IRREDUCIBLE BINARY CUBICS AND THE GENERALIZED SUPERELLIPTIC EQUATION OVER NUMBER FIELDS

GEORGE C. ŢURCAŞ

Abstract. For a large class (heuristically most) of irreducible binary cubic forms $F(x,y) \in \mathbb{Z}[x,y]$, Bennett and Dahmen proved that the generalized superelliptic equation $F(x,y) = z^l$ has at most finitely many solutions in $x, y \in \mathbb{Z}$ coprime, $z \in \mathbb{Z}$ and exponent $l \in \mathbb{Z}_{\geq 4}$. Their proof uses, among other ingredients, modularity of certain mod l Galois representations and Ribet's level lowering theorem. The aim of this paper is to treat the same problem for binary cubics with coefficients in $\mathcal{O}_K$, the ring of integers of an arbitrary number field K, using by now well-documented modularity conjectures.

1. Introduction

In their extraordinary paper Bennett and Dahmen [2] proved that for a large class of binary forms $F \in \mathbb{Z}[X,Y]$ of degrees $3, 4, 6$ and 12, including “most" cubic forms (see [2, Section 12]), the generalized superelliptic equation $F(x,y) = z^l$ has finitely many solutions for $x, y, z \in \mathbb{Z}$, $\gcd(x,y) = 1$ and $l \geq \max\{2, 7 - \deg F\}$ integer. To be precise, by attaching a family of Frey-Hellegouarch curves to putative solutions of the aforementioned equation and making essential use of modularity and level-lowering theorems due to Breuil, Conrad, Diamond, Taylor and respectively Ribet, they prove that no such solutions exists for l big enough. Darmon and Granville [5] gave a descent argument and made use of Falting's Theorem to conclude that for fixed values of l, the equation $F(x,y) = z^l$ has finitely many solutions in coprime integers x, y. Together these imply the result stated above.

Modular methods are undoubtedly an extremely powerful tool for proving that certain Diophantine equations have no solutions and, in some cases, finding the set of all solutions to these equations over $\mathbb{Z}$ (or $\mathbb{Q}$). Some number theorists are therefore interested in extending these methods over more general number fields. Such attempts were successfully carried out for the

2010 *Mathematics Subject Classification.* Primary 11G05, 11F80; Secondary 11F03, 11F75.

Key words and phrases. Galois representation, Superelliptic equation, Serre modularity.

The author is supported by an EPSRC PhD studentship.

Fermat equation over certain totally real number fields by Jarvis [14] and by Freitas and Siksek [8], [9]. These rely essentially on modularity lifting theorems over totally real fields due to Barnett-Lamb, Breuil, Diamond, Gee, Geraghty, Kisin, Skinner, Taylor, Wiles and others.

On the other hand, modularity of elliptic curves over number fields with complex embeddings is highly conjectural. Nevertheless, assuming by now well-documented conjectures in the Langlands programme, Şengün and Siksek [22] proved an asymptotic version of Fermat's Last Theorem over infinitely many general number fields.

In the spirit of [22], the purpose of this work is extend some of the results of Bennett and Dahmen [2] to the general number field setting and to highlight the additional challenges that arise in this context.

Fix once and for all an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Throughout, l denotes a rational prime. Given a number field $K \subset \overline{\mathbb{Q}}$, we denote by $\mathcal{O}_K$ its ring of integers and by $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ its absolute Galois group. To keep this introduction self-contained we postpone for later sections the precise statements of the two conjectures we assume. Instead, we only indicate briefly what they are.

- Conjecture 2.1 is a version of Serre's modularity conjecture for odd, irreducible, continuous 2-dimensional mod l representations of G_K that are finite flat at every prime over l.
- Conjecture 2.2, sometimes referred to as *Eichler-Shimura*, is part of the Langlands Programme (see [26]) and relates weight 2 newforms (for GL_2) over K that have integer Hecke eigenvalues to elliptic or fake elliptic curves over K.

Before presenting our main results, we have to set up some notation. Given a number field K, it is known that every class in its ideal class group contains infinitely many prime ideals. If $c_1, \dots, c_h$ are the ideal classes of K, for every $i \in \{1, \dots, h\}$ we choose a prime ideal $\mathfrak{m}_i \subset \mathcal{O}_K$ of smallest possible norm, such that $\mathfrak{m}_i \nmid 2$ and $\mathfrak{m}_i$ belongs to the class c_i. We fix the set

$$\mathcal{H}_K := \begin{cases} \emptyset, \text{ if } h = 1 \\ \{\mathfrak{m}_1, \dots, \mathfrak{m}_h\}, \text{ if } h \geq 2 \end{cases}. \tag{1}$$

Given an irreducible binary cubic $F \in \mathcal{O}_K[X, Y]$ of discriminant Δ_F (one could work in greater generality and choose F to be a Klein form, see [2]), we denote by

$$S_F := \mathcal{H}_K \cup \{\text{prime ideals dividing } 2\Delta_F\} \cup \{\text{real infinite places of } K\}. \tag{2}$$

This set depends on the form F (and of course, on the number field K).

A large part of the present paper is dedicated to proving the following result.

Theorem 1.1. *Let K be a number field for which Conjecture 2.1 and Conjecture 2.2 hold. Consider $F(x,y) = \alpha_0 x^3 + \alpha_1 x^2 y + \alpha_2 x y^2 + \alpha_3 y^3 \in \mathcal{O}_K[x,y]$ an irreducible binary cubic form such that there exists a prime ideal $\mathfrak{q} \mid\mid \Delta_F$ and $\mathfrak{q} \nmid (2\alpha_0)$. If the Thue-Mahler equation*

$$F(x,y) \in \mathcal{O}^*_{K,S_F} \tag{3}$$

has no solutions in $x, y \in \mathcal{O}_K$, then there exists a constant $A_F > 0$ such that for all rational primes $l > A_F$ the superelliptic equation

$$F(x,y) = z^l \tag{4}$$

does not have solutions in $x, y, z \in \mathcal{O}_K$ such that $\gcd(x,y,z)$ is supported on the primes in S_F and $\mathfrak{q} \nmid z$.

Proposition 2.1 of Darmon-Granville [5] implies that for any fixed value of $l \geq 4$, equation (4) has finitely many *proper solutions* $x, y, z \in \mathcal{O}_K$. The authors of *loc. cit.* introduce the notion of *proper solutions* to exclude the possibility of generating an infinite number in the following way. Suppose $x, y, z \in \mathcal{O}_K$ are a solution to (4) and $\xi \in \mathcal{O}_K^\times$ be a generator of the unit group. Then $\xi^{n \cdot l} x, \xi^{n \cdot l} y, \xi^{3 \cdot n} z$ for all $n \in \mathbb{N}$ will be an infinite family of integral solutions to our generalized superelliptic equation. A proper solution is, in fact, an equivalence class of solutions to (4) such that $\gcd(x,y)$ divides some a priori fixed ideal. Two such solutions are equivalent if we can obtain one from the other via a trivial action of the unit group $\mathcal{O}_K^\times$.

Corollary 1.1. *Let K and F satisfy all the hypothesis of Theorem 1.1. The superelliptic equation $F(x,y) = z^l$ has finitely many proper solutions in integers $l \geq 4$ and $x, y, z \in \mathcal{O}_K$ such that $\mathfrak{q} \nmid z$ and the ideal $\gcd(x,y,z)$ is supported on the primes in S_F.*

We remark that specializing to number fields of small degree and trivial class group, one could carry the proof of Theorem 1.1 and effectively compute the constant A_F. In particularly fortuitous situations, one could even find oneself in positions where Conjecture 2.2 is known to hold and therefore producing special cases of Theorem 1.1 that only depend on Conjecture 2.1. This is emphasized in [27], where the author worked on Fermat's equation over quadratic imaginary number fields. On the other hand, the finiteness result of Darmon and Granville is obtained by appealing to Falting's theorem, hence not giving any information about the number of *proper solutions* needed for making the above corollary effective.

Over totally real fields, instead of using Serre's conjecture (see Conjecture 2.1) we can take advantage of modularity theorems and prove the following more general result.

Theorem 1.2. *Let K be a totally real Galois number field for which Conjecture 2.2 holds and $F \in \mathcal{O}_K[x,y]$ an irreducible binary cubic. If the Thue-Mahler equation* (3) *does not have solutions in $x, y \in \mathcal{O}_K$, then there exists a constant $A_F > 0$ such that for all rational primes $l > A_F$, the superelliptic equation* (4) *does not have solutions in $x, y, z \in \mathcal{O}_K$ such that the* $\gcd(x,y,z)$ *is supported only on primes in S_F.*

Remark. The assumption that K is Galois is needed in order to prove that, for large l, a certain mod l Galois representation is irreducible. If the number field is totally real but not Galois, it will become clear from our proof that an analogous statement to Theorem 1.1 holds independently of Conjecture 2.1 and assuming only Conjecture 2.2. In general, it is not possible to compute the constant A_F introduced in the theorem above and the reason will be explained in Section 6.

