Canad. J. Math. Vol. 75 (4), 2023 pp. 1293–1313
http://dx.doi.org/10.4153/S0008414X22000311

On ternary Diophantine equations of signature $(p, p, 3)$ over number fields

Erman Isik, Yasemin Kara, and Ekin Ozman

Abstract. In this paper, we prove results about solutions of the Diophantine equation $x^p + y^p = z^3$ over various number fields using the modular method. First, by assuming some standard modularity conjecture, we prove an asymptotic result for general number fields of narrow class number one satisfying some technical conditions. Second, we show that there is an explicit bound such that the equation $x^p + y^p = z^3$ does not have a particular type of solution over $K = \mathbb{Q}(\sqrt{-d})$, where $d = 1, 7, 19, 43, 67$ whenever p is bigger than this bound. During the course of the proof, we prove various results about the irreducibility of Galois representations, image of inertia groups, and Bianchi newforms.

1 Introduction

Solving Diophantine equations is one of the oldest and widely studied topics in number theory. Yet we still do not have a general method that would allow us to produce solutions of a given Diophantine equation. Most of the time, it may be easier to show the nonexistence of solutions, but even this can be quite challenging as it was the case for the proof of Fermat's Last Theorem (FLT). The method to solve the Fermat equation, used by Wiles in his famous proof, can be adapted to solve similar Fermat-type equations. This strategy, which is referred as the "modular method," starts with an elliptic curve attached to a putative solution of the given equation. Then, using many celebrated theorems of the area, the problem can be reduced to one of the following: computing newforms of a certain level, or computing all elliptic curves of a given conductor with particular information about torsion subgroup and rational isogeny, or computing all solutions to an S-unit equation. Neither of these computations are easy in general. Especially if one needs to prove Fermat's theorem over a number field other than rationals, some fundamental theorems that go into the proof now become conjectures only, such as the modularity conjecture. Recently, there has been much progress in several different generalizations of this famous result. For instance, in [12], Freitas and Siksek proved the asymptotic FLT for certain totally real fields K. That is, they showed that there is a constant B_K such that, for any prime $p > B_K$, the only solutions to the Fermat equation $a^p + b^p + c^p = 0$ where $a, b, c \in \mathcal{O}_K$ are the

Received by the editors January 23, 2022; revised June 9, 2022; accepted June 20, 2022.
Published online on Cambridge Core June 24, 2022.
All authors are partially supported by the Turkish National and Scientific Research Council (TÜBİTAK) Research Grant 117F045. The second author is also supported by Bogazici University Research Fund Grant Number 19082.
AMS subject classification: **11D41**, 11F80, 11F03, 11F75.
Keywords: Diophantine equations, modular method, Galois representations.

trivial ones satisfying $abc = 0$. Then, Deconinck [7] extended the results of Freitas and Siksek [12] to the generalized Fermat equation of the form $Aa^p + Bb^p + Cc^p = 0$ where A, B, C are odd integers belonging to a totally real field. Later, in [27], Şengün and Siksek proved the asymptotic FLT for any number field K by assuming modularity. This result has been generalized by Kara and Ozman in [17] to the case of the generalized Fermat equation. Moreover, recently, in [31, 32], Turcas studied the Fermat equation over imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$ with class number one.

Similar generalizations are quite rare for other Fermat-type equations such as $x^p + y^q = z^r$. The solutions of this equation have been studied over rationals by many mathematicians including Darmon, Merel, Bennett, and Poonen. Several mathematicians have worked on similar Fermat-type equations with different exponents over rational numbers. We have summarized these results in [14]; therefore, we will not repeat them here, but we want to mention that not many results exist for generalizations of these to higher degree number fields. During the write-up of this paper, we have been informed about the work of Mocanu [23] where she improves the results in [14] and proves similar versions for the Diophantine equation of signature $(p, p, 3)$. In this paper, we also study the solutions of $x^p + y^p = z^3$ over number fields. However, our results differ from Mocanu (and hence the results in [14]) in the sense that we prove results about solutions of equation (1.1) over fields that are not totally real. In the Appendix, we mention versions of these results for the Diophantine equation of signature $(p, p, 2)$. Our results can be summarized as follows.

1.1 Our results

Let K be a number field, and let $\mathcal{O}_K$ be its ring of integers. For a prime number p, we refer the equation

$$a^p + b^p = c^3, \quad a, b, c \in \mathcal{O}_K, \tag{1.1}$$

as *the Fermat equation over K with signature (p,p,3)*. A solution (a, b, c) is called *trivial* if $abc = 0$, otherwise *non-trivial*. A solution (a, b, c) of equation (1.1) is called *primitive* if a, b, and c are pairwise coprime. Since we will consider number fields with class number one, a putative solution (a, b, c) can be scaled such that a, b, and c are coprime.

Note that if $p > 3$, then one can produce infinitely many nonprimitive solutions to equation (1.1). Indeed, if $p \equiv -1 \pmod 3$ and $a, b, c \in \mathcal{O}_K$ satisfying $a^p + b^p = c$, then $(ac, bc, c^{\frac{p+1}{3}})$ is a nonprimitive solution to equation (1.1). Observe that if $x, y, z \in \mathcal{O}_K$ satisfy $x^p + y^p = z$, then we have $(xz)^p + (yz)^p = (z^{\frac{p+1}{2}})^2$, so one can obtain $a, b, c \in \mathcal{O}_K$ such that $a^p + b^p = c^2$. If $p \equiv 1 \pmod 3$ and $a, b, c \in \mathcal{O}_K$ such that $a^p + b^p = c^2$, then $(ac, bc, c^{\frac{p+2}{3}})$ is a nonprimitive solution to equation (1.1). Thus, we consider only primitive solutions to equation (1.1). In [5], it was shown that equation (1.1) has finitely many primitive solutions.

We say that "*the asymptotic Fermat Theorem holds for K and signature* $(p, p, 3)$" if there is a constant B_K such that, for any prime $p > B_K$, the Fermat equation with signature $(p, p, 3)$ (given in equation (1.1)) does not have nontrivial, primitive solutions.

https://doi.org/10.4153/S0008414X22000311 Published online by Cambridge University Press

We have two main results about solutions of equation (1.1). The first result is an asymptotic result for some of the solutions over general number fields, and the second one is an explicit result for general solutions over some imaginary quadratic fields.

Theorem 1.1 *Let K be a number field with narrow class number $h_K^+ = 1$ satisfying Conjectures 2.2 and 2.3 and containing $\mathbb{Q}(\zeta_3)$ where ζ_3 is a primitive third root of unity. Assume that λ is the only prime of K lying above 3. Let W_K be the set of $(a, b, c) \in \mathcal{O}_K$ such that (a, b, c) is a primitive solution to $x^p + y^p = z^3$ with $\lambda | b$. Then there is a constant B_K—depending only on K—such that, for $p > B_K$, equation (1.1) has no solution $(a, b, c) \in W_K$. In this case, we say that the asymptotic FLT holds for W_K and signature $(p, p, 3)$.*

Theorem 1.2 *Let $K = \mathbb{Q}(\sqrt{-d})$, where $d \in \{1, 7, 19, 43, 67\}$, and let ℓ_K be the largest prime in Table 2 corresponding to K. Let C_K, M_K be defined as in Proposition 3.9 and Corollary 3.10. Assume that Conjecture 2.2 holds true for K. Let λ be the prime of $\mathcal{O}_K$ lying over 3. Then:*

Case I *For any prime $p > \max\{\ell_K, C_K\}$, the Fermat equation over K with signature $(p, p, 3)$ does not have any nontrivial primitive solutions $(a, b, c) \in \mathcal{O}_K$ such that $\lambda | b$.*

Case II *If $p > B_K = \max\{\ell_K, C_K, M_K\}$, p splits in K, and $p \equiv 3 \pmod 4$, then the Fermat equation over K with signature $(p, p, 3)$ does not have any nontrivial primitive solutions $(a, b, c) \in \mathcal{O}_K$.*

Remark 1.3 The bound for Case 1 above is 199, and this bound can be made smaller depending on the field we work on, as can be seen in Table 2. Combining this with Proposition 3.9 and Case 1 of Corollary 3.10, we see that the bound 199 works for all the five imaginary quadratic fields mentioned in the statement of Theorem 1.2.

Similarly, for Case 2 of Theorem 1.2, it is possible to take B_K as $44,483$, using Proposition 3.9 and Case 2(a) of Corollary 3.10.

Various different techniques have to be combined to achieve these results. For the asymptotic result, we mostly follow the approach in [14, 17], which relies on the paper of Şengün and Siksek [27]. For instance, we need the absolute irreducibility of the associated Galois representation in order to apply the Serre's modularity conjecture. In order to do this, one needs to prove the irreducibility first and then pass to absolute irreducibility. This is rather classical when the Frey curve has potentially multiplicative reduction at q for some q appearing in the denominator of the j-invariant of the Frey curve. However, for $(p, p, 3)$ case, the associated Frey elliptic curve has potentially good reduction when 3 does not divide the norm of ab. Therefore, one can only get a result about solutions of a particular type. This was also mentioned in the papers of Turcas [31, 32]. It is sometimes possible to overcome this obstruction when working over explicit fields. For instance, as done by Najman and Turcas in [24], using a result of Vaintrob and Larson, it is possible to prove the absolute irreducibility of the associated Galois representation when p is bigger than a computable constant B_K. One can apply a similar argument to the Galois representation related to the Diophantine equation of signature $(p, p, 3)$. Of course, in order to do this, we need an irreducibility result for $\overline{\rho}_{E,p}$ when p is bigger than an explicit constant B. This is a nontrivial task to do even in the case of the classical Fermat equation, which was done by Freitas and Siksek in

https://doi.org/10.4153/S0008414X22000311 Published online by Cambridge University Press

[13]. We combine all these to obtain our second result, which gives information about the solutions of $(p, p, 3)$ over imaginary quadratic number fields of class number one.

2 Preliminaries

In this section we give the necessary background to prove the results. We follow [12, 27] and the references therein.

2.1 Conjectures

In this subsection, we state the conjectures assumed in the above theorems. For more details, we refer to Sections 2 and 3 of [27].

Let K be a number field with the ring of integers $\mathcal{O}_K$, and let $\mathfrak{N}$ be an ideal of $\mathcal{O}_K$. The following result is proved by Şengün and Siksek in [27].

Proposition 2.1 [27, Proposition 2.1] *There is an integer $B(\mathfrak{N})$, depending only on $\mathfrak{N}$, such that, for any prime $p > B(\mathfrak{N})$, every weight-two, mod p eigenform of level $\mathfrak{N}$ lifts to a complex one.*

In order to run the modular approach to solve Diophantine equations, one needs generalized modularity theorems. Due to the lack of their existence, we can only prove our theorems up to some conjectures. One of the assumed conjectures is a special case of Serre's modularity conjecture over number fields, stated below.

