TWO RESULTS ON $x^r + y^r = dz^p$

NUNO FREITAS AND FILIP NAJMAN

Abstract. This note proves two theorems regarding Fermat-type equation $x^r + y^r = dz^p$ where $r \geq 5$ is a prime. Our main result shows that, for infinitely many integers $d$, the previous equation has no non-trivial primitive solutions such that $2 \mid x + y$ or $r \mid x + y$, for a set of exponents $p$ of positive density. We use the modular method with a symplectic argument to prove this result.

1. Introduction

We consider Fermat-type equations of the form

$$x^r + y^r = dz^p,$$

where $r, p > 3$ are primes and $d$ is an odd positive integer, not an $r$-th power and $r \nmid d$. A solution $(a, b, c)$ to (1.1) is called primitive if $\gcd(a, b, c) = 1$ and non-trivial if $abc \neq 0$.

We will study the above equation via the modular method. Since $d$ is not a $r$-th power, we have $d \neq 1$; this avoids the trivial solution $(1, 0, 1)$ which is a well known obstruction. Indeed, the modular method aims to obtain a contradiction with the existence of a solution, which is usually not possible once a solution does exist. More precisely, for $d = 1$, in the elimination stage of the method, we would have to distinguish the mod $p$ representation of the Frey curve attached to a non-trivial putative solution $(a, b, c)$ from the mod $p$ representation of the Frey curve attached to the solution $(1, 0, 1)$. Currently, with the exception of very few special cases, there are no techniques available to do this. The hypothesis that $d$ is odd avoids the solution $(1, 1, 1)$ for $d = 2$ but it also plays (together with $r \nmid d$) an essential rôle in the proof of Theorem 1.2 below (see Remark 3.2).

Equation (1.1) has been the focus of various recent works. It has been completely resolved for $(r, d) = (5, 3), (13, 3)$ and all $p \geq 2$ in [3, 2], and for $(r, d) = (7, 3)$ in [4]; moreover, in [12] it is shown for $d = 1$ and many values of $r < 150$ that it admits no non-trivial primitive solutions $(a, b, c)$ with $c$ even. Under the extra assumptions that $d$ is not divisible by $p$-th powers and is divisible only by primes $q \equiv 1 \pmod{r}$, an older result due to Kraus implies that, fixed both $r$ and $p$, the set of coefficients $d$ for which (1.1) has a non-trivial primitive solution is finite (see [11, Théorème 1]).

Given that we will focus on asymptotic results, i.e. for large enough $p$, we can also assume that $p$ is large compared to $r$ and $p \nmid d$. We will prove the following theorem.

The second author was supported by the QuantiXLie Centre of Excellence, a project co-financed by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Programme (Grant KK.01.1.1.01.0004) and by the Croatian Science Foundation under the project no. IP-2018-01-1313. The first author is partially supported by the PID2019-107297GB-I00 grant of the MICINN (Spain).
Theorem 1.2. Let \( r \) and \( d \) be as above. For a set of prime exponents \( p \) of positive density, the equation (1.1) has no non-trivial primitive solutions \((a, b, c)\) such that \( 2 \mid a + b \) or \( r \mid a + b \).

This result has no constraints on the value of \( r \) and \( d \) beyond those introduced in the first paragraph. Instead we have 2-adic or \( r \)-adic restrictions on the solutions, that naturally occur in the study of Fermat-type equations. In particular, the condition \( r \mid a + b \) is equivalent to \( r \mid c \) and this is analogous to what Darmon calls a first case solution to the Fermat-type equations \( x^p + y^p = z^r \) (see [5, Definition 3.6] and results in §3 of loc. cit.). A result of similar flavor to ours regarding \( x^p + y^p = z^r \) is given in [1], more precisely, it is shown this equation has no non-trivial primitive solutions with \( r \mid ab \) and \( 2 \nmid ab \). We remark that although in loc. cit. the proof uses Darmon’s higher dimensional abelian varieties instead of Frey elliptic curves, the condition \( r \mid ab \) plays a similar role to ours \( r \mid a + b \) in that it forces the Frey varieties to have multiplicative reduction at \( r \).

