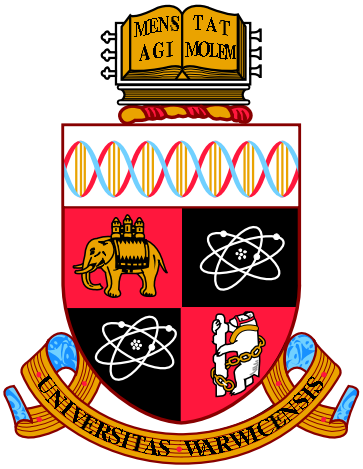

Diophantine applications of Serre's modularity conjecture over general number fields

by

George Cătălin Ţurcaş

Thesis

Submitted to the University of Warwick

for the degree of

Doctor of Philosophy

Department of Mathematics

April 2019

Contents

Acknowledgments

I would like to start by thanking my parents Carmen and Septimiu, without whose efforts and sacrifices towards my education and happiness, I would not have been the person I am today. Together with my brother Adi, they are always in my heart no matter how many thousands of kilometres set us apart. This thesis was not something I could leave at the office, so my deepest appreciation goes towards my wife Cristina for her infinite patience with my muddling mathematical thoughts and for her love which has given me such great happiness during the past three years.

My most sincere gratitude goes to Professor Samir Siksek, who guided me through these years with all his patience, brilliance and kindness. I am thankful for all the lessons he taught me, for the large amount of time he dedicated to me, for the mathematical problems he told me about and for the great insights he shared.

A very special thank you goes towards Professor John Cremona and Dr. Haluk Şengün for many illuminating answers to my questions concerning topics featured in this thesis. I extend my gratitude to the friendly staff, PhD students and to the Number Theory group at the University of Warwick for providing such a warm and prolific environment.

I would like to thank my examiners, Dr. Damiano Testa and Dr. Haluk Şengün for an enjoyable viva, for their time in reading my work and for their many valuable improvements and corrections to this thesis.

I am indebted to the anonymous referees from the journals *Research in Number Theory* and *Acta Arithmetica* for their careful reading of my first two papers and for many helpful remarks.

Last but not least, I am very thankful to Alice, Alessandro, Ferdinando, Fran-

cisco, Josha, James, Livia, Mattia, Marco and the entire Italian student community for their support, constant encouragement and delicious food.

Declarations

Chapters 1 and 2 in this thesis are of expository nature. The first one culminates with the proof of Theorem 1.4.1, which is due to Jordan [32, Section 3]. The discussion preceding Jordan's theorem is intended to provide the necessary background for understanding its proof. As such, the results presented there are not new: the source for the criterion of Néron-Ogg-Shafarevich and its applications is [50] and the proof of Theorem 1.3.1 is due to Morita [39]. In the second chapter, we follow [31, 46] to give an overview of the theory of eigenforms for GL_2 and the statements of two conjectures concerning these eigenforms.

The third chapter is an extended version of my paper [57], which has appeared in *Research in Number Theory*. In addition to the results on Fermat's equation over $\mathbb{Q}(i), \mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-7})$ published in the aforementioned article, this chapter contains proofs of similar results over all the other imaginary quadratic fields of trivial class number. As opposed to the published version, here we included proofs of essential results from [20], [19] and [46] for brevity.

The last chapter consists entirely of a paper which has already been accepted for publication in *Acta Arithmetica*. The problem considered here was inspired by the wonderful results of Bennett and Dahmen [3] on the generalised superelliptic equation over $\mathbb{Q}$. Following the skeleton of their article, we have considered the same problem over general number fields K.

Unless otherwise stated, the results in the last two chapters, consist of original material and are a product of my own research, under the guidance of my supervisor.

Abstract

The thesis starts with two expository chapters. In the first one we discuss abelian varieties with potential good reduction and their Galois representations. We proceed by presenting some of the theory concerning eigenforms for GL_2 over number fields in the second chapter. The last two chapters correspond to two papers I wrote during the course of my PhD studies. Both of these are concerned with applications of Serre's modularity conjecture (see Conjecture 2.2.1) to Diophantine equations over number fields.

As a corollary to Theorem 3.1.1, we show that assuming Conjecture 2.2.1, Fermat's Last Theorem holds over $\mathbb{Q}(i)$. Theorems 3.1.1 and 3.5.1 concern Fermat's equation with prime exponent and cover all the nine quadratic imaginary fields of class number 1. They are under the assumption of Serre's modularity conjecture.

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 $l \geq 5$ prime. Their proof uses, among other ingredients, modularity of certain mod l Galois representations and Ribet's level lowering theorem. In Chapter 3, we considered the same problem over general number fields K. Theorem 4.1.1 shows that, a similar (but more restrictive) criterion on the binary form $F \in \mathcal{O}_K[x, y]$ ensures that the generalised superelliptic equation has finitely many *proper* solutions in $\mathcal{O}_K$. This result is conjectural on Serre's modularity conjecture (see Conjecture 2.2.1) and on a version of Eichler-Shimura (see Conjecture 2.4.1). When K is totally real and Galois, we can make use of modularity theorems to obtain Theorem 4.1.2, independent of Conjecture 2.2.1.

Chapter 1

Abelian varieties with potential good reduction

In this expository chapter we present a detailed proof of the known fact that certain abelian surfaces with quaternionic multiplication have potential good reduction everywhere. Moreover, by going over the proof of the main theorem in [32, Section 3], we exhibit explicit upper bounds on the image of inertia in the Galois representations coming from the Tate module of such abelian surfaces.

Let K be a field, v a discrete valuation on K and $\mathcal{O}_v$ the valuation ring of v. Let us denote the residue field $\mathcal{O}_v/m_v$ by k_v, or just by k when the valuation is clear from the context. By K_s we will denote a separable closure of K and by $\overline{v}$ an extension of v to K_s. We write $D(\overline{v})$ and $I(\overline{v})$ for the decomposition group and the inertia group of $\overline{v}$, respectively. These are subgroups of the absolute Galois group $\mathrm{Gal}(K_s/K)$, which we will sometimes denote by G_K. The quotient $D(\overline{v})/I(\overline{v})$ is canonically isomorphic to $\mathrm{Gal}(\overline{k}/k)$. Here $\overline{k}$ is the residue field of $\overline{v}$, also an algebraic closure of k.

If $\overline{v}$ and $\overline{v}'$ are two extensions of v to K_s, then the inertia groups $I(\overline{v})$ and $I(\overline{v}')$ are conjugate. Suppose that G_K acts on a set S. We say that S is *unramified* at v if $I(\overline{v})$ acts trivially on it. In view of the first phrase of this paragraph, S being unramified at v is independent on the choice of the extension $\overline{v}$, so one could think that, if S is such, the Galois group $\mathrm{Gal}(K_s/K)$ acts on S via $\mathrm{Gal}(\overline{k}/k)$.

1.1 The Tate module

Definition 1.1.1. Let A be an abelian variety over the field K and let n be a positive integer. Denote by $[n] : A(K_s) \to A(K_s)$ the multiplication by n map and

by $A[n]$ its kernel. We call $A[n]$ the group of n-torsion points of A.

Theorem 1.1.1 ([37, IV.3])**.** *Let K be a field and A an abelian variety over K. If n is a positive integer coprime to the characteristic of K, then $A[n]$ is a free rank $2\dim(A)$ module over $\mathbb{Z}/n\mathbb{Z}$.*

The theorem is false when n is not coprime to the characteristic of K. One can see this by looking at what happens for elliptic curves, which are abelian varieties of dimension 1. It is explained for instance in [51, Section V.3] that if E is an elliptic curve over $\mathbb{F}_p$, then $E[p]$ is either trivial or of order p. The elliptic curve is called *supersingular* in the former case and *ordinary* in the latter.

There is a natural action of G_K on the points of $A(K_s)$ and the fixed points of this action are precisely the K-points of A. In particular the origin of the group law 0_A is fixed under the Galois action.

Let $\sigma \in G_K$ and $P \in A(K_s)$. Since the equations that define A and its group law have coefficients in K, we have that $[n](\sigma(P)) = \sigma([n](P))$ for any $n \in \mathbb{Z}$. This shows that the action of G_K on $A(K_s)$ descends to $A[n]$. We just described a representation

$$\overline{\rho}_n : G_K \to \mathrm{Aut}(A[n]).$$

Endowing G_K and $\mathrm{Aut}(A[n])$ with the Krull and discrete topology respectively, the representation $\overline{\rho}_n$ becomes continuous. One can see this by observing that the restriction of $\overline{\rho}_n$ to $\mathrm{Gal}(K_s/K(A[n]))$ is trivial. There are only finitely many points in $A[n]$ and their coordinates are all algebraic, therefore $K(A[n])/K$ is a finite extension and $\overline{\rho}_n$ factors through a finite quotient of G_K. Galois representations arising this way are going to be extensively discussed in this thesis, in the particular case when A is an elliptic curve and n is prime.

Definition 1.1.2. Let A be an abelian variety defined over K and let l be a prime number different from $\mathrm{char}(K)$. The l-adic Tate module of A is

$$T_l(A) = \varprojlim_n A[l^n],$$

where the transition morphisms are given by multiplication by l.

The definition above is saying that an element of $T_l(A)$ is an infinite sequence $\{a_0, a_1, \dots\}$ of torsion points on A such that for all $i \geq 0$, $a_i \in A[l^i]$ and $la_{i+1} = a_i$. As $A[l^i]$ are all free modules of rank $2\dim(A)$ over $\mathbb{Z}/l^i\mathbb{Z}$, by taking the limit we see that $T_l(A)$ is a free module of rank $2\dim(A)$ over the ring $\mathbb{Z}_l$ of l-adic integers.

We should remark that the continuous action of G_K on each $A[l^i]$ induces a continuous action of the same group on $T_l(A)$ endowed with the profinite topology.

1.2 The criterion of Néron-Ogg-Shafarevich

The following theorem, commonly referred to as "The criterion of Néron-Ogg-Shafarevich", was proved by Serre and Tate.

Theorem 1.2.1 ([50, Theorem 1]). *Let A be an abelian variety over K. Suppose that the residue field k of v is perfect and let l be a prime different from* $\mathrm{char}(k)$. *The following properties are equivalent:*

(a) A has good reduction at v.

(b) $A[n]$ is unramified at v for all n prime to $\mathrm{char}(k)$.

(b') There exist infinitely many integers n, prime to $\mathrm{char}(k)$, *such that $A[n]$ is unramified at v.*

(c) $T_l(A)$ is unramified at v.

The statement (a) does not depend on the prime l, hence an important consequence of the theorem above is that if $T_l(A)$ is unramified for one prime l different from the residue characteristic, then it is so for all such l.

Under the assumptions of the previous theorem, suppose that there exists a finite extension K' of K and a prolongation v' of v to K' such that $A \times_K K'$ has good reduction at v'. In this case, the authors of [50] say that A has *potential good reduction at v*. The same phenomena is sometimes described as A being of *integral modulus at v*. In the particular case when A is an elliptic curve, A has potentially good reduction at v if and only if its j invariant is integral at v, explaining why the second terminology might be preferred.

Let l be a prime number different from the residue characteristic, and let

$$\rho_l : G_K \to \mathrm{Aut}(T_l(A))$$

denote the l-adic representation corresponding to the G_K-module $T_l(A)$. An easy consequence of Theorem 1.2.1 is the assertion that an abelian variety A has potential good reduction at v if and only if the image $\rho_l(I(\overline{v}))$ of the inertia group is finite. In the same paper, Serre and Tate used the theory of Néron models to prove that, when A is such, the kernel and the determinant of the restriction $\rho_l|_{I(\overline{v})}$ are both independent of l. Moreover, the latter determinant is a $\mathbb{Z}$-valued character.

It is not at all surprising that the criterion of "Néron-Ogg-Shafarevich" can be used as a powerful tool for analysing the type of reduction an abelian variety has. We are going to discuss a few criteria that guarantee potential good reduction. For example, in most cases it is sufficient for the image of G_K in $\mathrm{Aut}(T_l(A))$ to be abelian in order to deduce that A has potential good reduction at v.

Proposition 1.2.1 ([50, Corollary 1 of Theorem 2])**.** *Suppose that the residue field k is finite of characteristic p, and that, for some $l \neq p$, the image $\rho_l(G_K)$ in $\mathrm{Aut}(T_l(A))$ is abelian. Then A has potential good reduction at v.*

Proof (sketch). By our previous discussion, A has potentially good reduction at v, if and only if the image of $I(\overline{v})$ is finite. It is easy to see that the latter happens if and only if $A \times_K K_v$ has potentially good reduction at v, where K_v is the completion of K at the place v. The image $\rho_l(G_{K_v})$ is a subgroup of $\rho_l(G_K)$, therefore if the latter is abelian the former is abelian too. Hence, for proving our proposition, we can assume without loosing generality that K is complete with respect to v.

Let U_K be the unit group of the ring of integers of K. By a classical result in the theory of local fields (see for example [49]), U_K is isomorphic to the product of a finite group of order $|k^\times|$ and a pro-p group which we denote by P.

We have the following natural exact sequence

$$1 \longrightarrow 1 + l \cdot \mathrm{End}(T_l(A)) \longrightarrow \mathrm{Aut}(T_l(A)) \longrightarrow \mathrm{Aut}(T_l(A)/l \cdot T_l(A)) \longrightarrow 1 \ .$$

We remark that $1 + l \cdot \mathrm{End}(T_l(A))$ is a pro-l group isomorphic to $\mathcal{M}_{2d}(\mathbb{Z}_l)$ and $\mathrm{Aut}(T_l(A)/l \cdot T_l(A))$ is a finite group isomorphic to $\mathrm{GL}_{2d}(\mathbb{F}_l)$, where d is the dimension of A.

On the other hand, local class field theory proves that the image of $I(\overline{v})$ in $\mathrm{Aut}(T_l(A))$ is isomorphic to a quotient of U_K. As the previous statement appeals to the Artin map, it crucially uses the hypothesis that $\rho_l(G_K)$ is abelian. Since $l \neq p = \mathrm{char}(k)$, the image of P in $\mathrm{Aut}(T_l(A))$ intersects trivially the pro-l part $1 + l \cdot \mathrm{End}(T_l(A))$, therefore it injects into the finite group $\mathrm{Aut}(T_l(A)/lT_l(A))$. The proof of our proposition is complete.

□

1.3 Quaternionic multiplication implies potential good reduction

Let A be an abelian variety over a field K and v be a place of K with finite residue ring. As an application to the above proposition, the authors of loc. cit. show that if there exists a number field F of degree $2 \cdot \deg(A)$ and a ring homomorphism $i : F \to \mathbb{Q} \otimes \mathrm{End}_K(A)$, then A has potential good reduction at v. Such a pair (A, i) is called an abelian variety with *complex multiplication by* F.

We are going to present an analogous result for abelian varieties with so-called *quaternion multiplication*. We follow closely the beautiful proof given by Morita in [39].

Theorem 1.3.1. *Consider B an indefinite division quaternion algebra over the rationals. Let A be a 2-dimensional abelian variety defined over K such that there exists an injection $i : B \to \mathbb{Q} \otimes \mathrm{End}_K(A)$. Then A has potentially good reduction at any discrete place of K.*

Proof. During this proof, we sometimes identify B with its image under i. Let v be a discrete place of K and let $\mathcal{O}$ and k be the valuation ring and the residue field of v, respectively.

Let $A_{\mathcal{O}}$ be the Néron minimal model relative to v. This is a smooth group scheme of finite type over $\mathcal{O}$, together with an isomorphism $A_{\mathcal{O}} \times_{\mathcal{O}} K \cong A$.

Let $\tilde{A}$ be the special fibre of $A_{\mathcal{O}}$ and $\tilde{A}^0$ the connected component of the former. From properties of Néron models, we know that $\tilde{A}$ is an algebraic group defined over k. It is mentioned in [50] that the connected component $\tilde{A}^0$ is an extension of an abelian variety C by a linear group H. For A to have good reduction at v is equivalent to $\tilde{A}$ being itself an abelian variety. Since properness is the only property that might be missing, it follows from [50, Lemma 3] that $\tilde{A}$ is an abelian variety if and only if $H = \{1\}$.

We would like to prove that there exists a finite extension K' of K such that the special fibre of the Néron model of $A \times_K K'$ with respect to a prolongation of v is an abelian variety.

The semistable reduction theorem of Grothendieck (see [24]) implies that there exists a finite extension K' of K such that the connected component of the special fibre of the Néron model of $A \times_K K'$ with respect to any place above v is an extension of an abelian variety by a torus. Therefore, changing K by the finite extension K', we assume that $\tilde{A}^0$ is an extension of an abelian variety C by the torus $(\mathbb{G}_m)^r$, where $\mathbb{G}_m$ is the multiplicative group and $0 \leq r \leq \dim(A) = 2$ is an integer. We aim to prove that $r = 0$.

The universal mapping property of the Néron model gives a map

$$\mathrm{End}_K(A) \to \mathrm{End}_{\mathcal{O}}(A_{\mathcal{O}})$$

and there is also a natural map $\mathrm{End}_{\mathcal{O}}(A_{\mathcal{O}}) \to \mathrm{End}_K(\tilde{A})$. We deduce that any endomorphism $f \in \mathrm{End}_K(A)$ induces one $\tilde{f} \in \mathrm{End}_K(\tilde{A})$. Every endomorphism is continuous in the Zariski topology, therefore $\tilde{f}$ can be restricted to an endomorphism of the connected component $\tilde{A}^0$. Since $(\mathbb{G}_m)^r$ is the maximal linear subgroup of $\tilde{A}^0$

and $f\left((\mathbb{G}_m)^r\right) \subset \tilde{A}^0$ must be a linear subgroup, we deduce that $f\left((\mathbb{G}_m)^r\right) \subseteq (\mathbb{G}_m)^r$. The process described above gives a ring homomorphism

$$\chi : \mathrm{End}_K(A) \to \mathrm{End}_K\left((\mathbb{G}_m)^r\right).$$

It is known that $\mathrm{End}_K\left((\mathbb{G}_m)^r\right) \cong \mathcal{M}_r(\mathbb{Z})$, the ring of $r \times r$ matrices with integral elements, therefore χ extends to a homomorphism $\chi : \mathbb{Q} \otimes \mathrm{End}_K(A) \to \mathbb{Q} \otimes \mathcal{M}_r(\mathbb{Z}) = \mathcal{M}_r(\mathbb{Q})$. Abusing notation, let us denote by χ the just-described homomorphism of rings $\mathrm{End}_K(A) \to \mathcal{M}_r(\mathbb{Q})$. All the homomorphisms presented above were unital, therefore so is χ. This means that χ maps the identity morphism on A to the multiplicative identity I_r. Since B is an indefinite division quaternion algebra defined over $\mathbb{Q}$, B is simple. Hence, the image $\chi(B)$ must be equal to $\{0\}$, which implies that $r = 0$. Our theorem is now proved. □

1.4 Fake elliptic curves

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.

The author learned from [44] that this term was coined by Serre in the 1970s, based on the observation that such a surface is isogenous to the square of an elliptic curve modulo every prime of good reduction. A conjecture belonging to the Langlands' programme predicts that some automorphic forms for GL_2 correspond, in a way that will be made precise in the second chapter, to elliptic curves or to fake elliptic curves. In view of Diophantine applications, we often need to be able to differentiate between these two.

