Local criteria for the unit equation and the asymptotic Fermat's Last Theorem

Nuno Freitas\textsuperscript{a,1}, Alain Kraus\textsuperscript{b,1}, and Samir Siksek\textsuperscript{c,1,2}

\textsuperscript{a}Departament de Matemàtiques i Informàtica, Universitat de Barcelona, 08007 Barcelona, Spain; \textsuperscript{b}Sorbonne Université, Institut de Mathématiques de Jussieu–Paris Rive Gauche, UMR 7586 CNRS–Paris Diderot, 75005 Paris, France; and \textsuperscript{c}Mathematics Institute, University of Warwick, CV4 7AL Coventry, United Kingdom

Edited by Kenneth A. Ribet, University of California, Berkeley, CA, and approved February 16, 2021 (received for review December 23, 2020)

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 nonexistence of solutions to the unit equation over $F$. For example, if two totally ramifies and three splits completely in $F$, then the asymptotic Fermat's Last Theorem holds over $F$.

Fermat | unit equation | number field

Let $F$ be a number field. The asymptotic Fermat's Last Theorem (FLT) 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 one. The following two theorems (corollary 1.1 in ref. 2 and theorem 4 in ref. 3, respectively) 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) two 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) two 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) two is either inert or totally ramifies in $F$;

(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 $5$ (mod 6);

(b) two is inert in $F$;

(c) three 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

Significance

In the nineteenth and twentieth centuries, number theorists have intermittently attacked the Fermat equation over number fields, seeking extensions to Kummer's approach. Nowadays, it is usual to follow in the footsteps of Frey, Serre, Ribet, and Wiles, whose efforts culminated in Wiles’ proof of Fermat’s Last Theorem. Until now, theorems giving a version of Fermat's Last Theorem over a family of number fields have been marred by a restriction on the class group or the Galois group. In this paper, we prove the asymptotic Fermat's Last Theorem for some number fields of odd degree, where the restrictions are much milder and local in nature.
(a) \( n \) is odd;
(b) two totally ramifies in \( F \);
(c) three totally splits in \( F \).

Then, the asymptotic Fermat’s Last Theorem holds over \( F \).

Unlike the aforementioned examples of recent results, Theorems 1, 2, and 3 give 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 with \( F \) is its unit equation:

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

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 Eq. 1 has no solutions.

The following remarkable theorem of Triantafillou (4) 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) three totally splits in \( F \).

Then, the unit equation Eq. 1 has no solutions.

Note the similarities in the statements of Theorems 4 and 5: assumption (i) in both is restriction on the degree, and assumption (ii) in both is purely local. Despite the vast literature surrounding unit equations (ref. 5 has 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 ref. 3, is furnished by the number field \( K = \mathbb{Q}(\theta) \) with \( \theta^3 - 6\theta^2 + 9\theta - 3 \). Here, there is three totally ramified, and the unit equation has 18 solutions including \((\lambda, \mu) = (2 - \theta, -1 + \theta)\). As Triantafillou (ref. 4, remark 3) points out, Theorem 5 no longer holds if 3 is replaced by five.

We now come to the other main ingredient needed for the proofs of Theorems 1, 2, and 3. Suppose two is either inert or totally ramified in \( F \), write \( q \) for the unique prime ideal above two, and let \( S = \{ q \} \). 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

\[
\lambda + \mu = 1, \quad \lambda, \mu \in \mathcal{O}_S^\times.
\]

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

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

\[
\max_{q} |\text{ord}(\lambda)|, |\text{ord}(\mu)| \leq 4 \text{ord}(2) \tag{3}
\]

If two is inert in \( F \), suppose that \( F \) has odd degree and that every solution \((\lambda, \mu)\) to Eq. 2 satisfies

\[
\max_{q} |\text{ord}(\lambda)|, |\text{ord}(\mu)| \leq 4, \quad \text{ord}(\lambda\mu) \equiv 1 \pmod{3} \tag{4}
\]

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 (7) 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 1, we prove Theorem 4. In section 2, we introduce a lemma that allows us to replace an arbitrary solution to the \( S \)-unit equation Eq. 2 with an integral solution. In section 3, we prove Theorem 5. In section 4, 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 (4) are needed for the proofs of Theorems 2 and 3. In section 5, we give Proofs of Theorems 2 and 3. In section 6, we give a conjectural generalization of Theorems 1 and 3 to number fields that are not totally real.