The proof of Theorem 1.2 was inspired by [10] and relies on combining the modular method with the symplectic argument. We refer the reader to [7] for a quick introduction to Diophantine applications of the symplectic argument; for a comprehensive study of symplectic criteria and further Diophantine applications we refer to [8].

We will also prove the following theorem about (1.1) where the 2-adic and \( r \)-adic conditions are replaced by a \( p \)-adic condition.

Theorem 1.3. Let \( r \) and \( d \) be as above. Then for prime exponents \( p \equiv \pm 1 \pmod{r} \) large enough the equation (1.1) has no non-trivial primitive solutions \((a, b, c)\) such that \( p \mid a + b \).

2. The Frey curve

We first recall the construction of a Frey curve from [6]. Let \( r \geq 5 \) be a prime and \( \zeta = \zeta_r \) a fixed primitive \( r \)-th root of unity. Let \( K = \mathbb{Q}(\zeta_r) \) be the maximal real subfield of \( \mathbb{Q}(\zeta_r) \).

Define the polynomials

\[
f_1 := x^2 + (\zeta^2 + \zeta^{-2})xy + y^2 \quad \text{and} \quad f_2 := x^2 + (\zeta + \zeta^{-1})xy + y^2
\]

and the constants

\[
\alpha = \zeta(1 - \zeta)(1 - \zeta^2), \quad \beta = (1 - \zeta)(1 - \zeta^{-1}), \quad \gamma = -(1 - \zeta^2)(1 - \zeta^{-2}).
\]

We set also

\[
A = A_{a, b} = \alpha(a + b)^2, \quad B = B_{a, b} = \beta f_1(a, b), \quad C = C_{a, b} = \gamma f_2(a, b)
\]

and define the Frey curve

\[
F_{a, b} : Y^2 = X(X - A_{a, b})(X + B_{a, b}).
\]

By construction we have \( A + B = C \) and the following standard invariants

\[
c_4(F_{a, b}) = 2^4(A_{a, b}^2 + A_{a, b}B_{a, b} + B_{a, b}^2),
\]

\[
c_6(F_{a, b}) = 2^5(2A_{a, b}^3 + 3A_{a, b}^2B_{a, b} - 3A_{a, b}B_{a, b}^2 - 2B_{a, b}^3),
\]

\[
\Delta(F_{a, b}) = 2^4(A_{a, b}B_{a, b}C_{a, b})^2.
\]

For \( n \in \mathbb{Z}_{>0} \) and \( x \in K \) denote by \( \text{Rad}_n(x) \) the product of the primes in \( K \) not dividing \( n \). Also let \( p_r \) denote the unique prime in \( K \) above \( r \).
Proposition 2.2. Let \((a, b, c)\) a primitive solution to (1.1) such that \(\gcd(a, b) = 1\). Then the conductor \(N_F\) of the curve \(F = F_{a,b}\) is of the form
\[
2^p \alpha \cdot \text{Rad}_r(a + b)
\]
where \(\alpha\) is a squarefree product of primes in \(K\) dividing \(c\).
Moreover, \(s = 1\) if \(2 \mid a + b\) and \(t = 1\) if \(r \mid a + b\).

Proof. Since \(\alpha, \beta, \gamma\) are of the form \(\pm \zeta^\alpha(1 - \zeta^z)(1 - \zeta^w)\), where neither \(t\) nor \(u\) are \(\equiv 0 \pmod{r}\), this means that the only prime dividing \(\alpha \beta \gamma\) is \(p_r\) and \(v_{p_r}(\alpha \beta \gamma) = 3\).