Let A be a fake elliptic curve defined over a number field K, v a discrete place of K and l a prime different from the residual characteristic of v. We previously saw that A has potential good reduction at v, therefore the image of inertia $\rho_l(I(\overline{v})) \subseteq \mathrm{Aut}(T_l(A))$ is finite. The knowledge of an upper bound on the size of this image is essential for the Diophantine applications we will later present.

Theorem 1.4.1 ([32, Section 3])**.** *Let K be a field that is complete with respect to a discrete valuation v of finite residue field k. Suppose that A is a fake elliptic curve defined over K. There is a totally ramified extension K'/K of degree dividing* 24 *such that A has good reduction over K'.*

Proof. Let l be a prime different from $\mathrm{char}(k)$, $B := \mathbb{Q} \otimes \mathrm{End}_K(A)$ an indefinite

quaternion algebra defined over $\mathbb{Q}$ and write

$$R_l : \mathrm{Gal}(K_s/K) \to \mathrm{Aut}_B(T_l(A))$$

for the l-adic representation attached to A, where

$$\mathrm{Aut}_B(T_l(A)) = \{f \in \mathrm{Aut}(T_l(A)) | f \text{ commutes with the action of } B \text{ on } \mathbb{Q} \otimes T_l(A)\}.$$

Let $N = \ker(R_l) \cap I(\overline{v})$ be the kernel of R_l restricted to the inertia. It coincides with the kernel of $\rho_l|_{I(\overline{v})} : I(\overline{v}) \to \mathrm{Aut}(T_l(A))$, subgroup which is independent of l and has finite index in $I(\overline{v})$ by the results of Serre discussed above. Write $\Phi(A/K) := I(\overline{v})/N$.

Denote by σ a Frobenius element and by Γ_σ the closure of the subgroup generated by it in $\mathrm{Gal}(K_s/K)$. The absolute Galois group $\mathrm{Gal}(K_s/K)$ is the semidirect product between $I(\overline{v})$ and Γ_σ. Since N is a closed subgroup of G_K which has finite index in $I(\overline{v})$, we see that $N \cdot \Gamma_\sigma$ is an open subgroup of G_K. Let K' be the (finite) extension of K cut out by the action of $N \cdot \Gamma_\sigma \subseteq G_K$.

By definition, the inertia subgroup of $\mathrm{Gal}(K_s/K')$ acts trivially on $T_l(A \times_K K')$, therefore $A' := A \times_K K'$ has good reduction by the criterion of Néron-Ogg-Shafarevich. Let v' be the restriction of $\overline{v}$ to K'. As K'/K is totally ramified, we deduce that the residue field of v' is k. Therefore, the special fibre $\tilde{A}'$ of the Néron model of A' corresponding to v' is an abelian surface defined over k whose endomorphism algebra $\mathbb{Q} \otimes \mathrm{End}_k(\tilde{A}')$ is isomorphic to B. Lemma 2 in [50] asserts that the Tate modules $T_l(A')$ and $T_l(\tilde{A}')$ are canonically isomorphic as $\mathrm{Gal}(K_s/K') = N \cdot \Gamma_\sigma$ modules. By the universal property of the Néron model, the action of $I(\overline{v})$ is compatible with the reduction map from the Néron model to its special fibre $\tilde{A}'$. Since $I(\overline{k})$ acts trivially on the residue field k, an argument of Serre and Tate in loc. cit. explains that $I(\overline{v})$ acts on the abelian variety $\tilde{A}'$ by k-automorphisms, i.e. *algebraic automorphisms* (see [50, pages 496-497] for further details). The restriction of R_l on $I(\overline{v})$ factors as follows

$$\begin{array}{ccc} I(\overline{v}) & \xrightarrow{\quad R_l \quad} & \mathrm{Aut}_B(T_l(A)) = \mathrm{Aut}_B(T_l(\tilde{A}')) \\ & \searrow \quad \nearrow & \\ & \mathrm{Aut}_B(\tilde{A}'/k) & \end{array} .$$

This proves that our defined group $\Phi(A/K)$ is isomorphic to a subgroup of $\mathrm{Aut}_B(\tilde{A}'/\overline{k})$. From Jordan's beautiful classification [32, Proposition 2.8] we see

that the group $\mathrm{Aut}_B(\tilde{A}'/\overline{k}) = \mathrm{Aut}_k(\tilde{A}') \cap \mathrm{End}_B(\tilde{A}'/k)$ isomorphic to a subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$, to a subgroup of the dihedral group of order 12 or it is a cyclic group of order $2, 4$ or 6. Our theorem is now proved. $\square$

Chapter 2

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

The exposition in this chapter follows closely the lines of [31, 46]. 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 chapter, 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.

2.1 Mod l and complex eigenforms

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 [26]) is given by

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

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

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

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

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 [8] 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 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 2.1.2. *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 $\Psi_f(T_{\mathfrak{q}}) = f(T_{\mathfrak{q}}) \bmod \mathfrak{l}$, 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 thesis allows us to avoid giving the definition of a "cuspidal" eigenform. The interested reader can find the precise definition in [2]. 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

$$\ldots H^i(Y_0(\mathfrak{N}), \mathbb{Z}_{(l)}) \xrightarrow{\times l} H^i(Y_0(\mathfrak{N}), \mathbb{Z}_{(l)}) \longrightarrow H^i(Y_0(\mathfrak{N}), \mathbb{F}_l) \xrightarrow{\delta} H^{i+1}(Y_0(\mathfrak{N}), \mathbb{Z}_{(l)}) \longrightarrow \ldots$$

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 $\bar{c}$ 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 [2, 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 $\bar{c}$. 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 [2, Section 1.2] for a more illuminating discussion.

2.2 Serre's modularity conjecture

In the proof of our theorems, we will be using a special case of Serre's modularity conjecture over number fields. Serre conjectured (see [47]) 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 [34]. We now state a conjecture concerning mod l representations of G_K, where K is an arbitrary number field.

Conjecture 2.2.1. *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) and 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 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. 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 totally real number fields was given by Buzzard et al. [7] and, in general for GL_n over number fields by Gee et al. [22]. 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 Serre's original weight recipe applies and predicts the trivial weight [47]. 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.

2.3 When K is imaginary quadratic of class number one

In Chapter 3, we will be restricting ourselves to the particular case in which K is quadratic imaginary of class number one. As we explain below, due to the low cohomological dimension, all the cuspidal eigenforms are equivalent to degree 1 such forms. The previous statement is true over all imaginary quadratic fields, not just the ones having class number one. we anticipate that it will play a key role in the computations we perform in Chapter 3.

Just for this section, let K be one of the nine imaginary quadratic fields of class number one. Let $G = \mathrm{Res}_{K/\mathbb{Q}}(\mathrm{GL}_2)$ be the algebraic group over $\mathbb{Q}$ that is obtained from GL_2 by restriction of scalars from K to $\mathbb{Q}$. The group of real points $G(\mathbb{R}) = \mathrm{GL}_2(K \otimes_{\mathbb{Q}} \mathbb{R}) \cong \mathrm{GL}_2(\mathbb{C})$ acts transitively on the hyperbolic 3-space $\mathcal{H}_3$. Fix an ideal $\mathcal{N} \subset \mathcal{O}_K$. The locally symmetric space $Y_0(\mathcal{N})$ defined previously is now much simpler,

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

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 $\mathrm{GL}_2(\mathcal{O}_K)$.

The arguments given in this paragraph are topological, so the conclusions about cohomology groups hold regardless of the characteristic of the field of coefficients. The space $Y_0(\mathcal{N})$ is 3 dimensional and non-compact, therefore $H^n(Y_0(\mathcal{N})) = 0$, for every $n > 2$. It is known that $H^0(Y_0(\mathcal{N}))$ is one-dimensional and does not hold any non-trivial eigenforms. This implies that all non-trivial eigenforms live in $H^1(Y_0(\mathcal{N}))$ or $H^2(Y_0(\mathcal{N}))$.

For $l \geq 5$, the cuspidal parts (see [2] for the precise definition) of $H^1(Y_0(\mathcal{N}), \overline{\mathbb{F}}_l)$ and $H^2(Y_0(\mathcal{N}), \overline{\mathbb{F}}_l)$ are isomorphic as Hecke modules and the same holds for the cuspidal parts of $H^1(Y_0(\mathcal{N}), \mathbb{C}))$ and $H^2(Y_0(\mathcal{N}), \mathbb{C})$. These isomorphisms follow from a duality result of Ash and Stevens [2, Lemma 1.4.3]. Therefore, in our setting, any mod l or complex eigenform is equivalent to one of the same level and degree 1. This particular case of a more general conjecture of Calegari and Emerton (see [8]) holds in the present situation due to the low dimension.

Since everything happens in degrees 1, 2 and the non-trivial parts of the corresponding Hecke algebras are isomorphic, in Chapter 3 we are going to forget about the upper script i and, we will just write write $\mathbb{T}_{\mathbb{F}_l}(\mathcal{N})$ respectively $\mathbb{T}_{\mathbb{C}}(\mathcal{N})$, sometimes referring to the non-trivial part of the degree one Hecke algebra and sometimes referring to the one of degree two. The eigenforms in these algebras are sometimes called mod l Bianchi modular forms, respectively Bianchi modular forms

in the literature.

In view of the above, we reiterate that the existence of a complex (or mod l) eigenform is equivalent to the existence of a class in $H^1(Y_0(\mathcal{N}), \mathbb{C}))$ (or $H^1(Y_0(\mathcal{N}), \overline{\mathbb{F}}_l)$) that is a simultaneous eigenvector for the Hecke operators such that its eigenvalues match the values of the eigenform. With this interpretation, from the previous discussion about lifting eigenforms, we deduce that every mod l eigenform of degree 1 lifts to a complex one when $H^2(Y_0(\mathcal{N}), \mathbb{Z}_{(l)})$ has no l-torsion.

We call an eigenform of level $\mathcal{N}$, complex or mod l, *new* if it is not equivalent to one of level strictly dividing $\mathcal{N}$.

Via the Eichler-Shimura-Harder isomorphism, Bianchi modular forms can be analytically interpreted as vector valued real-analytic functions on the hyperbolic 3-space (see [11] for more details). We are going to be using this point of view in our examination of the Mellin transform of a Bianchi modular form in Section 3.4.

2.4 An Eichler-Shimura conjecture

For every complex cuspidal newform $\mathfrak{f}$, Langland's philosophy (see [10, Theorem 5] or [20, Section 4]) predicts there should be either an elliptic curve or a fake elliptic curve attached to $\mathfrak{f}$.

We defined fake elliptic curves in Section 1.4. Let A/K be one such 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, the primes l such that $l \nmid \mathrm{Disc}(D)$ split the quaternion algebra D. Let l be one such prime. It is described in the Ohta's paper [40] 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 a left $\mathcal{O}$-module. The action of G_K on $T_l(A)$ is via $\mathcal{O}$-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 a conjecture used in the last chapter.

Conjecture 2.4.1. *Let $\mathfrak{f}$ be a complex eigenform over K of level $\mathcal{N}$ that is non-trivial, new and has integer Hecke eigenvalues. If K has some real place, then there*

exists an elliptic curve $E_{\mathfrak{f}}/K$, of conductor $\mathcal{N}$, such that

$$\#E_{\mathfrak{f}}(\mathcal{O}_K/\mathfrak{q}) = 1 + \mathbf{N}\mathfrak{q} - \mathfrak{f}(T_{\mathfrak{q}}) \quad \textit{for all } \mathfrak{q} \nmid \mathcal{N}. \tag{2.4.1}$$

If K is totally complex, then there exists either an elliptic curve $E_{\mathfrak{f}}$ of conductor $\mathcal{N}$ satisfying (2.4.1) *or a fake elliptic curve $A_{\mathfrak{f}}/K$, of conductor $\mathcal{N}^2$, such that*

$$\#A_{\mathfrak{f}}(\mathcal{O}_K/\mathfrak{q}) = (1 + \mathbf{N}\mathfrak{q} - \mathfrak{f}(T_{\mathfrak{q}}))^2 \quad \textit{for all } \mathfrak{q} \nmid \mathcal{N}. \tag{2.4.2}$$

For a partial result towards Conjecture 2.4.1 we refer to [20, Theorem 8], which was derived by Blasius from the work of Hida [28]. 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. We have dedicated the first chapter in this thesis to prove it.

Theorem 2.4.1 ([32, 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 2.4.1. *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 4.4 when we are showing that mod l Galois representations of elliptic curves attached to a solution of (4.1.4) are not *compatible* with representations $\overline{\rho}_{A,l}$ for any fake elliptic curve A.

Chapter 3

Fermat's equation over some quadratic imaginary fields

The first sections of this chapter consist of an article that has already been published in Research in Number Theory. The Open Access version can be accessed using DOI:10.1007/s40993-018-0117-y.

Assuming a deep but standard conjecture in the Langlands programme, we prove Fermat's Last Theorem over $\mathbb{Q}(i)$. Under the same assumption, we also prove that, for all prime exponents $p \geq 5$, Fermat's equation $a^p + b^p + c^p = 0$ does not have non-trivial solutions over $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-7})$.

3.1 Introduction

Wiles' remarkable proof of Fermat's Last Theorem inspired mathematicians to attack the Fermat equation over number fields via elliptic curves and modularity. Successful attempts over totally real quadratic fields had been carried out by Jarvis and Meekin [30], Freitas and Siksek [19], [20] and they rely on progress in modularity over totally real fields due to work of Barnett-Lamb, Breuil, Diamond, Gee, Geraghty, Kisin, Skinner, Taylor, Wiles and others. In particular, modularity of elliptic curves over real quadratic fields was proved by Freitas, Le Hung and Siksek [18].

On the other hand, modularity of elliptic curves over number fields with complex embeddings is highly conjectural. For general number fields, Şengün and Siksek [46] proved an asymptotic version of Fermat's Last Theorem, under the assumption of two standard, but very deep conjectures in the Langlands programme. They prove that for a number field K, satisfying some special properties, there exists

a 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 $K \setminus \{0\}$.

The present work follows the skeleton of their article. Specialising to the fields $\mathbb{Q}(i), \mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-7})$, we were able to make their result effective and to obtain optimal bounds for the constant B_K. Combining this with previous work on the Fermat equation over number fields, was sufficient to derive Theorem 3.1.1 below. Conjecture 4.1 in [46] is known to hold for base-change newforms via the theory of base change functoriality, therefore we obtain a result that is dependant only on Serre's modularity conjecture (see Conjecture 2.2.1).

Throughout this chapter, given a number field K, we are going to denote by $\mathcal{O}_K$ its ring of integers and by $G_K = \mathrm{Gal}(\overline{K}/K)$ its absolute Galois group. We should emphasize some of the difficulties that had to be overcome.

1. First, we had to obtain a small enough constant B_K such that for $p > B_K$ the mod p Galois representation that comes from a Frey curve is absolutely irreducible. This is treated asymptotically in [46], but we had to rely on upper bounds for possible prime torsion that can be achieved by elliptic curves defined over number fields of small degree and class field theory computations to make the bound B_K explicit. We should point out that the class field theory computations are different in an essential way from the ones that had been done in [35] and [19]. The latter rely on the presence of non-trivial units in $\mathcal{O}_K$, which are not available in our setting.

2. We are going to use the definition for eigenforms introduced in Section 2.3. Serre's modularity conjecture relates certain representations $G_K \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ to a mod p eigenform of weight 2 over K. In the classical situation Serre's modularity conjecture, now a theorem due to Khare and Wintenberger, relates some representations $G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ to a complex eigenform of weight 2 over $\mathbb{Q}$. The expression "mod p" does not appear there, because it turns out that all mod p eigenforms over $\mathbb{Q}$ are just reductions of complex eigenforms. This is not the case if K is imaginary quadratic, but Şengün and Siksek [46] managed to circumvent this difficulty by assuming that the prime p is large enough. Unfortunately this step makes their result ineffective. For our choices of K, we made this step effective by computing the torsion in certain cohomology groups using an algorithm of Şengün. This allowed us to lift the mod p eigenforms to complex ones.

3. A complex weight 2 newform over K with rational eigenvalues corresponds conjecturally to an elliptic curve or a fake elliptic curve defined over K (see [46]). The theory of base change functoriality shows that this conjecture holds for the newforms that are base-change lifts of classical newforms. By explicit computation we find that all the newforms that we need to deal with are base-change lifts.

Our results assume a version of Serre's modularity conjecture (see Conjecture 2.2.1) for odd, irreducible, continuous 2-dimensional mod p representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ that are finite flat at every prime over p.

From now on, we restrict ourselves to $K \in \{\mathbb{Q}(i), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-7})\}$ and we justify this restriction to the reader.

One reason is that we had to carry out some explicit computations in the cohomology groups of locally symmetric spaces (see Section 2) that were much simpler when the field had class number 1.

To carry out our argument and prove that there are no solutions to Fermat's equation, we had to prove that Galois representations associated to Frey curves are absolutely irreducible. In doing so, we made use of the fact that K has primes of residual degree 1 above 2 so we end up with the three number fields above. On top of that, one should be aware of the existence of solutions $1^p + (\omega)^p + (\omega^2)^p = 0$, where ω is a primitive third root of unity and p is an odd prime. These are defined over $\mathbb{Q}(\sqrt{-3})$, making a proof of Fermat's Last Theorem over $\mathbb{Q}(\sqrt{-3})$ hopeless.

Theorem 3.1.1. *Assume Conjecture 2.2.1 holds for K. If $p \geq 5$ is a rational prime number, then the equation*

$$a^p + b^p + c^p = 0 \tag{3.1.1}$$

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

We proved statements similar to Theorem 3.1.1 for the other imaginary quadratic fields of class number one, but in those cases at the moment we are just able to prove that there are no solutions to (3.1.1) such that $Norm(abc)$ is even. These are included in Section 6 of the present chapter. We also hope to extend the methods to prove analogous results for other quadratic imaginary fields of non-trivial class number in the spirit of [19].

Corollary 3.1.2. *Assume Conjecture 2.2.1 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 $a, b, c \in \mathbb{Q}(i) \setminus \{0\}$.

The reader might legitimately ask themselves why we were only able to derive this corollary for the case $K = \mathbb{Q}(i)$. Let us try to explain this now. In fact, our techniques prove the result claimed in Theorem 3.1.1 for $p \geq 19$ when $K \in \{\mathbb{Q}(i), \mathbb{Q}(\sqrt{-2})\}$ and $p \geq 17$ when $K = \mathbb{Q}(\sqrt{-7})$ and we rely on previous work on Fermat's Last Theorem over number fields to conclude the same result for small values of p. To be precise, a result of Gross and Rohrlich [23, Theorem 5.1] implies that there are no solutions to (3.1.1) for $p = 5, 7, 11$ and our three choices of K. The case $p = 13$ is covered completely by work of Tzermias [58].

Hao and Parry [27] also worked on Fermat's equation over quadratic fields and one of their results [27, Theorem 4] can be used to complete the remaining cases $p = 17$ and $K \in \{\mathbb{Q}(i), \mathbb{Q}(\sqrt{-2})\}$ of our Theorem 3.1.1. All these works do not depend on the aforementioned conjecture of Serre.