1. **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 \( p \) for the unique prime of \( \mathcal{O}_F \) above \( p \).

**Lemma 1.1.** Let \( \lambda \in \mathcal{O}_F \). Write \( \mathcal{O}_{F, \lambda}(X) \in \mathbb{Z}[X] \) for the characteristic polynomial of \( \lambda \). Then,

\[
\mathcal{O}_{F, \lambda}(X) \equiv (X - b)^n \mod p\mathbb{Z}[X],
\]

where \( b \in \mathbb{Z} \) satisfies \( \lambda \equiv b \pmod{p} \).

**Proof:** Note that \( \mathcal{O}_F/p \cong \mathbb{Z}/p\mathbb{Z} \). Hence, there is some \( b \in \mathbb{Z} \) such that \( \lambda \equiv b \pmod{p} \).
Let $L$ be the normal closure of $F/Q$. Note that $pO_F = p^n$. Hence, $pO_L = (pO_L)^n$. Let $\sigma \in \text{Gal}(L/Q)$. Applying $\sigma$ to the previous equality gives

$$(\sigma(pO_L))^n = \sigma(pO_L) = pO_L = (pO_L)^n.$$ 

By unique factorization of ideals, $\sigma(pO_L) = pO_L$. Applying $\sigma$ to $\lambda \equiv b \pmod{pO_L}$, we find $\sigma(\lambda) \equiv b \pmod{pO_L}$.

Now, let $\lambda_1, \ldots, \lambda_r$ 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 $\lambda$, the $\lambda_i$ are all conjugates of $\lambda$. Therefore, $\lambda_i \equiv b \pmod{pO_L}$ for all $i$. Thus,

$$C_{F, \lambda}(X) = (X - \lambda_1)(X - \lambda_2) \cdots (X - \lambda_r) \equiv (X - b)^n \pmod{pO_L}[X].$$

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

**Lemma 1.2.** Let $\lambda \in O_F$, and let $b \in \mathbb{Z}$ satisfy $\lambda \equiv b \pmod{p}$. Then,

$$\text{Norm}(\lambda) \equiv b^n \pmod{p}.$$ 

**Proof:** We obtain this immediately on comparing constant coefficients in Eq. 5. \qed

**Lemma 1.3.** Suppose $p$ is odd and that $\gcd(n, (p - 1)/2) = 1$. Let $\lambda \in O_F^\times$. Then, $\lambda \equiv \pm 1 \pmod{p}$.

**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 $\lambda \equiv b \pmod{p}$. By Lemma 1.2 and the fact that $\lambda$ is a unit, $b^n \equiv \pm 1 \pmod{p}$. However, $b(p - 1)/2 \equiv \pm 1 \pmod{p}$. It follows that

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

Therefore, $\lambda \equiv \pm 1 \pmod{p}$. \qed

**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 $F$, such that $\gcd(n, (p - 1)/2) = 1$. Let $(\lambda, \mu)$ be a solution to the unit equation Eq. 1. By Lemma 1.3, we see that $\mu \equiv \pm 1 \pmod{p}$ and $\lambda \equiv \pm 1 \pmod{p}$. Thus, $1 = \lambda + \mu \equiv \pm 1 \pmod{p}$. As $p \neq 3$, this is impossible. \qed

### 2. A Simplifying Lemma

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

**Lemma 2.1.** Let $(\lambda, \mu)$ be a solution to the $S$-unit equation Eq. 2, and write

$$m_{\lambda, \mu} = \max\{|\text{ord}_q(\lambda)|, |\text{ord}_q(\mu)|\}.$$ 

Then, there is a solution $(\lambda', \mu')$ to Eq. 2 with

$$\lambda' \in O_F \cap O_S^\times, \quad \mu' \in O_F^\times, \quad m_{\lambda', \mu'} = m_{\lambda, \mu}.$$ 

