LOCAL CRITERIA FOR THE UNIT EQUATION AND THE ASYMPTOTIC FERMAT'S LAST THEOREM

NUNO FREITAS, ALAIN KRAUS, AND SAMIR SIKSEK

Abstract. Let F be a totally real number field of odd degree. We prove several purely local criteria for the asymptotic Fermat's Last Theorem to hold over F, and also for the non-existence of solutions to the unit equation over F. For example, if 2 totally ramifies and 3 splits completely in F, then the asymptotic Fermat's Last Theorem holds over F.

1. Introduction

Let F be a number field. The **asymptotic Fermat's Last Theorem over** F is the statement that there exists a constant B_F, depending only on F, such that, for all primes $\ell > B_F$, the only solutions to the equation $x^\ell + y^\ell + z^\ell = 0$, with x, y, $z \in F$ satisfy $xyz = 0$. A suitable version of the ABC conjecture [1] over number fields implies asymptotic FLT for F provided F does not contain a primitive cube root of 1. The following two theorems (respectively [4, Corollary 1.1] and [5, Theorem 4]) are typical examples of recent work on asymptotic FLT.

Theorem. *Let F be a totally real number field. Suppose*

(i) h_F^+ is odd, where h_F^+ denotes the narrow class number of F;
(ii) 2 is totally ramified in F.

Then the asymptotic Fermat's Last Theorem holds for F.

Theorem. *Let F be a totally real number field and $p \geq 5$ a rational prime. Suppose*

(i) $F/\mathbb{Q}$ is a Galois extension of degree p^m for some $m \geq 1$;
(ii) p is totally ramified in F;
(iii) 2 is inert in F.

Then the asymptotic Fermat's Last Theorem holds for F.

These theorems and others give asymptotic FLT for families of number fields subject to restrictions on the class group, or on the Galois group. The purpose of this paper is to establish the following three theorems.

Theorem 1. *Let F be a totally real number field of degree n, and let $p \geq 5$ be a prime. Suppose*

(a) $\gcd(n, p-1) = 1$;
(b) 2 is either inert or totally ramifies in F;

Date: February 17, 2021.
2010 *Mathematics Subject Classification.* Primary 11D41.
Key words and phrases. Fermat, unit equation.
Freitas is supported by a Ramón y Cajal fellowship with reference RYC-2017-22262. Siksek is supported by the EPSRC grant *Moduli of Elliptic curves and Classical Diophantine Problems* (EP/S031537/1).

(c) p totally ramifies in F.

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

Theorem 2. *Let F be a totally real number field of degree n. Suppose*

(a) $n \equiv 1$ or $5 \pmod 6$;
(b) 2 is inert in F;
(c) 3 totally splits in F.

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

Theorem 3. *Let F be a totally real number field of degree n. Suppose*

(a) n is odd;
(b) 2 totally ramifies in F;
(c) 3 totally splits in F.

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

As far as we are aware, Theorems 1, 2 and 3 are the first in the literature giving sufficient criteria for asymptotic FLT where the criteria (apart from restrictions on the degree) are purely local.

Denote the ring of integers of F by $\mathcal{O}_F$, and the unit group of $\mathcal{O}_F$ by $\mathcal{O}_F^\times$. Associated to F is its unit equation,

$$\lambda + \mu = 1, \quad \lambda,\ \mu \in \mathcal{O}_F^\times. \tag{1}$$

A key step in the proofs of Theorems 1 and 2 is to rule out the existence of solutions to the unit equation. For the fields appearing in the statement of Theorem 1 this is furnished by the following theorem.

Theorem 4. *Let F be a number field of degree n, and let $p \geq 5$ be a prime. Suppose*

(i) $\gcd(n, (p-1)/2) = 1$;
(ii) p is totally ramified in F.

Then the unit equation (1) *has no solutions.*

The following remarkable theorem of Triantafillou [7] rules out solutions to the unit equation for the fields appearing in the statement of Theorem 2.

Theorem 5 (Triantafillou)**.** *Let F be a number field of degree n. Suppose*

(i) $3 \nmid n$;
(ii) 3 totally splits in F.

Then the unit equation (1) *has no solutions.*

Note the similarities in the statements of Theorems 4 and 5: assumptions (i) in both are restrictions on the degree, and assumptions (ii) in both are purely local. Despite the vast literature surrounding unit equations (see [3] for an extensive survey), the subject of local obstructions to solutions has received little attention.

