Algebra & Number Theory

Volume 14
2020
No. 9

On asymptotic Fermat over $\mathbb{Z}_p$-extensions of $\mathbb{Q}$

Nuno Freitas, Alain Kraus and Samir Siksek

msp

msp

ALGEBRA AND NUMBER THEORY 14:9 (2020)
https://doi.org/10.2140/ant.2020.14.2571

On asymptotic Fermat over $\mathbb{Z}_p$-extensions of $\mathbb{Q}$

Nuno Freitas, Alain Kraus and Samir Siksek

Let p be a prime and let $\mathbb{Q}_{n,p}$ denote the n-th layer of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. We prove the effective asymptotic FLT over $\mathbb{Q}_{n,p}$ for all $n \geq 1$ and all primes $p \geq 5$ that are non-Wieferich, i.e., $2^{p-1} \not\equiv 1 \pmod{p^2}$. The effectivity in our result builds on recent work of Thorne proving modularity of elliptic curves over $\mathbb{Q}_{n,p}$.

1. Introduction

Let F be a totally real 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 $x, y, z \in F$ are the trivial ones satisfying $xyz = 0$. If B_F is effectively computable, we refer to this as the *effective asymptotic Fermat's last theorem over F*. Let p be a prime, n a positive integer and write $\mathbb{Q}_{n,p}$ for the n-th layer of the cyclotomic $\mathbb{Z}_p$-extension. In [Freitas et al. 2020], the authors established the following theorem.

Theorem 1. *The effective asymptotic Fermat's last theorem holds over each layer $\mathbb{Q}_{n,2}$ of the cyclotomic $\mathbb{Z}_2$-extension.*

The proof of Theorem 1 relies heavily on class field theory and the theory of 2-extensions, and the method depends crucially on the fact that 2 is totally ramified in $\mathbb{Q}_{n,2}$. We establish the following.

Theorem 2. *Let $p \geq 5$ be a prime. Suppose p is non-Wieferich, i.e., $2^{p-1} \not\equiv 1 \pmod{p^2}$. The effective asymptotic Fermat's last theorem holds over each layer $\mathbb{Q}_{n,p}$ of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$.*

We remark that the only Wieferich primes currently known are 1093 and 3511. It is fascinating to observe that these primes originally arose in connection with historical attempts at proving Fermat's last theorem. Indeed Wieferich [1909] showed that if $2^{p-1} \not\equiv 1 \pmod{p^2}$ then the first case of Fermat's last theorem holds for exponent p.

In contrast to Theorem 1, the proof of Theorem 2 makes use of a criterion (Theorem 3 below) established in [Freitas and Siksek 2015] for asymptotic FLT in terms of solutions to a certain S-unit equation. The proof of that criterion builds on many deep results including modularity lifting theorems due to Breuil, Diamond, Gee, Kisin, and others, and Merel's uniform boundedness theorem, and exploits the strategy of Frey, Serre, Ribet, Wiles and Taylor, utilized in Wiles' proof of Fermat's last theorem [1995]. We use elementary

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).

MSC2020: primary 11D41; secondary 11R23.

Keywords: Fermat, unit equation, $\mathbb{Z}_p$-extensions.

arguments to study these S-unit equations in $\mathbb{Q}_{n,p}$ and this study, together with the S-unit criterion, quickly yields Theorem 2. The effectivity in Theorem 2 builds on the following great theorem due to Thorne [2019].

Theorem (Thorne). *Elliptic curves over $\mathbb{Q}_{n,p}$ are modular.*

2. An S-unit criterion for asymptotic FLT

The following criterion for asymptotic FLT is a special case of [Freitas and Siksek 2015, Theorem 3].

