JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Nuno FREITAS et Samir SIKSEK

Criteria for Irreducibility of mod p Representations of Frey Curves

Tome 27, nº 1 (2015), p. 67-76.

<http://jtnb.cedram.org/item?id=JTNB_2015__27_1_67_0>

Journal de Théorie des Nombres de Bordeaux **27** (2015), 67–76

Criteria for Irreducibility of mod p Representations of Frey Curves

par Nuno FREITAS et Samir SIKSEK

Résumé. Soit K un corps de nombres galoisien totalement réel, et soit $\mathcal{E}$ un ensemble de courbes elliptiques sur K. Nous donnons des conditions suffisantes pour l'existence d'un ensemble calculable de nombres premiers $\mathcal{P}$ tels que, pour $p \notin \mathcal{P}$ et $E \in \mathcal{E}$, la représentation $\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E[p])$ soit irréductible. Nos conditions sont en général satisfaites par les courbes de Frey associées à des solutions d'équations diophantiennes. Dans ce contexte, l'irréductibilité de la représentation mod p est une hypothèse requise pour l'application des théorèmes d'abaissement du niveau. Comme illustration de notre approche, nous avons amélioré le résultat de [6] pour les équations de Fermat de signature $(13, 13, p)$.

Abstract. Let K be a totally real Galois number field and let $\mathcal{E}$ be a set of elliptic curves over K. We give sufficient conditions for the existence of a finite computable set of rational primes $\mathcal{P}$ such that for $p \notin \mathcal{P}$ and $E \in \mathcal{E}$, the representation $\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E[p])$ is irreducible. Our sufficient conditions are often satisfied for Frey elliptic curves associated to solutions of Diophantine equations; in that context, the irreducibility of the mod p representation is a hypothesis needed for applying level-lowering theorems. We illustrate our approach by improving on a result of [6] for Fermat-type equations of signature $(13, 13, p)$.

1. Introduction

The 'modular approach' is a popular method for attacking Diophantine equations using Galois representations of elliptic curves; see [1], [21] for recent surveys. The method relies on three important and difficult theorems.

(i) Wiles et al.: elliptic curves over $\mathbb{Q}$ are modular [3], [23], [22].

(ii) Mazur: if $E/\mathbb{Q}$ is an elliptic curve and $p > 167$ is a prime, then the Galois representation on the p-torsion of E is irreducible [15] (and variants of this result).

(iii) Ribet's level-lowering theorem [19].

Manuscrit reçu le 6 octobre 2013, accepté le 14 janvier 2014.

The second-named author is supported by an EPSRC Leadership Fellowship.

Mathematics Subject Classification. 11F80, 11G05.

The strategy of the method is to associate to a putative solution of certain Diophantine equations a Frey elliptic curve, and apply Ribet's level-lowering theorem to deduce a relationship between the putative solution and a modular form of relatively small level. Modularity (i) and irreducibility (ii) are necessary hypotheses that need to be verified in order to apply level-lowering (iii).

Attention is now shifting towards Diophantine equations where the Frey elliptic curves are defined over totally real fields (for example [2], [6], [7], [8]). One now finds in the literature some of the necessary modularity (e.g. [9]) and level-lowering theorems (e.g. [10], [12] and [18]) for the totally real setting. Unfortunately, there is as of yet no analogue of Mazur's Theorem over any number field $K \neq \mathbb{Q}$, which does present an obstacle for applying the modular approach over totally real fields.

Let K be a number field, and write $G_K = \mathrm{Gal}(\overline{K}/K)$. Let E an elliptic curve over K. Let p be a rational prime, and write $\overline{\rho}_{E,p}$ for the associated representation of G_K on the p-torsion of E:

$$\overline{\rho}_{E,p} \,:\, G_K \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p). \tag{1.1}$$

Mazur's Theorem asserts that if $K = \mathbb{Q}$ and $p > 167$ then $\overline{\rho}_{E,p}$ is irreducible. For a general number field K, it is expected that there is some B_K, such that for all elliptic curves E/K without complex multiplication, and all $p > B_K$, the mod p representation $\overline{\rho}_{E,p}$ is irreducible. Several papers, including those by Momose [17], Kraus [13], [14] and David [5], establish a bound B_K depending on the field K, under some restrictive assumptions on E, such as semistability. The Frey elliptic curves one deals with in the modular approach are close to being semistable [21, Section 15.2.4]. The purpose of this note is to prove the following theorem, which should usually be enough to supply the desired irreducibility statement in that setting.