It is worth pointing out that if one knows that none of the equations $a^p + b^p + c^p = 0$ for $p \geq 3$ prime and $a^4 + b^4 = c^4$ have a solution in $(a, b, c) \in (K \setminus \{0\})^3$, then one can deduce results analogous to Corollary 3.1.2 for K. In fact that is how the corollary is proved.

The equation $a^3 + b^3 + c^3 = 0$ describes a curve of genus 1 and can be seen as an elliptic curve over K after a choice of base-point. This elliptic curve has Mordell-Weil group isomorphic to $\mathbb{Z}/3\mathbb{Z}$ when $K \in \{\mathbb{Q}(i), \mathbb{Q}(\sqrt{-7})\}$. The torsion points correspond to the trivial solutions (i.e. one of a, b, c is 0) to Fermat's equation under reparameterization. The situation is a little bit different when $K = \mathbb{Q}(\sqrt{-2})$, because the elliptic curve in play has rank 1 and the non-torsion points on this curve correspond to infinitely many solutions $(a, b, c) \in \left(\mathbb{Q}(\sqrt{-2}) \setminus \{0\}\right)^3$ to $a^3 + b^3 + c^3 = 0$. All the computations here have been carried with the elliptic curve packages available in Magma [4]. For the equation $a^4 + b^4 = c^4$, we are going to refer to the work of Aigner [1] who proved that the only non-trivial solutions to this equation over quadratic imaginary fields are defined over $\mathbb{Q}(\sqrt{-7})$. Note that $(1 + \sqrt{-7})^4 + (1 - \sqrt{-7})^4 = 2^4$ is one of them. One can see now how the above discussion together with Theorem 3.1.1 imply the corollary and also why such a corollary cannot be achieved for any of the other two fields that are covered in the theorem.

3.2 Fermat equation with exponent p and the Frey Curve

Let us fix some notation:

p - a rational prime number;

K is one of $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-7})$;
$\mathcal{O}_K$ - the ring of integers of K;
S - set of prime ideals of $\mathcal{O}_K$ that lie above the prime 2.

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

$$a^p + b^p + c^p = 0, \qquad a, b, c \in \mathcal{O}_K. \tag{3.2.1}$$

We say that a solution $(a, b, c) \in \mathcal{O}_K^3$ is trivial if $abc = 0$ and non-trivial otherwise. We shall henceforth assume that $p \geq 17$. Note that any solution (a, b, c) of (3.1.1) satisfying $abc \neq 0$ can be scaled such that a, b, c become integral and the triple gives a non-trivial solution to (3.2.1).

The rational prime 2 is ramified in the first choices of K and completely split in $\mathbb{Q}(\sqrt{-7})$. In particular, the residue field of the primes in S is always $\mathbb{F}_2$, and this is essential in our argument. Let $(a, b, c) \in \mathcal{O}_K^3$ be a non-trivial solution to the Fermat equation (3.2.1). Since the class number of K is 1, we can scale the solution such that a, b and c are coprime. Associated to (a, b, c) is the Frey curve

$$E = E_{a,b,c} : Y^2 = X(X - a^p)(X + b^p). \tag{3.2.2}$$

We will make use of the following lemma.

Lemma 3.2.1 ([19, Lemma 4.2])**.** *Suppose that K is a quadratic field and $\mathfrak{a}$ is a prime ideal of K that lies above 2. Let $(a, b, c) \in \mathcal{O}_K$ be a non-trivial solution of (3.2.1) with $p \geq 17$ such that a, b, c are coprime. The Frey curve E has potentially multiplicative reduction at $\mathfrak{a}$ if and only if*

(a) either 2 splits or ramifies in K,

(b) or 2 is inert in K and $\mathfrak{a} \mid abc$.

Moreover, if the reduction at $\mathfrak{a}$ is multiplicative, then $p \nmid v_{\mathfrak{a}}(\Delta_{\mathfrak{a}})$. Here $\Delta_{\mathfrak{a}}$ is the discriminant of a local minimal model for E.

Proof. Suppose (a) or (b) holds. We claim that $\mathfrak{a} \mid abc$. If (b) holds, this is true by hypothesis. If (a) holds, then the residue field at $\mathfrak{a}$ is $\mathbb{F}_2$. It follows since $a^p + b^p + c^p = 0$ that $\mathfrak{a}$ divides at least one of a, b, c. Moreover, as a, b, c are assumed to be coprime, it follows that $\mathfrak{a}$ divides precisely one of a, b, c. Let $t = v_{\mathfrak{a}}(abc) \geq 1$. From the well known identities, we see that

$$v_{\mathfrak{a}}(c_4) = v_{\mathfrak{a}}\left(2^4(b^{2p} - a^p c^p)\right) = 4v_{\mathfrak{a}}(2) \text{ and } v_{\mathfrak{a}}(\Delta) = v_{\mathfrak{a}}\left(2^4(abc)^{2p}\right) = 4v_{\mathfrak{a}}(2) + 2pt.$$

This implies that

$$v_{\mathfrak{a}}(j) = 8v_{\mathfrak{a}}(2) - 2pt < 0$$

as $p \geq 17$. Thus we have potentially multiplicative reduction at $\mathfrak{a}$.

We are proving the converse by contradiction. Assume that none of (a) and (b) holds. It follows that $2\mathcal{O}_K = \mathfrak{a}$ is inert in K and $\mathfrak{a} \nmid abc$. From the formula $j = c_4^3/\Delta$ we can see that

$$v_{\mathfrak{a}}(j) = v_{\mathfrak{a}}\left(2^8 \cdot \frac{\left(b^{2p} - a^p c^p\right)^3}{(abc)^{2p}}\right) = 8 + 3v_{\mathfrak{a}}(b^{2p} - a^p c^p) \geq 8,$$

so E has potentially good reduction at $\mathfrak{a}$.

To complete the proof suppose that the reduction is multiplicative, and let c_4' and $\Delta' = \Delta_{\mathfrak{a}}$ be the corresponding invariants of a local minimal model. We know that $\mathfrak{a} \mid \Delta'$ and $\mathfrak{a} \nmid c_4'$. The j invariant does not change with the model, so $p \nmid v_{\mathfrak{a}}(j) = v_{\mathfrak{a}}(j') = 3v_{\mathfrak{a}}(c_4') - v_{\mathfrak{a}}(\Delta') = -v_{\mathfrak{a}}(\Delta')$. □

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

$$\overline{\rho}_{E,p} : G_K \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$$

induced by the action of G_K on the p-torsion of E. For our fields K all the primes above 2 have residue field $\mathbb{F}_2$, the lemma above implies that E has potentially multiplicative reduction at $\mathfrak{a} \in S$. Moreover, as $p \nmid v_{\mathfrak{a}}(j(E))$, Lemma 3.7 of [20] implies that that $p \mid \#\overline{\rho}(I_{\mathfrak{a}})$, where $I_{\mathfrak{a}}$ denotes the inertia subgroup of G_K at $\mathfrak{a}$. This information is crucial for everything that follows.

The following is a particular case of [46, Lemma 5.4]. Since it is central to our discussion, we include a proof here.

Lemma 3.2.2. *The Frey curve E is semistable away from S. The determinant of $\overline{\rho}$ is the mod p cyclotomic character. Its Serre conductor $\mathcal{N}$ is supported on S and belongs to a finite set that depends only on the field K. The representation $\overline{\rho}$ is finite flat at every prime $\mathfrak{p}$ of K that lies above p.*

Proof. Let c_4 and Δ denote the usual invariants of the model E given in (3.2.2). These are given by the formulae

$$c_4 = 2^4(b^{2p} - a^p c^p) \text{ and } \Delta = 2^4(abc)^{2p}.$$

If a prime ideal $\mathfrak{q}$ of $\mathcal{O}_K$ divides both c_4 and Δ, the equations above together with $a^p + b^p + c^p = 0$ imply that $\mathfrak{q}$ divides 2, so $\mathfrak{q} \in S$.

Let $\mathfrak{q} \notin S$ be a prime of $\mathcal{O}_K$. By well-known results [51, Section VII], one deduces that the model (3.2.2) for E is minimal and the curve is semistable at $\mathfrak{q}$.

Moreover, $p \mid v_{\mathfrak{q}}(\Delta)$. It follows from [47] that $\overline{\rho}$ is finite flat at $\mathfrak{q}$ if $\mathfrak{q}$ lies above p. From the results in the same article, we can deduce that $\overline{\rho}$ is unramified at $\mathfrak{q}$ if $\mathfrak{q} \nmid p$. Since the Serre conductor $\mathcal{N}$ is by definition not supported on primes above p, we get that it is actually supported only on the primes in S. We also know that $\mathcal{N}$ divides the conductor of E, therefore we can bound the exponent of $\mathfrak{q}$ in $\mathcal{N}$ using [52, Theorem IV.10.4]. We get

$$v_{\mathfrak{q}}(\mathcal{N}) \leq 2 + 3v_{\mathfrak{q}}(3) + 6v_{\mathfrak{q}}(2) = 2 + 6v_{\mathfrak{q}}(2),$$

for all $\mathfrak{q} \in S$.

The statement concerning the determinant is a well known consequence of the theory of the Weil pairing. □

Let N_E be the conductor of E. We will make use of the following two lemmata proved in [19] to control the exponent of primes above 2 in the conductor N_E. Despite the fact that the results of [19] are stated for real quadratic fields, the arguments of these lemmas are purely local and they continue to apply in our setting.

The local conductor of an elliptic curve with potential multiplicative reduction can be explicitly computed from the discriminant of a quadratic extension of the base field as we describe below.

Lemma 3.2.3 ([19, Lemma 4.3])**.** *Let $K_{\mathfrak{P}}$ be a non-Archimedean local field and C an elliptic curve over $K_{\mathfrak{P}}$ with potentially multiplicative reduction. Let c_4, c_6 be the usual c-invariants of C. Let $L = K_{\mathfrak{P}}\left(\sqrt{-c_6/c_4}\right)$ and let $\Delta(L/K_{\mathfrak{P}})$ be the discriminant of this local extension. Then the conductor of C over $K_{\mathfrak{P}}$ is*

$$f(C/K_{\mathfrak{P}}) = \begin{cases} 1 & \text{if } v_{\mathfrak{P}}\left(\Delta(L/K_{\mathfrak{P}})\right) = 0, \\ 2v_{\mathfrak{P}}\left(\Delta(L/K_{\mathfrak{P}})\right) & \text{otherwise.} \end{cases}$$

Proof. The quadratic twist E' by $-c_6/c_4$ is isomorphic to E over L. From [52, Section V.5] it follows that E' is a Tate curve, hence the conductor of E' over $K_{\mathfrak{P}}$ is equal to 1. The stated formula follows from the main result in [42, Section 18]. □

Lemma 3.2.4 ([19, Lemma 4.4])**.** *Let $(a, b, c) \in \mathcal{O}_K^3$ be a nontrivial solution to the Fermat equation* (3.2.1) *such that a, b, c are coprime. Suppose that 2 is either split*

or ramified in K, or that 2 is inert and $2 \mid abc$. Let

$$\mathfrak{b} = \prod_{\substack{\mathfrak{a} \mid 2\mathcal{O}_K \\ \mathfrak{a} \text{ prime}}} \mathfrak{a}^{2v_{\mathfrak{a}}(2)+1},$$

and write

$$\Phi : \mathcal{O}_K^* \to (\mathcal{O}_K/\mathfrak{b})^* / \left((\mathcal{O}_K/\mathfrak{b})^*\right)^2$$

for the natural map. Choose a set $\lambda_1, \ldots, \lambda_k \in \mathcal{O}_K \setminus \mathfrak{b}$ that represents the elements of the cokernel of Φ. For $1 \leq i \leq k$, and for $\mathfrak{a}$ a prime of K that lies above 2, let $\Delta_{\mathfrak{a}}^{(i)}$ be the discriminant of the local extension $K_{\mathfrak{a}}(\sqrt{\lambda_i})/K_{\mathfrak{a}}$, and let

$$\epsilon_{\mathfrak{a}}^{(i)} = \begin{cases} 1 & \text{if } v_{\mathfrak{a}}(\Delta_{\mathfrak{a}}^{(i)}) = 0, \\ 2v_{\mathfrak{a}}(\Delta_{\mathfrak{a}}^{(i)}) & \text{otherwise.} \end{cases}$$

Then we may scale the triple (a, b, c) by an element of $\mathcal{O}_K^*$ so that for some i and for every prime $\mathfrak{a}$ of K that lies above 2, we have $v_{\mathfrak{a}}(N_E) = \epsilon_{\mathfrak{a}}^{(i)}$.

Proof. Let $\mathfrak{a}$ be any prime ideal of K that lies above 2. From Lemma 3.2.1 above we know that the conditions in the hypothesis imply that $\mathfrak{a}$ divides exactly one of a, b, c and E has potentially multiplicative reduction at $\mathfrak{a}$. As $c_4 = 2^4(b^{2p} - a^p c^p)$ and $c_6 = -2^5(a^p - b^p)(b^p - c^p)(c^p - a^p)$ we obtain that $v_{\mathfrak{a}}(c_4) = 4v_{\mathfrak{a}}(2)$ and that $v_{\mathfrak{a}}(c_6) = 6v_{\mathfrak{a}}(2)$. Therefore, the constant $\gamma = -c_6/4c_4$ is a $\mathfrak{a}$-adic unit and $K_{\mathfrak{a}}(\sqrt{\gamma}) = K_{\mathfrak{a}}(\sqrt{-c_4/c_6})$ for all such $\mathfrak{a}$.

From the Chinese remainder theorem and Hensel's lemma, it follows that

$$(\mathcal{O}_K/\mathfrak{b})^* / \left((\mathcal{O}_K/\mathfrak{b})^*\right)^2 \cong \prod_{\substack{\mathfrak{a} \mid 2\mathcal{O}_K \\ \mathfrak{a} \text{ prime}}} \mathcal{O}_{\mathfrak{a}}^* / (\mathcal{O}_{\mathfrak{a}}^*)^2.$$

Notice that scaling the triple (a, b, c) by a unit η has the effect of scaling γ with η^p. As p is odd, it follows from the definition of the map Φ and the isomorphism described above that we can scale (a, b, c) by a unit such that there is some $1 \leq i \leq k$ with γ/λ_i a square in $\mathcal{O}_{\mathfrak{a}}^*$ for each $\mathfrak{a}$ prime of $\mathcal{O}_K$ that lies above 2.

As a result, for each such prime $\mathfrak{a}$, $K_{\mathfrak{a}}(\sqrt{\gamma}) = K_{\mathfrak{a}}(\sqrt{\lambda_i})$. Now the result follows from Lemma 3.2.3 above. □

Remark. In the same paper, the authors remark that if $u \in \mathcal{O}_K^*$ is any unit, and $\lambda \in \mathcal{O}_K \setminus \mathfrak{b}$, then for every integer k, the same element in the cokernel of Φ is represented by $\lambda' = \pm u^k \lambda$. The local extension $K_{\mathfrak{a}}(\sqrt{\lambda'})/K_{\mathfrak{a}}$ depends only on the choice of $\pm$ and the parity of k, therefore for computational purposes it is good

to choose whichever element among $\lambda, -\lambda, u\lambda, -u\lambda$ minimises the norm of the level N_E.

We describe this process in details for $K = \mathbb{Q}(i)$ remarking that the computation is analogous for the other two number fields. Following the notation in [19], one can compute values of $\lambda_i \in \mathcal{O}_K \setminus \mathfrak{b}$, which are some cokernel representatives of the map $\Phi : \mathcal{O}_K^* \to (O_K/\mathfrak{b})^* / \left((\mathcal{O}_K/\mathfrak{b})^*\right)^2$.

When $K = \mathbb{Q}(i)$, let $2\mathcal{O}_K = \mathfrak{a}^2$. In the notation of [19], this gives $\mathfrak{b} = \mathfrak{a}^5$, an ideal of norm 32. The image of $\Phi : \mathcal{O}_K^* \to (O_K/\mathfrak{b})^* / \left((\mathcal{O}_K/\mathfrak{b})^*\right)^2$ has order 2 and the codomain $(O_K/\mathfrak{b})^* / \left((\mathcal{O}_K/\mathfrak{b})^*\right)^2$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$. One can take as representatives of the cokernel of Φ the elements $\lambda_1 = 1$, $\lambda_2 = 2 + i$, $\lambda_3 = -3$ and $\lambda_4 = -2 + i$ in $\mathcal{O}_K$. This gives $\max\limits_{1 \leq i \leq 4} v_{\mathfrak{a}}(\Delta(K_{\mathfrak{a}}(\sqrt{\lambda_i})/K_{\mathfrak{a}})) = 4$. Even though one could do all the above computations using pen and paper only, the author made use of basic features of Magma at some steps.

After performing analogous computations in $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-7})$, one can see that a consequence of Lemma 4.4 in loc. cit. is the following. We can scale the triple (a, b, c) by a unit in $\mathcal{O}_K^*$ such that we find ourselves in one of the cases listed in Table 3.1.

Table 3.1: Exponent conductor of E at $\mathfrak{a}$

Number field K	**Factorization of** $2\mathcal{O}_K$	**Valuation of** N_E
$\mathbb{Q}(i)$	$2\mathcal{O}_K = \mathfrak{a}^2$	$v_{\mathfrak{a}}(N_E) = 8$
$\mathbb{Q}(\sqrt{-2})$	$2\mathcal{O}_K = \mathfrak{a}^2$	$v_{\mathfrak{a}}(N_E) = 8$
$\mathbb{Q}(\sqrt{-7})$	$2\mathcal{O}_K = \mathfrak{a}_1 \cdot \mathfrak{a}_2$, $\mathfrak{a}_1 \neq \mathfrak{a}_2$	$v_{\mathfrak{a}_1}(N_E) = 4$ and $v_{\mathfrak{a}_2}(N_E) = 1$
		$v_{\mathfrak{a}_1}(N_E) = 1$ and $v_{\mathfrak{a}_2}(N_E) = 4$

3.3 Local computations and irreducibility of $\overline{\rho}$

For applying Conjecture 2.2.1 to the Galois representation $\overline{\rho} = \overline{\rho}_{E,p}$, we have to prove that it is absolutely irreducible. We first prove irreducibility and the stronger condition will follow.

The conductor exponent of an elliptic curve is defined (see [52, Chapter IV]) as the sum between a tame and a wild part. Similarly, the conductor exponent of a Galois representation can be written as the sum between a tame and a wild part. In the following lemma, we think of a mod p character as a 1 dimensional representation over $\mathbb{F}_p$ and we define the wild part of its conductor exponent accordingly.

Lemma 3.3.1. *Let E be an elliptic curve of conductor $\mathcal{N}$ defined over a number*

field K and p a rational prime. Suppose $\overline{\rho}_{E,p}$ is reducible, that is,

$$\overline{\rho}_{E,p} \sim \begin{pmatrix} \theta & \star \\ 0 & \theta' \end{pmatrix} \text{ with } \theta, \theta' : G_K \to \mathbb{F}_p^* \text{ satisfying } \theta\theta' = \chi_p,$$

where χ_p is the mod p cyclotomic character. Let $\mathfrak{q} \nmid p$ be a prime in K of additive reduction for E. Then $\delta_{\mathfrak{q}}(\mathcal{N})$ is even and

$$\delta_{\mathfrak{q}}(\theta) = \delta_{\mathfrak{q}}(\theta') = \frac{\delta_{\mathfrak{q}}(\mathcal{N})}{2},$$

where $\delta_{\mathfrak{q}}(\theta)$, $\delta_{\mathfrak{q}}(\theta')$ and $\delta_{\mathfrak{q}}(N)$ are the wild parts of the exponent at $\mathfrak{q}$ in the conductors of θ, θ' and E.

