Fermat's Last Theorem over Number Fields

Nuno Freitas
Universitat de Barcelona
Gran Via de Les Corts Catalanes 585
08007, Barcelona, Spain
e-mail: nunobarroso@ub.edu

Resumo: Discutimos a célebre demonstração do Último Teorema de Fermat e as dificuldades que surgem ao tentar aplicar a mesma estratégia de prova sobre corpos de números. Terminamos com uma amostra dos resultados conhecidos no caso de corpos quadráticos.

Abstract We overview the celebrated proof of Fermat's Last Theorem and the challenges that arise when trying to carry it over to number fields. We conclude with a sample of the known results for quadratic fields.

palavras-chave: Fermat, modularidade, curvas elípticas.

keywords: Fermat, modularity, elliptic curves.

1 Introduction

The search for a proof of Fermat's Last Theorem (FLT) is one of the richest and more romantic stories in the history of Mathematics. Remarkable progress in number theory as, for example, the origin of what is now algebraic number theory and some incredible breakthroughs in the Langlands program, have come to light due to this pursuit.

Theorem 1 (FLT) *The integer solutions to the Fermat equation*

$$x^n + y^n + z^n = 0 \tag{1}$$

with $n \geq 3$ are trivial, i.e., they satisfy $xyz = 0$.

The cases $n = 3$ and $n = 4$ of FLT were respectively solved by Euler and Fermat. From this it is easy to see that we only have to prove it for $n = p \geq 5$ a prime. If (a, b, c) is a solution, then by scaling we can suppose that $\gcd(a, b, c) = 1$; we call such a solution *primitive*. The Fermat equation, viewed as defining a curve in $\mathbb{P}^2$, has genus $(p-1)(p-2)/2$, and a celebrated theorem of Faltings tells us that there are only finitely many primitive solutions to (1), for each fixed $n = p$. Despite the efforts of many

great mathematicians through 350 years, it was only in 1995 that a complete proof was published. In this paper, we will discuss this modern approach to FLT due to Hellegouarch, Frey, Serre and Ribet which culminated in Wiles' proof [24] and created a new way of tackling Diophantine equations known as *the modular method*.

2 The modular method

The proof of FLT is based on three main pillars: Mazur's irreducibility theorem, Wiles' modularity theorem for semistable elliptic curves over $\mathbb{Q}$ and Ribet's level lowering theorem. Explaining these pillars will involve a detour into some of the most fascinating areas of modern number theory: elliptic curves, Galois representations, modular forms and modularity. For a comprehensive introduction to these topics we suggest [3, 21, 22]. For an overview and history of various methods to study the Generalized Fermat equation $x^r + y^q = z^p$ we refer to [1], which we follow closely in this section.

2.1 Elliptic curves

Let K be a field. The simplest definition of an *elliptic curve* E over K is: a smooth curve in $\mathbb{P}^2$ given by an equation of the form

$$E \ : \ y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3, \tag{2}$$

with a_1, a_2, a_3, a_4 and $a_6 \in K$. If the characteristic of K is not 2 or 3, then we can transform to a much simpler model given by the affine equation

$$E \ : \ Y^2 = X^3 + aX + b, \tag{3}$$

where a and $b \in K$, whose disriminant is

$$\Delta_E = -16(4a^3 + 27b^2).$$

We call (3) a *Weierstrass model of* E with *discriminant* Δ_E. The requirement that E is smooth is equivalent to the assumption that $\Delta_E \neq 0$. There is another very important quantity attached to an elliptic curve called the *j-invariant* which can be computed from the model (3) by the formula

$$j_E = \frac{(-48a)^3}{\Delta_E}.$$

Note however that j_E is an invariant of the isomorphism class of E over $\overline{K}$, the algebraic closure of K, and so independent of the choosen model.

There is a distinguished K-point, the 'point at infinity', which we denote by ∞. Given a field $L \supseteq K$, the set of L-points on E is given by

$$E(L) = \{(x, y) \in L^2 \ : \ y^2 = x^3 + ax + b\} \cup \{\infty\}.$$

It turns out that the set $E(L)$ has the structure of an abelian group with ∞ as the identity element. The group structure is easy to describe geometrically: three points P_1, P_2, $P_3 \in E(L)$ add up to the identity element if and only if there is a line ℓ defined over L meeting E in P_1, P_2, P_3 (with multiplicities counted appropriately). The classic Mordell–Weil Theorem states that for a number field K the group $E(K)$ is finitely generated. For a model as in (3), the 2-torsion subgroup $E[2]$ consists of the points with $y = 0$ plus ∞. It turns out that the proofs by Euler and Fermat of FLT for $n = 3, 4$ are simply special cases of what are now standard Mordell–Weil group computations, as discussed in [1, Examples 1 and 2].