Theorem 1. *Let K be a totally real Galois number field of degree d, with ring of integers $\mathcal{O}_K$ and Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$. Let $S = \{0, 12\}^G$, which we think of as the set of sequences of values 0, 12 indexed by $\tau \in G$. For $\mathbf{s} = (s_\tau) \in S$ and $\alpha \in K$, define the **twisted norm associated to** $\mathbf{s}$ by*

$$\mathcal{N}_{\mathbf{s}}(\alpha) = \prod_{\tau \in G} \tau(\alpha)^{s_\tau}.$$

Let $\epsilon_1, \dots, \epsilon_{d-1}$ be a basis for the unit group of K, and define

$$A_{\mathbf{s}} := \mathrm{Norm}\left(\gcd((\mathcal{N}_{\mathbf{s}}(\epsilon_1) - 1)\mathcal{O}_K, \dots, (\mathcal{N}_{\mathbf{s}}(\epsilon_{d-1}) - 1)\mathcal{O}_K)\right). \tag{1.2}$$

Let B be the least common multiple of the $A_{\mathbf{s}}$ taken over all $\mathbf{s} \neq (0)_{\tau \in G}$, $(12)_{\tau \in G}$. Let $p \nmid B$ be a rational prime, unramified in K, such that $p \geq 17$

or $p = 11$. Let E/K be an elliptic curve, and $\mathfrak{q} \nmid p$ be a prime of good reduction for E. Let

$$P_{\mathfrak{q}}(X) = X^2 - a_{\mathfrak{q}}(E)X + \mathrm{Norm}(\mathfrak{q})$$

be the characteristic polynomial of Frobenius for E at $\mathfrak{q}$. Let $r \geq 1$ be an integer such that $\mathfrak{q}^r$ is principal. If E is semistable at all $\mathfrak{p} \mid p$ and $\overline{\rho}_{E,p}$ is reducible then

$$p \mid \mathrm{Res}(\, P_{\mathfrak{q}}(X)\, ,\, X^{12r} - 1\,) \tag{1.3}$$

where Res *denotes resultant.*

We will see in due course that B above is non-zero. It is easy show that the resultant in (1.3) is also non-zero. The theorem therefore does give a bound on p so that $\overline{\rho}_{E,p}$ is reducible.

The main application we have in mind is to Frey elliptic curves associated to solutions of Fermat-style equations. In such a setting, one usually knows that the elliptic curve in question has semistable reduction outside a given set of primes, and one often knows some primes of potentially good reduction. We illustrate this, by giving an improvement to a recent theorem of Dieulefait and Freitas [6] on the equation $x^{13} + y^{13} = Cz^p$. In a forthcoming paper [2], the authors apply our Theorem 1 together with modularity and level-lowering theorems to completely solve the equation $x^{2n} \pm 6x^n + 1 = y^2$ in integers x, y, n with $n \geq 2$, after associating this to a Frey elliptic curve over $\mathbb{Q}(\sqrt{2})$. In another paper [7], the first-named author uses our Theorem 1 as part of an investigation that associates solutions of equations $x^r + y^r = Cz^p$ with (r, p prime) with Frey elliptic curves over real subfields of $\mathbb{Q}(\zeta_r)$.

The following is closely related to a result of David [5, Theorem 2], but formulated in a way that is more suitable for attacking specific examples.

