Fermat-type equations of signature $(13, 13, p)$ via Hilbert cuspforms

Luis Dieulefait · Nuno Freitas

Abstract In this paper we prove that for $p > 13649$ equations of the form $x^{13} + y^{13} = Cz^p$ have no non-trivial primitive solutions $(a, b, c)$ such that $13 \nmid c$ for an infinite family of values for $C$. Our method consists on relating a solution $(a, b, c)$ to the previous equation to a solution $(a, b, c_1)$ of another Diophantine equation with coefficients in $\mathbb{Q}(\sqrt{13})$. Then we attach to $(a, b, c_1)$ a Frey curve $E_{(a,b)}$ defined over $\mathbb{Q}(\sqrt{13})$ that is not a $\mathbb{Q}$-curve. We prove a modularity result of independent interest for certain elliptic curves over totally real abelian number fields satisfying some local conditions at 3. This theorem, in particular, implies modularity of $E_{(a,b)}$. This enables us to use level lowering results and apply the modular approach via Hilbert cuspforms over $\mathbb{Q}(\sqrt{13})$ to prove the non-existence of $(a, b, c_1)$ and, consequently, of $(a, b, c)$.

Mathematics Subject Classification (2010) Primary 11D41 · 11F80; Secondary 11G05

L. Dieulefait supported by project MICINN MTM2009-07024 from MECD, Spain, and ICREA Academia Research Prize.
N. Freitas supported by the scholarship with reference SFRH/BD/44283/2008 from Fundação para a Ciência e a Tecnologia, Portugal.
1 Introduction

Since Wiles’ [31] proof of Fermat’s Last Theorem, the modular approach to Diophantine equations has become increasingly popular. In particular, the original strategy of Frey, Hellegouarch, Serre, Ribet and Wiles was strengthened and achieved great success in solving other equations that previously seemed intractable. As a consequence of these efforts, the generalized Fermat equation

$$Ax^p + By^q = Cz^r,$$  \hspace{1cm} (1)

with $p, q, r$ primes and $A, B, C$ pairwise coprime integers became the new focus of attention. It is conjectured that for a fixed triple $A, B, C$ the equation (1) admits only a finite number of non-trivial solutions $(x, y, z, p, q, r)$ satisfying $\gcd(x, y, z) = 1$. This conjecture has been proved to be true in various particular cases, including infinite families of exponents. In particular, an important progress was the work of Ellenberg on the representations attached to $\mathbb{Q}$-curves. It allowed him to introduce the use of $\mathbb{Q}$-curves as Frey curves and, in particular, led him to solving the equation $x^4 + y^2 = z^p$ (see [15] and [2]). Moreover, another important result from Darmon-Granville [11] states that for a fixed triple $(p, q, r)$ there exists only a finite number of solutions satisfying $\gcd(x, y, z) = 1$. For a recent overview and summary of known results see the introduction in [1].

Another particularly important subfamily of the generalized Fermat equation are the equations of signature $(r, r, p)$, that is, $Ax^r + By^r = Cz^p$ with $r$ a fixed prime. For this type of signatures there is work for $(3, 3, p)$ by Kraus [22], Bruin [7], Chen-Siksek [9] and Dahmen [10]; for $(5, 5, p)$ by Billerey [3], Dieulefait-Billerey [4] and the authors [14]; for $(7, 7, p)$ by the second author [16]. In this paper we will go further into this family of equations by applying a modular approach via Hilbert modular forms to study equations of signature $(13, 13, p)$ with the form

$$x^{13} + y^{13} = Cz^p.$$  \hspace{1cm} (2)

Given a solution $(a, b, c)$ of equation (2) we will call it a primitive solution if $(a, b) = 1$ (in particular, $\gcd(a, b, c) = 1$) and we will also say it is a trivial solution if $|abc| \leq 1$. The following definition follows the terminology introduced by Sophie Germain in her work on the FLT and, after taking $r = 13$, divides solutions of (2) into two cases.

**Definition 1.1** A primitive solution $(a, b, c)$ of $x^r + y^r = Cz^p$ is called a first case solution if $r$ do not divide $c$, and a second case solution otherwise.

Summarily, the strategy we will use goes as follows: we first relate a putative non-trivial primitive solution of (2) to a solution $(a, b, c)$ of another Diophantine equation (independent of $C$) with coefficients in $\mathbb{Q}(\sqrt{13})$. Second, we attach to the latter solution a Frey curve $E$ over $\mathbb{Q}(\sqrt{13})$ that is not a $\mathbb{Q}$-curve. We then prove a modularity result of independent interest for certain elliptic curves that, in particular, guarantees modularity of $E$. 
Theorem 1.2 Let $F$ be a totally real abelian number field and $C$ an elliptic curve defined over $F$. Suppose that $3$ splits completely in $F$ and that $C$ has good reduction at the primes above $3$. Then $C$ is modular.

With modularity established, we prove irreducibility of $\tilde{\rho}_{E,p}$ for $p$ greater than an explicit constant. Then from the level lowering results for Hilbert modular forms it follows that the existence of the solution $(a, b, c)$ implies an isomorphism between two residual Galois representations. More precisely, $\tilde{\rho}_{E,p} \sim \tilde{\rho}_{f,P}$, where $f$ is a Hilbert newform over $\mathbb{Q}(\sqrt{13})$ and weight $(2, 2)$, with level almost independent of $(a, b, c)$. Finally we will show that if $13 \nmid a + b$ this isomorphism cannot hold and so the equation over $\mathbb{Q}(\sqrt{13})$ cannot have non-trivial primitive solutions satisfying $13 \nmid a + b$. Consequently (2) cannot have non-trivial primitive first case solutions. The main arithmetic result regarding equation (2) in this paper is the following theorem.

Theorem 1.3 Let $d = 3, 5, 7$ or $11$ and $\gamma$ be an integer divisible only by primes $\ell \not\equiv 1 \pmod{13}$. Let also $\mathcal{L} := \{2, 3, 5, 7, 11, 13, 19, 23, 29, 37, 71, 191, 251, 438, 1511, 13649\}$. If $p$ is a prime not belonging to $\mathcal{L}$, then:

(I) The equation $x^{13} + y^{13} = d\gamma z^p$ has no non-trivial primitive first case solutions.

(II) The equation $x^{26} + y^{26} = 10\gamma z^p$ has no primitive non-trivial solutions.

We will first prove part (I) of Theorem 1.3 and then explain the small tweak needed to conclude part (II). Observe that in part (II) replacing $10$ by twice $d$ for $d = 3, 7, 11$ the statement is also true but trivial, because the left-hand side is a sum of two relatively prime squares. The proof of Theorem 1.2 can be found in Sect. 4.1.

Jarvis and Meekin [20] solve the classic Fermat equation $x^p + y^p = z^p$ over the field $\mathbb{Q}(\sqrt{2})$ by using the modular approach with Hilbert modular forms. In [16] the second author of this work describes a general method to attack the equations (over $\mathbb{Q}$) of the form $x^r + y^r = Cz^p$ also using Hilbert modular forms. The strategy in this work is a particular application of that method complemented with the modularity result above together with effective computations of Hilbert newforms. To our knowledge this is the first time that Frey curves that do not give rise to GL$_2$-type abelian varieties over $\mathbb{Q}$ are used to solve a Diophantine equation over $\mathbb{Q}$. In particular, this means that instead of classical modular forms we must use Hilbert cuspforms.

2 Relating two Diophantine equations

In this section we will relate a solution of (2) to a solution of a Diophantine equation with coefficients in $\mathbb{Q}(\sqrt{13})$. In order to do that we will need a few properties on the factors of $x^{13} + y^{13}$ over the cyclotomic field $\mathbb{Q}(\zeta_{13})$. Since these properties are not exclusive of degree 13 we will prove them in general. Observe that if $r$ is an odd prime then

$$x^r + y^r = (x + y)\phi_r(x, y)$$
where

\[ \phi_r(x, y) = \prod_{i=0}^{r-1} (-1)^i x^{r-i} y^i. \]

Let \( \zeta = \zeta_r \) be a primitive \( r \)-th root of unity and consider the decomposition over the cyclotomic field \( \mathbb{Q}(\zeta) \)

\[ \phi_r(x, y) = \sum_{i=1}^{r-1} (x + \zeta^i y). \quad (3) \]

**Proposition 2.1** Let \( \mathfrak{P}_r \) be the prime in \( \mathbb{Q}(\zeta) \) above the rational prime \( r \) and suppose that \( (a, b) = 1 \). Then, any two distinct factors \( a + \zeta^j b \) and \( a + \zeta^i b \) in the factorization of \( \phi_r(a, b) \) are coprime outside \( \mathfrak{P}_r \). Furthermore, if \( r \mid a + b \) then \( v_{\mathfrak{P}_r}(a + \zeta^i b) = 1 \) for all \( i \).