2.2 Modular forms

Let $\mathbb{H} = \{z \in \mathbb{C} \ : \ \mathrm{Im}(z) > 0\}$. Let k and N be positive integers and set

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : \ c \equiv 0 \pmod{N} \right\},$$

which is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of finite index. The group $\Gamma_0(N)$ acts on $\mathbb{H}$ via fractional linear transformations

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \ : \ \mathbb{H} \to \mathbb{H}, \qquad z \mapsto \frac{az + b}{cz + d}.$$

The quotient $Y_0(N) = \Gamma_0(N) \backslash \mathbb{H}$ has the structure of a non-compact Riemann surface. This has a standard compactification denoted $X_0(N)$ and the difference $X_0(N) \setminus Y_0(N)$ is a finite set of points called the *cusps*.

A *modular form f of weight k and level N* is a function $f \ : \ \mathbb{H} \to \mathbb{C}$ that satisfies the following conditions:

(i) f is holomorphic on $\mathbb{H}$;

(ii) f satisfies the property

$$f\left(\frac{az + b}{cz + d}\right) = (cz + d)^k f(z), \tag{4}$$

for all $z \in \mathbb{H}$ and $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$;

(iii) f extends to a function that is holomorphic at the cusps.

It follows from these properties, and the fact that one of the cusps is the cusp at $i\infty$, that f must have a Fourier expansion

$$f(z) = \sum_{n \geq 0} c_n q^n \quad \text{where} \quad q(z) = \exp(2\pi i z). \tag{5}$$

It turns out that the set of modular forms of weight k and level N, denoted by $M_k(N)$, is a finite-dimensional vector space over $\mathbb{C}$. A *cusp form* of weight k and level N is an $f \in M_k(N)$ that vanishes at all the cusps. As $q(i\infty) = 0$ we see in particular that a cusp form must satisfy $c_0 = 0$. The cusp forms naturally form a subspace of $M_k(N)$ which we denote by $S_k(N)$.

There is a natural family of commuting operators $T_n : S_2(N) \to S_2(N)$ (with $n \geq 1$) called the *Hecke operators*. The *eigenforms* of level N are the weight 2 cusp forms that are simultaneous eigenvectors for all the Hecke operators. Such an eigenform is called *normalized* if $c_1 = 1$ and thus its Fourier expansion has the form

$$f = q + \sum_{n \geq 1} c_n q^n.$$

2.3 Modularity

Let $E/\mathbb{Q}$ be given by a model (2) where the $a_i \in \mathbb{Z}$, and having (non-zero) discriminant $\Delta_E \in \mathbb{Z}$. Carrying out a suitable linear substitution, we generally work with a *minimal model*: that is one where the $a_i \in \mathbb{Z}$ and with discriminant having the smallest possible absolute value. Associated to E is another, more subtle, invariant called the *conductor* N_E, which we shall not define precisely, but we merely point that it is a positive integer sharing the same prime divisors as the minimal discriminant; that it measures the 'bad behavior' of the elliptic curve E modulo primes; and that it can be computed easily through *Tate's algorithm* [22, Chapter IV]. In particular, the primes p not dividing N_E are the primes of *good reduction* while those satisfying $p \| N_E$ are the primes of *multiplicative reduction*.

Now let $p \nmid \Delta_E$ be a prime. Reducing modulo p a minimal equation (2) we obtain an elliptic curve $\tilde{E}$ over $\mathbb{F}_p$. The set $\tilde{E}(\mathbb{F}_p)$ is an abelian group as before, but now necessarily finite, and we denote its order by $\#\tilde{E}(\mathbb{F}_p)$. Let

$$a_p(E) = p + 1 - \#\tilde{E}(\mathbb{F}_p).$$

We are now ready to state a version of the modularity theorem due to Wiles, Breuil, Conrad, Diamond and Taylor [2, 23, 24]. This remarkable theorem was previously known as the Shimura–Taniyama conjecture.