Recall the factorisation
\begin{equation}
2^r + 2^r = (a + b)\Phi_r(a, b) = dc^p
\end{equation}
where \(\Phi_r(a, b)\) is the \(r\)-th cyclotomic polynomial; we have \(\gcd(a + b, \Phi_r(a, b)) = 1\) or \(r\) since \(a, b\) are coprime. Moreover, the polynomials \(f_1(a, b)\) and \(f_2(a, b)\) in the definitions of \(B\) and \(C\) are factors of \(\Phi_r(a, b)\) over \(K\); see [6, §2] for proofs of these elementary properties (in particular, Corollary 2.2 and the discussion after Corollary 2.6 in loc. cit.).

Let \(q \mid 2r\) be a prime in \(K\). Then \(v_q(\Delta(F)) = 2(v_q(A) + v_q(B) + v_q(C))\).

If \(q \mid a^r + b^r\) we have \(v_q(\Delta(F)) = 0\), so \(q\) is a prime of good reduction.

Assume \(q \mid a^r + b^r\). Then \(q \mid A\) or \(q \mid \Phi_r(a, b)\) and not both simultaneously.

If \(q \mid \Phi_r(a, b)\) and \(q \mid BC\), then \(q\) is a prime of good reduction.
Otherwise, either \(q \mid A\) and \(q \mid BC\) or \(q \mid A\) and \(q \mid BC\). In both cases, we get \(v_q(\Delta(F)) > 0\) and \(v_q(c_4(F)) = 0\), so \(q\) is a prime of multiplicative reduction.

We now consider the prime \(p_r\) above \(r\). Assume \(r \mid a + b\). We have
\[
v_{p_r}(c_4) = 4, \quad v_{p_r}(c_6) = 6, \quad v_{p_r}(\Delta) = 10 + 4v_{p_r}(a + b).
\]

Since \(v_{p_r}(a + b) \geq (r - 1)/2\) the equation is non-minimal and after a coordinate change we have \(v_{p_r}(c_4) = 0\) and \(v_{p_r}(\Delta) > 0\). Thus \(F\) has bad multiplicative reduction, i.e. \(v_{p_r}(N_F) = 1\).

Finally we consider a prime \(q_2 \mid 2\). As 2 is unramified in \(K\) we will use [13, Table IV] to read the conductor at \(q_2\) in terms of the \(q_2\)-adic valuations of the standard invariants \((c_4, c_6, \Delta)\).

Assume \(2 \mid a + b\) so \(2 \nmid \Phi(a, b)\). Since \(p > 3\), the shape of equation (1.1) implies \(8 \mid a + b\). Moreover,
\[
v_{q_2}(c_4) = 4, \quad v_{q_2}(c_6) = 6, \quad v_{q_2}(\Delta) = 10 + 4v_{q_2}(a + b).
\]

The corresponding entries in [13, Table IV] give us Tate case 7 with \(v_{q_2}(N_F) = 4\) or the equation for \(F\) is non-minimal as \(v_{q_2}(a + b) \geq 3\). We will apply [13, Prop. 4] to show that we are in the non-minimal case; we state it here for convenience.

Proposition 2.4. Let \(K/\mathbb{Q}_2\) be a finite extension with ring of integers \(\mathcal{O}\) and uniformizer \(\pi\). Let \(W/K\) be an elliptic curve given by a Weierstrass model \((W)\) with standard invariants \(a_i\) and \(b_i\). Assume that \((W)\) is in a Tate case \(\geq 7\).

(a) There is \(r \in \mathcal{O}\) such that
\[
b_8 + 3r b_6 + 3r^2 b_4 + r^3 b_2 + 3r^4 \equiv 0 \pmod{\pi^5}
\]
Let $z = -\zeta_r - \zeta_r^{-1}$. Using $a \equiv -b \pmod{q_2^2}$ we get
\[
B = (2 + z)(a^2 + (z^2 - 2)ab + b^2) = (2 + z)((a + b)^2 - (z^2 - 4)ab)
\equiv (z + 2)(z^2 - 4)ab \equiv -b^2(z + 2)^2(z - 2) \pmod{q_2^2}.
\]
Moreover,
\[
2 - z = (\zeta_r^{\frac{r+1}{2}} + \zeta_r^{-\frac{r+1}{2}})^2
\]
with $\zeta_r^{\frac{r+1}{2}} + \zeta_r^{-\frac{r+1}{2}} \in \mathcal{O}_K$ because it is fixed by complex conjugation; thus $B$ is a square mod $q_2^2$ so part (b) is satisfied and we are in the non-minimal case. After a change of variables we get
\[
\tag{2.5}
\nu_{q_2}(c_4) = \nu_{q_2}(c_6) = 0, \quad \nu_{q_2}(\Delta(F)) = -8 + 4\nu_{q_2}(a + b) > 0,
\]
from which we see that $F$ has multiplicative reduction, i.e $\nu_{q_2}(N_F) = 1$. \qed