We do not expect a common generalization of Theorems 4 and 5. For example, if we let $K = \mathbb{Q}(\sqrt{-3})$ then the unit equation has the solution $(\lambda, \mu) = ((1+\sqrt{-3})/2, (1-\sqrt{-3})/2)$, showing that Theorem 4 is false for $p = 3$, and that Theorem 5 is no longer valid if we allow 3 to ramify instead of splitting. Another interesting example, given in [5], is furnished by the number field $K = \mathbb{Q}(\theta)$ with $\theta^3 - 6\theta^2 + 9\theta - 3$. Here 3 is totally ramified and the unit equation has 18 solutions including $(\lambda, \mu) = (2-\theta, -1+\theta)$. As Triantafillou [7, Remark 3] points out, Theorem 5 no longer holds if 3 is replaced by 5.

We now come to the other main ingredient needed for the proofs of Theorems 1, 2 and 3. Suppose 2 is either inert or totally ramified in F, and write $\mathfrak{q}$ for the unique prime ideal above 2, and let $S = \{\mathfrak{q}\}$. We write $\mathcal{O}_S$ for the ring of S-integers of F, and $\mathcal{O}_S^\times$ for the group of S-units. We consider the S-unit equation

$$\lambda + \mu = 1, \qquad \lambda,\ \mu \in \mathcal{O}_S^\times, \tag{2}$$

The following is a special case of [6, Theorem 3], which gives a criterion for asymptotic FLT in terms of the solutions to (2).

Theorem 6. *Let F be a totally real number field. Assume that 2 is inert or totally ramified in F, write $\mathfrak{q}$ for the unique prime ideal above 2, and let $S = \{\mathfrak{q}\}$. If 2 is totally ramified in F, suppose that every solution (λ, μ) to (2) satisfies*

$$\max\{|\mathrm{ord}_{\mathfrak{q}}(\lambda)|,\ |\mathrm{ord}_{\mathfrak{q}}(\mu)|\} \leq 4\,\mathrm{ord}_{\mathfrak{q}}(2). \tag{3}$$

If 2 is inert in F, suppose that F has odd degree and that every solution (λ, μ) to (2) satisfies

$$\max\{|\mathrm{ord}_{\mathfrak{q}}(\lambda)|,\ |\mathrm{ord}_{\mathfrak{q}}(\mu)|\} \leq 4, \qquad \mathrm{ord}_{\mathfrak{q}}(\lambda\mu) \equiv 1 \pmod 3. \tag{4}$$

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

The proof [6] of this theorem exploits the strategy of Frey, Serre, Ribet, Wiles and Taylor, utilized in Wiles' proof [8] of Fermat's Last Theorem, and builds on many deep results including Merel's uniform boundedness theorem, and modularity lifting theorems due to Barnett-Lamb, Breuil, Diamond, Gee, Geraghty, Kisin, Skinner, Taylor, Wiles, and others.

The paper is organized as follows. In Section 2 we prove Theorem 4. In Section 3 we introduce a lemma that allows us to replace an arbitrary solution to the S-unit equation (2) with an integral solution. In Section 4 we prove Theorem 1. In Section 5 we give a quick proof of Triantafillou's theorem (Theorem 5). This is partly for the convenience of the reader, but also because some of the details implicit in Triantafillou's paper [7] are needed for the proofs of Theorems 2 and 3. In Section 6 we give proofs of Theorems 2 and 3. In Section 7 we give a conjectural generalization of Theorems 1 and 3 to number fields that are not totally real.

We are grateful to Alex Bartel for useful discussions, and to the referees for suggesting several improvements.

2. Proof of Theorem 4

In this section F is a number field of degree n, and p is a prime that totally ramifies in F. We write $\mathfrak{p}$ for the unique prime of $\mathcal{O}_F$ above p.

Lemma 2.1. *Let $\lambda \in \mathcal{O}_F$. Write $C_{F,\lambda}(X) \in \mathbb{Z}[X]$ for the characteristic polynomial of λ. Then*

$$C_{F,\lambda}(X) \equiv (X - b)^n \mod p\mathbb{Z}[X] \tag{5}$$

where $b \in \mathbb{Z}$ satisfies $\lambda \equiv b \pmod{\mathfrak{p}}$.