**Proof** Suppose that \( (a, b) = 1 \). Let \( \mathfrak{P} \) be a prime in \( \mathbb{Q}(\zeta) \) above \( p \in \mathbb{Q} \) and a common prime factor of \( a + \zeta^i b \) and \( a + \zeta^j b \), with \( i > j \). Observe that \( (a + \zeta^i b) - (a + \zeta^j b) = b\zeta^j (1 - \zeta^{i-j}) \) and since \( \mathfrak{P} \) must divide the difference it cannot divide \( b \) because in this case it would also divide \( a \), and since \( a, b \) are rational integers \( p \) would divide both. So \( \mathfrak{P} \) must be a factor of \( \zeta^i (1 - \zeta^{i-j}) \) but \( \zeta^i \) is a unit for all \( i \) then \( \mathfrak{P} \) divides \( 1 - \zeta^{i-j} \), that is \( \mathfrak{P} = \mathfrak{P}_r \). Now for the last statement in the proposition, suppose that \( r \mid a + b \). Then,

\[ a + \zeta^i b = a + b - b + \zeta^i b = (a + b) + (\zeta^i - 1)b, \]

and since \( v_{\mathfrak{P}_r}(\zeta^i - 1) = 1 \) we have \( v_{\mathfrak{P}_r}(a + \zeta^i b) = \min\{(r - 1) v_r(a + b), 1\} = 1 \) □

**Corollary 2.2** If \( (a, b) = 1 \), then \( a + b \) and \( \phi_r(a, b) \) are coprime outside \( r \). Furthermore, if \( r \mid a + b \) then \( v_r(\phi_r(a, b)) = 1 \).

**Proof** Let \( p \) be a prime dividing \( a + b \) and \( \phi_r(a, b) \) and denote by \( \mathfrak{P} \) a prime in \( \mathbb{Q}(\zeta) \) above \( p \). Then \( \mathfrak{P} \) must divide at least one of the factors \( a + \zeta^i b \). Since \( a, b \) are rational integers \( \mathfrak{P} \) cannot divide \( b \) then it follows from

\[ a + b = a + \zeta^i b - \zeta^i b + b = (a + \zeta^i b) + (1 - \zeta^i)b \]

that \( \mathfrak{P} = \mathfrak{P}_r \). Moreover, if \( r \mid a + b \) it follows from the proposition that \( v_{\mathfrak{P}_r}(a + \zeta^i b) = 1 \) for all \( i \) then \( v_{\mathfrak{P}_r}(\phi_r(a, b)) = r - 1 \) thus \( v_r(\phi_r(a, b)) = 1 \). □

**Proposition 2.3** Let \( (a, b) = 1 \) and \( l \not\equiv 1 \pmod{r} \) be a prime dividing \( a^r + b^r \). Then \( l \mid a + b \).

**Proof** Since \( l \) divides \( a^r + b^r \), \( l \nmid ab \). Let \( b_0 \) be the inverse of \( -b \) modulo \( l \). We have \( a^r \equiv (-b)^r \pmod{l} \), hence \( (ab_0)^r \equiv 1 \pmod{l} \). Thus the multiplicative order of \( ab_0 \) in \( \mathbb{F}_l \) is 1 or \( r \). From the congruence \( ab_0 \equiv 1 \pmod{l} \) it follows \( a + b \equiv 0 \pmod{l} \). If \( l \nmid a + b \) then the order of \( ab_0 \) is \( r \) and \( l \equiv 1 \pmod{r} \). □
From now on we specialize to $r = 13$ and we denote $\phi_{13}$ only by $\phi$. We have $x^{13} + y^{13} = (x + y)\phi(x, y)$, where

\[ \phi(x, y) = x^{12} - x^{11}y + x^{10}y^2 - x^9y^3 + x^8y^4 - x^7y^5 + x^6y^6 - x^5y^7 + x^4y^8 - x^3y^9 + x^2y^{10} - xy^{11} + y^{12}. \]

Suppose that there exists a non-trivial primitive solution $(a, b, c')$ to (2) with $C = d\gamma$, $d$ and $\gamma$ as in Theorem 1.3. Then it follows from Corollary 2.2 and Proposition 2.3 that there exists a non-trivial primitive solution $(a, b, c_0)$ to

\[ \phi(x, y) = z^p, \quad (4) \]

with $d \mid a + b$ and $13 \nmid a + b$ or to

\[ \phi(x, y) = 13z^p \quad (5) \]

with $d \mid a + b$ and $13 \mid a + b$, where in both cases $c_0$ is only divisible by primes congruent to 1 modulo 13. Consider the factorization of $\phi$ in $\mathbb{Q}(\zeta)$

\[ \phi(x, y) = \prod_{i=1}^{12} (x + \zeta^i y). \]

We have $\phi = \phi_1\phi_2$ where $\phi_i$ are both of degree 6 with coefficients in $\mathbb{Q}(\sqrt{13})$, given by

\[ \phi_1(x, y) = (x + \zeta y)(x + \zeta^{12}y)(x + \zeta^4y)(x + \zeta^9y)(x + \zeta^3y)(x + \zeta^{10}y), \]
\[ \phi_2(x, y) = (x + \zeta^2y)(x + \zeta^5y)(x + \zeta^6y)(x + \zeta^7y)(x + \zeta^8y)(x + \zeta^{11}y). \]

The proof of the following corollary of Proposition 2.1 is immediate.

**Corollary 2.4** Let $\pi_{13}$ be the prime of $\mathbb{Q}(\sqrt{13})$ above 13. If $(a, b) = 1$, then $\phi_1(a, b)$ and $\phi_2(a, b)$ are coprime outside $\pi_{13}$. Moreover, $\nu_{\pi_{13}}(\phi_i(a, b)) = 1$ or 0 for both $i$ if $13 \mid a + b$ or $13 \nmid a + b$, respectively.

Since $\mathbb{Q}(\sqrt{13})$ has class number one, Corollary 2.4 and the existence of a solution $(a, b, c_0)$ to (4) or (5) implies that for some unit $\mu$ there exists a solution $(a, b, c)$ (with $c$ an integer in $\mathbb{Q}(\sqrt{13})$) to the equation

\[ \phi_1(x, y) = \mu z^p, \quad (6) \]

with $d \mid a + b$ and $13 \nmid a + b$ or to

\[ \phi_1(x, y) = \mu \sqrt{13}z^p, \quad (7) \]

with $d \mid a + b$ and $13 \mid a + b$, respectively.
Then Theorem 1.3 will hold if we prove that there are no solutions \((a, b, c)\) in \(\mathbb{Z}^2 \times \mathcal{O}_{\mathbb{Q}([\sqrt{13}])}\) to equations (6) and (7) such that \(|\text{Norm}_{\mathbb{Q}([\sqrt{13}]/\mathbb{Q})}(abc)| > 1\) (non-trivial), \((a, b) = 1\) (primitive), \(d \mid a + b\) and \(13 \nmid c\).

Observe that Proposition 2.3 and the form of equation (2) implies that \(13 \mid c\) is equivalent to \(13 \mid a + b\). Moreover, Proposition 2.3 also guarantees that when passing from the equation in (I) of Theorem 1.3 to equations (6) or (7) the prime factors of \(\gamma\) will also divide \(a + b\). However, to the proof of Theorem 1.3 we will only need \(d \mid a + b\).