**Proof:** Let $(\lambda, \mu)$ be a solution to Eq. 2. If $\text{ord}_q(\lambda) = \text{ord}_q(\mu) = 0$, then $\lambda, \mu \in O_S^\times$, and we take $\lambda' = \lambda$ and $\mu' = \mu$. If $\text{ord}_q(\lambda) > 0$, then the relation $\lambda + \mu = 1$ forces $\text{ord}_q(\mu) = 0$. In this case, we have $\lambda \in O_F, \mu \in O_S^\times$, and we again take $\lambda' = \lambda$ and $\mu' = \mu$. If $\text{ord}_q(\mu) > 0$, then we take $\lambda' = \mu$ and $\mu' = \lambda$. We have therefore reduced to the case where $\text{ord}_q(\lambda) < 0$ and $\text{ord}_q(\mu) < 0$. From the relation $\lambda + \mu = 1$, we have $\text{ord}_q(\lambda) = \text{ord}_q(\mu) = -t$ for some positive $t = m_{\lambda, \mu}$. In this case, the lemma follows on choosing $\lambda' = 1/\lambda$, $\mu' = -\mu/\lambda$. \qed

### 3. 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 two 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 $q$ to be the unique prime above two and $S = \{q\}$, and we write $p$ for the unique prime above $p$.

**Lemma 3.1.** Every solution $(\lambda, \mu)$ to the $S$-unit equation Eq. 2 satisfies

$$m_{\lambda, \mu} < 2 \text{ord}(2)_q.$$ 

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

**Proof:** Suppose that $m_{\lambda, \mu} \geq 2 \text{ord}(2)_q$. By Lemma 2.1, there is a solution $(\lambda', \mu')$ to the $S$-unit equation Eq. 2 with $\lambda' \in O_F \cap O_S^\times$ and $\mu' \in O_F^\times$ so that $\text{ord}_q(\lambda') = m_{\lambda', \mu'} = m_{\lambda, \mu} \geq 2 \text{ord}(2)_q$. Since $\mu' = 1 - \lambda'$, we see that $\mu' \equiv 1 \pmod{4}$. Hence, $\text{Norm}_{F/Q}(\mu') \equiv 1 \pmod{4}$. However, $\text{Norm}_{F/Q}(\mu') \equiv 1 \pmod{4}$.

Next, we utilize the assumption $\text{gcd}(n, p - 1) = 1$. From Lemma 1.3, we have $\mu' \equiv 1 \pmod{p}$. If $\mu' \equiv 1 \pmod{p}$, then $\lambda' = 1 - \mu' \equiv 0 \pmod{p}$, and this gives a contradiction since $\lambda' \in O_S^\times$ and $p \notin S$. Thus, $\mu' \equiv -1 \pmod{p}$. However, as $\text{gcd}(n, p - 1) = 1$, the degree $n$ is odd. By Lemma 1.2, we have $\text{Norm}_{F/Q}(\mu') \equiv (-1)^n \equiv -1 \pmod{p}$, and so, $\text{Norm}_{F/Q}(\mu') = -1$. This gives a contradiction, thereby establishing the lemma. \qed

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

**Lemma 3.2.** Suppose two is inert in $F$. Then, every solution $(\lambda, \mu)$ to the $S$-unit equation Eq. 2 satisfies

$$\{\text{ord}(\lambda), \text{ord}(\mu)\} \in \{(0, 1), (1, 0)\}.$$
Theorem 6: The following lemma is a slight generalization of an idea that is implicit in ref. 4.4 follows immediately from Theorem 1, and this assures us that every solution to Eq. 1 is a solution to the unit equation Eq. 2. Therefore, \( m_{\lambda, \mu} = 1 \). Now, this combined with the relation \( \lambda + \mu = 1 \) yields the lemma.

Proof of Theorem 1: If two is ramified, then Lemma 3.1 ensures that every solution to Eq. 2 satisfies Eq. 3. If two is inert, then Lemma 3.2 assures us that every solution to Eq. 2 satisfies Eq. 4. Moreover, since \( \gcd(n, p - 1) = 1 \), the degree of \( F \) is odd. Theorem 1 follows immediately from Theorem 6.

4. Proof of Theorem 5

The following lemma is a slight generalization of an idea that is implicit in ref. 4.

