Nuno FREITAS et Samir SIKSEK

Criteria for Irreducibility of mod $p$ Representations of Frey Curves


<http://jtnb.cedram.org/item?id=JTNB_2015__27_1_67_0>
Criteria for Irreducibility of mod $p$
Representations of Frey Curves

par Nuno FREITAS et Samir SIKSEK

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

\begin{equation}
\rho_{E,p} : G_K \to \text{Aut}(E[p]) \cong \text{GL}_2(\mathbb{F}_p).
\end{equation}

Mazur’s Theorem asserts that if $K = \mathbb{Q}$ and $p > 167$ then $\rho_{E,p}$ 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 $\rho_{E,p}$ 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 $G = \text{Gal}(K/\mathbb{Q})$. Let $S = \{0, 12\}^G$, which we think of as the set of sequences of values $0, 12$ indexed by $\tau \in G$. For $s = (s_\tau) \in S$ and $\alpha \in K$, define the **twisted norm associated to $s$** by

\[ N_s(\alpha) = \prod_{\tau \in G} \tau(\alpha)^{s_\tau}. \]

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

\begin{equation}
A_s := \text{Norm}(\gcd((N_s(\epsilon_1) - 1)\mathcal{O}_K, \ldots, (N_s(\epsilon_{d-1}) - 1)\mathcal{O}_K)).
\end{equation}

Let $B$ be the least common multiple of the $A_s$ taken over all $s \neq (0)_{\tau \in G}$, $(12)_{\tau \in G}$. 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 $q \nmid p$ be a prime of good reduction for $E$. Let

$$P_q(X) = X^2 - a_q(E)X + \text{Norm}(q)$$

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

$$(1.3) \quad p \mid \text{Res}(P_q(X), X^{12r} - 1)$$

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 $\rho_{E,p}$ 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 $(r, p \text{ prime})$ 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 $p | p$ and $\rho_{E,p}$ is reducible then $p < (1 + 3^{6h})^2$, where $h$ is the class number of $K$.

**2. Preliminaries**

We shall henceforth fix the following notation and assumptions.
Suppose $\overline{\rho}_{E,p}$ is reducible. With an appropriate choice of basis for $E[p]$ we can write

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

where $\lambda, \lambda' : G_K \to \mathbb{F}_p^*$ are characters. Thus $\lambda \lambda' = \det(\overline{\rho}_{E,p}) = \chi_p$. The character $\lambda$ 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 $\lambda, \lambda'$ at places above $p$.

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

$$
\lambda^{12} | I_p = (\chi_p | I_p)^{s_p}
$$

where $s_p \in \{0, 12\}$.

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

(i) if $p$ is a prime of potentially multiplicative reduction or potentially good ordinary reduction for $E$ then $s_p = 0$ or $s_p = 12$;

(ii) if $p$ is a prime of potentially good supersingular reduction for $E$ then $s_p = 4, 6, 8$.

However, we have assumed that $E$ is semistable at $p$ and that $p$ is unramified in $K$. By Serre [20, Proposition 12], if $E$ has good supersingular reduction at $p$, then the image of $\overline{\rho}_{E,p}$ contains a non-split Cartan subgroup of $GL_2(\mathbb{F}_p)$ and is therefore irreducible, contradicting the assumption that $\overline{\rho}_{E,p}$ is reducible. Hence $E$ has multiplicative or good ordinary reduction at $p$. \hfill \Box

**Remark.** The order of $\chi_p | I_p$ is $p - 1$. Hence the value of $s_p$ in the above proposition is well-defined modulo $p - 1$. Of course, since $0 \leq s_p \leq 12$, it follows for $p \geq 17$ that $s_p$ is unique.
As $K$ is Galois, $G$ acts transitively of $p \mid p$. Fix $p_0 \mid p$. For each $\tau \in G$ write $s_\tau$ for the number $s_p$ associated to the ideal $p := \tau^{-1}(p_0)$ by the previous proposition. We shall refer to $s := (s_\tau)_{\tau \in G}$ 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 $s \in S$ by

$$N_s(\alpha) = \prod_{\tau \in G} \tau(\alpha)^{s_\tau}.$$ 

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

$$N_s(\alpha) \equiv \prod \left( \lambda^{12}(\sigma_q) \right)^{v_q(\alpha)} \pmod{p_0},$$

where the product is taken over all prime $q$ in the support of $\alpha$.

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

Let $q$ be a prime of potentially good reduction for $E$. Denote by $P_q(X)$ the characteristic polynomial of Frobenius for $E$ at $q$.

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

$$p_0 \mid \text{Res}(P_q(X), X^{12r} - N_s(\alpha)),$$

where $\text{Res}$ denotes the resultant.

**Proof.** From (2.1), it is clear that

$$P_q(X) \equiv (X - \lambda(\sigma_q))(X - \lambda'(\sigma_q)) \pmod{p}.$$ 

Moreover, from Proposition 2.2, $\lambda(\sigma_q)$ is a root modulo $p_0$ of the polynomial $X^{12r} - N_s(\alpha)$. As $p_0 \mid p$, the lemma follows. \hfill $\square$

We note the following surprising consequence.