Theorem 2. *Let K be a totally real Galois field of degree d. Let B be as in the statement of Theorem 1. Let $p \nmid B$ be a rational prime, unramified in K, such that $p \geq 17$ or $p = 11$. If E is an elliptic curve over K which is semistable at all $\mathfrak{p} \mid p$ and $\overline{\rho}_{E,p}$ is reducible then $p < (1 + 3^{6dh})^2$, where h is the class number of K.*

2. Preliminaries

We shall henceforth fix the following notation and assumptions.

K	a Galois number field,
d_K	the degree of $K/\mathbb{Q}$,
G_K	$\mathrm{Gal}(\overline{K}/K)$,
$\mathfrak{q}$	a finite prime of K,
$I_\mathfrak{q}$	the inertia subgroup of G_K corresponding to $\mathfrak{q}$,
G	$\mathrm{Gal}(K/\mathbb{Q})$,
p	a rational prime unramified in K satisfying $p \geq 17$, or $p = 11$,
χ_p	the mod p cyclotomic character $G_K \to \mathbb{F}_p^*$,
E	an elliptic curve semistable at all places $\mathfrak{p}$ of K above p,
$\overline{\rho}_{E,p}$	the mod p representation associated to E as in (1.1).

Suppose $\overline{\rho}_{E,p}$ is reducible. With an appropriate choice of basis for $E[p]$ we can write

$$\overline{\rho}_{E,p} \sim \begin{pmatrix} \lambda & * \\ 0 & \lambda' \end{pmatrix}, \tag{2.1}$$

where λ, $\lambda' : G_K \to \mathbb{F}_p^*$ are characters. Thus $\lambda\lambda' = \det(\overline{\rho}_{E,p}) = \chi_p$. The character λ is known as the **isogeny character** of $E[p]$.

As in the aforementioned works of Momose, Kraus and David, our approach relies on controlling the ramification of the characters λ, λ' at places above p.

Proposition 2.1. (David [5, Propositions 1.2, 1.3]) *Suppose $\overline{\rho}_{E,p}$ is reducible and let λ, λ' be as above. Let $\mathfrak{p} \mid p$ be a prime of K. Then*

$$\lambda^{12}|_{I_\mathfrak{p}} = (\chi_\mathfrak{p}|_{I_\mathfrak{p}})^{s_\mathfrak{p}}$$

where $s_\mathfrak{p} \in \{0, 12\}$.

Proof. Indeed, by [5, Propositions 1.2, 1.3],

(i) if $\mathfrak{p}$ is a prime of potentially multiplicative reduction or potentially good ordinary reduction for E then $s_\mathfrak{p} = 0$ or $s_\mathfrak{p} = 12$;
(ii) if $\mathfrak{p}$ is a prime of potentially good supersingular reduction for E then $s_\mathfrak{p} = 4$, 6, 8.

However, we have assumed that E is semistable at $\mathfrak{p} \mid p$ and that p is unramified in K. By Serre [20, Proposition 12], if E has good supersingular reduction at $\mathfrak{p}$, then the image of $\overline{\rho}_{E,p}$ contains a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ and is therefore irreducible, contradicting the assumption that $\overline{\rho}_{E,p}$ is reducible. Hence E has multiplicative or good ordinary reduction at $\mathfrak{p}$. □

Remark. The order of $\chi_\mathfrak{p}|_{I_\mathfrak{p}}$ is $p - 1$. Hence the value of $s_\mathfrak{p}$ in the above proposition is well-defined modulo $p - 1$. Of course, since $0 \leq s_\mathfrak{p} \leq 12$, it follows for $p \geq 17$ that $s_\mathfrak{p}$ is unique.