Proof. Note that $\mathcal{O}_F/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}$. Hence there is some $b \in \mathbb{Z}$ such that $\lambda \equiv b \pmod{\mathfrak{p}}$.

Let L be the normal closure of $F/\mathbb{Q}$. Note that $p\mathcal{O}_F = \mathfrak{p}^n$. Hence $p\mathcal{O}_L = (\mathfrak{p}\mathcal{O}_L)^n$. Let $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. Applying σ to the previous equality gives

$$(\sigma(\mathfrak{p}\mathcal{O}_L))^n = \sigma(p\mathcal{O}_L) = p\mathcal{O}_L = (\mathfrak{p}\mathcal{O}_L)^n.$$

By unique factorization of ideals, $\sigma(\mathfrak{p}\mathcal{O}_L) = \mathfrak{p}\mathcal{O}_L$. Applying σ to $\lambda \equiv b \pmod{\mathfrak{p}\mathcal{O}_L}$ we find $\sigma(\lambda) \equiv b \pmod{\mathfrak{p}\mathcal{O}_L}$.

Now let $\lambda_1, \ldots, \lambda_n$ be the roots in L of the characteristic polynomial $C_{F,\lambda}(X)$. Since $C_{F,\lambda}$ is a power of the minimal polynomial of λ, the λ_i are all conjugates of λ. Therefore $\lambda_i \equiv b \pmod{\mathfrak{p}\mathcal{O}_L}$ for all i. Thus

$$C_{F,\lambda}(X) = (X-\lambda_1)(X-\lambda_2)\cdots(X-\lambda_n) \equiv (X-b)^n \mod \mathfrak{p}\mathcal{O}_L[X].$$

However $C_{F,\lambda}(X)$ and $(X-b)^n$ both belong to $\mathbb{Z}[X]$. This gives (5). □

Lemma 2.2. *Let $\lambda \in \mathcal{O}_F$, and let $b \in \mathbb{Z}$ satisfy $\lambda \equiv b \pmod{\mathfrak{p}}$. Then*

$$\mathrm{Norm}_{F/\mathbb{Q}}(\lambda) \equiv b^n \pmod{p}.$$

Proof. We obtain this immediately on comparing constant coefficients in (5). □

Lemma 2.3. *Suppose p is odd, and that $\gcd(n,(p-1)/2) = 1$. Let $\lambda \in \mathcal{O}_F^\times$. Then $\lambda \equiv \pm 1 \pmod{\mathfrak{p}}$.*

Proof. Our assumption $\gcd(n,(p-1)/2) = 1$ is equivalent to the existence of integers u, v so that $un + v(p-1)/2 = 1$. Let $b \in \mathbb{Z}$ satisfy $\lambda \equiv b \pmod{\mathfrak{p}}$. By Lemma 2.2 and the fact that λ is a unit, $b^n \equiv \pm 1 \pmod{p}$. However, $b^{(p-1)/2} \equiv \pm 1 \pmod{p}$. It follows that

$$b \;\equiv\; (b^n)^u \cdot \left(b^{(p-1)/2}\right)^v \;\equiv\; \pm 1 \pmod{p}.$$

Therefore $\lambda \equiv \pm 1 \pmod{\mathfrak{p}}$. □

Proof of Theorem 4. Let F be a number field of degree n and let $p \geq 5$ be a prime that totally ramifies in F, and such that $\gcd(n,(p-1)/2) = 1$. Let (λ,μ) be a solution to the unit equation (1). By Lemma 2.3, we see that $\lambda \equiv \pm 1 \pmod{\mathfrak{p}}$ and $\mu \equiv \pm 1 \pmod{\mathfrak{p}}$. Thus $1 = \lambda + \mu \equiv \pm 1 \pm 1 \pmod{\mathfrak{p}}$. As $p \neq 3$, this is impossible. □

3. A simplifying lemma

Let F be a number field in which 2 is either inert or totally ramified. We write $\mathfrak{q}$ for the unique prime above 2 and let $S = \{\mathfrak{q}\}$. To deduce Theorems 1, 2 and 3 from Theorem 6 we need strong control of the solutions to the S-unit equation (2). The following lemma facilitates this by allowing us replace arbitrary solutions by integral ones.