3 The Frey-Hellegouarch curves

We will now construct the Frey curves. Let \(\sigma\) be the generator of \(G = \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})\) such that \(\sigma(\zeta) = \zeta^{11}\). Let also \(K\) be the maximal totally real subfield of \(\mathbb{Q}(\zeta)\) and \(p_{13}\) the single prime in \(K\) above 13. The field \(K\) is of degree 6 and fixed by \(\sigma^6\). Consider the factorization \(\phi_1 = f_1 f_2 f_3\), where

\[
\begin{align*}
  f_1(x, y) &= (x + \zeta y)(x + \zeta^{12} y) = x^2 + (\zeta + \zeta^{12})xy + y^2 \\
  f_2(x, y) &= (x + \zeta^3 y)(x + \zeta^{10} y) = x^2 + (\zeta^3 + \zeta^{10})xy + y^2 \\
  f_3(x, y) &= (x + \zeta^4 y)(x + \zeta^9 y) = x^2 + (\zeta^4 + \zeta^9)xy + y^2
\end{align*}
\]

are the degree two factors of \(\phi_1\) with coefficients in \(K\). Now we are interested in finding a triple \((\alpha, \beta, \gamma)\) such that

\[
\alpha f_1 + \beta f_2 + \gamma f_3 = 0.
\]

Solving a linear system in the coefficients of the \(f_i\) we find that one of its solutions in \(\mathcal{O}_K^3\) is given by

\[
\begin{align*}
  \alpha &= -\zeta^{10} + \zeta^9 + \zeta^4 - \zeta^3 \\
  \beta &= \zeta^{12} - \zeta^9 - \zeta^4 + \zeta \\
  \gamma &= -\zeta^{12} + \zeta^{10} + \zeta^3 - \zeta
\end{align*}
\]

and satisfies \(v_{p_{13}}(\alpha) = v_{p_{13}}(\beta) = v_{p_{13}}(\gamma) = 1\).

Suppose now that \((a, b, c) \in \mathbb{Z} \times \mathbb{Z} \times \mathcal{O}_{\mathbb{Q}([\sqrt{13}])}\) is a primitive solution to equation (6) or (7) and let \(A(a, b) = \alpha f_1(a, b), B(a, b) = \beta f_2(a, b)\) and \(C(a, b) = \gamma f_3(a, b)\). Since

\[
A + B + C = 0
\]

we can consider the Frey-Hellegouarch curve over \(K\) with the classic form

\[
E_{(a, b)} : y^2 = x(x - A(a, b))(x + B(a, b)).
\]

A similar construction of Frey curves for signature \((7, 7, p)\) was given by Kraus in [23].
In the rest of this section we will denote $E_{(a,b)}$ only by $E$ whenever it causes no ambiguity. Note that $2$ is inert in $K$ and denote by $p_2$ the prime in $K$ above it. To the curves $E = E_{(a,b)}$ are associated the following quantities:

\[
\begin{align*}
\Delta(E) &= 2^4(ABC)^2 = 2^4(\alpha\beta\gamma)^2\phi_1(a, b)^2 \\
c_4(E) &= 2^4(A^2 + AB + B^2) = 2^4(AB + BC + AC) \\
c_6(E) &= -2^5(C + 2B)(A + 2B)(2A + B) \\
j(E) &= 2^8(A^2 + AB + B^2)^3/(ABC)^2
\end{align*}
\]

and since $(\alpha\beta\gamma) = p_{13}^3$ the discriminant of $E$ takes the following values

\[
\Delta(E) = \begin{cases} 
p_2^4p_{13}^6c^2p & \text{if } 13 \nmid a + b \\
p_2^4p_{13}^{12}c^2p & \text{if } 13 \mid a + b
\end{cases}
\]

**Proposition 3.1** Let $p$ be a prime of $K$ distinct from $p_2$ and $p_{13}$. The curve $E_{(a,b)}$ has good or multiplicative reduction at $p$. Moreover, the curve has good $(\nu_{p_{13}}(N_E) = 0)$ or bad additive $(\nu_{p_{13}}(N_E) = 2)$ reduction at $p_{13}$ if $13 \mid a + b$ or $13 \nmid a + b$, respectively. In particular, $E$ has multiplicative reduction at primes dividing $c$.

**Proof** For the results used in this proof we followed [24]. Let $p$ be as in the hypothesis and observe that $\nu_p(\Delta(E)) = 2p\nu_p(c)$. Then if $p \nmid c$ we have $\nu_p(\Delta) = 0$ and the curve has good reduction. It follows from Proposition 2.1 that $A(a, b), B(a, b)$ and $C(a, b)$ are pairwise coprime outside $p_{13}$ and recall that the three are divisible by $p_{13}$. If $p \mid c$ then $p$ must divide only one among $A$, $B$ or $C$. From the form of $c_4$ it can be seen that $\nu_p(c_4) = 0$. Also, $\nu_p(\Delta) > 0$ thus $E$ has multiplicative reduction at $p$. Moreover, we see from the above expressions for $\Delta(E)$ and $c_4(E)$ and Proposition 2.1 that if $13 \mid a + b$ then $\nu_{p_{13}}(\Delta) = 12$ and $\nu_{p_{13}}(c_4) \geq 4$. This means that the equation is not minimal and hence $E$ has good reduction at $p_{13}$. On the other hand if $13 \nmid a + b$ then $\nu_{p_{13}}(\Delta) = 6$ and $\nu_{p_{13}}(c_4) > 0$ hence bad additive reduction at $p_{13}$. \hfill \Box

**Proposition 3.2** The short Weierstrass model of the curves $E_{(a,b)}$ is defined over $\mathbb{Q}(\sqrt{13})$.

**Proof** First observe that $\sigma^4 \pmod{\sigma^6}$ generates $\text{Gal}(K/\mathbb{Q}(\sqrt{13}))$. Since the curves $E$ are defined over $K$ they are invariant under $\sigma^6$ and in particular $j(E)$ is invariant by $\sigma^6$ by definition. We also have that

\[
\sigma^4(A) = B, \quad \sigma^4(B) = C, \quad \sigma^4(C) = A,
\]

and from

\[
j(E) = 2^8(AB + BC + CA)^3/(ABC)^2
\]
it is clear that \( j \) is also invariant under \( \sigma^4 \). Then the \( j \)-invariant that \textit{a priori} belonged to the field \( K \) of degree 6, in reality is in \( \mathbb{Q}(\sqrt{13}) \). Now we write \( E_{(a,b)} \) in the short Weierstrass form to get a model

\[
\begin{align*}
E_0 : y^2 &= x^3 + a_4x + a_6, \quad \text{where} \\
 a_4 &= -432(AB + BC + CA) \\
 a_6 &= -1728(2A^3 + 3A^2B - 3AB^2 - 2B^3)
\end{align*}
\]

Since \( a_4 \) is clearly invariant under \( \sigma^4 \) and

\[
 a_6 = -1728(2A^3 + 3A^2B - 3AB^2 - 2B^3) \\
 = -1728(2(-B - C)^3 + 3(-B - C)^2B - 3(-B - C)B^2 - 2B^3) \\
 = -1728(2B^3 + 3B^2C - 3BC^2 - 2C^3) = \sigma^4(a_6)
\]

we conclude that the short Weierstrass model is already defined over \( \mathbb{Q}(\sqrt{13}) \). \( \square \)

Writing \( E_{(a,b)} \) in the short Weierstrass form we get the elliptic curve \( E_0(a, b) \) defined over \( \mathbb{Q}(\sqrt{13}) \) given by

\[
E_0(a, b) : y^2 = x^3 + a_4(a, b)x + a_6(a, b),
\]

\[
a_4(a, b) = (216w - 2808)a^4 + (-1728w + 5616)a^3b \\
+ (1728w - 11232)a^2b^2 + (-1728w + 5616)ab^3 \\
+ (216w - 2808)b^4,
\]

\[
a_6(a, b) = (-8640w + 44928)a^6 + (49248w - 235872)a^5b \\
+ (-129600w + 471744)a^4b^2 + (152928w - 662688)a^3b^3 \\
+ (-129600w + 471744)a^2b^4 + (49248w - 235872)ab^5 \\
+ (-8640w + 44928)b^6,
\]

where \( w^2 = 13 \). Observe that writing a curve in short Weierstrass form changes the values of \( \Delta \), \( c_4 \) and \( c_6 \) according to \( \Delta(E_0) = 6^{12}\Delta(E) \), \( c_4(E_0) = 6^4c_4(E) \) and \( c_6(E_0) = 6^6c_6(E) \). Note that 2 is inert in \( \mathbb{Q}(\sqrt{13}) \subset K \). From now on we will use 2 and \( w \) to denote also the ideals in \( \mathbb{Q}(\sqrt{13}) \) above 2 and 13, respectively.

