

Manuscript version: Author's Accepted Manuscript

The version presented in WRAP is the author's accepted manuscript and may differ from the published version or Version of Record.

Persistent WRAP URL:

<http://wrap.warwick.ac.uk/125395>

How to cite:

Please refer to published version for the most recent bibliographic citation information. If a published version is known of, the repository item page linked to above, will contain details on accessing it.

Copyright and reuse:

The Warwick Research Archive Portal (WRAP) makes this work by researchers of the University of Warwick available open access under the following conditions.

© 2019 Elsevier. Licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International <http://creativecommons.org/licenses/by-nc-nd/4.0/>.



Publisher's statement:

Please refer to the repository item page, publisher's statement section, for further information.

For more information, please contact the WRAP Team at: wrap@warwick.ac.uk.

**ON SERRE'S MODULARITY CONJECTURE AND FERMAT'S
EQUATION OVER QUADRATIC IMAGINARY FIELDS OF
CLASS NUMBER ONE**

GEORGE C. ȚURCAȘ

ABSTRACT. In the present article, we extend previous results of the author and we show that when K is any quadratic imaginary field of class number one, Fermat's equation $a^p + b^p + c^p = 0$ does not have integral coprime solutions $a, b, c \in K \setminus \{0\}$ such that $2 \mid abc$ and $p \geq 19$ is prime. The results are conjectural upon the veracity of a natural generalisation of Serre's modularity conjecture.

1. INTRODUCTION

Let K be a number field and denote by \mathcal{O}_K its ring of integers. The Fermat equation with prime exponent p over K is the equation

$$(1) \quad a^p + b^p + c^p = 0, \quad a, b, c \in \mathcal{O}_K.$$

Wiles's extraordinary proof of Fermat's Last Theorem inspired mathematicians to attack (1) via Frey elliptic curves and modularity over K . Successful attempts had been carried out by Jarvis and Meekin [14], and Freitas and Siksek [9], [10]. They all rely on progress in modularity lifting over totally real fields due to work of Barnett-Lamb, Breuil, Diamond, Gee, Geraghty, Kisin, Skinner, Taylor, Wiles and others. Modularity of elliptic curves over real quadratic fields was proved by Freitas, Le Hung and Siksek [8]. Recently, Derickx, Najman and Siksek [6] proved that elliptic curves over totally real cubic fields are modular.

On the other hand, modularity of elliptic curves over number fields with complex embeddings is highly conjectural. For general number fields, Şengün and Siksek [21] proved an asymptotic version of Fermat's Last Theorem, under the assumption of two standard, but very deep conjectures in the Langlands programme. They proved that for a number field K satisfying a precise S -unit equation criterion, there exists an ineffective constant B_K , depending only on the field K , such that for all primes $p > B_K$, the equation

$$a^p + b^p + c^p = 0,$$

does not have solutions in $K \setminus \{0\}$.

Let us denote by $G_K = \text{Gal}(\overline{K}/K)$ the absolute Galois group of K . Our results assume a version of Serre's modularity conjecture (see Conjecture 2.2) for odd, absolutely irreducible, continuous 2-dimensional mod p representations of G_K that are finite flat at every prime above p .

In [26], the author proved the following theorem

2010 *Mathematics Subject Classification.* Primary 11D41, Secondary 11F03, 11F80, 11F75.
Key words and phrases. Fermat, Bianchi, Galois representation, Serre modularity.

Theorem 1.1. *Let $K = \mathbb{Q}(\sqrt{-d})$, where $d \in \{1, 2, 7\}$. Assume Conjecture 2.2 holds for K . If $p \geq 5$ is a rational prime number, then the equation*

$$(2) \quad a^p + b^p + c^p = 0$$

has no solutions $a, b, c \in K \setminus \{0\}$.

Using known results about solutions to the equations $a^3 + b^3 = c^3$ and $a^4 + b^4 = c^4$ over $\mathbb{Q}(i)$, one obtains the easy corollary (see [26, Corollary 1.2])

Corollary 1.2. *Assume Conjecture 2.2 holds for $\mathbb{Q}(i)$. Then, Fermat's Last Theorem holds over $\mathbb{Q}(i)$. In other words, for any integer $n \geq 3$, the equation*

$$a^n + b^n = c^n$$

has no solution $a, b, c \in \mathbb{Q}(i) \setminus \{0\}$.

In the present work, we consider Fermat's equation over the remaining six quadratic imaginary fields of class number one. Our main result is as follows.

Theorem 1.3. *Let $K = \mathbb{Q}(\sqrt{-d})$, where $d \in \{3, 11, 19, 43, 67, 163\}$. Assume Conjecture 2.2 holds for K . For any prime $p \geq 19$, the Fermat equation*

$$a^p + b^p + c^p = 0,$$

does not have solutions in coprime $a, b, c \in \mathcal{O}_K \setminus \{0\}$ such that $2 \mid abc$.

Remark 1.4. *When $d \neq 163$, the statement of the previous theorem is true for $p \geq 17$. We only have to take $p \geq 19$ for $K = \mathbb{Q}(\sqrt{-163})$ due to the presence of 17-torsion in the integral cohomology of the relevant locally symmetric space.*

For an overview of the difficulties that had to be overcome to prove Theorems 1.1 and 1.3, we refer to [26, Section 1]. To prove Theorem 1.1, we made essential use of the fact that there is a prime ideal of \mathcal{O}_K of residue field \mathbb{F}_2 . This turns out to be an essential ingredient for proving that certain mod p Galois representations are absolutely irreducible, a hypothesis of Conjecture 2.2. Indeed, the rational prime 2 ramifies in $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-2})$ and splits completely in $\mathbb{Q}(\sqrt{-7})$. The remaining quadratic imaginary fields of class number one are $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$ and $\mathbb{Q}(\sqrt{-163})$. The prime 2 is inert in all six of them. In order to prove that certain mod p Galois representations are absolutely irreducible, we need to add the assumption that $2 \mid abc$.

It would have been extremely satisfying to obtain a statement of Theorem 1.3 analogous to Theorem 1.1, showing that for p larger than a fixed constant depending only on K , the equation (2) has no solutions $a, b, c \in K \setminus \{0\}$ for all the six fields K . Such a statement is not even true when $K = \mathbb{Q}(\sqrt{-3})$. One can see this by considering the triple $(a, b, c) = (1, \omega, \omega^2)$, where $\omega \in \mathbb{Q}(\sqrt{-3})$ is a primitive third root of unity, a solution to (2) for every prime exponent $p \geq 5$. However, in Section 5 we show that another folklore conjecture due to Serre, which concerns the surjectivity of mod p Galois representations, together with Conjecture 2.2 imply that when K is imaginary quadratic of class number one, there is a constant B_K , depending only on K , such that for every prime $p > B_K$ if $(a, b, c) \in K \setminus \{0\}$ is a solution to (1.1), then $K = \mathbb{Q}(\sqrt{-3})$ and $(a, b, c) = (1, \omega, \omega^2)$, up to permutation.