Recall from [6, §2] that $\gcd(a + b, \Phi_r(a,b)) = 1$ or $r$ and $\Phi_r(a,b)$ is divisible only by $r$ and primes $q \equiv 1 \pmod{r}$. Write $d = d_0d_1$ where a prime $q \mid d_1$ if and only if $q \equiv 1 \pmod{r}$.

**Proposition 2.6.** For large enough $p$ the following holds. For all primitive solutions $(a, b, c)$ of \eqref{1.1} with $\gcd(a, b) = 1$ the representation $\overline{\rho}_{F, p}$ is irreducible and modular of weight 2. Moreover, it’s Serre level is $2^s p_r'R \text{Rad}_{2r}(d_0d_1')$ where $q \mid d_1'$ if and only if $q \mid d_1$ and $q \mid c$ where $s$, $t$ and $c$ are as in Proposition 2.2.

**Proof.** From [6, Theorems 4.3 and 4.4], it follows that there exists a constant $C_r$, depending only on $r$, such that for all $p > C_r$ the representation $\overline{\rho}_{F, p}$ is modular of weight 2 and absolutely irreducible.

Let $q \nmid 2r$ be a prime dividing $a + b$. From Proposition 2.2, we know $q$ is a prime of bad multiplicative reduction.

From \eqref{2.3} we have $a + b = 2^{sp} \cdot r^k \cdot d_0 \cdot c_0^p$ with $s, k \geq 0$ and $c_0 \mid c$. Thus
\[
\tag{2.7}
\nu_q(\Delta(F)) = 2\nu_q(A) = 4\nu_q(a + b) = 4\nu_q(d_0) + 4\nu_q(c_0) \equiv 4\nu_q(d_0) \pmod{p}.
\]
When $\nu_q(d_0) \neq 0$ then $4\nu_q(d_0) \not\equiv 0 \pmod{p}$ for large enough $p$; further enlarging $p$ we can assume $p \mid d$. Hence the primes $q \mid 2r$ dividing $a + b$ that also divide the Serre level of $\overline{\rho}_{E, p}$ are precisely those dividing $d_0$.

Finally, the multiplicative primes $q \mid c$ divide the Serre level if and only if $q \mid d_1$. Indeed, recall that $p_1$ is the only prime that can divide both $B$ and $C$, and that they are both coprime to $a + b$ as well (and hence to $d_0$) so both $B$ and $C$ are $p$-th powers times a divisor in $\mathcal{O}_K$ of $d_1r$. We have
\[
\tag{2.8}
\nu_q(\Delta(F)) \equiv 2\nu_q(\Delta(d_1)) \pmod{p},
\]
hence, for large \( p \), a prime \( q \mid c \) satisfies \( v_q(\Delta(F)) \not\equiv 0 \pmod{p} \) if and only if \( q \mid d_1 \).

\[ \square \]

3. Proof of Theorem 1.2

We will use the following lemma several times, so we state it here before proceeding further.

**Lemma 3.1** ([10, Lemma 1.6]). Let \( E \) and \( E' \) be two elliptic curves over \( \mathbb{Q} \) and \( p, \ell_1, \ell_2 \) three distinct primes with \( p > 2 \). Suppose \( E[p] \) and \( E'[p] \) are isomorphic. Suppose \( E \) and \( E' \) have multiplicative reduction at \( \ell_1 \) and \( p \) does not divide \( v_{\ell_1}(\Delta(E)) \), which implies that \( p \) does not divide \( v_{\ell_1}(\Delta(E')) \). Then the reduction mod \( p \) of \( v_{\ell_1}(\Delta(E))v_{\ell_2}(\Delta(E))v_{\ell_1}(\Delta(E'))v_{\ell_2}(\Delta(E')) \) is a square in \( \mathbb{F}_p \).