Conjecture 2.2 [11, Conjecture 4.1] *Let $\overline{\rho} : G_K \to GL_2(\overline{\mathbb{F}}_p)$ be an odd, irreducible, continuous representation with Serre conductor $\mathfrak{N}$ (prime-to-p part of its Artin conductor) such that $\det(\overline{\rho}) = \chi_p$ is the mod p cyclotomic character. Assume that p is unramified in K and that $\overline{\rho}|_{G_{K_\mathfrak{p}}}$ arises from a finite-flat group scheme over $\mathcal{O}_{K_\mathfrak{p}}$ for every prime $\mathfrak{p}|p$. Then there is a weight-two, mod p eigenform θ over K of level $\mathfrak{N}$ such that, for all primes $\mathfrak{q}$ coprime to $p\mathfrak{N}$, we have*

$$\mathrm{Tr}(\overline{\rho}(\mathrm{Frob}_\mathfrak{q})) = \theta(T_\mathfrak{q}),$$

where $T_\mathfrak{q}$ denotes the Hecke operator at $\mathfrak{q}$.

Additionally, we will use a special case of a fundamental conjecture from the Langlands program for the asymptotic result. Note that we do not need Conjecture 2.3 for Theorem 1.2 since K is restricted to a finite (fixed) list of fields.

Conjecture 2.3 [27, Conjecture 4.1] *Let $\mathfrak{f}$ be a weight-two complex eigenform over K of level $\mathfrak{N}$ that is nontrivial and new. If K has some real place, then there exists an elliptic curve $E_\mathfrak{f}/K$ of conductor $\mathfrak{N}$ such that*

$$\#E_\mathfrak{f}(\mathcal{O}_K/\mathfrak{q}) = 1 + \mathrm{Norm}(\mathfrak{q}) - \mathfrak{f}(T_\mathfrak{q}) \quad \textit{for all} \quad \mathfrak{q} \nmid \mathfrak{N}. \tag{2.1}$$

If K is totally complex, then there exists either an elliptic curve $E_\mathfrak{f}$ of conductor $\mathfrak{N}$ satisfying (2.1) or a fake elliptic curve $A_\mathfrak{f}/K$, of conductor $\mathfrak{N}^2$, such that

$$\#A_\mathfrak{f}(\mathcal{O}_K/\mathfrak{q}) = (1 + \mathrm{Norm}(\mathfrak{q}) - \mathfrak{f}(T_\mathfrak{q}))^2 \quad \textit{for all} \quad \mathfrak{q} \nmid \mathfrak{N}. \tag{2.2}$$

https://doi.org/10.4153/S0008414X22000311 Published online by Cambridge University Press

2.2 Frey curve and related facts

In this subsection, we collect some facts related to the Frey curve associated with a putative solution of equation (1.1) and the associated Galois representation.

Let G_K be the absolute Galois group of a number field K, let E/K be an elliptic curve, and let $\overline{\rho}_{E,p}$ denote the mod p Galois representation of E. We use $\mathfrak{q}$ for an arbitrary prime of K, and $G_\mathfrak{q}$ and $I_\mathfrak{q}$, respectively, for the decomposition and inertia subgroups of G_K at $\mathfrak{q}$. For a putative solution (a, b, c) to equation (1.1) with a prime exponent p, we associate the Frey elliptic curve as in [2],

$$E = E_{a,b,c} : Y^2 + 3cXY + b^p Y = X^3 \tag{2.3}$$

whose arithmetic invariants are given by $\Delta_E = 3^3(ab^3)^p$, $j_E = \dfrac{3^3c^3(9a^p + b^p)^3}{(ab^3)^p}$, and $c_4(E) = 9c(9a^p + b^p)$, $c_6(E) = -3^3(3^3c^6 - 2^2 3^2 c^3 b^p + 2^3 b^{2p})$.

For the result below, we have the same assumptions on the number field K mentioned in the introduction. Namely, K is a number field of degree d such that the narrow class number of K, $h_K^+ = 1$ and there is a unique prime λ over 3.

Lemma 2.4 *Let $\lambda^e = 3\mathcal{O}_K$ where $\mathcal{O}_K$ is the integer ring of K. The Frey curve E is semistable away from λ and has a K-rational point of order 3. The determinant of $\overline{\rho}_{E,p}$ is the mod p cyclotomic character. The Galois representation $\overline{\rho}_{E,p}$ is finite flat at every prime $\mathfrak{p}$ of K that lies above p. Moreover, the conductor $\mathcal{N}_E$ attached to the Frey curve E is given by*

$$\mathcal{N}_E = \lambda^\varepsilon \prod_{\mathfrak{q}|ab, \mathfrak{q}\nmid 3} \mathfrak{q},$$

where

(1) $\varepsilon \in \{0, 1\}$ *if* $\lambda | ab$ *and* $p > 2e$.
(2) $\varepsilon \geq 2, 3$ *if* $\lambda \nmid ab$. *Moreover, if* $e = 1$, $\varepsilon \in \{2, 3\}$.

In particular, if $\lambda | ab$, the curve E is semistable, and otherwise, the curve E has additive reduction at λ.

The Serre conductor $\mathfrak{N}_E$, which is the prime-to-p part of the Artin conductor of $\overline{\rho}_{E,p}$, is supported on λ and belongs to a finite set depending only on the field K.

Proof Assume that the narrow class number $h_K^+ = 1$. Recall that the invariants $c_4(E)$, $c_6(E)$, and Δ_E of the model E are given by

$$c_4(E) = 9c(9a^p + b^p),\ c_6(E) = -3^3(3^3c^6 - 2^2 3^2 c^3 b^p + 2^3 b^{2p}),\ \Delta_E = 3^3(ab^3)^p.$$

Suppose that $\mathfrak{q} \neq \lambda$ divides Δ_E, which implies that ab is divisible by $\mathfrak{q}$. Since a, b, and c are pairwise coprime, $\mathfrak{q}$ divides either a or b. Therefore, $c_4(E) = 9c(9a^p + b^p)$ is not divisible by $\mathfrak{q}$, i.e., $v_\mathfrak{q}(c_4(E)) = 0$. Hence, the given model is minimal and E is semistable at $\mathfrak{q}$. Moreover, we have $p | v_\mathfrak{q}(\Delta_E)$. It follows from [28] that $\overline{\rho}_{E,p}$ is finite flat at $\mathfrak{q}$ if $\mathfrak{q}$ lies above p. We can also deduce that $\overline{\rho}_{E,p}$ is unramified at $\mathfrak{q}$ if $\mathfrak{q} \nmid p$.

Now, assume that λ divides ab. Note that λ can only divide one of a or b. Without loss of generality, say $\lambda | b$. The result regarding $\lambda \nmid ab$ can be handled in an identical manner.

https://doi.org/10.4153/S0008414X22000311 Published online by Cambridge University Press

In all cases, the valuation $v_\lambda(\mathcal{N}_E) = \varepsilon$ can be calculated via [25, Tableau III]. Note that, when $\lambda | ab$, the equation is not minimal. After using the change of variables $X = 3^2x$, $Y = 3^3y$, we get $v_\lambda(c_4(E)) = v_\lambda(c_6(E)) = 0$ when $p > 2e$, and hence $\varepsilon = 0, 1$.

The statement concerning the determinant is a well-known consequence of the Weil pairing attached to elliptic curves. The fact that the Frey curve E has a K-rational point of order 3 follows from [2, Lemma 2.1(c)].

Finally, to show that there can be only finitely many Serre conductors $\mathfrak{N}_E$, note that only the prime λ can divide $\mathfrak{N}_E$. As $\mathfrak{N}_E$ divides the conductor $\mathcal{N}_E$ of E, $v_\lambda(\mathfrak{N}_E) \leq v_\lambda(\mathcal{N}_E) \leq 2 + 3v_\lambda(3) + 6v_\lambda(2)$ by [29, Theorem IV.10.4]. Hence, there can be only finitely many Serre conductors and they only depend on K. ∎

Given a number field K, we obtain a *complex conjugation* for every real embedding $\sigma : K \hookrightarrow \mathbb{R}$ and every extension $\tilde{\sigma} : \overline{K} \hookrightarrow \mathbb{C}$ of σ as $\tilde{\sigma}^{-1}\iota\tilde{\sigma} \in G_K$ where ι is the usual complex conjugation. Recall that a representation $\overline{\rho}_{E,p} : G_K \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ is *odd* if the determinant of every complex conjugation is -1. If the number field K has no real embeddings, then we immediately say that $\overline{\rho}_{E,p}$ is odd.

The following results give us information about the image of inertia groups under the Galois representation $\overline{\rho}_{E,p}$.

Lemma 2.5 [12, Lemma 3.4] *Let E be an elliptic curve over K with j-invariant j_E. Let $p \geq 5$, and let $\mathfrak{q} \nmid p$ be a prime of K. Then $p | \#\overline{\rho}_{E,p}(I_\mathfrak{q})$ if and only if E has potentially multiplicative reduction at $\mathfrak{q}$ (i.e., $v_\mathfrak{q}(j_E) < 0$) and $p \nmid v_\mathfrak{q}(j_E)$.*

By using the previous result, we obtain the following lemma.

Lemma 2.6 *Let λ be the only prime ideal of K lying above 3, and let $(a, b, c) \in W_K$ with prime exponent $p > v_\lambda(3)$. Let E be the Frey curve as in (2.3), and write j_E for its j-invariant. Then E has potentially multiplicative reduction at λ and $p | \#\overline{\rho}_{E,p}(I_\lambda)$ where I_λ denotes an inertia subgroup of G_K at λ.*

Proof Assume that λ is the only prime ideal of K lying above 3 with $v_\lambda(b) = k$. Then $v_\lambda(j_E) = 3v_\lambda(3) - 3pk$. Since $p > v_\lambda(3)$, and $k \geq 1$, we have $v_\lambda(j_E) < 0$ and clearly $p \nmid v_\lambda(j_E)$. This implies that E has potentially multiplicative reduction at λ and $p | \#\overline{\rho}_{E,p}(I_\lambda)$. ∎

The following well-known result about subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ will be frequently used.