Acknowledgements. We are indebted to the referee for his careful reading of this paper and for suggesting numerous improvements. The author is grateful to his advisor Samir Siksek for suggesting the problem and for his great support. It is also a pleasure to thank John Cremona, Toby Gee, Aurel Page and Haluk Şengün for useful discussions. The author is supported by EPSRC Programme Grant EP/K034383/1 LMF: L-Functions and Modular Forms.

2. SERRE'S MODULARITY CONJECTURE

Throughout this section K is a quadratic imaginary field of class number one and $p \geq 5$ a rational prime that does not ramify in K . For notations, relevant definitions and a detailed discussion concerning complex and mod p eigenforms for GL_2 over K , we refer the reader to [26, Section 2].

Let $\mathcal{N} \subseteq \mathcal{O}_K$ be an ideal and consider the locally symmetric space

$$Y_0(\mathcal{N}) = \Gamma_0(\mathcal{N}) \backslash \mathcal{H}_3,$$

where $\Gamma_0(\mathcal{N}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_K) \mid c \in \mathcal{N} \right\}$ is the usual congruence subgroup for the modular group $\mathrm{GL}_2(\mathcal{O}_K)$ and \mathcal{H}_3 is the hyperbolic 3-space. It is explained in detail in loc. cit. that, in our setting, we can use the following definition.

Definition 2.1. *By a complex (or mod p) eigenform of level \mathcal{N} we understand a cohomology class $c \in H^1(Y_0(\mathcal{N}), \mathbb{C})$ (or $H^1(Y_0(\mathcal{N}), \overline{\mathbb{F}}_p)$) that is a simultaneous eigenvector for all the Hecke operators T_π , where $(\pi) \subset \mathcal{O}_K$ is a prime ideal coprime to \mathcal{N} (or $p\mathcal{N}$ respectively).*

The eigenforms in these algebras are sometimes called Bianchi modular forms (or mod p Bianchi modular forms) in the literature. Via the Eichler-Shimura-Harder isomorphism [13, Section 3.1], Bianchi modular forms can be analytically interpreted as vector valued real-analytic functions on the hyperbolic 3-space (see [5] for more details). Unlike the classical situation in which $K = \mathbb{Q}$, when K is quadratic imaginary not all the mod p eigenforms lift to complex ones. The obstruction for such lifting is the possible presence of p -torsion in the second integral cohomology $H^2(Y_0(\mathcal{N}), \mathbb{Z}_{(p)})$, where $\mathbb{Z}_{(p)}$ is the set of rational numbers with denominators prime to p . In the proof of Theorem 1.3, we prove that for the prime numbers p under consideration, the aforementioned cohomology group does not have p -torsion. Appealing to a result of Ash and Stevens [1], we show that mod p eigenforms lift to complex ones.

We will be using a special case of Serre's modularity conjecture over number fields. In his landmark paper [22], Serre conjectured that all absolutely irreducible, odd mod p Galois representation of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arise from a cuspidal eigenform f . Here f is a classical cuspidal modular form. In the same article, Serre gave a recipe for the level N and the weight k of the sought after eigenform. This conjecture was proved by Khare and Wintenberger [16].

We are going to state a conjecture which concerns mod p representations of G_K , the absolute Galois group of the quadratic imaginary K .

Conjecture 2.2 (compare to [21, Conjecture 3.1]). *Let $p > 3$ be a prime and E an elliptic curve defined over K . Suppose that the mod p Galois representation*

$\bar{\rho}_E : G_K \rightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_p)$, induced by the action of G_K on the p -torsion of E , is absolutely irreducible, continuous with Serre conductor \mathcal{N} (prime-to- p part of its Artin conductor). Assume that $\bar{\rho}_E|_{G_{K_{\mathfrak{p}}}}$ arises from a finite-flat group scheme over $\mathcal{O}_{K_{\mathfrak{p}}}$ for every prime $\mathfrak{p}|p$. Then there is a mod p eigenform $c \in H^1(Y_0(\mathcal{N}), \overline{\mathbb{F}}_p)$ such that for all prime ideals $(\pi) \subseteq \mathcal{O}_K$, coprime to $p\mathcal{N}$

$$T_{\pi}(c) = \mathrm{Trace}(\bar{\rho}_E(\mathrm{Frob}_{(\pi)})) \cdot c.$$

Although it is conjecturally easy to predict the level \mathcal{N} of such an eigenform, doing the same thing for the weight can be very difficult. A quite involved general weight recipe for GL_2 over number fields was given by Gee, Herzig and Savitt in [11]. We just mention that this recipe depends on the restriction $\bar{\rho}|_{I_{\mathfrak{p}}}$ to the inertia subgroups for the primes $\mathfrak{p} \subset \mathcal{O}_K$ above p . We only considered very special representations $\bar{\rho}$ (that are finite flat at $\mathfrak{p}|p$), for which Serre's original weight recipe applies and predicts the trivial weight [22]. This is why we end up with classes in $H^1(Y_0(\mathfrak{N}), \overline{\mathbb{F}}_p)$, the trivial weight meaning that we get $\overline{\mathbb{F}}_p$ as coefficient module.

As opposed to [21, Conjecture 3.1], in Conjecture 2.2 we allow for the prime p to ramify in K . The restriction in loc. cit. originates in the weight recipe given by Buzzard, Diamond and Jarvis [4], where the authors had to assume that the prime p is unramified in K . This restriction was since then removed in a series of papers of Gee et al. [11, 12]. Due to technicalities arising in the weight recipe when p is ramified in K , we had to assume that our Galois representation is the reduction of one coming from an elliptic curve. Indeed, by [12, Section 4.1.2] the hypothesis on $\bar{\rho}_E$ imply that all $a_i = b_i = 0$ in loc. cit. and this predicts a trivial weight if and only if the representation has a crystalline lift with all pairs of labelled Hodge-Tate weights equal to $\{0, 1\}$. In the hypothesis of the conjecture formulated above, $\bar{\rho}_E$ is the mod p reduction of a p -adic representation coming from an elliptic curve, therefore such a lift already exists. The recipes for the weights in [4] and [12] were given for totally real fields but as the problem of weights is a local issue, these (conjecturally) apply to any number field.

Remark. When stated for more general number fields, this conjecture restricts to odd representations. A representation is odd if the determinant of every complex conjugation is -1 , but since our K is totally complex G_K does not contain any complex conjugations and we will regard every mod p representation of G_K automatically as odd.

