ANNALES MATHÉMATIQUES

BLAISE PASCAL

Nuno Freitas, Alain Kraus & Samir Siksek

On asymptotic Fermat over the $\mathbb{Z}_2$-extension of $\mathbb{Q}$

Volume 28, n° 1 (2021), p. 1-6.

<http://ambp.centre-mersenne.org/item?id=AMBP_2021__28_1_1_0>

Publication éditée par le laboratoire de mathématiques Blaise Pascal
de l'université Clermont Auvergne, UMR 6620 du CNRS
Clermont-Ferrand — France

CENTRE MERSENNE

Publication membre du
Centre Mersenne pour l'édition scientifique ouverte
http://www.centre-mersenne.org/

Annales mathématiques Blaise Pascal **28**, 1-6 (2021)

On asymptotic Fermat over the $\mathbb{Z}_2$-extension of $\mathbb{Q}$

Nuno Freitas
Alain Kraus
Samir Siksek

Abstract

In a recent work the authors prove the effective asymptotic Fermat's Last Theorem for the infinite family of fields $\mathbb{Q}(\zeta_{2^{r+2}})^+$ where $r \geq 0$. A crucial step in their proof is the following conjecture of Kraus. Let K be a number field having odd narrow class number and a unique prime λ above 2. Then there are no elliptic curves defined over K with conductor λ and a K-rational point of order 2. In this note we give a new elementary proof of Kraus' conjecture that makes use only of basic facts about elliptic curves, Tate curves and Tate modules.

Le théorème de Fermat asymptotique sur la $\mathbb{Z}_2$-extension de $\mathbb{Q}$

Résumé

Les auteurs ont démontré récemment le théorème de Fermat asymptotique pour la famille infinie de corps $\mathbb{Q}\left(\zeta_{2^{r+2}}\right)^+$ avec $r \geq 0$. Un argument essentiel de la démonstration est relié à la conjecture suivante de Kraus. Soit K un corps de nombres ayant un nombre de classes restreint impair et un unique idéal premier λ au-dessus de 2. Alors il n'existe pas de courbes elliptiques définies sur K, de conducteur λ, ayant un point d'ordre 2 rationnel sur K. On présente dans cette note une nouvelle preuve élémentaire de la conjecture de Kraus, en utilisant seulement des résultats de base sur les courbes elliptiques, qui concernent les courbes de Tate et les modules de Tate.

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

$$a^p + b^p + c^p = 0, \qquad a, b, c \in \mathcal{O}_K. \tag{1.1}$$

A solution (a, b, c) of (1.1) 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 (1.1) 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] the following two theorems are established.

Freitas is supported by a Ramón y Cajal fellowship (RYC-2017-22262).
Siksek is supported by EPSRC grant *Moduli of Elliptic curves and Classical Diophantine Problems* (EP/S031537/1).
Keywords: Fermat, modularity, elliptic curves, real abelian fields.
2020 *Mathematics Subject Classification*: 11D41, 11F80, 11G05.

Theorem 1.1. *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 $r \geq 0$, and let $\zeta_{2^{r+2}}$ be a primitive 2^{r+2}-th root of unity. Write $\mathbb{Q}_{r,2} = \mathbb{Q}(\zeta_{2^{r+2}})^+$ for the maximal real subfield of the cyclotomic field $\mathbb{Q}(\zeta_{2^{r+2}})$. This is the r-th layer of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$.

Theorem 1.2. *The effective asymptotic Fermat's Last Theorem holds over $\mathbb{Q}_{r,2}$.*

Observe that $\mathbb{Q}_{0,2} = \mathbb{Q}$ and $\mathbb{Q}_{1,2} = \mathbb{Q}(\sqrt{2})$. Thus Theorem 1.2 generalizes, albeit asymptotically, both Fermat's Last Theorem over $\mathbb{Q}$ due to Wiles [8], and the corresponding theorem over $\mathbb{Q}(\sqrt{2})$ due to Jarvis and Meekin [3].

Proof of Theorem 1.2. Theorem 1.2 follows from Theorem 1.1 and the fact that $\mathbb{Q}_{r,2}$ has odd narrow class number, as shown by Iwasawa [2]. The effectivity follows as elliptic curves over $\mathbb{Z}_p$-extensions of $\mathbb{Q}$ are modular thanks to the work of Thorne [7]. ◻

The proof of Theorem 1.1 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 on rational points on curves of genus ≥ 2, and of course the strategy of Frey, Serre, Ribet, Wiles and Taylor exploited in Wiles' proof of Fermat's Last Theorem. A crucial ingredient in the proof of Theorem 1.1 is furnished by the following theorem, which had originally been a conjecture of Kraus [4].

Theorem 1.3. *Let ℓ be a rational prime. Let K be a number field satisfying the following conditions:*

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

(ii) *K has a unique prime λ above ℓ;*

(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 good reduction away from λ, potentially multiplicative reduction at λ, and a K-rational ℓ-isogeny.