**Proposition 3.3** \textit{The possible values for the conductors of} \( E_0(a, b) \) \textit{are}

\[
N_{E_0} = 2^s w^2 \text{rad}(c),
\]

where \( s = 3, 4 \) and \( \text{rad}(c) \) is the product of the prime factors of \( c \). Moreover, when \( a + b \) is even, \( s = 3 \) if 4 \mid a + b \) and \( s = 4 \) if 4 \nmid a + b \).

**Proof** As in Proposition 3.1 we followed the results in \([24]\) to compute the conductor. Since the primes dividing 6 do not ramify in \( K/\mathbb{Q}(\sqrt{13}) \) and do not divide \( c \) the conductor of \( E_0 \) and \( E \) is same at these primes.

Since \( (w) = p_3^2 \) in \( K \) we see from Proposition 3.1 that \( \nu_w(\Delta(E_0)) = 4 \) or 2 if 13 \mid a + b \) or 13 \nmid a + b \), respectively. Also, \( \nu_w(c_4(E_0)) > 0 \) and since we are
Lemma 3.4 There are coprime values of \( a, b \in \mathbb{Z} \) such that the Frey curve \( E_{(a,b)} \) is not a \( \mathbb{Q} \)-curve.

Proof Assume that \( E = E_{(a,b)} \) is a \( \mathbb{Q} \)-curve. From the work of Quer [25] we know there exists a field \( L \supset \mathbb{Q}(\sqrt{13}) \) and an element \( \delta \in L \) such that the curve \( E_{\delta} \) obtained by twisting \( E \) by \( \delta \) is a \( \mathbb{Q} \)-curve completely defined over \( L \). In particular, if \( L_1 \neq L_2 \) are two primes in \( L \) above the same rational prime \( \ell \) the trace values \( a_{L_i}(E_{\delta}) \) differ at most by a sign.

Observe that 3 splits in \( \mathbb{Q}(\sqrt{13}) \) and let \( p_1, p_2 \) be the two primes above 3. Now take, for example, \( a, b \in \mathbb{Z} \) such that \( (a, b) \equiv (1, 0) \pmod{3} \). Using SAGE we compute the values \( a_{p_i}(E_{(a,b)}) \) to find that one is \(-1\) and the other \(-3\). Therefore, the traces \( a_{L_i}(E_{(a,b)}) \), where \( L_i \mid p_i \) in \( L \), have different absolute values. Thus \( a_{L_i}(E_{\delta}) \) cannot differ by a sign and we conclude that \( E_{(a,b)} \) is not a \( \mathbb{Q} \)-curve.

4 The Galois representations of \( E_{(a,b)} \)

For an elliptic curve \( C \) over a totally real field \( F \) we let \( \rho_{C,p} : G_F \to \text{GL}_2(\mathbb{Q}_p) \) be the \( p \)-adic representation associated with \( C \) and \( \bar{\rho}_{C,p} \) its reduction modulo \( p \). In this section we will prove that the Frey-Hellegouarch curves \( E = E_{(a,b)} \) are modular and that \( \bar{\rho}_{E,p} \) is irreducible for \( p > 37 \). These results together allow us to apply level lowering results for Hilbert modular forms.

4.1 Modularity

Modularity of \( E_{(a,b)} \) follows from Theorem 4.3. For the proof we will first recall an auxiliary result due to Savitt generalizing a result of Breuil and an important consequence of the Langlands-Tunnell theorem.

**Theorem 4.1** (Savitt) Let \( p > 2 \) and \( \rho : G_{\mathbb{Q}_p} \to \text{GL}_2(\mathbb{Q}_p) \) be a potentially Barsotti-Tate Galois representation. Suppose also that \( \rho|G_{\mathbb{Q}_p(\zeta)} \) is Barsotti-Tate and that \( \bar{\rho} \)
is reducible. Then \( \rho \) is nearly-ordinary. Furthermore, if \( \rho \) is Barsotti-Tate then it is ordinary.

**Proof** See Theorem 6.11 in [27]. For the last statement: we have \( \rho \) nearly-ordinary and Barsotti-Tate (hence crystalline) then by the description of lattices in section 9.1 of [6] we find that we are in case \((i)\) thus \( \rho \) is ordinary. \( \square \)

**Lemma 4.2** Let \( C/F \) be an elliptic curve defined over a totally real field \( F \) and put \( \rho = \rho_{C,3} \). If \( \bar{\rho} \) is irreducible then it is modular arising from a Hilbert newform \( f \) over \( F \) of parallel weight \( 2 \).

**Proof** Since \( \bar{\rho} : G_F \to \text{GL}_2(\mathbb{F}_3) \) is totally odd, absolutely irreducible and of solvable image, the discussion after Theorem 5.1 in [31] can be reproduced also over the totally real field \( F \) (see [18] for details over \( \mathbb{Q} \)). Thus there is a Hilbert eigenform \( f_1 \) of parallel weight 1 defined over \( F \) such that \( \bar{\rho} \sim \bar{\rho}_{f_1,\lambda} \), where \( \lambda \mid 3 \) is a prime in \( \bar{\mathbb{Q}} \). From Lemma 1.4.2 in [30] we know there exists a normalized Hilbert modular form \( \theta \) of parallel weight 1 for some integer \( i \geq 0 \) such that \( \theta \equiv 1 \pmod{3} \). Consider the product \( \theta f_1 \) of parallel weight \( w = 2^{i+1} + 1 \). Since \( \theta f_1 \equiv f_1 \pmod{3} \) we have that \( \theta f_1 \) is a modulo 3 eigenform and by the Deligne-Serre Lemma (see [12], Lemma 6.11) we can find an eigenform \( f_w \) of parallel weight \( w \) such that \( \bar{\rho} \sim \bar{\rho}_{f_w,\lambda} \). Finally, from the comments preceding Corollary 2.12 in [8] it follows that there is a Hilbert eigenform \( f_2 \) of parallel weight 2 (and level not necessary prime to 3) such that \( \bar{\rho} \sim \bar{\rho}_{f_2,\lambda} \) for a prime \( \lambda \) above 3. We take \( f = f_2 \). \( \square \)

**Theorem 4.3** Let \( F \) be a totally real abelian number field and \( C \) an elliptic curve defined over \( F \). Suppose that \( 3 \) splits completely in \( F \) and \( C \) has good reduction at the primes above \( 3 \). Then \( C \) is modular.

**Proof** Let \( \bar{\rho} = \bar{\rho}_{C,3} \) be as before. We divide the proof into three cases:

1. Suppose that \( \bar{\rho} \) and \( \bar{\rho}|G_{F(\sqrt{-3})} \) are both absolutely irreducible. Here we apply Corollary 2.1.3 in [21]. Condition (1) holds because \( C \) has good reduction at the primes above 3 and 3 splits in \( F \). Lemma 4.2 guarantees condition (2) and (3) holds by hypothesis. Then \( \rho \) is modular.

2. Suppose that \( \bar{\rho} \) is absolutely irreducible and \( \bar{\rho}|G_{F(\sqrt{-3})} \) absolutely reducible. This means that the image of \( \bar{\rho} \) is dihedral. Namely, that the image of \( \bar{\rho} \) is contained in the normalizer \( N \) of a Cartan subgroup \( C_0 \) of \( \text{GL}_2(\mathbb{F}_3) \) but not contained in \( C_0 \). Moreover, the restriction to \( F(\sqrt{-3}) \) of our representation has its image inside \( C_0 \). Thus, the composition of \( \bar{\rho} \) with the quotient \( N/C_0 \),

\[
\text{Gal}(\bar{\mathbb{Q}}/F) \to N \to N/C_0,
\]

(8)
gives the quadratic character of \( F(\sqrt{-3})/F \) which ramifies at 3 because 3 is unramified in \( F \).

Let \( t \) be a prime in \( F \) above 3. Since \( C \) has good reduction at \( t \) and 3 splits in \( F \) the restriction of the residual representation \( \bar{\rho} \) to the inertia subgroup \( I_t \) has only two possibilities
\[ \tilde{\rho}|I_t = \begin{pmatrix} \tilde{\chi} \ast & \psi_2 \\ 0 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} \psi_2 & 0 \\ 0 & \psi_2^3 \end{pmatrix}, \]  

where \( \chi \) is the 3-adic cyclotomic character and \( \psi_2 \) is the fundamental character of level 2.