3. FERMAT EQUATION WITH EXPONENT p AND THE FREY CURVE

Let us fix some notation:

p - a rational prime number;

$K = \mathbb{Q}(\sqrt{-d})$ where d is one of 3, 11, 19, 43, 67 or 163;

\mathcal{O}_K - the ring of integers of K ;

$\mathfrak{q} = (2\mathcal{O}_K)$ - the prime ideal of residue field \mathbb{F}_4 that lies above 2.

By the Fermat equation with exponent p over K , we mean

$$(3) \quad a^p + b^p + c^p = 0, \quad a, b, c \in \mathcal{O}_K.$$

We say that a solution $(a, b, c) \in \mathcal{O}_K^3$ to the equation above is trivial if $abc = 0$ and non-trivial otherwise. We shall henceforth assume that $p \geq 19$ when $d = 163$ and $p \geq 17$ otherwise.

Let $(a, b, c) \in \mathcal{O}_K^3$ be a non-trivial solution to (3) such that a, b, c are coprime. One can always assume that a, b, c are coprime, since the class number of K is one. Associated to (a, b, c) is the Frey curve

$$(4) \quad E = E_{a,b,c} : Y^2 = X(X - a^p)(X + b^p).$$

Write $\bar{\rho} = \bar{\rho}_{E,p}$ for the residual Galois representation

$$\bar{\rho}_{E,p} : G_K \rightarrow \text{Aut}(E[p]) \cong \text{GL}_2(\mathbb{F}_p)$$

induced by the action of G_K on the p -torsion of $E[p]$. The following are easy to deduce properties of E and $\bar{\rho}$ which are proved in multiple papers concerning Fermat's equation over number fields. For a precise reference, see [26, Lemma 3.1]:

- the elliptic curve E is semistable away from $\mathfrak{q} = (2\mathcal{O}_K)$;
- the Galois representation $\bar{\rho}$ is unramified at the primes not dividing $2p$, finite flat at every prime \mathfrak{p} of \mathcal{O}_K that lies above p and $\det(\bar{\rho}) = \chi_p$, the mod p cyclotomic character.

From now on, we add the assumption that $2 \mid abc$. It follows from [10, Lemma 4.2] that E has potentially multiplicative reduction at \mathfrak{q} . We denote by N_E the conductor of E and we will apply [10, Lemma 4.4] to determine $v_{\mathfrak{q}}(N_E)$, the valuation of N_E at \mathfrak{q} . Let us demystify the quantities introduced in the aforementioned lemma. The ideal \mathfrak{b} is equal to \mathfrak{q}^3 and has norm 64. The group of units of the quotient $\mathcal{O}_K/\mathfrak{b}$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2 \oplus \mathbb{Z}/12\mathbb{Z}$ and therefore the co-domain of $\Phi : \mathcal{O}_K^* \rightarrow (\mathcal{O}_K/\mathfrak{b})^*/(\mathcal{O}_K/\mathfrak{b})^{*2}$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$. For every considered K , the image of Φ is isomorphic with $\mathbb{Z}/2\mathbb{Z}$, so $\text{Coker}(\Phi) \cong (\mathbb{Z}/2\mathbb{Z})^2$.

We present, for each of the considered six fields $K = \mathbb{Q}(\sqrt{-d})$, a complete list of representatives of this cokernel and the maximal value for the exponent of \mathfrak{q} in N_E . As it can be seen in the table below, if $K = \mathbb{Q}(\sqrt{-d})$ is one of the aforementioned fields and $2 \mid abc$, by [10, Lemma 4.4] we can scale the triple (a, b, c) by a unit so that the valuation of the conductor N_E of the Frey curve at $\mathfrak{q} = 2\mathcal{O}_K$ is at most 4.

TABLE 1. Computations associated to Lemma 4.4 in [10]

d	Reps. $\lambda_1, \lambda_2, \lambda_3, \lambda_4 \in \mathcal{O}_K$ of $\text{Coker}(\Phi)$	$v_{\mathfrak{q}}(N_E)$
3	$1, \frac{-1+3\sqrt{-3}}{2}, 3+2\sqrt{-3}, \frac{3-\sqrt{-3}}{2}$	4
11	$1, \frac{-1+\sqrt{-11}}{2}, -1+2\sqrt{-11}, \frac{-5-3\sqrt{-11}}{2}$	4
19	$1, \frac{1+3\sqrt{-19}}{2}, 3+2\sqrt{-19}, \frac{9+3\sqrt{-19}}{2}$	4
43	$1, \frac{-7-\sqrt{-43}}{2}, -1+2\sqrt{-43}, \frac{-3+3\sqrt{-43}}{2}$	4
67	$1, \frac{1+3\sqrt{-67}}{2}, 1+2\sqrt{-67}, \frac{-9-3\sqrt{-67}}{2}$	4
163	$1, \frac{1+3\sqrt{-163}}{2}, 1+2\sqrt{-163}, \frac{-9-3\sqrt{-163}}{2}$	4

For applying Conjecture 2.2 to the Galois representation $\bar{\rho} = \bar{\rho}_{E,p}$, we have to prove that it is absolutely irreducible.

Theorem 3.1. *Let K be one of the six fields above and consider a prime $p \geq 17$. If $(a, b, c) \in \mathcal{O}_K^3$ with $2 \mid \text{Norm}(abc)$ is a non-trivial solution to (3) such that a, b and c are coprime, then $\bar{\rho}_{E,p}$ is absolutely irreducible.*

Proof. We claim that absolute irreducibility follows from irreducibility. Suppose that $\bar{\rho}_{E,p}$ is irreducible. Let \mathfrak{q} be a prime of K above 2 that divides the product abc . Recall that E has potentially multiplicative reduction at \mathfrak{q} .

Using the identity $j(E) = \frac{2^4(b^{2p}-a^pc^p)}{(abc)^{2p}}$, we see that $v_{\mathfrak{q}}(j(E)) = 4 - 2pv_{\mathfrak{q}}(abc)$ is negative and $p \nmid v_{\mathfrak{q}}(j(E))$. It follows from the theory of Tate curves [25, Proposition 6.1] that there is an element $\sigma \in I_{\mathfrak{q}} \subseteq G_K$ that acts on $E[p]$ via a matrix of the form $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. The image $\bar{\rho}_{E,p}(G_K)$ is therefore an irreducible subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ which contains an element of order p and the classification [23, Proposition 15] of maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ implies that $\mathrm{SL}_2(\mathbb{F}_p) \subseteq \bar{\rho}_{E,p}(G_K)$. As $\mathrm{SL}_2(\mathbb{F}_p)$ is an absolutely irreducible subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$, the claim is proved. If p does not ramify in K , we can say even more, namely that $\bar{\rho}_{E,p}$ is surjective. This is a consequence of the fact that $\det(\bar{\rho}_{E,p})$ is the mod p cyclotomic character, which is surjective when $K \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$.

