^\times$ ramified at the primes in Q_{++}, Q_{-+}, Q_{+-} and eventually at 2. 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 $\varepsilon_t = \begin{cases} \delta_t^{\#Q_{+-}+\#Q_{--}+v_t(d)+v_2(d)+1} & \text{if } t \equiv 3 \pmod 8, \\ \delta_t^{\#Q_{+-}+\#Q_{--}+v_t(d)+1} & \text{if } t \equiv 7 \pmod 8. \end{cases}$
  By Lemma 6.1 ε_t is trivial if t splits in K and equals δ_t if t is inert in K.
- 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.

An easy computation from the above definitions shows that

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

Theorem 6.2. *There exists a Hecke character $\chi : \mathrm{Gal}_K \to \overline{\mathbb{Q}}$ such that:*

(1) $\chi^2 = \varepsilon$ as characters of Gal_K,
(2) χ is unramified at primes not dividing $2t\prod_{p\in Q_{+-}\cup Q_{--}} p$,
(3) ${}^\tau\chi = \chi \cdot \psi_{-t}$ as characters of Gal_K.

Proof. Once again, we follow the general strategy to define the local components of the character χ at primes not dividing $2t$:

- If $\mathfrak{p}$ is an odd unramified prime, let $\chi_\mathfrak{p}$ be the trivial character. The same applies to primes in K dividing the primes in $Q_{++} \cup Q_{-+}$.
- If $\mathfrak{p}$ is an odd prime of norm $p \in Q_{--}$, let $\chi_\mathfrak{p}$ correspond to the quadratic character δ_p (identifying $(\mathcal{O}_\mathfrak{p}/\mathfrak{p})^\times \simeq (\mathbb{Z}/p)^\times$).
- If $\mathfrak{p}$ is an odd prime of norm $p \in Q_{+-}$, let $\chi_\mathfrak{p}$ be the character $\varepsilon_p\delta_p$ (identifying $(\mathcal{O}_\mathfrak{p}/\mathfrak{p})^\times \simeq (\mathbb{Z}/p)^\times$).
- Let $\mathfrak{p}$ be a prime (take one) in K dividing t and define $\chi_\mathfrak{p}$ by
  (1) If t ramifies in K, $\chi_t = \varepsilon_t$.
  (2) If t splits in K, $\chi_t = \delta_t$ and $\chi_{\overline{\mathfrak{p}}}$ is the trivial character.
  (3) If t is inert in K, χ_t is an order 4 character (hence its restriction to $\mathbb{F}_t^\times$ is trivial).
- At primes dividing 2, define the character as follows:
  (1) If 2 is not ramified in $K/\mathbb{Q}$ it is trivial.
  (2) If 2 ramifies in $K/\mathbb{Q}$ but $2 \nmid d$, it equals the character of conductor 2 sending $\sqrt{-d}$ to -1.
  (3) If $2 \mid d$ and $t \equiv 3 \pmod 8$, it equals the order four character of conductor $\mathfrak{p}_2^5$ sending $1 + \sqrt{-d}$ to $\sqrt{-1}$, -1 to -1 and 5 to -1. In particular, its restriction to $\mathbb{Z}_2^\times$ equals δ_{-2}.
  (4) If $2 \mid d$ and $t \equiv 7 \pmod 8$, it equals the order four character of conductor $\mathfrak{p}_2^5$ sending $1 + \sqrt{-d}$ to $\sqrt{-1}$, -1 to 1 and 5 to -1. In particular, its restriction to $\mathbb{Z}_2^\times$ equals δ_2.

Then the local components of χ satisfy the theorem conditions.

(1) Is proven in the general strategy for primes not diving $2t$. For primes dividing 2 it is clear because all the characters have at most order 2. For primes dividing t, the first two cases are trivial, as both χ_t^2 and $\varepsilon \circ \mathcal{N}$ 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 $\mathbb{F}_t^\times$.
(2) The ramification statement is clear from the definition.
(3) For primes $\mathfrak{p}$ not dividing t the statement is clear since $(\psi_{-t} \circ \mathcal{N})_p$ is trivial, and ${}^\tau\chi_\mathfrak{p} = \chi_\mathfrak{p}$. As for the prime t, if it ramifies in K, $(\psi_{-t} \circ \mathcal{N})_t$ is trivial while ${}^\tau\chi_t = \chi_t$, hence the statement. Otherwise, the norm map is surjective. If t splits, one of $\chi_\mathfrak{p}$ matches $(\psi_{-t} \circ \mathcal{N})_p$ and the other one is trivial (hence the statement). At last, if t is inert, note that χ_t restricted to $\mathbb{F}_t^\times$ is trivial (since $p \equiv 3 \pmod 4$). Let g be a generator of $\mathbb{F}_{t^2}^\times$, then ${}^\tau\chi(g)\chi(g) = \chi(\mathcal{N}(g)) = 1$ and $\delta_t(\mathcal{N}(g)) = -1$ since $\mathcal{N}(g)$ is a generator of $\mathbb{F}_t^\times$. Since χ has order 4, ${}^\tau\chi = \chi \cdot \psi_{-t} \circ \mathcal{N}$ as claimed.

