TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 371, Number 12, 15 June 2019, Pages 8651–8677
https://doi.org/10.1090/tran/7477
Article electronically published on March 7, 2019

A MULTI-FREY APPROACH TO FERMAT EQUATIONS OF SIGNATURE (r, r, p)

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

Abstract. In this paper, we give a resolution of the generalized Fermat equations

$$x^5 + y^5 = 3z^n \quad \text{and} \quad x^{13} + y^{13} = 3z^n,$$

for all integers $n \geq 2$ and all integers $n \geq 2$ which are not a power of 7, respectively, using the modular method with Frey elliptic curves over totally real fields. The results require a refined application of the multi-Frey technique, which we show to be effective in new ways to reduce the bounds on the exponents n.

We also give a number of results for the equations $x^5 + y^5 = dz^n$, where $d = 1, 2$, under additional local conditions on the solutions. This includes a result which is reminiscent of the second case of Fermat's Last Theorem and which uses a new application of level raising at p modulo p.

1. Introduction

Wiles' 1995 proof [43] of Fermat's Last Theorem pioneered a new strategy to attack Diophantine equations, now known as *the modular method*. The strategy, originally due to Frey, Serre, Ribet, and Wiles is to attach to a putative solution of a Diophantine equation an elliptic curve E (known as a Frey elliptic curve) and study the mod p representation attached to E via modularity and level lowering. This relates the solution to a modular form of weight 2 and small level, and, to conclude, one needs to show that such relation leads to a contradiction (see Section 2 for more details).

The idea of using this same strategy to study variants of FLT goes back to the work of Serre [42, Section 4.3] and Ribet [40]. Since Wiles' breakthrough, mathematicians have generalized and improved the method and applied it to many other Diophantine equations. In particular, it was natural to use the modular approach to study the *Generalized Fermat Equation*

$$(1.1) \qquad Ax^p + By^q = Cz^r, \qquad p, q, r \in \mathbb{Z}_{\geq 2}, \qquad A, B, C \in \mathbb{Z}_{\neq 0}$$

with A, B, C pairwise coprime. This equation is the subject of the following conjecture.

Conjecture 1. Fix A, B, C as above. Over all choices of prime exponents p, q, r satisfying $1/p + 1/q + 1/r < 1$ the equation (1.1) admits only finitely many solutions

Received by the editors October 8, 2017, and, in revised form, November 30, 2017.

2010 *Mathematics Subject Classification.* Primary 11D41; Secondary 11F80, 11G05.

Key words and phrases. Fermat equations, modular method, multi-Frey.

The first author acknowledges the financial support of ANR-14-CE-25-0015 Gardio.

The fourth author was partly supported by the grant Proyecto RSME-FBBVA 2015 José Luis Rubio de Francia.

(a,b,c) such that $abc \neq 0$ and $\gcd(a,b,c) = 1$. (Here solutions like $2^3 + 1^q = 3^2$ are counted only once.)

The only general result towards the above conjecture is a theorem due to Darmon and Granville [19] which states that if besides A, B, C we also fix the prime exponents p, q, r, then there are only finitely many solutions as above. The conjecture is also known to hold in some particular cases including certain infinite families, for which the authors of this paper have previously made contributions. Moreover, it is also known that the full conjecture is a consequence of the ABC-conjecture (see [19, Section 5.2]).

Bennett [2], [3], Kraus [34], [35], and Siksek [13], [12] and their collaborators have developed and clarified the method using Frey elliptic curves over $\mathbb{Q}$. Unfortunately, there is a restrictive set of exponents (p,q,r) which can be approached using the modular method over $\mathbb{Q}$ due to constraints coming from the classification of Frey representations [19]. As a consequence, attention has now shifted towards using Frey elliptic curves over totally real fields and is made possible because of advances on the Galois representation side (i.e., modularity results).

