A result on the equation $x^p + y^p = z^r$ using Frey abelian varieties

Nicolas Billerey, Imin Chen, Luis Dieulefait, Nuno Freitas

A RESULT ON THE EQUATION $x^p + y^p = z^r$ USING FREY ABELIAN VARIETIES

NICOLAS BILLEREY, IMIN CHEN, LUIS DIEULEFAIT, AND NUNO FREITAS

Abstract. We prove a Diophantine result on generalized Fermat equations of the form $x^p + y^p = z^r$ which for the first time requires the use of Frey abelian varieties of dimension ≥ 2 in Darmon's program. More precisely, for $r \geq 5$ a regular prime we prove that there exists a constant $C(r)$ such that for every prime number $p > C(r)$ the equation $x^p + y^p = z^r$ has no non-trivial primitive integer solutions (a, b, c) satisfying $r \mid ab$ and $2 \nmid ab$.

For the proof, we complement Darmon's ideas in a particular case by providing an irreducibility criterion for the mod $\mathfrak{p}$ representations attached to certain families of abelian varieties of GL_2-type over totally real fields.

1. Introduction

Darmon [2] has initiated a remarkable program to study the generalized Fermat equation

$$x^p + y^q = z^r, \qquad 1/p + 1/q + 1/r < 1, \qquad x, y, z \in \mathbb{Z}, \qquad xyz \neq 0, \qquad \gcd(x, y, z) = 1, \tag{1.1}$$

where the exponents $p, q, r \geq 2$ are prime numbers. He divides the analysis of this equation into the three one-parameter families (r, r, p), (p, p, r) and (r, q, p) where in each case the parameter p is allowed to vary and the other exponents are fixed. A notable feature of his program is that it uses higher dimensional abelian varieties and their (still mostly conjectural) modularity instead of just elliptic curves. However, very little is understood about the relevant abelian varieties and Darmon's program has not yet produced any Diophantine result, apart from a few cases where the abelian varieties involved are of dimension one, i.e. elliptic curves.

Darmon's program follows the strategy of the 'modular method': the Frey abelian variety $A(x, y, z)$ attached to a non-trivial (i.e. $xyz \neq 0$) putative solution (x, y, z) of (1.1) can be distinguished from the abelian varieties attached to the known trivial solutions (i.e. $xyz = 0$) through their Galois representations. Indeed, the p-torsion representation attached to $A(x, y, z)$ should be large in general, while if (x, y, z) is a trivial solution then this image is usually reducible or contained in the normalizer of a Cartan subgroup. Modularity of the abelian varieties $A(x, y, z)$ and level lowering results imply a congruence mod p between eigenforms, which bounds p under the set-up described above. Another interesting feature of Darmon's program is the use of classical cyclotomic criteria to eliminate the possibility of a congruence to an $\mathfrak{r}$-Eisenstein $\mathbb{Q}$-form at the lower levels [2, Proposition 3.20].

Date: August 16, 2016.

2010 *Mathematics Subject Classification.* Primary 11D41.

Key words and phrases. Fermat equations, Frey abelian varieties, Irreducibility.

We acknowledge the financial support of CNRS and ANR-14-CE-25-0015 Gardio (N. B.), an NSERC Discovery Grant (I. C.), and the grant *Proyecto RSME-FBBVA* 2015 *José Luis Rubio de Francia* (N. F.).

The objective of this work is twofold. We first develop an irreducibility criterion for the p-torsion representations attached to certain families of abelian varieties. Secondly, by following the idea in the previous paragraph and results from [2], we will show how the criterion can be used to unconditionally establish a Diophantine statement via Darmon's program that for the first time requires Frey abelian varieties of dimension ≥ 2.

We recall that an odd prime number r is called *regular* if it does not divide the class number of the cyclotomic field $\mathbb{Q}(\zeta_r)$. It is an open conjecture due to Siegel that there are infinitely many regular primes. We will prove the following theorem.

Theorem 1. *Let $r \geq 5$ be a regular prime. There exists a constant $C(r)$ such that for every prime number $p > C(r)$ the equation*

$$x^p + y^p = z^r \tag{1.2}$$

has no non-trivial (i.e. $abc \neq 0$) primitive (i.e. $\gcd(a,b,c) = 1$) solutions $(a,b,c) \in \mathbb{Z}^3$ satisfying $r \mid ab$ and $2 \nmid ab$.