Theorem 2.7 *Let E be an elliptic curve over a number field K of degree d, and let $G \leq \mathrm{GL}_2(\mathbb{F}_p)$ be the image of the mod p Galois representation of E. Then the following holds:*

- *If $p | \#G$, then either G is reducible or G contains $\mathrm{SL}_2(\mathbb{F}_p)$, and hence it is absolutely irreducible.*
- *If $p \nmid \#G$ and $p > 15d + 1$, then G is contained in a Cartan subgroup or G is contained in the normalizer of Cartan subgroup but not the Cartan subgroup itself.*

Proof For the proof, the main reference is [30, Lemma 2]. The version above including the proof of the second part is from [10, Propositions 2.3 and 2.6]. ∎

https://doi.org/10.4153/S0008414X22000311 Published online by Cambridge University Press

3 Properties of Galois representations

3.1 Level reduction

In this subsection, we will be relating the Galois representation attached to the Frey curve with another representation of lower level.

Theorem 3.1 *Let K be a number field with $h_K^+ = 1$ satisfying Conjectures 2.2 and 2.3. Assume that λ is the only prime of K above 3. Then there is a constant B_K depending only on K such that the following holds. Let $(a, b, c) \in W_K$ be a nontrivial solution to equation (1.1) with exponent $p > B_K$. Let E/K be the associated Frey curve defined in (2.3). Then there is an elliptic curve E'/K such that the following statements hold:*

(1) *E' has good reduction away from λ.*
(2) *E' has a K-rational point of order 3.*
(3) $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$.
(4) $v_\lambda(j') < 0$ *where j' is the j-invariant of E'.*

We will give the proof of this theorem in Section 3.1.1 after stating the necessary lemmas. The following is Proposition 6.1 of [27]. We include its statement for the convenience of the reader, but we will omit its proof and refer to [27] instead.

Proposition 3.2 *Let L be a Galois number field, and let $\mathfrak{q}$ be a prime of L. There is a constant $B_{L,\mathfrak{q}}$ such that the following is true. Let $p > B_{L,\mathfrak{q}}$ be a rational prime. Let E/L be an elliptic curve that is semistable at all $\mathfrak{p}|p$ and having potentially multiplicative reduction at $\mathfrak{q}$. Then $\overline{\rho}_{E,p}$ is irreducible.*

By applying the above proposition to the Frey curve, we get the following corollary.

Corollary 3.3 *Let K be a number field with $h_K^+ = 1$, and suppose that λ is the only prime of K above 3. There is a constant C_K such that if $p > C_K$ and $(a, b, c) \in W_K$ is a nontrivial solution to the Fermat equation with signature $(p, p, 3)$, then $\overline{\rho}_{E,p}$ is surjective, where E is the Frey curve given in (2.3).*

Proof By Lemma 2.6, E has potentially multiplicative reduction at λ. Moreover, E is semistable away from λ from Lemma 2.4. Let L be the Galois closure of K, and let $\mathfrak{q}$ be a prime of L above λ. Now, by applying Proposition 3.2, we get a constant $B_{L,\mathfrak{q}}$ such that $\overline{\rho}_{E,p}(G_L)$ is irreducible whenever $p > B_{L,\mathfrak{q}}$. Note that there are only finitely many choices of $\mathfrak{q}|3$ in L and L only depends on K. Hence, we can obtain a constant depending only on K and we denote it by C_K. If necessary, enlarge C_K so that $C_K > v_\lambda(3)$. Now, we apply Lemma 2.6 and see that the image of $\overline{\rho}_{E,p}$ contains an element of order p. By Theorem 2.7, any subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ having an element of order p is either reducible or contains $\mathrm{SL}_2(\mathbb{F}_p)$. As $p > C_K > v_\lambda(3)$, the image contains $\mathrm{SL}_2(\mathbb{F}_p)$. Finally, we can ensure that $K \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$ by taking C_K large enough if needed. Hence, $\chi_p = \det(\overline{\rho}_{E,p})$ is surjective. ∎

3.1.1 Proof of Theorem 3.1

In this subsection, Theorem 3.1 will be proved. Although the proof closely follows the ideas in [17], we will give it here for the sake of completeness and for the convenience

https://doi.org/10.4153/S0008414X22000311 Published online by Cambridge University Press

of the reader. We continue with the notations introduced in the statement of Theorem 3.1 and the assumptions of the theorem.

Lemma 3.4 *There is a nontrivial, new (weight-two) complex eigenform* $\mathfrak{f}$ *which has an associated elliptic curve* $E_{\mathfrak{f}}/K$ *of conductor* $\mathfrak{N}'$ *dividing* $\mathfrak{N}_E$.

Proof We first show the existence of such an eigenform $\mathfrak{f}$ of level $\mathfrak{N}_E$ supported only on $\{\lambda\}$.

By Corollary 3.3, the representation $\overline{\rho}_{E,p} : G_K \to GL_2(\mathbb{F}_p)$ is surjective and hence is absolutely irreducible for $p > C_K$. Now, we apply Conjecture 2.2 to deduce that there is a weight-two, mod p eigenform θ over K of level $\mathfrak{N}_E$, with $\mathfrak{N}_E$ as in Lemma 2.4, such that, for all primes $\mathfrak{q}$ coprime to $p\mathfrak{N}$, we have

$$\mathrm{Tr}(\overline{\rho}_{E,p}(\mathrm{Frob}_{\mathfrak{q}})) = \theta(T_{\mathfrak{q}}).$$

We also know from the same lemma that there are only finitely many possible levels $\mathfrak{N}$. Thus, by taking p large enough (see Proposition 2.1) for any level $\mathfrak{N}$, there is a weight-two complex eigenform $\mathfrak{f}$ with level $\mathfrak{N}$ which is a lift of θ. Note that since there are only finitely many such eigenforms $\mathfrak{f}$ and they depend only on K, from now on, we can suppose that every constant depending on these eigenforms depends only on K.

Next, we recall that if $\mathbb{Q}_{\mathfrak{f}} \neq \mathbb{Q}$, then there is a constant $C_{\mathfrak{f}}$ depending only on $\mathfrak{f}$ such that $p < C_{\mathfrak{f}}$ [27, Lemma 7.2]. Therefore, by taking p sufficiently large, we assume that $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$. In order to apply Conjecture 2.3, we need to show that $\mathfrak{f}$ is nontrivial and new. As $\overline{\rho}_{E,p}$ is irreducible, the eigenform $\mathfrak{f}$ is nontrivial. If $\mathfrak{f}$ is new, we are done. If not, we can replace it with an equivalent new eigenform of smaller level. Therefore, we can take $\mathfrak{f}$ new with level $\mathfrak{N}'$ dividing $\mathfrak{N}_E$. Finally, we apply Conjecture 2.3 and obtain that $\mathfrak{f}$ either has an associated elliptic curve $E_{\mathfrak{f}}/K$ of conductor $\mathfrak{N}'$, or has an associated fake elliptic curve $A_{\mathfrak{f}}/K$ of conductor $\mathfrak{N}_E^2$.

By Lemma 3.5, if $p > 24$, then $\mathfrak{f}$ has an associated elliptic curve $E_{\mathfrak{f}}$. As a result, we can assume that $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$ where $E' = E_{\mathfrak{f}}$ is an elliptic curve with conductor $\mathfrak{N}'$ dividing $\mathfrak{N}_E$. ∎

Lemma 3.5 [27, Lemma 7.3] *If* $p > 24$, *then* $\mathfrak{f}$ *has an associated elliptic curve* $E_{\mathfrak{f}}$.

We can now give the proof of Theorem 3.1.

Proof of Theorem 3.1. Lemma 3.5 gives us that if $p > 24$, then $\mathfrak{f}$ has an associated elliptic curve $E_{\mathfrak{f}}$. Therefore, by Lemma 3.4 we can assume that $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$, where $E' = E_{\mathfrak{f}}$ is an elliptic curve of conductor $\mathfrak{N}'$ dividing $\mathfrak{N}_E$.

Lemma 3.6 *If* E' *does not have a nontrivial* K*-rational point of order* 3 *and is not isogenous to an elliptic curve with a nontrivial* K*-rational point of order* 3, *then* $p < C_{E'}$ *where* $C_{E'}$ *is a constant depending only on* E'. ∎

Proof By Theorem 3.7, there are infinitely many primes $\mathfrak{q}$ such that $\#E'(\mathbb{F}_{\mathfrak{q}}) \not\equiv 0 \pmod 3$. Fix such a prime $\mathfrak{q} \neq \lambda$, and note that E is semistable at $\mathfrak{q}$. If E has good reduction at $\mathfrak{q}$, then $\#E(\mathbb{F}_{\mathfrak{q}}) \equiv \#E'(\mathbb{F}_{\mathfrak{q}}) \pmod p$. Since $3|\#E(\mathbb{F}_{\mathfrak{q}})$, the difference, which is divisible by p, is nonzero. As the difference belongs to a finite set depending on $\mathfrak{q}$, p becomes bounded. If E has multiplicative reduction at $\mathfrak{q}$, we obtain

$$\pm(\,\mathrm{Norm}(\mathfrak{q}) + 1) \equiv a_{\mathfrak{q}}(E') \pmod p$$

https://doi.org/10.4153/S0008414X22000311 Published online by Cambridge University Press

by comparing the traces of Frobenius. We see that this difference being also nonzero and depending only on $\mathfrak{q}$ gives a bound for p. ∎

Now, suppose that E' is 3-isogenous to an elliptic curve E''. As the isogeny induces an isomorphism $E'[p] \cong E''[p]$ of Galois modules ($p \neq 3$), we get $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p} \sim \overline{\rho}_{E'',p}$ completing the proof of (iii). After possibly replacing E' by E'', we can suppose that E' has a K-rational point of order 3 giving us (ii).

It remains to prove $v_\lambda(j') < 0$ where j' is the j-invariant of E'. By Lemma 5.2 of [27], p divides the size of $\overline{\rho}_{E,p}(I_\lambda)$. Now, Lemma 2.5 implies that $v_\lambda(j') < 0$ since the sizes of $\overline{\rho}_{E,p}(I_\lambda)$ and $\overline{\rho}_{E',p}(I_\lambda)$ are equal.

The following theorem of Katz is used in the proof of the above lemma.

Theorem 3.7 [18, Theorem 2] *Let E be an elliptic curve over a number field K, and let $m \geq 2$ be, an integer. For each prime $\mathfrak{p}$ of K at which E has good reduction let $N(\mathfrak{p})$ denote the number of $\mathbb{F}_\mathfrak{p}$-rational points on $E \bmod \mathfrak{p}$. If we have*

$$N(\mathfrak{p}) \equiv 0 \pmod{m}$$

for a set of primes $\mathfrak{p}$ of density one in K, then there exists a K-isogenous elliptic curve E' defined over K such that

$$\#(\operatorname{Tors} E'(K)) \equiv 0 \pmod{m}.$$

3.2 Irreducibility of Galois representations

Throughout this subsection, $K = \mathbb{Q}(\sqrt{-d})$, where $d \in \{1, 7, 19, 43, 67\}$, $(a, b, c) \in \mathcal{O}_K$, is a nontrivial, primitive, putative solution of the equation $x^p + y^p = z^3$.