Proof. The first equality follows from the fact that $\theta\theta' = \chi_p$, therefore when restricted to the absolute inertia group $I_{\mathfrak{q}}$, the characters are inverses of each other.

In what follows, we are going to think of θ and θ' as one dimensional representations from G_K targeting the one dimensional subspaces of $E[p]$ on which we see their actions.

Denote by $K_{\mathfrak{q}}$ the completion of the number field K at the prime $\mathfrak{q}$ and by $L = K_{\mathfrak{q}}(E[p])$ the extension of $K_{\mathfrak{q}}$ that we get by adjoining the coordinates of the p-torsion of E. The restriction $\overline{\rho}|_{\mathrm{Gal}(\overline{K_{\mathfrak{q}}}/K_{\mathfrak{q}})}$ factors through $\mathrm{Gal}(L/K_{\mathfrak{q}})$.

As one can see in [52, chapter IV], the wild part of the exponent of $\mathcal{N}$ at $\mathfrak{q}$ can be computed as

$$\sum_{i \geq 1} \frac{g_i(L/K_{\mathfrak{q}})}{g_0(L/K_{\mathfrak{q}})} \cdot \dim_{\mathbb{F}_p} \left(E[p]/E[p]^{G_i(L/K_{\mathfrak{q}})} \right),$$

where $G_0(L/K)$ is the inertia group and $G_i(L/K_{\mathfrak{q}})$ the i-th ramification group of $L/K_{\mathfrak{q}}$. The quantities $g_0(L/K_{\mathfrak{q}})$ and $g_i(L/K_{\mathfrak{q}})$ are the orders of the aforementioned groups.

It is known that $G_1(L/K_{\mathfrak{q}})$ is a Sylow group of order coprime to p, which implies that when restricted to the wild inertia $G_1(L/K_{\mathfrak{q}})$, the representation $\overline{\rho}$ becomes

$$\overline{\rho}|_{G_1(L/K_{\mathfrak{q}})} \sim \begin{pmatrix} \theta & 0 \\ 0 & \theta' \end{pmatrix}.$$

In fact, since $\mathfrak{q} \nmid p$, the cyclotomic character $\chi_p = \theta\theta'$ is trivial on $G_0(L/K_{\mathfrak{q}})$, we see that

$$\overline{\rho}|_{G_1(L/K_{\mathfrak{q}})} \sim \begin{pmatrix} \theta & 0 \\ 0 & \theta^{-1} \end{pmatrix}.$$

When restricted to $G_1(L/K_\mathfrak{q})$, let V_1 be the subspace of $E[p]$ on which θ acts and V_2 the subspace of $E[p]$ on which we see the action of θ'. One can see that $E[p]/E[p]^{G_i(L/K_\mathfrak{q})} \equiv V_1/V_1^{G_i(L/K_\mathfrak{q})} \oplus V_2/V_2^{G_i(L/K_\mathfrak{q})}$ and $\dim_{\mathbb{F}_p} V_1/V_1^{G_i(L/K_\mathfrak{q})} = \dim_{\mathbb{F}_p} V_2/V_2^{G_i(L/K_\mathfrak{q})}$ for all $i \geq 1$.

If we think of θ as a 1 dimensional representation from $\mathrm{Gal}(K(E[p])/K) \to V_1$, then the definition of the wild part of its conductor at $\mathfrak{q}$ is

$$\delta_\mathfrak{q}(\theta) = \sum_{i \geq 1} \dim_{\mathbb{F}_p} \left(V_1/V_1^{G_i(F/K)} \right),$$

where V_1 is the subspace of $E[p]$ on which $\overline{\rho}|_{G_1(F/K)}$ acts as θ. Using the analogous formula for $\delta_\mathfrak{q}(\theta')$, the conclusion follows.

□

Theorem 3.3.2. *Let $p \geq 19$ if $K \in \{\mathbb{Q}(i), \mathbb{Q}(\sqrt{-2})\}$ and $p \geq 17$ if $K = \mathbb{Q}(\sqrt{-7})$. Then $\overline{\rho}$ is irreducible.*

Proof. If $\overline{\rho}_{E,p}$ is reducible, then we can write

$$\overline{\rho}_{E,p} \sim \begin{pmatrix} \theta & * \\ 0 & \theta' \end{pmatrix},$$

where θ and θ' are characters $G_K \to \mathbb{F}_p^*$, 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.

From the proof of Lemma 1 in [35] we know that θ, θ' are unramified away from p and the primes of additive reduction of E, i.e. the primes above 2 in $\mathcal{O}_K$. Using the notation introduced in Lemma 3.3.1, we have that

$$\delta_\mathfrak{a}(\mathcal{N}_\theta) = \delta_\mathfrak{a}(\mathcal{N}_{\theta'}) = \frac{1}{2}\delta_\mathfrak{a}(N_E),$$

where $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$ above 2.

The tame part of the exponent of a prime in the conductor of a character is at most 1 and must be equal 1 if the wild part is non-zero. On the other hand, the corresponding quantity in the conductor of an elliptic curve is at most 2 and must be equal to 2 if its wild part is non-zero. For the precise definitions, see [52, Chapter IV].

(i) Suppose p is coprime to $\mathcal{N}_\theta$ or $\mathcal{N}_{\theta'}$. Since the conductor of an elliptic curve is isogeny invariant, by replacing E with the p-isogenous curve $E/\langle\theta\rangle$ we can assume that p is coprime to $\mathcal{N}_\theta$ and hence deduce that θ is unramified away from the primes in S.

For $K = \mathbb{Q}(\sqrt{-7})$, denote by $\mathfrak{a}_1, \mathfrak{a}_2$ the prime ideals of K above 2. From the table above, we see that

$$\mathcal{N}_\theta \in \{\mathfrak{a}_1^2, \mathfrak{a}_2^2\}.$$

Therefore, θ is a character of the ray class group of modulus $\mathfrak{a}_1^2$ or $\mathfrak{a}_2^2$. Both of these ray class groups are trivial, which implies that θ has order 1 and hence that E has a point of order p defined over K. Our assumption $p \geq 17$ contradicts the results of Theorem 3.1 in [33] which implies the order of such a torsion point is less than or equal to 13.

We treat the cases $K = \mathbb{Q}(i), \mathbb{Q}(\sqrt{-2})$ together. Here we assumed that $p \geq 19$. Using the values computed in the previous table and Lemma 3.3.1, we see that the only possibility for the conductor of θ is

$$\mathcal{N}_\theta = \mathfrak{a}^4,$$

where $\mathfrak{a}$ is the unique prime above 2 in $\mathcal{O}_K$. The ray class groups for these fields and modulus are $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$ respectively. These computations were done using Magma.

In turn, for $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-2})$, θ is a character of that corresponding ray class group, therefore the order of θ divides the exponent of the group. If θ has order 1 then E has a point of order p over K and we get a contradiction exactly as before. Similarly, if the order of θ is 2 then E has a p-torsion point defined over a quadratic extension L of K. But $[L : \mathbb{Q}] = [L : K] \cdot [K : \mathbb{Q}] = 4$ and the possible prime torsion of elliptic curves over quartic fields determined by Derickx, Kamienny Stein and Stoll [14] would imply that $p \leq 17$, a contradiction.

If θ has order 4, then let L be the quadratic extension of K that is cut by the character θ^2. The restriction $\phi = \theta|_{G_L}$ is a quadratic character of G_L and therefore the twist by ϕ of E, regarded as an elliptic curve over L, is an elliptic curve with a p-torsion point defined over L. The field L is of total degree 4 over $\mathbb{Q}$ and hence we get a contradiction as in the other case.

(ii) Suppose now that p is not coprime with $\mathcal{N}_\theta$ nor with $\mathcal{N}_{\theta'}$. Since $p \geq 19$, we know that p is not ramified in K. If we suppose that p is inert in K, then from [35, Lemme 1] it follows that p divides only one of the conductors, a contradiction with the hypothesis.

The only case that has to be considered now is when p splits in K. Let $\mathfrak{p}_1, \mathfrak{p}_2$ be the two ideals of $\mathcal{O}_K$ such that $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$. We can suppose that $\mathfrak{p}_1 | \mathcal{N}_\theta$, $\mathfrak{p}_1 \nmid \mathcal{N}_{\theta'}$ and $\mathfrak{p}_2 | \mathcal{N}_{\theta'}$, $\mathfrak{p}_2 \nmid \mathcal{N}_\theta$. The primes $\mathfrak{p}_1$, $\mathfrak{p}_2$ are unramified so it follows from [48, Proposition 12] that E has good ordinary or multiplicative reduction at these

primes and $\theta|_{I_{\mathfrak{p}_1}} = \chi_p|_{I_{\mathfrak{p}_1}}$ and $\theta'|_{I_{\mathfrak{p}_2}} = \chi_p|_{I_{\mathfrak{p}_2}}$.

The character θ^2 is unramified everywhere except $\mathfrak{p}_1$, because all the bad places for E are of potentially multiplicative reduction. We also know that $\theta^2|_{I_{\mathfrak{p}_1}} = \chi_p^2|_{I_{\mathfrak{p}_1}}$.

From Lemma 3.3.3 below, it follows that

$$\theta^2(\sigma_{\mathfrak{a}}) \equiv N_{K_{\mathfrak{p}_1}/\mathbb{Q}_p}(\iota_{\mathfrak{p}_1}(\mathfrak{a}))^2 \pmod{p},$$

where $\mathfrak{a}$ is a prime ideal of $\mathcal{O}_K$ that lies above 2 (principal, of course) and $\sigma_{\mathfrak{a}}$ is the Frobenius element at $\mathfrak{a}$.

As explained in [46, Lemma 6.3], by replacing E with the p-isogenous curve $E/\langle\theta\rangle$ we can assume that $\theta^2(\sigma_{\mathfrak{a}}) \equiv 1 \pmod{p}$. We have that

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

so $p \mid 3$ which gives a contradiction.

□

We have used above the following class field theory lemma. We do not include a proof here since that would be *mutatis mutandis*, just a specialisation of [13, Proposition 2.4].

Lemma 3.3.3. *Let $(p) = \mathfrak{p}_1\mathfrak{p}_2$ be a rational prime that splits in K and let $\theta : G_K \to \mathbb{F}_p^*$, be a character with the property that θ^2 is unramified everywhere except $\mathfrak{p}_1$. Then, for any prime to p element $0 \neq \alpha \in K$, the following congruence relation holds*

$$\prod_{\mathfrak{q}\nmid p} \theta^2(\sigma_{\mathfrak{q}})^{v_{\mathfrak{q}}(\alpha)} \equiv N_{K_{\mathfrak{p}_1}/\mathbb{Q}_p}(\iota_{\mathfrak{p}_1}(\alpha))^2 \pmod{p}.$$

Remark 3.3.4. For every place v, the map ι_v is the inclusion of K into the completion K_v. Abusing notation we write $i_{\mathfrak{q}}$ and $K_{\mathfrak{q}}$ for the inclusion, respectively the completion of K, with respect to the corresponding prime ideal $\mathfrak{q}$.

We obtain the following corollary, which implies absolute irreducibility.

Corollary 3.3.5. *For $p \geq 19$, the Galois representation $\overline{\rho}$ is surjective.*

Proof. In the proof of [20, Lemma 3.7], the authors used that $v_{\mathfrak{a}}(j(E)) < 0$ and $p \nmid v_{\mathfrak{a}}(j(E))$ to deduce that E has multiplicative reduction at $\mathfrak{a} \in S$ and that the cardinality of $\overline{\rho}(I_{\mathfrak{a}})$ is also divisible by p, where $I_{\mathfrak{a}}$ is the inertia subgroup at $\mathfrak{a}$. Since all the irreducible subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ that contain an element of order p have $\mathrm{SL}_2(\mathbb{F}_p)$ as a subgroup, we get that $\mathrm{SL}_2(\mathbb{F}_p) \subseteq \overline{\rho}(G_K)$. The determinant of $\overline{\rho}$ is the

mod p cyclotomic character χ_p, and since $K \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$, the latter is surjective. All the above imply that $\overline{\rho}(G_K) = \mathrm{GL}_2(\mathbb{F}_p)$.

□

3.4 Applying Serre's conjecture

We are now making use of the Conjecture 2.2.1. This predicts the existence of a mod p eigenform $\Phi : \mathbb{T}_{\overline{\mathbb{F}}_p}(\mathcal{N}) \to \overline{\mathbb{F}}_p$ over K such that for every prime ideal $(\pi) \subset \mathcal{O}_K$, coprime to $p\mathcal{N}$.

$$\mathrm{Trace}\left(\overline{\rho}(\mathrm{Frob}_{(\pi)})\right) = \Phi(T_\pi),$$

where T_π is a Hecke operator.

The trace elements $\mathrm{Trace}\left(\overline{\rho}(\mathrm{Frob}_{(\pi)})\right)$ lie in $\mathbb{F}_p$, therefore Φ corresponds to a class in $H^1(Y_0(\mathcal{N}), \mathbb{F}_p)$ that is an eigenvector for all such Hecke operators T_π.

As previously described, the obstruction in lifting such mod p eigenforms to complex eigenforms is given by the presence of p-torsion in $H^2(Y_0(\mathcal{N}), \mathbb{Z}_{(p)})$. Let us remark that $H^2(Y_0(\mathcal{N}), \mathbb{Z}_{(p)})$ and $H^2(Y_0(\mathcal{N}), \mathbb{Z})$ have the same p-torsion. It is known (see for example [2, page 202]) that 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 other words $H^2(Y_0(\mathcal{N}), \mathbb{Z}[\frac{1}{6}]) \cong H^2(\Gamma_0(\mathcal{N}), \mathbb{Z}[\frac{1}{6}])$.

Lefschetz duality for cohomology with compact support [45, Section 2] gives a relation between the first homology and the second cohomology $H_1(\Gamma_0(\mathcal{N}), \mathbb{Z}\left[\frac{1}{6}\right]) \cong H^2(\Gamma_0(\mathcal{N}), \mathbb{Z}\left[\frac{1}{6}\right])$. 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.

Using the Magma implementation, kindly provided to us by Haluk Şengün, of his algorithm in [45] we computed the abelianizations $\Gamma_0(\mathcal{N})^{ab}$. This algorithm uses as input generators and relations for $\mathrm{GL}_2(\mathcal{O}_K)$ which were computed by Swan in [53]. Alternatively one could use an algorithm of Page [41] to compute presentations for $\mathrm{GL}_2(\mathcal{O}_K)$. The reader can consult the Magma code at:

`https://warwick.ac.uk/fac/sci/maths/people/staff/turcas/fermatprog`.

We list the torsion found in Table 3.2, where $\mathfrak{a}, \mathfrak{a}_1$ and $\mathfrak{a}_2$ are primes above 2 in the corresponding number fields.

Table 3.2: prime torsion in $\Gamma_0(\mathcal{N})^{ab}$

Number field	**Level $\mathcal{N}$**	**primes l such that $\Gamma_0(\mathcal{N})^{ab}[l] \neq 0$**
$\mathbb{Q}(i)$	$\mathfrak{a}^8$	2
$\mathbb{Q}(\sqrt{-2})$	$\mathfrak{a}^8$	2
$\mathbb{Q}(\sqrt{-7})$	$\mathfrak{a}_1^4\mathfrak{a}_2$	2,3
	$\mathfrak{a}_1\mathfrak{a}_2^4$	2,3

Since we have chosen $p \geq 19$ and there is no p-torsion in the subgroups of interest, the mod p eigenforms lift to complex ones. Using the available Magma package for Bianchi modular forms, we compute these spaces of eigenforms. The implementation, due to Dan Yasaki, is based on an algorithm of Gunnels [25] for computing the Voronoi polyhedron and provides a replacement for the modular symbol algorithm used by Cremona to compute the action of the Hecke operators in [9].

The dimension of the respective cuspidal spaces for $\mathbb{Q}(i), \mathbb{Q}(\sqrt{-7})$ is 0 and the dimension of the cuspidal space of level $\mathfrak{a}^8$ for $\mathbb{Q}(\sqrt{-2})$ is 6.

Since there are no eigenforms at the predicted levels for $K = \mathbb{Q}(i)$ or $K = \mathbb{Q}(\sqrt{-7})$, the proof of Theorem 3.1.1 in those cases is complete.

Let us now focus on $K = \mathbb{Q}(\sqrt{-2})$. As previously noted, the total dimension of the cuspidal space is 6, there are only 2 newforms at this level. On the levels $\mathfrak{a}^i$, $1 \leq i \leq 7$ there is only newform at level $\mathfrak{a}^5$, where $\mathfrak{a}$ is the only prime ideal above 2. All these forms have integer Hecke eigenvalues.

At the moment of writing the first version of this chapter LMFDB [38] did not include a database for Bianchi modular forms, so the author computed the eigenvalues independently using the available Magma packages. The results match perfectly with the ones that were since then made available in the LMFDB by John Cremona and Haluk Şengün.

We prove Theorem 3.1.1 here by first proving that these newforms correspond to elliptic curves.

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

If C/K doesn't have complex multiplication and in addition $L(C, s)$ together with its character twists have analytic continuation and satisfy the functional equation, then by results of [29] it follows that there exists a Bianchi modular form for $\Gamma_0(\mathcal{N})$, that is a newform, such that its Mellin transform is equal to $L(C, s)$.

We will make all of the above explicit for our curves. Looking in the LMFDB

database we found three elliptic curves that are good candidates for such a correspondence with our three newforms. By checking the traces of Frobenius at the first few primes, we notice that the curve

$$E_1 : y^2 = x^3 + x,$$

with $j(E_1) = 1728$ and LMFDB label 2.0.8.1-32.1-a2 should correspond to the newform at level $\mathfrak{a}^5$, i.e. the Bianchi modular form 2.0.8.1-32.1-a, if we want to stay in the language of the LMDFDB.

Similarly,

$$E_2 : y^2 = x^3 + x^2 + x + 1,$$

with $j(E_2) = 128$ and LMFDB label 2.0.8.1-256.1-a1 should correspond to the Bianchi modular form 256.1-a and

$$E_3 : y^2 = x^3 - x^2 + x - 1,$$

with $j(E_3) = 128$ and LMFDB label 2.0.8.1-256.1-b1, should correspond to the Bianchi modular form 256.1-b.

Since the curves E_1, E_2 and E_3 are base changes from elliptic curves defined over $\mathbb{Q}$, by the celebrated modularity theorem [5], we know that their L-functions have analytic continuation.

In this very fortunate situation, we can establish the desired connection between these curves defined over K and the Bianchi modular forms mentioned above. Instead of using the Faltings-Serre-Livné method [15], we are going to use the theory of lifting classical modular forms from $\mathbb{Q}$ to forms of imaginary quadratic fields with discriminant. A summary of the theory in this special case is given in [10, Section 4].