It remains to prove that $\bar{\rho}_{E,p}$ is irreducible. If we suppose the contrary, we can write

$$(5) \quad \bar{\rho}_{E,p} \sim \begin{pmatrix} \theta & * \\ 0 & \theta' \end{pmatrix}$$

where θ and θ' are characters $G_K \rightarrow \mathbb{F}_p^*$ and $\theta\theta' = \chi_p$, the mod p cyclotomic character given by the action of G_K on the group μ_p of p -th roots of unity. Let us denote by $\mathcal{N}_{\theta}, \mathcal{N}_{\theta'}$ the conductors of θ, θ' respectively. These characters are unramified away from p and $2\mathcal{O}_K = \mathfrak{q}$, the only prime of additive reduction for E (see [17, Lemma 1]).

Moreover, we saw above that \mathfrak{q} is a prime of potentially multiplicative reduction for E . Write $D_{\mathfrak{q}} \subseteq G_K$ for the decomposition subgroup at \mathfrak{q} . The restriction $\bar{\rho}_{E,p}$ to $D_{\mathfrak{q}}$ is, up to semi-simplification, equal to $\phi \oplus \phi \cdot \chi_p$, where ϕ is at worst a quadratic character (see [25, Theorem V.5.3]). In particular, both θ^2 and θ'^2 are unramified at \mathfrak{q} .

(i) We will first assume that p is coprime to either \mathcal{N}_{θ} or $\mathcal{N}_{\theta'}$. Since the conductor of an elliptic curve is isogeny invariant, by eventually replacing E with the p -isogenous curve $E/\langle \theta \rangle$ we can assume that p is coprime to \mathcal{N}_{θ} . This implies that θ is unramified away from \mathfrak{q} . By the above, we infer that θ^2 is everywhere unramified. The crucial fact that K has class number 1 allows us to deduce that θ^2 is the trivial character. Now, observe that either E or its twist by the quadratic character θ has a point of order p defined over K . The former instance happens precisely when θ is trivial itself and the latter when θ is quadratic.

The possible prime torsion of elliptic curves over quadratic fields have been determined by Kamienny and his result [15, Theorem 3.1] implies that $p \leq 13$, a contradiction.

(ii) Suppose that p is not coprime with \mathcal{N}_{θ} nor with $\mathcal{N}_{\theta'}$.

We now show that under the assumption that $\bar{\rho}_{E,p}$ is reducible, the prime p does not ramify in K . Suppose it does and let \mathfrak{p} be the unique prime ideal of \mathcal{O}_K such that $p\mathcal{O}_K = \mathfrak{p}^2$. Recall that the Frey curve E has semistable reduction at \mathfrak{p} . We therefore see from [9, Proposition 6.1 (ii)] that if \mathfrak{p} is a prime of good ordinary, or multiplicative reduction then

$$\bar{\rho}_{E,p}|_{I_{\mathfrak{p}}} \sim \begin{pmatrix} \chi_{\mathfrak{p}} & * \\ 0 & 1 \end{pmatrix}.$$

This would imply that one of the diagonal characters is not ramified at \mathfrak{p} and we showed in (i) that this is not possible. That leaves us with the possibility for \mathfrak{p} to be a prime of good supersingular reduction. In this situation [9, Proposition 6.1.]

asserts that either

$$(6) \quad \bar{\rho}_{E,p}|_{I_{\mathfrak{p}}} \sim \begin{pmatrix} \psi_2^2 & 0 \\ 0 & \psi_2^{2p} \end{pmatrix} \text{ or } \bar{\rho}_{E,p}|_{I_{\mathfrak{p}}} \sim \begin{pmatrix} \psi_1 & 0 \\ 0 & \psi_1 \end{pmatrix},$$

where $\psi_1 : I_{\mathfrak{p}} \rightarrow \mathbb{F}_p^*$ and $\psi_2 : I_{\mathfrak{p}} \rightarrow \mathbb{F}_{p^2}^*$ are the level 1 and respectively 2 fundamental characters defined in [23]. The first possibility in (6) implies that $\theta|_{I_{\mathfrak{p}}} = \psi_2^2$ or $\theta|_{\mathfrak{p}} = \psi_2^{2p}$, which is impossible since ψ_2^2 and ψ_2^{2p} are not \mathbb{F}_p -valued. Hence the restrictions of both θ and θ' to $I_{\mathfrak{p}}$ coincide with ψ_1 .

Recall that θ and θ' are unramified outside $2\mathcal{O}_K = \mathfrak{q}$ and \mathfrak{p} , so their conductors $\mathcal{N}_{\theta}, \mathcal{N}_{\theta'}$ are supported on these two primes. Define $\varepsilon : G_K \rightarrow \mathbb{F}_p^*$ by

$$\varepsilon = \theta/\theta' = \theta^2/\chi_p.$$

Since the restrictions of θ, θ' to $I_{\mathfrak{p}}$ coincide, the character ε is unramified at \mathfrak{p} . The latter is also unramified away from \mathfrak{q} , because θ and θ' are so. Its conductor $\mathcal{N}_{\varepsilon}$ is then a power of \mathfrak{q} . When restricted to the inertia subgroup of \mathfrak{q} the cyclotomic character χ_p is trivial, hence $\varepsilon|_{I_{\mathfrak{q}}} = \theta^2|_{I_{\mathfrak{q}}}$. We remarked at the start of this proof that θ^2 is unramified at \mathfrak{q} , so ε is everywhere unramified. Again, from the fact that K has class number one we derive that ε is trivial.

Let $\sigma_{\mathfrak{q}}$ be a Frobenius element of \mathfrak{q} . Since \mathfrak{q} is a prime of potentially multiplicative reduction, it is known (see for instance [21, Lemma 6.3]) that the possible pairs of eigenvalues of $\bar{\rho}_{E,p}(\sigma_{\mathfrak{q}})$ are $(1, \text{Norm}(\mathfrak{q}))$ or $(-1, -\text{Norm}(\mathfrak{q}))$. We therefore get

$$1 = \varepsilon(\sigma_{\mathfrak{q}}) = \theta(\sigma_{\mathfrak{q}})/\theta'(\sigma_{\mathfrak{q}}) \equiv \text{Norm}(\mathfrak{q})^{\pm 1} \pmod{p},$$

so $p \mid \text{Norm}(\mathfrak{q}) - 1 = 3$, which contradicts the hypothesis on p .

We proved that p does not ramify in K . If p is inert, we can apply [17, Lemme 1] to deduce that at least one of θ or θ' does not ramify at $p\mathcal{O}_K$, which puts us again in case (i).