Lemma 4.1. Let \( F \) be a number field in which three splits completely. Let \( S \) be a finite set of primes of \( F \) that is disjoint from the primes above three. Let \( (\lambda, \mu) \) be a solution to the \( S \)-unit equation Eq. 2 with \( \lambda, \mu \in \mathcal{O}_F \). Then,

\[
\lambda \equiv \mu \equiv -1 \pmod{3}.
\]

Proof: Let \( p_1, \ldots, p_n \) be the primes of \( F \) above three. Then, \( \mathcal{O}_F / p_i \cong \mathbb{F}_3 \), and so, the possible residue classes modulo \( p_i \) are 0, 1, -1. However, \( \lambda, \mu \in \mathcal{O}_F^2 \), and \( p_i \notin S \), so \( \lambda \not\equiv 0 \pmod{p_i} \) and \( \mu \not\equiv 0 \pmod{p_i} \). Hence, \( \lambda \equiv 1 \pmod{p_i} \) and \( \mu \equiv 1 \pmod{p_i} \). However, \( \lambda + \mu = 1 \). It follows that \( \lambda \equiv \mu \equiv -1 \pmod{3} \). The lemma follows as \( 3\mathcal{O}_F \) is the product of the distinct primes \( p_1, \ldots, p_n \).

Proof of Theorem 5: Let \( F \) be a number field of degree \( n \). Suppose that \( 3 \mid n \) and that 3 splits completely in \( F \). Let \( (\lambda, \mu) \) be a solution to the unit equation Eq. 1. By Lemma 4.1, applied with \( S = \emptyset \), we have \( \lambda = -1 + 3\phi, \mu = -1 + 3\psi \), where \( \phi, \psi \in \mathcal{O}_F \). Moreover, from \( \lambda + \mu = 1 \), we obtain \( \phi + \psi = 1 \). Let \( \phi_1, \ldots, \phi_n \) be the images of \( \phi \) under the \( n \) embeddings \( F \hookrightarrow \overline{F} \). As \( \lambda \) is a unit

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

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

\[
n = \text{Trace}_{F/Q}(\phi + \psi) = \text{Trace}_{F/Q}(\phi) + \text{Trace}_{F/Q}(\psi) \equiv 0 \pmod{3},
\]

giving a contradiction.

5. Proofs 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 \( \pmod{6} \), and suppose that two is inert in \( F \) and three totally splits in \( F \). As before, we write \( q = 2\mathcal{O}_F \), and let \( S = \{ q \} \). Note that two and three do not divide the degree \( n \). To deduce Theorem 2 from Theorem 6, all we need to do is show that every solution \( (\lambda, \mu) \) to the \( S \)-unit equation Eq. 2 satisfies Eq. 4. Just as in the proof of Theorem 1, it is enough to show that \( m_{\lambda, \mu} = 1 \) for every solution \( (\lambda, \mu) \) to Eq. 2. We know from Theorem 5 that \( m_{\lambda, \mu} \neq 0 \). Suppose \( m_{\lambda, \mu} \geq 2 \). By Lemma 2.1, there is a solution \( (\lambda', \mu') \) to Eq. 2 such that \( \lambda' \in \mathcal{O}_F \), \( \mu' \in \mathcal{O}_F^2 \), and \( \text{ord}_q(\lambda') = m_{\lambda', \mu'} = m_{\lambda, \mu} \geq 2 \). Thus, \( \mu' = 1 - \lambda' \equiv 1 \pmod{4} \), and hence, \( \text{Norm}_{F/Q}(\mu') = 1 \).

However, by Lemma 4.1, we have \( \mu' \equiv -1 \pmod{3} \), and so, \( \text{Norm}_{F/Q}(\mu') \equiv (-1)^n = -1 \) 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 two is totally ramified in \( F \) and that three splits completely in \( F \). We write \( q \) for the unique prime above two and let \( S = \{ q \} \). We claim that every solution to \( (\lambda, \mu) \) to the \( S \)-unit equation Eq. 2 satisfies \( m_{\lambda, \mu} < 2 \text{ord}_q(2) \). Our claim combined with Theorem 6 immediately implies Theorem 3. Suppose \( (\lambda, \mu) \) is a solution to the \( S \)-unit equation with \( m_{\lambda, \mu} \geq 2 \text{ord}_q(2) \). By Lemma 2.1, there is a solution \( (\lambda', \mu') \) to Eq. 2 such that \( \lambda' \in \mathcal{O}_F \), \( \mu' \in \mathcal{O}_F^2 \), and \( \text{ord}_q(\lambda') = m_{\lambda', \mu'} = m_{\lambda, \mu} \geq 2 \text{ord}_q(2) \). Thus, \( \mu' = 1 - \lambda' \equiv 1 \pmod{4} \). The remainder of the argument is identical to that in the above proof of Theorem 2.