As K is Galois, G acts transitively of $\mathfrak{p} \mid p$. Fix $\mathfrak{p}_0 \mid p$. For each $\tau \in G$ write s_τ for the number $s_\mathfrak{p}$ associated to the ideal $\mathfrak{p} := \tau^{-1}(\mathfrak{p}_0)$ by the previous proposition. We shall refer to $\mathbf{s} := (s_\tau)_{\tau \in G}$ as the **isogeny signature** of E at p. The set $S := \{0, 12\}^G$ shall denote the set of all possible sequences of values 0, 12 indexed by elements of G. For an element $\alpha \in K$, we define the **twisted norm associated to $\mathbf{s} \in S$** by

$$\mathcal{N}_\mathbf{s}(\alpha) = \prod_{\tau \in G} \tau(\alpha)^{s_\tau}.$$

Proposition 2.2. (David [5, Proposition 2.6]) *Suppose $\overline{\rho}_{E,p}$ is reducible with isogeny character λ, having isogeny signature $\mathbf{s} \in S$. Let $\alpha \in K$ be non-zero. Suppose $\upsilon_\mathfrak{p}(\alpha) = 0$ for all $\mathfrak{p} \mid p$. Then*

$$\mathcal{N}_\mathbf{s}(\alpha) \equiv \prod \left(\lambda^{12}(\sigma_\mathfrak{q})\right)^{\upsilon_\mathfrak{q}(\alpha)} \pmod{\mathfrak{p}_0},$$

where the product is taken over all prime $\mathfrak{q}$ in the support of α.

3. A bound in terms of a prime of potentially good reduction

Let $\mathfrak{q}$ be a prime of potentially good reduction for E. Denote by $P_\mathfrak{q}(X)$ the characteristic polynomial of Frobenius for E at $\mathfrak{q}$.

Lemma 3.1. *Let $\mathfrak{q}$ be a prime of potentially good reduction for E, and suppose $\mathfrak{q} \nmid p$. Let $r \geq 1$ be such that $\mathfrak{q}^r$ is principal, and write $\alpha\mathcal{O}_K = \mathfrak{q}^r$. Let $\mathbf{s} = (s_\tau)_{\tau \in G}$ be the isogeny signature of E at p. Then*

$$\mathfrak{p}_0 \mid \mathrm{Res}(\, P_\mathfrak{q}(X)\,,\, X^{12r} - \mathcal{N}_\mathbf{s}(\alpha)\,),$$

where Res *denotes the resultant.*

Proof. From (2.1), it is clear that

$$P_\mathfrak{q}(X) \equiv (X - \lambda(\sigma_\mathfrak{q}))(X - \lambda'(\sigma_\mathfrak{q})) \pmod{p}.$$

Moreover, from Proposition 2.2, $\lambda(\sigma_\mathfrak{q})$ is a root modulo $\mathfrak{p}_0$ of the polynomial $X^{12r} - \mathcal{N}_\mathbf{s}(\alpha)$. As $\mathfrak{p}_0 \mid p$, the lemma follows. □

We note the following surprising consequence.

Corollary 3.2. *Let ϵ be a unit of $\mathcal{O}_K$. If the isogeny signature of E at p is $\mathbf{s}$ then $\mathcal{N}_\mathbf{s}(\epsilon) \equiv 1 \pmod{\mathfrak{p}_0}$.*

Proof. Let $\mathfrak{q} \nmid p$ be any prime of good reduction of E. Let h be the class number of K. Choose any $\alpha \in \mathcal{O}_K$ so that $\alpha\mathcal{O}_K = \mathfrak{q}^h$. By Proposition 2.2,

$$\mathcal{N}_\mathbf{s}(\alpha) \equiv (\lambda(\sigma_\mathfrak{q}))^{12h} \pmod{\mathfrak{p}_0}.$$

However, if ϵ is unit, then $\epsilon\alpha\mathcal{O}_K = \mathfrak{q}^h$ too. So

$$\mathcal{N}_\mathbf{s}(\epsilon\alpha) \equiv (\lambda(\sigma_\mathfrak{q}))^{12h} \pmod{\mathfrak{p}_0}.$$

Taking ratios we have $\mathcal{N}_\mathbf{s}(\epsilon) \equiv 1 \pmod{\mathfrak{p}_0}$. □

Corollary 3.2 is only useful in bounding p for a given signature $\mathbf{s}$, if there is some unit ϵ of K such that $\mathcal{N}_{\mathbf{s}}(\epsilon) \neq 1$. Of course, if $\mathbf{s}$ is either of the constant signatures $(0)_{\tau\in G}$ or $(12)_{\tau\in G}$ then

$$\mathcal{N}_{\mathbf{s}}(\epsilon) = (\operatorname{Norm} \epsilon)^{0 \text{ or } 12} = 1.$$

Given a non-constant signature $\mathbf{s} \in S$, does there exist a unit ϵ such that $\mathcal{N}_{\mathbf{s}}(\epsilon) \neq 1$? It is easy construct examples where the answer is no. The following lemma gives a positive answer when K is totally real.