Theorem 3. *Let F be a totally real number field. Suppose the Eichler–Shimura conjecture over F holds. Assume that 2 is inert in F and write $\mathfrak{q} = 2\mathcal{O}_F$ for the prime ideal above 2. Let $S = \{\mathfrak{q}\}$ and write $\mathcal{O}_S^\times$ for the group of S-units in F. Suppose every solution (λ, μ) to the S-unit equation*

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

satisfies both of the following conditions:

$$\max\{|\mathrm{ord}_{\mathfrak{q}}(\lambda)|, |\mathrm{ord}_{\mathfrak{q}}(\mu)|\} \le 4, \qquad \mathrm{ord}_{\mathfrak{q}}(\lambda\mu) \equiv 1 \pmod 3. \tag{2-2}$$

Then the asymptotic Fermat's last theorem holds over F. Moreover, if all elliptic curves over F with full 2-torsion are modular, then the effective asymptotic Fermat's last theorem holds over F.

For a discussion of the Eichler–Shimura conjecture see [Freitas and Siksek 2015, Section 2.4], but for the purpose of this paper we note that the conjecture is known to hold for all totally real fields of odd degree. In particular, it holds for $\mathbb{Q}_{n,p}$ for all odd p.

To apply Theorem 3 to $F = \mathbb{Q}_{n,p}$ we need to know for which p is 2 inert in F. The answer is given by the following lemma, which for $n = 1$ is [Washington 1997, Exercise 2.4].

Lemma 2.1. *Let $p \ge 3$, q be distinct primes. Then q is inert in $\mathbb{Q}_{n,p}$ if and only if $q^{p-1} \not\equiv 1 \pmod{p^2}$.*

Proof. Let $L = \mathbb{Q}(\zeta_{p^{n+1}})$ and $F = \mathbb{Q}_{n,p}$. Write σ_q and τ_q for the Frobenius elements corresponding to q in $\mathrm{Gal}(L/\mathbb{Q})$ and $\mathrm{Gal}(F/\mathbb{Q})$. The prime q is inert in F precisely when τ_q has order p^n. The natural surjection $\mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{Gal}(F/\mathbb{Q})$ sends σ_q to τ_q and its kernel has order $p-1$. Thus q is inert in F if and only if the order of σ_q is divisible by p^n, which is equivalent to σ_q^{p-1} having order p^n. There is a canonical isomorphism $\mathrm{Gal}(L/\mathbb{Q}) \to (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$ sending σ_q to $q + p^{n+1}\mathbb{Z}$. Thus q is inert in F if and only if $q^{p-1} + p^{n+1}\mathbb{Z}$ has order p^n. This is equivalent to $q^{p-1} \not\equiv 1 \pmod{p^2}$. □

3. Proof of Theorem 2

Lemma 3.1. *Let $\mathfrak{p}$ be the unique prime above p in $F = \mathbb{Q}_{n,p}$. Let $\lambda \in \mathcal{O}_F$. Then $\lambda \equiv \mathrm{Norm}_{F/\mathbb{Q}}(\lambda) \pmod{\mathfrak{p}}$.*

Proof. As p is totally ramified in F, we know that the residue field $\mathcal{O}_F/\mathfrak{p}$ is $\mathbb{F}_p$. Thus there is some $a \in \mathbb{Z}$ such that $\lambda \equiv a \pmod{\mathfrak{p}}$. Let $\sigma \in G = \mathrm{Gal}(F/\mathbb{Q})$. Since $\mathfrak{p}^\sigma = \mathfrak{p}$, we have $\lambda^\sigma \equiv a \pmod{\mathfrak{p}}$. Hence

$$\mathrm{Norm}_{F/\mathbb{Q}}(\lambda) = \prod_{\sigma \in G} \lambda^\sigma \equiv a^{\#G} \pmod{\mathfrak{p}}.$$

However $\#G = p^n$ so $\mathrm{Norm}_{F/\mathbb{Q}}(\lambda) \equiv a \equiv \lambda \pmod{\mathfrak{p}}$. □

Lemma 3.2. *Let $p \neq 3$ be a rational prime. Let $F = \mathbb{Q}_{n,p}$. Then the unit equation*

$$\lambda + \mu = 1, \quad \lambda, \mu \in \mathcal{O}_F^\times \tag{3-1}$$

has no solutions.