An aspect of this theory worth mentioning is the following. Suppose that f is a cuspidal modular form (in the classical sense) such that f does not have complex multiplication by K (i.e. $f \otimes \chi \neq f$, where χ is the quadratic character attached to $K/\mathbb{Q}$). Then, the lift F of f is a cusp form for K for $\Gamma_0(\mathfrak{N})$, where $\mathfrak{N}$ is an ideal of $\mathcal{O}_K$ supported only on the primes of K that divide D (the discriminant of the quadratic extension) and the level of the cusp form f we started with. If F is the lift of a newform f, then it is also the lift of $f \otimes \chi$ and of no other cuspidal newform over $\mathbb{Q}$.

In terms of L-series we have

$$L(F, s) = L(f, s)L(f \otimes \chi, s).$$

Lemma 3.4.1. *Let K be a quadratic imaginary field of discriminant $-D$ and χ the Dirichlet character associated to $K/\mathbb{Q}$. Suppose $f \in S_2(\Gamma_0(N_1))$ is a classical cuspidal newform of level $N_1 \in \mathbb{Z}_{\geq 1}$ such that $f \otimes \chi \in S_2(\Gamma_0(N_2))$ is a classical cupidal form of level $N_2 \in \mathbb{Z}_{\geq 1}$, $f \neq f \otimes \chi$. Then f and $f \otimes \chi$ lift to the same form F for K with level an ideal of norm $N_1 N_2 / D^2$.*

Proof. We only have to prove the statement about the norm of level of F and this is a relatively easy exercise which makes use of the functional equations.

The completed L functions $\Lambda(f,s) = (2\pi)^{-s} N_1^{s/2} \Gamma(s) L(f,s)$ and $\Lambda(f \otimes \chi, s) = (2\pi)^{-s} N_2^{s/2} \Gamma(s) L(f \otimes \chi, s)$ satisfy functional equations

$$\Lambda(f,s) = \pm \Lambda(f, 2-s) \text{ and } \Lambda(f \otimes \chi, s) = \pm \Lambda(f \otimes \chi, 2-s).$$

It is known (see, for example, page 414 of [10] or the discussion in [11]) that the Mellin transform of F,

$$\Lambda(F,s) = D^{s-1} (2\pi)^{-2s} \Gamma(s) L(F,s)$$

is an entire function of s with functional equation

$$\Lambda(F,s) = \pm N(\mathfrak{N})^{1-s} \Lambda(F,s), \tag{3.4.1}$$

where $\mathfrak{N} \subset \mathcal{O}_K$ is the level of the newform F.

One can see that

$$\Lambda(F,s) = D^{s-1} (N_1 N_2)^{-s/2} \Lambda(f,s) \Lambda(f \otimes \chi, s).$$

Now if we make the substitution $s \leftrightarrow 2-s$ and use the functional equations we get

$$\Lambda(F, 2-s) = \pm D^{1-s} (N_1 N_2)^{\frac{s-2}{2}} \Lambda(f,s) \Lambda(f \otimes \chi, s) \Leftrightarrow$$

$$\Lambda(F, 2-s) = \pm D^{1-s} (N_1 N_2)^{\frac{s-2}{2}} \cdot (N_1 N_2)^{s/2} D^{1-s} \Lambda(F,s).$$

Rearranging the terms, we get

$$\Lambda(F,s) = \pm \left[\left(\frac{N_1 N_2}{D^2} \right) \right]^{1-s} \Lambda(F, 2-s)$$

and comparing with (3.4.1) we finish the proof. □

We remark that when an elliptic curve E corresponds to a newform F, according to the modularity notion used in Conjecture 2.4.1, the L-functions of E and

F are the same.

The rational elliptic curve $E_1/\mathbb{Q}$ corresponds to the cuspidal modular form $f_1(z) = q - 2q^5 - 3q^9 + O(q^{10})$ of weight 2 and level 32 and coefficient field $\mathbb{Q}$.

If we let χ be the character associated to the quadratic imaginary extension $K/\mathbb{Q}$ and twist f_1 by this character, we get $f_1 \otimes \chi(z) = q + 2q^5 - 3q^9 + O(q^{10})$, a rational cuspidal modular form of the same weight. The level of $f_1 \otimes \chi$ is 64 and its L-function matches the one of the rational elliptic curve E_1^{χ} (the twist of E_1 by χ).

Using the previous lemma, we know that the holomorphic cusp forms f_1 and $f_1 \otimes \chi$ lift to K the same newform F_1 over K of level with norm 32. But there is just one ideal of norm 32 in $\mathcal{O}_K$, namely $\mathfrak{a}^5$. We computed that there is only one newform at this level, so this must be our F_1. Thus,

$$L(F_1, s) = L(f_1, s)L(f_1 \otimes \chi, s),$$

By definition,

$$L(E_1/K, s) = L(E_1, s) \cdot L(E_1^{\chi}, s),$$

therefore

$$L(E_1/K, s) = L(f_1, s) \cdot L(f_1 \otimes \chi, s) = L(F, s).$$

In exactly the same way, we prove that E_2 and E_3 correspond to newforms with level of norm 256. Therefore, the level of these newforms is $\mathfrak{a}^8$. There are 2 newforms at this level, and they have LMFDB label 2.0.8.1-256.1-a and 2.0.8.1-256.1-b. By looking at the first few Hecke eigenvalues, we observe that E_2 corresponds to the 1-a Bianchi modular form and E_3 corresponds to the other.

Definition 3.4.2. Given two elliptic curves E and E', defined over a number field K, and some rational prime number p, we write that $E \sim_p E'$ if their corresponding mod p Galois representations $\overline{\rho}_E, \overline{\rho}_{E'} : G_K \to \mathrm{GL}_2(\mathbb{F}_p)$ are isomorphic.

Denote by $\overline{\rho}_{E_i}$ the mod p Galois representations associated to E_i for all $1 \leq i \leq 3$. So far, we have used Conjecture 2.2.1 to prove that from $(a, b, c) \in \mathcal{O}_K$, a non-trivial solution to 3.2.1, one obtains an elliptic curve $E_{a,b,c}$. The mod p Galois representation of this curve has the property there exists $i \in \{1, 2, 3\}$ such that for almost all prime ideals $(\pi) \subseteq \mathcal{O}_K$, $\mathrm{Trace}\,\overline{\rho}_{E,a,b,c}(\mathrm{Frob}_{(\pi)}) = \mathrm{Trace}\,\overline{\rho}_{E_i}(\mathrm{Frob}_{(\pi)})$.

Since the Frobenius elements are dense and $\overline{\rho}_{E,a,b,c}$ is irreducible, the Brauer-Nesbitt theorem gives that $\overline{\rho}_{E,a,b,c}$ and $\overline{\rho}_{E_i}$ are isomorphic.

In order to finish the proof of Theorem 3.1.1, we have to eliminate all of the following possibilities

$$E = E_{a,b,c} \sim_p E_1, \tag{3.4.2}$$

$$E = E_{a,b,c} \sim_p E_2, \tag{3.4.3}$$

or that

$$E = E_{a,b,c} \sim_p E_3 \tag{3.4.4}$$

The huge advantage now is that the curves E_1, E_2 and E_3 do not depend on the exponent p nor on the unknown solution $(a, b, c) \in \mathcal{O}_K^3$ of (3.2.1).

It's very easy to see that (3.4.2) can't happen. This is because E_1 has complex multiplication and this imposes extra restrictions on its mod p representation $\overline{\rho}_{E_1}$. In particular, the latter is not surjective, but we proved that $\overline{\rho}_{E,a,b,c}$ is surjective.

Now we restrict our attention to (3.4.3) and (3.4.4). Notice that the ideal $(3)\mathcal{O}_K$ splits as $(3) = (\sqrt{-2}+1)(\sqrt{-2}-1)$. We denote by $\mathfrak{m}_1 = (\sqrt{-2}+1)$.

Suppose that $E = E_{a,b,c}$ has good reduction at $\mathfrak{m}_1$. The fact that E/K has full 2-torsion implies that $4|\#E(\mathcal{O}_K/\mathfrak{m}_1)$. The Hasse bounds $1 \leq \#E(\mathcal{O}_K/\mathfrak{m}_1) \leq 7$ imply that $\#E(\mathcal{O}_K/\mathfrak{m}_1) = 4$.

The curves E_2 and E_3 have good reduction at $\mathfrak{m}_1$ and $\#E_2(\mathcal{O}_K/\mathfrak{m}_1) = 6$ and $\#E_3(\mathcal{O}_K/\mathfrak{m}_1) = 2$. If (3.4.3) holds, then $p|\#E_2(\mathcal{O}_K/\mathfrak{m}_1) - \#E(\mathcal{O}_K/\mathfrak{m}_1) = 2$. Similarly, if (3.4.4) is true, then $p|\#E_3(\mathcal{O}_K/\mathfrak{m}_1) - \#E(\mathcal{O}_K/\mathfrak{m}_1) = -2$. Both lead us to contradictions with the size of the exponent p.

Suppose that E has multiplicative reduction at $\mathfrak{m}_1$. Looking at the traces of Frobenius, we get that

$$\begin{cases} (3.4.3) \Longrightarrow \pm(3+1) = 3+1-6 \pmod{p} \text{ and} \\ (3.4.4) \Longrightarrow \pm(3+1) = 3+1-2 \pmod{p} \end{cases}$$

both leading to contradictions to our assumption that $p \geq 19$.

Remark 3.4.3. If it would've been for the Bianchi newform F_1, which corresponds to the CM elliptic curve E_1, we could have finished the proof of our main theorem on the Bianchi side just by computing Hecke eigenvalues for Bianchi newforms. We take this path in the next section, where we treat Fermat's equation over the other quadratic imaginary fields of class number one.

3.5 Fermat's equation over other quadratic imaginary number fields

Throughout this section we are going to keep the notation introduced in the previous one and used so far, remarking that K is going to be one of $\{\mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-11}), \mathbb{Q}(\sqrt{-19}), \mathbb{Q}(\sqrt{-43}), \mathbb{Q}(\sqrt{-67})$ or $\mathbb{Q}(\sqrt{-163})\}$, the remaining quadratic imaginary

fields of class number 1. The prime 2 is inert in all these six fields.

Let p be a rational prime number and $a, b, c \in \mathcal{O}_K$ coprime such that the triple (a, b, c) is a non-trivial solution to the Fermat equation with exponent p defined in (3.2.1). Associated to this solution is the Frey curve described in (3.2.2):

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

Recall that we denoted by $\overline{\rho} = \overline{\rho}_{E,p}$ the residual Galois representation induced by the action of G_K on $E[p]$. Lemma 3.2.2 applies here as well and implies that:

- E is semistable away from $\mathfrak{a} = 2\mathcal{O}_K$, the only prime of K that lies above 2;
- $\overline{\rho}$ is finite flat at every prime $\mathfrak{p}$ of K that lies above p;
- the Serre conductor of $\overline{\rho}$ is a power of $\mathfrak{a}$ and belongs to a finite set;
- the determinant of $\overline{\rho}$ is the mod p cyclotomic character.

The same sequence of three lemmas 3.2.1, 3.2.3, 3.2.4 play a pivotal role for the task of getting control over the exponent of $\mathfrak{a} = 2\mathcal{O}_K$ in the conductor N_E of the Frey curve E. We already emphasized their utility while proving our results for the fields $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-7})$.

Recall that we are discussing Fermat's equation over K, where $K = \mathbb{Q}(\sqrt{-d})$ and $d = 3, 11, 19, 43, 67$ or 163. The prime 2 is inert in K. Let the coprime $(a, b, c) \in \mathcal{O}_K^3$ be a non-trivial solution to (3.2.1) such that $\mathfrak{a} = 2\mathcal{O}_K$ divides abc. We will apply Lemma 3.2.4 to the Frey curve E. Let us demystify the quantities introduced in the aforementioned lemma. The ideal $\mathfrak{b}$ is equal to $\mathfrak{a}^3$ 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 Φ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$. For every considered K, the image of Φ is isomorphic with $\mathbb{Z}/2\mathbb{Z}$ (including the case $K = \mathbb{Q}(\sqrt{-3})$ where $\mathcal{O}_K$ has extra units), so $\mathrm{Coker}(\Phi) \cong (\mathbb{Z}/2\mathbb{Z})^2$.

We present, for each d, a complete list of representatives of this cokernel and the maximal value for the exponent of $\mathfrak{a}$ in the local extensions mentioned above. As it can be seen in the table below, if $K = \mathbb{Q}(\sqrt{-d})$ is one of the aforementioned fields and $2 \mid abc$, 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 $\mathfrak{a} = 2\mathcal{O}_K$ is at most 4. For completeness, we mention that c.f. [19, Lemma 4.1] in the case $\mathfrak{a} = 2\mathcal{O}_K \nmid abc$, after suitably permuting (a, b, c) we have $v_{\mathfrak{a}}(N_E) = 4$.

For applying Conjecture 2.2.1 to the Galois representation $\overline{\rho} = \overline{\rho}_{E,p}$, we have to prove that it is absolutely irreducible.

Table 3.3: Computations associated to Lemma 3.2.4

d	**Reps.** $\lambda_1, \lambda_2, \lambda_3, \lambda_4 \in \mathcal{O}_K$ **of** $\mathrm{Coker}(\Phi)$	$\max_{i=\overline{1,4}} v_{\mathfrak{a}}(\Delta_{\mathfrak{a}}^{(i)}))$	$v_{\mathfrak{a}}(N_E)$
3	$1,\ \frac{-1+3\sqrt{-3}}{2},\ 3+2\sqrt{-3},\ \frac{3-\sqrt{-3}}{2}$	2	4
11	$1,\ \frac{-1+\sqrt{-11}}{2},\ -1+2\sqrt{-11},\ \frac{-5-3\sqrt{-11}}{2}$	2	4
19	$1,\ \frac{1+3\sqrt{-19}}{2},\ 3+2\sqrt{-19},\ \frac{9+3\sqrt{-19}}{2}$	2	4
43	$1,\ \frac{-7-\sqrt{-43}}{2},\ -1+2\sqrt{-43},\ \frac{-3+3\sqrt{-43}}{2}$	2	4
67	$1,\ \frac{1+3\sqrt{-67}}{2},\ 1+2\sqrt{-67},\ \frac{-9-3\sqrt{-67}}{2}$	2	4
163	$1,\ \frac{1+3\sqrt{-163}}{2},\ 1+2\sqrt{-163},\ \frac{-9-3\sqrt{-163}}{2}$	2	4

Proposition 3.5.1. *Let $p \geq 17$ and fix $K = \mathbb{Q}(\sqrt{-d})$, where d is one of* 3, 11, 19, 43, 67, *or* 163. *If $(a, b, c) \in \mathcal{O}_K^3$ with $2 \mid abc$ is a non-trivial solution to* (3.2.1) *that is scaled as in Table 3.3, then $\overline{\rho}_{E,p}$ is irreducible.*

Proof. If $\overline{\rho}_{E,p}$ is reducible, then we can write

$$\overline{\rho}_{E,p} \sim \begin{pmatrix} \theta & * \\ 0 & \theta' \end{pmatrix} \tag{3.5.1}$$

where θ and θ' are characters $G_K \to \mathbb{F}_p^*$ 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 $2\mathcal{O}_K = \mathfrak{a}$, the only prime of additive reduction for E (see [35, Lemma 1]).

We saw in Lemma 3.2.1 that $\mathfrak{a}$ is a prime of potentially multiplicative reduction for E. Write $D_{\mathfrak{a}} \subseteq G_K$ for the decomposition subgroup at $\mathfrak{a}$. The restriction $\overline{\rho}_{E,p}$ to $D_{\mathfrak{a}}$ is, up to semi-simplification, equal to $\phi \oplus \phi \cdot \chi_p$, where ϕ is at worst a quadratic character. In particular, both θ^2 and θ'^2 are unramified at $\mathfrak{a}$.

(i) We will first assume that p is coprime to either $\mathcal{N}_\theta$ or $\mathcal{N}_{\theta'}$. Since the conductor of an elliptic curve is isogeny invariant, by replacing E with the p-isogenous curve $E/\langle\theta\rangle$ we can assume that p is coprime to $\mathcal{N}_\theta$. This implies that θ is unramified away from $\mathfrak{a}$. 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 [33, Theorem 3.1] implies that $p \leq 13$, a contradiction.

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

We will first prove that under the assumption that $\overline{\rho}_{E,p}$ is reducible, the prime p does not ramify in K. Suppose it does, i.e. we are in one of the cases $p = d = 19, 43, 67$ or 163, and let $\mathfrak{p}$ be the unique prime ideal of $\mathcal{O}_K$ such that $p\mathcal{O}_K = \mathfrak{p}^2$. We see from [19, Proposition 6.1 (ii)] that if $\mathfrak{p}$ is a prime of good ordinary, or multiplicative reduction then

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

This would imply that the second diagonal character θ' 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 [19, Proposition 6.1.] asserts that either

$$\overline{\rho}_{E,p}|_{I_\mathfrak{p}} \sim \begin{pmatrix} \psi_2^2 & 0 \\ 0 & \psi_2^{2p} \end{pmatrix} \text{ or } \overline{\rho}_{E,p}|_{I_\mathfrak{p}} \sim \begin{pmatrix} \psi_1 & 0 \\ 0 & \psi_1 \end{pmatrix}, \tag{3.5.2}$$

where $\psi_1 : I_\mathfrak{p} \to \mathbb{F}_p^*$ and $\psi_2 : I_\mathfrak{p} \to \mathbb{F}_{p^2}^*$ are the level 1 and respectively 2 fundamental characters defined in [48]. The first possibility in (3.5.2) implies that $\theta|_{I_\mathfrak{p}} = \psi_2^2$, which is impossible since ψ_2^2 is 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 $2\mathcal{O}_K = \mathfrak{a}$ and $\mathfrak{p}$, so their conductors $\mathcal{N}_\theta, \mathcal{N}_{\theta'}$ are supported on these two primes. Define $\varepsilon : G_K \to \mathbb{F}_p^*$ 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 $\mathfrak{a}$, because θ and θ' are so. Its conductor $\mathcal{N}_\varepsilon$ is then a power of $\mathfrak{a}$. When restricted to the inertia subgroup of $\mathfrak{a}$ the cyclotomic character χ_p is trivial, hence $\varepsilon|_{I_\mathfrak{a}} = \theta^2|_{I_\mathfrak{a}}$. We remarked at the start of this proof that θ^2 is unramified at $\mathfrak{a}$, so ε is everywhere unramified. Again, from the fact that K has class number one we derive that ε is trivial.

Let $\sigma_\mathfrak{a}$ be a Frobenius element of $\mathfrak{a}$. Since $\mathfrak{a}$ is a prime of potentially multiplicative reduction, it is know (see for instance [46, Lemma 6.3]) that the possible pairs of eigenvalues of $\overline{\rho}_{E,p}(\sigma_\mathfrak{a})$ are $(1, \mathrm{Norm}(\mathfrak{a}))$ or $(-1, -\mathrm{Norm}(\mathfrak{a}))$. We therefore

get

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

so $p \mid \mathrm{Norm}(\mathfrak{a}) - 1 = 3$, which is not possible for our choice of $p \in \{19, 43, 67, 163\}$.