The idea of this section is to prove that when p is bigger than an explicit constant, then the mod p Galois representation $\overline{\rho}_{E,p} : G_\mathbb{Q} \to \operatorname{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$ attached to E is absolutely irreducible.

We will use the following result of Freitas and Siksek.

Lemma 3.8 [13, Lemma 6.3] *Let E be an elliptic curve over a number field K with conductor $\mathcal{N}_E$, and let p be a prime > 5. Suppose that $\rho_p = \overline{\rho}_{E,p}$ is reducible. Write $\rho_p \sim \begin{pmatrix} \theta & * \\ 0 & \theta' \end{pmatrix}$, where $\theta, \theta' : G_K \to \mathbb{F}_p^*$ are the isogeny characters. Let $\mathcal{N}_\theta, \mathcal{N}_{\theta'}$ denote the conductors of these characters. Fix a prime $\mathfrak{q} \nmid p$ of $\mathcal{O}_K$.*

We have the following:

- *If E has good or multiplicative reduction at $\mathfrak{q}$, then $v_\mathfrak{q}(\mathcal{N}_\theta) = v_\mathfrak{q}(\mathcal{N}_{\theta'}) = 0$.*
- *If E has additive reduction at $\mathfrak{q}$, then $v_\mathfrak{q}(\mathcal{N}_E)$ is even and $v_\mathfrak{q}(\mathcal{N}_\theta) = v_\mathfrak{q}(\mathcal{N}_{\theta'}) = v_\mathfrak{q}(\mathcal{N}_E)/2$.*

Proposition 3.9 *Let E/K be the Frey curve attached to a putative solution to equation (1.1), and let $p > C_K$ be a prime where C_K is defined as below. Then $\overline{\rho}_{E,p}$ is irreducible.*

$C_K = 47$ if the equation $y^3 + 24b^p c\, y + 16b^{2p} \equiv 0 \pmod{\lambda^2}$ has a solution in the ring of integers of the local field K_λ, and otherwise $C_K = 44,483$.

https://doi.org/10.4153/S0008414X22000311 Published online by Cambridge University Press

Proof Suppose that $\rho_p = \overline{\rho}_{E,p}$ is reducible. Write $\rho_p \sim \begin{pmatrix} \theta & * \\ 0 & \theta' \end{pmatrix}$, where $\theta, \theta' : G_K \to \mathbb{F}_p^*$ are the isogeny characters. Let $\mathcal{N}_\theta, \mathcal{N}_{\theta'}$ denote the conductors of these characters. Fix a prime $\mathfrak{q} \nmid 3p$ of $\mathcal{O}_K$. By [13, Lemma 6.3], we get $v_\mathfrak{q}(\mathcal{N}_\theta) = v_\mathfrak{q}(\mathcal{N}_{\theta'}) = 0$ since E is semistable away from λ.

By Lemmas 2.4 and 3.8, $v_\lambda(\mathcal{N}_\theta) = v_\lambda(\mathcal{N}_{\theta'}) \in \{0, 1\}$.

Now, we deal with $\mathfrak{p}|p$.

(1) Say $\mathcal{N}_\theta$ or $\mathcal{N}_{\theta'}$ is relatively prime to p. Note that interchanging θ and θ' corresponds to replacing E with an isogenous elliptic curve $E/\ker\theta$. Since $\ker\theta$ is a K-rational subgroup of $E[p]$ of order p, the elliptic curves E and $E/\ker\theta$ are p-isogenous. Therefore, without loss of generality, assume that $(p, \mathcal{N}_\theta) = 1$ and $v_\mathfrak{p}(\mathcal{N}_\theta) = 0$ for all $\mathfrak{p}|p$ as in the previous case. We also have $v_\mathfrak{q}(\mathcal{N}_\theta) = 0$ for all $\mathfrak{q} \nmid 3p$, as explained above. Therefore, $\mathcal{N}_\theta = \lambda^m$, where $m = 0$ or 1, which implies that θ is a character of the ray class group of modulus λ^m of K.

Using `Magma`, we computed the ray class groups for these moduli and get the following groups only:

$$\{1\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}.$$

- If the order of θ is one then θ is trivial. Then $\rho_p \sim \begin{pmatrix} 1 & * \\ 0 & \theta' \end{pmatrix}$, and this implies that E has a K-rational point of order p. By Lemma 2.4, E has also a point of order 3, then $E(K)$ has a $3p$-torsion point, but by the work of Kamienney, Kenku, and Momose [16, 19], this is not possible when $p \geq 7$, hence a contradiction.
- If the order of θ is two, then we can conclude that E has a point of order $3p$ over a quadratic extension L of K and get a contradiction since, by [8], $E(L)[p] = \{0\}$ if $p > 17$. Here, L is the number field cut out by the character θ^2, i.e., $|L : \mathbb{Q}| = 4$.
- If the order of θ is four, let L be the unique quadratic extension of K cut out by θ^2. Then θ_{G_L} is quadratic. Let E' be the twist of E by θ_{G_L}. The elliptic curve E' is also over L and has a point of order p as in the previous case. Again, we get a contradiction by [8].

(2) Now, we are left with the case that neither $\mathcal{N}_\theta$ nor $\mathcal{N}_{\theta'}$ is relatively prime to p. Recall that E is semistable away from λ and p is not ramified in K. Then either p is inert or p splits in K.

(a) p is inert in K: By [13, Corollary 6.2], E cannot have good supersingular reduction at p. Therefore, E has good ordinary or multiplicative reduction at p and

$$\rho_p|_{I_p} \sim \begin{pmatrix} \chi_p & * \\ 0 & 1 \end{pmatrix} \tag{3.1}$$

(see [4, Section 3]), where χ_p is the mod p cyclotomic character. By [21, Lemma 1], p has to be relatively prime with $\mathcal{N}_\theta$ or $\mathcal{N}_{\theta'}$, which contradicts to the assumption of item (2).

(b) p splits in K: Say $p = \mathcal{P}\mathcal{P}'$ and $\mathcal{P}|\mathcal{N}_\theta, \mathcal{P}' \nmid \mathcal{N}_\theta$ and $\mathcal{P} \nmid \mathcal{N}_{\theta'}, \mathcal{P}'|\mathcal{N}_{\theta'}$. By [13, Corollary 6.2], we know that E has good ordinary or multiplicative reduction

https://doi.org/10.4153/S0008414X22000311 Published online by Cambridge University Press

at $\mathcal{P}$ and $\mathcal{P}'$ by equation (3.1), we see that one of the characters θ, θ' is ramified at $\mathcal{P}$ and the other is ramified at $\mathcal{P}'$, $\theta|_{I_\mathcal{P}} = \chi_p|_\mathcal{P}$, and $\theta'|_{I_{\mathcal{P}'}} = \chi_p|_{\mathcal{P}'}$. Hence, θ is unramified away from $\mathcal{P}$ and λ since all bad places of E except possibly λ are of potentially multiplicative reduction.

(i) λ divides ab: In this case, by Lemma 2.4, E has multiplicative or good reduction at λ; therefore, we can say that θ is unramified away from $\mathcal{P}$. The character $\theta^2|_{I_\mathcal{P}} = \chi_p^2|_{I_\mathcal{P}}$ is also unramified away from $\mathcal{P}$; therefore, by [31, Lemma 4.3], $\theta(\sigma_\lambda) \equiv \mathrm{Norm}_{K_\mathcal{P}/\mathbb{Q}_p}(\alpha)^2 \pmod p$, where σ_λ is the Frobenius automorphism at $\lambda = \langle 3 \rangle$. We also know that, by [27, Lemma 6.3], $\theta^2(\sigma_\lambda) \equiv 1 \pmod p$ (note that E has multiplicative reduction at λ). Therefore, we have $p|\mathrm{Norm}_{K_\mathcal{P}/\mathbb{Q}_p}(\lambda)^2 - 1$, a contradiction since $p > 20$.

(ii) λ does not divide ab: In this case, by Lemma 2.4, E has additive reduction at λ, so the above argument fails. Recall that $v_\lambda(\Delta_E) = v_\lambda(3^3 b^{3p} a^p) = 3$ and $v_\lambda(c_6(E)) = 3$. By [20, p. 356], we see that θ^4 or θ^{12} is unramified at λ. The case θ^{12} happens when the equation $y^3 + 24b^p cy + 16b^{2p} \equiv 0 \pmod \lambda^2$ does not have a solution. Therefore, we have $\theta^4|_{I_\mathcal{P}} = \chi_p^4|_{I_\mathcal{P}}$ is unramified away from $\mathcal{P}$ or $\theta^{12}|_{I_\mathcal{P}} = \chi_p^{12}|_{I_\mathcal{P}}$ is unramified away from $\mathcal{P}$.

By [31, Lemma 4.3], $\theta^4(\sigma_\mathfrak{P}) \equiv \mathrm{Norm}_{K_\mathcal{P}/\mathbb{Q}_p}(\alpha)^2 = 9 \pmod p$, where α is a nonzero prime-to-p element of K and $\sigma_\mathfrak{P}$ is the Frobenius automorphism at $\mathfrak{P} = \langle \alpha \rangle$. Therefore, the polynomial $x^4 - 9$ has a root $\theta(\sigma_\mathfrak{P})$ modulo p. Recall that E has potentially good reduction at λ since $v_\lambda(j_E) > 0$. Let $P_\lambda(x)$ be the characteristic polynomial of the Frobenius of E at λ. Since $\rho_p \sim \begin{pmatrix} \theta & * \\ 0 & \theta' \end{pmatrix}$, we get $P_\lambda(x) \equiv (x - \theta(\sigma_\lambda))(x - \theta'(\sigma_\lambda)) \pmod p$.