In the proof of Fermat's Last Theorem, Ribet's Level Lowering Theorem asserts that the mod p representation of the Frey elliptic curve arises from a newform of weight 2 and level 2. The fact that there are no such newforms is a seemingly trivial but indeed crucial step in the proof of Fermat's Last Theorem. In the proof of Theorem 1.1, Theorem 1.3 (with $\ell = 2$) plays a similar rôle to the absence of newforms of weight 2 and level 2. For the deduction of Theorem 1.1 from Theorem 1.3 we refer to [1]. The proof of Theorem 1.1 in [1] makes heavy use of the theory of p-groups and p-extensions. In the present note we give a simpler proof of Theorem 1.3, which uses nothing beyond basic facts about elliptic curves, Tate curves and Tate modules.

2. **Proof of Theorem 1.3**

Suppose K satisfies conditions (i)–(iii). In particular there is a unique prime λ of K above ℓ. Let E/K be an elliptic curve with good reduction away from λ, potentially multiplicative reduction at λ. We derive a contradiction by studying the mod ℓ and the ℓ-adic representations of E (and those of a semistable twist). Write $G_K = \mathrm{Gal}(\overline{K}/K)$. Denote a decomposition and inertia subgroups of G_K corresponding to λ by D_λ and I_λ respectively.

We first show that E has a quadratic twist F/K with conductor λ and a K-rational ℓ-isogeny. Write $\bar{\rho}_{E,\ell}$ for the mod ℓ representation of E. By the theory of the Tate curve (c.f. [6, Exercises V.5.11 and V.5.13]): $(\bar{\rho}_{E,\ell}|_{D_\lambda})^{\mathrm{ss}} \sim \tau \cdot \chi_\ell \oplus \tau$, where χ_ℓ is the modulo ℓ cyclotomic character, and τ is a character of D_λ which is either trivial or quadratic. Moreover, the twist $E \otimes \tau$ is an elliptic curve defined over K_λ having split multiplicative reduction at λ. However, by assumption (i), χ_ℓ is trivial on G_K. Hence $(\bar{\rho}_{E,\ell}|_{D_\lambda})^{\mathrm{ss}} \sim \tau \oplus \tau$.

As E has a K-rational ℓ-isogeny, the mod ℓ representation is reducible, and we can write

$$\bar{\rho}_{E,\ell} \sim \begin{pmatrix} \theta_1 & * \\ 0 & \theta_2 \end{pmatrix}$$

where θ_1, θ_2 are characters $G_K \to \mathbb{F}_\ell^*$, and these must satisfy $\theta_1|_{I_\lambda} = \theta_2|_{I_\lambda} = \tau|_{I_\lambda}$. As τ is a quadratic character we see that θ_1^2 and θ_1/θ_2 are unramified at λ. Since E/K has good reduction away from λ, by the criterion of Néron–Ogg–Shafarevich [6, Proposition IV.10.3] the characters θ_1 and θ_2 are unramified except possibly at λ and the infinite places. We deduce that θ_1^2 and θ_1/θ_2 are characters of G_K unramified at the finite places having orders dividing $\ell - 1$. Assumption (iii) immediately implies that $\theta_1 = \theta_2$ is a quadratic character of G_K. We let F be the quadratic twist $F = E \otimes \theta_1$. Note that locally at λ the curve F/K becomes $E \otimes \tau$ and θ_1 is unramified away from λ, hence F/K

has conductor λ, and

$$\bar{\rho}_{F,\ell} \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}. \tag{2.1}$$

Write $T_\ell(F)$ for the ℓ-adic Tate module of E, and let

$$\rho = \rho_{F,\ell^\infty} : G_K \to \mathrm{GL}(T_\ell(F))$$

be the representation induced by the action of G_K.

As F has multiplicative reduction at λ, the theory of the Tate curve tells us [6, Exercise V.5.13] that there is some choice of basis elements $P, Q \in T_\ell(F)$ such that

$$\rho|_{I_\lambda} = \begin{pmatrix} \chi_{\ell^\infty} & * \\ 0 & 1 \end{pmatrix} \tag{2.2}$$

where $\chi_{\ell^\infty} : G_K \to \mathbb{Z}_\ell^\times$ is the ℓ-adic cyclotomic character. Fixing this choice of basis P, Q, we will show inductively that, as a representation of G_K, we have

$$\rho \equiv \begin{pmatrix} \chi_{\ell^n} & * \\ 0 & 1 \end{pmatrix} \pmod{\ell^n} \tag{2.3}$$

for all $n \geq 1$, where χ_{ℓ^n} is the mod ℓ^n cyclotomic character. The case $n = 1$ is already established in equation (2.1).