The insolubility of (3) seems at first look very restrictive. As pointed out in [2], even when $K = \mathbb{Q}$ one has to go up to discriminant $|\Delta_F| = 2063$ to find the first example of a binary cubic where the S_F-units equation is insoluble. We refer to Section 9 of the respective paper for an example of an infinite family of rational binary cubics satisfying the hypothesis of this theorem. In the same paper, the authors give a heuristic argument for the fact that Theorem 1.2 is applicable to a density one subset of the set of all rational cubic forms.

An analogous corollary to the one above follows from the last theorem when combined with the aforementioned results of [5].

1.1. Differences between general and totally real number fields.

Although sharing similar hypothesis and conclusions, the proofs of Theorems 1.1 and 1.2 are fundamentally different. We highlight here some of the most important differences.

(1) For a general number field K, Serre's modularity conjecture relates a representation $G_K \to \mathrm{GL}_2(\mathbb{F}_l)$, satisfying certain conditions, to a mod l eigenform of weight 2 over K. If K is totally real such a mod l eigenform lifts to a complex eigenform over K, but this is not generally the case for a number field with complex embeddings. We proceed as in [22], showing that if l is sufficiently large then all mod l eigenforms lift. This step makes the computation of the constant A_F

in Theorem 1.1 not feasible in general. To write down a formula for this constant, we would need bounds for the size of torsion subgroups of integral cohomology groups associated to locally symmetric spaces (see Section 2). It is maybe just worth remarking that if one chooses K totally real in Theorem 1.1, then one could compute the constant A_F explicitly.

(2) In order to make the required hypothesis of Theorem 1.2 more general, we do not work with Serre's modularity conjecture but instead we use the known fact that for a fixed totally real field K, all but finitely many $\overline{K}$-isomorphism classes of elliptic curves defined over K are modular (see [7, Theorem 5]). By increasing the value of l, we can make sure that the j-invariants of our family of Frey-Hellegouarch curves are not among the j-invariants of the non-modular curves. Unfortunately, this step makes the constant A_F in Theorem 1.2 ineffective, the reason being that Theorem 5 in loc. cit. matches certain non-modular curves with rational points on a finite set of curves of genus > 1 and then appeals to Faltings' theorem to deduce that there are only finitely many of them.

(3) If K has a real embedding, then a weight 2 complex eigenform over K with rational eigenvalues conjecturally (see Conjecture 2.2) corresponds to an elliptic curve over K. However, for a general number field K, the same conjecture predicts that such an eigenform corresponds to either an elliptic curves or a *fake elliptic curve*. Following the recipe of [22], we show that the images of inertia at some fixed prime dividing Δ_F of the mod l representation of our Frey-Hellegouarch curves are incompatible with images of inertia for fake elliptic curves, thereby eliminating the second possibility in our setting.

2. Eigenforms for GL_2 over number fields and Serre's modularity conjecture

The exposition in this section follows closely the lines of [15, 22]. A celebrated theorem of Khare and Wintenberger connects certain 2-dimensional continuous representations of $G_{\mathbb{Q}}$ into $\mathrm{GL}_2(\mathbb{F}_l)$ with classical modular forms of the hyperbolic plane $\mathcal{H}_2$. In this section, we are about to discuss a conjecture that aims to generalise the theorem of Khare and Wintenberger in a way that is going to be soon clarified.

Let K be a number field with signature (r, s) and let $G := \mathrm{GL}_2(K \otimes \mathbb{R})$, a real Lie group. If we denote by A the diagonal embedding of $\mathbb{R}_{>0}$ into G and by M the maximal compact subgroup of G, the associated symmetric space (see [12]) is given by

$$D := G/AK \cong \mathcal{H}_2^r \times \mathcal{H}_3^s \times \mathbb{R}_{>0}^{r+s-1},$$

where $\mathcal{H}_2, \mathcal{H}_3$ are the hyperbolic plane and space respectively.

We are going to denote by $\widehat{\mathcal{O}}_K, \mathbb{A}_K^f$ the rings of finite adèles of $\mathcal{O}_K$ and K respectively. Fix an ideal $\mathcal{N} \subset \mathcal{O}_K$ and define the compact open subgroup

$$U_0(\mathcal{N}) := \left\{ \gamma \in \mathrm{GL}_2(\widehat{\mathcal{O}}_K) \middle| \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod \mathcal{N} \right\}.$$

Consider the adelic locally symmetric space

$$Y_0(\mathcal{N}) := \mathrm{GL}_2(K) \backslash \left(\left(\mathrm{GL}_2(\mathbb{A}_K^f)/U_0(\mathcal{N}) \right) \times D \right).$$

This space is a disjoint union

$$Y_0(\mathcal{N}) = \bigcup_{j=1}^{h_K} \Gamma_j \backslash D,$$

where Γ_j are arithmetic subgroups of $\mathrm{GL}_2(K)$ with Γ_1 being the usual congruence subgroup $\Gamma_0(\mathcal{N})$ of $\mathrm{GL}_2(\mathcal{O}_K)$ and h_K the class number of K.

The cohomology groups $H^i(Y_0(\mathcal{N}), \overline{\mathbb{F}}_l)$ come equipped with commutative Hecke algebras $\mathbb{T}^i_{\mathbb{F}_l}$. The latter are generated by Hecke operators $T_{\mathfrak{q}}$ associated to prime ideals $\mathfrak{q}$ of $\mathcal{O}_K$ coprime to $l\mathcal{N}$.

Definition 2.1. *A mod l eigenform Ψ of level $\mathcal{N}$ and degree i is a ring homomorphism $\Psi : \mathbb{T}^i_{\mathbb{F}_l} \to \overline{\mathbb{F}}_l$.*

It is known that the values of a mod l eigenform Ψ generate a finite field extension of $\mathbb{F}_l$. We will call two mod l eigenforms of levels $\mathcal{N}, \mathcal{M}$ equivalent if their values agree on Hecke operators associated to prime ideals away from $l\mathcal{N}\mathcal{M}$. It was conjectured by Calegari and Emerton in [3] that every mod l eigenform should be equivalent to one with the same level and degree $r + s$. This conjecture is known to hold for K imaginary quadratic due to low virtual cohomological dimension.

Similarly, the complex cohomology groups $H^i(Y_0(\mathcal{N}), \mathbb{C})$ come equipped with Hecke operators $T_{\mathfrak{q}}$ for all prime ideals $\mathfrak{q} \subset \mathcal{O}_K$ not dividing $\mathcal{N}$. These operators generate a commutative Hecke algebra $\mathbb{T}^i_{\mathbb{C}}(\mathcal{N})$.

Definition 2.2. *A complex eigenform f of level $\mathcal{N}$ and degree i is a complex valued character of $\mathbb{T}^i_{\mathbb{C}}(\mathcal{N})$, i.e. a ring homomorphism $\mathbb{T}^i_{\mathbb{C}}(\mathcal{N}) \to \mathbb{C}$.*

Given such complex eigenform f, it is known that its values generate a finite extension $\mathbb{Q}_f$ of $\mathbb{Q}$. Therefore, one can fix an ideal $\mathfrak{l}$ of $\mathbb{Q}_f$ above l and obtain a mod l eigenform, of the same degree and level, by just setting $\Psi_f(T_\mathfrak{q}) = f(T_\mathfrak{q}) \mod \mathfrak{l}$, for all primes $\mathfrak{q}$ coprime to $l\mathcal{N}$. It is said that a mod l eigenform Ψ lifts to a complex one if there is a complex eigenform f with the same level and degree such that we can obtain Ψ reducing f as above, i.e. $\Psi = \Psi_f$.

A complex eigenform f is called trivial if $f(T_\mathfrak{q}) = \mathrm{Norm}_{\mathbb{Q}_f/\mathbb{Q}}(\mathfrak{q}) + 1$ for all prime ideals $\mathfrak{q}$ of $\mathcal{O}_K$ coprime to the level. Similarly, a mod l eigenform Ψ is called trivial if $\Psi(T_\mathfrak{q}) \equiv \mathrm{Norm}_{\mathbb{Q}_f/\mathbb{Q}}(\mathfrak{q}) + 1 \mod l$ for all prime ideals $\mathfrak{q}$ away from l and the level. Every trivial mod l eigenform can be obtained by reducing an Eisenstein series associated to some cusp of $Y_0(\mathcal{N})$, hence they lift to complex ones. The restriction to eigenforms for GL_2 made in this paper allows us to avoid giving the definion of a “cuspidal" eigenform. In the setting of GL_2, non-triviality amounts to cuspidality.