Lemma 3.1. *Let (λ,μ) be a solution to the S-unit equation (2), and write*

$$m_{\lambda,\mu} = \max\{|\mathrm{ord}_{\mathfrak{q}}(\lambda)|,\ |\mathrm{ord}_{\mathfrak{q}}(\mu)|\}. \tag{6}$$

Then there is a solution (λ',μ') to (2) with

$$\lambda' \in \mathcal{O}_F \cap \mathcal{O}_S^\times, \qquad \mu' \in \mathcal{O}_F^\times, \qquad m_{\lambda',\mu'} = m_{\lambda,\mu}.$$

Proof. Let (λ,μ) be a solution to (2). If $\mathrm{ord}_{\mathfrak{q}}(\lambda) = \mathrm{ord}_{\mathfrak{q}}(\mu) = 0$ then $\lambda,\ \mu \in \mathcal{O}_F^\times$ and we take $\lambda' = \lambda$ and $\mu' = \mu$. If $\mathrm{ord}_{\mathfrak{q}}(\lambda) > 0$ then the relation $\lambda + \mu = 1$ forces $\mathrm{ord}_{\mathfrak{p}}(\mu) = 0$. In this case we have $\lambda \in \mathcal{O}_F$, $\mu \in \mathcal{O}_F^\times$ and we again take $\lambda' = \lambda$ and $\mu' = \mu$. If $\mathrm{ord}_{\mathfrak{q}}(\mu) > 0$ then we take $\lambda' = \mu$ and $\mu' = \lambda$. We have therefore reduced to the case where $\mathrm{ord}_{\mathfrak{q}}(\lambda) < 0$ and $\mathrm{ord}_{\mathfrak{q}}(\mu) < 0$. From the relation $\lambda + \mu = 1$ we have $\mathrm{ord}_{\mathfrak{q}}(\lambda) = \mathrm{ord}_{\mathfrak{q}}(\mu) = -t$ for some positive $t = m_{\lambda,\mu}$. In this case the lemma follows on choosing $\lambda' = 1/\lambda$, $\mu' = -\mu/\lambda$. □

4. Proof of Theorem 1

In this section we suppose that F and p satisfy the hypotheses of Theorem 1. Namely, F is a totally real field of degree n such that 2 is either inert or totally ramifies in F, and $p \geq 5$ is a prime totally ramified in F and satisfying $\gcd(n, p-1) = 1$. As before we take $\mathfrak{q}$ to be the unique prime above 2 and $S = \{\mathfrak{q}\}$, and we write $\mathfrak{p}$ for the unique prime above p.

Lemma 4.1. *Every solution (λ, μ) to the S-unit equation (2) satisfies*

$$m_{\lambda,\mu} < 2\,\mathrm{ord}_{\mathfrak{q}}(2),$$

where $m_{\lambda,\mu}$ is defined in (6).

Proof. Suppose that $m_{\lambda,\mu} \geq 2\,\mathrm{ord}_{\mathfrak{q}}(2)$. By Lemma 3.1, there is a solution (λ', μ') to the S-unit equation (2) with $\lambda' \in \mathcal{O}_F \cap \mathcal{O}_S^\times$ and $\mu' \in \mathcal{O}_F^\times$ so that $\mathrm{ord}_{\mathfrak{q}}(\lambda') = m_{\lambda',\mu'} = m_{\lambda,\mu} \geq 2\,\mathrm{ord}_{\mathfrak{q}}(2)$. Since $\mu' = 1 - \lambda'$ we see that $\mu' \equiv 1 \pmod 4$. Hence $\mathrm{Norm}_{F/\mathbb{Q}}(\mu') \equiv 1 \pmod 4$. But $\mathrm{Norm}_{F/\mathbb{Q}}(\mu') = \pm 1$ as μ' is a unit. Hence $\mathrm{Norm}_{F/\mathbb{Q}}(\mu') = 1$.

Next we utilize the assumption $\gcd(n, p-1) = 1$. From Lemma 2.3, we have $\mu' \equiv \pm 1 \pmod{\mathfrak{p}}$. If $\mu' \equiv 1 \pmod{\mathfrak{p}}$ then $\lambda' = 1 - \mu' \equiv 0 \pmod{\mathfrak{p}}$ and this gives a contradiction, since $\lambda' \in \mathcal{O}_S^\times$ and $\mathfrak{p} \notin S$. Thus $\mu' \equiv -1 \pmod{\mathfrak{p}}$. But as $\gcd(n, p-1) = 1$, the degree n is odd. By Lemma 2.2 we have $\mathrm{Norm}_{F/\mathbb{Q}}(\mu') \equiv (-1)^n \equiv -1 \pmod p$ and so $\mathrm{Norm}_{F/\mathbb{Q}}(\mu') = -1$. This gives a contradiction, thereby establishing the lemma. □

Note that the S-unit equation (2) has the following three solutions $(\lambda, \mu) = (1/2, 1/2), (-1, 2), (2, -1)$. The following lemma says that if 2 is inert then every other solution must have the same valuations as these.