In this paper, we establish further cases of the conjecture above based on extensions of the modular method to the setting of Hilbert modular forms as introduced in the work of the last two authors [22] and powered by the multi-Frey technique as explained by Siksek in [14], [11].

The results in this paper provide evidence that the multi-Frey technique applied with a ‘sufficiently rich’ set of Frey curves can be used to ‘patch together’ a complete resolution of a one-parameter family of generalized Fermat equations. As will be seen throughout the paper, the multi-Frey technique complements methods used in several steps in the modular method, allowing for refined bounds.

1.1. **Our Diophantine results.**

Let $d \geq 1$ be an integer. We are concerned with Fermat-type equations of the form

$$x^r + y^r = dz^p, \qquad xyz \neq 0, \qquad \gcd(x,y,z) = 1 \tag{1.2}$$

where r, p are prime exponents with r fixed and p is allowed to vary.

We say that a solution $(x,y,z) = (a,b,c)$ of equation (1.2) is *non-trivial* if it satisfies $|abc| > 1$ and we call it *primitive* if $\gcd(a,b,c) = 1$. In the case of most interest to us, $d = 3$, the condition $|abc| > 1$ is equivalent to $abc \neq 0$, but it is important to note that for $d = 2$ there are also the extra trivial solutions $\pm(1,1,1)$.

The equation (1.2) with $r = 5$ and $d = 2, 3$ has already been the subject of the papers [4], [6], and [23], where it was resolved for 3/4 of prime exponents p. For $r = 13$ and $d = 3$, it has been resolved in the papers [22], [28] under the assumption $13 \nmid z$.

Our main Diophantine results are that we completely solve equation (1.2) for $d = 3$ when $r = 5$ (resp. $r = 13$) and $p = n \geq 2$ is any integer (resp. $p = n \geq 2$ is any integer which is not a power of 7). Clearly, this will follow directly from the same statements for prime exponents. More precisely, we will prove the following theorems.

Theorem 1. *For all primes p, there are no non-trivial primitive solutions to*

$$x^5 + y^5 = 3z^p. \tag{1.3}$$

Theorem 2. *For all primes $p \neq 7$, there are no non-trivial primitive solutions to*

$$x^{13} + y^{13} = 3z^p. \tag{1.4}$$

In the previous papers concerning equations (1.3) and (1.4), the main tool used was the modular method, where the Frey elliptic curves were obtained by exploiting the factorization over $\mathbb{Q}(\zeta_r)$ (for $r = 5$ or $r = 13$) of the left-hand side of each equation. More generally, in the work of the last author [26], for each $r \geq 5$, several Frey elliptic curves defined over real subfields of $\mathbb{Q}(\zeta_r)$ are attached to equation (1.2). Our proofs of Theorems 1 and 2 build on these previous works and are made possible by introducing new multi-Frey techniques.

In particular, we show how the multi-Frey technique can be used to obtain tight bounds on the exponent p, improve bounds coming from Mazur-type irreducibility results (see Theorem 8), and move to another level where the required computations of Hilbert modular forms is within the range of what is currently feasible (see paragraph after Lemma 11). We also need a refined 'image of inertia argument' (see Section 3) for the elimination step of the modular method.

A major obstruction to the success of the modular method for solving (1.2) for $d = 1, 2$ is the existence of trivial solutions like $(1, 0, 1)$, $(1, -1, 0)$, or $(1, 1, 1)$. Indeed, when the Frey elliptic curve evaluated at a trivial solution is non-singular its corresponding (via modularity) newform will be among the newforms after level lowering; in particular, the mod p representations of the Frey curve and a newform can be isomorphic, requiring the use of global methods to distinguish Galois representations which are uniform in p.

It is sometimes possible to resolve equation (1.2) by assuming additional q-adic conditions to avoid the obstructing trivial solutions. Indeed, we will prove a number of partial results for the equation (1.2) with $r = 5$ and $d = 1, 2$ under certain q-adic conditions.