Hence, we can conclude that $p|\,\mathrm{Res}(x^4 - 9, P_\lambda(x))$, where Res denotes the resultant of the polynomials. Note that $P_\lambda(x) \in \mathbb{Z}[x]$ and its roots have absolute value less than or equal to $\sqrt{\mathrm{Norm}(\lambda)} = 3$ (see [6, Proposition 1.6]). Then the possibilities for $P_\lambda(x)$ are as follows:

$$P_1(x) = x^2 + 9, P_2(x) = x^2 - x + 9, P_3(x) = x^2 - 2x + 9,$$

$$P_4(x) = x^2 + x + 9, P_5(x) = x^2 + 2x + 9,$$

$$P_6(x) = x^2 + 3x + 9, P_7(x) = x^2 - 3x + 9, P_8(x) = x^2 + 4x + 9,$$

$$P_9(x) = x^2 - 4x + 9,$$

$$P_{10}(x) = x^2 + 5x + 9, P_{11}(x) = x^2 - 5x + 9, P_{12}(x) = x^2 + 6x + 9,$$

$$P_{13}(x) = x^2 - 6x + 9.$$

We computed these 13 resultants, and none of them has a prime divisor greater than 47. Since $p > 47$, we get a contradiction.

For the case of $\theta^{12}|_{I_\mathcal{P}} = \chi_p^{12}|_{I_\mathcal{P}}$, similarly we need to compute the resultants of P_i with $x^{12} - 9$ and see that none of them has a prime divisor greater than 44, 483. ∎

https://doi.org/10.4153/S0008414X22000311 Published online by Cambridge University Press

In this corollary, we will summarize the cases where we have absolute irreducibility.

Corollary 3.10 (1) *Let p be odd. If $\lambda | ab$ and $\overline{\rho}_{E,p}$ is irreducible, then $\overline{\rho}_{E,p}$ is absolutely irreducible.*

(2) *Assume that $\lambda \nmid ab$. Let K be an imaginary quadratic field, and let $p > M_K$ for some effectively computable constant M_K depending only on K.*
   (a) *Say p splits in K and $p \equiv 3 \pmod 4$. If $\overline{\rho}_{E,p}$ is irreducible, then $\overline{\rho}_{E,p}$ is absolutely irreducible.*
   (b) *Say $p \equiv 1 \pmod 3$ and $\overline{\rho}_{E,p}(I_\lambda)$ is divisible by 3 (which means that the inertia has order 12 and this happens if and only if $y^3 + 24b^p c\, y + 16b^{2p} \equiv 0 \pmod{\lambda^2}$ does not have a solution). If $\overline{\rho}_{E,p}$ is irreducible, then $\overline{\rho}_{E,p}$ is absolutely irreducible.*

(3) *Let p be odd. If K is totally real, then $\overline{\rho}_{E,p}$ is irreducible if and only if it is absolutely irreducible.*

Proof (1) The Frey curve E attached to a putative primitive solution $(a, b, c) \in \mathcal{O}_K^3$ of $x^p + y^p = z^3$ is semistable when $\lambda | ab$ where λ is the prime of $\mathcal{O}_K$ lying over 3. These were discussed in Lemma 2.4. By Proposition 3.9, we know that $\overline{\rho}_{E,p}$ is irreducible when p is big enough. In Proposition 3.9, we make this bound explicit. Recall that the j-invariant of E is $j_E = \frac{3^3 c^3 (9a^p + b^p)^3}{(ab^3)^p}$. Therefore, $v_\lambda(j_E) = 3v_\lambda(3) - 3pv_\lambda(b) < 0$ and $p \nmid v_\lambda(j_E)$ when $p > 5$. Therefore, by the theory of Tate curve, the inertia group I_λ contains an element which acts on $E[p]$ via $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ which has order p. By Theorem 2.7, the image $\overline{\rho}_{E,p}$ contains $\mathrm{SL}_2(\mathbb{F}_p)$ and hence is an absolutely irreducible group of $\mathrm{GL}_2(\mathbb{F}_p)$.

(2) Assume that $\lambda \nmid ab$. We will use the below theorem of Larson and Vaintrob (Theorem 3.11).

Assume that $\overline{\rho}_{E,p}$ is irreducible but absolutely reducible. Then, by Part 1 of Theorem 2.7, p cannot divide the order of $\overline{\rho}_{E,p}(G_K)$. By the second part of the same theorem, for big enough p, the image $\overline{\rho}_{E,p}(G_K)$ is in a nonsplit Cartan subgroup or it is in the normalizer of a Cartan subgroup but not in the Cartan itself. Now, we will rule out the second case. Say $\overline{\rho}_{E,p}(G_K)$ has an element g which is not in nonsplit Cartan but in the normalizer of nonsplit Cartan. Let h be any element of the nonsplit Cartan subgroup different from the identity element. Then h and g do not share a common eigenvector, and this contradicts to the assumption that $\overline{\rho}_{E,p}(G_K)$ is absolutely reducible.

Similar argument can be made if $\overline{\rho}_{E,p}(G_K)$ is in the normalizer of a split Cartan case but not in the split Cartan itself.

Therefore, we can conclude that $\overline{\rho}_{E,p}(G_K)$ is in a nonsplit Cartan subgroup. The rest of the argument is similar as in [24]. Up to conjugation, $\overline{\rho}_{E,p} \otimes \mathbb{F}_p \sim \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^p \end{pmatrix}$, where $\lambda : G_K \to \mathbb{F}_{p^2}$ and $\lambda^{p+1} = \chi_p$, where χ_p is the cyclotomic character.

   (a) Assume that p splits in K and $p \equiv 3 \pmod 4$. We will assume that $\overline{\rho}_{E,p}$ is irreducible but absolutely reducible and get a contradiction. We will apply

https://doi.org/10.4153/S0008414X22000311 Published online by Cambridge University Press

the above theorem to the elliptic curve E attached to a putative solution of equation (1.1). Assuming that the prime p is greater than the constant given in the theorem, we get a complex multiplication (CM) elliptic curve E'/K with $\overline{\rho}_{E',p} \otimes \overline{\mathbb{F}}_p \sim \begin{pmatrix} \theta & 0 \\ 0 & \theta' \end{pmatrix}$ such that $\theta^{12} = \lambda^{12}$.

Since p splits in K, we see that the image $\overline{\rho}_{E',p}(G_K)$ is contained inside a split Cartan subgroup, which implies that the character θ is in fact $\mathbb{F}_p$-valued. In particular, the order of θ is divisible by $p-1$.

We also know that, by Theorem 1 of [22], $\lambda\theta^{-1}$ is unramified away from the additive primes of E. Therefore, $\lambda\theta^{-1}$ is unramified at $\mathcal{P}|p$. Since $\lambda^{p+1} = \chi_p$, we get $\theta^{p+1}|_{I_\mathcal{P}} = \chi_p|_{I_\mathcal{P}}$. Note that $p \equiv 3 \pmod 4$, $\frac{p-1}{2}$ is odd. We deduce that $\chi_p^{(p-1)/2}|_{I_\mathcal{P}} = (\theta^{p-1})^{(p+1)/2}|_{I_\mathcal{P}} = 1$. However, the order of $\chi_p^{(p-1)/2}|_{I_\mathcal{P}}$ is $p-1$ since it surjects on $\mathbb{F}_p^*$.

(b) If $\overline{\rho}_{E,p}(I_\lambda)$ is divisible by 3, then there exists an element $g \in \overline{\rho}_{E,p}(I_\lambda)$ which has order 3, and hence $\lambda(g) \in \mathbb{F}_{p^2}^\times$ has order 3. Moreover, note that χ_p is unramified at p. Therefore, $\chi_p(g) = \lambda^{p+1}(g) = 1$, which implies that $3|p+1$.

(3) When K is totally real, then the absolute Galois group G_K contains a complex conjugation. The image of this complex conjugation under $\overline{\rho}_{E,p}$ is similar to $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, which implies that if $\overline{\rho}_{E,p}$ is irreducible, then it is absolutely irreducible. ∎

The following theorem of Larson and Vaintrob is used in the proof of the above corollary.

Theorem 3.11 [22, Theorem 1] *Let K be a number field. There exists a finite set of primes M_K, depending only on K, such that, for any prime $p \notin M_K$ and any elliptic curve E/K for which $\overline{\rho}_{E,p} \otimes \overline{\mathbb{F}}_p$ is conjugate to $\begin{pmatrix} \lambda & * \\ 0 & \lambda' \end{pmatrix}$ where $\lambda, \lambda' : G \to \mathbb{F}_p^\times$ are characters, one of the following happens.*

(1) *There exists an elliptic curve E'/K with CM, whose CM field is contained in K, with $\overline{\rho}_{E',p} \otimes \overline{\mathbb{F}}_p$ is conjugate to $\begin{pmatrix} \theta & * \\ 0 & \theta' \end{pmatrix}$ and such that $\theta^{12} = \lambda^{12}$.*

(2) *The Generalized Riemann Hypothesis (GRH) fails for $K = \mathbb{Q}(\sqrt{-p})$ and $\theta^{12} = \chi_p^6$. Moreover, in this case, $\overline{\rho}_{E',p}$ is already reducible over $\mathbb{F}_p$ and $p \equiv 3 \pmod 4$.*

4 Proof of Theorem 1.1

In this section, we will prove Theorem 1.1.

Let K be a number field with $h_K^+ = 1$ satisfying Conjectures 2.2 and 2.3 and containing $\mathbb{Q}(\zeta_3)$ where ζ_3 is a primitive third root of unity. Assume that λ is the only prime of K above 3. Let B_K be as in Theorem 3.1, and let $(a, b, c) \in W_K$ be a nontrivial solution to the Fermat equation with signature $(p, p, 3)$ given in (1.1). We now apply Theorem 3.1 and obtain an elliptic curve E'/K having a K-rational point of order 3 and (potentially) good reduction away from λ with j-invariant j' satisfying $v_\lambda(j') < 0$.

https://doi.org/10.4153/S0008414X22000311 Published online by Cambridge University Press

n	$\lvert\mathcal{F}_n\rvert$	$\lvert\mathcal{K}_n\rvert$
4	998, 395	28, 750
6	605, 497	20, 320
8	26, 361	1, 264
10	895, 218	51, 527
12	67, 466	750

Table 1: Numerical examples.

However, by Theorem 4.1 applied with $\ell = 3$, there is no such an elliptic curve, which gives us a contradiction.

Theorem 4.1 [11, Theorem 1] *Let ℓ be a rational prime. Let K be a number field satisfying the following conditions:*

- *$\mathbb{Q}(\zeta_\ell) \subset K$, where ζ_ℓ is a primitive ℓth root of unity;*
- *K has a unique prime λ above ℓ;*
- *$gcd(h_K^+, \ell(\ell-1)) = 1$, where h_K^+ is the narrow class number of K.*

Then there is no elliptic curve E/K with a K-rational ℓ-isogeny, good reduction away from λ, potentially multiplicative reduction at λ.

Remark 4.2 Since we assume that $\mathbb{Q}(\zeta_3) \subset K$, the triple $(\zeta_3, \zeta_3^2, 1)$ is a nontrivial solution to equation (1.1) in $\mathcal{O}_K$. However, as ζ_3 is a unit in $\mathcal{O}_K$, the prime λ does not divide $(\zeta_3) = \mathcal{O}_K$, so $(\zeta_3, \zeta_3^2, 1) \notin W_K$.