Acknowledgements. Dieulefait would like to thank Eknath Ghate for several useful conversations during an early phase of this project.

2. An irreducibility criterion

The following terminology has been introduced by Ribet.

Definition 2.1. An abelian variety A over a number field K is said to be of GL_2-type if its endomorphism algebra $\mathrm{End}_K(A) \otimes \mathbb{Q} = F$ is a number field satisfying $[F : \mathbb{Q}] = \dim A$.

Let A/K be an abelian variety of GL_2-type. Set $F = \mathrm{End}_K(A) \otimes \mathbb{Q}$ and let p be a prime number. Denote by $T_p(A)$ the Tate module of A and write $V_p(A) = T_p(A) \otimes \mathbb{Q}_p$. Then, for each prime ideal $\mathfrak{p}$ of F over p, the absolute Galois group G_K of K acts $F_\mathfrak{p}$-linearly on $V_\mathfrak{p}(A) = V_p(A) \otimes_{F_p} F_\mathfrak{p}$ where $F_\mathfrak{p}$ denotes the completion of F at $\mathfrak{p}$ and $F_p = F \otimes \mathbb{Q}_p = \prod_{\mathfrak{p}|p} F_\mathfrak{p}$. This gives rise to a strictly compatible system of 2-dimensional p-adic Galois representations

$$\widetilde{\rho}_{A,\mathfrak{p}} : G_K \longrightarrow \mathrm{GL}_2(F_\mathfrak{p}).$$

The representation $\widetilde{\rho}_{A,\mathfrak{p}}$ can be conjugated to take values in $\mathrm{GL}_2(\mathcal{O}_\mathfrak{p})$ where $\mathcal{O}_\mathfrak{p}$ stands for the ring of integers in $F_\mathfrak{p}$. By reduction modulo the maximal ideal, we then get a representation

$$\rho_{A,\mathfrak{p}} : G_K \longrightarrow \mathrm{GL}_2(\mathbb{F}_\mathfrak{p}),$$

with values in the residue field $\mathbb{F}_\mathfrak{p}$ of $F_\mathfrak{p}$ which is unique up to semi-simplification and isomorphism.

The aim of this section is to provide a uniform bound on the residual characteristic of prime ideals $\mathfrak{p}$ for which the corresponding representations $\rho_{A,\mathfrak{p}}$ is reducible when A runs through certain families of abelian varieties of GL_2-type. For elliptic curves over totally real fields, such irreducibility criteria were previously known and different variants (for various families of curves) can be found in the work of Serre [11], Kraus [7, 8], Billerey [1], David [3], Dieulefait-Freitas [4] and Freitas-Siksek [5].

Recently, Larson and Vaintrob [9] have proven general results which classify the so-called associated mod p characters of abelian varieties A over a number field K for p sufficiently large.

Their results have consequences to proving irreducibility criteria for the representations $\rho_{A,\mathfrak{p}}$ which we discuss here with a view towards applications to Frey abelian varieties.

For that purpose, we introduce some useful definitions.

Definition 2.2. Let A/K be an abelian variety with potentially good reduction at a prime $\mathfrak{q}$ of a number field K. We say that A *has residual degree* f *at* $\mathfrak{q}$ if f is minimal among the degrees of the residual extensions corresponding to all extensions $L/K_{\mathfrak{q}}$ such that A/L has good reduction.

The following definition is motivated by [9, Lemma 4.6].

Definition 2.3. We say that an abelian variety A/K *has inertial exponent* $c \in \mathbb{N}$ if for every finite prime v of the number field K, there exists a finite Galois extension M/K such that A/M is semistable at all primes of M lying over v, and the exponent of the inertia subgroup at v of $\mathrm{Gal}(M/K)$ divides c.

We write $\overline{\mathbb{Z}}$ for the ring of integers of $\overline{\mathbb{Q}}$. Given an ideal $\mathfrak{q}$ of the ring of integers of a number field K, we write $N(\mathfrak{q})$ for its norm.

