ON THE ASYMPTOTIC FERMAT’S LAST THEOREM

NUNO FREITAS AND SAMIR SIKSEK

Abstract. Let $K$ be a number field having odd narrow class number and a unique prime $\lambda$ above 2. Inspired by recent work of Kraus, we prove that there are no elliptic curves defined over $K$ with conductor $\lambda$ and a $K$-rational 2-torsion point.

Furthermore, in the case of $K$ a totally real field where 2 is totally ramified, we establish the asymptotic Fermat’s Last Theorem over $K$. As another consequence, we prove the effective asymptotic Fermat’s Last Theorem for the infinite family of fields $K = \mathbb{Q}(\zeta_{2^r})^+$ where $r \geq 2$.

1. Introduction

Let $K$ be a totally real field, and let $\mathcal{O}_K$ be its ring of integers. The Fermat equation with exponent $p$ over $K$ is the equation

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

A solution $(a, b, c)$ of (1) is called trivial if $abc = 0$, otherwise non-trivial. The asymptotic Fermat’s Last Theorem over $K$ is the statement that there is a bound $B_K$, depending only on the field $K$, such that for all primes $p > B_K$, all solutions to (1) are trivial. If $B_K$ is effectively computable, we shall refer to this as the effective asymptotic Fermat’s Last Theorem over $K$. In [1], we give a criterion for asymptotic FLT in terms of solutions of a certain $S$-unit equation, where the set $S$ is the set of primes of $K$ above 2. The proof of this criterion is a generalization of Wiles’ celebrated proof of Fermat’s Last Theorem [8] over $\mathbb{Q}$, and builds on many deep results, including modularity lifting theorems over totally real fields due to Kisin, Gee and others, Merel’s uniform boundedness theorem, and Faltings’ theorem for rational points on curves of genus $\geq 2$. Naturally the criterion is simpler to apply if $S$ consists of precisely one element. In this special case, Kraus established asymptotic FLT over many explicit totally real fields of degrees $\leq 8$, by translating our criterion into an easier to check congruence condition on certain Hilbert modular forms ([5, Théorème 2]). Based on his extensive experimentation, he also posed the following conjecture:

Conjecture (Kraus). Let $K$ be a totally real number field with narrow class number 1. Suppose 2 is totally ramified in $K$ and write $\mathfrak{P}$ for the unique prime above 2. Then there are no elliptic curves over $K$ with full 2-torsion and conductor $\mathfrak{P}$.
Furthermore, using the results of [1] he showed that this conjecture implies asymptotic FLT over \( K \) without further assumptions. In this paper we prove Kraus’ conjecture in the following generalized form.

**Theorem 1.** Let \( \ell \) be a rational prime. Let \( K \) be a number field satisfying the following conditions:

(i) \( \mathbb{Q}(\zeta_\ell) \subseteq K \), where \( \zeta_\ell \) is a primitive \( \ell \)-th root of unity;

(ii) \( K \) has a unique prime \( \lambda \) above \( \ell \);

(iii) \( \gcd(h^+_K, \ell(\ell - 1)) = 1 \) where \( h^+_K \) is the narrow class number of \( K \).

Then there is no elliptic curve \( E/K \) with conductor \( \lambda \) and a \( K \)-rational \( \ell \)-isogeny.

As we shall explain, the proof of Kraus’ conjecture removes the need to solve an \( S \)-unit equation or compute Hilbert modular forms of a certain level over \( K \). Such computations quickly become unmanageable as the degree or discriminant of the field grows; this is a major obstruction to attacking Diophantine problems through Galois representations. In particular, without further computations, we will deduce from Theorem 1 the following two Diophantine applications.

**Theorem 2.** Let \( K \) be a totally real field satisfying the following two hypotheses:

(a) \( 2 \) totally ramifies in \( K \);

(b) \( K \) has odd narrow class number.

Then the asymptotic Fermat’s Last Theorem holds over \( K \). Moreover, if all elliptic curves over \( K \) with full 2-torsion are modular, then the effective asymptotic Fermat’s Last Theorem holds over \( K \).

Let \( r \geq 2 \), and let \( \zeta_{2^r} \) be a primitive \( 2^r \)-th root of unity. Write \( \mathbb{Q}(\zeta_{2^r})^r \) for the maximal real subfield of the cyclotomic field \( \mathbb{Q}(\zeta_{2^r}) \).