Lemma 3.3. *Let K be totally real of degree $d \geq 2$. Suppose $\mathbf{s} \neq (0)_{\tau\in G}$, $\neq (12)_{\tau\in G}$. Then there exists a unit ϵ of K such that $\mathcal{N}_{\mathbf{s}}(\epsilon) \neq 1$.*

Proof. Let $\tau_1, \dots, \tau_d$ be the elements of G. Fix an embedding $\sigma : K \hookrightarrow \mathbb{R}$, and denote $\sigma_i = \sigma \circ \tau_i$. Rearranging the elements of G, we may suppose that

$$s_{\tau_1} = \cdots = s_{\tau_r} = 12, \qquad s_{\tau_{r+1}} = \cdots = s_{\tau_d} = 0$$

where $1 \leq r \leq d-1$. Suppose that $\mathcal{N}_{\mathbf{s}}(\epsilon) = 1$ for all $\epsilon \in U(K)$, where $U(K)$ is the unit group of K. Then the image of $U(K)$ under the Dirichlet embedding

$$U(K)/\{\pm 1\} \hookrightarrow \mathbb{R}^{d-1}, \qquad \epsilon \mapsto (\log|\sigma_1(\epsilon)|, \dots, \log|\sigma_{d-1}(\epsilon)|)$$

is contained in the hyperplane $x_1 + x_2 + \cdots + x_r = 0$. This contradicts the fact the image must be a lattice in $\mathbb{R}^{d-1}$ of rank $d-1$. ☐

4. Proof of Theorem 1

We now prove Theorem 1. Suppose $\overline{\rho}_{E,p}$ is reducible and let $\mathbf{s}$ be the isogeny signature. Let $A_{\mathbf{s}}$ be as in (1.2). By Corollary 3.2, $p \mid A_{\mathbf{s}}$. If $\mathbf{s} \neq (0)_{\tau\in G}$, $(12)_{\tau\in G}$ then $A_{\mathbf{s}} \neq 0$ by Lemma 3.3. Now, suppose $p \nmid B$, where B is as in the statement of Theorem 1. Then $\mathbf{s} = (0)_{\tau\in G}$, $(12)_{\tau\in G}$.

Suppose first that $\mathbf{s} = (0)_{\tau\in G}$. Then $\mathcal{N}_{\mathbf{s}}(\alpha) = 1$ for all α. Let $\mathfrak{q} \nmid p$ be a prime of good reduction for E. It follows from Lemma 3.1 that $\mathfrak{p}_0$ divides the resultant of $P_{\mathfrak{q}}(X)$ and $X^{12r} - 1$. As both polynomials have coefficients in $\mathbb{Z}$, the resultant belongs to $\mathbb{Z}$, and so is divisible by p. This completes the proof for $\mathbf{s} = (0)_{\tau\in G}$.

Finally, we deal with the case $\mathbf{s} = (12)_{\tau\in G}$. Let $C \subset E[p]$ be the subgroup of order p corresponding to λ. Replacing E by the isogenous curve $E' = E/C$ has the effect of swapping λ and λ' in (2.1). As $\lambda\lambda' = \chi_p$, the isogeny signature for E' at p is $(0)_{\tau\in G}$. The theorem follows.