Lemma 4.2. *Suppose 2 is inert in F. Then every solution (λ, μ) to the S-unit equation (2) satisfies*

$$(\mathrm{ord}_{\mathfrak{q}}(\lambda), \mathrm{ord}_{\mathfrak{q}}(\mu)) \in \{(-1,-1),\ (0,1),\ (1,0)\}.$$

Proof. Let (λ, μ) be a solution to (2). From Lemma 4.1 we know that $m_{\lambda,\mu} = 0$ or 1. However if $m_{\lambda,\mu} = 0$ then (λ, μ) is a solution to the unit equation (1) and this contradicts Theorem 4. Therefore $m_{\lambda,\mu} = 1$. Now this combined with the relation $\lambda + \mu = 1$ yields the lemma. □

Proof of Theorem 1. If 2 is ramified then Lemma 4.1 ensures that every solution to (2) satisfies (3). If 2 is inert the Lemma 4.2 assures us that every solution to (2) satisfies (4). Moreover, since $\gcd(n, p-1) = 1$, the degree of F is odd. Theorem 1 follows immediately from Theorem 6. □

5. Proof of Theorem 5

The following lemma is a slight generalization of an idea that is implicit in [7].

Lemma 5.1. *Let F be a number field in which 3 splits completely. Let S be a finite set of primes of F that is disjoint from the primes above 3. Let (λ, μ) be a solution to the S-unit equation (2) with λ, $\mu \in \mathcal{O}_F$. Then*

$$\lambda \equiv \mu \equiv -1 \pmod 3.$$

Proof. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the primes of F above 3. Then $\mathcal{O}_F/\mathfrak{p}_i \cong \mathbb{F}_3$, and so the possible residue classes modulo $\mathfrak{p}_i$ are 0, 1, -1. However λ, $\mu \in \mathcal{O}_S^\times$ and $\mathfrak{p}_i \notin S$, so $\lambda \not\equiv 0 \pmod{\mathfrak{p}_i}$ and $\mu \not\equiv 0 \pmod{\mathfrak{p}_i}$. Hence $\lambda \equiv \pm 1 \pmod{\mathfrak{p}_i}$ and $\mu \equiv \pm 1 \pmod{\mathfrak{p}_i}$. But $\lambda + \mu = 1$. It follows that $\lambda \equiv \mu \equiv -1 \pmod{\mathfrak{p}_i}$. The lemma follows as $3\mathcal{O}_F$ is the product of the distinct primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. □

Proof of Theorem 5. Let F be a number field of degree n. Suppose that $3 \nmid n$ and that 3 splits completely in F. Let (λ, μ) be a solution to the unit equation (1). By Lemma 5.1, applied with $S = \emptyset$, we have $\lambda = -1 + 3\phi$, $\mu = -1 + 3\psi$ where ϕ, $\psi \in \mathcal{O}_F$. Moreover, from $\lambda + \mu = 1$ we obtain $\phi + \psi = 1$. Let $\phi_1, \ldots, \phi_n$ be the images of ϕ under the n embeddings $F \hookrightarrow \overline{F}$. As λ is a unit

$$\pm 1 = \mathrm{Norm}_{F/\mathbb{Q}}(\lambda) = (-1 + 3\phi_1) \cdots (-1 + 3\phi_n) \equiv (-1)^n + (-1)^{n-1} \cdot 3\,\mathrm{Trace}_{F/\mathbb{Q}}(\phi) \pmod 9.$$