**Theorem 3.** The effective asymptotic Fermat’s Last Theorem holds over \( \mathbb{Q}(\zeta_{2^r})^r \).

Of course if \( r = 2 \) then \( K = \mathbb{Q} \) and if \( r = 3 \) then \( K = \mathbb{Q}(\sqrt{2}) \). In these cases Theorem 3 is known in the stronger (non-asymptotic) form and is due respectively to Wiles [8] and to Jarvis and Meekin [3]. For \( r = 4, 5 \), it is proved by Kraus [5, Théorème 9] with small explicit bounds \( B_K \) on the exponent \( p \). The deduction of Theorem 3 rests on two beautiful key ingredients:

- A well-known special case [2] of the Iwasawa Growth Formula for the \( p \)-part of the class number of layers in a \( \mathbb{Z}_p \)-extension.
- A theorem of Thorne [4] asserting modularity of elliptic curves over \( \mathbb{Z}_p \)-extensions of \( \mathbb{Q} \).

### 2. Proof of Theorem 1

Suppose \( K \) satisfies conditions (i)–(iii) and let \( E/K \) be an elliptic curve of conductor \( \lambda \) and having a \( K \)-rational \( \ell \)-isogeny. Let \( G_K = \text{Gal}(\overline{K}/K) \), write \( T_\ell(E) \) for the \( \ell \)-adic Tate module of \( E \), and let

\[
\rho = \rho_{E, \ell}\colon G_K \to \text{GL}(T_\ell(E))
\]

be the representation induced by the action of \( G_K \). We shall show that this representation is reducible. As \( E \) does not have complex multiplication (it has a multiplicative prime) this contradicts Serre’s Open Image Theorem [6, Chapter IV], completing the proof.
As $E$ has multiplicative reduction at $\lambda$, the theory of the Tate curve tells us (c.f. [2] Exercise V.5.13] that there is some choice of basis elements $P, Q \in T_\ell(E)$ such that
\begin{equation}
\rho|_{I_\lambda} = \begin{pmatrix} \chi_{\ell^n} & * \\ 0 & 1 \end{pmatrix}
\end{equation}
where $I_\lambda$ is an inertia subgroup of $G_K$ at $\lambda$, and $\chi_{\ell^n} : G_K \rightarrow \mathbb{Z}_\ell^*$ is the $\ell$-adic cyclotomic character. Fixing this choice of basis $P, Q$, we will show inductively that, as a representation of $G_K$, we have
\begin{equation}
\rho \equiv \begin{pmatrix} \chi_{\ell^n} & * \\ 0 & 1 \end{pmatrix} \pmod{\ell^n}
\end{equation}
for all $n \geq 1$, where $\chi_{\ell^n}$ is the mod $\ell^n$ cyclotomic character. Hence $\rho$ is reducible.

We start with the case $n = 1$. Write $\overline{\rho}$ for $\rho$ modulo $\ell$. As $E$ has an $\ell$-isogeny, we know that $\overline{\rho}^n = \psi_1 \oplus \psi_2$ where $\psi_1, \psi_2$ are characters $G_K \rightarrow \mathbb{F}_\ell^*$. From [2], the restriction of this to $I_\lambda$ is $\chi_{\ell} \oplus 1 = 1 \oplus 1$ as $\mathbb{Q}(\zeta_\ell) \subseteq K$. Thus $\psi_1, \psi_2$ are unramified at $\lambda$. Since $E$ has good reduction away from $\lambda$, by Néron–Ogg–Shafarevich [7 Proposition IV.10.3], the characters $\psi_1, \psi_2$ are unramified at all the finite primes. As the narrow class number of $K$ is coprime to $\ell - 1$ (assumption (iii)), and the characters $\psi_1, \psi_2$ have order dividing $\ell - 1$, they are trivial. We conclude that either $\overline{\rho}$ is trivial or, for some choice of basis for $E[\ell]$, $\overline{\rho} \sim \begin{pmatrix} 1 & \phi \\ 0 & 1 \end{pmatrix}$

where $\phi : G_K \rightarrow \mathbb{F}_\ell$ is a non-trivial additive character. If $\overline{\rho}$ is trivial clearly [3] holds for $n = 1$, so we can assume $\overline{\rho}$ is non-trivial. The character $\phi$ has order $\ell$ and is unramified away from $\lambda$ and the infinite primes. As $\ell \nmid h_K^+$ (assumption (iii)) and $\phi$ is non-trivial we deduce that $\phi|_{I_\lambda}$ is non-trivial. Thus there is a unique subgroup of $E[\ell]$ of order $\ell$ that is stable under $I_\lambda$. This must be $(P_1)$, where $P_1$ denotes the mod $\ell$ component of $P$. This completes the proof of [3] for $n = 1$.