5. Proof of Theorem 2

Suppose $\overline{\rho}_{E,p}$ is reducible with signature $\mathbf{s}$. As in the proof of Theorem 1, we may suppose $\mathbf{s} = (0)_{\tau\in G}$ or $\mathbf{s} = (12)_{\tau\in G}$. Moreover, replacing E by an isogenous elliptic curve we may suppose that $\mathbf{s} = (0)_{\tau\in G}$. By definition of $\mathbf{s}$, we have λ^{12} is unramified at all $\mathfrak{p} \mid p$. As is well-known (see for example [5, Proposition 1.4 and Proposition 1.5]), λ^{12} is unramified at the finite places outside p; λ^{12} is clearly unramified at the infinite places because of the even exponent 12. Thus λ^{12} is everywhere unramified. Thus λ has order dividing $12 \cdot h$, where h is the class number of K. Let L/K be the extension cut out by λ; this has degree dividing $12 \cdot h$. Then E/L has a point of order p. Applying Merel's bounds [16], we conclude that

$$p < (1 + 3^{[L:\mathbb{Q}]/2})^2 \leq (1 + 3^{6dh})^2.$$

6. An Example: Frey Curves Attached to Fermat Equations of Signature $(13, 13, p)$

In [6], Dieulefait and Freitas, used the modular method to attack certain Fermat-type equations of the form $x^{13} + y^{13} = Cz^p$, for infinitely many values of C. They attach Frey curves (independent of C) over $\mathbb{Q}(\sqrt{13})$ to primitive solutions of these equations, and prove irreducibility of the mod p representations attached to these Frey curves, for $p > 7$ and $p \neq 13$, 37 under the assumption that the isogeny signatures are $(0,0)$ or $(12,12)$. Here we improve on the argument by dealing with the isogeny signature $(0,12)$, $(12,0)$ and also by dealing with $p = 37$. More precisely, we prove the following.

Theorem 3. *Let $d = 3$, 5, 7 or 11 and let γ be an integer divisible only by primes $\ell \not\equiv 1 \pmod{13}$. Let p be a prime satisfying $p \geq 17$ or $p = 11$. Let $(a, b, c) \in \mathbb{Z}^3$ satisfy*

$$a^{13} + b^{13} = d\gamma c^p, \qquad \gcd(a, b) = 1, \qquad abc \neq 0, \pm 1.$$

Write $K = \mathbb{Q}(\sqrt{13})$; this has class number 1. Let $E = E_{(a,b)}/K$ be the Frey curve defined in [6]. Then, the Galois representation $\overline{\rho}_{E,p}$ is irreducible.

Proof. Suppose $\overline{\rho}_{E,p}$ is reducible. For a quadratic field such as K, the set S of possible isogeny signatures $(s_\tau)_{\tau \in G}$ is

$$S = \{(12, 12), (12, 0), (0, 12), (0, 0)\}.$$

Note that $(13) = (\sqrt{13})^2$ is the only prime ramifying in K. In [6] it is shown that the curves E have additive reduction only at 2 and $\sqrt{13}$. Moreover, E has good reduction at all primes $\mathfrak{q} \nmid 26$ above rational primes $q \not\equiv 1 \pmod{13}$. Furthermore, the trace $a_{\mathfrak{q}}(E_{(a,b)})$ depends only on the values of a, b modulo q. By the assumption $\gcd(a, b) = 1$, we have $(a, b) \not\equiv 0 \pmod{q}$.

The fundamental unit of K is $\epsilon = (3 + \sqrt{13})/2$. Then

$$\mathrm{Norm}(\epsilon^{12} - 1) = -2^6 \cdot 3^4 \cdot 5^2 \cdot 13.$$

As $p \geq 17$ or $p = 11$, it follows from Corollary 3.2 that the isogeny signature of E at p is either $(0,0)$ or $(12,12)$. As in the proof of Theorem 1, we may suppose that the isogeny signature is $(0,0)$.