We proved that p does not ramify in K. If p is inert, we can apply [35, 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. 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 [48, 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 $\theta'|_{I_{\mathfrak{p}_2}} = \chi_p|_{I_{\mathfrak{p}_2}}$.

The character θ^2 is unramified everywhere except $\mathfrak{p}_1$, because the only bad place $\mathfrak{a}$ of E is of potential multiplicative reduction. Using Lemma 3.3.3 in the previous section with $\alpha = 2 \in K$, it follows that

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

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

Appealing to Lemma 6.3 in [46] again, we derive that $\theta^2(\sigma_{\mathfrak{a}}), \theta'^2(\sigma_{\mathfrak{a}})$ are congruent (up to reordering) to 1 and $\mathrm{Norm}^2(\mathfrak{a})$ modulo p. By replacing E with the p-isogenous curve $E/\langle\theta\rangle$ we can assume that $\theta^2(\sigma_{\mathfrak{a}}) \equiv 1 \pmod{p}$. We have that

$$\mathrm{Norm}_{K_{\mathfrak{p}_1}/\mathbb{Q}_p}(\iota_{\mathfrak{p}_1}(2))^2 - 1 = 15,$$

so $p \mid 15$ which gives a contradiction. □

Let us stay in the hypothesis of the previous proposition. In Lemma 3.2.1 we saw that E has potentially multiplicative reduction at $\mathfrak{a}$ and that $p \nmid v_{\mathfrak{a}}(j(E))$. It follows from the theory of Tate curves [52, Proposition 6.1] that there is an element $\sigma \in I_{\mathfrak{a}} \subseteq G_K$ that acts on $E[p]$ via a matrix of the form $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. The image $\overline{\rho}_{E,p}(G_K)$ is therefore an irreducible subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ which contains an element of order p and the classification [48, Proposition 15] of maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ implies that $\mathrm{SL}_2(\mathbb{F}_p) \subseteq \overline{\rho}_{E,p}(G_K)$. The determinant of $\overline{\rho}_{E,p}$ is the mod p cyclotomic character, which is surjective when $K \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$, i.e. when p is not ramified in K. If that is the case, $\overline{\rho}_{E,p}$ is surjective, hence absolutely irreducible.

We now prove the absolute irreducibility of $\overline{\rho}_{E,p}$ in the cases where p ramifies

in K. Recall that under the restrictions required in the hypothesis of the above proposition, these are $p = d = 19, 43, 67$ or 163. Suppose now that $\overline{\rho}_{E,p}$ is irreducible but absolutely reducible. As in the preceding proof, this means that over $\mathrm{GL}_2(\mathbb{F}_{p^2})$ we have

$$\overline{\rho}_{E,p} \sim \begin{pmatrix} \theta & * \\ 0 & \theta' \end{pmatrix}, \tag{3.5.3}$$

where θ and θ' are now characters $G_K \to \mathbb{F}_{p^2}^*$, which are not $\mathbb{F}_p$-valued, such that $\theta\theta' = \chi_p$. For the reasons discussed above, the characters θ, θ' are unramified everywhere outside $2\mathcal{O}_K = \mathfrak{a}$ and p. The squares of these two characters are unramified at $\mathfrak{a}$, as before.

Now we observe that a case analogous to **(i)** above cannot occur, for if does we can assume without losing generality that θ' is unramified at p. This makes θ'^2 an everywhere unramified, hence trivial character. Using the relation stated above, we obtain $\theta^2 = \chi_p^2$. The last relation implies that $\theta : G_K \to \mathbb{F}_{p^2}^*$ is in fact $\mathbb{F}_p$-valued, a contradiction.

Suppose that both θ and θ' are ramified at p and write $\mathfrak{P}$ for the unique prime of $\mathcal{O}_K$ that lies above p. Using the notation described in (3.5.2), either

$$\overline{\rho}_{E,p}|_{I_\mathfrak{P}} \sim \begin{pmatrix} \psi_2^2 & 0 \\ 0 & \psi_2^{2p} \end{pmatrix} \text{ or } \overline{\rho}_{E,p}|_{I_\mathfrak{P}} \sim \begin{pmatrix} \psi_1 & 0 \\ 0 & \psi_1 \end{pmatrix}.$$

The argument given in the proof of the proposition above shows that the latter can't happen. Hence the restrictions of θ, θ' to the inertia subgroup at $\mathfrak{P}$ must be squares of the level 2 fundamental characters. Define $\varepsilon : G_K \to \mathbb{F}_{p^2}$ by

$$\varepsilon = \theta^p/\theta' = \theta^{p+1}/\chi_p.$$

It is clear from the definition that ε is unramified at $\mathfrak{P}$. Since θ^2 is unramified at $\mathfrak{a}$, the same is true for θ^{p+1}. This proves that ε is unramified everywhere, hence trivial. We showed that $\theta' = \theta^p$, so $\theta^{p+1} = \chi_p$. As the order of the mod p cyclotomic character is $p-1$, we infer that $\theta : G_K \to \mathbb{F}_{p^2}^*$ has order p^2-1. This cuts an extension of K with order p^2-1 that is unramified everywhere outside $\mathfrak{P}$. In particular, there is a quadratic extension of K that is unramified everywhere outside $\mathfrak{P}$. Assisted by **Sage** [56] we verify that such an extension does not exist in all of our cases. We present our computations for the case $p = d = 163$, mentioning that everything works identically for all the other three cases.

```
sage: K.<a> = QuadraticField(-163)
sage: OK = K.ring_of_integers()
```

```
sage: S = set((163*OK).prime_factors()) # primes above 163
sage: S
{Fractional ideal (-a)}
sage: Sel163 = K.selmer_group(S,2, proof = True)
sage: Sel163
[-a, -1]
```

The output of the last line of code above is a list of generators for the Selmer group $K(\{\mathfrak{P}\},2)$. All of them have order 2 in $K^\times/(K^\times)^2$. The group $K(\{\mathfrak{P}\},2)$ contains the subgroup of those $t \in K$ such that $K(\sqrt{t})/K$ is unramified at all primes outside $\mathfrak{P}$, but may contain it properly. It is indeed the case that for all $t \in K(\{\mathfrak{P}\},2)$ the extension $K(\sqrt{t})/K$ is ramified at the prime above 2.

```
sage: L.<b> = K.extension(x^2-Sel163[0])
sage: L.<b> = L.absolute_field()
sage: OL = L.ring_of_integers()
sage: L2 = (2*OL).prime_factors()
sage: L2
[Fractional ideal (2, b + 1)]
sage: L2[0].norm()
4
sage: L.<b> = K.extension(x^2-Sel163[1])
sage: L.<b> = L.absolute_field()
sage: OL = L.ring_of_integers()
sage: L2 = (2*OL).prime_factors()
sage: L2
[Fractional ideal (2, 1/324*b^3 + 83/162*b + 1)]
sage: L2[0].norm()
4
sage: L.<b> = K.extension(x^2-(Sel163[0]*Sel163[1]))
sage: L.<b> = L.absolute_field()
sage: OL = L.ring_of_integers()
sage: L2 = (2*OL).prime_factors()
sage: L2
[Fractional ideal (2, b + 1)]
sage: L2[0].norm()
4
```

The computations listed above show that for each $t \in K(\{\mathfrak{P}\},2)$, there is

only one prime above 2 in the number field $K(\sqrt{t})$. This prime can be inert or ramified in $K(\sqrt{t})/K$. As the absolute norm of the aforementioned prime ideal is equal to $4 = \mathrm{Norm}(2 \cdot \mathcal{O}_K)$, we know that it is ramified. The outcomes of analogue computations in the remaining cases $p = d = 19, 43$ and 67 are identical.

This shows that there are no quadratic extension of K unramified outside p, contradicting our previous conclusion. We therefore proved that $\overline{\rho}_{E,p}$ is absolutely irreducible.

Suppose we want to follow the strategy in previous sections and want to prove that for some fixed $K = \mathbb{Q}(\sqrt{-d})$, the Fermat equation (3.2.1) does not have non-trivial solutions in $(a, b, c) \in \mathcal{O}_K^3$ and $p \geq 19$, prime. We proceed by contradiction and, assuming there is such a solution, we construct the Frey curve $E = E_{a,b,c,p} : Y^2 = X(X - a^p)(X + b^p)$. The next step in our approach is to show the mod p Galois representation $\overline{\rho}_{E,p}$ satisfies the hypothesis of Serre's conjecture. Absolute irreducibility is the only condition in the aforementioned hypothesis that is not straightforward and, as we saw above, requires quite a bit of work.

In every instance in which we succeeded to prove the absolute irreducibility of $\overline{\rho}_{E,p}$ we made essential use of the fact that E had potentially multiplicative reduction at a prime above 2. This is quite a nuisance since it only allows us to prove that when K is among the last six quadratic imaginary fields considered, Fermat's equation $a^p + b^p + c^p = 0$ does not have non-trivial solutions $(a, b, c) \in \mathcal{O}_K^*$, $p \geq 19$ such that $2 \mid abc$. We believe that it would be extremely hard to overcome this nuisance. In fact, over $\mathbb{Q}(\sqrt{-3})$ it is impossible. One could see that the three roots of unity of order 3 provide a non-trivial solution to Fermat for every exponent $p \geq 5$. Standard conjectures imply that, for p large enough, these are the only non-trivial solutions over quadratic imaginary fields of class number 1. We will discuss the last assertion in the next section.

Before proceeding further with applying Serre's conjecture, let us remark that we can adapt the above to prove the following statement.

Proposition 3.5.1. Let $K = \mathbb{Q}(\sqrt{-d})$ where $d = 3$, 11, 19, 43, 67 or 163 and fix $\mathfrak{q}$ a prime ideal of $\mathcal{O}_K$. There is a constant $B_{d,\mathfrak{q}}$, depending only on d and $\mathfrak{q}$, such that if $p \geq B_{\mathfrak{q}}$ and $(a, b, c) \in \mathcal{O}_K^3$ with $\mathfrak{q} \mid abc$ is a non-trivial solution to the Fermat equation (3.2.1), then $\overline{\rho}_{E,p}$ is absolutely irreducible.

It will be clear by the end of this section that the above implies that for $p \geq B_{d,\mathfrak{q}}$, the Fermat equation does not have non-trivial coprime solutions $(a, b, c) \in \mathcal{O}_K^3$ such that $\mathfrak{q} \mid abc$.

Let us now go back to our task of proving that for $p \geq 19$ prime, the Fermat equation (3.2.1) does not have any non-trivial coprime solution $(a, b, c) \in \mathcal{O}_K^3$ such

that $2 \mid abc$. Suppose it does and let $(a,b,c) \in \mathcal{O}_K^3$ and p be such a solution. We saw above that the Galois representation on the p-torsion of the Frey curve E satisfies the hypothesis of Conjecture 2.2.1. As discussed in the previous section, this predicts the existence of a mod p eigenform $\Phi : \mathbb{T}_{\overline{\mathbb{F}}_p}(\mathcal{N}) \to \overline{\mathbb{F}}_p$ over K such that for every prime ideal $(\pi) \subset \mathcal{O}_K$, coprime to $p\mathcal{N}$.

$$\text{Trace}\left(\overline{\rho}(\text{Frob}_{(\pi)})\right) = \Phi(T_\pi),$$

where T_π is a Hecke operator.

The trace elements $\text{Trace}\left(\overline{\rho}(\text{Frob}_{(\pi)})\right)$ lie in $\mathbb{F}_p$, therefore Φ corresponds to a class in $H^1(Y_0(\mathcal{N}), \mathbb{F}_p)$ that is an eigenvector for all such Hecke operators T_π. Recall that $\mathcal{N}$ is just the Serre conductor of $\overline{\rho}_{E,p}$ which by Table 3.3 is a divisor of $\mathfrak{a}^4 = (2\mathcal{O}_K)^4$.

As previously described, the obstruction in lifting such mod p eigenforms to complex eigenforms is given by the presence of p-torsion in $H^2(Y_0(\mathcal{N}), \mathbb{Z}_{(p)})$. Observe 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 [2, 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 other words $H^2(Y_0(\mathcal{N}), \mathbb{Z}[\frac{1}{6}]) \cong H^2(\Gamma_0(\mathcal{N}), \mathbb{Z}[\frac{1}{6}])$.

Lefschetz duality for cohomology with compact support [45, Section 2] gives a relation between the first homology and the second cohomology $H_1(\Gamma_0(\mathcal{N}), \mathbb{Z}\left[\frac{1}{6}\right]) \cong H^2(\Gamma_0(\mathcal{N}), \mathbb{Z}\left[\frac{1}{6}\right])$. 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 the previously mentioned algorithm of Haluk Şengün. The Magma implementation of this algorithm was kindly provided to us by its author. The algorithm requires as input presentations for $\text{PGL}_2(\mathcal{O}_K)$, which we compute using a program of Page [41]. The relevant Magma files can be found at

`https://warwick.ac.uk/fac/sci/maths/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 3.4.

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 $\mathfrak{a}^4$ to which our mod p eigenform

Table 3.4: prime torsion in $\Gamma_0(\mathcal{N})^{ab}$

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

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 $\mathfrak{q} \nmid \mathfrak{a}^4 \cdot p$, prime ideal of K we get the following congruence

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

between the trace of the image of Frobenius at $\mathfrak{q}$ in $\overline{\rho}_{E,p}$ and the Hecke eigenvalue of $\mathfrak{f}$ at $\mathfrak{q}$. Here $\mathfrak{P}$ is some ideal of $\mathbb{Q}_\mathfrak{f}$ that lies above the prime p. We now use the idea in [19, 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 $\mathfrak{q}$ as above. The Frey curve $E = E_{p,a,b,c}$ has good or multiplicative reduction at $\mathfrak{q}$. If it has good reduction, then $\mathrm{Trace}(\overline{\rho}_{E,p}(\sigma_\mathfrak{q})) \equiv a_\mathfrak{q}(E) \equiv a_\mathfrak{q}(\mathfrak{f}) \pmod{\mathfrak{P}}$. By definition, E has full two-torsion defined over K and $\mathfrak{q} \nmid 2$, so $4 \mid \#E(\mathbb{F}_\mathfrak{q}) = \mathrm{Norm}(\mathfrak{q}) + 1 - a_\mathfrak{q}(E)$. Adding the information provided by the Hasse-Weil bounds we get that $a_\mathfrak{q}(E)$ belongs to the finite set

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

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

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

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

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

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

Using Magma, we computed the cuspidal newforms $\mathfrak{f}$ at levels dividing $\mathfrak{a}^4$, the fields $\mathbb{Q}_\mathfrak{f}$ and eigenvalues $a_\mathfrak{q}(\mathfrak{f})$ at primes $\mathfrak{q}$ of K that have small norms. We computed the ideal $C_{S,\mathfrak{f}} \subseteq \mathcal{O}_K$, the greatest common divisor of $B_{\mathfrak{f},\mathfrak{q}}$ when $\mathfrak{q} \nmid 2$ runs throw a set S of prime ideals of K that have small norm. If $C_{S,\mathfrak{f}}$ is not zero, then $p \mid \mathrm{Norm}(C_\mathfrak{f})$ gives an upper bound on p.

The Magma routine below, takes as input a quadratic imaginary field K and a finite set S of prime ideals $\mathfrak{q} \nmid 2$ of $\mathcal{O}_K$ that have small norm. For each newform $\mathfrak{f}$, the routine detects the forms with $C_\mathfrak{f} = 0$ (if there are any) and outputs the list of all rational primes dividing $\mathrm{Norm}(C_\mathfrak{f})$ if the latter is non-zero. We baptised these as "the surviving primes" and, by the discussion above, p must be one of them.

```
BS := function(form, order, S); //
    B := &+[Bfq(form,order,q): q in S];
    return Integers()!Norm(B);
end function;

SurvivingForms := procedure(K,OK,level,S);
    print "The space of Bianchi modular forms was created
     in time:";
    time M := BianchiCuspForms(K,level);
    print "The newspace was created in time:";
    time Mnew := NewSubspace(M);
    print "The newspace at this level has dimension :",
            Dimension(Mnew);
    decomp := NewformDecomposition(Mnew);
    print "There are", #decomp, "irreducible subspaces.
    Each one corresponds to a Bianchi newform form";
    for i in [1..#decomp] do
        ff := Eigenform(decomp[i]);
        print "Dealing with", i,"-th eigenform";
        Qff := BaseField(ff);
        print "Degree, Discriminant, Signature of Qff:",
         Degree(Qff), Discriminant(Qff), Signature(Qff);
        Off := MaximalOrder(Qff);
        Cff := BS(ff,Off,S);
        if Cff eq 0 then
            print "!This form is problematic as Cff=0
             and has to be dealth with separately!!";
```

```
            break;
        end if;
        print "Factorization of Cff:", Factorization(Cff);
        survivors := [l : l in PrimeDivisors(Norm(Cff))];
        print "Surviving Primes and p must be among them:",
        survivors;
    end for;
end procedure;
```

Over the field $K = \mathbb{Q}(\sqrt{-3})$ there are no cuspidal Bianchi modular forms of level dividing $\mathfrak{a}^4$, so there is nothing to check. This proves that the Fermat equation (3.2.1) does not have non-trivial solutions for prime exponent $p \geq 17$ and coprime $(a, b, c) \in \mathcal{O}_K^3$ such that $2 \mid abc$. The triple $(a, b, c) = (1, \omega, \omega^2) \in \mathcal{O}_K^3$ is a non-trivial solution to (3.2.1) for every prime $p \geq 5$, where $\omega \in K$ is a primitive third root of unity. The Frey curve

$$E := E_{p,1,\omega,\omega^2} : Y^2 = X(X - 1^p)(X + \omega^p)$$

is, for every prime $p \geq 5$, a twist of the CM curve with LMFDB label 256.1-CMb1. As we can see on the corresponding page on the LMFDB website, its Bianchi modular form is not cuspidal. This explains why we didn't find it.

When $K = \mathbb{Q}(\sqrt{-11})$, the space of Bianchi modular forms of level $\mathfrak{a}^4$ has dimension 2. Both of the eigenforms are new at this level. By running the above procedure at level $\mathfrak{a}^4$ with S consisting of the odd primes of K of norm up to 37, we get the following output.

```
Creating the Newspace
Time: 0.400
The newspace at this level has dimension 2
There are 2 irreducible subspaces
Dealing with 1 -th eigenform
Degree, Discriminant, Signature of Qff: 1 1 1 0
Factorization of Cff: [ <3, 1>, <5, 1> ]
Surviving Primes and p must be among them: [ 3, 5 ]
Dealing with 2 -th eigenform
Degree, Discriminant, Signature of Qff: 1 1 1 0
Factorization of Cff: [ <3, 1>, <5, 1> ]
Surviving Primes and p must be among them: [ 3, 5 ]
```

In both cases, this contradicts our assumption that $p > 17$.