4.1 Numerical examples

Let $\mathcal{F}_n$ denote the set of number fields of degree n and class number 1 with discriminant less than D_n, where D_n is 10^8 if $n = 4, 6, 8$ and 10^{16} if $n = 10, 12$. Let $\mathcal{K}_n$ denote the subset of $\mathcal{F}_n$ such that if $K \in \mathcal{K}_n$, then K satisfies the following:

- $\mathbb{Q}(\zeta_3) \subset K$;
- the narrow class number of K is 1;
- there is only one prime ideal of K lying above 3.

We computed the complete sets $\mathcal{F}_n$ and $\mathcal{K}_n$ for $n = 4, 6, 8, 10, 12$ in the John Jones `Number Field Database` [15]. The cardinalities of these sets are given in Table 1, and details can be found online at https://sites.google.com/view/erman-isik/research?authuser=0.

It then follows from Theorem 1.1 that, for any K that belongs to $\mathcal{K}_n$, the asymptotic FLT holds for W_K.

5 Proof of Theorem 1.2

In this section, we will prove Theorem 1.2. One of the main steps toward the proof is to lift mod p eigenforms to complex ones. Recall that it follows from Proposition 2.1 that

https://doi.org/10.4153/S0008414X22000311 Published online by Cambridge University Press

there is a constant $B(\mathfrak{N})$ such that, for $p > B(\mathfrak{N})$, all weight-two, mod p eigenforms lift to complex ones. However, we want to make this bound explicit for the fields we consider for Theorem 1.2. Before the proof of Theorem 1.2, we will state the key point to overcome this difficulty. Note that our approach follows closely [31, Section 2] and [27, Sections 2 and 3].

Let K be a number field with the integer ring $\mathcal{O}_K$, and let $\mathfrak{N}$ be an ideal of $\mathcal{O}_K$. Assume that p is a rational prime unramified in K and relatively prime to $\mathfrak{N}$. Consider the following short exact sequence given by a multiplication-by-p map

$$0 \to \mathbb{Z}_{(p)} \xrightarrow{\times p} \mathbb{Z}_{(p)} \to \mathbb{F}_p \to 0,$$

where $\mathbb{Z}_{(p)}$ denotes the ring of rational numbers with denominators prime to p.

This exact sequence gives rise to a long exact sequence on the cohomology groups from which we can extract the following short exact sequence:

$$0 \to H^1(Y_0(\mathfrak{N}), \mathbb{Z}_{(p)}) \otimes \mathbb{F}_p \to H^1(Y_0(\mathfrak{N}), \mathbb{F}_p) \to H^2(Y_0(\mathfrak{N}), \mathbb{Z}_{(p)})[p] \to 0, \tag{5.1}$$

where $H^2(Y_0(\mathfrak{N}), \mathbb{Z}_{(p)})[p]$ denotes the p-torsion subgroup of $H^2(Y_0(\mathfrak{N}), \mathbb{Z}_{(p)})$. Hence, we deduce that the p-torsion subgroup of $H^2(Y_0(\mathfrak{N}), \mathbb{Z}_{(p)})$ is trivial if and only if the reduction map from $H^1(Y_0(\mathfrak{N}), \mathbb{Z}_{(p)})$ to $H^1(Y_0(\mathfrak{N}), \mathbb{F}_p)$ is surjective. As explained in [27, 31], we see that, for primes $p > 3$, if the group $H^2(\Gamma_0(\mathfrak{N}), \mathbb{Z}_{(p)})$ has a nontrivial p-torsion element, then $\Gamma_0(\mathfrak{N})^{\mathrm{ab}}$ will have a p-torsion as well. If $H^2(Y_0(\mathfrak{N}), \mathbb{Z}_{(p)})$ has only trivial p-torsion, then we deduce that the map

$$H^1(Y_0(\mathfrak{N}), \mathbb{Z}_{(p)}) \otimes \mathbb{F}_p \xrightarrow{\delta} H^1(Y_0(\mathfrak{N}), \mathbb{F}_p)$$

is surjective. Therefore, any Hecke eigenvector in $H^1(Y_0(\mathfrak{N}), \mathbb{F}_p)$ comes from such an eigenvector in $H^1(Y_0(\mathfrak{N}), \mathbb{Z}_{(p)}) \otimes \mathbb{F}_p$. We can now utilize a lifting lemma of Ash and Stevens [1, Proposition 1.2.2] to deduce that, by fixing an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, we can regard a cohomology class in $H^1(Y_0(\mathfrak{N}), \mathbb{Z}_{(p)})$ as a class in $H^1(Y_0(\mathfrak{N}), \mathbb{C})$.

The existence of an eigenform (complex or mod p) is equivalent to the existence of a cohomology class in the corresponding cohomology group that is a simultaneous eigenvector for the Hecke operators such that its eigenvalues match the values of the eigenform. With this interpretation, we see that, for $p > 3$, the mod p eigenforms lift to complex eigenforms whenever the abelianization $\Gamma_0(\mathfrak{N})^{\mathrm{ab}}$ has only trivial p-torsion element.

5.1 Proof of Theorem 1.2

Let $K = \mathbb{Q}(\sqrt{-d})$ with $d \in \{1, 7, 19, 43, 67\}$, and let λ denote the prime ideal of K lying above 3. Suppose that $(a, b, c) \in \mathcal{O}_K^3$ is a nontrivial primitive solution to equation (1.1).

Let $\overline{\rho}_{E,p}$ be the residual Galois representation induced by the action of G_K on $E[p]$. We want to apply Conjecture 2.2 to $\overline{\rho}_{E,p}$. Note that in order to do this, we need $\overline{\rho}_{E,p}$ to be absolutely irreducible. It follows from Corollary 3.10 that $\overline{\rho}_{E,p}$ is absolutely irreducible under the assumptions of Theorem 1.2 and hence satisfies the hypotheses of Conjecture 2.2. This will be explained in Cases I and II below. For now, let us assume that Conjecture 2.2 is applicable. Applying this conjecture, we deduce that there exists

https://doi.org/10.4153/S0008414X22000311 Published online by Cambridge University Press

Number fields	$\mathrm{val}_\lambda(\mathfrak{N}_E)$	Primes ℓ such that $\Gamma_0(\mathfrak{N}_E)^{\mathrm{ab}}[\ell] \neq 0$
$\mathbb{Q}(i)$	1,2,3	2,3
$\mathbb{Q}(\sqrt{-7})$	1,2,3	2,3
$\mathbb{Q}(\sqrt{-19})$	1,2,3	2,3 ,5
$\mathbb{Q}(\sqrt{-43})$	1,2,3	2,3,5,59,67,199
$\mathbb{Q}(\sqrt{-67})$	1,2,3	2,3,5,17,19,37,47,67

Table 2: Prime torsions in $\Gamma_0(\mathfrak{N}_E)^{\mathrm{ab}}$.

a weight-two, mod p eigenform θ over K of level $\mathfrak{N}_E$ such that, for all primes $\mathfrak{q}$ coprime to $p\mathfrak{N}_E$, we have

$$\mathrm{Tr}(\overline{\rho}_{E,p}(\mathrm{Frob}_\mathfrak{q})) = \theta(T_\mathfrak{q}),$$

where $T_\mathfrak{q}$ denotes the Hecke operator at $\mathfrak{q}$.

Recall that $\mathfrak{N}_E$ denotes the Serre conductor of the residual representation $\overline{\rho}_{E,p}$, which is a power of λ. We now aim to lift this mod p Bianchi modular form to a complex one.

We compute the abelianizations $\Gamma_0(\mathfrak{N}_E)^{\mathrm{ab}}$ implementing the algorithm of Şengün [26]. One can access to the relevant `Magma` codes online at https://warwick.ac.uk/fac/sci/maths/people/staff/turcas/fermatprog. The results of the algorithm can be found at https://sites.google.com/view/erman-isik/research?authuser=0. We record here the primes ℓ that appear as orders of torsion elements of $\Gamma_0(\mathfrak{N}_E)^{\mathrm{ab}}$ for each number field in Table 2.

Assume that ℓ_K is the largest prime in Table 2 related to the number field K, and that $p > \ell_K$. It then follows that the p-torsion subgroups of $\Gamma_0(\mathfrak{N}_E)^{\mathrm{ab}}$ are all trivial, so the mod p eigenforms must lift to complex ones. The procedure explained at the beginning of Section 5 together with Conjecture 2.2 implies that there exists a (complex) Bianchi modular form $\mathfrak{f}$ over K of level $\mathfrak{N}_E$ such that, for all prime ideals $\mathfrak{q}$ coprime to $p\mathfrak{N}_E$, we have

$$\mathrm{Tr}(\overline{\rho}_{E,p}(\mathrm{Frob}_\mathfrak{q})) \equiv \mathfrak{f}(T_\mathfrak{q}) \pmod{\mathfrak{p}},$$

where $\mathfrak{p}$ is a prime ideal of $\mathbb{Q}_\mathfrak{f}$ lying above p and $\mathbb{Q}_\mathfrak{f}$ is the number field generated by the eigenvalues. Let us denote this relation by $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\mathfrak{p}}$.

Recall that the constants C_K and M_K were defined in Proposition 3.9 and in Corollary 3.10.

5.2 Case I

Assume that the prime ideal λ of K lying above 3 divides b. Note that, in this case, the associated Frey curve is semistable by Lemma 2.4. By Proposition 3.9, $\overline{\rho}_{E,p}$ is irreducible when $p > C_K$. By Part 1 of Corollary 3.10, $\overline{\rho}_{E,p}$ is absolutely irreducible if it is irreducible. Therefore, Conjecture 2.2 is applicable to $\overline{\rho}_{E,p}$. When we apply Conjecture 2.2 and the lifting argument above, we see that the corresponding Bianchi

https://doi.org/10.4153/S0008414X22000311 Published online by Cambridge University Press

modular form $\mathfrak{f}$ is of level 1 or λ. Since there are no Bianchi newforms at these levels over K, it follows that Theorem 1.2 holds true for $p > \max\{\ell_K, C_K\}$. This proves Case I of Theorem 1.2.

5.3 Case II

Assume now that λ does not divide b.