If we suppose that \( \tilde{\rho}|I_t \) acts through level 2 fundamental characters, the image of \( I_t \) by \( \mathbb{P}(\tilde{\rho}) \) gives a cyclic group of order 4 \( > 2 \), thus it has to be contained in \( \mathbb{P}(C_0) \) (if it not contained in \( \mathbb{P}(C_0) \) and has order 4 it must be isomorphic to \( C_2 \times C_2 \)). But this implies that the quadratic character defined by composition (8) should be unramified at 3, contradicting the fact that this character corresponds to \( F(\sqrt{-3}) \). Thus we can assume that we are in the first case, that is, \( \tilde{\rho}|I_t \) is reducible.

The previous holds for all primes \( t \mid 3 \) hence we can apply Lemma 4.5 below to \( \tilde{\rho} \). Let \( \psi \) and \( f_2 \) be given by applying Lemma 4.5 to \( \tilde{\rho} \). Let \( \psi_0 \) be a finite order lifting of \( \psi \) satisfying \( \rho \otimes \psi_0 = \tilde{\rho} \otimes \psi \). Note that \( \rho|D_t \) is ordinary for all \( t \) by Theorem 4.1. Then \( \rho \otimes \psi_0 \) satisfy all the conditions of Theorem 5.1 in [29]. Thus \( \rho \otimes \psi_0 \) is modular hence \( \rho \) is also modular.

3. Suppose that \( \tilde{\rho} \) is absolutely reducible. We want to apply Theorem A in [28]. The hypothesis there are not numerated but we will refer to them as conditions (1) to (5) in descending order.

Since the representation is totally odd and \( F \) is totally real, \( \tilde{\rho} \) is reducible if and only if it is absolutely reducible, hence reducibility of \( \tilde{\rho} \) must take place over \( \mathbb{F}_3 \). Together with \( C \) having good reduction at \( t \mid 3 \), by restricting \( \tilde{\rho} \) to \( I_t \), we see that the case of the fundamental characters of level 2 in (9) cannot occur. Thus we have \( \tilde{\rho}^{ss} = \chi_1 \otimes \chi_2 \), where \( \chi_1 = \psi \tilde{\chi}, \chi_2 = \psi^{-1} \) where \( \tilde{\chi} \) is the mod 3 cyclotomic character and \( \psi \) is ramified only at primes dividing the conductor of \( E \). Note also that \( \psi \) must be quadratic because \( \mathbb{F}_3^* \) has only two elements. Then \( \chi_1 / \chi_2 = \psi^2 \tilde{\chi} = \tilde{\chi} \) and conditions (2) and (3) are satisfied. Moreover, \( \rho|D_t \) is Barsotti-Tate (\( C \) has good reduction at all \( t \mid 3 \)) then by Theorem 4.1 we conclude that \( \rho|D_t \) is ordinary for all \( t \), which establishes condition (4). Finally, the extension \( F(\chi_1 / \chi_2) = F(\sqrt{-3}) \) of \( \mathbb{Q} \) is abelian because \( F \) and \( \mathbb{Q}(\sqrt{-3}) \) are both abelian. This establishes condition (1) and condition (5) holds because \( \rho \) arises from an elliptic curve. Thus by Theorem A in [28] we conclude that \( \rho \) is modular. \( \square \)

**Remark 4.4** In case (2) of the previous proof we apply Theorem 5.1 of [29]. This theorem has a mistake in it: the pathology might happen if \( p \) ramifies in the base field \( F \) (hence \( F(\sqrt{-p})/F \) might be unramified above \( p \)), because this interferes with key estimates in the reducible locus in that paper. Since our field \( F \) is unramified at \( p = 3 \) this does not affect our application of the theorem.

**Lemma 4.5** Let \( C \) and \( F \) be as in the Theorem 4.3. Suppose also that for all \( t \mid 3 \) we have that \( \tilde{\rho} = \tilde{\rho}_{C,3} \) satisfies

\[ \tilde{\rho}|I_t = \begin{pmatrix} \tilde{\chi} \ast \\ 0 & 1 \end{pmatrix}. \]
Suppose further that \( \bar{\rho} \) is modular. Then, there is a character \( \psi \) of \( G_F \) of finite order and a Hilbert modular form \( f_2 \) over \( F \) of level \( N \) and parallel weight 2 such that \( \bar{\rho} \otimes \psi \sim \bar{\rho}_{f_2,\lambda} \) for some prime \( \lambda \mid 3 \). Furthermore, the level \( N \) divides \( n3 \) (with 3 and \( n \) coprime) and, for each \( t \mid 3 \), \( f_2 \) is ordinary or nearly-ordinary at \( t \) if \( t \nmid N \) or \( t \mid N \), respectively.

**Proof** From the comments preceding Corollary 2.12 in [8] (also used in the proof of Lemma 4.2) it follows that there is a character \( \psi \) of finite order and a Hilbert eigenform \( f_2 \) of parallel weight 2 such that \( \bar{\rho} \otimes \psi \sim \bar{\rho}_{f_2,\lambda} \) for a prime \( \lambda \) above 3. Moreover, the level \( N \) of \( f_2 \) divides \( n3 \) with 3 and \( n \) coprime.

Let \( t \mid 3 \) be a prime and note that since 3 splits in \( F \) the restriction of \( \psi \) to \( D_t \) must be equal to the mod 3 cyclotomic character \( \bar{\chi} \) or the trivial character. Hence \( (\bar{\rho} \otimes \psi)|_{D_t} \) is residually ordinary. We now divide into two cases:

1. Suppose that \( t \nmid N \). From \( f_2 \) being of parallel weight 2 and 3 unramified in \( F \) it follows that \( \rho_{f_2,\lambda}|_{D_t} \) is Barsotti-Tate. Since \( \bar{\rho}_{f_2,\lambda}|_{D_t} \equiv (\bar{\rho} \otimes \psi)|_{D_t} \) is residually ordinary (hence reducible) we apply Theorem 4.1 to conclude that \( \rho_{f_2,\lambda}|_{D_t} \) is ordinary.

2. Suppose that \( t \mid N \). Here we have two cases: \( f_2 \) is Steinberg or principal series.

   - If \( f_2 \) is Steinberg then \( \rho_{f_2,\lambda}|_{D_t} \) is semi-stable non-crystalline, hence we are in case (iii) of section 9.1 in [6] then \( \rho_{f_2,\lambda} \) is ordinary at \( t \). If \( f_2 \) is a principal series then it is known that \( \rho_{f_2,\lambda}|_{D_t} \) is potentially Barsotti-Tate and Barsotti-Tate over \( \mathbb{Q}_3(\zeta_3) \). From \( \bar{\rho} \otimes \psi \sim \bar{\rho}_{f_2,\lambda} \) follows that \( \bar{\rho}_{f_2,\lambda}|_{D_t} \) is reducible and by Theorem 4.1 \( \rho_{f_2,\lambda}|_{D_t} \) is nearly-ordinary at \( t \).

\( \square \)

**Theorem 4.6** Let \( (a, b, c) \) be a non-trivial primitive solution of (6) or (7). Then the Frey curve \( E_{(a,b)} \) over \( \mathbb{Q}(\sqrt{13}) \) are modular.

**Proof** \( \mathbb{Q}(\sqrt{13}) \) is an abelian extension in which 3 splits. Since the primes \( t \mid 3 \) in \( \mathbb{Q}(\sqrt{13}) \) do not divide \( c \) (because \( 3 \nmid \phi(a, b) \)) it follows from Proposition 3.3 that \( E_{(a,b)} \) has good reduction at all \( t \mid 3 \). Now the result is immediate from Theorem 4.3.

\( \square \)

### 4.2 Irreducibility

**Theorem 4.7** Let \( p > 7 \) and \( p \neq 13, 37 \) be a prime. Then, the representation \( \bar{\rho}_{E,p} \) is absolutely irreducible.