The only possibility remaining is that p splits in K . Let $\mathfrak{p}_1, \mathfrak{p}_2$ be the two ideals of \mathcal{O}_K such that $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$. These primes are both of semistable reduction for E so by Lemme 1 in loc. cit., swapping θ and θ' if necessary, we can suppose that $\mathfrak{p}_1 \mid \mathcal{N}_{\theta}$, $\mathfrak{p}_1 \nmid \mathcal{N}_{\theta'}$ and $\mathfrak{p}_2 \mid \mathcal{N}_{\theta'}$, $\mathfrak{p}_2 \nmid \mathcal{N}_{\theta}$. The primes $\mathfrak{p}_1, \mathfrak{p}_2$ are unramified so it follows from [23, Proposition 12] that E has good ordinary or multiplicative reduction at these primes and that $\theta|_{I_{\mathfrak{p}_1}} = \chi_p|_{I_{\mathfrak{p}_1}}$ and $\theta'|_{I_{\mathfrak{p}_2}} = \chi_p|_{I_{\mathfrak{p}_2}}$.

It follows that the character θ^2 is unramified everywhere except \mathfrak{p}_1 , because the only bad place \mathfrak{q} of E is of potential multiplicative reduction, as explained at the beginning of the proof. Using Lemma 4.3 in [26] with $\alpha = 2 \in K$, it follows that

$$\theta^2(\sigma_{\mathfrak{q}}) \equiv \text{Norm}_{K_{\mathfrak{p}_1}/\mathbb{Q}_p}(\iota_{\mathfrak{p}_1}(2))^2 \pmod{p},$$

where $\sigma_{\mathfrak{q}}$ is the Frobenius element at \mathfrak{q} .

Appealing to Lemma 6.3 in [21] again, we derive that $\theta^2(\sigma_{\mathfrak{q}}), \theta'^2(\sigma_{\mathfrak{q}})$ are congruent (up to reordering) to 1 and $\text{Norm}^2(\mathfrak{q})$ modulo p . After replacing E by the isogenous curve $E/\langle \theta \rangle$, we can assume that $\theta^2(\sigma_{\mathfrak{q}}) \equiv 1 \pmod{p}$. We have that

$$\text{Norm}_{K_{\mathfrak{p}_1}/\mathbb{Q}_p}(\iota_{\mathfrak{p}_1}(2))^2 - 1 = 3,$$

so $p \mid 3$, a contradiction. \square

Let K be a general number field and E an elliptic curve defined over K such that it is semistable at all primes $\mathfrak{p} \subset \mathcal{O}_K$ above p and has potentially multiplicative reduction at a prime $\mathfrak{q} \neq \mathfrak{p}$. There exists an explicit constant $B_{K,\mathfrak{q}}$ such that for

all $p > B_{K,\mathfrak{q}}$ the mod p Galois representation arising by the action of G_K on the p -torsion points of E is absolutely irreducible (see [21, Proposition 6.1 and Corollary 6.2]). In Theorem 3.1 we find the smallest possible values for $B_{\mathfrak{q},K}$ in the case when K is quadratic imaginary of class number one and \mathfrak{q} is a prime above 2.

4. THE PROOF OF THEOREM 1.3

We proceed by contradiction and, assuming there is such a solution, we first scale it such as in Table 1 and then construct the Frey curve

$$E = E_{a,b,c} : Y^2 = X(X - a^p)(X + b^p).$$

The next step in our approach is to show the mod p Galois representation $\bar{\rho}_{E,p}$ satisfies the hypothesis of Serre's conjecture. Absolute irreducibility was proved in Theorem 3.1 and all the other hypothesis follow easily from the discussion at the beginning of the previous section. The Serre conductor \mathcal{N} of $\bar{\rho}_{E,p}$ is supported only on the prime $\mathfrak{q} = (2\mathcal{O}_K)$ and from Table 1 we know that \mathcal{N} is a divisor of \mathfrak{q}^4 .

Conjecture 2.2 predicts the existence of a mod p Bianchi modular form $c \in H^1(Y_0(\mathcal{N}), \bar{\mathbb{F}}_p)$ such that for every prime ideal $(\pi) \subset \mathcal{O}_K$, coprime to $p\mathcal{N}$ we have

$$T_\pi(c) = \text{Trace}(\bar{\rho}_{E,p}(\text{Frob}_{(\pi)})) \cdot c.$$

The trace elements $\text{Trace}(\bar{\rho}_{E,p}(\text{Frob}_{(\pi)}))$ lie in \mathbb{F}_p , therefore $c \in H^1(Y_0(\mathcal{N}), \mathbb{F}_p)$.

We fix an embedding from $\bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$. Unlike the classical situation in which $K = \mathbb{Q}$, when K is a general number field not all mod p eigenforms lift to complex ones. To explain this, let us denote by $\mathbb{Z}_{(p)}$ the ring of rational numbers with denominators prime to p . Consider the following short exact sequence given by multiplication-by- p

$$0 \longrightarrow \mathbb{Z}_{(p)} \xrightarrow{\times p} \mathbb{Z}_{(p)} \longrightarrow \mathbb{F}_p \longrightarrow 0.$$

This gives rise to a long exact sequence on cohomology

$$\begin{array}{c} \dots H^1(Y_0(\mathfrak{N}), \mathbb{Z}_{(p)}) \xrightarrow{\times p} H^1(Y_0(\mathfrak{N}), \mathbb{Z}_{(p)}) \longrightarrow H^1(Y_0(\mathfrak{N}), \mathbb{F}_p) \\ \left. \begin{array}{l} \xrightarrow{\hspace{15em} \delta \hspace{15em}} \\ \hookrightarrow H^2(Y_0(\mathfrak{N}), \mathbb{Z}_{(p)}) \longrightarrow \dots \end{array} \right\} \end{array}$$

from which we can extract the short exact sequence

$$0 \longrightarrow H^1(Y_0(\mathfrak{N}), \mathbb{Z}_{(p)}) \otimes \mathbb{F}_p \longrightarrow H^1(Y_0(\mathfrak{N}), \mathbb{F}_p) \xrightarrow{\delta} H^2(Y_0(\mathfrak{N}), \mathbb{Z}_{(p)})[p] \longrightarrow 0.$$

In the above, the presence of p -torsion in $H^2(Y_0(\mathfrak{N}), \mathbb{Z}_{(p)})$ is the obstruction to surjectivity for the map $H^1(Y_0(\mathfrak{N}), \mathbb{Z}_{(p)}) \otimes \mathbb{F}_p \rightarrow H^1(Y_0(\mathfrak{N}), \mathbb{F}_p)$. If there is only trivial such torsion, then any Hecke eigenvector \bar{c} in $H^1(Y_0(\mathfrak{N}), \mathbb{F}_p)$ comes from such an eigenvector in $H^1(Y_0(\mathfrak{N}), \mathbb{Z}_{(p)}) \otimes \mathbb{F}_p$. Using a lifting lemma of Ash and Stevens [1, Proposition 1.2.2], we deduce that there are

- (1) a finite integral extension R of $\mathbb{Z}_{(p)}$
- (2) a prime \mathfrak{p} of R above p and
- (3) a Hecke eigenvector c in $H^1(Y_0(\mathfrak{N}), R)$

such that the Hecke eigenvalues of c reduced modulo \mathfrak{p} are equal to the ones of \bar{c} . Using our fixed embedding $\bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$ we can regard c as a class in $H^1(Y_0(\mathcal{N}), \mathbb{C})$, which implies the existence of our sought after complex eigenform.