**Corollary 3.2.** Let $\epsilon$ be a unit of $\mathcal{O}_K$. If the isogeny signature of $E$ at $p$ is $s$ then $N_s(\epsilon) \equiv 1 \pmod{p_0}$.

**Proof.** Let $q \nmid p$ 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 $\alpha\mathcal{O}_K = q^h$. By Proposition 2.2,

$$N_s(\alpha) \equiv (\lambda(\sigma_q))^{12h} \pmod{p_0}.$$ 

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

$$N_s(\epsilon\alpha) \equiv (\lambda(\sigma_q))^{12h} \pmod{p_0}.$$ 

Taking ratios we have $N_s(\epsilon) \equiv 1 \pmod{p_0}$. \hfill $\square$
Corollary 3.2 is only useful in bounding \( p \) for a given signature \( s \), if there is some unit \( \epsilon \) of \( K \) such that \( \mathcal{N}_s(\epsilon) \neq 1 \). Of course, if \( s \) is either of the constant signatures \((0)_{\tau \in G}\) or \((12)_{\tau \in G}\) then
\[
\mathcal{N}_s(\epsilon) = (\text{Norm } \epsilon)^0 \text{ or } 12 = 1.
\]
Given a non-constant signature \( s \in S \), does there exist a unit \( \epsilon \) such that \( \mathcal{N}_s(\epsilon) \neq 1 \)? 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 \( s \neq (0)_{\tau \in G}, (12)_{\tau \in G} \). Then there exists a unit \( \epsilon \) of \( K \) such that \( \mathcal{N}_s(\epsilon) \neq 1 \).

**Proof.** Let \( \tau_1, \ldots, \tau_d \) 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
\[
s_{\tau_1} = \cdots = s_{\tau_r} = 12, \quad s_{\tau_{r+1}} = \cdots = s_{\tau_d} = 0
\]
where \( 1 \leq r \leq d - 1 \). Suppose that \( \mathcal{N}_s(\epsilon) = 1 \) 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
\[
U(K)/\{\pm 1\} \hookrightarrow \mathbb{R}^{d-1}, \quad \epsilon \mapsto (\log |\sigma_1(\epsilon)|, \ldots, \log |\sigma_{d-1}(\epsilon)|)
\]
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 \( d - 1 \).

\( \square \)

### 4. Proof of Theorem 1

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

Suppose first that \( s = (0)_{\tau \in G} \). Then \( \mathcal{N}_s(\alpha) = 1 \) for all \( \alpha \). Let \( q \nmid p \) be a prime of good reduction for \( E \). It follows from Lemma 3.1 that \( p_0 \) divides the resultant of \( P_q(X) \) 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 \( s = (0)_{\tau \in G} \).

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

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

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 $x^{13} + y^{13} = C^{p}$, 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 $\gamma$ 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

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

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 $q \nmid 26$ above rational primes $q \not\equiv 1 \pmod{13}$. Furthermore, the trace $a_{q}(E_{(a,b)})$ 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

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

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 $(0, 0)$. 

Irreducibility of mod $p$ Representations

73
Let \( q \) be a rational prime \( \not\equiv 1 \pmod{13} \) that splits as \( (q) = q_1 \cdot q_2 \) in \( K \). By the above, \( q_1, q_2 \) must be primes of good reduction. The trace \( a_{q_i}(E_{(a,b)}) \) depends only on the values of \( a, b \) modulo \( q \). For each non-zero pair \( (a, b) \) (mod \( q \)), let

\[
(6.1) \quad P_{q_1}^{a,b}(X) = X^2 - a_{q_1}(E_{(a,b)})X + q, \quad P_{q_2}^{a,b}(X) = x^2 - a_{q_2}(E_{(a,b)})x + q,
\]

be the characteristic polynomials of Frobenius at \( q_1, q_2 \). Let

\[
R_{q}^{a,b} = \gcd( \text{Res}(P_{q_1}^{a,b}(X), X^{12} - 1), \text{Res}(P_{q_2}^{a,b}(X), X^{12} - 1) ).
\]

Let

\[
R_q = \text{lcm}\{ R_q^{a,b} : 0 \leq a, b \leq q - 1, \quad (a, b) \neq (0, 0) \}.
\]

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

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

As \( p \geq 17 \) or \( p = 11 \) we see that \( \bar{\rho}_{E,p} \) is irreducible. \( \square \)

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 \( \gamma \) be an integer divisible only by primes \( \ell \neq 1 \) (mod 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 \( \gcd(a, b) = 1, \quad ab \neq 0, \pm 1 \) and \( 13 \nmid c \).

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

**Proof.** Suppose there is a solution \( (a, b, c) \), satisfying \( \gcd(a, b) = 1 \), to the equation in part (I) of the theorem for \( p \geq 17 \) 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

\[
(6.2) \quad \bar{\rho}_{E,p} \sim \bar{\rho}_{f,p},
\]

where \( p \mid p \) 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 $S_1$ with the same argument as in [6]. Suppose now that isomorphism (6.2) holds with a form in $S_2$. Also in [6], using the primes dividing 3, a contradiction is obtained if we assume that

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

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


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

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

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

References


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