For $K = \mathbb{Q}(\sqrt{-19})$ the cuspidal Bianchi spaces of levels strictly dividing $\mathfrak{a}^4$ are empty. There are 4 newforms at level $\mathfrak{a}^4$, two of them having rational Hecke eigenvalues. The remaining pair has eigenvalues defined over $\mathbb{Q}(\sqrt{17})$. Running the *SurvivingForms* procedure at this level with S being the set of odd prime ideals in $\mathcal{O}_K$ that have norm less than 37 we obtain

```
Creating the space of BianchiModular Forms in time:
Time: 0.240
Creating the Newspace
Time: 0.980
The newspace at this level has dimension 6
There are 4 irreducible subspaces
Dealing with 1 -th eigenform
Degree, Discriminant, Signature of Qff: 1 1 1 0
Factorization of Cff: [ <3, 1>, <5, 1> ]
Surviving Primes and p must be among them: [ 3, 5 ]
Dealing with 2 -th eigenform
Degree, Discriminant, Signature of Qff: 1 1 1 0
Factorization of Cff: [ <3, 1>, <5, 1> ]
Surviving Primes and p must be among them: [ 3, 5 ]
Dealing with 3 -th eigenform
Degree, Discriminant, Signature of Qff: 2 17 2 0
Factorization of Cff: []
Surviving Primes and p must be among them: []
Dealing with 4 -th eigenform
Degree, Discriminant, Signature of Qff: 2 17 2 0
Factorization of Cff: []
Surviving Primes and p must be among them: []
```

Recall that our procedure had a flag for the situation in which $C_{\mathfrak{f}}$ is equal to zero and this is not the case for the last two eigenforms above. The output emphasizes the fact that $C_{\mathfrak{f}}$ is the whole of $\mathcal{O}_K$, so there are no primes dividing its norm. Again, this is a contradiction with the assumption that the exponent of the Fermat equation p is greater than 17.

Suppose that $K = \mathbb{Q}(\sqrt{-43})$. At level $\mathfrak{a}^2$ there is one newform $\mathfrak{f}$ with $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}(\sqrt{5})$. Running the procedure using an analogous set of primes as before, we get

```
Creating the space of BianchiModular Forms in time:
Time: 0.480
```

```
Creating the Newspace
Time: 0.350
The newspace at this level has dimension 2
There are 1 irreducible subspaces
Dealing with 1 -th eigenform
Degree, Discriminant, Signature of Qff: 2 20 2 0
Factorization of Cff: [ <5, 1> ]
Surviving Primes and p must be among them: [ 5 ]
```

There are 11 cuspidal Bianchi newforms at level $\mathfrak{a}^4$. By running the same procedure we observe that the list of surviving primes is composed of 3 and 5, therefore reaching a contradiction.

Exactly in the same way we obtain a contradiction over $K = \mathbb{Q}(\sqrt{-67})$. We just remark that, in this case, the space of cuspidal Bianchi modular forms at level $\mathfrak{a}^4$ consists of 8 eigenforms, none of them having rational coefficients.

Finally, let $\mathbb{Q}(\sqrt{-163})$. There are no cuspidal Bianchi modular forms of levels strictly dividing $\mathfrak{a}^4$. On the other hand, at level $\mathfrak{a}^4$ there are 10 eigenforms. The output of running *SurvivingForms* procedure is the following. It is worth remarking that already the procedure of computing the newspace is expensive. The complexity seems to grow exponentially with the discriminant of K and with the level.

```
Creating the space of BianchiModular Forms in time:
Time: 5.440
Creating the Newspace
Time: 6080.940
The newspace at this level has dimension 78
There are 10 irreducible subspaces
Dealing with 1 -th eigenform
Degree, Discriminant, Signature of Qff: 1 1 1 0
Factorization of Cff: [ <3, 2>, <5, 2>, <7, 1> ]
Surviving Primes and p must be among them: [ 3, 5, 7 ]
Dealing with 2 -th eigenform
Degree, Discriminant, Signature of Qff: 1 1 1 0
Factorization of Cff: [ <3, 2>, <5, 2>, <7, 1> ]
Surviving Primes and p must be among them: [ 3, 5, 7 ]
Dealing with 3 -th eigenform
Degree, Discr., Sign. of Qff: 6 2872879192353793 6 0
Factorization of Cff: [ <7, 1> ]
Surviving Primes and p must be among them: [ 7 ]
```

```
Dealing with 4 -th eigenform
Degree, Discr., Sign. of Qff: 6 19979480143625 6 0
Factorization of Cff: [ <5, 2>, <7, 1> ]
Surviving Primes and p must be among them: [ 5, 7 ]
Dealing with 5 -th eigenform
Degree, Discr., Sign. of Qff: 6 12175652072825 6 0
Factorization of Cff: [ <5, 1>, <7, 1> ]
Surviving Primes and p must be among them: [ 5, 7 ]
Dealing with 6 -th eigenform
Degree, Discr., Sign. of Qff: 6 12175652072825 6 0
Factorization of Cff: [ <5, 1>, <7, 1> ]
Surviving Primes and p must be among them: [ 5, 7 ]
Dealing with 7 -th eigenform
Degree, Discr., Sign. of Qff: 6 19979480143625 6 0
Factorization of Cff: [ <5, 2>, <7, 1> ]
Surviving Primes and p must be among them: [ 5, 7 ]
Dealing with 8 -th eigenform
Degree, Discr., Sign. of Qff: 6 2872879192353793 6 0
Factorization of Cff: [ <7, 1> ]
Dealing with 9 -th eigenform
Degree, Sign. of Qff: 20 20 0
Factorization of Cff: []
Surviving Primes and p must be among them: []
Dealing with 10 -th eigenform
Degree, Sign. of Qff: 20 20 0
Factorization of Cff: []
Surviving Primes and p must be among them: []
```

We have not listed the discriminant of $\mathbb{Q}_{\mathfrak{f}}$ for the last two forms above purely for reasons concerning formatting. It has 158 digits and we print it here to illustrate how quickly Bianchi modular forms get complicated:
78421838844986627516008957681004121247595825201938135271756615451404679945421860384592062363894532632444698012244915940759330253612735960780311769726173839 36.

Since p, the exponent in Fermat's equation was assumed to always be greater than 17, the above yields a contradiction. The previous discussion contains the proof of the following theorem.

Theorem 3.5.1. *Let $K = \mathbb{Q}(\sqrt{-d})$, when $d = 3, 11, 19, 43, 67$ or 163. Assume Conjecture 2.2.1 holds for K. For any prime $p \geq 19$, the Fermat equation*

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

does not have non-trivial solutions in coprime $(a, b, c) \in \mathcal{O}_K^3$ such that $2 \mid abc$.

Remark. *When $d = 3$, 11, 19, 43 or 67, 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.*

3.6 Conjectures 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 with prime exponent $a^p + b^p + c^p = 0$ 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 [17] point out that it is reasonable to make the following conjecture, a consequence of the *abc*-conjecture for number fields (see [6]).

Conjecture 3.6.1. *Let K be a number field such that $\omega \notin K$. Then the Asymptotic Fermat's Last Theorem holds over K.*

Theorem 3.5.1 presented 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. 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 immediately 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 $E := E_{p,1,\omega,\omega^2}$ is, for every such p, a twist of the CM curve with LMFDB label 256.1-CMb1. The representation $\overline{\rho}_{E,p}$ of this curve is never absolutely irreducible. To be precise, for $p \geq 5$, the image $\overline{\rho}_{E,p}(G_K)$ 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 more conjectures.

Conjecture 3.6.2 (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 $\overline{\rho}_{E,p} : G_K \to \mathrm{GL}_2(\mathbb{F}_p)$ is surjective.*

Let K be one of the six quadratic imaginary fields listed above. Assume that Serre's modularity and the Uniformity conjectures (Conjectures 2.2.1 and 3.6.2) hold for K. As there are elliptic curves with 17-isogenies defined over K (there are such elliptic curves defined over $\mathbb{Q}$), we must take $C(K) > 17$.

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

$$a^p + b^p + c^p = 0. \tag{3.6.1}$$

As before, we can scale the solution of (3.6.1) such that $a, b, c \in \mathcal{O}_K \setminus \{0\}$ are coprime. From Theorem 3.5.1 we know that $2 \nmid abc$. Let

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

be the usual Frey curve and denote by $\overline{\rho}_{E,p} : G_K \to \mathrm{GL}_2(\mathbb{F}_p)$ the Galois representation on the p-torsion. The discussion in previous sections shows that $\overline{\rho}_{E,p}$ is unramified away from the primes above 2 and p, it is finite flat at every prime of K that lies above p and $\det(\overline{\rho}_{E,p})$ is the mod p cyclotomic character. Lemma 3.2.1 in the previous section shows 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 [19, Lemma 4.1]).

Suppose that E does not have CM. Our assumption of the Uniformity conjecture implies that $\overline{\rho}_{E,p}$ is surjective, hence absolutely irreducible. Its Serre conductor is $\mathcal{N} = 2^4\mathcal{O}_K$. Thus, $\overline{\rho}_{E,p}$ satisfies the hypothesis of Conjecture 2.2.1 and this predicts the existence of a mod p eigenform $\Phi : \mathbb{T}_{\overline{\mathbb{F}}_p}(\mathcal{N}) \to \overline{\mathbb{F}}_p$ over K such that for every prime ideal $(\pi) \subset \mathcal{O}_K$, coprime to $p\mathcal{N}$,

$$\mathrm{Trace}\left(\overline{\rho}(\mathrm{Frob}_{(\pi)})\right) = \Phi(T_\pi),$$

where T_π is a Hecke operator. The computations carried at the end of last section

show that this is not possible for $p \geq C(K) > 17$.

Suppose that E has CM. As we discussed in the introductory chapter, Serre and Tate [50] showed that such abelian varieties have everywhere potential good reduction, hence $j(E)$ is an algebraic integer. Recall that

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

We know that the ideal $\gcd(c_4(E), \Delta(E))$ is supported only on the prime above 2 and this prime does not divide abc. We obtain that abc is a unit and 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 (3.2.1), 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 this with Theorem 3.1.1.

Theorem 3.6.1. *Let $K = \mathbb{Q}(\sqrt{-d})$ be a quadratic imaginary number field of class number 1 and suppose that Conjectures 2.2.1 and 3.6.2 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.*

If $K \neq \mathbb{Q}(\sqrt{-3})$ is any *fixed* quadratic imaginary number field of arbitrary class number, one could in theory follow the strategy we recurrently used in this thesis to prove that, under the same two conjectures, Asymptotic Fermat's Last Theorem holds over K. The key steps are ordered as follow:

1. Assuming Conjecture 3.6.2, if the solutions a, b, c are not units, for p large enough we know that the mod p representation $\overline{\rho}_{E,p}$ is surjective. The other conditions required in the hypothesis of Conjecture 2.2.1 are trivially satisfied. The latter conjecture predicts the existence of a non-trivial mod p eigenform for GL_2 over K, which has fixed level $\mathcal{N}$ and is associated to our hypothetical Frey curve.

2. Şengün and Siksek show in [46, Section 2] that if p is large enough, every such mod p eigenform lifts to a non-cuspidal Bianchi newform F of fixed level $\mathcal{N}$ whose eigenvalues must satisfy a precise congruence modulo primes above p with the traces of Frobenius of the Frey curve E. Using **Magma**, we can compute the space of Bianchi newforms of level $\mathcal{N}$ for K and produce a list

of finitely many candidates for F. The complexity of this computation grows exponentially with the discriminant of K and with the norm of the ideal $\mathcal{N}$ and, so the computation become impractical very quickly.

3. Assuming the previous steps were completed, using a few primes of small norm in K, for each newform $\mathfrak{f}$ in our list we compute a constant $C_{\mathfrak{f}}$, as presented at the end of last section. The latter has the property that if F satisfies the aforementioned congruence involving the traces of Frobenius of E, then the exponent p must divide $C_{\mathfrak{f}}$. If the constant $C_{\mathfrak{f}}$ is non-zero this gives an upper bound on p, proving the Asymptotic Fermat's Last Theorem.

4. When the previous constant $C_{\mathfrak{f}} = 0$, the newform $\mathfrak{f}$ necessarily has rational eigenvalues. We can sometimes prove that $\mathfrak{f}$ corresponds to an elliptic curve $E_{\mathfrak{f}}$ of fixed level $\mathcal{N}$. Proving that $\mathfrak{f}$ and $E_{\mathfrak{f}}$ have isomorphic l-adic Galois representations (for every prime l) can be done in finite time using the *Faltings-Serre-Livné* method [15] or, when $\mathfrak{f}$ is base-change, the theory of base-change for GL_2 as we have done in our work over $\mathbb{Q}(\sqrt{-2})$. Our experience suggest that in practice the curves $E_{\mathfrak{f}}$ have CM. These do not have surjective mod p Galois representation, therefore contradicting our requirement that $\overline{\rho}_{E,p} \sim \overline{\rho}_{E_{\mathfrak{f}},p}$.

It was remarked earlier in the thesis that, unlike classical modular forms, Bianchi newforms do not always correspond to elliptic curves. This intriguing phenomena has been intensively studied by many people, amongst which we mention works of Cremona [10] in the nineties and the recent paper of Schembri [44]. An Eichler-Shimura type conjecture (see Conjecture 2.4.1) predicts that such a non-cuspidal Bianchi newform $\mathfrak{f}$ with integral Hecke eigenvalues corresponds to an elliptic curve $E_{\mathfrak{f}}$ or to a fake elliptic curve $A_{\mathfrak{f}}$ defined over K. Our computations suggest that when $\mathfrak{f}$ corresponds to a fake elliptic curve, the constant $C_{\mathfrak{f}}$ produced at Step 3 is non-zero, giving a bound on p. Although we cannot prove that $C_{\mathfrak{f}} \neq 0$ for such $\mathfrak{f}$, one possible explanation for why experiments suggest that happens could be found in Theorem 1.4.1. This theorem shows that $A_{\mathfrak{f}}$ has potential good reduction everywhere, therefore imposing restrictions on the size of images of inertia subgroups under the Galois representations attached to $A_{\mathfrak{f}}$. These restrictions are sometimes incompatible with the images of the same subgroups under the Galois representations attached to the Frey curve E. Hopefully the next chapter unveils more of the mysteries regarding images of inertia.

It is essential that K is fixed for the above sequence of steps to have any chance of successful ending. Such a strategy is doomed to failure if one tries to

prove Asymptotic Fermat's Last Theorem holds over an infinite family of quadratic imaginary fields. The vital missing ingredient is a result analogous to the classical Eichler-Shimura theorem. The author has learned from [46] that an Eichler-Shimura conjecture (see Conjecture 2.4.1) has been formulated. Şengün and Siksek proved the following wonderful result in loc. cit. Although their theorem is stated for general number fields, we restrict our discussion to quadratic imaginary ones.

Theorem 3.6.2 ([46, Theorem 1.2])**.** *Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field where d is a squarefree positive integer satisfying $-d \equiv 2$ or $3 \pmod 4$. Assume Conjectures 2.2.1 and 2.4.1. Then the Asymptotic Fermat's Last Theorem holds over K.*

The main theorem in [46] gives a sufficient criterion for Asymptotic Fermat's Last Theorem to hold over an arbitrary number field K, assuming the two conjectures. The criterion is automatically satisfied for the quadratic imaginary fields in the theorem above. In order to prove such a result, it is vital for K to have a prime ideal of residue field $\mathbb{F}_2$. Such an ideal is needed for proving the absolute irreducibility of the mod p Galois representation of the usual Frey curve and to guarantee the non-existence of an elliptic curve defined over K with very special properties. The theorem stated above covers the imaginary quadratic fields in which 2 ramifies.

Let us see what can be said about this problem over the quadratic imaginary fields where 2 is either split or inert. Let K be such a field. Suppose $a, b, c \in K \setminus \{0\}$ is a solution to the Fermat equation

$$a^p + b^p + c^p = 0, \tag{3.6.2}$$

where p is some prime exponent larger than some constant B_K that will be decided later. It is explained in [46, Section 5] that we can scale the solution (a, b, c) so that the triple is integral and $\mathfrak{G} := \gcd(a, b, c)$ is a prime ideal that belongs to a finite set, which depends only on the field K. This is slightly different from the situation in which the class number of K was assumed to be trivial.

We are going to denote by $E := E_{a,b,c,p} : Y^2 = X(X - a^p)(X + b^p)$ the usual Frey curve and, after fixing a basis for $E[p]$, by $\overline{\rho}_{E,p} : G_K \to \mathrm{GL}_2(\mathbb{F}_p)$ its mod p Galois representation. We would like to show that the latter satisfies the conditions required in the hypothesis of Conjecture 2.2.1. All of these except absolute irreducibility of $\overline{\rho}_{E,p}$ are trivially satisfied as we discussed in the previous sections. In general, we do not know how to prove the absolute irreducibility of $\overline{\rho}_{E,p}$ for p large enough. When 2 is inert in K, we can prove this if we assume that $2 \mid abc$, but we would then be only able produce an asymptotic version of Theorem 3.5.1 for the

field K. Let us not impose this restriction on the product abc, but rather assume Conjecture 3.6.2.

If the Frey curve E has complex multiplication, the integrality of its j-invariant imposes severe restrictions on the product abc. Increasing p, one can prove that a, b, c are units in $\mathcal{O}_K$. We saw that such solutions only exists over $\mathbb{Q}(\sqrt{-3})$ and a, b, c must then be the third roots of unity.

If E does not have CM, then from Conjecture 3.6.2 we get that there exists a constant $C(K)$ such that if $p > C(K)$, the representation $\overline{\rho}_{E,p}$ is surjective. The determinant of $\overline{\rho}_{E,p}$ is the mod p cyclotomic character, the representation is finite flat at every prime $\mathfrak{p} \mid p$ and its Serre conductor is supported only on the primes $\{2\mathcal{O}_K, \mathfrak{G}\}$ (see [46, Lemma 5.4]). Obviously, this conductor belongs to a finite set depending only on the field K. We therefore arrange that the constant $B(K)$ is larger than $C(K)$.

From the proof of [46] we see that, by increasing B_K, we can find:
(A) either an elliptic curve E'/K such that the following hold:

1. E' has good reduction away from $\{2\mathcal{O}_K, \mathfrak{G}\}$, and potentially good reduction away from $2\mathcal{O}_K$,

2. E' has full 2-torsion,

3. the representations $\overline{\rho}_{E,p}$ and $\overline{\rho}_{E',p}$ are isomorphic

(B) or a fake elliptic curve A, of conductor $\mathcal{N}^2$, supported only on $\{2\mathcal{O}_K, \mathfrak{G}\}$, such that for all prime ideals $\mathfrak{q} \nmid \mathcal{N}$,

$$\#A(\mathcal{O}_K/\mathfrak{q}) = \#E(\mathcal{O}_K/\mathfrak{q})^2 \pmod{p}.$$

We believe that for p large enough, **(B)** should be impossible and hence **(A)** must hold. When 2 splits in K, this was proved by Şengün and Siksek [46] by studying the images of inertia at primes above 2 of the relevant mod p Galois representations. A deep conjecture atributed to Frey and Mazur asserts that if E_1/K is a fixed elliptic curve, there exists a bound $B_{1,K}$ such that for $p > B_{1,K}$, if E_2/K is an elliptic curve such that $E_1[p] \cong E_2[p]$ as G_K-modules then E_1 and E_2 must be isogenous. If such a conjecture would hold for two dimensional abelian varieties, then one could show that for p large enough, **(B)** can't happen. We are not aware if the Frey-Mazur conjecture was even formulated in the literature in such generality.