Theorem 2 (The Modularity Theorem) *Let $E/\mathbb{Q}$ be an elliptic curve with conductor N_E. There exists a normalized eigenform $f = q + \sum c_n q^n$ of weight 2 and level N_E with $c_n \in \mathbb{Z}$ for all n, and such that for every prime $p \nmid \Delta_E$ we have $c_p = a_p(E)$.*

For an elliptic curve E and an eigenform f as in this theorem we will also say that *f corresponds to E via modularity.*

2.4 Galois representations

Let E be an elliptic curve over $\mathbb{C}$. The structure of the abelian group $E(\mathbb{C})$ is particularly easy to describe. There is a discrete lattice $\Lambda \subset \mathbb{C}$ of rank 2 (that is, as an abelian group $\Lambda \simeq \mathbb{Z}^2$) depending on E, and an isomorphism

$$E(\mathbb{C}) \simeq \mathbb{C}/\Lambda. \tag{6}$$

Let p be a prime. By the p-torsion of $E(\mathbb{C})$ we mean the subgroup

$$E[p] = \{Q \in E(\mathbb{C}) \ : \ pQ = 0\}.$$

It follows from (6) that

$$E[p] \simeq (\mathbb{Z}/p\mathbb{Z})^2, \tag{7}$$

which can be viewed as 2-dimensional $\mathbb{F}_p$-vector space. Now let E be an elliptic curve over $\mathbb{Q}$. Then we may view E as an elliptic curve over $\mathbb{C}$, and with the above definitions obtain an isomorphism $E[p] \simeq (\mathbb{Z}/p\mathbb{Z})^2$. However, in this setting, the points of $E[p]$ have algebraic coordinates, and are acted on by $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, *the absolute Galois group of the rational numbers.* Via the isomorphism (7), the group $G_{\mathbb{Q}}$ acts on $(\mathbb{Z}/p\mathbb{Z})^2$. Thus we obtain a 2-dimensional representation depending on $E/\mathbb{Q}$ and the prime p:

$$\overline{\rho}_{E,p} \ : \ G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p). \tag{8}$$

We say that the $\overline{\rho}_{E,p}$ is *reducible* if the matrices of the image $\overline{\rho}_{E,p}(G_{\mathbb{Q}})$ share some common eigenvector. Otherwise we say that $\overline{\rho}_{E,p}$ is irreducible. We have now given enough definitions to be able to state Mazur's theorem; this is often considered as the first step in the proof of FLT.

Theorem 3 (Mazur [15]) *Let $E/\mathbb{Q}$ be an elliptic and p a prime.*

(i) If $p > 163$, then $\overline{\rho}_{E,p}$ is irreducible.

(ii) If E has full 2-torsion (that is $E[2] \subseteq E(\mathbb{Q})$), square-free conductor and $p \geq 5$, then $\overline{\rho}_{E,p}$ is irreducible.

2.5 Ribet's level lowering theorem

Let $E/\mathbb{Q}$ be an elliptic curve and associated mod p Galois representation $\overline{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ as above. Let f be an eigenform. Deligne and Serre showed that such an f gives rise, for each prime p, to a Galois representation $\overline{\rho}_{f,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_{p^r})$, where $r \geq 1$ depends on f. If E corresponds to f via the Modularity Theorem, then $\overline{\rho}_{E,p} \sim \overline{\rho}_{f,p}$ (the two representations are isomorphic). Thus the representation $\overline{\rho}_{E,p}$ is *modular* in the sense that it arises from a modular eigenform. Recall also from the Modularity Theorem that, if f corresponds to E via modularity, then the conductor of E is equal to the level of f. Sometimes it is possible to replace f by another eigenform of smaller level which has the same mod p representation. This process is called *level lowering*. We now state a special case of Ribet's level lowering theorem. For a prime ℓ, we let $v_\ell(x)$ denote the ℓ-adic valuation of $x \in \mathbb{Q}$.

Theorem 4 (Ribet's level lowering theorem [18]) *Let $E/\mathbb{Q}$ be an elliptic curve with minimal discriminant Δ and conductor N. Let $p \geq 3$ be prime. Suppose that (i) the curve E is modular and (ii) the mod p representation $\overline{\rho}_{E,p}$ is irreducible. Let*

$$N_p = \frac{N}{M_p}, \quad \textit{where} \quad M_p = \prod_{\substack{\ell \| N, \\ p \,|\, v_\ell(\Delta)}} \ell. \tag{9}$$

Then $\overline{\rho}_{E,p} \sim \overline{\rho}_{g,p}$ for some eigenform g of weight 2 and level N_p.

We now know, by the Modularity Theorem that all elliptic curves over $\mathbb{Q}$ are modular, so condition (i) in Ribet's theorem is automatically satisfied. We include it here both for historical interest but also because analogous level lowering results are available over other fields and modularity of all elliptic curves is still an open question over general fields.