Theorem 2. *Let K be a totally real number field and fix a prime $\mathfrak{q}$ of K. Let $c, f \geq 1$ be integers with c even. Consider a finite set $S_f(\mathfrak{q})$ of elements of the form $\alpha_1 + \alpha_2$ where $\alpha_i \in \overline{\mathbb{Z}}$ are (for every embedding $\overline{\mathbb{Z}} \hookrightarrow \mathbb{C}$) of complex absolute value $N(\mathfrak{q})^{f/2}$ and $\alpha_1\alpha_2 = N(\mathfrak{q})^f$.*

Then there exists a constant $c_1 = c_1(K, c, f, S_f(\mathfrak{q}))$ such that the following holds. Suppose that $p > c_1$ and A/K is an abelian variety satisfying

(i) A is semistable at the primes of K above p,
(ii) A is of GL_2-type with multiplications by some totally real field F,
(iii) all endomorphisms of A are defined over K, that is $\mathrm{End}_K(A) = \mathrm{End}_{\overline{K}}(A)$,
(iv) A over K has inertial exponent c,
(v) A has potentially good reduction at $\mathfrak{q}$ with residual degree f,
(vi) the trace of $\mathrm{Frob}_{\mathfrak{q}}^f$ acting on $V_{\mathfrak{p}}(A)$ lies in $S_f(\mathfrak{q})$, where $\mathfrak{p}$ is a prime of F above p.

Then the representation $\rho_{A,\mathfrak{p}}$ is irreducible.

Remark 2.4. Let $L/K_{\mathfrak{q}}$ be an extension with residual degree f such that A over L has good reduction. Let $\mathfrak{q}'$ be the maximal ideal of L. Then $\mathrm{Frob}_{\mathfrak{q}'} = \mathrm{Frob}_{\mathfrak{q}}^f$ and hence the characteristic polynomial of $\rho_{A,\mathfrak{p}}(\mathrm{Frob}_{\mathfrak{q}}^f)$ is well-defined.

Remark 2.5. In the application to the generalized Fermat equation, we will take $S_f(\mathfrak{q})$ to be the set of possible traces of $\mathrm{Frob}_{\mathfrak{q}}^f$ on $V_{\mathfrak{p}}(A(x,y,z))$, where $A(x,y,z)$ is a Frey abelian variety defined over K attached to a primitive solution $(x,y,z) \in \mathbb{Z}^3$ of $x^p + y^p = z^r$, $A(x,y,z)$ satisfies (i)-(iv), and we impose a collection of q-adic conditions on $(x,y,z) \in \mathbb{Z}^3$ so that $A(x,y,z)$ satifies (v).

To make this more concrete, let us suppose, for simplicity, there is a fixed finite extension $L/K_{\mathfrak{q}}$ with inertia degree f and ring of integers $\mathcal{O}_L$, and some q-adic conditions on $(x,y,z) \in \mathbb{Z}^3$ allow one to give a model over $\mathcal{O}_L$ for $A(x,y,z)$ with good reduction at the prime $\mathfrak{q}'$ of L above $\mathfrak{q}$ such that the reduction modulo $\mathfrak{q}'$ is the same for any $(x,y,z) \in \mathbb{Z}^3$ satisfying the

q-adic conditions. In particular, the trace of $\mathrm{Frob}_{\mathfrak{q}}^f$ on $V_{\mathfrak{p}}(A(x,y,z))$ is a single well-defined value for $(x,y,z) \in \mathbb{Z}^3$ satisfying these q-adic conditions.

Let $S_f(\mathfrak{q})$ be the set of traces of $\mathrm{Frob}_{\mathfrak{q}}^f$ on $V_{\mathfrak{p}}(A(x,y,z))$ for a collection of q-adic conditions on $(x,y,z) \in \mathbb{Z}^3$ as above. Applying Theorem 2, we deduce the irreducibility of $\rho_{A(x,y,z),\mathfrak{p}}$ for $(x,y,z) \in \mathbb{Z}^3$ a primitive solution of $x^p + y^p = z^r$ satisfying the collection of q-adic conditions.