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

$$0 \longrightarrow \mathbb{Z}_{(l)} \xrightarrow{\times l} \mathbb{Z}_{(l)} \longrightarrow \mathbb{F}_l \longrightarrow 0 \ .$$

This gives rise to a long exact sequence on cohomology

$$\begin{tikzcd}
\ldots H^i(Y_0(\mathfrak{N}), \mathbb{Z}_{(l)}) \arrow[r, "\times l"] & H^i(Y_0(\mathfrak{N}), \mathbb{Z}_{(l)}) \arrow[r] & H^i(Y_0(\mathfrak{N}), \mathbb{F}_l) \arrow[dll, "\delta"] \\
H^{i+1}(Y_0(\mathfrak{N}), \mathbb{Z}_{(l)}) \arrow[r] & \ldots &
\end{tikzcd}$$

from which we can extract the short exact sequence

$$0 \longrightarrow H^i(Y_0(\mathfrak{N}), \mathbb{Z}_{(l)}) \otimes \mathbb{F}_l \longrightarrow H^i(Y_0(\mathfrak{N}), \mathbb{F}_l) \xrightarrow{\delta} H^{i+1}(Y_0(\mathfrak{N}), \mathbb{Z}_{(l)})[l] \longrightarrow 0 \ .$$

In the above, the presence of l-torsion in $H^{i+1}(Y_0(\mathfrak{N}), \mathbb{Z}_{(l)})$ is the obstruction to surjectivity for the map $H^i(Y_0(\mathfrak{N}), \mathbb{Z}_{(l)}) \otimes \mathbb{F}_l \to H^i(Y_0(\mathfrak{N}), \mathbb{F}_l)$. If there is only trivial such torsion, then any Hecke eigenvector $\overline{c}$ in $H^i(Y_0(\mathfrak{N}), \mathbb{F}_l)$ comes from such an eigenvector in $H^i(Y_0(\mathfrak{N}), \mathbb{Z}_{(l)}) \otimes \mathbb{F}_l$. 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 $\mathbb{Z}_{(l)}$

(2) a prime $\mathfrak{l}$ of R above l and
(3) a Hecke eigenvector c in $H^i(Y_0(\mathfrak{N}), R)$

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

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

In the proof of our first theorem, we will be using a special case of Serre's modularity conjecture over number fields. Serre conjectured (see [23]) that all absolutely irreducible, odd mod l Galois representations of $G_{\mathbb{Q}}$ arise from a classical cuspidal eigenform f. In the same article, Serre gave a recipe for the level N and the weight k of the sought after eigenform. As previously mentioned, this conjecture was proved by Khare and Wintenberger [17]. We now state a conjecture concerning mod l representations of G_K, where K is an arbitrary number field.

Conjecture 2.1 (see [22, Conjecture 3.1]). *Let $\overline{\rho} : G_K \to \mathrm{GL}_2(\overline{\mathbb{F}}_l)$ be an odd, irreducible, continuous representation with Serre conductor $\mathcal{N}$ (prime-to-l part of its Artin conductor) such that $\det(\overline{\rho}) = \chi_l$, the mod l cyclotomic character. Assume that l is unramified in K and that $\overline{\rho}|_{G_{K_{\mathfrak{l}}}}$ arises from a finite-flat group scheme over $\mathcal{O}_{K_{\mathfrak{l}}}$ for every prime $\mathfrak{l} \mid l$. Then there is a (weight 2) mod l eigenform θ over K of level $\mathcal{N}$ such that for all primes $\mathfrak{P}$ coprime to $l\mathcal{N}$, we have*

$$\mathrm{Trace}(\overline{\rho}(\mathrm{Frob}_{\mathfrak{P}})) = \theta(T_{\mathfrak{P}}).$$

Remark. One of the hypothesis required in [22, Conjecture 3.1] is that the prime to l part of $\det(\overline{\rho})$ is trivial. This means that $\det(\overline{\rho})$ could a priori be a power of χ_l, the mod l cyclotomic character. The authors of [22] informed us that after a discussion with Alain Krauss they have strong reasons to believe that the aforementioned conjecture should be more restrictive. This is the reason why the present Conjecture 2.1 is an augmented version of [22, Conjecture 3.1], which requires that $\det(\overline{\rho})$ should be equal to χ_l and not just a power of it.

Remark. For every real embedding $\sigma : K \hookrightarrow \mathbb{R}$ and every extension $\tau : \overline{K} \to \mathbb{C}$ of σ, we obtain a complex conjugation $\tau^{-1} \circ c \circ \tau \in G_K$, where c is the non-trivial element of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$. A representation $\overline{\rho} : G_K \to \mathrm{GL}_2(\overline{\mathbb{F}}_l)$ is called *odd* if the determinant of every complex conjugation is -1. In the absence of such complex conjugations (i.e. when the field K is totally complex) we regard every representation as odd.

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 et al. [11]. We will just mention that this recipe depends on the restriction $\overline{\rho}|_{I_{\mathfrak{l}}}$ to the inertia subgroups for the primes $\mathfrak{l} \subset \mathcal{O}_K$ above l. We only considered very special representations $\overline{\rho}$ (that are finite flat at $\mathfrak{l} \mid l$), for which SerreâĂŹs original weight recipe applies and predicts the trivial weight [23]. This is why we end up with classes in $H^i(Y_0(\mathcal{N}), \overline{\mathbb{F}}_l)$, the trivial weight meaning that we get $\overline{\mathbb{F}}_l$ as coefficient module.

For every complex cuspidal newform $\mathfrak{f}$ with rational integer Hecke eigenvalues, Langland's philosophy predicts there should be a motif attached to $\mathfrak{f}$. This motif is not always an elliptic curve. Some such newforms correspond to a special type of abelian surface as one can see in [4, Theorem 5] or [9, Section 4].

A simple abelian surface A over K whose algebra $D := \mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ of K-endomorphisms is an indefinite division quaternion algebra over $\mathbb{Q}$ is called a *fake elliptic curve*. It is known that if A/K is a fake elliptic curve, then K must be totally complex.

Let A/K be a fake elliptic curve and let l be a prime of good reduction for A. From the l-adic Tate module $T_l(A)$ we get a representation $\sigma_{A,l} : G_K \to \mathrm{GL}_4(\mathbb{Z}_l)$. Let $\mathcal{O}$ be $\mathrm{End}_K(A)$, viewed as an order in D. It is a standard fact in the theory of quaternion algebras over number fields K, as discussed for example in [21], that all but finitely many primes l split the quaternion algebra D. It is described in Ohta's paper [19] that if one denotes $\mathcal{O}_l := \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_l$, then $T_l(A)$ is isomorphic to $\mathcal{O}_l$ as left $\mathcal{O}$ module. The action of $\mathcal{O}$ on $T_l(A)$ is via endomorphisms. This is the source of a two dimensional l-adic Galois representation

$$\rho_{A,l} : G_K \to \mathrm{Aut}_{\mathcal{O}}(T_l(A)) = \mathcal{O}_l^{\times} \cong \mathrm{GL}_2(\mathbb{Z}_l).$$

Moreover, the author of *loc. cit.* proves that $\sigma_{A,l} = \rho_{A,l} \oplus \rho_{A,l}$.

We are now ready to state the second conjecture used in this paper.

Conjecture 2.2 ([22, Conjecture 4.1])**.** *Let $\mathfrak{f}$ be a (weight 2) complex eigenform over K of level $\mathcal{N}$ that is non-trivial, new and has rational integer Hecke eigenvalues. If K has some real place, then there exists an elliptic curve $E_{\mathfrak{f}}/K$, of conductor $\mathfrak{N}$, such that*

$$\#E_{\mathfrak{f}}(\mathcal{O}_K/\mathfrak{q}) = 1 + \mathbf{N}\mathfrak{q} - \mathfrak{f}(T_{\mathfrak{q}}) \quad \textit{for all } \mathfrak{q} \nmid \mathcal{N}. \tag{5}$$

If K is totally complex, then there exists either an elliptic curve $E_{\mathfrak{f}}$ of conductor $\mathcal{N}$ satisfying (5) *or a fake elliptic curve $A_{\mathfrak{f}}/K$, of conductor $\mathcal{N}^2$, such that*

$$\#A_{\mathfrak{f}}(\mathcal{O}_K/\mathfrak{q}) = (1 + \mathbf{N}\mathfrak{q} - \mathfrak{f}(T_{\mathfrak{q}}))^2 \quad \textit{for all } \mathfrak{q} \nmid \mathcal{N}. \tag{6}$$

For a partial result towards Conjecture 2.2 we refer to [9, Theorem 8], which was derived by Blasius from the work of Hida [13]. In particular, the aforementioned conjecture holds when K is totally real such that $[K : \mathbb{Q}]$ is odd.