In this case, we do not have the absolute irreducibility of $\overline{\rho}_{E,p}$ for all primes p as illustrated in Corollary 3.10. Therefore we need the restrictions in the statement of Part II of Theorem 1.2, i.e., $p \equiv 3 \bmod 4$ and p splits in K. Under these restrictions and when $p > \max\{C_K, M_K\}$, $\overline{\rho}_{E,p}$ is absolutely irreducible by Corollary 3.10. We also need $p > \ell_K$ to lift the mod p eigenforms to complex ones as explained above. Therefore, from now on, we assume that $p > B_K = \max\{C_K, M_K, \ell_K\}$.

Recall that, in this case, the associated Frey curve is semistable away from λ and the power of λ in the conductor of E is 2 or 3 by Lemma 2.4. Then the corresponding Bianchi modular form is of level dividing λ^3.

Lemma 5.1 *Let us fix a prime ideal* $\mathfrak{q} \neq \lambda$ *of* K*, and let* $\mathfrak{f}$ *be a newform of level dividing* λ^3*. Define the following set:*

$$\mathcal{A}(\mathfrak{q}) = \{a \in \mathbb{Z} \,:\, |a| \leq 2\sqrt{\mathrm{Norm}(\mathfrak{q})},\ \mathrm{Norm}(\mathfrak{q}) + 1 - a \equiv 0 \pmod 3\}.$$

If $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\mathfrak{p}}$*, where* $\mathfrak{p}$ *is the prime ideal of* $\mathbb{Q}_\mathfrak{f}$ *lying above* p*, then* $\mathfrak{p}$ *divides*

$$B_{\mathfrak{f},\mathfrak{q}} := \mathrm{Norm}(\mathfrak{q}) \cdot \left(\mathrm{Norm}(\mathfrak{q}+1)^2 - \mathfrak{f}(T_\mathfrak{q})^2\right) \cdot \prod_{a \in \mathcal{A}(\mathfrak{q})} (a - \mathfrak{f}(T_\mathfrak{q}))\mathcal{O}_{\mathbb{Q}_\mathfrak{f}}.$$

Proof If $\mathfrak{q}|p$, then $\mathrm{Norm}(\mathfrak{q})$ is a power of p. Now, assume that $\mathfrak{q}$ does not divide p. Then the Frey curve E has semistable reduction at $\mathfrak{q}$. If it has a good reduction, then we have

$$\mathrm{Tr}(\overline{\rho}_{E,p}(\mathrm{Frob}_\mathfrak{q})) \equiv a_\mathfrak{q}(E) \equiv \mathfrak{f}(T_\mathfrak{q}) \pmod{\mathfrak{p}}.$$

Note that, by Lemma 2.4, the Frey curve E, given in (2.3), has a 3-torsion point, so 3 divides $\#E(\mathbb{F}_\mathfrak{q}) = \mathrm{Norm}(\mathfrak{q}) + 1 = a_\mathfrak{q}(E)$. By the Hasse–Weil bound, we know that $|a_\mathfrak{q}(E)| \leq 2\sqrt{\mathrm{Norm}(\mathfrak{q})}$. So $a_\mathfrak{q}(E)$ belongs to the finite set $\mathcal{A}(\mathfrak{q})$. Finally, suppose that E has multiplicative reduction at $\mathfrak{q}$. Then, by comparing the traces of the images of Frobenius at $\mathfrak{q}$ under $\overline{\rho}_{E,p}$, we have

$$\pm(\mathrm{Norm}(\mathfrak{q}) + 1) \equiv \mathfrak{f}(T_\mathfrak{q}) \pmod{\mathfrak{p}}.$$

It then follows that $\mathfrak{p}$ divides $(\mathrm{Norm}(\mathfrak{q}) + 1)^2 - \mathfrak{f}(T_\mathfrak{q})^2$. Hence, $\mathfrak{p}$ divides $B_{\mathfrak{f},\mathfrak{q}}$. ∎

Using `Magma`, we computed the cuspidal newforms at the predicted levels, the fields $\mathbb{Q}_\mathfrak{f}$, and eigenvalues $\mathfrak{f}(T_\mathfrak{q})$ at the prime ideals $\mathfrak{q}$ of norm less that 50 for each imaginary quadratic number field $K = \mathbb{Q}(\sqrt{-d})$ with $d \in \{1, 7, 19, 43, 67\}$. For each modular form $\mathfrak{f}$ of level dividing λ^3, we computed the ideal

$$B_\mathfrak{f} := \sum_{\mathfrak{q} \in S} B_{\mathfrak{f},\mathfrak{q}},$$

https://doi.org/10.4153/S0008414X22000311 Published online by Cambridge University Press

where S denotes the set of prime ideals $\mathfrak{q} \neq \lambda$ of K of norm less than 50. The algorithm that we implemented and the results for the following fields can be found online at https://sites.google.com/view/erman-isik/research?authuser=0.

Set $C_\mathfrak{f} := \mathrm{Norm}_{\mathbb{Q}_\mathfrak{f}/\mathbb{Q}}(B_\mathfrak{f})$. It then follows from Lemma 5.1 that if $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\mathfrak{p}}$, then p divides $C_\mathfrak{f}$. Note that it is possible to find $C_\mathfrak{f} = 0$. In this case, we need to deal with such modular forms individually.

We say that an elliptic curve C/K of conductor $\mathcal{N} \subset \mathcal{O}_K$ corresponds to a cuspidal Bianchi modular form F for $\Gamma_0(\mathcal{N})$, if the L-series $L(C/K, s)$ attached to C/K is equal to the Mellin transform $L(F, s)$ of F.

(1) If $K = \mathbb{Q}(i)$, then there is no Bianchi modular form at level λ^ε where $\varepsilon = 1, 2$. There is only one modular form at level λ^3. For this modular form, we have $C_\mathfrak{f} = 0$ and $\mathbb{Q}_\mathfrak{f} = \mathbb{Q}$. The elliptic curves in the isogeny class given in the LMFDB label `2.0.4.1-729.1-a` correspond to this form. All the elliptic curves in this class are defined over $\mathbb{Q}$ and have CM.

(2) If $K = \mathbb{Q}(\sqrt{-7})$, then there is no Bianchi modular form at level λ^ε with $\varepsilon = 1, 2$. There are three modular forms at level λ^3. For one of these forms, $C_\mathfrak{f}$ is divisible by 2 and 5, and for the other, $C_\mathfrak{f}$ is divisible by 2 and 7. For the third modular form, we get $C_\mathfrak{f} = 0$, and $\mathbb{Q}_\mathfrak{f} = \mathbb{Q}$. The elliptic curves in the isogeny class given in the LMFDB label `2.0.7.1-729.1-a` correspond to this cuspidal form. All the elliptic curves in this class are defined over $\mathbb{Q}$ and have CM.

(3) If $K = \mathbb{Q}(\sqrt{-19})$, then there is no Bianchi modular form at level λ. There are two Bianchi modular forms at level λ^2. For both of these forms, $C_\mathfrak{f}$ is divisible by 2. There are three modular forms at level λ^3. For one of these forms, $C_\mathfrak{f}$ is divisible by 7, and for the other, $C_\mathfrak{f}$ is divisible by 2 and 17. For the third modular form, we get $C_\mathfrak{f} = 0$ and $\mathbb{Q}_\mathfrak{f} = \mathbb{Q}$. The elliptic curves in the isogeny class given in the LMFDB label `2.0.19.1-729.1-a` correspond to this modular form. All the elliptic curves in this class are defined over $\mathbb{Q}$ and have CM.

(4) If $K = \mathbb{Q}(\sqrt{-43})$, then there is no Bianchi modular form at level λ. There are two Bianchi modular forms at level λ^2. For one of these forms, $C_\mathfrak{f}$ is divisible by 2 and 5, and for the other, $C_\mathfrak{f}$ is a power of 2. There are three modular forms at level λ^3. For one of these modular forms, $C_\mathfrak{f}$ is one, and for the other modular form, $C_\mathfrak{f}$ is divisible by 2 and 23. For the third modular form, we get $C_\mathfrak{f} = 0$, and $\mathbb{Q}_\mathfrak{f} = \mathbb{Q}$. The elliptic curves in the isogeny class given in the LMFDB label `2.0.43.1-729.1-a` correspond to this Bianchi modular form. All the elliptic curves in this class are defined over $\mathbb{Q}$ and have CM.

(5) If $K = \mathbb{Q}(\sqrt{-67})$, then there is no Bianchi modular form at level λ. There are two Bianchi modular forms at level λ^2. For both of these forms, $C_\mathfrak{f}$ is divisible by 2. At level λ^3, we find three modular forms. For one of these modular forms, $C_\mathfrak{f}$ is one, and for the other, $C_\mathfrak{f}$ is divisible by 11 and 19. For the third modular form, we get $C_\mathfrak{f} = 0$ and $\mathbb{Q}_\mathfrak{f} = \mathbb{Q}$. The elliptic curves in the isogeny class given in the LMFDB label `2.0.67.1-729.1-a` correspond to this modular form. All the elliptic curves in this class are defined over $\mathbb{Q}$ and have CM.

If $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\mathfrak{p}}$, then by Lemma 5.1 we have $p | C_\mathfrak{f}$. Since $p > B_K$ and B_K is large enough, the isomorphism $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\mathfrak{p}}$ is impossible when $C_\mathfrak{f} \neq 0$. If $C_\mathfrak{f} = 0$, then the Bianchi modular forms correspond to elliptic curves defined over $\mathbb{Q}$ with CM. Let

https://doi.org/10.4153/S0008414X22000311 Published online by Cambridge University Press

$\overline{\rho}_{E',p} : G_K \to \mathrm{GL}_2(\mathbb{F}_p)$ denote the mod p Galois representation attached to E', where E' is an elliptic curve that corresponds to the Bianchi modular form with $C_{\mathfrak{f}} = 0$. Then, for all but finitely many primes $\mathfrak{q} \subset \mathcal{O}_K$, we have $\mathrm{Tr}(\overline{\rho}_{E,p}(\mathrm{Frob}_{\mathfrak{q}})) = \mathrm{Tr}(\overline{\rho}_{E',p}(\mathrm{Frob}_{\mathfrak{q}}))$. Since the set of Frobenius elements is dense in G_K and the representation $\overline{\rho}_{E,p}$ is irreducible, it follows from Brauer–Nesbitt theorem (see [3], and for our application, see [9, Theorem 5.7]) that $\overline{\rho}_{E,p}$ and $\overline{\rho}_{E',p}$ are isomorphic.

To complete the proof, we must eliminate the possibility that $\overline{\rho}_{E,p}$ and $\overline{\rho}_{E',p}$ are isomorphic. Recall that, by Corollary 3.10, the mod p Galois representation $\overline{\rho}_{E,p}$ is absolutely irreducible, but $\overline{\rho}_{E',p}$ can never be absolutely irreducible since E' has CM. This proves Case II of Theorem 1.2.