Proof of Theorem 2. Let A be an abelian variety satisfying conditions (i)-(v) in the statement. Suppose that $\rho_{A,\mathfrak{p}}$ is reducible. Let $\psi_i : G_K \to \mathbb{F}_{\mathfrak{p}}^\times$, for $i = 1, 2$, denote the two diagonal characters of $\rho_{A,\mathfrak{p}}$. Then each ψ_i is an associated mod p character of A of degree 1 in the sense of [9, p. 518]. Since A has inertial exponent c, then ψ_i^c is unramified at all primes $v \nmid p$ of K by [6, Proposition 3.5 (iv)]. Moreover, since by assumption c is even, ψ_i^c is unramified at infinity.

We note that in [9] a quantity $c = c(g)$ is used, however, the proofs of the results there are still valid as long as the A in question has inertial exponent c which is even.

We identify ψ_i with a character of the ideles using the reciprocity map of global class field theory. Let θ^S be defined as in [9, Definition 2.6] (with $L = \overline{\mathbb{Q}}$ in their notation), where $S \in \mathbb{Z}[\Gamma_K]$ and Γ_K is the set of embeddings of K into $\overline{\mathbb{Q}}$.

By [9, Lemma 5.4] and the semistability assumption (i), there exists $S_i \in \mathbb{Z}[\Gamma_K]$ such that $\psi_i(x_{\hat{p}})^c \equiv \theta^{S_i}(x)^c \pmod{\mathfrak{p}}$ for all $x \in K^\times$ relatively prime to p, where $x_{\hat{p}}$ is the prime to p-part of x regarded as an idèle of K.

We note that the invocation of [9, Lemma 5.4] requires $p \nmid \Delta_K$, where Δ_K is the absolute discriminant of K, because the proof of this lemma uses [9, Lemma 4.10]. However, the condition $p \nmid c$ is not necessary as we assume semi-stability at p by (i), and hence there is no need to use [9, Lemma 4.8].

Let $B_{\mathrm{char}}(K,c)$ be as given in [9, §7.2, p. 548]. For $p \nmid B_{\mathrm{char}}(K,c)$, θ^{S_i} is balanced by [9, Lemma 2.15, Lemma 5.6 and §7.2]. As K is totally real, a balanced character for K means being a power of the norm character [9, Definition 2.13]. Thus, θ^{S_i} is a non-negative power of the norm character.

From (ii) F is totally real, and from (iii) A has all of its endomorphisms defined over K. Hence [10, Lemma 4.5.1] says that we have

$$\det \rho_{A,\mathfrak{p}} = \psi_1\psi_2 = \mathrm{cyc}_p, \tag{2.6}$$

where cyc_p denotes the mod p cyclotomic character. Thus, θ^{S_i} is either trivial or the norm character and $\theta^{S_1}\theta^{S_2}$ is the norm character. Hence, by relabelling ψ_1 and ψ_2 if necessary, we may assume ψ_1^c, is unramified at all primes of K.

Let $\iota : \mathbb{F}_{\mathfrak{p}}^\times \to \mathbb{C}^\times$ be an injective homomorphism. Then $\iota \circ \psi_1$ is unramified at a prime v of K if and only if ψ_1 is unramified at v. The group of continuous characters of G_K with values in $\mathbb{C}^\times$ which are unramified at all primes of K are dual to the class group of K. Hence, we have that $(\iota \circ \psi_1^c)^{h'_K} = 1$ where h'_K is the exponent of the class group of K. Thus, $\psi_1^{ch'_K} = 1$. By (v), (vi), and Remark 2.4, we obtain that

$$p \mid \prod_{a \in S_f(\mathfrak{q})} \mathrm{Res}(X^{ch'_K} - 1, X^2 - aX + N(\mathfrak{q})^f),$$

where Res denotes the resultant. Since the polynomials in the resultant have no common roots (because the absolute value of the roots of $X^2 - aX + N(\mathfrak{q})^f$ is different from 1) we conclude that the resultant is non-zero. Therefore, letting c_1 denote a constant larger than any prime dividing $B_{\mathrm{char}}(K, c)$, Δ_K, and the above resultant, gives the desired bound. □

Corollary 1. *Let K be a totally real field, $\mathfrak{q}$ a prime of K and g a positive integer. There is a constant $C(K, g, \mathfrak{q})$ such that the following holds: Suppose $p > C(K, g, \mathfrak{q})$ is a prime. Then for all g-dimensional abelian varieties A/K with potentially good reduction at $\mathfrak{q}$ satisfying conditions (i)-(iii) in Theorem 2 the representation $\rho_{A,\mathfrak{p}}$ is irreducible.*

Proof. Since A achieves semistable reduction over $K(A[12])$ by [6, Proposition 4.7], and the degree of the Galois extension $K(A[12])/K$ is bounded in terms of g, this bounds the possible residual degrees of A at $\mathfrak{q}$ and inertial exponents of A in terms of g.