A standard fact about fake elliptic curves is the following.

Theorem 2.1 ([16, Section 3])**.** *Let A/K be a fake elliptic curve. Then A has potentially good reduction everywhere. More precisely, let $\mathfrak{q}$ be a prime of K and consider $A/K_{\mathfrak{q}}$. There is a totally ramified extension $K'/K_{\mathfrak{q}}$ of degree dividing 24 such that A/K' has good reduction.*

The above theorem trivially implies the following proposition, which we just record here for further reference.

Proposition 2.1. *If $\overline{\rho}_{A,l} : G_K \to \mathrm{GL}_2(\mathbb{F}_l)$ is the mod l reduction of the l-adic representation defined above, then for every prime ideal $\mathfrak{q} \subseteq \mathcal{O}_K$ we have*

$$\#\overline{\rho}_{A,l}(I_{\mathfrak{q}}) \leq 24,$$

where $I_{\mathfrak{q}} \trianglelefteq G_K$ is the inertia subgroup at $\mathfrak{q}$.

This is going to be crucial in Section 5 when we are showing that mod l Galois representations of elliptic curves attached to a solution of (4) are not *compatible* with representations $\overline{\rho}_{A,l}$ for any fake elliptic curve A.

3. Properties of the Frey curve

The proofs of Theorem 1.1 and 1.2 use a construction of Bennett and Dahmen [2]. For every Klein form (see [2, Section 2] for the precise definition of these special binary forms) $F(x, y) \in \mathcal{O}_K[X, Y]$, the authors of *loc. cit* constructed a family of Frey-Hellegouarch curves $E_{x,y}$. Important properties of this family of curves are nicely controlled by the Klein form $F(x, y)$. It turns out that all non-singular binary cubics are Klein forms (of index 2) and from now on we restrict ourselves to these particular forms. One could write similar, more general, statements for our main two theorems when F is allowed to be a general Klein form. Although these could be proved following the strategy presented here, we only treat binary cubics. In this case, the computations are shorter and easier to follow, therefore facilitating a better exposition of the main ideas in our proofs. The author is considering dedicating a chapter from his PhD thesis to analogous work on all the types of Klein forms.

Let $F(x,y) \in K[X,Y]$ be an irreducible binary cubic of discriminant Δ_F. Its Hessian is the quadratic form

$$H(x,y) = \frac{1}{4}\begin{vmatrix} F_{xx} & F_{xy} \\ F_{xy} & F_{yy} \end{vmatrix}$$

and the *Jacobian determinant* of F and H is the cubic form

$$G(x,y) = \begin{vmatrix} F_x & F_y \\ H_x & H_y \end{vmatrix}.$$

Connecting them there is the following identity, vital for the construction of the family of Frey-Hellegouarch curves in [2],

$$4H(x,y)^3 + G(x,y)^2 = -27 \cdot \Delta_F \cdot F(x,y)^2. \tag{7}$$

The identity above holds for every binary cubic $F \in K[X,Y]$ whose discriminant Δ_F is non-zero, not just the irreducible ones. There are similar identities, called *syzygies*, for all types of Klein forms. Non-existence of such syzygies is the obstruction in extending this construction of such families of elliptic curves associated to all irreducible binary forms.

For future use, we record the following proposition.

Proposition 3.1 ([2, Prop. 2.1]). *The resultant of a binary form F of degree k with its Hessian H satisfies*

$$\operatorname{Res}(H(x,y), F(x,y)) = (-1)^k \Delta_F^2.$$

Suppose now that F has integral coefficients, more precisely $F(x,y) = \alpha_0 x^3 + \alpha_1 x^2 y + \alpha_2 xy^2 + \alpha_3 y^3$ with $\alpha_i \in \mathcal{O}_K$, for all $i \in \{0,1,2,3,4\}$. Set $T(x,y) = \alpha_1 x - \alpha_2 y$. The authors of [2] constructed the following Frey-Hellegouarch curve

$$E_{x,y} : Y^2 = X^3 + TX^2 + \frac{T^2+H}{3}X + \frac{T^3+3TH+G}{27}. \tag{8}$$

The dependence of x, y is implicit, as $T = T(x,y)$ and $H = H(x,y)$.

It is easy to show that $(T^2+H)/3$ and $(T^3+3TH+G)/27 \in \mathcal{O}_K[X,Y]$. Making use of the formula for the discriminant of an elliptic curve and of the syzygy (7), the fundamental quantities associated to (8) can be computed as

(9)

$$\Delta(x,y) = 2^4\Delta_F F(x,y)^2, \quad c_4(x,y) = -2^4 H(x,y), \quad c_6(x,y) = -2^5 G(x,y)$$

and

$$j(x,y) = \frac{-2^8 H(x,y)^3}{\Delta_F F(x,y)^2} \tag{10}$$

Proposition 3.2. *Let $E_{x,y}$ be a family of Frey curves associated to a binary cubic form $F \in \mathcal{O}_K[x,y]$, as in* (8)*. Let $\mathfrak{P} \notin S_F$ be a prime ideal in $\mathcal{O}_K$ and $x_1, y_1 \in \mathcal{O}_K$ such that $\mathfrak{P} \nmid \gcd(x_1,y_1)$. Then E_{x_1,y_1} is semistable at $\mathfrak{P}$.*

Proof. It is known that if a Weierstrass model of E_{x_1,y_1} over $\mathcal{O}_K$ has $\mathfrak{P} \nmid c_4(x,y)$ or $\mathfrak{P} \nmid \Delta(x_1,y_1)$ then E_{x_1,y_1} is semistable at $\mathfrak{P}$. Recall that the set S_F contains the prime ideals dividing $2\Delta_F$. The proposition follows from the formulas for $\Delta(x_1,y_1)$ and $c_4(x_1,y_1)$ and the resultant identity in Proposition 3.1. □

Proposition 3.3. *Let $E_{x,y}$ be a family of elliptic curves defined as above. Suppose that for some $x_1, y_1 \in K$ the conductor of E_{x_1,y_1} is supported only on S_F. If the class number of K is greater than one, there exists $\xi \in K^\times$ such that $\xi \cdot x_1, \xi \cdot y_1$ are integral,* $\gcd(\xi \cdot x_1, \xi \cdot y_1) \in \mathcal{H}_K$ *and the conductor of $E_{\xi\cdot x_1,\xi\cdot y_1}$ is supported only on S_F. If the class number of K is one, there exists $\xi \in K^\times$ such that $\xi \cdot x_1, \xi \cdot y_1$ are integral,* $\gcd(\xi \cdot x_1, \xi \cdot y_1) = 1$ *and the same conclusion about the conductor holds.*

Proof. We only threat the case in which K has non-trivial class group, as the proof for the latter case follows obviously from the former. As a consequence of cancelling denominators, it is obvious that we can scale the pair (x_1,y_1) by some non-zero $\xi_1 \in \mathcal{O}_K$ such that $\xi_1 x_1, \xi_1 y_1$ are integral. Recall that in (1), we defined $\mathcal{H}_K = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_h\}$ and therefore $[\gcd(\xi_1 x_1, \xi_1 y_1)]$ must be equal to $[\mathfrak{m}_i]$, for some $i \in \{1,\ldots,h\}$. Hence, there exists $\xi_2 \in K^\times$ such that $\xi_2 \cdot \gcd(\xi_1 x_1, \xi_1 y_1) = \mathfrak{m}_i$.