For example, we will prove the following result resembling the second case of Fermat's Last Theorem. Its proof involves a new application of the condition for level raising at p modulo p.

Theorem 3. *For all primes p, the equation*

$$x^5 + y^5 = dz^p, \qquad \text{with } d \in \{1, 2\},$$

has no non-trivial solutions (a, b, c) satisfying $p \mid c$.

In addition, we will use the multi-Frey technique to prove the following result, which was known in the case $d = 1$ by work of Billerey ([4, Théorème 1.1]) and Dahmen-Siksek ([18, Proposition 3.3]) using the Frey curve introduced in Section 4.1.

Theorem 4. *For all primes p, the equation*

$$x^5 + y^5 = dz^p$$

has no non-trivial solutions (a, b, c) in each of the following situations:

(i) *$d = 1, 2$, and $5 \mid c$ or*
(ii) *$d = 1$ and c even or*
(iii) *$d = 2$ and c even.*

We remark that, in all our theorems, to deal with certain small primes, we invoke references where the results are obtained using Frey elliptic curves different from the ones used in this paper; this is another instance of the multi-Frey technique.

The computations required to support the proof of our main theorems were performed using `Magma` [7]. The program files are provided with this paper, and we refer to [5] whenever an assertion involves a computation in `Magma` from one of these programs.

2. Overview of the multi-Frey modular method

Notation 1. Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$ and let p be a prime number. For a totally real subfield K of $\overline{\mathbb{Q}}$, we write $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ for its absolute Galois group. For a prime ℓ of K we write I_ℓ for an inertia subgroup at ℓ in G_K. Given E an elliptic curve defined over K, we denote by $\overline{\rho}_{E,p}$ the representation giving the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ on the p-torsion points of E. For a Hilbert modular form f defined over K and a prime ideal $\mathfrak{p}$ in its field of coefficients $\mathbb{Q}_f$, we write $\overline{\rho}_{f,\mathfrak{p}}$ for the mod $\mathfrak{p}$ Galois representation attached to f; when $K = \mathbb{Q}$ we get classical modular forms.

We now recall the main steps of the modular method.

> **Step 1: Constructing a Frey curve.** Attach a Frey elliptic curve E/K to a putative solution of a Diophantine equation, where K is a totally real field. A Frey curve E/K has the property that the Artin conductor of $\overline{\rho}_{E,p}$ is bounded independently of the putative solution.
>
> **Step 2: Irreducibility.** Prove the irreducibility of $\overline{\rho}_{E,p}$.
>
> **Step 3: Modularity.** Prove the modularity of E/K, and hence modularity of $\overline{\rho}_{E,p}$.
>
> **Step 4: Level lowering.** Use level lowering theorems, which require irreducibility of $\overline{\rho}_{E,p}$, to conclude that $\overline{\rho}_{E,p} \cong \overline{\rho}_{f,\mathfrak{p}}$ where f is a Hilbert newform over K of parallel weight 2, is of trivial character, and is level among finitely many explicit possibilities N_i and $\mathfrak{p}$ is a prime ideal above p in the field of coefficients $\mathbb{Q}_f$ of f.
>
> **Step 5: Contradiction.** Compute all the Hilbert newforms predicted in Step 4 and show that $\overline{\rho}_{E,p} \ncong \overline{\rho}_{f,\mathfrak{p}}$ for all of them. This typically uses various methods to distinguish local Galois representations.

In current applications of the modular method, the most challenging step is often Step 5, contrasting with the proof of Fermat's Last Theorem (the origin of the modular method), where the big issue was modularity. Indeed, in the proof of FLT we have $K = \mathbb{Q}$, and in Step 4 there is only one level $N_1 = 2$. Since there are no newforms at this level we get directly a contradiction in Step 5. In essentially every other application of the method, there are candidates for f; therefore more work is needed to complete the argument, namely Step 5. It is now convenient for us to divide Step 5 into two substeps.