2.6 The proof of Fermat's Last Theorem

Suppose $p \geq 5$ is prime, and a, b and c are non-zero pairwise coprime integers satisfying (1) with $n = p$. We reorder (a, b, c) so that

$$b \equiv 0 \pmod 2 \quad \text{and} \quad a^p \equiv -1 \pmod 4. \tag{10}$$

We consider the *Frey–Hellegouarch curve* which depends on (a, b, c):

$$E \ : \ Y^2 = X(X - a^p)(X + b^p) \tag{11}$$

whose minimal discriminant and conductor are:

$$\Delta = \frac{a^{2p}b^{2p}c^{2p}}{2^8}, \qquad N = \prod_{\ell|\Delta} \ell.$$

Note that the conductor is square-free; conditions (10) ensure that $2 \,||\, N$. The 2-torsion subgroup of E is $E[2] = \{\infty,\ (0,0),\ (a^p,0),\ (-b^p,0)\} \subset E(\mathbb{Q})$. As $p \geq 5$, we know by part (ii) of Mazur's irreducibility theorem that $\overline{\rho}_{E,p}$ is irreducible. Moreover, E is modular by the Modularity Theorem[1], and so the hypotheses of Ribet's theorem are satisfied. We compute $N_p = 2$ using the recipe in (9). It follows that $\overline{\rho}_{E,p} \sim \overline{\rho}_{g,p}$, where g has weight 2 and level 2. But there are no eigenforms of weight 2 and level 2, a contradiction.

2.6.1 Some Historical Remarks

In the early 1970s, Hellegouarch had the idea of associating to a non-trivial solution of the Fermat equation the elliptic curve (11); he noted that the number field generated by its p-torsion subgroup $E[p]$ has surprisingly little ramification. In the early 1980s, Frey observed that this elliptic curve enjoys certain remarkable properties that should rule out its modularity. Motivated by this, in 1985 Serre made precise his modularity conjecture and showed that it implies Fermat's Last Theorem. Serre's remarkable paper [20] also uses several variants of the Frey–Hellegouarch curve to link modularity to other Diophantine problems. Ribet announced his level-lowering theorem 1987, showing that modularity of the Frey–Hellegouarch curve implies FLT.

3 Fermat's Last Theorem over Number Fields

3.1 Historical background

Interest in the Fermat equation over various number fields goes back to the 19th and early 20th Century. For example, Dickson's *History of the Theory of Numbers* [4, pages 758 and 768] mentions extensions by Maillet (1897) and Furtwängler (1910) of classical ideas of Kummer to the Fermat equation $x^p + y^p = z^p$ ($p > 3$ prime) over the cyclotomic field $\mathbb{Q}(\zeta_p)$. However, the elementary, cyclotomic and Mordell–Weil approaches to the Fermat equation have had limited success. Indeed, even over $\mathbb{Q}$, no combination of these

[1] In fact, we only need modularity of *semistable* elliptic curves over $\mathbb{Q}$, i.e. those with square-free conductor, which was the original modularity result proved by Wiles.

approaches is known to yield a proof of FLT for infinitely many prime exponents p. It is therefore natural to attempt to carry Wiles' proof over to general number fields. The first work in this direction is due to Jarvis and Meekin [12] who showed FLT holds for the field $\mathbb{Q}(\sqrt{2})$. They further analyzed the situation over other real quadratic fields to conclude that

> *"... the numerology required to generalise the work of Ribet and Wiles directly continues to hold for $\mathbb{Q}(\sqrt{2})$... there are no other real quadratic fields for which this is true ... "*

3.2 The asymptotic Fermat's conjecture

Let K be a number field and $\mathcal{O}_K$ its ring of integers. By the *Fermat equation with exponent p over K* we mean

$$x^p + y^p + z^p = 0, \qquad x, y, z \in \mathcal{O}_K. \tag{12}$$

A solution (a, b, c) of (12) is called *trivial* if $abc = 0$, otherwise *non-trivial*. Clearly, over any K there are trivial solutions, such as $(1, -1, 0)$, but sometimes more, for example,

$$(18 + 17\sqrt{2})^3 + (18 - 17\sqrt{2})^3 = 42^3,$$

$$(1 + \sqrt{-7})^4 + (1 - \sqrt{-7})^4 = 2^4,$$

showing that the exact same statement as of FLT does not hold over $\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{-7})$. Instead it makes sense to consider the question only for large enough exponents. More precisely, we will say that the **asymptotic Fermat's Last Theorem over K holds** if there is some bound B_K such that for prime $p > B_K$, all solutions to the Fermat equation (12) are trivial.

Now let $K = \mathbb{Q}(\sqrt{-3})$ and consider the element $\omega = \frac{\sqrt{-3}-1}{2}$. We have that $\omega^3 = 1$ and it is easy to see that, for all primes $p \geq 5$, the equality

$$\omega^p + (\omega^2)^p + 1^p = 0,$$

holds, hence the asymptotic FLT does not hold over $\mathbb{Q}(\sqrt{-3})$.