Proof. Let (λ, μ) be a solution to (3-1). By Lemma 3.1, $\lambda \equiv \pm 1 \pmod{\mathfrak{p}}$ and $\mu \equiv \pm 1 \pmod{\mathfrak{p}}$. Thus $\pm 1 \pm 1 \equiv \lambda + \mu = 1 \pmod{\mathfrak{p}}$. This is impossible as $p \neq 3$. □

Remark 3.3. Lemma 3.2 is false for $p = 3$. Indeed, let $p = 3$ and $n = 1$. Then $F = \mathbb{Q}_{1,3} = \mathbb{Q}(\theta)$, where θ satisfies $\theta^3 - 6\theta^2 + 9\theta - 3 = 0$. The unit equation has solution $\lambda = 2 - \theta$ and $\mu = -1 + \theta$. In fact, the unit equation solver of the computer algebra system `Magma` [Bosma et al. 1997] gives a total of 18 solutions.

Lemma 3.4. *Let $p \geq 5$ be a rational prime. Let $F = \mathbb{Q}_{n,p}$. Suppose 2 is inert in F and write $\mathfrak{q} = 2\mathcal{O}_F$ for the unique prime above 2. Let $S = \{\mathfrak{q}\}$ and write $\mathcal{O}_S^\times$ for the group of S-units. Then every solution to the S-unit equation* (2-1) *satisfies one of the following*:

(i) $\mathrm{ord}_{\mathfrak{q}}(\lambda) = 1$, $\mathrm{ord}_{\mathfrak{q}}(\mu) = 0$;

(ii) $\mathrm{ord}_{\mathfrak{q}}(\lambda) = 0$, $\mathrm{ord}_{\mathfrak{q}}(\mu) = 1$;

(iii) $\mathrm{ord}_{\mathfrak{q}}(\lambda) = \mathrm{ord}_{\mathfrak{q}}(\mu) = -1$.

Proof. Write $n_\lambda = \mathrm{ord}_{\mathfrak{q}}(\lambda)$ and $n_\mu = \mathrm{ord}_{\mathfrak{q}}(\mu)$. Suppose first $n_\lambda \geq 2$. Then $n_\mu = 0$ and so $\mu \in \mathcal{O}_F^\times$. Moreover, as $4 \mid \lambda$, we have $\mu \equiv 1 \pmod 4$ and so $\mu^\sigma \equiv 1 \pmod 4$ for all $\sigma \in G = \mathrm{Gal}(F/\mathbb{Q})$. Hence $\mathrm{Norm}_{F/\mathbb{Q}}(\mu) = \prod \mu^\sigma \equiv 1 \pmod 4$. But $\mathrm{Norm}_{F/\mathbb{Q}}(\mu) = \pm 1$, thus $\mathrm{Norm}_{F/\mathbb{Q}}(\mu) = 1$. As before, denote the unique prime above p by $\mathfrak{p}$. By Lemma 3.1 we have $\mu \equiv 1 \pmod{\mathfrak{p}}$. Hence $\mathfrak{p}$ divides $1 - \mu = \lambda$ giving a contradiction.

Thus $n_\lambda \leq 1$. Next suppose $n_\lambda \leq -2$. Then $n_\lambda = n_\mu$. Let $\lambda' = 1/\lambda$ and $\mu' = -\mu/\lambda$. Then (λ', μ') is a solution to the S-unit equation satisfying $n_{\lambda'} \geq 2$, giving a contradiction by the previous case. Hence $-1 \leq n_\lambda \leq 1$ and by symmetry $-1 \leq n_\mu \leq 1$. From Lemma 3.2 either $n_\lambda \neq 0$ or $n_\mu \neq 0$. Thus one of (i), (ii), (iii) must hold. □

Remark 3.5. Possibilities (i), (ii), (iii) cannot be eliminated because of the solutions $(2, -1)$, $(-1, 2)$ and $\left(\frac{1}{2}, \frac{1}{2}\right)$ to the S-unit equation.