Note that from a non-trivial solution \((a, b, c)\) to equation (1.1) with \( m = \gcd(a, b) > 1 \) and \( \gcd(a, b, c) = 1 \), we obtain a non-trivial primitive solution to \( x^r + y^r = d^r z^p \) with \( \gcd(a, b) = 1 \) where \( d = \frac{d'}{m^r} \). Since \( d \) is not an \( r \)-power, the same is true for \( d' \). Clearly \( d' \) is also odd and \( r \notdiv d' \), hence we are reduced to the case of solutions satisfying \( \gcd(a, b) = 1 \). The argument below is inspired by [10, Theorem 2.1] and it will show by contradiction that these latter solutions do not exist for \( p \) in a set of primes of density \( > 0 \).

Suppose there is a non-trivial primitive solution \((a, b, c)\) to (1.1) with \( a, b \) coprime\(^1\).

By Proposition 2.6, for sufficiently large \( p \), we have \( \bar{\rho}_{F,p} \simeq \bar{\rho}_{f,p} \), where \( f \) is a Hilbert newform of level \( 2^r \cdot p \cdot \text{Rad}_{2r}(d_0d'_1) \), where \( p \) is a prime in the field of coefficients \( K_f \) of \( f \). Since the field of coefficients of \( F \) is \( \mathbb{Q} \), by enlarging \( p \) if needed, we can assume that \( K_f = \mathbb{Q} \). Moreover, since \( d \notdiv 1 \), there is at least one prime \( q \) in \( K \) dividing \( \text{Rad}_{2r}(d_0d'_1) \), which is a Steinberg prime of \( f \). Therefore, by the Eichler-Shimura correspondence for \( f \), there is an isogeny class of elliptic curves defined over \( K \) corresponding to \( f \). Let \( E \) denote an elliptic curve in that isogeny class. Since \( F \) has full 2-torsion over \( K \), by further enlarging \( p \) if necessary, we can also assume that \( E \) has full 2-torsion; see [9, §2.4 and §4] for the previous claims.

From the above, in particular, we have an isomorphism of \( G_K \)-modules \( \phi : F[p] \rightarrow E[p] \).

(1) Suppose \( 2 \mid a + b \). Let \( q_2 \mid 2 \) and \( q \mid d \) be primes in \( K \).

Recall that \( d = d_0d_1 \) where a prime \( q \mid d_1 \) if and only if \( q \equiv 1 \pmod{r} \).

(1a) Assume that \( q \mid d_0 \). Then the curve \( F \) has multiplicative reduction at \( q_2 \) and \( q \) by Proposition 2.2; we will apply Lemma 3.1.

Note that \( a + b = 2^{sp} \cdot r^k \cdot d_0 \cdot c_0^s \) with \( s \geq 1 \), therefore from (2.5) and (2.7) we have,

\[
v_{q_2}(\Delta(F)) \equiv -8 \pmod{p} \quad \text{and} \quad v_q(\Delta(F)) \equiv 4v_q(d_0) \not\equiv 0 \pmod{p}.
\]

Therefore, by Lemma 3.1 we must have

\[
-2v_q(d_0) = v_{q_2}(\Delta(E))v_q(\Delta(E)) \in (\mathbb{F}_p^*)/(\mathbb{F}_p^*)^2.
\]

\(^1\)In the paper [6] where our Frey curve \( F \) was introduced, a solution \((a, b, c)\) is called primitive when \( \gcd(a, b) = 1 \). Here we decided to use the condition \( \gcd(a, b, c) = 1 \) instead because this is more standard in the context of the generalized Fermat equation \( Ax^{r} + By^{q} = Cz^p \).
Let \( k \) be the number of isogeny classes of elliptic curves over \( K \) with full 2-torsion and conductor \( 2 \cdot \text{Rad}_{2^s}(d) \cdot p_i^s \). For \( i = 1, \ldots, k \), we let \( E_i \) be a representative of each isogeny class and set

\[
n_i := -2n_q(d_0)v_q(\Delta(E_i))v_q(\Delta(E_i))
\]

which are negative integers as the valuations used in their definition are positive.