Conjecture 1 (Asymptotic Fermat's Conjecture) *Let K be a number field. If $\omega \notin K$ then the asymptotic FLT over K holds.*

4 The modular method over totally real fields

We restrict ourselves to *totally real fields*, i.e., number fields such that all embeddings into $\mathbb{C}$ have image in $\mathbb{R}$. This is a natural restriction, because modularity related objects and questions are very poorly understood for fields with at least one complex embedding, consequently all results about FLT for such fields are conditional on two deep conjectures of the Langlands program (see [19] for details). In contrast, for a totally real field K there is a well established theory of *Hilbert modular forms* which are the natural replacement for the modular forms over $\mathbb{Q}$; it is not our objective to discuss details of this theory here. The only thing to keep in mind is that they satisfy the analogous properties over K to those described in §2.2 and that modularity of elliptic curves over K can be defined by a correspondence with Hilbert eigenforms, similar to the discussion in §2.3

In particular, since K is totally real, we have $\omega \notin K$ and we expect the Asymptotic Fermat Conjecture to hold for K. To properly discuss the challenges we face it helps to break the method into the following steps:

1. **Constructing a Frey curve.** Attach a Frey elliptic curve E/K to a putative solution of (12).
2. **Modularity.** Prove modularity of E/K.
3. **Irreducibility.** Prove irreducibility of $\overline{\rho}_{E,p}$, the mod p Galois representation attached to E.
4. **Level lowering.** Conclude that $\overline{\rho}_{E,p} \sim \bar{\rho}_{\mathfrak{f},\mathfrak{p}}$ where $\mathfrak{f}$ is a Hilbert eigenform over K of (parallel) weight 2 and level among finitely many possibilities N_i. Here, $\bar{\rho}_{\mathfrak{f},\mathfrak{p}}$ denotes the mod $\mathfrak{p}$ Galois representation attached to $\mathfrak{f}$ for some $\mathfrak{p} \mid p$ in the field of coefficients $\mathbb{Q}_{\mathfrak{f}}$ of $\mathfrak{f}$.
5. **Contradiction.** Compute all the eigenforms $\mathfrak{f}$ predicted in Step 4 and show that $\overline{\rho}_{E,p} \not\sim \bar{\rho}_{\mathfrak{f},\mathfrak{p}}$ for all of them.

Suppose that $a, b, c \in \mathcal{O}_K$ is a solution to (12) such that $abc \neq 0$. Since (12) is equation (1) over K we consider in step 1 the classical Frey curve over K:

$$E_{a,b,c} \ : \ Y^2 = X(X - a^p)(X + b^p). \tag{13}$$

4.1 The case of $\mathbb{Q}(\sqrt{2})$

Recall that steps 2–4 in the proof of FLT over $\mathbb{Q}$ are covered respectively by the three remarkable theorems of Wiles, Mazur and Ribet. However, at the

time of writing [12] only step 4 was known to hold over a general K (due to the combined work of Jarvis, Rajae and Fijuwara [9, 10, 17]). To complete the modularity step Jarvis and Meekin showed that, under some non-restrictive assumptions on a, b, c (analogous to (10)), the curve $E_{a,b,c}$ is semistable and its modularity followed by a result of Jarvis–Manoharmayum [11] stating that all semistable elliptic curves over $\mathbb{Q}(\sqrt{2})$ are modular. For the irreducibility part they applied a criterion of Kraus [14] for $p \geq 17$ and, finally, a contradiction follows because after completing step 4 there are again no eigenforms.

4.2 The contradiction step

By looking at the proofs of FLT over $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2})$, the reader may wonder why is there a step 5, as the contradiction happens automatically. It turns out these are the only cases where such convenient coincidence occurs. For example, if the class number of K is > 1, we cannot assume coprimality of a, b, c, and the Frey curve will not be semistable, consequently the levels obtained after level lowering will have larger norms and, in general, there are eigenforms at these levels. In fact, step 5 is nowadays the most difficult part when applying the modular method to solve (12) or any other Diophantine equation assuming, of course, that an associated Frey curve exists (i.e. step 1 can be done); unfortunately, there are only a few Diophantine equations known to have attached Frey curves.

4.3 Modularity and Irreducibility

Although the modularity of the Frey curve was the hardest step in the proof of FLT, nowadays we know it holds in full generality due to a result of Freitas–Le Hung–Siksek [6].

Theorem 5 (F.–Le Hung–Siksek) *Let K be a totally real field. Up to isomorphism over $\overline{K}$, there are at most finitely many non-modular elliptic curves E over K.*

Moreover, if K is quadratic, then all elliptic curves over K are modular.

Furthermore, in the recent work of Derickx–Najman–Siksek [5], modularity of elliptic curves was extended to the case of totally real cubic fields.