Extend χ to $K^\times \cdot (\prod_\mathfrak{q} \mathcal{O}_\mathfrak{q}^\times \times \mathbb{C}^\times)$ by making it trivial in $K^\times$, so all the above properties continue to hold.

Compatibility: since all 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 $Q_{\pm,\pm}$ are empty and the compatibility at $\sqrt{-1}$ follows

from two facts: $\tilde{\chi}_2(\sqrt{-1}) = -1$, and the fact that $p \equiv 3 \pmod 4$ implies that $\sqrt{-1} \notin \mathbb{F}_p$, but it square does, hence $\chi_t(\sqrt{-1}) = -1$ as well.

To check the compatibility at -1, abusing notation we have

$$\chi(-1) = \prod_{\mathfrak{p} \in Q_{+-} \cup Q_{--}} \chi_{\mathfrak{p}}(-1)\chi_{\mathfrak{p}_2}(-1)\chi_t(-1) = (-1)^{\#Q_{+-}+\#Q_{--}}\chi_{\mathfrak{p}_2}(-1)\chi_t(-1) = 1.$$

By quadratic reciprocity (see Lemma 6.1), 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 giving the compatibility when d is odd. When $2 \mid d$, the compatibility follows from the fact that $\delta_t(2) = \chi_{\mathfrak{p}_2}(-1)$.

At last, when t ramifies in K, by definition $\chi_t = \varepsilon_t$ whose value at -1 equals $(-1)^{\#Q_{+-}+\#Q_{--}}\delta_t(2)^{v_2(d)}$. Also $\chi_{\mathfrak{p}_2}(-1) = \delta_t(2)^{v_2(d)}$ hence the equality.

Extension: We proceed as for $t = 2$, but equation (12) becomes

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

If $q \equiv 1 \pmod 4$ (hence a square) the last product is 1 by quadratic reciprocity, while if $q \equiv 3 \pmod 4$ it equals $(-1)^{\#Q_{-+}+\#Q_{--}}$, i.e. it equals $\delta_{-1}(q)^{\#Q_{-+}+\#Q_{--}}$. We make the following claim (note that the factor $\varepsilon_q(-1)$ is removed):

$$\left(\chi_2^{-1}(q)\chi_t^{-1}(q)\varepsilon_2(q)\varepsilon_t(q)\delta_q(2)^{v_2(d)}\delta_q(t)^{v_t(d)}\right)\delta_{-1}(q)^{\#Q_{-+}+\#Q_{--}} = \delta_q(t). \tag{26}$$

Note that $\delta_q(2) = \delta_2(q)$; for the first factor we have the following equalities:

- $\chi_t^{-1}(q)\varepsilon_t(q) = \delta_t(q)^{1+v_t(d)} = \delta_q(t)^{1+v_t(d)}\delta_{-1}(q)^{1+v_t(d)}$, so $\chi_t^{-1}(q)\varepsilon_t(q)\delta_q(t)^{v_t(d)} = \delta_q(t)\delta_{-1}(q)^{1+v_t(d)}$.
- If $t \equiv 3 \pmod 8$, $\chi_2^{-1}(q)\delta_2(q)^{v_2(d)} = \delta_{-1}(q)^{v_2(d)}$.
- If $t \equiv 7 \pmod 8$, $\chi_2^{-1}(q)\delta_2(q)^{v_2(d)} = 1$.

Then the first factor equals $\delta_q(t)\delta_{-1}(q)^{1+v_t(d)}\varepsilon_2(q)$ if $t \equiv 7 \pmod 8$ and the same with an extra factor $\delta_{-1}(q)^{v_2(d)}$ otherwise so the claim follows from the definition of ε_2.

Then we are led to prove that $\delta_q(t)\varepsilon_q(-1) = 1$, an equality that follows from the definitions (that are collected in Table 6.1).