Observe that our result now follows if, for a positive density of primes \( p \), we have that \( n_i \) is not a square modulo \( p \) for all \( i \). We claim that the set of such primes is non-empty. Then the Dirichlet density theorem guarantees that this set has density \( \geq (1/2)^k \).

To finish the proof we now prove the claim. Choose \( p \equiv 7 \pmod{8} \) such that for all odd primes \( q \mid v_q(d_0) \prod n_i \) the condition \( \left( \frac{q}{p} \right) = 1 \) is satisfied. Such primes exist by the Dirichlet density theorem. Let \( n_i = -2^s q_{i_1}^{e_1} \ldots q_{i_j}^{e_j} \) be the prime factorisation. Then

\[
\left( \frac{n_i}{p} \right) = \frac{-1 \cdot 2^s q_{i_1}^{e_1} \ldots q_{i_j}^{e_j}}{p} = \left( \frac{-1}{p} \right) \left( \frac{2}{p} \right)^s \cdot 1 \cdot \ldots \cdot 1 = -1,
\]

that is, \( n_i \) is not a square mod \( p \) for all \( i \), as desired.

(1b) Assume now \( q \mid d_1 \). Thus \( q \nmid a + b \) and, after replacing \( q \) by a conjugate if needed, we can assume that \( q \mid c \) where \( c \) is given by Proposition 2.2. Thus \( F \) has multiplicative reduction at \( q_2 \) and \( q \). From (2.8) we also know that \( v_q(\Delta(F)) \equiv 2v_q(\Delta(d_1^s)) \neq 0 \pmod{p} \). The conclusion now follows similar to the previous case where the integers \( n_i \) are instead defined by \( n_i := -v_q(d_1^s)q_2(\Delta(E_i))v_q(\Delta(E_i)) \).

(2) Suppose \( r \mid a + b \). Now the curve \( F \) has multiplicative reduction at \( p_r \) and \( q \) by Proposition 2.2. Because \( v_r(\Phi_r(a, b)) = 1 \) when \( r \mid a + b \), we have \( a + b = 2^{sp} \cdot r^{k_p - 1} \cdot d \cdot r_{i}^{j} \). Therefore it follows from the proof of Proposition 2.2 that a minimal discriminant at \( p_r \) for \( F \) satisfies

\[
v_{p_r}(\Delta) = 10 + 4v_{p_r}(a + b) - 12 = -2 + 4(sp - 1) \frac{r - 1}{2} \equiv -2r \pmod{p}
\]

We now apply Lemma 3.1 with primes \( p_r \) and \( q \). Recall that \( v_q(\Delta(F)) \equiv 4v_q(d) \pmod{p} \), leading to

\[
v_q(\Delta(F))v_{p_r}(\Delta(F)) = -2v_q(d)r \in (\mathbb{F}_p)^*/(\mathbb{F}_p)^2
\]

and

\[
n_i = -2v_q(d)r \cdot v_{q_2}(\Delta(E_i))v_{p_r}(\Delta(E_i)).
\]

Since the \( n_i \) are again all negative we complete the proof analogously to case (1). \( \square \)

**Remark 3.2.** The argument above succeeds due to the negative sign in the definition of the integers \( n_i \). More precisely, this sign arises due to the congruence \( v_{q_2}(\Delta(F)) \equiv -8 \pmod{p} \) in case (1) and \( v_{q_r}(\Delta(F)) \equiv -2r \pmod{p} \) in case (2). We observe these congruences hold only because \( d \) is odd and not divisible by \( r \).