> **Step 5a: Computing newforms.** Compute all the Hilbert newforms of parallel weight 2, trivial character, and levels N_i predicted in Step 4.
>
> **Step 5b: Discarding newforms.** For each newform f computed in Step 5a and each prime ideal $\mathfrak{p}$ above p in its field of coefficients show that $\overline{\rho}_{E,p} \ncong \overline{\rho}_{f,\mathfrak{p}}$.

With the objective of succeeding more often in Step 5, Siksek introduced the **multi-Frey technique** in [14] and [11]. This is a variant of Step 1 where more than one Frey curve is used simultaneously in order to put more restrictions on the putative solutions, thereby increasing the likelihood of a contradiction in Step 5b.

It is a common assumption in discussions about the modular method found in the literature that Step 5a can be completed. We want to stress that more recently Step 5a is becoming a real obstruction to the method. This computational obstruction was not noticed in initial applications since they only required small (even empty) spaces of newforms over $\mathbb{Q}$ which were easily accessible. However, when working over totally real fields this is no longer the case as the dimensions of spaces of Hilbert cusp forms grow very fast.

Besides the Diophantine results mentioned in the Introduction, one of the underlying themes of this paper is to illustrate that the multi-Frey approach is a powerful and versatile tool with applications at various stages of the modular method. Indeed, in the proofs of our main results, we will use it to circumvent challenges in Steps 2, 5a, and 5b.

Notation 2. Let E be an elliptic curve defined over a totally real field K and let q be a rational prime such that E has good reduction at each prime ideal $\mathfrak{q}$ dividing q in K. For f a Hilbert newform over K of parallel weight 2 and trivial character, define

$$B_q(E,f) = \gcd\left(\{\mathrm{Norm}\left(a_\mathfrak{q}(E) - a_\mathfrak{q}(f)\right) : \mathfrak{q} \mid q\}\right),$$

where $\mathfrak{q}$ runs through the prime ideals above q in K. Here $a_\mathfrak{q}(f)$ denotes the $\mathfrak{q}$-th Fourier coefficient of f and $a_\mathfrak{q}(E) = \#\mathbb{F}_\mathfrak{q} + 1 - \#\widetilde{E}(\mathbb{F}_\mathfrak{q})$, where $\mathbb{F}_\mathfrak{q}$ is the residual field at $\mathfrak{q}$ and $\widetilde{E}$ denotes the reduction of E modulo $\mathfrak{q}$.

If for some prime ideal $\mathfrak{p}$ above p in the coefficient field of f we have $\overline{\rho}_{E,p} \cong \overline{\rho}_{f,\mathfrak{p}}$, then by considering the trace of Frobenius elements at each prime ideal above q on both sides, we get that p divides $qB_q(E,f)$.

Throughout the paper, we write $\upsilon_\mathfrak{q}(a)$ for the valuation at the prime ideal $\mathfrak{q}$ of the ideal generated by $a \in K$.

3. The image of inertia argument

In this section we recall and generalize the image of inertia argument. This technique, originated in [2], is used to distinguish local Galois representations in Step 5b of the modular method. We start with the well-known version and then provide two generalizations. All three versions are used later in the paper.

Let L be a finite extension of $\mathbb{Q}_\ell$ contained in some fixed algebraic closure $\overline{\mathbb{Q}}_\ell$ of $\mathbb{Q}_\ell$. Let E/L be an elliptic curve with potentially good reduction. Let $m \in \mathbb{Z}_{\geq 3}$ be coprime to ℓ and consider the *inertial field of* E given by $L_E = L^{un}(E[m])$, where L^{un} is the maximal unramified extension of L in $\overline{\mathbb{Q}}_\ell$. The extension L_E/L^{un} is independent of m and it is the minimal extension of L^{un} where E achieves good reduction.