Let $c_{K,g}$ be the product of all the possible inertial exponents from the above paragraph.

If A has residual degree f at the prime $\mathfrak{q}$ of K, then the characteristic polynomial of $\mathrm{Frob}_{\mathfrak{q}}^f$ on $T_{\mathfrak{p}}(A)$ divides the characteristic polynomial of $\mathrm{Frob}_{\mathfrak{q}}^f$ on $T_p(A)$. If the dimension of A is fixed, then by [9, Lemma 7.6] there are only finitely many possibilities for the latter. Hence, for each possible f from the first paragraph, take $S_f(\mathfrak{q})$ to be the set of traces of the finitely many possibilities for the characteristic polynomial of $\mathrm{Frob}_{\mathfrak{q}}^f$ on $T_{\mathfrak{p}}(A)$.

For each f apply Theorem 2 with $S_f(\mathfrak{q})$ and $c = c_{K,g}$ to get a bound $c_f = c(K, c_{K,g}, f, S_f(\mathfrak{q}))$. The corollary follows by letting $C(K, g, \mathfrak{q})$ be the maximum of the c_f. □

Remark 2.7. There is an alternate method to deduce irreducibility which follows more directly from [9, Corollary 5.19]. We instead picked the proof above for two reasons. On the one hand, it is more natural as an extension of the proofs known for the case of elliptic curves and, on the other hand, since it uses properties that are normally satisfied by Frey abelian varieties, it should be better suited to giving simpler bounds in concrete Diophantine applications.

3. Application to $x^p + y^p = z^r$

In this section we use the irreducibility criterion from the previous section to establish an unconditional Diophantine statement as an application of Darmon's program [2] which requires Frey abelian varieties of dimension ≥ 2.

For an odd prime r, let ζ_r be a primitive r-th root of unity and denote by K the maximal totally real subfield of $\mathbb{Q}(\zeta_r)$. Let $(a, b, c) \in \mathbb{Z}^3$ be a non-trivial primitive solution of (1.2). Put $t = a^p/c^r$ and consider the abelian variety $J_r^+(t)$ defined in Section 1.3 of [2]. According to Eq. (5) in *loc. cit.*, one has

$$\mathrm{End}_{\overline{K}}(J_r^+(t)) = \mathcal{O}_K.$$

In particular, $J_r^+(t)$ becomes of GL_2-type over K with real multiplication by K (see also [12]). Let $J_r^+(a, b, c)$ be the $\mathbb{Q}$-model of $J_r^+(a^p/c^r)$ defined in [2, p.18].

The following two results follow from (the proof of) Proposition 1.15, Theorem 3.22 and Definition 3.6 of [2].

Lemma 1. *Let $(a,b,c) \in \mathbb{Z}^3$ be a non-trivial primitive solution to $x^p + y^p = z^r$. Suppose $r \mid ab$. Then the abelian variety $J_r^+(a,b,c)/K$ is semistable. Moreover, if $2 \nmid ab$ it has good reduction at all primes $\mathfrak{q}$ above 2 and its reduction mod $\mathfrak{q}$ is well-defined on the congruence class of $(a,b,c) \pmod 2$.*

Theorem 3. *Let r be a regular prime. Then there exists a constant $c_2(r)$ such that, for all $p > c_2(r)$, and non-trivial primitive solutions $(a,b,c) \in \mathbb{Z}^3$ to (1.2) with $r \mid ab$, the mod $\mathfrak{p}$ representation $\rho^+_{r,\mathfrak{p}}$ associated to $J_r^+(a,b,c)$ is reducible.*

As a consequence of these results and our irreducibility criterion in Theorem 2 we can now prove our main Diophantine application.