Now suppose $n \geq 2$. By the inductive hypothesis,
\begin{equation}
\rho \equiv \begin{pmatrix} \chi_{\ell^n} + \ell^{n-1} \phi & * \\ \ell^{n-1} \psi & 1 + \ell^{n-1} \eta \end{pmatrix} \pmod{\ell^n}
\end{equation}
where $\phi, \psi, \eta$ are functions $G_K \rightarrow \mathbb{Z}/\ell\mathbb{Z}$. Let $\sigma, \tau \in G_K$. Comparing the expressions modulo $\ell^n$ for $\rho(\sigma \tau)$ with $\rho(\sigma)\rho(\tau)$ we obtain
\begin{equation}
\psi(\sigma \tau) \equiv \psi(\sigma)\chi_{\ell^n}(\tau) + \psi(\tau) \equiv \psi(\sigma) + \psi(\tau) \pmod{\ell};
\end{equation}

here we have used the fact that $\chi_{\ell^n} \equiv 1$ (mod $\ell$) and also the fact that $\chi_{\ell} = 1$ as $\mathbb{Q}(\zeta_\ell) \subseteq K$. Thus $\psi : G_K \rightarrow \mathbb{Z}/\ell\mathbb{Z}$ is an additive character of $G_K$. By [2], $\psi$ is unramified at $\lambda$. Again the assumptions force $\psi = 0$.

Comparing $\rho(\sigma \tau)$ with $\rho(\sigma)\rho(\tau)$ once more we obtain
\begin{equation}
\eta(\sigma \tau) \equiv \eta(\sigma) + \eta(\tau) \pmod{\ell},
\end{equation}
and deduce that $\eta = 0$. The fact that the determinant of $\rho$ modulo $\ell^n$ must be $\chi_{\ell^n}$ now completes the proof of [3].
3. Proof of Theorem 2

The following is a special case of [11, Theorem 9]. See also the remark after the proof of [11, Theorem 9].

**Theorem 4.** Let $K$ be a totally real field such that $2$ is totally ramified in $K$. Let $\mathfrak{p}$ be the unique prime of $K$ above $2$. There is a constant $B_K$ depending only on $K$ such that the following holds. If the Fermat equation [11] has a non-trivial solution with prime exponent $p > B_K$ then there is an elliptic curve $E'/K$ satisfying the following three properties:

(i) $E'$ has full $2$-torsion;
(ii) $E'$ has potentially good reduction away from $\mathfrak{p}$;
(iii) $E'$ has potentially multiplicative reduction at $\mathfrak{p}$.

If all elliptic curves over $K$ with full $2$-torsion are modular then the constant $B_K$ is in fact effectively computable.

The following result is extracted from the statement and proof of [5, Lemme 1]. In loc. cit. Lemme 1 is important as it allows the computations of Hilbert modular forms to be performed at a level that is often smaller than the Serre conductor of the mod $p$ representation attached to the Frey curve. As we do not need the full strength of Kraus’ Lemme 1, we are able to give a simpler proof, which we include for the convenience of the reader.

**Theorem 5** (Kraus). Let $K$ be a number field such that there is a unique prime $\mathfrak{p}$ above $2$. Let $E/K$ be an elliptic curve with full $2$-torsion, potentially good reduction away from $\mathfrak{p}$, and potentially multiplicative reduction at $\mathfrak{p}$. Then there is a quadratic twist $E'/K$ of $E$ with conductor $\mathfrak{p}$.

**Proof.** The elliptic curve $E$ has the form

$$E : Y^2 = X(X - a)(X + b)$$

with $a, b \in K$ and $ab(a + b) \neq 0$. Let $c = -a - b$. Then $a + b + c = 0$. Applying a permutation to $a$, $b$, $c$ allows us to suppose that $\text{ord}_\mathfrak{p}(b) \geq \text{ord}_\mathfrak{p}(c) \geq \text{ord}_\mathfrak{p}(a)$.

If this permutation is cyclic then the resulting elliptic curve is isomorphic to our original model, and if non-cyclic then it is a quadratic twist by $-1$.

Let $\lambda = -b/a$. The quadratic twist of $E$ by $-a$ is

$$E' : Y^2 = X(X + 1)(X + \lambda),$$

and also has potentially multiplicative reduction at $\mathfrak{p}$ and potentially good reduction away from $\mathfrak{p}$. We will in fact show that $E'$ has conductor $\mathfrak{p}$. In the usual notation, the invariants of $E'$ are

$$c_4 = 16(\lambda^2 - \lambda + 1), \quad c_6 = -64(1 - \lambda/2)(1 - 2\lambda)(1 + \lambda)$$

and

$$\Delta = 16\lambda^2(\lambda - 1)^2, \quad j = \frac{2^8(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