Now suppose $n \geq 2$ and the result holds for $n - 1$. By the inductive hypothesis,

$$\rho \equiv \begin{pmatrix} \chi_{\ell^n} + \ell^{n-1}\phi & * \\ \ell^{n-1}\psi & 1 + \ell^{n-1}\eta \end{pmatrix} \pmod{\ell^n}$$

where ϕ, ψ, η are functions $G_K \to \mathbb{Z}/\ell\mathbb{Z}$. Let $\sigma_1, \sigma_2 \in G_K$. Comparing the expressions modulo ℓ^n for $\rho(\sigma_1\sigma_2)$ with $\rho(\sigma_1)\rho(\sigma_2)$ we obtain

$$\psi(\sigma_1\sigma_2) \equiv \psi(\sigma_1)\chi_{\ell^n}(\sigma_2) + \psi(\sigma_2) \equiv \psi(\sigma_1) + \psi(\sigma_2) \pmod{\ell};$$

here we have used the fact that $\chi_{\ell^n} \equiv \chi_\ell \pmod{\ell}$ and also the fact that $\chi_\ell = 1$ as $\mathbb{Q}(\zeta_\ell) \subseteq K$. Thus $\psi : G_K \to \mathbb{Z}/\ell\mathbb{Z}$ is an additive character of G_K. By (2.2), ψ is unramified at λ, and at all other finite primes by Néron–Ogg–Shafarevich. Since ψ has order dividing ℓ assumption (iii) allows us to conclude that $\psi = 0$.

Comparing $\rho(\sigma_1\sigma_2)$ with $\rho(\sigma_1)\rho(\sigma_2)$ once more we obtain

$$\eta(\sigma_1\sigma_2) = \eta(\sigma_1) + \eta(\sigma_2) \pmod{\ell},$$

and deduce, as above, that $\eta = 0$. The fact that the determinant of ρ modulo ℓ^n must be χ_{ℓ^n} then implies $\phi = 0$, completing the proof of (2.3).

To complete the proof it remains to demonstrate a contradiction. One approach is to observe that (2.3) forces ρ to be reducible and to invoke Serre's Open Image Theorem [5, Chapter IV] for a contradiction, because F does not have complex multiplication (it has multiplicative reduction prime λ).

There is however a more elementary argument which also yields a contradiction. Let $\mathfrak{p}$ be any prime of K distinct from λ. Let P_n and Q_n be the images of P, Q in $F[\ell^n]$. From (2.3), we note the following.

- The cyclic subgroup $\langle P_n \rangle$ is fixed by G_K and therefore the isogenous elliptic curve $F_n = F/\langle P_n \rangle$ is defined over K.

- $\sigma(Q_n) = a_\sigma P_n + Q_n$ for any $\sigma \in G_K$ where $a_\sigma \in \mathbb{Z}/\ell^n\mathbb{Z}$. Thus $Q_n + \langle P_n \rangle$ is a K-point of order ℓ^n on F_n.

Since F_n has good reduction at $\mathfrak{p}$, by the injectivity of torsion under reduction we see that $\ell^n \mid \#F_n(\mathbb{F}_\mathfrak{p})$ and as F and F_n are isogenous, $\ell^n \mid \#F(\mathbb{F}_\mathfrak{p})$. This gives a contradiction for n large.

References

[1] Nuno Freitas, Alain Kraus, and Samir Siksek. Class field theory, Diophantine analysis and the asymptotic Fermat's Last Theorem. *Adv. Math.*, 363: article no. 106964, 2020.

[2] Kenkichi Iwasawa. A note on class numbers of algebraic number fields. *Abh. Math. Semin. Univ. Hamb.*, 20:257–258, 1956.

[3] Frazer Jarvis and Paul Meekin. The Fermat equation over $\mathbb{Q}(\sqrt{2})$. *J. Number Theory*, 109(1):182–196, 2004.

[4] Alain Kraus. Le théorème de Fermat sur certains corps de nombres totalement réels. *Algebra Number Theory*, 13(2):301–332, 2019.

[5] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves*. Advanced Book Classics. Addison-Wesley Publishing Group, second edition, 1989. With the collaboration of Willem Kuyk and John Labute.

[6] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer, 1994.

[7] Jack A. Thorne. Elliptic curves over $\mathbb{Q}_\infty$ are modular. *J. Eur. Math. Soc.*, 21(7):1943–1948, 2019.

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

NUNO FREITAS
Departament de Matemàtiques i Informàtica
Universitat de Barcelona (UB)
Gran Via de les Corts Catalanes 585
08007 Barcelona
Spain
nunobfreitas@gmail.com

ALAIN KRAUS
Sorbonne Université
Institut de Mathématiques de Jussieu - Paris Rive Gauche
UMR 7586 CNRS - Paris Diderot
4 Place Jussieu
75005 Paris
France
alain.kraus@imj-prg.fr

SAMIR SIKSEK
Mathematics Institute
University of Warwick
CV4 7AL
United Kingdom
s.siksek@warwick.ac.uk