Theorem 6 (Derickx–Najman–Siksek) *All elliptic curves over totally real cubic fields are modular.*

These modularity results have the following important consequence.

Corollary 4.1 *Let K be a totally real field. There is some constant A_K, depending only on K, such that for any non-trivial solution (a, b, c) of the Fermat equation* (12) *with prime exponent $p > A_K$, the Frey curve $E_{a,b,c}$ given by* (13) *is modular.*

Moreover, if K is quadratic or cubic then $A_K = 0$.

There is no irreducibility result for $\bar{\rho}_{E,p}$ over K analogous to Mazur's theorem. Instead, we can derive the following result from the works of David and Momose, who build on Merel's Uniform Boundedness Theorem [16].

Theorem 7 *Let K be a totally real field. There is a constant C_K, depending only on K, such that the following holds. If $p > C_K$ is prime, and E is an elliptic curve over K with either good or multiplicative reduction at all $\mathfrak{q} \mid p$, then $\overline{\rho}_{E,p}$ is irreducible.*

4.4 A refined level lowering

The next step in the strategy is level lowering which is known to hold for general K due to the combined work of Fujiwara, Jarvis and Rajaei. As explained above, after applying level lowering, we will not obtain a contradiction due to the presence of eigenforms. Instead, the idea is to use finer properties of the Frey curve $E_{a,b,c}$, to show that many of the eigenforms are not a real obstruction.

Before proceeding, it is helpful here to make a comparison with the equation $x^p + y^p + L^\alpha z^p = 0$ over $\mathbb{Q}$, with L an odd prime and α a positive integer, considered by Serre and Mazur [20, p. 204]. A non-trivial solution to this latter equation gives rise, via modularity and level lowering, to a classical weight 2 newform f of level $2L$; for $L \geq 13$ there are such eigenforms and we face the same difficulty. Mazur however shows that if p is sufficiently large then f corresponds to an elliptic curve E' with full 2-torsion and conductor $2L$, and by classifying such elliptic curves concludes that L is either a Fermat or a Mersenne prime. To be able to transfer and refine Mazur's argument to our setting, we need the following conjecture, which is the opposite direction to modularity and generalizes the Eichler–Shimura Theorem over $\mathbb{Q}$.

Conjecture 2 ("Eichler–Shimura") *Let K be a totally real field. Let $\mathfrak{f}$ be a Hilbert newform of level $\mathcal{N}$ and parallel weight 2, and rational field of coefficients. Then there is an elliptic curve $E_{\mathfrak{f}}/K$ with conductor $\mathcal{N}$ having the same* L*-function as $\mathfrak{f}$.*

We will also need some more notation. For K a totally real field, an element $x \in K$ and a prime ideal $\mathfrak{q}$ in $\mathcal{O}_K$ we write $v_{\mathfrak{q}}(x)$ to denote a $\mathfrak{q}$-adic valuation of x. Moreover, let

$$\begin{gathered} S = \{\mathfrak{P} \,:\, \mathfrak{P} \text{ is a prime ideal of } \mathcal{O}_K \text{ dividing } 2\mathcal{O}_K\}, \\ T = \{\mathfrak{P} \in S \,:\, \mathcal{O}_K/\mathfrak{P} = \mathbb{F}_2\}, \qquad U = \{\mathfrak{P} \in S \,:\, 3 \nmid v_{\mathfrak{P}}(2)\}. \end{gathered} \tag{14}$$

We choose a set $\mathcal{H}$ of prime ideals $\mathfrak{m} \notin S$ representing the elements in the class group of K. We also need an assumption, which we refer to as **(ES)**:

$$\textbf{(ES)} \qquad \begin{cases} \text{either } [K:\mathbb{Q}] \text{ is odd;} \\ \text{or } T \neq \emptyset; \\ \text{or Conjecture 2 holds for } K. \end{cases}$$

For a non-trivial solution (a, b, c) to the Fermat equation (12), let

$$\mathcal{G}_{a,b,c} := a\mathcal{O}_K + b\mathcal{O}_K + c\mathcal{O}_K. \tag{15}$$

Now Mazur's argument adapted to our setting gives the following result.