We set $\xi := \xi_2 \cdot \xi_1$ and let $(x_2,y_2) = \xi \cdot (x_1,y_1) \in \mathcal{O}_K^2$. Suppose that $\mathfrak{P} \notin S_F$ is a prime ideal. By the previous proposition, we know that E_{x_2,y_2} is semistable at $\mathfrak{P}$. If $\mathfrak{P}$ divides the conductor of E_{x_2,y_2} then it must be a prime of multiplicative reduction. This implies the fact that $v_{\mathfrak{P}}(j(x_2,y_2)) < 0$. But since

$$j(x_2,y_2) = \frac{-2^8 \cdot H(x_2,y_2)^3}{\Delta_F \cdot F(x_2,y_2)^2} = \frac{-2^8 \cdot \xi^6 \cdot H(x_1,y_1)^3}{\Delta_F \cdot \xi^6 \cdot F(x_1,y_1)^2} = j(x_1,y_1),$$

$\mathfrak{P}$ must be a prime of multiplicative reduction for E_{x_1,y_1}, which is a contradiction since the conductor of this curve is supported only on S_F. □

Lemma 3.4. *Let $F \in \mathcal{O}_K[x,y]$ be an irreducible binary cubic with corresponding family of Frey curves $E_{x,y}$. Write $j(x,y)$ for the j-invariant of $E_{x,y}$. Let E/K be an elliptic curve whose conductor $\mathcal{N}$ is supported on the set S_F. If $j(E) = j(x_1,y_1)$ for some some $x_1, y_1 \in \mathcal{O}_K$ that are coprime outside S_F, then $F(x_1,y_1) \in \mathcal{O}^*_{K,S_F}$.*

Proof. Suppose that $j(E) = j(x_1,y_1)$ for some $x, y \in \mathcal{O}_K$ that are coprime outside $\mathcal{H}_K$. Assume that $F(x_1,y_1) \notin \mathcal{O}^*_{K,S}$. There is a prime $\mathfrak{P} \notin S_F$ such that $\mathfrak{P} \mid F(x_1,y_1)$. From the explicit equation (10) for $j(x_1,y_1)$ and the resultant identity from Proposition 3.1 we deduce that $\mathfrak{P}$ (since it does not divide Δ_F by definition) cannot divide $H(x_1,y_1)$, so $v_{\mathfrak{P}}(j(E)) < 0$. This implies that E has potentially multiplicative reduction at $\mathfrak{P}$ and hence $\mathfrak{P} \mid \mathcal{N}$, a contradiction. □

4. An effective Chebotarev theorem

In this section, we extend the main result in Section 7 of [2] to general number fields. More precisely, given two elliptic curves E_1, E_2 defined over K such that the G_K modules $E_1[2]$ and $E_2[2]$ are not isomorphic, we would like to effectively bound the norm of a prime ideal $\mathfrak{l}$ such that traces of Frobenii $a_{\mathfrak{l}}(E_1)$ and $a_{\mathfrak{l}}(E_2)$ are distinct. We follow the exposition of the aforementioned section in *loc. cit.*

Given a Galois extension of number fields L/K and a prime ideal $\mathfrak{l}$ of K which is unramified in L/K, we write $\left[\frac{L/K}{\mathfrak{l}}\right]$ for the conjugacy class in $\mathrm{Gal}(L/K)$ consisting of the Frobenius elements at $\mathfrak{l}$.

Theorem 4.1 (Theorem 1.1 in [18]). *There is an absolute, effectively computable, constant A such that for every finite extension K of $\mathbb{Q}$, every finite Galois extension L of K and every conjugacy class C of $\mathrm{Gal}(L/K)$, there exists a prime ideal $\mathfrak{l}$ of K which is unramified in L, for which $\mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{l})$ is a rational prime such that*

$$\mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{l}) \leq 2d_L^A \text{ and } \left[\frac{L/K}{\mathfrak{l}}\right] = C.$$

We will need the following result about the norm of the smallest prime ideal in a given ideal class, which is an easy consequence of [20, Theorem 1.8].

Theorem 4.2. *Given a number field K and a finite set of prime ideals S of $\mathcal{O}_K$, there exists an effective constant $C_{K,S} > 0$, depending only on K and* *the set S, such that every ideal class of K contains a prime ideal $\mathfrak{P} \notin S$ such that* $\mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{P}) < C_{K,S}$.

Although Theorem 1.8 in [20] is stated assuming the Generalised Riemann hypothesis, the statement that we wrote holds without assuming it. Using GRH, the author of *loc. cit.* achieves better bounds for the norm of the sought after prime ideal. He obtains a lower bound on the density of primes with norm smaller than a constant C in every ideal class group, observing that by choosing C large enough the number of such primes must be greater than one. We actually have to make sure that we find a prime outside of a fixed set S, so we need to increase the constant C such that the number of prime ideals is strictly greater than $|S|$. Under GRH, one can take $C_{K,S} = A \cdot \max(2|S|h_K, (h_K \log(d_K))^2)$ where A is an implicit constant (explicitly computable) in [20, inequality (3.17)], h_K is the class number and d_K is the absolute discriminant of the number field K. It was communicated to us via e-mail by Sardari that without using GRH, one can obtain a polynomial bound in terms of $|S|d_K$ for the constant $C_{K,S}$.

Theorem 4.3. *Given L/K a fixed Galois extension of number fields and a finite set S of prime ideals in $\mathcal{O}_K$, there exists a constant $A > 0$ such that for every conjugacy class C of* $\mathrm{Gal}(L/K)$*, there is a prime ideal $\mathfrak{l} \notin S$ of $\mathcal{O}_K$ for which*

$$\mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{l}) \leq A \text{ and } \left[\frac{L/K}{\mathfrak{l}}\right] = C.$$

The constant A is explicitly computable and depends only on L, K and S.

Proof. Let S' be the subset of S consisting of all the prime ideals from S that do not ramify in L/K. If S' is empty, the conclusion follows by applying Theorem 4.1 to the extension L directly. Define the ideal $\mathfrak{m} = \prod_{\mathfrak{P} \in S'} \mathfrak{P}$. By Theorem 4.2, we know that there is a constant $C_{K,S}$ and a prime ideal $\mathfrak{a}$ of norm less than $C_{K,S}$ that lies in $[\mathfrak{m}]^{-1}$, the inverse class of $\mathfrak{m}$ in the ideal class group of K. If we denote by $t \in \mathcal{O}_K$ a generator of the principal ideal $\mathfrak{m} \cdot \mathfrak{a} = (t)$, then the quadratic extension $K(\sqrt{t})/K$ is unramified at the primes not dividing $2t$. The norm of its discriminant is bounded in terms of K and the set S.

The extensions L/K and $K(\sqrt{t})/K$ are Galois. We have the inclusion $K \subseteq L \cap K(\sqrt{t}) \subseteq K(\sqrt{t})$, which together with the fact that $L \cap K(\sqrt{t})/K$ is unramified at $\mathfrak{a}$ implies that $L \cap K(\sqrt{t}) = K$. As a consequence, the compositum $L' := LK(\sqrt{t})$ is such that

$$L'/K \text{ is Galois and } \mathrm{Gal}(L'/K) \cong \mathrm{Gal}(L/K) \times \mathrm{Gal}(K(\sqrt{t})/K).$$

Let us now pick g_t, the non-identity element of the group $\mathrm{Gal}(K(\sqrt{t})/K)$. Applying Theorem 4.1 above, one obtains a prime ideal $\mathfrak{l}$ of $\mathcal{O}_K$ such that $\mathfrak{l}$ is unramified in L'/K, $\mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{l}) \leq 2\,(d_{L'})^A$ and

$$\left[\frac{L'/K}{\mathfrak{l}}\right] = C \times g_t \text{ as a conjugacy class of } \mathrm{Gal}(L'/K).$$

Firstly one observes that since L'/K is ramified at the primes in S, the ideal $\mathfrak{l}$ does not belong to S. Also, $\mathfrak{l}$ does not ramify in the extension L/K and

$$\left[\frac{L/K}{\mathfrak{l}}\right] = C.$$

Finally, as a consequence of the formula $d_{L'} = d_L^2 \cdot \mathrm{Norm}_{L/\mathbb{Q}}\left(\Delta_{L'/L}\right)$, the absolute discriminant $d_{L'}$ depends on the fields K, L and the primes in the set S and can be computed effectively.

□

Using the theorem above, it becomes immediately clear that [2, Proposition 7.4] holds general number fields. For brevity, we include its proof here.

Proposition 4.1. *Let p be a rational prime and E_1/K and E_2/K elliptic curves with conductors $\mathcal{N}_1$ and $\mathcal{N}_2$, respectively, where $\mathcal{N}_1 \mid \mathcal{N}_2$. Write $\rho_i = \overline{\rho}_{E_i,p}$ for $i = 1$ and 2. Suppose that ρ_2 is unramified outside primes dividing pN_1 and that ρ_2 is irreducible. If $\rho_1 \not\cong \rho_2$, then there exists a prime $\mathfrak{l} \subset \mathcal{O}_K$ with $\mathfrak{l} \nmid p\mathcal{N}_1$, for which both*

$$\mathrm{Trace}(\rho_1(\mathrm{Frob}_{\mathfrak{l}})) \not\equiv \mathrm{Trace}(\rho_2(\mathrm{Frob}_{\mathfrak{l}})) \pmod{p}$$

and

$$l < A$$

where l is the rational prime $\mathfrak{l}$ lies over and A is an effectively computable constant depending only on $K, \mathcal{N}_1$ and p.

Proof. Consider the (continuous) homomorphism $G_K \to \mathrm{GL}_2(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$ given by $\sigma \mapsto (\rho_1(\sigma), \rho_2(\sigma))$. Denote by H its image and by L the fixed field of its kernel. Then L/K is finite Galois, unramified outside the set of primes dividing $p\mathcal{N}_1$ and $\mathrm{Gal}(L/K) \cong H$.