Proof of Theorem 1. Let $(a,b,c) \in \mathbb{Z}^3$ be a non-trivial primitive solution to $x^p + y^p = z^r$ satisfying $r \mid ab$ and $2 \nmid ab$. Write $J = J_r^+(a,b,c)/K$. From Lemma 1, we have that J is semistable with good reduction at all $\mathfrak{q} \mid 2$ and where the reduction mod $\mathfrak{q}$ is well-defined on the congruence class of $(a,b,c) \pmod 2$. In particular, for J we have even inertial exponent $c = 2$ and residual degree $f = 1$ at all $\mathfrak{q} \mid 2$. Recalling Remark 2.5 with the 2-adic condition $2 \nmid ab$, we take $S_f(\mathfrak{q})$ to be the singleton set consisting of the trace of $\mathrm{Frob}_\mathfrak{q}$ acting on the $\mathfrak{p}$-torsion of $J_r^+(1,-1,0)$.

From Theorem 2 we obtain a constant $c_1(r)$ such that if $p > c_1(r)$ and $\mathfrak{p} \mid p$ in K then the mod $\mathfrak{p}$ representation $\rho^+_{r,\mathfrak{p}}$ is irreducible.

From Theorem 3 we obtain a constant $c_2(r)$ such that if $p > c_2(r)$ and $\mathfrak{p} \mid p$ in K then $\rho^+_{r,\mathfrak{p}}$ is reducible.

Letting $C(r)$ be the maximum of $c_1(r)$ and $c_2(r)$, we obtain a contradiction for all exponents $p > C(r)$. □

References

[1] Nicolas Billerey. Critères d'irréductibilité pour les représentations des courbes elliptiques. *Int. J. Number Theory*, 7(4):1001–1032, 2011. 2

[2] Henri Darmon. Rigid local systems, Hilbert modular forms, and Fermat's last theorem. *Duke Math. J.*, 102(3):413–449, 2000. 1, 1, 3

[3] Agnès David. Caractère d'isogénie et critéres d'irréductibilité. *arXiv:1103.3892*, 2012. 2

[4] Luis Dieulefait and Nuno Freitas. Fermat-type equations of signature $(13,13,p)$ via Hilbert cuspforms. *Math. Ann.*, 357(3):987–1004, 2013. 2

[5] Nuno Freitas and Samir Siksek. Criteria for irreducibility of mod p representations of Frey curves. *J. Théor. Nombres Bordeaux*, 27(1):67–76, 2015. 2

[6] Alexander Grothendieck. Modèles de Néron et monodromie. *In Séminaire de Géométrie Algébrique*, 7, Exposé 9, 1967–1969. 2, 2

[7] Alain Kraus. Courbes elliptiques semi-stables et corps quadratiques. *J. Number Theory*, 60(2):245–253, 1996. 2

[8] Alain Kraus. Courbes elliptiques semi-stables sur les corps de nombres. *Int. J. Number Theory*, 3(4):611–633, 2007. 2

[9] Eric Larson and Dmitry Vaintrob. Determinants of subquotients of Galois representations associated with abelian varieties. *J. Inst. Math. Jussieu*, 13(3):517–559, 2014. With an appendix by Brian Conrad. 2, 2, 2, 2, 2.7

[10] Kenneth A. Ribet. Galois action on division points of Abelian varieties with real multiplications. *Amer. J. Math.*, 98(3):751–804, 1976. 2

[11] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972. 2

[12] Walter Tautz, Jaap Top, and Alain Verberkmoes. Explicit hyperelliptic curves with real multiplication and permutation polynomials. *Canad. J. Math.*, 43(5):1055–1064, 1991. 3

(1) Université Clermont Auvergne, Université Blaise Pascal, Laboratoire de Mathématiques, BP 10448, F-63000 Clermont-Ferrand, France. (2) CNRS, UMR 6620, LM, F-63171 Aubière, France

E-mail address: Nicolas.Billerey@math.univ-bpclermont.fr

Department of Mathematics, Simon Fraser University, Burnaby, BC V5A 1S6, Canada

E-mail address: ichen@sfu.ca

Departament d'Algebra i Geometria, Universitat de Barcelona, G.V. de les Corts Catalanes 585, 08007 Barcelona, Spain

E-mail address: ldieulefait@ub.edu

University of British Columbia, Department of Mathematics, Vancouver, BC V6T 1Z2 Canada

E-mail address: nunobfreitas@gmail.com