Remark 5.2 For simplicity, we only considered the fields where there is only one prime ideal lying above 3, so we excluded the fields $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-11})$. Note that the triple $(\omega, \omega^2, 1)$, where ω is a primitive third root of unity, is a solution to equation (1.1). Hence, we had to exclude the case $\mathbb{Q}(\sqrt{-3})$.

One can try to apply the argument above to deal with the Fermat equation with signature $(p, p, 3)$ defined over the imaginary quadratic field $\mathbb{Q}(\sqrt{-163})$. However, we were unable to compute all the Bianchi modular forms over $\mathbb{Q}(\sqrt{-163})$ at level λ^3.

A Appendix. Ternary equation of signature $(p, p, 2)$

In [14], we have proved that the equation $x^p + y^p = z^2$ has no solutions asymptotically where $2|b$ over certain number fields. Using the method in the proof of Theorem 1.1, we can extend the results to any number field K with $h_K^+ = 1$. The difference relies in the proof method. Generally speaking, in order to solve a Diophantine equation using the modular method, one needs to either compute newforms of a certain level or compute all elliptic curves of a given conductor and particular information about torsion subgroup and/or rational isogeny or compute all solutions to an S-unit equation.

In [14], we used the S-unit equation method and this restricted us to the totally real number fields. However, using Theorem 4.1 as we did for proving Theorem 1.1, we can get the following result about the solutions of $x^p + y^p = z^2$.

Theorem A.1 *Let K be a number field with narrow class number $h_K^+ = 1$ satisfying Conjectures 2.2 and 2.3. Assume that β is the only prime of K lying above 2. Let W_K be the set of $(a, b, c) \in \mathcal{O}_K$ such that $a^p + b^p = c^2$ with $\beta|b$. Then there is a constant B_K—depending only on K—such that, for $p > B_K$, the equation $x^p + y^P = z^2$ has no solution $(a, b, c) \in W_K$.*

A hypothetical solution $(a, b, c) \in W_K$ with exponent $p > B_K$ gives rise to an elliptic curve E'/K with a K-rational 2-isogeny, good reduction away from $\mathfrak{P}$ and potentially multiplicative reduction at $\mathfrak{P}$. However, this contradicts with Theorem 4.1, and hence there is no such a solution.

Now, we give some examples of totally real number fields with $h_K^+ = 1$, in which 2 is totally ramified.

Degree 2^n case. Let $f_1(x) = x^2 - 2$, and $f_n(x) = (f_{n-1}(x))^2 - 2$ for $n \geq 2$. Let $K_n = \mathbb{Q}(\theta_n)$, where θ_n is a root of the polynomial $f_n(x)$. Then it can be seen that $K_n = \mathbb{Q}(\sqrt{2 + \cdots + \sqrt{2}}) = \mathbb{Q}(\zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1})$, the maximal totally real subfield of $\mathbb{Q}(\zeta_{2^{n+2}})$.

https://doi.org/10.4153/S0008414X22000311 Published online by Cambridge University Press

Then, K_n is a totally real number field of degree 2^n in which 2 is totally ramified. For $2 \le n \le 5$, it is possible to check that the narrow class number of K_n is 1, and hence it follows from Corollary 6.5 of [14] that the asymptotic FLT holds for all K_n with $2 \le n \le 5$. For some other higher values of n, it is only conjecturally true that the narrow class number is 1 (using MAGMA under GRH).

Degree 3, 4, 5 **case.** For $n \ge 3$, let $\mathcal{F}_n$ be the set of totally real number fields of degree n, discriminant $\le 10^6$, in which 2 totally ramifies. We are able to find the complete sets $\mathcal{F}_3, \mathcal{F}_4$, and $\mathcal{F}_5$ in the John Jones Number Field Database [15]. We define the following sets:

- Let $\mathcal{G}_n$ be the set of $K \in \mathcal{F}_n$ such that h_K^+ is odd.
- Let $\mathcal{K}_n$ be the set of $K \in \mathcal{G}_n$ such that $h_K^+ = 1$.

Of course, $\mathcal{K}_n \subseteq \mathcal{G}_n \subseteq \mathcal{F}_n$, and the asymptotic FLT holds for any K belonging to $\mathcal{K}_n$ by Corollary 6.5 of [14]. The cardinalities of $\mathcal{K}_n, \mathcal{G}_n$, and $\mathcal{F}_n$ are given in the following table, and can be found online at https://sites.google.com/view/erman-isik/research?authuser=0.

n	$\lvert\mathcal{F}_n\rvert$	$\lvert\mathcal{G}_n\rvert$	$\lvert\mathcal{K}_n\rvert$
3	8,600	3,488	3,046
4	1,243	1	1
5	23	13	13

Acknowledgment We are grateful to Samir Siksek for very helpful comments and discussions. We also would like to thank the referees for their comments and corrections which improved the paper a lot.

References

[1] A. Ash and G. Stevens, *Cohomology of arithmetic groups and congruences between systems of Hecke eigenvalues*. J. Reine Angew. Math. **365**(1986), 192–220.
[2] M. A. Bennett, V. Vatsal, and S. Yazdani, *Ternary Diophantine equations of signature* $(p, p, 3)$. Compos. Math. **140**(2004), no. 6, 1399–1416.
[3] R. Brauer and C. Nesbitt, *On the modular representations of groups of finite order I*. In: Richard Brauer: collected papers. Vol. **I**, MIT Press, Cambridge, MA, 1980, pp. 336–354.
[4] J. Coates and S. T. Yau (eds.), *Elliptic curves, modular forms & Fermat's last theorem*, International Press, Cambridge, MA, 1997.
[5] H. Darmon and A. Granville, *On the equations* $z^m = F(x, y)$ *and* $Ax^p + By^q = Cz^r$. Bull. Lond. Math. Soc. **27**(1995), no. 6, 513–543.
[6] A. David, *Caractère d'isogénie et critères d'irréductibilité*. Preprint, 2012. arXiv:1103.3892
[7] H. Deconinck, *On the generalized Fermat equation over totally real fields*. Acta Arith. **173**(2016), no. 3, 225–237.
[8] M. Derickx and S. Kamienny, *William stein, and Michael Stoll*. Torsion points on elliptic curves over number fields of small degree, 2021.
[9] R. Eggermont, *Generalizations of a theorem of Brauer and Nesbitt*. Master's thesis, Mathematisch Instituut, Universiteit Leiden, 2011.
[10] A. Etropolski, *Local-global principles for certain images of Galois representations*. Preprint, 2015. arXiv:1502.01288
[11] N. Freitas, A. Kraus, and S. Siksek, *Class field theory, Diophantine analysis and the asymptotic Fermat's last theorem*. Adv. Math. **363**(2020), Article no. 106964, 37 pp.

https://doi.org/10.4153/S0008414X22000311 Published online by Cambridge University Press

[12] N. Freitas and S. Siksek, *The asymptotic Fermat's last theorem for five-sixths of real quadratic fields*. Compos. Math. **151**(2015), no. 8, 1395–1415.
[13] N. Freitas and S. Siksek, *Fermat's last theorem over some small real quadratic fields*. Algebra Number Theory **9**(2015), no. 4, 875–895.
[14] E. Işik, Y. Kara, and E. Ozman, *On ternary Diophantine equations of signature* $(p, p, 2)$ *over number fields*. Turkish J. Math. **44**(2020), no. 4, 1197–1211.
[15] J. W. Jones and D. P. Roberts, *A database of number fields*. London J. Math. Comput. **17**(2014), 595–618.
[16] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*. Invent. Math. **109**(1992), no. 2, 221–229.
[17] Y. Kara and E. Ozman, *Asymptotic generalized Fermat's last theorem over number fields*. Int. J. Number Theory **16**(2020), no. 5, 907–924.
[18] N. M. Katz, *Galois properties of torsion points on abelian varieties*. Invent. Math. **62**(1981), no. 3, 481–502.
[19] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*. Nagoya Math. J. **109**(1988), 125–149.
[20] A. Kraus, *Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive*. Manuscripta Math. **69**(1990), no. 4, 353–385.
[21] A. Kraus, *Courbes elliptiques semi-stables et corps quadratiques*. J. Number Theory **60**(1996), no. 2, 245–253.
[22] E. Larson and D. Vaintrob, *Determinants of subquotients of Galois representations associated with abelian varieties*. J. Inst. Math. Jussieu **13**(2014), no. 3, 517–559. With an appendix by Brian Conrad.
[23] D. Mocanu. *Asymptotic Fermat for signatures* $(p, p, 2)$ *and* $(p, p, 3)$ *over totally real fields*. https://warwick.ac.uk/fac/sci/maths/people/staff/mocanu/summer_project.pdf
[24] F. Najman and G. C. Ţurcaş, *Irreducibility of mod p Galois representations of elliptic curves with multiplicative reduction over number fields*. Int. J. Number Theory **17**(2021), no. 8, 1729–1738.
[25] I. Papadopoulos, *Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle* 2 *et* 3. J. Number Theory **44**(1993), no. 2, 119–152.
[26] M. H. Şengün, *On the integral cohomology of Bianchi groups*. Exp. Math. **20**(2011), no. 4, 487–505.
[27] M. H. Şengün and S. Siksek, *On the asymptotic Fermat's last theorem over number fields*. Comment. Math. Helv. **93**(2018), no. 2, 359–375.
[28] J.-P. Serre, *Divisibilité de certaines fonctions arithmétiques*. Enseign. Math. (2) **22**(1976), nos. 3–4, 227–260.
[29] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, 151, Springer, New York, 1994.
[30] H. P. F. Swinnerton-Dyer, *On l-adic representations and congruences for coefficients of modular forms*. In: Modular functions of one variable, III (Proceedings International Summer School, University of Antwerp, 1972), Lecture Notes in Mathematics, 350, Springer, Berlin, 1973, pp. 1–55.
[31] G. C. Ţurcaş, *On Fermat's equation over some quadratic imaginary number fields*. Res. Number Theory **4**(2018), no. 2, Article no. 24, 16 pp.
[32] G. C. Ţurcaş, *On Serre's modularity conjecture and Fermat's equation over quadratic imaginary fields of class number one*. J. Number Theory **209**(2020), 516–530.

Mathematics Department, University College Dublin, Dublin, Ireland

e-mail: erman.isik@ucdconnect.ie

Mathematics Department, Bogazici University, Istanbul, Turkey

e-mail: yasemin.kara@boun.edu.tr

Mathematics Department, Bogazici University, Istanbul, Turkey & *University of Texas at Austin, Austin, TX, USA*

e-mail: ekin.ozman@boun.edu.tr