Brauer-Nesbitt together with the classical Chebotarev's density theorem guarantees the existence of such a prime $\mathfrak{l}$ whose Frobenius at $\mathfrak{l}$ is an element $(a, b) \in H$ such that

$$\mathrm{Trace}(a) \not\equiv \mathrm{Trace}(b) \pmod{p}$$

and by using $S = \{\mathfrak{P} \subseteq \mathcal{O}_K \mid \mathfrak{P} \text{ is prime and } \mathfrak{P} \mid p\mathcal{N}_1\}$ in Theorem 4.3 above, one gets the desired bound on l.

□

5. The proof of Theorem 1.1

We would like to emphasize that the idea of considering a prime $\mathfrak{q}$ such that $\mathfrak{q}||\Delta_F$ and the computations carried out in (11) - (15) are due to Bennett and Dahmen [2, Appendix A.2], who worked out the particular case $K = \mathbb{Q}$.

Our hypotheses imply that there are $a, b \in \mathcal{O}_K$ such that

$$F(x,y) = \alpha_0(x-ay)^2(x-by) \pmod{\mathfrak{q}}, \text{ for all } x, y \in \mathcal{O}_K. \tag{11}$$

It is important to observe that $a \not\equiv b \pmod{\mathfrak{q}}$. Indeed, suppose that is not the case and $a \equiv b \pmod{\mathfrak{q}}$. By using a linear translation, we can assume that $a \equiv b \equiv 0 \pmod{\mathfrak{q}}$, which is equivalent to $\alpha_1 \equiv \alpha_2 \equiv \alpha_3 \equiv 0 \pmod{\mathfrak{q}}$. Using the formula

$$\Delta_F = 18\alpha_0\alpha_1\alpha_2\alpha_3 + (\alpha_1\alpha_2)^2 - 27(\alpha_0\alpha_3)^2 - 4\alpha_0\alpha_2^3 - 4\alpha_1^3\alpha_3 \tag{12}$$

for the discriminant of a binary cubic, this would imply that $\mathfrak{q}^2 \mid \Delta_F$, which is excluded in our hypothesis. So $a \not\equiv b \pmod{\mathfrak{q}}$ indeed. The formula in (11) implies that

$$H(x,y) \equiv -\alpha_0^2(a-b)^2(x-ay)^2 \pmod{\mathfrak{q}}, \text{ for all } x, y \in \mathcal{O}_K. \tag{13}$$

Suppose that $x_0, y_0, z_0 \in \mathcal{O}_K$ is a solution to (4) such that $\gcd(x_0, y_0, z_0)$ is supported only on S_F and $\mathfrak{q} \nmid z_0$. We will prove that the Frey curve $E := E_{x_0,y_0}$ constructed as in (8) has potentially multiplicative reduction at $\mathfrak{q}$. The discriminant $\Delta(x_0, y_0) = 2^4 \cdot \Delta_F \cdot F(x_0, y_0)^2$ is clearly divisible by $\mathfrak{q}$. The j-invariant of E can be expressed as

$$j(x_0, y_0) = -\frac{2^8 \cdot H(x_0, y_0)^3}{\Delta_F \cdot F(x_0, y_0)^2} \tag{14}$$

If $\mathfrak{q} \mid H(x_0, y_0)$, then from (13) we get that $\mathfrak{q} \mid x_0 - ay_0$. But this would imply that $\mathfrak{q} \mid F(x_0, y_0) = z_0^l$, which is not allowed. Therefore, $\mathfrak{q} \nmid H(x_0, y_0)$ and

$$v_{\mathfrak{q}}(j(x_0, y_0)) = -1 - 2l \cdot v_{\mathfrak{q}}(z_0) = -1. \tag{15}$$

This means that, in particular, E has potentially multiplicative reduction at $\mathfrak{q}$.

Write $\overline{\rho}_{E,l}$ for the residual Galois representation $\overline{\rho}_{E,l} : G_K \to \mathrm{Aut}(E[l]) \cong \mathrm{GL}_2(\mathbb{F}_l)$ induced by the action of G_K on the l-torsion of E. We prove that

$\overline{\rho}_{E,l}$ satisfies the hypothesis of Serre's conjecture starting by proving its absolute irreducibility.

Let L be the Galois closure of K. Denote by $\mathcal{O}_L$ the ring of integers of this number field and by $\mathfrak{q}_L$ a prime above $\mathfrak{q}$. The base change of E to L has potentially multiplicative reduction at $\mathfrak{q}_L$ and [22, Proposition 6.1] guarantees the existence of a constant $B_{L,\mathfrak{q}_L}$ such that if $l > B_{L,\mathfrak{q}_L}$ the restriction $\overline{\rho}_{E,l}|_{G_L} : G_L \to \mathrm{GL}_2(\mathbb{F}_l)$ is irreducible. Eventually increasing l such that $l > v_{\mathfrak{q}_L}(\Delta_F \mathcal{O}_L)$, from the formulas (14, 15) we see that $l \nmid v_{\mathfrak{q}_L}(j(x_0, y_0))$. Using Lemma 5.1 in [22], we obtain that $l \mid \#\overline{\rho}_{E,l}(I_{\mathfrak{q}_L})$, where $I_{\mathfrak{q}_L} \leqslant G_L$ is the inertia subgroup corresponding to $\mathfrak{q}_L$. It is known that every irreducible subgroup of $\mathrm{GL}_2(\mathbb{F}_l)$ which has an element of order l contains $\mathrm{SL}_2(\mathbb{F}_l)$.

As a consequence of the Weil pairing we have that $\det(\overline{\rho}_{E,l}) = \chi_l$, the mod l cyclotomic character. By eventually increasing l such that $L \cap \mathbb{Q}(\zeta_l) = \mathbb{Q}$, we can ensure that $\det(\overline{\rho}_{E,l}|_{G_L})$ is surjective and together with the observations above this implies the surjectivity of $\overline{\rho}_{E,l}|_{G_L}$. Running through all the prime ideals of $\mathcal{O}_L$ above $\mathfrak{q}$ we observe that there exists a constant $B_{K,\mathfrak{q}}$ that depends only on K and $\mathfrak{q}$, such that if $l > B_{K,\mathfrak{q}}$ then $\overline{\rho}_{E,l}$ is surjective.

Our condition that $\gcd(x_0, y_0, z_0)$ is supported on primes contained in S_F implies that if $\mathfrak{P} \notin S_F$ divides $F(x_0, y_0)$, then $\mathfrak{P} \nmid \gcd(x_0, y_0)$. By Proposition 3.2 we see that E is semistable at such primes $\mathfrak{P}$. From results in [23] it follows that the mod l Galois representation $\overline{\rho}_{E,l}$ is unramified away from $S_F \cup \{\mathfrak{l} | \mathfrak{l} \subseteq \mathcal{O}_K \text{ is prime and } \mathfrak{l} \mid l\}$. In addition, at every prime $\mathfrak{l} \mid l$ the valuation of the discriminant of E

$$v_{\mathfrak{l}}(\Delta(x_0, y_0)) = l \cdot v_{\mathfrak{l}}(z_0) \equiv 0 \pmod{l}.$$

This congruence translates into the technical condition that $\overline{\rho}_{E,l}$ is finite flat at $\mathfrak{l}$, required in the hypothesis of Conjecture 2.1. The Serre conductor $\mathcal{N}$ (prime to l part of its Artin conductor) of this representation is supported only on primes in S_F. We also know that $\mathcal{N}$ divides the conductor of E, therefore we can bound the exponent of $\mathfrak{a}$ in $\mathcal{N}$ using [24, Theorem IV.10.4]. We get

$$v_{\mathfrak{a}}(\mathcal{N}) \leq 2 + 3v_{\mathfrak{a}}(3) + 6v_{\mathfrak{a}}(2) \leq 2 + 6 \cdot |K : \mathbb{Q}|$$

for all prime ideals $\mathfrak{a} \in S_F$. The essential fact is that $\mathcal{N}$ belongs to a finite set that depends only on the form F and, of course, K.