Remark. We observe that in the paragraph above, \bar{c} is not necessarily the reduction of c . The result that we cite only states that a system of eigenvalues occurring in \mathbb{F}_p may, after finite base extension, be lifted to a system occurring in $\mathbb{Z}_{(p)}$. The interested reader should consult [1, Section 1.2] for a more illuminating discussion.

One sees that $H^2(Y_0(\mathcal{N}), \mathbb{Z}_{(p)})$ and $H^2(Y_0(\mathcal{N}), \mathbb{Z})$ have the same p -torsion. As discussed in [1, page 202], if the least common multiple of the orders of elements of finite order in $\Gamma_0(\mathcal{N})$ is invertible in the coefficients module, then simplicial cohomology and group cohomology are the same. In our case, $\mathcal{N} = \mathfrak{q}^4$ and all the elements of finite order in $\Gamma_0(\mathcal{N})$ have orders dividing 6. Therefore, $H^2(Y_0(\mathcal{N}), \mathbb{Z}[\frac{1}{6}])$ and $H^2(\Gamma_0(\mathcal{N}), \mathbb{Z}[\frac{1}{6}])$ are isomorphic as Hecke modules.

Lefschetz duality for cohomology with compact support [20, Section 2] gives a relation between the first homology and the second cohomology $H_1(\Gamma_0(\mathcal{N}), \mathbb{Z}[\frac{1}{6}]) \cong H^2(\Gamma_0(\mathcal{N}), \mathbb{Z}[\frac{1}{6}])$. It is also known that the abelianization $\Gamma_0(\mathcal{N})^{ab} \cong H_1(\Gamma_0(\mathcal{N}), \mathbb{Z})$ and therefore, for primes $p > 3$, if the group $H^2(Y_0(\mathcal{N}), \mathbb{Z})$ has a p -torsion element, then $\Gamma_0(\mathcal{N})^{ab}$ will have a p -torsion as well. We compute the abelianizations $\Gamma_0(\mathcal{N})^{ab}$ using an algorithm of Haluk Şengün [20]. The **Magma** implementation of this algorithm was kindly provided to us by its author. The algorithm requires as input presentations for $\mathrm{PGL}_2(\mathcal{O}_K)$, which we compute using a program of Page [19]. The relevant **Magma** files can be found at

<https://warwick.ac.uk/fac/sci/math/people/staff/turcas/fermatprog>.

We record the primes l that appear as orders of torsion elements in $\Gamma_0(\mathcal{N})^{ab}$, for each of the six number fields in Table 2.

TABLE 2. prime torsion in $\Gamma_0(\mathcal{N})^{ab}$

Number field	Level \mathcal{N}	primes l such that $\Gamma_0(\mathcal{N})^{ab}[l] \neq 0$
$\mathbb{Q}(\sqrt{-3})$	$(2\mathcal{O}_K)^4$	2, 3
$\mathbb{Q}(\sqrt{-11})$	$(2\mathcal{O}_K)^4$	2, 3
$\mathbb{Q}(\sqrt{-19})$	$(2\mathcal{O}_K)^4$	2, 3
$\mathbb{Q}(\sqrt{-43})$	$(2\mathcal{O}_K)^4$	2, 3
$\mathbb{Q}(\sqrt{-67})$	$(2\mathcal{O}_K)^4$	2, 3
$\mathbb{Q}(\sqrt{-163})$	$(2\mathcal{O}_K)^4$	2, 3, 5, 11, 17

Since we have chosen $p \geq 19$ and there is no p -torsion in the subgroups of interest, the mod p eigenforms must lift to complex ones. We obtain a fixed, finite list of cuspidal Bianchi newforms of level dividing \mathfrak{q}^4 to which our mod p eigenform can lift. For each Bianchi newform \mathfrak{f} in this list, we denote by $\mathbb{Q}_{\mathfrak{f}}$ the number field generated by their eigenvalues. The process described above guarantees that for every $\mathfrak{l} \nmid \mathfrak{q}^4 \cdot p$, prime ideal of K we get the following congruence

$$\mathrm{Trace}(\bar{\rho}_{E,p}(\sigma_{\mathfrak{l}})) \equiv a_{\mathfrak{l}}(\mathfrak{f}) \pmod{\mathfrak{P}},$$

between the trace of the image of Frobenius at \mathfrak{l} in $\bar{\rho}_{E,p}$ and the Hecke eigenvalue of \mathfrak{f} at \mathfrak{l} . Here \mathfrak{P} is some ideal of $\mathbb{Q}_{\mathfrak{f}}$ that lies above the prime p . We now use the idea in [9, Lemma 7.1] to obtain an upper bound on the prime exponent p . Although the work in loc. cit. is carried for Hilbert modular forms, the proof of this lemma holds through for Bianchi modular forms \mathfrak{f} . We describe the idea below.

Let us fix a prime ideal \mathfrak{l} as above. The Frey curve $E = E_{a,b,c}$ has good or multiplicative reduction at \mathfrak{l} . If it has good reduction, then $\text{Trace}(\overline{\rho}_{E,p}(\sigma_{\mathfrak{l}})) \equiv a_{\mathfrak{l}}(E) \equiv a_{\mathfrak{l}}(\mathfrak{f}) \pmod{\mathfrak{P}}$. By definition, E has full two-torsion defined over K and $\mathfrak{l} \nmid 2$, so $4 \mid \#E(\mathbb{F}_{\mathfrak{l}}) = \text{Norm}(\mathfrak{l}) + 1 - a_{\mathfrak{l}}(E)$. Adding the information provided by the Hasse-Weil bounds we get that $a_{\mathfrak{l}}(E)$ belongs to the finite set

$$\mathcal{A}_{\mathfrak{l}} = \{a \in \mathbb{Z} : |a| \leq 2\sqrt{\text{Norm}(\mathfrak{l})}, \text{Norm}(\mathfrak{l}) + 1 - a \equiv 0 \pmod{4}\}.$$

If $\mathfrak{q} \nmid 2p$ is a prime of multiplicative reduction, then

$$\text{Trace}(\overline{\rho}_{E,p}(\sigma_{\mathfrak{l}})) = \pm(\text{Norm}(\mathfrak{l}) + 1) \Rightarrow \mathfrak{P} \mid (\text{Norm}(\mathfrak{l}) + 1)^2 - a_{\mathfrak{l}}(\mathfrak{f})^2.$$

If $\mathfrak{l} \mid p$, obviously $p \mid \text{Norm}(\mathfrak{l})$. For every prime ideal \mathfrak{l} of K that does not divide 2, denote

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

The above proves that $\mathfrak{P} \mid B_{\mathfrak{f},\mathfrak{l}}$ and, by taking norms, that $p \mid \text{Norm}(B_{\mathfrak{f},\mathfrak{l}})$.