Let us ignore the problems caused by **(B)** for the rest of this section. Suppose

that **(A)** holds. We are now following closely [46, Section 8]. Write

$$E' : Y^2 = X(X - e_1)(X - e_2),$$

where $e_1, e_2 \in \mathcal{O}_K$. Denote by S the set of prime ideals in K that lie above 2, by $\lambda := e_1/e_2$ and let λ' be any of the following six expressions:

$$\lambda, \quad 1/\lambda, \quad 1-\lambda, \quad 1/(1-\lambda), \quad \lambda/(\lambda-1), \quad (\lambda-1)/\lambda.$$

Then,

$$j(E') = 2^8 \cdot \frac{(\lambda'^2 - \lambda' + 1)^3}{\lambda'^2(1-\lambda')^2}. \tag{3.6.3}$$

If $\mathfrak{q} \notin S$ is a prime ideal of K, as E' has potentially good reduction at $\mathfrak{q}$ we know that $v_{\mathfrak{q}}(j(E')) \geq 0$. Thus λ' is the root of a degree six monic polynomial with coefficients that are $\mathfrak{q}$-integral, hence $v_{\mathfrak{q}}(\lambda') \geq 0$. This is true for both $\lambda' = \lambda$ and $\lambda' = 1/\lambda$, therefore $\lambda \in \mathcal{O}_{K,S}^{\times}$. The same is true for $\mu := 1 - \lambda$, so pair $(\lambda, \mu) = (\lambda, 1-\lambda)$ is a solution to the S-unit equation $x + y = 1$, where $x, y \in \mathcal{O}_{K,S}^{\times}$.

If 2 is inert in K, it can be easily verified that the only solutions to the S-unit equation above are $(\lambda, \mu) = (2, -1)$, $(-1, 2)$ or $(1/2, 1/2)$. By substituting in the expression for the j-invariant, we see that $v(j(E')) = 2^6 \cdot 3^3 = 1728$, which is a known CM j-invariant. This implies that $\overline{\rho}_{E',p}$ is not surjective and in particular we cannot have $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$, yielding a contradiction.

The case in which 2 splits in K is more complicated, as there are many more solutions to the above S-unit equation. However, one could follow the method in [19, Section 6] to prove that for p large enough the Asymptotic Fermat's Last theorem holds over K, where K belongs to a large density subset of quadratic imaginary fields in which 2 splits.

We hope that the previous discussion motivates and aligns Conjecture 3.6.1 with other conjectures in the literature, in the particular case in which K is quadratic imaginary.

Remark. *Over $\mathbb{Q}(\sqrt{-3})$, assuming Conjectures 3.6.2 and 2.2.1, we can prove that there is a constant C such that if $p > C$, the only non-trivial solutions to the Fermat equation $a^p + b^p + c^p = 0$ are permutations of the third roots of unity. We don't have to assume Conjecture 2.4.1 over this number field, since the spaces of Bianchi modular forms we obtain are empty.*

Chapter 4

Irreducible binary cubics and the generalized superelliptic equation

For a large class of (heuristically most) 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.

4.1 Introduction

In their extraordinary paper Bennett and Dahmen [3] 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 [3, 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 [12] 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 Fermat equation over certain totally real number fields by Jarvis [30] and by Freitas and Siksek [19], [20]. 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 [46] proved an asymptotic version of Fermat's Last Theorem over infinitely many general number fields.

In the spirit of [46], the purpose of this work is extend some of the results of Bennett and Dahmen [3] 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. We briefly recall the two conjectures described in Section 2, whose veracity will be assumed in the main theorem of this chapter.

- Conjecture 2.2.1 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 2.4.1, sometimes referred to as *Eichler-Shimura*, is part of the Langlands Programme (see [54]) 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 $c_1, \ldots, c_h$ are the ideal classes of K, for every $i \in \{1, \ldots, h\}$ 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

$$\mathcal{H}_K := \begin{cases} \emptyset, \text{ if } h = 1 \\ \{\mathfrak{m}_1, \ldots, \mathfrak{m}_h\}, \text{ if } h \geq 2 \end{cases}. \tag{4.1.1}$$

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 [3]), we denote by

$$S_F := \mathcal{H}_K \cup \{\text{prime ideals dividing } 2\Delta_F\} \cup \{\text{real infinite places of } K\}. \tag{4.1.2}$$

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 4.1.1. *Let K be a number field for which Conjecture 2.2.1 and Conjecture 2.4.1 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 $\mathfrak{q} \,||\, \Delta_F$ and $\mathfrak{q} \nmid (2\alpha_0)$. If the Thue-Mahler equation*

$$F(x, y) \in \mathcal{O}_{K,S_F}^* \tag{4.1.3}$$

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

$$F(x, y) = z^l \tag{4.1.4}$$

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 [12] implies that for any fixed value of $l \geq 4$, equation (4.1.4) 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 (4.1.4) 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 (4.1.4) 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 4.1.1. *Let K and F satisfy all the hypothesis of Theorem 4.1.1. 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 4.1.1 and effectively compute the constant A_F. In particularly fortuitous situations, one could even find oneself in positions where Conjecture 2.4.1 is known to hold and therefore producing special cases of Theorem 4.1.1 that only depend on Conjecture 2.2.1. This is emphasized in [57], 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 2.2.1) we can take advantage of modularity theorems and prove the following more general result.

Theorem 4.1.2. *Let K be a totally real Galois number field for which Conjecture 2.4.1 holds and $F \in \mathcal{O}_K[x, y]$ an irreducible binary cubic. If the Thue-Mahler equation* (4.1.3) *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* (4.1.4) *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 4.1.1 holds independently of Conjecture 2.2.1 and assuming only Conjecture 2.4.1. 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 4.5.

The insolubility of (4.1.3) seems at first look very restrictive. As pointed out in [3], 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 4.1.2 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 [12].

4.1.1 Differences between general and totally real number fields

Although sharing similar hypothesis and conclusions, the proofs of Theorems 4.1.1 and 4.1.2 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 [46], 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 4.1.1 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 4.1.1, then one could compute the constant A_F explicitly.

2. In order to make the required hypothesis of Theorem 4.1.2 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 [18, 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 4.1.2 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 2.4.1) 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 [46], 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.

4.2 Properties of the Frey curve

The proofs of Theorem 4.1.1 and 4.1.2 use a construction of Bennett and Dahmen [3]. For every Klein form (see [3, 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.

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 [3],

$$4H(x, y)^3 + G(x, y)^2 = -27 \cdot \Delta_F \cdot F(x, y)^2. \tag{4.2.1}$$

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 obstruc-

tion 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 4.2.1 ([3, Prop. 2.1])**.** *The resultant of a binary form F of degree k with its Hessian H satisfies*

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

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

$$E_{x,y} : Y^2 = X^3 + TX^2 + \frac{T^2+H}{3}X + \frac{T^3+3TH+G}{27}. \tag{4.2.2}$$

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 (4.2.1), the fundamental quantities associated to (4.2.2) can be computed as

$$\Delta(x,y) = 2^4 \Delta_F F(x,y)^2, \quad c_4(x,y) = -2^4 H(x,y), \quad c_6(x,y) = -2^5 G(x,y) \tag{4.2.3}$$

and

$$j(x,y) = \frac{-2^8 H(x,y)^3}{\Delta_F F(x,y)^2} \tag{4.2.4}$$

Proposition 4.2.2. *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* (4.2.2)*. 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 4.2.1. □

Proposition 4.2.3. *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 (4.1.1), 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 4.2.4. *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 $x_1, y_1 \in \mathcal{O}_K$ 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 (4.2.4) for $j(x_1, y_1)$ and the resultant identity from Proposition 4.2.1 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. □

4.3 An effective Chebotarev theorem

In this section, we extend the main result in Section 7 of [3] 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 4.3.1 (Theorem 1.1 in [36]). *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 [43, Theorem 1.8].

Theorem 4.3.2. *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 [43] 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 [43, 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 4.3.3. *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 4.3.1

to the extension L directly. Define the ideal $\mathfrak{m} = \prod_{\mathfrak{P} \in S'} \mathfrak{P}$. By Theorem 4.3.2, 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

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

Let us now pick g_t, the non-identity element of the group $\operatorname{Gal}(K(\sqrt{t})/K)$. Applying Theorem 4.3.1 above, one obtains a prime ideal $\mathfrak{l}$ of $\mathcal{O}_K$ such that $\mathfrak{l}$ is unramified in L'/K, $\operatorname{Norm}_{K/\mathbb{Q}}(\mathfrak{l}) \leq 2\,(d_{L'})^A$ and

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

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 $d_{L'} = d_L^2 \cdot \operatorname{Norm}_{L/\mathbb{Q}}\left(\Delta_{L'/L}\right)$, 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 [3, Proposition 7.4] holds for general number fields. For brevity, we include its proof here.

Proposition 4.3.1. *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 $p\mathcal{N}_1$ and that ρ_2 is irreducible. If $\rho_1 \not\simeq \rho_2$, then there exists a prime $\mathfrak{l} \subset \mathcal{O}_K$ with $\mathfrak{l} \nmid p\mathcal{N}_1$, for which both*

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

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 4.3.3 above, one gets the desired bound on l.

□

4.4 The proof of Theorem 4.1.1

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 (4.4.1) - (4.4.5) are due to Bennett and Dahmen [3, 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

$$F(x, y) = \alpha_0(x - ay)^2(x - by) \pmod{\mathfrak{q}}, \text{ for all } x, y \in \mathcal{O}_K. \tag{4.4.1}$$

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

$$\Delta_F = 18\alpha_0\alpha_1\alpha_2\alpha_3 + (\alpha_1\alpha_2)^2 - 27(\alpha_0\alpha_3)^2 - 4\alpha_0\alpha_2^3 - 4\alpha_1^3\alpha_3 \tag{4.4.2}$$

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 (4.4.1) implies that

$$H(x, y) \equiv -\alpha_0^2(a - b)^2(x - ay)^2 \pmod{\mathfrak{q}}, \text{ for all } x, y \in \mathcal{O}_K. \tag{4.4.3}$$

Suppose that $x_0, y_0, z_0 \in \mathcal{O}_K$ is a solution to (4.1.4) 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 (4.2.2) 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

$$j(x_0, y_0) = -\frac{2^8 \cdot H(x_0, y_0)^3}{\Delta_F \cdot F(x_0, y_0)^2} \tag{4.4.4}$$

If $\mathfrak{q} \mid H(x_0, y_0)$, then from (4.4.3) 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

$$v_{\mathfrak{q}}(j(x_0, y_0)) = -1 - 2l \cdot v_{\mathfrak{q}}(z_0) = -1. \tag{4.4.5}$$

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 [46, 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 (4.4.4, 4.4.5) we see that $l \nmid v_{\mathfrak{q}_L}(j(x_0, y_0))$. Using Lemma 5.1 in [46], 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 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 4.2.2 we see that E is semistable at such primes $\mathfrak{P}$. From results in [47] it follows that the mod l Galois representation $\overline{\rho}_{E,l}$ is unramified away from $S_F \cup \{\mathfrak{l} | \mathfrak{l} \subseteq \mathcal{O}_K$ 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 2.2.1. 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 [52, 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 2.2.1 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

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

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 [57], 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 [46, 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 2.4.1, $\mathfrak{f}$ 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 2.4.1, 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 (4.1.4). 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

$$\#E(\mathcal{O}_K/\mathfrak{P}) \equiv \#E_{\mathfrak{f}}(\mathcal{O}_K/\mathfrak{P}) \pmod{l}. \tag{4.4.6}$$

We will now prove that, for l large enough, $E[2]$ and $E_{\mathfrak{f}}[2]$ are isomorphic as G_K modules. From [3, 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 4.3.1 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 [16], the elliptic curves $E = E_{x_0,y_0}$ and $E_{\mathfrak{f}}$ are said to be 2-congruent. Proposition 6.2 in [3] 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 4.2.3 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 4.2.4 to get that $F(x_1, y_1) \in \mathcal{O}_{K,S_F}^*$, a contradiction to (4.1.3).

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.

4.5 K totally real and the proof of Theorem 4.1.2

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

$$\rho_{E,l} \cong \rho_{\mathfrak{f},l}. \tag{4.5.1}$$

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 [55]. We are going to make use of the known fact [18, 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 4.1.2. Before we start the actual proof, we need the following lemma.

Lemma 4.5.1. *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 (4.2.2) 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 (4.2.4) 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 4.2.1, 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 4.1.2.

Suppose $x_0, y_0, z_0 \in \mathcal{O}_K$ is a solution to the generalised superelliptic equation (4.1.4) 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 $E := E_{x_0,y_0}$ as in (4.2.2).

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 4.5.1 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 [20]. 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 4.2.2 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 [21]. 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 [20] 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 [46] 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, i.e. $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$. For such a rational eigenform $\mathfrak{f}$, Conjecture 2.2.1 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 4.4. As it was pointed out previously, the irreducibil-

ity of F implies that $\overline{\rho}_{E,2}$ is irreducible. Using Proposition 4.3.1 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 [3, 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 4.2.3, 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 4.2.4 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 4.5.1, which guarantees that for l large enough, the Frey-Hellegouarch curves we care about are modular.

Bibliography

[1] A. Aigner, *Über die möglichkeit van $x^4 + y^4 = z^4$ in quadratische körpen*, Monatsh. Math. **56** (1952), 335–338.

[2] A. Ash and G. Stevens, *Cohomology of arithmetic groups and congruences between systems of Hecke eigenvalues.*, J. Reine Angew. Math. **365** (1986), 192–220.

[3] M. A. Bennett and S. R. Dahmen, *Klein forms and the generalized superelliptic equation*, Ann. of Math. **177** (2013), 171–239.

[4] W. Bosma, *The Magma algebra system. I. The user language*, Vol. 24, 1997.

[5] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over Q: Wild 3-adic exercises*, Journal of the American Mathematical Society **14** (2001), no. 4, 843–939.

[6] J. Browkin, *The abc–conjecture for algebraic numbers*, Acta Mathematica Sinica **22** (2006Jan), no. 1, 211–222.

[7] K. Buzzard, Diamond F, and Jarvis F., *On Serre's conjecture for mod l Galois representations over totally real fields*, Duke Math. J. **155** (2010), no. 1, 105–161.

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

[9] J. E. Cremona, *Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields*, Compos. Math. **51** (1984), no. 3, 275–324.

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

[11] 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. MR1185241 (94c:11046)

[12] 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.

[13] A. David, *Caractère d'isogénie et critéres d'irréductibilité*, ArXiv e-prints (March 2011), available at `1103.3892`.

[14] M. Derickx, S. Kamienny, W. Stein, and M. Stoll, *Torsion points on elliptic curves over number fields of small degree*, ArXiv e-prints (July 2017), available at `1707.00364`.

[15] L. Dieulefait, L. Guerberoff, and A. Pacetti, *Proving modularity for a given elliptic curve over an imaginary quadratic field*, Math. Comp. **79** (2010), 1145–1170.

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

[17] 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.

[18] 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.

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

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

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

[22] T. Gee, F. Herzig, and D. Savitt, *General Serre weight conjectures*, J. Eur. Math. Soc. (JEMS) **20** (2018), no. 12, 28592949.

[23] B. H. Gross and D. E. Rohrlich, *Some results on the Mordell-Weil group of the Jacobian of the Fermat Curve*, Invent. Math. **44** (1978), 201–224.

[24] M. Grothendieck A. Raynaud and D. Sang, *Groupes de monodromie en gomtrie algbrique*, Lecture Notes in Mathematics, Seminaire de Geometrie Algebrique du Bois-Marie 1967-1969 (SGA 7 I), Springer.

[25] P. E. Gunnells, *Modular symbols for ($\mathbb{Q}$)-rank one groups and Voronoi reduction*, J. Number Theory **52** (1999), 198–219.

[26] ———, *Lectures on Computing Cohomology of Arithmetic Groups* (2014), 3–45.

[27] F. H. Hao and C. J. Parry, *The Fermat Equation over Quadratic Fields*, J. of Number Theory **19** (1984), 115–130.

[28] H. Hida, *On Abelian Varieties with Complex Multiplication as Factors of the Jacobians of Shimura Curves*, American Journal of Mathematics **103** (1981), no. 4, 727–776.

[29] H. Jacquet, *Automorphic Forms on GL(2)*, II, Lecture Notes in Mathematics, Springer, Berlin, 1972.

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

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

[32] B. W. Jordan, *Points on Shimura curves rational over number fields*, Journal für die reine und angewandte Mathematik **371** (1986), 92–114.

[33] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Inventiones Math. **109** (1992Dec), no. 1, 221–229.

[34] C. Khare and J. P. Wintenberger, *Serre's modularity conjecture (ii)*, Inventiones Math. **178** (2009Jul), no. 3, 505.

[35] A. Kraus, *Courbes elliptiques semi-stables et corps quadratiques*, Manuscripta Math. **69** (1990), no. 4, 245–253.

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

[37] S. Lang, *Abelian varieties*, Springer-Verlag, New York, 1983.

[38] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, 2013. [Online; accessed 16 September 2013].

[39] Y. Morita, *On potential good reduction of abelian varieties*, J. Fac. Sci. Univ. Tokyo Sect, I A Math. **22** (1975), no. 3, 437–447.

[40] M. Ohta, *On l-adic representations of Galois groups obtained from certain two-dimensional abelian varieties*, Journal of the Faculty of Science, The University of Tokyo. Sect. 1 A, Mathematics **21** (December 14, 1974), no. 3, 299 –308.

[41] A. Page, *Computing arithmetic Kleinian groups*, Math. Comp. **84** (2015), 2361–2390.

[42] D. Rohrlich, *Elliptic curves and the Weil-Deligne group*, Elliptic curves and related topics, 1994, pp. 125–157.

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

[44] Ciaran Schembri, *Examples of genuine QM abelian surfaces which are modular*, Research in Number Theory **5** (2019Jan), no. 1.

[45] M. H. Şengün, *On the Integral Cohomology of Bianchi Groups*, Experiment. Math. **20** (2011), 487–505.

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

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

[48] ———, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1971/72), 259–331.

[49] ———, *Local fields*, Vol. 67, Springer GTM, New York, 1979.

[50] J. P. Serre and J. Tate, *Good reduction of abelian varieties*, Annals of Mathematics **88** (1968), no. 3, 492–517.

[51] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Vol. 106, Springer, GMT, 1986.

[52] ———, *Advanced Topics in the Arithmetic of Elliptic Curves*, Vol. 151, Springer, GMT, 1994.

[53] R. Swan, *Generators and relations for certain special linear groups*, Advances in Mathematics **6** (1971), no. 1, 1 –77.

[54] R. Taylor, *Representations of Galois groups associated to modular forms*, Preceedings of the ICM.

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

[56] The Sage Developers, *Sagemath, the Sage Mathematics Software System (Version 8.5)*, 2018. `https://www.sagemath.org`.

[57] G. C. Ţurcaş, *On Fermat's equation over some quadratic imaginary number fields*, Research in Number Theory **4** (2018May), no. 2, 24.

[58] P. Tzermias, *Low-degree points on Hurwiz-Klein curves*, Trans. of the American Math. Soc. **356**, no. 3, 939951.