By considering all the choices for ± 1 and $(-1)^n$, we obtain $3\,\mathrm{Trace}_{F/\mathbb{Q}}(\phi) \equiv -2$, 2 or 0 (mod 9). The first two are plainly impossible and so $\mathrm{Trace}_{F/\mathbb{Q}}(\phi) \equiv 0 \pmod 3$. Similarly $\mathrm{Trace}_{F/\mathbb{Q}}(\psi) \equiv 0 \pmod 3$. But, as $\phi + \psi = 1$,

$$n = \mathrm{Trace}_{F/\mathbb{Q}}(\phi + \psi) = \mathrm{Trace}_{F/\mathbb{Q}}(\phi) + \mathrm{Trace}_{F/\mathbb{Q}}(\psi) \equiv 0 \pmod 3,$$

giving a contradiction. □

6. Proof of Theorems 2 and 3

Proof of Theorem 2. We now prove Theorem 2. Thus we let F be a totally real field of degree $n \equiv 1$ or 5 (mod 6), and suppose that 2 is inert in F and 3 totally splits in F. As before, we write $\mathfrak{q} = 2\mathcal{O}_F$, and let $S = \{\mathfrak{q}\}$. Note that 2 and 3 do not divide the degree n. To deduce Theorem 2 from Theorem 6 all we need to do is show that every solution (λ, μ) to the S-unit equation (2) satisfies (4). Just as in the proof of Theorem 1 it is enough to show that $m_{\lambda,\mu} = 1$ for every solution (λ, μ) to (2). We know from Theorem 5 that $m_{\lambda,\mu} \neq 0$. Suppose $m_{\lambda,\mu} \geq 2$. By Lemma 3.1 there is a solution (λ', μ') to (2) such that $\lambda' \in \mathcal{O}_F$, $\mu' \in \mathcal{O}_F^\times$, and $\mathrm{ord}_{\mathfrak{q}}(\lambda') = m_{\lambda',\mu'} = m_{\lambda,\mu} \geq 2$. Thus $\mu' = 1 - \lambda' \equiv 1 \pmod 4$, and hence $\mathrm{Norm}_{F/\mathbb{Q}}(\mu') = 1$.

However, by Lemma 5.1, we have $\mu' \equiv -1 \pmod 3$ and so $\mathrm{Norm}_{F/\mathbb{Q}}(\mu') = (-1)^n = -1$ since n is odd. This gives a contradiction, and completes the proof of Theorem 2.

Proof of Theorem 3. Finally we prove Theorem 3. Thus we let F be a totally real field of odd degree n, and suppose that 2 is totally ramified in F and that 3 totally splits in F. We write $\mathfrak{q}$ for the unique prime above 2 and let $S = \{\mathfrak{q}\}$. We claim that every solution to (λ, μ) to the S-unit equation (2) satisfies $m_{\lambda,\mu} < 2\,\mathrm{ord}_{\mathfrak{q}}(2)$. Our claim combined with Theorem 6 immediately implies Theorem 3. Suppose (λ, μ) is a solution to the S-unit equation with $m_{\lambda,\mu} \geq 2\,\mathrm{ord}_{\mathfrak{q}}(2)$. By Lemma 3.1 there is a solution (λ', μ') to (2) such that $\lambda' \in \mathcal{O}_F$, $\mu' \in \mathcal{O}_F^\times$, and $\mathrm{ord}_{\mathfrak{q}}(\lambda') = m_{\lambda',\mu'} = m_{\lambda,\mu} \geq 2\,\mathrm{ord}_{\mathfrak{q}}(2)$. Thus $\mu' = 1 - \lambda' \equiv 1 \pmod 4$. The remainder of the argument is identical to that in the above proof of Theorem 2.

7. A conjectural generalization to arbitrary number fields

Theorem 6 is critical for the proofs of Theorems 1, 2 and 3. As previously mentioned, the proof of that theorem relies on the extraordinary progress in proving modularity lifting theorems over totally real fields. Unfortunately, our understanding of modularity over non-totally real number fields is largely conjectural. However, in [2], a version of Theorem 6 is established for general (as opposed to totally real) number fields assuming two standard conjectures from the Langlands programme. In this section we give versions of Theorems 1 and 3 which are valid for general number fields F, assuming those two conjectures. For the precise statements of the two conjectures, we refer to [2]; instead we give a brief indication of what they are:

- Conjecture 3.1 of [2] is a weak version of Serre's modularity conjecture for odd, absolutely irreducible, continuous 2-dimensional mod ℓ representations of $\mathrm{Gal}(\overline{F}/F)$ that are finite flat at every prime above ℓ;
- Conjecture 4.1 of [2] states that every weight 2 newform for GL_2 over F with integer Hecke eigenvalues has an associated elliptic curve over F, or a fake elliptic curve over F.