Theorem 8 *Let K be a totally real field satisfying* **(ES)**. *There is a constant B_K, depending only on K, such that the following holds. Let (a, b, c) be a non-trivial solution to* (12) *with prime exponent $p > B_K$, and rescale (a, b, c) so that it remains integral and satisfies $\mathcal{G}_{a,b,c} = \mathfrak{m}$ for some $\mathfrak{m} \in \mathcal{H}$. Write E for the Frey curve* (13). *Then there is an elliptic curve E' over K such that*

(i) the conductor of E' is divisible only by primes in $S \cup \{\mathfrak{m}\}$;

(ii) $\#E'(K)[2] = 4$;

(iii) $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$;

Write j' for the j-invariant of E'. Then,

(a) for $\mathfrak{P} \in T$, we have $v_{\mathfrak{P}}(j') < 0$;

(b) for $\mathfrak{P} \in U$, we have either $v_{\mathfrak{P}}(j') < 0$ or $3 \nmid v_{\mathfrak{P}}(j')$;

(c) for $\mathfrak{q} \notin S$, we have $v_{\mathfrak{q}}(j') \geq 0$.

In particular, E' has potentially good reduction away from S.

5 Results over totally real fields

5.1 S-unit equations

Assuming **(ES)**, Theorem 8 implies that a non-trivial solution to the Fermat equation over K with sufficiently large exponent p yields an elliptic curve E'/K with full 2-torsion and potentially good reduction away from the set S of primes above 2. There are such elliptic curves over every K, for example the curve $Y^2 = X^3 - X$, and so we still do not get a simple contradiction. Note however that the latter elliptic curve does not satisfy conclusion (a) of Theorem 8 when the field K is such that $T \neq \emptyset$, hence it is not an obstruction in that case. An element $x \in K$ is called an *S-unit* if $\upsilon_{\mathfrak{q}}(x) = 0$ for all $\mathfrak{q} \notin S$. Using the fact that elliptic curves with full 2-torsion and good reduction away from S are classified by solutions to S-unit equations, we have the following result that describes when there are no E'/K as in Theorem 8, and so no obstruction to the desired contradiction.

Theorem 9 (F.–Siksek) *Let K be a totally real field satisfying (ES). Let S, T and U be as in* (14)*. Write $\mathcal{O}_S^*$ for the group of S-units of K. Suppose that for every solution (λ, μ) to the S-unit equation*

$$\lambda + \mu = 1, \qquad \lambda,\, \mu \in \mathcal{O}_S^* \tag{16}$$

there is

(A) either some $\mathfrak{P} \in T$ that satisfies $\max\{|\upsilon_{\mathfrak{P}}(\lambda)|, |\upsilon_{\mathfrak{P}}(\mu)|\} \leq 4\,\upsilon_{\mathfrak{P}}(2)$,

(B) or some $\mathfrak{P} \in U$ that satisfies both $\max\{|\upsilon_{\mathfrak{P}}(\lambda)|, |\upsilon_{\mathfrak{P}}(\mu)|\} \leq 4\,\upsilon_{\mathfrak{P}}(2)$, and $\upsilon_{\mathfrak{P}}(\lambda\mu) \equiv \upsilon_{\mathfrak{P}}(2) \pmod 3$.

Then the asymptotic Fermat's Last Theorem holds over K.

For all fields K, equation (16) has solutions in $\mathbb{Q} \cap \mathcal{O}_S^*$, namely $(\lambda, \mu) = (2, -1), (-1, 2), (1/2, 1/2)$ which correspond to the elliptic curve $Y^2 = X^3 - X$, however these solutions satisfy (A) if $T \neq \emptyset$ and (B) if $U \neq \emptyset$.

5.2 The quadratic case

In view of Theorem 9, we have to solve the S-unit equation (16) and test the solutions in order to decide whether the asymptotic FLT holds over K. There are algorithms that, in principle, could do that for each particular K, but what is more interesting is to show that asymptotic FLT holds for infinite

families of fields. For this we need to control the solutions to (16) over varying fields. This can be very hard but, in the case of real quadratic fields, we achieved considerable success, as illustrated by the following series of theorems taken from the joint works with Siksek [7, 8].

Theorem 10 *Let $d \geq 2$ be square-free, such that $d \equiv 6, 10 \pmod{16}$ or $d \equiv 3 \pmod{8}$. Then the asymptotic FLT holds over $\mathbb{Q}(\sqrt{d})$.*

Moreover, for $d > 5$ satisfying $d \equiv 5 \pmod{8}$, the same is true assuming that Conjecture 2 holds over $\mathbb{Q}(\sqrt{d})$.

There are other explicit congruence conditions on d for which asymptotic FLT is known to hold over $\mathbb{Q}(\sqrt{d})$ (see [7, Theorem 1]) and, moreover, there are also real quadratic fields $\mathbb{Q}(\sqrt{d})$ not given by a congruence condition on d for which asymptotic FLT holds. We have the following density theorem.

Theorem 11 (F.–Siksek) *The asymptotic FLT holds for a set of real quadratic fields of density $5/6$. Assuming Conjecture 2 this density becomes 1.*

The following result shows that it is possible to optimize B_K by making K concrete. In this case the proof does not pass through Theorem 9, but instead one needs to optimize the exponent bound at every step of the strategy, which raises other challenges not discussed here.