Suppose that, for a prime $p \neq \ell$, we have

$$\overline{\rho}_{E,p} \cong \overline{\rho}_{Z,p}, \tag{3.1}$$

where E and Z are elliptic curves over the local field L and let I_L denote the inertia subgroup of L. In our applications below E and Z will be defined over a totally real number field K and L will be the completion of K at some prime of K above ℓ. Moreover, E will be a Frey elliptic curve and Z an elliptic curve corresponding to a (Hilbert) newform with rational coefficients, as predicted in Step 4 of the modular method. The objective of the inertia argument is to obtain a contradiction to (3.1), thereby establishing

$$\overline{\rho}_{E,p} \not\simeq \overline{\rho}_{Z,p}, \tag{3.2}$$

as required in Step 5b. We will now describe the three versions, each version generalizing the previous one.

Version 1: Different inertia sizes. Show that $\#\overline{\rho}_{E,p}(I_L) \neq \#\overline{\rho}_{Z,p}(I_L)$; this clearly implies (3.2). This is effective when one curve has potentially good reduction and the other has potentially multiplicative reduction and is the original version which has been used in many papers applying the modular method.

Version 2: The field of good reduction. Suppose both E and Z have potentially good reduction. Note that the inertial field L_E corresponds to the field fixed by the restriction $\overline{\rho}_{E,p}|_{I_L}$ and that isomorphism (3.1) implies $\overline{\rho}_{E,p}|_{I_L} \cong \overline{\rho}_{Z,p}|_{I_L}$. Then the inertial fields of E and Z must be the same. Therefore, even when $\#\overline{\rho}_{E,p}(I_L) = \#\overline{\rho}_{Z,p}(I_L)$ (i.e., version 1 fails) we can still establish (3.2) by showing that $L_E \neq L_Z$ (working in a fixed algebraic closure of L).

In practice, this is achieved by finding an extension M/L where Z has good reduction and E does not. Indeed, consider the compositum $M' = L^{un}M$, which is an unramified extension of M. Therefore, the type of reduction of E and Z over M' is the same as over M. Since Z/M' has good reduction by minimality of L_Z, it follows $L_Z \subset M'$; since E/M' does not have good reduction, we have $L_E \not\subset M'$, and hence $L_E \neq L_Z$. We note that (when both curves have potentially good reduction) Version 1 boils down to showing that L_E and L_Z are different because they have different degrees over L^{un}. This version was used in [1] for instance.

Version 3: Different conductors. Let M be an extension of L and let $G_M \subset \mathrm{Gal}(\overline{L}/L)$ be its corresponding subgroup. Note that the isomorphism (3.1) implies that $\overline{\rho}_{E,p}|_{G_M} \cong \overline{\rho}_{Z,p}|_{G_M}$. In particular, the restrictions $\overline{\rho}_{E,p}|_{G_M}$ and $\overline{\rho}_{Z,p}|_{G_M}$ must have the same conductor exponent. Therefore, we can establish (3.2) if we find a field M/L where the two restrictions have different conductor exponents.

In practice, we compute the conductor exponents of A/M, where $A = E$ or Z. However, if A/M has potentially good reduction, then the $\overline{\rho}_{A,p}|_{I_M}$ factors through a finite group of order only divisible by 2 and 3. Hence, the conductor exponent of $\overline{\rho}_{A,p}|_{G_M}$ is the same as the conductor exponent of $\rho_{A,p}|_{G_M}$, where $\rho_{A,p}$ denotes the p-adic representation attached to A. This in turn coincides with the conductor exponent of A/M, provided $p \neq 2, 3$.

Note that Version 2 is obtained by taking $M = L_E$. Indeed, we get $G_M = I_L$, and $\overline{\rho}_{E,p}|_{G_M}$ will have conductor exponent 0 (because E/M has good reduction), whereas $\overline{\rho}_{Z,p}|_{G_M}$ has non-zero conductor exponent (because Z/M does not have good reduction).

Remark 3.3. In applications, the curves are often defined over a totally real number field K. Therefore, we can test if any of the versions above succeed for different primes. Success at one prime is enough to discard the global isomorphism of two mod p representations.