$q \pmod 4$	$q \pmod t$	$\varepsilon_q(-1)$	$\delta_q(t)$	$q \pmod 4$	$q \pmod t$	$\varepsilon_q(-1)$	$\delta_q(t)$
1	□	1	1	3	□	-1	-1
1	⊠	-1	-1	3	⊠	1	1

TABLE 6.1. Table

Finally, by a consequence of an analogous analysis that has been done for the case $t = 2$, to verify that ${}^{\tau}\chi = \chi \cdot \psi_{-t} \circ \mathcal{N}$ on $\mathbb{I}_K$ we have to check (following the previous notation) that

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

which follows directly from (26) . □

We want to apply the previous result to our curve $\tilde{E}$. Let us make some remarks on the conductor of twisted representation $\rho_{\tilde{E},p} \otimes \chi$. Let $\mathfrak{q}$ be an odd prime ramifying in $K/\mathbb{Q}$ not dividing 3. Recall that $\tilde{E}$ has additive reduction at all such primes and its local type (by Remark 11) 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 $\rho_{\tilde{E},p}$, hence the conductor of the twisted representation at $\mathfrak{q}$ is still 2.

At primes dividing 2, the conductor never decreases (from the definition of χ_t and the conductor of $\tilde{E}$ given in Lemma 5.3). 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 $K/$ and $\tilde{E}$ 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 12). Then twisting by χ_3 (also a character whose inertia has order 4) cancels one of the characters, hence the twisted representation has conductor valuation 1.

Theorem 6.3. *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 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ attached to a newform g of weight 2, Nebentypus ε, level N given by*

$$N = 2^a 3^b \prod_q q^{v_{\mathfrak{q}}(N_E)} \cdot \prod_{q\in Q_{\pm\pm}} q^2,$$

where the product is over odd primes, and $\mathfrak{q}$ is any prime of K dividing q. 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 existence of the extension, and its Nebentypus follows the proof of Theorem 2.3. Regarding the conductor of the representation, recall (by Lemma 5.5) that if $\mathfrak{q} \mid q$ is an odd ramified prime ideal not dividing 3, then $v_{\mathfrak{q}}(\rho_{\tilde{E},p}) = 2$. The same holds for $\rho_{\tilde{E},p}\otimes\chi$ (as explained before). Then the conductor formula (18) implies that the four dimensional representation has conductor with valuation 3 or 4 at such primes, so the valuation $v_q(N) = 1, 2$. The same argument gives the exponent at the prime 2 (using Lemma 5.3) and at the prime 3 (using Lemma 5.4 and Remark 12). □

Using Ribet's lowering the level, we can remove the primes dividing the conductor of the curve.

7. Solving equation (3)

We follow closely the tools of Section 4. In particular, Theorem 4.1 holds as does Ribet's lowering the level and Ellenberg's big image result. Theorem 4.1 is true in this setting, and to make it effective, we search for a prime ℓ such that $\ell \equiv 1 \pmod{3^2\cdot\tilde{d}}$ (since $v_2(\mathrm{cond}(\varepsilon_2)) \le 4$, we can assume ν is unramified at 2), where $\tilde{d}$ is the prime to 6 part of d, and $p > 2\sqrt{\ell}+\ell+1$ is enough for it to hold.

7.1. Some cases of (3).

In this section we apply the previous results to solve some cases of equation (1).

7.1.1. *The equation $x^2+2y^6 = z^p$.* 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 $\mathbb{Q}(\sqrt{-2})$. This is a very interesting example, as the curve $\tilde{E}$ 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, also available in the lmfdb) it turns out that there are no Bianchi modular forms in any level but 3^3, whose space contains three elliptic curves (2.0.8.1-729.4-a1, 2.0.8.1-729.4-b1, 2.0.8.1-729.4-c1), one of which has complex multiplication and is the base change of a rational elliptic curve (hence cannot be congruent to $\tilde{E}$). The other two ones satisfy that $a_5 = -1$. It is easy to compute for each possible value of (A,B) modulo 5 the value of $a_5(\tilde{E}_{(A,B)})$ and verify it belongs to the set $\{2,0,-7,-10\}$ hence both curves cannot be congruent if $p > 5$.

Theorem 7.1. *Let $p > 23$ be a prime number. Then there are no non-trivial solutions of the equation*

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

Proof. We need $p > 23$ to apply the analogue of Theorem 4.1, while $p > 11$ is enough to use Ellenberg's result (see Remark 10). □

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

7.1.3. *The equation $x^2 + 5y^6 = z^p$.* The only non-empty set is $Q_{+-} = \{5\}$. The character ε has conductor $4 \cdot 5$, of order 4 at 5 hence χ has order 8. We compute the space $S_2(2^4 \cdot 5^2 \cdot 3^a, \varepsilon)$ with $a = 2, 3$ and our form g has coefficient field $\mathbb{Q}(\sqrt{3}, \sqrt{-1}, \sqrt{-2})$ (by Remark 6). The first space has 15 Galois orbits (for $a = 2$), three of them with coefficient field $\mathbb{Q}(\sqrt{-1})$, three with a quadratic extension of it, and the other ones a degree 4 extension of $\mathbb{Q}(\sqrt{-1})$. There are seven forms with complex multiplication.