If $q$ is a prime $\neq 2$ then $\text{ord}_q(j) \geq 0$, and we easily check from the above formulae that this forces $\text{ord}_q(\Delta) = 0$. Thus the model $E'$ has good reduction away from $\mathfrak{p}$. Since $\text{ord}_\mathfrak{p}(b) \geq \text{ord}_\mathfrak{p}(c) \geq \text{ord}_\mathfrak{p}(a)$ we have $\text{ord}_\mathfrak{p}(\lambda) \geq \text{ord}_\mathfrak{p}(1 - \lambda) \geq 0$. If $\text{ord}_\mathfrak{p}(\lambda) = 0$ then $\text{ord}_\mathfrak{p}(1 - \lambda) = 0$ and so $\text{ord}_\mathfrak{p}(j) > 0$ giving a contradiction. Thus $\text{ord}_\mathfrak{p}(\lambda) = t$ with $t > 0$. Since $\text{ord}_\mathfrak{p}(j) = 8 \cdot \text{ord}_\mathfrak{p}(2) - 2t < 0$ we have $\text{ord}_\mathfrak{p}(\lambda) = t > 4 \cdot \text{ord}_\mathfrak{p}(2)$. It follows from Hensel’s Lemma that the expressions $\lambda^2 - \lambda + 1$, $1 - \lambda/2$, $1 - 2\lambda$ and $1 + \lambda$
are all \( \mathfrak{P} \)-adic squares. Thus \(-c_4/c_6\) is an \( \mathfrak{P} \)-adic square. By [7, Theorem V.5.3] the elliptic curve \( E' \) has split multiplicative reduction at \( \mathfrak{P} \), completing the proof. \( \square \)

3.1. **Proof of Theorem 2**. Let \( K \) be a totally real field satisfying assumptions (a), (b) in the statement of Theorem 2. Let \( B_K \) be as in the statement of Theorem 4. Suppose the Fermat equation (1) has a non-trivial solution \( (a,b,c) \) with prime exponent \( p > B_K \). By Theorem 4 there is an elliptic curve \( E'/K \) having full 2-torsion, potentially good reduction away from \( \mathfrak{P} \) and potentially multiplicative reduction at \( \mathfrak{P} \). By Theorem 5 this has a quadratic twist \( E''/K \) that has conductor \( \mathfrak{P} \) and full 2-torsion. As the narrow class number \( h_K^+ \) is odd (assumption (b)), this immediately contradicts Theorem 1 with \( \ell = 2 \) and \( \lambda = \mathfrak{P} \).

4. **Proof of Theorem 3**

Let \( r \geq 2 \) and \( K = \mathbb{Q}(\zeta_{2^r})^+ \). The prime 2 is totally ramified in \( K \) and we let \( \mathfrak{P} \) be the unique prime of \( K \) above 2. Let \( B_K \) be the constant in Theorem 4. As \( K \) is a subfield of the unique \( \mathbb{Z}_2 \)-extension of \( \mathbb{Q} \), it follows from Thorne [4] that all elliptic curves over \( K \) are modular. Thus the constant \( B_K \) is effectively computable. Suppose the Fermat equation (1) has a non-trivial solution with exponent \( p > B_K \). By Theorems 4 and 5 there is an elliptic curve \( E''/K \) defined over \( K \) having full 2-torsion and conductor \( \mathfrak{P} \). The class number of \( K \), and indeed of any abelian field of conductor 2 for any \( s \), is odd [2]. However we do not know if the narrow class number of \( K \) is odd. Instead let \( L = \mathbb{Q}(\zeta_{2^r}) \) which also has odd class number. As \( L \) is totally complex, the narrow class number equals the class number. Thus \( L \) has odd narrow class number. Note that 2 ramifies totally in \( L \) and let \( p \) be the unique prime above 2. Thus the base change of \( E''/L \) has conductor \( p \) and full 2-torsion. This contradicts Theorem 1 with \( \ell = 2 \) and \( \lambda = p \) and completes the proof.

**References**

[1] 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.
[2] K. Iwasawa, *A note on class numbers of algebraic number fields*, Abh. Math. Sem. Univ. Hamburg 20 (1956), 257–258.
[3] F. Jarvis and P. Meekin, *The Fermat equation over \( \mathbb{Q}(\sqrt{2}) \)*, J. Number Theory 109 (2004), no. 1, 182–196.
[4] J. Thorne, *Elliptic curves over \( \mathbb{Q}_\infty \) are modular*, to appear in JEMS.
[5] A. Kraus, *Le théorème de Fermat sur certains corps de nombres totalement réels*, arXiv:1709.08356.
[6] J.-P. Serre, *Abelian \( \ell \)-adic representations and elliptic curves*, Addison-Wesley Publ. Co., Reading, Mass., 1989.
[7] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, GTM 151, Springer, 1994.
[8] A. Wiles, *Modular elliptic curves and Fermat’s last theorem*, Ann. of Math. (2) 141 (1995), no. 3, 443–551.

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

E-mail address: nunofreitas@gmail.com

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

E-mail address: samir.siksek@gmail.com