Let q be a rational prime $\not\equiv 1 \pmod{13}$ that splits as $(q) = \mathfrak{q}_1 \cdot \mathfrak{q}_2$ in K. By the above, $\mathfrak{q}_1$, $\mathfrak{q}_2$ must be primes of good reduction. The trace $a_{\mathfrak{q}_i}(E_{(a,b)})$ depends only on the values of a, b modulo q. For each non-zero pair $(a,b) \pmod{q}$, let

(6.1)
$$P_{\mathfrak{q}_1}^{(a,b)}(X) = X^2 - a_{\mathfrak{q}_1}(E_{(a,b)})X + q \qquad P_{\mathfrak{q}_2}^{(a,b)}(X) = x^2 - a_{\mathfrak{q}_2}(E_{(a,b)})x + q,$$

be the characteristic polynomials of Frobenius at $\mathfrak{q}_1$, $\mathfrak{q}_2$. Let

$$R_q^{a,b} = \gcd(\,\mathrm{Res}(P_{\mathfrak{q}_1}^{a,b}(X), X^{12}-1)\,,\,\mathrm{Res}(P_{\mathfrak{q}_2}^{a,b}(X), X^{12}-1)\,).$$

Let

$$R_q = \mathrm{lcm}\{R_q^{a,b}\ : 0 \le a, b \le q-1, \qquad (a,b) \neq (0,0)\}.$$

By the proof of Theorem 1, we have that p divides R_q. Using a short `SAGE` script we computed the values of R_q for $q = 3$, 17. We have

$$R_3 = 2^6 \cdot 3^2 \cdot 5^2 \cdot 37, \qquad R_{17} = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 19 \cdot 23 \cdot 53 \cdot 97 \cdot 281 \cdot 21481 \cdot 22777.$$

As $p \ge 17$ or $p = 11$ we see that $\bar{\rho}_{E,p}$ is irreducible. ☐

We will now use the improved irreducibility result (Theorem 3) to correctly restate Theorem 1.3 in [6]. Furthermore, we will also add an argument using the primes above 17 that actually allows us to improve it. More precisely, we will prove.

Theorem 4. *Let $d = 3$, 5, 7 or 11 and let γ be an integer divisible only by primes $\ell \not\equiv 1 \pmod{13}$. Let also $\mathcal{L} := \{2,3,5,7,11,13,19,23,29,71\}$.*

If p is a prime not belonging to $\mathcal{L}$, then:

(I) *The equation $x^{13} + y^{13} = d\gamma z^p$ has no solutions (a,b,c) such that*
$$\gcd(a,b) = 1, \qquad abc \neq 0, \pm 1 \qquad \text{and} \qquad 13 \nmid c.$$

(II) *The equation $x^{26} + y^{26} = 10\gamma z^p$ has no solutions (a,b,c) such that*
$$\gcd(a,b) = 1, \qquad \text{and} \qquad abc \neq 0, \pm 1.$$

Proof. Suppose there is a solution (a,b,c), satisfying $\gcd(a,b) = 1$, to the equation in part (I) of the theorem for $p \ge 17$ or $p = 11$. Let $E = E_{(a,b)}$ be the Frey curves attached to it in [6]. As explained in [6], but now using Theorem 3 above instead of Theorem 4.1 in *loc. cit.*, we obtain an isomorphism

$$\bar{\rho}_{E,p} \sim \bar{\rho}_{f,\mathfrak{p}}, \tag{6.2}$$

where $\mathfrak{p} \mid p$ and $f \in S_2(2^i w^2)$ for $i = 3, 4$. In *loc. cit* the newforms are divided into the sets

S1: The newforms in $S_2(2^i w^2)$ for $i = 3, 4$ such that $\mathbb{Q}_f = \mathbb{Q}$,
S2: The newforms in the same levels with $\mathbb{Q}_f$ strictly containing $\mathbb{Q}$.