**4. Proof of Theorem 1.3**

As in Theorem 1.2 we apply the modular method with the Frey curve \( F \). Moreover, the simplifications at the start of the proof of Theorem 1.2 also apply.
Namely, let \((a, b, c)\) be a non-trivial solution to (1.1) such that \(p \mid a + b \) and \(\gcd(a, b) = 1\). For primes \(p\) sufficiently large, we obtain \(\tilde{\rho}_{E, p} \simeq \tilde{\rho}_{E, f, p}\), where \(E_f\) is an elliptic curve with full 2-torsion associated with a Hilbert newform \(f\) of level \(2^s \cdot p^r \cdot \text{Rad}_{2r}(d_0 d'_1)\).

Furthermore, \(E_f\) has good reduction at all primes \(p \mid p\) in \(K\) as \(p \notdiv 2rd\), and \(F\) has multiplicative reduction at all \(p \mid p\) as \(p\) \(a + b\) by Proposition 2.2.

The assumption \(p \equiv \pm 1 \pmod{r}\) implies that \(p\) splits completely in \(K = \mathbb{Q}(\zeta_r)^+\). In particular, locally at any \(p \mid p\) the curves \(F\) and \(E_f\) become curves over \(\mathbb{Q}_p\); therefore, by restricting \(\tilde{\rho}_{F, p} \simeq \tilde{\rho}_{E_f, p}\) to decomposition subgroups at \(p\), we also have the isomorphism

\[
\tilde{\rho}_{F, p}|_{\text{Gal}(\mathbb{Q}_p/\mathbb{Q}_p)} \simeq \tilde{\rho}_{E_f, p}|_{\text{Gal}(\mathbb{Q}_p/\mathbb{Q}_p)},
\]

where the representation on the right is the reduction of a crystalline representation and the one on the left is the reduction of a semistable non-crystalline representation. More precisely, the \(p\)-adic representation \(\rho_{F, p}\) when restricted to \(D_p \simeq \text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)\) is given by the first case in [14, §2.2.3] with \(e = 1\) whilst \(\rho_{E_f, p}\) restricted to \(D_p\) is given by the second case also with \(e = 1\). In particular, their semisimplifications are given by

\[
(\rho_{E_f, p}|_{D_p})^{ss} \simeq \eta_{a}^{-1}\chi \oplus \eta_{a} \quad \text{and} \quad (\rho_{F, p}|_{D_p})^{ss} \simeq \eta_{a}^{-1}\chi \oplus \eta_{a} \cdot \eta_{a} - 1,
\]

where the characters \(\eta_{a}, \eta_{1}\) are unramified, \(\eta_{-1}\) is quadratic, \(a \in \{0, 1\}\), \(\chi\) is the \(p\)-adic cyclotomic character and \(a_p(E_f/\mathbb{Q}_p) = u^{-1}p + u\) with \(u = \eta_{a}(\text{Frob}) \in \mathbb{Z}_p^*\). By putting together the reduction mod \(p\) of the representations in (4.2) with the semisimplification of (4.1) we conclude that either

\[
(\eta_{a}^{-1}\chi, \eta_{a}) \equiv (\eta_{a}^{-1}\chi, \eta_{a} - 1) \quad \text{or} \quad (\eta_{a}^{-1}\chi, \eta_{a}) \equiv (\eta_{a} - 1\chi, \eta_{a} - 1\chi) \quad \text{(mod } p\text{)}.
\]

Since \(\chi\) (mod \(p\)) is the mod \(p\) cyclotomic character which is ramified and \(\eta_{a}, \eta_{1}\) are unramified we must be in the first case. Therefore,

\[
a_p(E_f/\mathbb{Q}_p) = u^{-1}p + u \equiv u = \eta_{a}(\text{Frob}) \equiv \eta_{a}^{-1}(\text{Frob}) = \pm 1 \quad \text{(mod } p\text{)}.
\]

Since \(a_p(E_f) = a_p(E_f/\mathbb{Q}_p)\) we have

\[
a_p(E_f) \equiv \pm 1 \quad \text{(mod } p\text{)} \implies a_p(E_f) = \pm 1 + kp, \quad k \in \mathbb{Z}.
\]

Furthermore, from the Weil bound, we get

\[
|a_p(E_f)| \leq 2\sqrt{\text{Norm}(p)} \implies (\pm 1 + kp)^2 \leq 4p
\]

since \(\text{Norm}(p) = p\) because \(p\) splits completely in \(K\). The previous inequality does not hold for large \(p\) unless \(k = 0\), that is \(a_p(E_f) = \pm 1\).