The Galois representation $\overline{\rho}_{E,l}$ satisfies all the hypothesis of Conjecture 2.1 and hence the latter implies the existence of a weight 2 mod l eigenform

θ over K of level $\mathcal{N}$, such that for all primes $\mathfrak{P}$ coprime to $l\mathcal{N}$, we have

$$\mathrm{Trace}(\overline{\rho}_{E,l}(\mathrm{Frob}_{\mathfrak{P}})) = \theta(T_{\mathfrak{P}}).$$

Since there are only finitely many possible levels $\mathcal{N}$ and the integral cohomology subgroups of $Y_0(\mathcal{N})$ are known to be finitely generated, one can conclude that there is a constant C_1 that depends only on K and the set S_F such that by taking $l > C_1$ the cohomology subgroups $H^i(Y_0(\mathcal{N}), \mathbb{Z})$ have trivial l torsion for every $i \geq 1$. This implies that the l-torsion of every $H^i(Y_0(\mathcal{N}), \mathbb{Z}_{(l)})$ is trivial for all $i \geq 1$, hence we can guarantee that there exists a weight 2 complex eigenform $\mathfrak{f}$ with level $\mathcal{N}$ that is a lift of θ as explained in Section 2. This is the only ineffective step in our theorem, in the sense that although one can use algorithms to compute C_1 for an individual level $\mathcal{N}$ as it was done in [27], we do not know how to write down a formula for the constant C_1 in terms of $\mathcal{N}, F$ and K.

Since $\mathcal{N}$ belongs to a finite set, the list of such possible eigenforms $\mathfrak{f}$ is finite and depends only on K. It follows from [22, Lemma 7.2] that there is a constant C_2 such that if we make sure that $l > C_2$, then the Hecke eigenvalues of $\mathfrak{f}$ belong to $\mathbb{Z}$. By Conjecture 2.2, $\mathfrak{f}$ corresponds to an elliptic curve $E_{\mathfrak{f}}$ of conductor $\mathcal{N}$ or to a fake elliptic curve $A_{\mathfrak{f}}$ of conductor $\mathcal{N}^2$. We observed earlier in this proof that $l \mid \#\overline{\rho}_{E,l}(I_{\mathfrak{q}})$, therefore using Proposition 2.1, we see that for $l > 24$ the latter situation cannot happen and for such primes l, $\mathfrak{f}$ corresponds to an elliptic curve $E_{\mathfrak{f}}$ of conductor $\mathcal{N}$. It is worth mentioning that $E_{\mathfrak{f}}$ does not depend on the solution (x_0, y_0, z_0, l) of the superelliptic equation (4). On the other hand, for all primes $\mathfrak{P} \nmid l\mathcal{N}$ we have

$$\mathrm{Trace}(\overline{\rho}_{E,l}(\mathrm{Frob}_{\mathfrak{P}})) = \mathrm{Trace}(\overline{\rho}_{E_{\mathfrak{f}}}(\mathrm{Frob}_{\mathfrak{P}}))$$

which implies

$$\#E(\mathcal{O}_K/\mathfrak{P}) \equiv \#E_{\mathfrak{f}}(\mathcal{O}_K/\mathfrak{P}) \pmod{l}. \tag{16}$$

We will now prove that, for l large enough, $E[2]$ and $E_{\mathfrak{f}}[2]$ are isomorphic as G_K modules. From [2, Proposition 6.8] it follows that, since the binary cubic F is irreducible over K, the mod 2 representation $\overline{\rho}_{E,2}$ is also irreducible. Now if the G_K modules $E[2]$ and $E_{\mathfrak{f}}[2]$ are not isomorphic, by Proposition 4.1 used with $p = 2$ we obtain a prime ideal $\mathfrak{P} \subset O_K$, of norm that is bounded in terms of K and S_F such that $\#E(\mathcal{O}_K/\mathfrak{P}) \not\equiv \#E_{\mathfrak{f}}(\mathcal{O}_K/\mathfrak{P}) \pmod 2$. In particular, $\#E(\mathcal{O}_K/\mathfrak{P}) - \#E_{\mathfrak{f}}(\mathcal{O}_K/\mathfrak{P})$ is non-zero and bounded above in terms of K and S_F as a consequence of the Hasse bounds. Since l divides $\#E(\mathcal{O}_K/\mathfrak{P}) - \#E_{\mathfrak{f}}(\mathcal{O}_K/\mathfrak{P})$, we infer that there exists a constant C_3 such that if $l > C_3$ then $E[2]$ and $E_{\mathfrak{f}}[2]$ are isomorphic as G_K modules.

In the terminology used by Fisher in [6], the elliptic curves $E = E_{x_0,y_0}$ and $E_{\mathfrak{f}}$ are said to be 2-congruent. Proposition 6.2 in [2] implies that $E_{\mathfrak{f}}$ is isomorphic over K to a Frey curve E_{x_1,y_1} for some $x_1, y_1 \in K$. In fact, by Proposition 3.3 we can scale the pair (x_1, y_1) such that $x_1, y_1 \in \mathcal{O}_K$, $\gcd(x_1, y_1) \in \mathcal{H}_K$ (or is trivial if the class group of K is) and the conductor of E_{x_1,y_1} is still supported only on S_F. We now make use of Lemma 3.4 to get that $F(x_1, y_1) \in \mathcal{O}^*_{K,S_F}$, a contradiction to (3).

All of the constants defined in this section depend only on F and K, therefore if we choose $A_{K,F}$ to be larger than all of them the proof of our theorem is completed.

6. K totally real and the proof of Theorem 1.2

When K is totally real, recall that an elliptic curve E defined over K is *modular* if there exists a Hilbert cuspidal eigenform $\mathfrak{f}$ of parallel weight 2, with rational Hecke eigenvalues, such that there is an isomorphism of compatible Galois representations

$$\rho_{E,l} \cong \rho_{\mathfrak{f},l}. \tag{17}$$

The left-hand side of the above is the Galois representation arising from the action of G_K on the l-adic Tate module $T_l(E)$, while the right-hand side is the Galois representation associated to $\mathfrak{f}$ by Taylor in [25]. We are going to make use of the known fact [7, Theorem 5] that if an elliptic curve E/K is not modular, then its j-invariant belongs to a finite set $\mathcal{W}_K$ that depends only on the base field K. Since the finiteness of $\mathcal{W}_K$ is obtained by applying Falting's theorem to curves of genus greater than one, unfortunately we cannot find the points in $\mathcal{W}_K$ nor the cardinality of this set.

As it is anticipated in the title, we dedicate this section to proving Theorem 1.2. Before we start the actual proof, we need the following lemma.

Lemma 6.1. *Let $F \in \mathcal{O}_K[x, y]$ be an irreducible binary cubic. There is a constant $C := C_{K,F} > 0$, depending only on F and on the field K, such that the following statement holds:*

For all $x, y \in \mathcal{O}_K$, if there exists a prime $\mathfrak{P} \notin S_F$ such that $v_{\mathfrak{P}}(F(x, y)) \geq C$ and $\mathfrak{P} \nmid \gcd(x, y)$ then the Frey curve $E_{x,y}$ constructed as in (8) *is modular.*

Proof. From the irreducibility of F it follows that $\Delta_F \neq 0$ and $F(x, y) \neq 0$, hence the elliptic curve $E_{x,y}$ is well-defined. Suppose that the curve $E_{x,y}$ is not modular. Without losing generality we can assume that $v_{\mathfrak{P}}(y) = 0$.

Let H be the Hessian of F. Recall the formula (10) for the j-invariant from which

$$H(x,y)^3 = -2^{-8} \cdot \Delta_F \cdot j(x,y) \cdot F(x,y)^2$$

and therefore

$$v_{\mathfrak{P}}(H(x,y)) = 2v_{\mathfrak{P}}(F(x,y))/3 + v_{\mathfrak{P}}(j(x,y))/3.$$

Since $j(x,y)$ belongs to the finite set $\mathcal{W}_K$, we find that there exists a constant B, that depends only on K such that $v_{\mathfrak{P}}(j(x,y))/3 \geq B$. Now, if we set $C := \max(1, -B/2+1)$, we observe that $\min(v_{\mathfrak{P}}(F(x,y)), v_{\mathfrak{P}}(H(x,y))) \geq 1$.

Using the resultant identity in Proposition 3.1, we can see that $\mathfrak{P} \mid \Delta_F$ and therefore $\mathfrak{P} \in S_F$, a contradiction. □

Having all of this, let us get back to the proof of Theorem 1.2.

Suppose $x_0, y_0, z_0 \in \mathcal{O}_K$ is a solution to the generalised superelliptic equation (4) and that $\gcd(x_0, y_0, z_0)$ is supported only on primes in S_F. To the pair (x_0, y_0) we can attach an elliptic curve curve $E := E_{x_0,y_0}$ as in (8).

The hypothesis of the theorem implies that there exists a prime ideal $\mathfrak{P} \notin S_F$ such that $\mathfrak{P} \mid z_0$. As $F(x_0, y_0) = z_0^l$, we know that $\mathfrak{P} \nmid \gcd(x_0, y_0)$ and we can apply Lemma 6.1 to see that for $l > C_1$, a constant depending only on K and F, the elliptic curve E is modular. Denote by $\mathcal{N}$, the conductor of our elliptic curve. $\mathcal{N}$ depends on the solution x_0, y_0, as E does.