We eliminate the newforms in S1 with the same argument as in [6]. Suppose now that isomorphism (6.2) holds with a form in S2. Also in [6], using the primes dividing 3, a contradiction is obtained if we assume that

$$p \notin \mathcal{P} = \{2, 3, 5, 7, 11, 13, 19, 23, 29, 71, 191, 251, 439, 1511, 13649\}.$$

Going through analogous computations, using the two primes dividing 17, gives a contradiction if p does not belong to

$$\begin{aligned}\mathcal{P}' = \{&2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 37, 41, 43, 47, 59, 71, 73, 79, 83, 89, 109, \\ &113, 157, 167, 197, 227, 229, 239, 281, 359, 431, 461, 541, 1429, 5237, 253273, \\ &271499, 609979, 6125701, 93797731, 530547937, 733958569, 6075773983, \\ &11740264873\}.\end{aligned}$$

Thus, we have a contradiction as long as p is not in the intersection

$$\mathcal{P} \cap \mathcal{P}' = \{2, 3, 5, 7, 11, 13, 19, 23, 29, 71\}.$$

Thus part (I) of the theorem follows. Part (II) follows exactly as in [6] □

References

[1] M.A. Bennett, I. Chen, S.R. Dahmen and S. Yazdani, *Generalized Fermat equations: a miscellany*, preprint, (2013).

[2] M.A. Bennett, S.R. Dahmen, M. Mignotte and S. Siksek, *Shifted powers in binary recurrence sequences*, Mathematical Proceedings Cambridge Philosophical Society, **158**, (2015), 305–329.

[3] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, Journal of the American Mathematical Society **14**, (2001), 843–939.

[4] H. Cohen, *Number Theory, Volume II: Analytic and Modern Tools*, GTM 240, Springer-Verlag, (2007).

[5] A. David, *Caractère d'isogénie et critéres d'irréductibilité*, `arXiv:1103.3892v2`.

[6] L. Dieulefait and N. Freitas, *Fermat-type equations of signature* $(13, 13, p)$ *via Hilbert cuspforms*, Math. Ann. **357**, 3 (2013), 987–1004.

[7] N. Freitas, *Recipes to Fermat-type equations of the form* $x^r + y^r = Cz^p$, Mathematische Zeitschrift, **279**, (2015), 605–639.

[8] N. Freitas and S. Siksek, *The asymptotic Fermat's last theorem for five-sixths of real quadratic fields*, Compositio Mathematica, to appear.

[9] N. Freitas, B.V. Le Hung and S. Siksek, *Elliptic curves over real quadratic fields are modular*, Inventiones Mathematicae, to appear.

[10] K. Fujiwara, *Level optimisation in the totally real case*, `arXiv:math/0602586v1`.

[11] F. Jarvis, *Level lowering for modular mod ℓ representations over totally real fields*, Math.Ann. **313**, 1 (1999), 141–160.

[12] F. Jarvis, *Correspondences on Shimura curves and Mazur's principle at p*, Pacific J. Math., **213**, 2 (2004), 267–280.

[13] A. Kraus, *Courbes elliptiques semi-stables et corps quadratiques*, Journal of Number Theory **60**, (1996), 245–253.

[14] A. Kraus, *Courbes elliptiques semi-stables sur les corps de nombres*, International Journal of Number Theory **3**, (2007), 611–633.

[15] B. Mazur, *Rational isogenies of prime degree*, Inventiones Math. **44**, (1978), 129–162.

[16] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent.Math. **124**, (1996), 437–449.

[17] F. Momose, *Isogenies of prime degree over number fields*, Compositio Mathematica, **97**, (1995), 329–348.

[18] A. Rajaei, *On the levels of mod ℓ Hilbert modular forms*, J. Reine Angew. Math., **537**, (2001), 33–65.

[19] K.A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Inventiones Math., **100**, (1990), 431–476.

[20] J.-P. Serre, *Properiétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inventiones Math., **15**, (1972), 259–331.

[21] S. Siksek, *The modular approach to Diophantine equations*, chapter 15 of [4].

[22] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Annals of Mathematics **141**, 3 (1995), 553–572.

[23] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Mathematics **141**, 3 (1995), 443–551.

Nuno Freitas
Mathematisches Institut
Universität Bayreuth
95440 Bayreuth, Germany
E-mail: nunobfreitas@gmail.com

Samir Siksek
Mathematics Institute
University of Warwick
CV4 7AL
United Kingdom
E-mail: samir.siksek@gmail.com