Using **Magma**, we computed the cuspidal newforms \mathfrak{f} at levels dividing \mathfrak{q}^4 , the fields $\mathbb{Q}_{\mathfrak{f}}$ and eigenvalues $a_{\mathfrak{l}}(\mathfrak{f})$ at primes \mathfrak{l} of K that have norm less than 50. We computed the ideal $C_{S,\mathfrak{f}} \subseteq \mathcal{O}_K$, the greatest common divisor of $B_{\mathfrak{f},\mathfrak{l}}$ when $\mathfrak{l} \nmid 2$ runs through a set S of prime ideals of K that have norm less than 50. If $C_{S,\mathfrak{f}}$ is not zero, then $p \mid \text{Norm}(C_{\mathfrak{f}})$ gives an upper bound on p . For every number field K in the statement of Theorem 1.3 and every cuspidal eigenform \mathfrak{f} of level dividing \mathfrak{q}^4 , we computed a non-zero constant $C_{S,\mathfrak{f}}$ and we found that $\text{Norm}(C_{\mathfrak{f}})$ is only supported on $\{3, 5, 7\}$. As p is assumed to be greater or equal to 17, this is a contradiction and the proof of our theorem is now complete.

5. SERRE'S UNIFORMITY CONJECTURE AND ASYMPTOTIC FERMAT

For a number field K , the **Asymptotic Fermat's Last Theorem** over K is the statement that there exists a bound B_K such that for all primes $p > B_K$, the Fermat equation $a^p + b^p + c^p = 0$ does not have solutions in $a, b, c \in K \setminus \{0\}$.

Let $\omega \in \mathbb{Q}(\sqrt{-3})$ be a primitive cube root of unity. For every $p \geq 5$, we have $1^p + \omega^p + \omega^{2p} = 0$, hence the Asymptotic Fermat's Last Theorem does not hold over $\mathbb{Q}(\sqrt{-3})$. The authors of [7] point out that it is reasonable to make the following conjecture, a consequence of the *abc*-conjecture for number fields (see [3]).

Conjecture 5.1. *Let K be a number field such that $\omega \notin K$. Then the Asymptotic Fermat's Last Theorem holds over K .*

Theorem 1.3 proved in the previous section can be a little bit unsatisfying, since it only rules out the possible existence of coprime integral solutions (a, b, c) such that $2 \mid abc$. Let $K = \mathbb{Q}(\sqrt{-d})$, where $d = 3, 11, 19, 43, 67$ or 163 , as in the hypothesis of the aforementioned theorem. If $a, b, c \in \mathcal{O}_K$ is a non-trivial solution to the Fermat equation with prime exponent such that $2 \nmid abc$, then it is explained in Lemmas 4.1 and 4.2 of [10] that E has potentially good reduction at $\mathfrak{q} = 2\mathcal{O}_K$ and, after possibly permuting (a, b, c) , the Serre conductor of $\overline{\rho}_{E,p}$ is equal to \mathfrak{q}^4 .

Assuming Serre's modularity conjecture, we would like to have a full resolution of the Fermat equation $a^p + b^p + c^p = 0$, where $a, b, c \in K$ and $p \geq 17$ prime. Using our approach, this would follow if we could prove that the mod p representation attached to the usual Frey curve is absolutely irreducible. Unfortunately, this is not true. We saw that when $K = \mathbb{Q}(\sqrt{-3})$, the triple formed from the third roots

of unity is a solution to the Fermat equation for every prime $p \geq 5$. The Frey curve $E := E_{1,\omega,\omega^2}$ is, for every such p , a twist of the CM curve with LMFDB [18] label 256.1-CMb1. The representation $\bar{\rho}_{E,p}$ of this curve is never absolutely irreducible. To be precise, for $p \geq 5$, the image $\bar{\rho}_{E,p}(G_K)$ is contained in a split Cartan subgroup if $\left(\frac{-3}{p}\right) = 1$, respectively in a non-split Cartan subgroup if $\left(\frac{-3}{p}\right) = -1$. The former is reducible whereas the latter is irreducible but absolutely reducible.

To emphasize that a resolution of Fermat equation with prime exponent over the fields K considered above is a task worth pursuing, we will show that such a resolution is possible if we assume a folklore conjecture (see [2]) motivated by a question of Serre.

Conjecture 5.2 (Uniformity conjecture). *Fix a number field K . There exists a constant $C(K)$ such that for all non-CM elliptic curves E/K and all primes $p \geq C(K)$, the mod p Galois representation $\bar{\rho}_{E,p} : G_K \rightarrow \mathrm{GL}_2(\mathbb{F}_p)$ is surjective.*

Let K be one of the six quadratic imaginary fields listed above. Assume that Serre's modularity conjecture and the Uniformity conjecture (Conjectures 2.2 and 5.2) hold for K . As there are elliptic curves with 17-isogenies defined over K (there are such elliptic curves defined over \mathbb{Q}), we know that $C(K) > 17$.

Suppose $(a, b, c) \in K^3$ is a non-trivial solution to the Fermat equation with prime exponent $p \geq C(K)$,

$$(7) \quad a^p + b^p + c^p = 0.$$

As before, we can scale the solution of (7) such that $a, b, c \in \mathcal{O}_K \setminus \{0\}$ are coprime. From Theorem 1.3 we know that $2 \nmid abc$. Let

$$E := E_{a,b,c} : Y^2 = X(X - a^p)(X + b^p)$$

be the usual Frey curve and denote by $\bar{\rho}_{E,p} : G_K \rightarrow \mathrm{GL}_2(\mathbb{F}_p)$ the Galois representation on the p -torsion. The discussion in previous sections shows that $\bar{\rho}_{E,p}$ is unramified away from the primes above 2 and p , it is finite flat at every prime of K that lies above p and $\det(\bar{\rho}_{E,p})$ is the mod p cyclotomic character. Lemma 4.2 in [10] proves that E has potential good reduction at the prime ideal $2\mathcal{O}_K$. Applying the Tate algorithm one can prove that, after possibly permuting (a, b, c) , the valuation of the conductor of E at $2\mathcal{O}_K$ is equal to 4 (see [9, Lemma 4.1]).