A major step in this proof is obtainining a Hilbert modular form $\mathfrak{f}$ of parallel weight 2 whose l-adic Galois representation matches the one coming from the l-adic Tate module of $E = E_{x_0,y_0}$ such that the level of the form $\mathfrak{f}$ does not depend on the putative solution x_0, y_0. Such an object will arrise after applying Theorem 7 of [9]. The latter is a level lowering result, obtained from the combined works of Fujiwara, Jarvis and Rajaei, whose hypothesis requires that the residual Galois representation $\overline{\rho}_{E,l}$ is irreducible.

Proposition 3.2 implies that for l large enough such that it is not supported on primes in S_F, the elliptic curve E is semistable at all primes above l. By eventually increasing l, we can assume that l does not ramify in K. Irreducibility of $\overline{\rho}_{E,l}$ follows from Theorem 2 of [10]. To be precise, from the just mentioned theorem it follows that there exists an explicit constant C_2, depending only on the number field K, such that for $l > C_2$, the representation $\overline{\rho}_{E,l}$ is irreducible. For every prime ideal $\mathfrak{P} \notin S_F$ we know from the proposition mentioned at the beginning of this paragraph that the model of E is minimal, semistable at $\mathfrak{P}$ and that $l \mid v_{\mathfrak{P}}(\Delta(x_0, y_0))$. Hence, by [9] it follows that there are

- a Hilbert modular form $\mathfrak{f}$ of parallel weight 2 that is new at level
$$\mathcal{N}_l = \prod_{\mathfrak{P} \in S_F} \mathfrak{P}^{v_{\mathfrak{P}}(\mathcal{N})},$$
- some prime ideal ω of the number field $\mathbb{Q}_{\mathfrak{f}}$ generated by the Hecke eigenvalues of $\mathfrak{f}$, such that $\omega \mid l$ and $\overline{\rho}_{E,l} \cong \overline{\rho}_{\mathfrak{f},\omega}$.

As we discussed in the previous section, since $\mathcal{N}_l$ divides the conductor $\mathcal{N}$ of the elliptic curve E, the exponents of the primes dividing $\mathcal{N}_l$ are bounded. The possible levels $\mathcal{N}_l$ belong to a fixed finite set, hence $\mathfrak{f}$ belongs to a finite set of Hilbert modular forms, a set that depends only on the field K. From Lemma 7.2 in [22] it follows that there exists a constant C_3, depending only on K such that if $l > C_3$ then $\mathfrak{f}$ must have rational Hecke eigenvalues eigenvalues, i.e. $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$. For such a rational eigenform $\mathfrak{f}$, Conjecture 2.1 implies the existence of an elliptic curve $E_{\mathfrak{f}}$ of conductor $\mathcal{N}_l$ that corresponds to $\mathfrak{f}$. In particular, for all primes $\mathfrak{P} \nmid l\mathcal{N}_l$ we have that

$$\mathrm{Trace}(\overline{\rho}_{E,l}(\mathrm{Frob}_{\mathfrak{P}})) = \mathrm{Trace}(\overline{\rho}_{E_{\mathfrak{f}}}(\mathrm{Frob}_{\mathfrak{P}})),$$

which is equivalent to

$$\#E(\mathcal{O}_K/\mathfrak{P}) \equiv \#E_{\mathfrak{f}}(\mathcal{O}_K/\mathfrak{P}) \pmod{l}.$$

The reader should be aware that the final part of this proof is identical to the one presented at the end of Section 5. As it was pointed out previously, the irreducibility of F implies that $\overline{\rho}_{E,2}$ is irreducible. Using Proposition 4.1 we observe that there exists a constant C_4 such that if $l > C_4$, then $E[2]$ and $E_{\mathfrak{f}}[2]$ are isomorphic as G_K modules. Using the same result as in the previous section, namely [2, Proposition 6.2], we get that $E_{\mathfrak{f}}$ is isomorphic over K to a curve in our Frey-Hellegouarch family, E_{x_1,y_1} for some $x_1, y_1 \in K$. As explained in Proposition 3.3, we can scale the pair (x_1, y_1) such that it becomes integral, $\gcd(x_1, y_1) \in \mathcal{H}_K$ (it can be made trivial if K has class number one) and the conductor of the Frey curve E_{x_1,y_1} remains supported only on the primes in S_F. We now get a contradiction to the hypothesis of our theorem, since Lemma 3.4 implies $F(x_1, y_1) \in \mathcal{O}_{K,S_F}^{\times}$.

All four constants defined in this section depend only on the form F and the number field K. We conclude the proof of the theorem by choosing the constant A_F to be greater than all these constants.

Remark. The only “ineffective" step in this section is the application of Lemma 6.1, which guarantees that for l large enough, the Frey-Hellegouarch curves we care about are modular.

Acknowledgements. We are indebted to the anonymous referee for carefully reading this paper and for many helpful remarks. The author is very grateful to his advisor Samir Siksek for suggesting the problem and for his great support. It is also a pleasure to thank Oleksiy Klurman, Vlad Matei, Naser Sardari and Haluk Şengün for useful discussions.

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 and S. R. Dahmen, *Klein forms and the generalized superelliptic equation*, Ann. of Math. **177** (2013), 171–239.

[3] F. Calegari and M. Emerton, *Completed cohomology - a survey*, Non-abelian Fundamental Groups and Iwasawa theory **393** (2011), 239–257.

[4] J. E. Cremona, *Abelian varieties with extra twist, cusp forms and elliptic curves over imaginary quadratic fields*, J. London Math. Soc. **45** (1992), 404–416.

[5] H. Darmon and A. Granville, *On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$*, Bull. London Math. Soc. **27** (1995), no. 6.

[6] T. Fisher, *The Hessian of a genus one curve*, Proc. Lond. Math. Soc. **104** (2012), no. 3, 613–648.

[7] 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.

[8] N. Freitas and S. Siksek, *Fermat's Last Theorem over some small real quadratic fields*, Algebra & Number Theory **9** (2015), 875–895.

[9] ———, *An asymptotic Fermat's Last Theorem over five-sixths of real quadratic fields*, Compos. Math. **151** (2015), 1395–1415.

[10] ———, *Criteria for Irreducibility of mod p Representations of Frey Curves*, J. Théor. Nombres Bordeaux **27** (2015), no. 1, 67–76.

[11] T. Gee, F. Herzig, and D. Savitt, *General Serre weight conjectures*, J. Eur. Math. Soc. (JEMS) **20** (2018), no. 12, 2859âĂŞ2949.

[12] P. E. Gunnells, *Lectures on Computing Cohomology of Arithmetic Groups* (2014), 3–45.

[13] H. Hida, *On Abelian Varieties with Complex Multiplication as Factors of the Jacobians of Shimura Curves*, Amer. J. of Math. **103** (1981), no. 4, 727–776.

[14] F. Jarvis and P. Meekin, *The Fermat equation over $\mathbb{Q}(\sqrt{2})$*, J. Number Theory **109** (2004), no. 1, 182–196.

[15] A. Jones and M. H. Şengün, *Mod p base change transfer for* GL_2, J. Ramanujan Math. Soc. **33** (2018), no. 3, 297–334.

[16] B. W. Jordan, *Points on Shimura curves rational over number fields*, J. Reine Angew. Math. **371** (1986), 92–114.

[17] C. Khare and J. P. Wintenberger, *Serre's modularity conjecture. II.*, Invent. Math. **178** (2009), no. 3, 505–586.

[18] J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko, *A Bound for the Least Prime Ideal in the Chebotarev Density Theorem.*, Invent. Math. **54** (1979), 271–296.

[19] M. Ohta, *On l-adic representations of Galois groups obtained from certain two-dimensional abelian varieties*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **21** (1974), no. 3, 299 –308.

[20] N. T. Sardari, *The least prime ideal in a given ideal class*, ArXiv e-prints (February 2018), available at `1802.06193`.

[21] M. H. Şengün, *Some Applications of Number Theory to 3-Manifold Theory*, ArXiv e-prints (March 2012), available at `1203.1428`.

[22] M. H. Şengün and S. Siksek, *On the asymptotic Fermat's Last Theorem over number fields*, Commentarii Matematici Helvetici **93** (2018), 359–372.

[23] J. P. Serre, *Sur les représentations modulaires de degré 2 de Gal*$(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987), 179–230.

[24] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Vol. 151, Springer, GMT, 1994.

[25] R. Taylor, *On Galois representations associated to Hilbert modular forms.*, Invent. Math. **98** (1989), no. 2, 265–280.

[26] ______, *Representations of Galois groups associated to modular forms*, Preceedings of the ICM **1,2** (1994), 435–442.

[27] G. C. Ţurcaş, *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, CV4 7AL, United Kingdom

E-mail address: `g.c.turcas@warwick.ac.uk`