On the other hand, since \(E_f\) has full 2-torsion over \(\mathbb{Q}\) and reduction modulo a rational prime \(q\) of good reduction is injective on \(E_f(\mathbb{Q})_{\text{tors}}\), it follows that \(a_q(E_f)\) is even for all primes \(\ell\) in \(K\) of good reduction; in particular, \(a_p(E_f)\) is even, a contradiction. \(\square\)

References

[1] N. Billerey, I. Chen, L. Dieulefait, N. Freitas, A result on the equation \(x^p + y^p = z^r\) using Frey abelian varieties, Proc. Amer. Math. Soc. 145 (2017), 4111–4117.

[2] N. Billerey, I. Chen, L. Dembele, L. Dieulefait and N. Freitas, Some extensions of the modular method and Fermat equations of signature \((13, 13, n)\), Publ. Math. to appear.

[3] N. Billerey, I. Chen, L. Dieulefait, N. Freitas, A multi-Frey approach to Fermat equations of signature \((r, r, p)\), Trans. Amer. Math. Soc. 371 (2019), 8651–8677.
[4] N. Billerey, I. Chen, L. Dieulefait, and N. Freitas. Appendix by F. Najman, *On Darmon’s program for the generalized Fermat equation*, preprint. Available at https://arxiv.org/pdf/2205.15861.pdf

[5] H. Darmon, *Rigid local systems, Hilbert modular forms, and Fermat’s last theorem*, Duke Math. J. 102 (2000), 413–449.

[6] N. Freitas, *Recipes for Fermat-type equations of the form $x^r + y^r = Cz^p$*, Math. Z. 279 (2015), 605–639.

[7] N. Freitas and A. Kraus, *An application of the symplectic argument to some Fermat-type equations*, C. R. Math. Acad. Sci. Paris 354 (2016), no. 8, 751–755.

[8] N. Freitas and A. Kraus, *On the symplectic type of isomorphisms of the $p$-torsion of elliptic curves*, Mem. Amer. Math. Soc. 277 (2022), no. 1361, v+105 pp.

[9] N. Freitas and S. Siksek, *The Asymptotic Fermat’s Last Theorem for Five-Sixths of Real Quadratic Fields*, Compositio Mathematica 151 (2015), no. 8, 1395–1415.

[10] E. Halberstadt and A. Kraus, *Courbes de Fermat: résultats et problèmes*, J. Reine Angew. Math. 548 (2002), 167–234.

[11] Kraus, A. *Une question sur les équations $x^m - y^m = Rz^n$ (A Question on the Equations $x^m - y^m = Rz^n$)*, Compositio Mathematica 132, 1–26 (2002).

[12] D. Mocanu, *Asymptotic Fermat for signatures $(r, r, p)$ using the modular approach*, preprint. Available at https://arxiv.org/pdf/2212.10627.pdf

[13] I. Papadopoulos, *Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle 2 et 3*, J. Number Theory 44 (1993), 119–152.

[14] M. Volkov, *Les représentations $l$-adiques associées aux courbes elliptiques sur $Q_p$*, J. Reine Angew. Math. 535 (2001), 65–101.

Instituto de Ciencias Matemáticas, CSIC, Calle Nicolás Cabrera 13–15, 28049 Madrid, Spain

Email address: nuno.freitas@icmat.es

University of Zagreb, Faculty of Science, Department of Mathematics, Bijenička cesta 30, 10000 Zagreb, Croatia

Email address: fnajman@math.hr