Theorem 12 (F.–Siksek) *Let $3 \leq d \leq 23$ be square-free and $d \neq 5, 17$ or $d = 79$. Then, all solutions (a, b, c) to the equation*

$$x^p + y^p + z^p = 0, \qquad a, b, c \in \mathbb{Q}(\sqrt{d}) \qquad p \geq 5 \text{ prime}$$

satisfy $abc = 0$. Moreover, the same is true over $\mathbb{Q}(\sqrt{17})$ for half the exponents, more precisely, for all primes $p \geq 5$ such that $p \equiv 3, 5 \pmod{8}$.

5.2.1 FLT over $\mathbb{Q}(\sqrt{5})$

Note that the field $\mathbb{Q}(\sqrt{5})$ is not covered by any of the theorems above and indeed asymptotic FLT over $\mathbb{Q}(\sqrt{5})$ seems to be a very hard open problem. The main reason being that the modular method does not see the difference between the Fermat equation (12) and its variant with unit coefficients

$$\frac{1+\sqrt{5}}{2}x^p + \frac{1-\sqrt{5}}{2}y^p + z^p = 0$$

which has a solution $(1, 1, -1)$. Nevertheless, the following result gives evidence that FLT should be true over $\mathbb{Q}(\sqrt{5})$, as predicted by Conjecture 1.

Theorem 13 (Kraus [13]) *Let $K = \mathbb{Q}(\sqrt{5})$ and $p < 10^7$ be a prime. Then the Fermat equation with exponent p over K has only the trivial solutions.*

References

[1] M. A. Bennett, P. Mihăilescu and S. Siksek *The Generalized Fermat Equation*, pages 173–205 of Open Problems in Mathematics (J. F. Nash, Jr. and M. Th. Rassias eds), Springer, New York, 2016.

[2] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, Journal of the American Mathematical Society **14** (2001), 843–939.

[3] F. Diamond and J. Shurman, *A First Course on Modular Forms*, GTM **228**, Springer, 2005.

[4] L. E. Dickson, *History of the Theory of Numbers, Vol. II*, Chelsea, New York, 1971.

[5] M. Derickx, F. Najman and S. Siksek, *Elliptic curves over real cubic fields are modular*, preprint.

[6] N. Freitas, B. V. Le Hung and S. Siksek, *Elliptic curves over real quadratic fields are modular*, Inventiones Mathematicae **201** (2015), 159–206.

[7] N. Freitas and S. Siksek, *The asymptotic Fermat's last theorem for five-sixths of real quadratic fields*, Compos. Math. **151** (2015), no. 8, 1395–1415.

[8] N. Freitas and S. Siksek, *Fermat's Last Theorem over some small real quadratic fields*, Algebra & Number Theory **9** (2015), no. 4, 875–895.

[9] K. Fujiwara, *Level optimisation in the totally real case*, `arXiv:0602586v1`, 27 February 2006.

[10] F. Jarvis *Correspondences on Shimura curves and Mazur's principle at p*, Pacific J. Math., **213** (2), 2004, 267–280.

[11] F. Jarvis and J. Manoharmayum, *On the modularity of supersingular elliptic curves over certain totally real number fields*, Journal of Number Theory **128** (2008), no. 3, 589–618.

[12] F. Jarvis and P. Meekin, *The Fermat equation over $\mathbb{Q}(\sqrt{2})$*, J. Number Theory **109** (2004), 182–196.

[13] A. Kraus, *Sur le théorème de Fermat sur $\mathbb{Q}(\sqrt{5})$*, Annales Mathématiques du Québec 39.1 (2015), 49–59.

[14] A. Kraus, *Courbes elliptiques semi-stables et corps quadratiques*, J. of number theory **60** (1996), 245–253

[15] B. Mazur, *Rational isogenies of prime degree*, Inventiones Math. **44** (1978), 129–162.

[16] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), 437–449.

[17] A. Rajaei, *On the levels of mod ℓ Hilbert modular forms*, J. reine angew. Math. **537** (2001), 33–65.

[18] K. A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), 431–476.

[19] M. H. Şengün and S. Siksek, *On the asymptotic Fermat's Last Theorem over numbers fields*, Commentarii Mathematici Helvetici **93** (2018), 359–375.

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

[21] J. H. Silverman, *The Arithmetic of Elliptic Curves*, GTM **106**, Springer, 1986.

[22] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, GTM **151**, Springer, 1994.

[23] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. **141** (1995), 553–572.

[24] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. of Math. **141** (1995), 443–551.