**Proof** Recall that 2 is inert in \( \mathbb{Q}(\sqrt{13}) \) and \( w^2 = 13 \). Since \( \bar{\rho}_{E,p} \) is odd and \( \mathbb{Q}(\sqrt{13}) \) is totally real it is known that \( \bar{\rho}_{E,p} \) is absolutely irreducible if and only if it is irreducible then we only need to rule out the case where \( \bar{\rho}_{E,p} \) is reducible and has the form

\[
\bar{\rho}_{E,p} = \begin{pmatrix}
\epsilon^{-1} \chi_p & * \\
0 & \epsilon
\end{pmatrix},
\]

where \( \chi_p \) is the mod \( p \) cyclotomic character and \( \epsilon \) is a character (depending on \( p \)) of \( G_{\mathbb{Q}(\sqrt{13})} \) with values in \( \mathbb{F}_p^* \) unramified at primes dividing \( p \). Since the image of
inertia at semistable primes is of the form \( \begin{pmatrix} 1 & \ast \\ 0 & 1 \end{pmatrix} \) the conductor of \( \epsilon \) only contains additive primes. By the work of Carayol the conductor at bad additive primes of \( \bar{\rho}_{E,p} \) is the same as that of \( \rho_{E,p} \). Since the conductors of \( \epsilon \) and \( \epsilon^{-1} \) are equal it follows from Proposition 3.3 that the cond(\( \epsilon \)) = 2w or \( 2^2w \). The characters of \( G_{\mathbb{Q}(\sqrt{13})} \) with conductor dividing \( 2^2w \) are in correspondence with the characters of the finite group

\[
H = (\mathcal{O}_{\mathbb{Q}(\sqrt{13})}/2^2w)^* \cong \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.
\]

The group of characters of \( H \) is dual to \( H \), so all the characters have order dividing 12.

Let \( \mathfrak{p}_3 \) be a prime above 3 in \( \mathbb{Q}(\sqrt{13}) \). By evaluating at \( \text{Frob}_{\mathfrak{p}_3} \) and taking traces on equality (10) we get

\[
a_{\mathfrak{p}_3}(E) \equiv \epsilon(\text{Frob}_{\mathfrak{p}_3}) + 3\epsilon^{-1}(\text{Frob}_{\mathfrak{p}_3}) \pmod{p},
\]

which implies that \( \epsilon(\text{Frob}_{\mathfrak{p}_3}) \) satisfies the polynomial \( q_2 := x^2 - a_{\mathfrak{p}_3}x + 3 \pmod{p} \). Since \( \epsilon \) has order dividing 12, in particular, \( \epsilon(\text{Frob}_{\mathfrak{p}_3}) \) is a root of the polynomial \( q_1 := x^{12} - 1 \pmod{p} \). Let \( \zeta = \zeta_{12} \), then the resultant of \( q_1 \) and \( q_2 \) is given by

\[
\text{res}(q_1, q_2) = \prod_{i=1}^{12} \left( \frac{a_{\mathfrak{p}_3} + \sqrt{a_{\mathfrak{p}_3}^2 - 12}}{2} - \zeta^i \right) \left( \frac{a_{\mathfrak{p}_3} - \sqrt{a_{\mathfrak{p}_3}^2 - 12}}{2} - \zeta^i \right)
\]

\[
= \prod_{i=1}^{12} (\zeta^{2i} - a_{\mathfrak{p}_3}\zeta^i + 3)
\]

Using SAGE we see that for one of the primes above 3 the value of \( a_{\mathfrak{p}_3}(E) \) is \(-1 \) or \(-3 \) (see also Table 1). We compute the previous product replacing \( a_{\mathfrak{p}_3} \) by these values to find the possible prime divisors of it are \( \{2, 3, 5, 7, 13, 37\} \). Observe that as polynomials over \( \mathbb{Z} \), \( q_1 \) and \( q_2 \) has no common roots, hence \( 0 \neq \text{res}(q_1, q_2) \in \mathbb{Z} \). Therefore, since \( \epsilon(\text{Frob}_{\mathfrak{p}_3}) \) is a common root of the \( q_1 \) (mod \( p \)) then \( \text{res}(q_1, q_2) \equiv 0 \pmod{p} \), which is impossible if \( p > 7 \) and \( p \neq 13, 37 \). Thus \( \bar{\rho}_{E,p} \) is absolutely irreducible if \( p > 7 \) and \( p \neq 13, 37 \). \( \square \)

With Theorems 4.6 and 4.7 in hand we are now able to apply the level lowering results for Hilbert modular forms from Rajaei [26], Fujiwara [17] and Jarvis [19]. Our application of these theorems follow exactly the same lines as in Jarvis-Meekin [20] (see the discussion following Theorem 3.3 in loc. cit). For an ideal \( N \) in \( \mathbb{Q}(\sqrt{13}) \) we denote by \( S_2(N) \) the set of Hilbert modular cusp forms over \( \mathbb{Q}(\sqrt{13}) \) of parallel weight \( (2, 2) \) and level \( N \). It follows from the modularity that there exists a newform \( f_0 \) in \( S_2(2^i w^2 \text{rad}(c)) \) where \( i = 3 \) or 4 such that \( \rho_{E,p} \) is isomorphic to the \( p \)-adic representation attached to \( f_0 \), which we denote by \( \rho_{f_0,p} \). For a prime \( l \) of multiplicative reduction of \( E \) (i.e. \( l \mid c \)) we see that \( l \) appears to a \( p \)-th power in the discriminant of a minimal model at \( l \). Thus we know by an argument of Hellegouarch that the representation \( \bar{\rho}_{E,p} \) will not ramify at the primes dividing \( c \). Furthermore, when reducing to
the residual representation the conductor at the bad additive primes cannot decrease hence \( \tilde{\rho}_{E,p} \) has Artin conductor \( N(\tilde{\rho}_{E,p}) \) equal to that of \( \rho_{E,p} \) without the factor \( \text{rad}(c) \), that is \( N(\tilde{\rho}_{E,p}) = 2^i w^2 \) where \( i = 3 \) or \( 4 \). Since \( \rho_{E,p} \) is modular then \( \tilde{\rho}_{E,p} \), when irreducible, is modular and by the results on level lowering for Hilbert modular forms we know that there exists a newform \( f \) in \( S_2(2^i w^2) \) and a prime \( \mathfrak{p} \mid p \) in \( \mathbb{Q} \) such that its associated residual Galois representation \( \tilde{\rho}_{f,\mathfrak{p}} \) satisfies

\[
\tilde{\rho}_{E,p} \sim \tilde{\rho}_{f,0,p} \sim \tilde{\rho}_{f,\mathfrak{p}}. \tag{11}
\]

5 Eliminating newforms

In this section we will find a contradiction to the isomorphism (11) for all \( f \) in the predicted spaces. This shows that the Frey curves associated with primitive non-trivial first case solutions \( (a, b, c) \) to equation (6) or (7) cannot exist and ends the proof of part (I) in Theorem 1.3. Then we explain a small trick that allows to conclude part (II) from part (I).

Note that 3 and 17 split in \( \mathbb{Q}(\sqrt{13}) \) and that 5, 7 and 11 are inert. Recall that \( w^2 = 13 \) and consider the following prime ideals in \( \mathbb{Q}(\sqrt{13}) \):

\[
\begin{align*}
L_3^0 &= \langle \frac{1}{2}(w + 1) \rangle, & L_3^1 &= \langle \frac{1}{2}(-w + 1) \rangle, \\
L_{17}^0 &= \langle \frac{1}{2}(w + 9) \rangle, & L_{17}^1 &= \langle \frac{1}{2}(-w + 9) \rangle, \\
L_{11} &= \langle 11 \rangle, & L_5 &= \langle 5 \rangle, & L_7 &= \langle 7 \rangle.
\end{align*}
\]

Suppose that (11) holds for some newform \( f \) in the predicted spaces. Hence, for any prime \( L \mid \ell \) of good reduction of \( E = E_{(a,b)} \) we have \( a_L(\rho_{E,p}) \equiv a_L(\rho_{f,p}) \) (mod \( p \)), where \( p \mid p \) in \( \mathbb{Q} \). To find the desired contradiction to isomorphism (11) we will compute the trace values \( a_L(\rho_{E,p}) \) and \( a_L(\rho_{f,p}) \) and show that the previous congruence cannot hold, using the primes listed above.