The following is a special case of [2, Theorem 1.1].

Theorem 7. *(Şengün and Siksek) Let F be a number field for which Conjectures 3.1 and 4.1 of* [2] *hold. Assume that 2 is totally ramified in F, write $\mathfrak{q}$ for the unique prime ideal above 2, and let $S = \{\mathfrak{q}\}$. Suppose that every solution (λ, μ) to* (2) *satisfies*

$$\max\{|\mathrm{ord}_{\mathfrak{q}}(\lambda)|,\ |\mathrm{ord}_{\mathfrak{q}}(\mu)|\} \leq 4\,\mathrm{ord}_{\mathfrak{q}}(2).$$

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

We note that the assumption that F is totally real played no role in the proofs of Theorems 1, 2 and 3 except when invoking Theorem 6. We also note that Theorems 6 and 7 have identical hypotheses and conclusions for the case when 2 is totally ramified in F, except for the two additional conjectural assumptions in Theorem 7. The following two theorems are proved simply by invoking Theorem 7 instead of Theorem 6 in the proofs of Theorems 1 and 3.

Theorem 8. *Let F be a number field of degree n, for which Conjectures 3.1 and 4.1 of* [2] *hold, and let $p \geq 5$ be a prime. Suppose*

(a) $\gcd(n, p-1) = 1$*;*
(b) 2 totally ramifies in F;
(c) p totally ramifies in F.

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

Theorem 9. *Let F be a number field of degree n, for which Conjectures 3.1 and 4.1 of* [2] *hold. Suppose*

(a) n is odd;
(b) 2 totally ramifies in F;
(c) 3 totally splits in F.

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

Unfortunately, we are unable to prove similar statements in the case 2 is inert. Indeed, the existence of a degree 1 prime above 2 is critical in [2] at two points. It is needed when proving that the mod ℓ representation of the Frey elliptic curve is

absolutely irreducible, which is a prerequisite for applying [2, Conjecture 3.1]. It is also needed after invoking [2, Conjecture 4.1] to rule out the possibility that a particular weight 2 newform with rational Hecke eigenvalues is associated to a fake elliptic curve. We note in passing that the Fermat equation $x^\ell + y^\ell + z^\ell = 0$ has the solution $(1, \zeta_3, \zeta_3^2)$ for all $\ell \neq 3$, where $\zeta_3 = (-1 + \sqrt{-3})/2$. The existence of this solution suggests that variants of the above theorems with 2 inert might be harder to prove.

References

[1] Jerzy Browkin. The *abc*-conjecture for algebraic numbers. *Acta Math. Sin. (Engl. Ser.)*, 22(1):211–222, 2006.

[2] Mehmet Haluk Şengün and Samir Siksek. On the asymptotic Fermat's last theorem over number fields. *Comment. Math. Helv.*, 93(2):359–375, 2018.

[3] Jan-Hendrik Evertse and Kálmán Győry. *Unit equations in Diophantine number theory*, volume 146 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2015.

[4] Nuno Freitas, Alain Kraus, and Samir Siksek. Class field theory, Diophantine analysis and the asymptotic Fermat's last theorem. *Adv. Math.*, 363:106964, 37, 2020.

[5] Nuno Freitas, Alain Kraus, and Samir Siksek. On asymptotic Fermat over $\mathbb{Z}_p$-extensions of $\mathbb{Q}$. *Algebra Number Theory*, 14(9):2571–2574, 2020.

[6] Nuno Freitas and Samir Siksek. The asymptotic Fermat's last theorem for five-sixths of real quadratic fields. *Compos. Math.*, 151(8):1395–1415, 2015.

[7] Nicholas Triantafillou. The unit equation has no solutions in number fields of degree prime to 3 where 3 splits completely, 2020.

[8] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

Departament de Matemàtiques i Informàtica, Universitat de Barcelona (UB), Gran Via de les Corts Catalanes 585, 08007 Barcelona, Spain

E-mail address: nunobfreitas@gmail.com

Sorbonne Université, Institut de Mathématiques de Jussieu - Paris Rive Gauche, UMR 7586 CNRS - Paris Diderot, 4 Place Jussieu, 75005 Paris, France

E-mail address: alain.kraus@imj-prg.fr

Mathematics Institute, University of Warwick, CV4 7AL, United Kingdom

E-mail address: s.siksek@warwick.ac.uk