Proof of Theorem 2. We suppose $p \geq 5$ and non-Wieferich. It follows from Lemma 2.1 that 2 is inert in $F = \mathbb{Q}_{n,p}$. Write $\mathfrak{q} = 2\mathcal{O}_F$. By Lemma 3.4 all solutions (λ, μ) to the S-unit equation (2-1) satisfy (2-2). We now apply Theorem 3. As elliptic curves over $\mathbb{Q}_{n,p}$ are modular thanks to Thorne's theorem, we conclude that the effective Fermat's last theorem holds over $\mathbb{Q}_{n,p}$. □

Remark 3.6. The proof of Theorem 2 for $p = 3$ and for the Wieferich primes seems out of reach at present. There are solutions to the unit equation in $\mathbb{Q}_{1,3}$ (as indicated in Remark 3.3), and therefore in $\mathbb{Q}_{n,3}$ for all n, and these solutions violate the criterion of Theorem 3. For p a Wieferich prime, 2 splits in $\mathbb{Q}_{n,p}$ into at least p prime ideals and we would need to consider the S-unit equation (2-1) with S the set of primes above 2. It appears difficult to treat the S-unit equation in infinite families of number fields where $\#S \geq 2$ (see [Freitas et al. 2020, Theorem 7] and its proof).

4. A generalization

In fact, the proof of Theorem 2 establishes the following more general theorem.

Theorem 4. *Let F be a totally real number field and $p \geq 5$ be a rational prime. Suppose that the following conditions are satisfied.*

(a) *F is a p-extension of $\mathbb{Q}$ (i.e., $F/\mathbb{Q}$ is a Galois extension of degree p^n for some $n \geq 1$).*

(b) *p is totally ramified in F.*

(c) *2 is inert in F.*

Then the asymptotic Fermat's last theorem holds for F.

Example 4.1. A quick search on the L-Functions and Modular Forms Database [LMFDB 2020] yields 153 fields of degree 5 satisfying conditions of the theorem with $p = 5$. The one with smallest discriminant is $\mathbb{Q}_{1,5}$. The one with the next smallest discriminant is $F = \mathbb{Q}(\theta)$ where $\theta^5 - 110\theta^3 - 605\theta^2 - 990\theta - 451 = 0$. The discriminant of F is $5^8 \cdot 11^4$. It is therefore not contained in any $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

References

[Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system, I: The user language", *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. See also Magma computational algebra system. MR Zbl

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

[Freitas et al. 2020] N. Freitas, A. Kraus, and S. Siksek, "Class field theory, Diophantine analysis and the asymptotic Fermat's last theorem", *Adv. Math.* **363** (2020), art. id. 106964. MR Zbl

[LMFDB 2020] The LMFDB Collaboration, "The L-functions and modular forms database", 2020, http://www.lmfdb.org.

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

[Washington 1997] L. C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Grad. Texts in Math. **83**, Springer, 1997. MR Zbl

[Wieferich 1909] A. Wieferich, "Zum letzten Fermatschen Theorem", *J. Reine Angew. Math.* **136** (1909), 293–302. MR Zbl

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

Communicated by Andrew Granville
Received 2020-04-02 Accepted 2020-05-11

nunobfreitas@gmail.com *Department de Matemàtiques i Informàtica, Universitat de Barcelona, Barcelona, Spain*

alain.kraus@imj-prg.fr *Institut de Mathématiques de Jussieu - Paris Rive Gauche, Sorbonne Université, UMR 7586 CNRS - Paris Diderot, Paris, France*

s.siksek@warwick.ac.uk *Mathematics Institute, University of Warwick, Coventry, United Kingdom*

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2020 is US $415/year for the electronic version, and $620/year (+$60, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 14 No. 9 2020

1937-0652(2020)14:9;1-T