On the one hand, we used SAGE to compute the values \( a_L(\rho_{E,p}) = a_L(E) \). Since we are interested in putative solutions \( (a, b, c) \in \mathbb{Z}^2 \times \mathcal{O}_{\mathbb{Q}(\sqrt{13})} \) there is \( (x, y) \in \mathbb{F}_\ell \times \mathbb{F}_\ell \) such that \( (a, b) \equiv (x, y) \) (mod \( \ell \)). Thus, fixed a prime \( L \) above \( \ell \) we can go through all non-zero pairs \( (a, b) \in \mathbb{F}_\ell \times \mathbb{F}_\ell \), consider the corresponding residual elliptic curve and compute the value \( a_L(E) \). We now focus on the primes above 3. Since \( a, b \) are integers, \( (a, b) \equiv (x, y) \) (mod \( 3 \)) implies \( (a, b) \equiv (x, y) \) (mod \( L_i^0 \)) for \( i = 0, 1 \) and we can compute simultaneously the values \( a_{L_i^0}(E) \) and \( a_{L_i^1}(E) \) (Table 1).

Remark 5.1 In general, since \( a, b \) are not concrete, it is not possible to obtain the values \( a_L(E_{(a,b)}) \) for different primes simultaneously. This argument works here because we are taking primes above the same rational prime and, despite the Frey curves being defined over \( \mathbb{Q}(\sqrt{13}) \), we are only interested in solutions \( (a, b, c) \) with \( a, b \in \mathbb{Z} \). In particular, in the classical case of Frey curves over \( \mathbb{Q} \) this is never possible.

On the other hand, to obtain the values of \( a_L(\rho_{f,p}) \), we had the help of John Voight. He used algorithms to compute Hilbert modular forms implemented in MAGMA [5] (an expository account can be found in [13]) and gave us two lists of newforms. One list contains the characteristic polynomials of the Hecke operators \( T_L \) (for primes
Fermat-type equations of signature \((13, 13, p)\) via Hilbert cuspforms

### Table 1

| \(a \pmod{3}\) | \(b \pmod{3}\) | \(a_{L^0_{3}}\) | \(a_{L^1_{3}}\) |
|-----------------|-----------------|-----------------|-----------------|
| 0               | 1               | -1              | -3              |
| 0               | 2               | -1              | -3              |
| 1               | 0               | -1              | -3              |
| 1               | 2               | -1              | 1               |
| 1               | 0               | -3              | -1              |
| 2               | 1               | -1              | -3              |
| 2               | 2               | -3              | -1              |
| 2               | 0               | -1              | 1               |

\(L \nmid 2, 13\) in \(\mathbb{Q}(\sqrt{13})\) with norm \(\leq 200\) factored on Hecke irreducible subspaces for the newforms of level \(23^3 13\). The other list has the same information for level \(24^3 13\). For example, in level \(23^3 13\) there is a newform \(g_1\) with rational coefficients such that the data corresponding to the primes of small norm is

\[
[x - 3, x + 1, x + 7, x - 1, x + 2, x + 2, x - 7, x, x + 8],
\]

and also a newform \(g_2\) with non-rational coefficients

\[
[x^2 - 3x + 1, x^2 - x - 1, x^2 - 2x - 4, x + 2, x + 2, x^2 + 4x - 16, x^2 + 6x + 4, x^2 + x - 1].
\]

The complete data can be found at [http://www.ub.edu/tn/visitant/amat.php](http://www.ub.edu/tn/visitant/amat.php).

Before proceeding to eliminate the newforms we divide them into two 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 \(\mathbb{Q}\).

**Newforms in S1**: Note that equations (6) and (7) have trivial solutions \((1, 1, 1), \pm(0, 1, 1), \pm(1, 0, 1)\) and \((1, -1, 1), (-1, 1, 1)\), respectively. These solutions correspond to the Frey curves \(E_{(1,1)}, E_{(0,1)}\) and \(E_{(1,-1)}\) that indeed exist, so there must be newforms associated with them in S1 which, \(a priori\), will not be possible to eliminate only by comparing the traces \(a_{L}(f)\) and \(a_{L}(E)\).

Suppose that isomorphism (11) holds for some \(f \in S1\). In particular, we have that

\[
(a_{L^0_{3}}(E), a_{L^1_{3}}(E)) \equiv (a_{L^0_{3}}(f), a_{L^1_{3}}(f)) \pmod{p}.
\]

Let \(p_f\) and \(q_f\) be the minimal polynomials of \(a_{L^0_{3}}(f)\) and \(a_{L^1_{3}}(f)\), respectively. Thus,

\[
(p_f(a_{L^0_{3}}(E)), q_f(a_{L^1_{3}}(E))) \equiv (p_f(a_{L^0_{3}}(f)), q_f(a_{L^1_{3}}(f))) \equiv (0, 0) \pmod{p}
\]

and we obtain a contradiction with

\[
p \nmid \gcd(p_f(a_{L^0_{3}}(E)), q_f(a_{L^1_{3}}(E))).
\]
Table 2 Values of \(a_L(f)\) for surviving forms in \(S_1\)

| \(a_{L,3}^0\) | \(a_{L,3}^1\) | \(a_{L,17}^0\) | \(a_{L,17}^1\) | \(a_{L,23}^0\) | \(a_{L,23}^1\) | \(a_{L,29}^0\) | \(a_{L,29}^1\) | \(a_{L,31}\) | \(a_{L,11}\) |
|---|---|---|---|---|---|---|---|---|---|
| \(f_1\) | -1 | 1 | 3 | 7 | -7 | -1 | 2 | -3 | -7 | -1 | 3 |
| \(f_2\) | -1 | -3 | -1 | -5 | 5 | -9 | -6 | -3 | 1 | -5 | 15 |
| \(f_3\) | -3 | -1 | 1 | -3 | -3 | -9 | -2 | -7 | 5 | -11 | -15 |

Now, for each \(f \in S_1\) we use the lists provided by John Voight to get the minimal polynomials of \(a_{L,3}^0(f)\) and \(a_{L,3}^1(f)\), denoted by \(p_f\) and \(q_f\). Then, for \((a, b) \in \mathbb{F}_3^2\) we compute \(p_f(a_{L,3}^0(E(a,b)))\) and \(q_f(a_{L,3}^1(E(a,b)))\). If at least one of them is non-zero then the exponent \(p\) must divide \(\gcd(p_f(a_{L,3}^0(E)), q_f(a_{L,3}^1(E)))\). Obtaining, for each \((a, b)\) (mod 3), a similar condition on \(p\) gives a contradiction if we take \(p\) not dividing any of the the \(\gcd\). This eliminates \(f\). For example, for \(f = g_1\) we have a contradiction for \(p > 3\). If \(p_f(a_{L,3}^0(E(a,b))) = q_f(a_{L,3}^1(E(a,b))) = 0\) for some pair \((a, b)\) we need to use other primes. After eliminating all the newforms we can using the primes above 3, on the forms that survived, we used simultaneously the primes above 17 and then the prime above 11. After this process, we have a contradiction for \(p > 13\) with all newforms, except for those associated with trivial solutions. We list some of their coefficients in Table 2.

To be able to eliminate these newforms we need to use the extra conditions on \(d\) and \(a + b\). Recall that the solutions \((a, b, c)\) to equation (6) or (7) satisfy \(d \mid a + b\). Recomputing the possibilities for some \(a_L\) but with this extra condition we find that \(a_{L,3}^0 = -3\) and \(a_{L,3}^1 = -1\) (if \(d = 3\)), \(a_{L,5}^0 = -2\) (if \(d = 5\)), \(a_{L,7}^0 = -11\) (if \(d = 7\)) or \(a_{L,11}^0 = -15\) (if \(d = 11\)). By checking in Table 2 we see that any of the previous conditions is enough to eliminate \(f_1\) and \(f_2\). Since \(f_3\) is the newform associated with the trivial solution \((1, -1, 0)\) it cannot be eliminated this way because \(d \mid (-1 + 1) = 0\). Finally, if we assume that the solution is first case (13 \(\mid c\)), Proposition 3.1 says that the conductors at \(p_{13}\) of \(\rho_{f_5,p}|G_K\) and \(\rho_{E,p}|G_K\) are \(p_{13}^0\) and \(p_{13}^1\), respectively. Then, their reduction modulo \(p\) will also have different conductors at \(p_{13}\) if \(p > 13\). Thus they cannot be isomorphic.