6. 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 not totally real number fields is largely conjectural. However, in ref. 8, a version of Theorem 6 is established for general (as opposed to totally real) number fields assuming two standard conjectures from the Langlands program. 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 ref. 8; instead, we give a brief indication of what they are:

- Conjecture 3.1 of ref. 8 is a weak version of Serre’s modularity conjecture for odd, absolutely irreducible, continuous two-dimensional mod \( \ell \) representations of \( \text{Gal} (\overline{F}/F) \) that are finite flat at every prime above \( \ell \);
- Conjecture 4.1 of ref. 8 states that every weight two newform for \( \text{GL}_2 \) 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 ref. 8, Theorem 1.1.

Theorem 7 (Szegö and Siksek). Let \( F \) be a number field for which conjectures 3.1 and 4.1 of ref. 8 hold. Assume that two is totally ramified in \( F \), write \( q \) for the unique prime ideal above two, and let \( S = \{ q \} \). Suppose that every solution \( (\lambda, \mu) \) to Eq. 2 satisfies

\[
\max \{ \left| \text{ord}_q(\lambda) \right|, \left| \text{ord}_q(\mu) \right| \} \leq 4 \text{ord}_q(2).
\]

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 two 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 ref. 8 hold, and let $p \geq 5$ be a prime. Suppose

(a) $\gcd(n, p - 1) = 1$;
(b) two 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 ref. 8 hold. Suppose

(a) $n$ is odd;
(b) two totally ramifies in $F$;
(c) three 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 two is inert. Indeed, the existence of a degree one prime above two is critical in ref. 8 at two points. It is needed when proving that the mod $\ell$ representation of the Frey elliptic curve is absolutely irreducible, which is a prerequisite for applying conjecture 3.1 in ref. 8. It is also needed after invoking conjecture 4.1 in ref. 8 to rule out the possibility that a particular weight two newform with rational Hecke eigenvalues is associated with a fake elliptic curve. We note in passing that the Fermat equation $x^\ell + y^\ell + z^\ell = 0$ has the solution $(1, \zeta_3, \zeta_2^2)$ 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 two inert might be harder to prove.

**Data Availability.** There are no data underlying this work.

**ACKNOWLEDGMENTS.** We thank Alex Bartel for useful discussions and the referees for suggesting several improvements. N.F. is supported by Ramón y Cajal Fellowship RYC-2017-22262. S.S. is supported by the Engineering and Physical Sciences Research Council Grant Moduli of Elliptic Curves and Classical Diophantine Problems EP/S031537/1.

1. J. Browkin, The abc-conjecture for algebraic numbers. Acta Math. Sin. 22, 211–222 (2006).
2. N. Freitas, A. Kraus, S. Siksek, Class field theory, Diophantine analysis and the asymptotic Fermat’s last theorem. Adv. Math. 363, 106964 (2020).
3. N. Freitas, A. Kraus, S. Siksek, On asymptotic Fermat over $\mathbb{Q}_p$-extensions of $\mathbb{Q}$. Algebra Number Theor. 14, 2571–2574 (2020).
4. N. Triantafillou, The unit equation has no solutions in number fields of degree prime to 3 where 3 splits completely. arXiv [Preprint] (2020). https://arxiv.org/abs/2003.02414 (Accessed 5 March 2021).
5. J. H. Evertse, K. Györy, Unit Equations in Diophantine Number Theory (Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, United Kingdom, 2015), vol. 146.
6. N. Freitas, S. Siksek, The asymptotic Fermat’s last theorem for five-sixths of real quadratic fields. Compos. Math. 151, 1395–1415 (2015).
7. A. Wiles, Modular elliptic curves and Fermat’s last theorem. Ann. Math. 141, 443–551 (1995).
8. M. H. Şengün, S. Siksek, On the asymptotic Fermat’s last theorem over number fields. Comment Math. Helv. 93, 359–375 (2018).