Suppose that E does not have CM. Our assumption of the Uniformity conjecture implies that $\bar{\rho}_{E,p}$ is surjective, hence absolutely irreducible. Its Serre conductor divides $\mathcal{N} = 2^4\mathcal{O}_K$. Thus, $\bar{\rho}_{E,p}$ satisfies the hypothesis of Conjecture 2.2 and this predicts the existence of a mod p eigenform $c \in H^1(Y_0(\mathcal{N}), \overline{\mathbb{F}}_p)$ such that for every prime ideal $(\pi) \subset \mathcal{O}_K$, coprime to $p\mathcal{N}$ we have

$$T_\pi(c) = \mathrm{Trace}(\bar{\rho}_{E,p}(\mathrm{Frob}_{(\pi)})) \cdot c,$$

where T_π is a Hecke operator. In the previous section we have shown that this is not possible for $p \geq C(K) > 17$.

Suppose that E has CM. Serre and Tate [24] showed that elliptic curves with CM have everywhere potential good reduction, hence $j(E)$ is an algebraic integer. Recall that

$$j(E) = \frac{c_4(E)^3}{\Delta(E)} = 2^8 \cdot \frac{(b^{2p} - a^p c^p)^3}{(abc)^{2p}}.$$

Since a, b and c are integral and coprime, one can see from the usual formulas that $c_4(E)$ and $\Delta(E)$ are coprime outside the prime above 2. The latter does not divide

abc . This implies that abc is a unit, since any odd prime dividing abc would be a prime of potentially multiplicative reduction, contradicting the fact that E has CM. Hence a, b, c are units in \mathcal{O}_K . There are not that many possible units over the six quadratic imaginary fields that are discussed and, by trying all of the possibilities, we obtain that the only solutions are permutations of $(1, \omega, \omega^2) \in \mathbb{Q}(\sqrt{-3})^3$, where ω is a non-trivial third root of unity. In addition to solutions $(a, b, c) \in K^3$ with $abc = 0$ to the Fermat equation (3), let us call trivial those with the property that $a + b + c = 0$. It can be proved that the latter are just scalar multiples of permutations of $(1, \omega, \omega^2)$. The next result follows by combining the above with Theorems 1.1 and 1.3.

Theorem 5.3. *Let $K = \mathbb{Q}(\sqrt{-d})$ be a quadratic imaginary number field of class number 1 and suppose that Conjectures 2.2 and 5.2 hold over K . There is an absolute constant $C(K) > 0$ such that the only solutions to the Fermat equation $a^p + b^p + c^p = 0$ with $a, b, c \in K$ and $p > C(K)$ prime are trivial.*

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] A. Bourdon, O. Ejder, Y. Liu, F. Odumodu, and B. Viray, *On the level of modular curves that give rise to sporadic j -invariants*, arXiv e-prints (2018Aug), available at [1808.04520](#).
- [3] J. Browkin, *The abc -conjecture for algebraic numbers*, Acta Mathematica Sinica **22** (2006Jan), no. 1, 211–222.
- [4] K. Buzzard, F. Diamond, and F. Jarvis, *On Serre’s conjecture for mod l Galois representations over totally real fields* **155** (2010), no. 1, 105–161.
- [5] J. E. Cremona and E. Whitley, *Periods of cusp forms and elliptic curves over imaginary quadratic fields*, Math. Comp. **62** (1994), no. 205, 407–429.
- [6] M. Derickx, F. Najman, and S. Siksek, *Elliptic Curves over Totally Real Cubic Fields are Modular*, arXiv e-prints (2019Jan), available at [1901.03436](#).
- [7] N. Freitas, A. Kraus, and S. Siksek, *Class field theory, Diophantine analysis and the asymptotic Fermat’s Last Theorem*, arXiv e-prints (2019Feb), arXiv:1902.07798, available at [1902.07798](#).
- [8] N. Freitas, B. V. Le Hung, and S. Siksek, *Elliptic curves over real quadratic fields are modular*, Invent. Math. **201** (2015), no. 1, 159–206.
- [9] N. Freitas and S. Siksek, *Fermat’s Last Theorem over some small real quadratic fields*, Algebra & Number Theory **9** (2015), 875–895.
- [10] ———, *An asymptotic Fermat’s Last Theorem over five-sixths of real quadratic fields*, Compos. Math. **151** (2015), 1395–1415.
- [11] T. Gee, F. Herzig, and D. Savitt, *General Serre weight conjectures*, J. Eur. Math. Soc. (JEMS) **20** (2018), no. 12, 2859–2949.
- [12] T. Gee, T. Liu, and D. Savitt, *The weight part of Serre’s conjecture for $GL(2)$* , Forum Maths., Pi **1** (2015), no. e1, 50pp.
- [13] G. Harder, *Eisenstein cohomology of arithmetic groups. The case GL_2* , Invent. Math. **89** (1987), 37–118.
- [14] F. Jarvis and P. Meekin, *The Fermat equation over $\mathbb{Q}(\sqrt{2})$* , J. Number Theory **109** (2004), no. 1, 182–196.
- [15] S. Kamienny, *Torsion points on elliptic curves and q -coefficients of modular forms*, Invent. Math. **109** (1992Dec), no. 1, 221–229.
- [16] C. Khare and J. P. Wintenberger, *Serre’s modularity conjecture. II.*, Invent. Math. **178** (2009), no. 3, 505–586.
- [17] A. Kraus, *Courbes elliptiques semi-stables et corps quadratiques*, Manuscripta Math. **69** (1990), no. 4, 245–253.
- [18] The LMFDB Collaboration, *The L -functions and Modular Forms Database*, 2013. [Online; accessed 16 September 2013].
- [19] A. Page, *Computing arithmetic Kleinian groups*, Math. Comp. **84** (2015), 2361–2390.

- [20] M. H. Şengün, *On the Integral Cohomology of Bianchi Groups*, Experiment. Math. **20** (2011), 487–505.
- [21] M. H. Şengün and S. Siksek, *On the asymptotic Fermat's Last Theorem over number fields*, Commentarii Mathematici Helvetici **93** (2018), 359–372.
- [22] J. P. Serre, *Sur les représentations modulaires de degré 2 de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$* , Duke Math. J. **54** (1987), 179–230.
- [23] ———, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1971/72), 259–331.
- [24] J. P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. **88** (1968), no. 3, 492–517.
- [25] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Vol. 151, Springer, GMT, 1994.
- [26] G. C. Turcaş, *On Fermat's equation over some quadratic imaginary number fields*, Research in Number Theory **4** (2018), no. 2, 24 pages.

MATHEMATICS INSTITUTE, UNIVERSITY OF WARWICK, COVENTRY, UNITED KINGDOM
E-mail address: `george.turcas@warwick.ac.uk`