Newforms in \(S_2\): We will now eliminate the newforms in \(S_2\) with a similar argument. The following lemma is a consequence of the methods used by John Voight.

**Lemma 5.2** Let \(f\) be a newform in \(S_2(2^s \omega^2)\) for \(s = 3, 4\) such that \(\mathbb{Q}_f\) strictly contains \(\mathbb{Q}\). Then, the Fourier coefficient \(a_{L,3}^0(f)\) is not in \(\mathbb{Q}\).

Suppose isomorphism (11) holds for some \(f \in S_2\) and let \(p_f\) and \(q_f\) be as before. Since \(a_{L,3}^0(E) \in \{-3, -1\}\) and \(a_{L,3}^0(f)\) is not in \(\mathbb{Z}\) we have \(p_f(a_{L,3}^0(E)) \neq 0\) hence the primes above 3 are enough to eliminate all the newforms in \(S_2\). As we have done with \(S_1\), we apply the same arguments using \(\gcd(p_f(a_{L,3}^0(E)), q_f(a_{L,3}^1(E)))\) for all \(f \in S_2\). We obtain a contradiction with all newforms in \(S_2\) if we take...
Remark 5.3 We picked the specific newforms that gave rise to the primes \( p > 100 \) in the previous list and eliminated them using other primes. Unfortunately, this does not help to improve the result because even bigger primes appeared.

Together with the restrictions on \( p \) in the statement of Theorem 4.7 this ends the proof of part (I) of Theorem 1.3. Part (II) now follows easily from the proof of part (I). First note that as before it follows from the factorization
\[
x^{26} + y^{26} = (x^2 + y^2)\phi(x^2, y^2) = 10z^p,
\]
(12)

Proposition 2.3 and Corollary 2.2, that a solution \((a, b, c)\) must verify \( 10 \mid a^2 + b^2 \).
To a primitive solution \((a, b, c)\) we now attach the Frey curve \( E_{(a^2, b^2)} \). Observe also that \( 4 \nmid a^2 + b^2 \) by looking modulo 4. It now follows from Proposition 3.3, modularity and level lowering that the set \( S_1 \) will only have newforms of level \( 2^4w^2 \). This means that after comparing the values \( a_L \) as before, we eliminate all newforms except for the one corresponding to the curve \( E_{(1,1)} \). As we already know, the extra restriction \( 5 \mid a^2 + b^2 \) is enough to deal with this newform. In fact, recall that in this case the Frey curve has \( a_5 = -2 \), and this is different from the corresponding coefficient \( a_5 \) of \( E_{(1,1)} \). The newforms in \( S_2 \) can be eliminated exactly as in the proof of part (I).

Acknowledgments The authors want to thank John Voight for performing multiple computations that were fundamental to finish this work and John Cremona for providing a list of elliptic curves that was useful to test our strategy. We also want to thank the anonymous referee for many comments and suggestions. The second author is also indebted to Ariel Pacetti for helpful conversations.

References
1. Bennett, M., Chen, I.: Multi-Frey \( \mathbb{Q} \)-curves and the Diophantine equation \( a^2 + b^6 = c^p \). Algebra Number Theory 6(4), 707–730 (2012)
2. Bennett, M.A., Ellenberg, J.S., Nathan, C.N.: The Diophantine equation \( A^4 + 2^8B^2 = C^n \). Int. J. Number Theory 6(2), 311–338 (2010)
3. Billerey, N.: Équations de Fermat de type \((5,5,p)\). Bull. Austral. Math. Soc. 76(2), 161–194 (2007)
4. Billerey, N., Dieulefait, L.V.: Solving Fermat-type equations \( x^5 + y^5 = dz^p \). Math. Comp. 79(269), 535–544 (2010)
5. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I: The user language. J. Symbolic Comput. 24, 235–265 (1997)
6. Breuil, C.: \( p \)-adic Hodge theory, deformations and local Langlands. notes of a course at CRM, Bellaterra, Spain, July 2001. http://www.math.u-psud.fr/breuil/PUBLICATIONS/Barcelone.pdf
7. Bruin, N.: On powers as sums of two cubes. Algorithmic number theory (Leiden, 2000), volume 1838 of Lecture Notes in Comput. Sci., pp. 169–184. Springer, Berlin (2000)
8. Buzzard, K., Diamond, F., Jarvis, F.: On Serre’s conjecture for mod \( \ell \) Galois representations over totally real fields. Duke Math. J. 155(1), 105–161 (2010)
9. Chen, I., Siksek, S.: Perfect powers expressible as sums of two cubes. J. Algebra 322(3), 638–656 (2009)
10. Dahmen, S.: Classical and modular methods applied to Diophantine equations. PhD thesis, University of Utrecht.http://igitur-archive.library.uu.nl/dissertations/2008-0820-200949/UiIndex.html (2008)
11. Darmon, H., Granville, A.: On the equations \( z^n = F(x,y) \) and \( Ax^p + By^q = Cz^r \). Bull. London Math. Soc. 27(6), 513–543 (1995)
1004  L. Dieulefait, N. Freitas

12. Deligne, P., Serre, J.-P.: Formes modulaires de poids 1. Ann. Sci. École Norm. Sup. 7(4), 507–530 (1974)

13. Dembélé, L., Voight, J.: Explicit methods for Hilbert modular forms. Elliptic curves, Hilbert modular forms and Galois deformations. In: Diamond, F., et al. (eds.) Birkhauser, Progress in Mathematics (2013, to appear)

14. Dieulefait, L., Freitas, N.: The Fermat-type equations \( x^5 + y^5 = 2z^p \) or \( 3z^p \) solved through \( \mathbb{Q} \)-curves. Math. Comp. (2013, to appear)

15. Ellenberg, J.S.: Galois representations attached to \( \mathbb{Q} \)-curves and the generalized Fermat equation \( A^3 + B^2 = C^p \). Am. J. Math. 126(4), 763–787 (2004)

16. Freitas, N.: Recipes to Fermat-type equations of the form \( (x^r + y^r = Cz^p) \) (2013, Preprint). Available at http://arxiv.org/abs/1203.3371

17. Fujiwara, K.: Level optimization in the totally real case (2006, Preprint). Available at http://arxiv.org/abs/math/0602586

18. Gelbart, S.: Three lectures on the modularity of \( \mathcal{P}_{E,3} \) and the Langlands reciprocity conjecture. In: Modular forms and Fermat’s last theorem (Boston, MA, 1995), pp. 155–207. Springer, New York

19. Jarvis, F.: Correspondences on Shimura curves and Mazur’s principle at \( p \). Pacific J. Math. 213(2), 267–280 (2004)

20. Jarvis, F., Meekin, P.: The Fermat equation over \( \mathbb{Q}(\sqrt{2}) \). J. Number Theory 109(1), 182–196 (2004)

21. Kisin, M.: Modularity of 2-dimensional Galois representations. In: Current developments in mathematics, 2005, pp. 191–230. International Press, Somerville (2007)

22. Kraus, A.: Sur l’équation \( a^3 + b^3 = c^p \). Experiment. Math. 7(1), 1–13 (1998)

23. Kraus, A.: On the equation \( x^p + y^q = z^r \): a survey. Ramanujan J. 3(3), 315–333 (1999)

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

25. Jordi, Q.: \( \mathbb{Q} \)-curves and abelian varieties of \( GL_2 \)-type. Proc. London Math. Soc. (3) 81(2), 285–317 (2000)

26. Rajaei, A.: On the levels of mod \( l \) Hilbert modular forms. J. Reine Angew. Math. 537, 33–65 (2001)

27. Savitt, D.: On a conjecture of Conrad, Diamond, and Taylor. Duke Math. J. 128(1), 141–197 (2005)

28. Skinner, C.M., Wiles, A.J.: Residually reducible representations and modular forms. Inst. Hautes Études Sci. Publ. Math (1999), 89:5–126 (2000)

29. Skinner, C.M., Wiles, A.J.: Nearly ordinary deformations of irreducible residual representations. Ann. Fac. Sci. Toulouse Math. (6) 10(1), 185–215 (2001)

30. Wiles, A.: On ordinary \( \lambda \)-adic representations associated to modular forms. Invent. Math. 94(3), 529–573 (1988)

31. Wiles, A.: Modular elliptic curves and Fermat’s last theorem. Ann. Math. (2) 141(3), 443–551 (1995)