In this case, Mazur's trick does not work, due to the existence of many elliptic curves in the given space (see lmfdb conductor 2916). Although such curves do not seem to come from solutions, we do not know how to discard them. Doing a simple search for solutions with A, B at most 10^5 we found the unique solution (for $p > 2$):

$$79^2 + 5 \cdot 2^6 = 3^8.$$

7.1.4. *The equation $x^2 + 6y^6 = z^p$.* All sets $Q_{\pm,\pm}$ are empty, the character ε equals the quadratic character of conductor 12, while χ is a quadratic character of conductor $3 \cdot \langle 2, \sqrt{-6} \rangle^5$. The new subspace of $S_2(2^8 \cdot 3^5, \varepsilon)$ has dimension 1152 and splits in 58 conjugacy classes. Note that any primitive solution corresponds to values (A, B, C) where C is prime to 3, hence the integer C needs to be divisible by a prime number greater than 3, hence the curve $\tilde{E}_{(A,B)}$ cannot have complex multiplication. The first six newforms (given by magma) have complex multiplication, hence we can discard them. For the remaining ones Mazur's trick is enough to discard them all. Using primes q dividing the set $\{5, 11, 13, 17, 19\}$ we get that p belongs to the set $\{2, 3, 5, 7, 11, 13, 17, 23, 31, 37, 59, 71, 73, 107, 109\}$.

Theorem 7.2. *Let $p > 109$ be a prime number. Then there are no non-trivial solutions of the equation*

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

Proof. As what happened for equation (1), the fact that $6 \mid d$ implies C is prime to 6, hence the curve attached to a primitive solution always has a prime of multiplicative reduction. The result follows from the fact that $N_6 = 11$ by Proposition 4.3 (and Remark 10). □

7.1.5. *The equation $x^2 + 7y^6 = z^p$.* The set $Q_{-+} = \{7\}$ while the other ones are empty. The character ε has order 2 and conductor 21, while χ has order 4. A solution to our equation gives an elliptic curve congruent to a newform in the space $S_2(2^a \cdot 3^b \cdot 7^2, \varepsilon)$, where $a = 1, 2$ and $b = 1, 3$. At 7, by Remark 11 the representation $\rho_{\tilde{E},p}$ has local type that of a principal series, whose character restricted to inertia has order 3 (recall that χ_7 is unramified, hence the same happens for the twisted representation). In particular, since 7 ramifies in the quadratic field, such character factors through the norm map, hence the local type of g must be that of a ramified principal series (whose inertia is given as the sum of an order 3 and an order 6 character).

In the space $S_2(2 \cdot 3 \cdot 7^2, \varepsilon)$ we can discard all non-CM forms using Mazur's trick, but in the space $S_2(2 \cdot 3^3 \cdot 7^2, \varepsilon)$ there are three forms without CM, whose local type at 7 correspond to a principal series representation that cannot be discarded just using Mazur's trick.

It should be noticed that there are some solutions with exponents up to 7, namely

$$11^2 + 7 \cdot 1^6 = 2^7.$$

or

$$181^2 + 7 \cdot 1^6 = 2^{15}.$$

References

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

[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.

[cS18] Mehmet Haluk Şengün and Samir Siksek. On the asymptotic Fermat's last theorem over number fields. *Comment. Math. Helv.*, 93(2):359–375, 2018.

[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 Q-curves over polyquadratic fields. *J. Reine Angew. Math.*, 633:183–195, 2009.

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

[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.

[Hen79] Guy Henniart. *Représentations du groupe de Weil d'un corps local*, volume 2 of *Publications Mathématiques d'Orsay 79 [Mathematical Publications of Orsay 79]*. Université de Paris-Sud, Département de Mathématique, Orsay, 1979. With an English summary.

[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.

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

[Pyl04] Elisabeth E. Pyle. Abelian varieties over Q with large endomorphism algebras and their simple components over $\overline{Q}$. In *Modular curves and abelian varieties*, volume 224 of *Progr. Math.*, pages 189–239. Birkhäuser, Basel, 2004.

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

[Que01] Jordi Quer. Embedding problems over abelian groups and an application to elliptic curves. *J. Algebra*, 237(1):186–202, 2001.

[Rib91] Kenneth A. Ribet. Lowering the levels of modular representations without multiplicity one. *Internat. Math. Res. Notices*, (2):15–19, 1991.

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

[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.

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

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