4. A multi-Frey approach to the equation $x^5 + y^5 = 3z^p$

In this section, we will use the following factorization and notation,

$$x^5 + y^5 = (x+y)\phi_5(x,y) = (x+y)\psi_5(x,y)\bar{\psi}_5(x,y),$$

where ω and $\bar{\omega}$ are the complex roots of $X^2 + X - 1$, and

$$\phi_5(x,y) = x^4 - x^3y + x^2y^2 - xy^3 + y^4,$$
$$\psi_5(x,y) = x^2 + \omega xy + y^2, \qquad \bar{\psi}_5(x,y) = x^2 + \bar{\omega}xy + y^2.$$

4.1. **The modular method over $\mathbb{Q}$.**

Here we compile results from [4] and [6].

Let a, b be coprime integers with $a+b \neq 0$. We consider the following Frey elliptic curve over $\mathbb{Q}$, denoted $E(a,b)$ or E in [4] and [6], and whose construction is due to Darmon:

$$W_{a,b} \,:\, y^2 = x^3 - 5(a^2+b^2)x^2 + 5\phi_5(a,b)x.$$

The discriminant $\Delta(W_{a,b})$ of $W_{a,b}$ is given by

$$\Delta(W_{a,b}) = 2^4 5^3 (a+b)^2 (a^5+b^5)^2.$$

The following lemma is a reformulation of results proved in Section 2 of [4].

Lemma 1. *The conductor $N_{W_{a,b}}$ of $W_{a,b}$ is*

$$N_{W_{a,b}} = 2^\alpha \cdot 5^2 \cdot r,$$

where r is the product of all prime divisors $\neq 2, 5$ of $a^5 + b^5$ and

$$\alpha = \begin{cases} 3 & \text{if } ab \equiv 0 \pmod 4, \\ 4 & \text{if } ab \equiv 2 \pmod 4 \text{ or } \upsilon_2(a+b) = 1, \\ 0 & \text{if } \upsilon_2(a+b) = 2, \\ 1 & \text{if } \upsilon_2(a+b) \geq 3. \end{cases}$$

Furthermore, the following properties hold where $j(W_{a,b})$ denotes the j-invariant of $W_{a,b}$:

- *if $\ell \neq 2, 5$ is a prime of bad reduction, then the model defining $W_{a,b}$ is minimal at ℓ and we have $\upsilon_\ell(\Delta(W_{a,b})) = \delta\upsilon_\ell(a^5+b^5)$ where $\delta = 2$, 4 if ℓ divides $\phi_5(a,b)$ or ℓ divides $a+b$ respectively;*
- *we have $\upsilon_2(j(W_{a,b})) \geq 0$ if and only if $\upsilon_2(a+b) \leq 2$;*
- *we have $\upsilon_5(j(W_{a,b})) = 1 - 4\upsilon_5(a+b) < 0$ if $5 \mid a+b$ and $\upsilon_5(j(W_{a,b})) = 0$ otherwise.*

Let W_0 and W_0' be the rational elliptic curves defined by the following equations:

$$W_0 \,:\, y^2 = x^3 + x^2 + 592x - 16812 \quad \text{and} \quad W_0' \,:\, y^2 = x^3 - x^2 - 333x - 2088.$$

They are labelled [37, 1200.k8] and [37, 1200.a1] in LMFDB respectively. In [4], the elliptic curves W_0 and W_0' were referred to as 1200P1 and 1200N1 (in Cremona's labelling) respectively, whereas in [6] the authors used Stein's notation 1200K1 and 1200A1.

Proposition 1. *Let (a,b,c) be a non-trivial primitive solution to (1.3) for $p \geq 5$. Write $W = W_{a,b}$. Then we have $p > 10^7$, $\upsilon_2(ab) = 1$, and $5 \nmid a+b$. Furthermore, we have $\overline{\rho}_{W,p} \cong \overline{\rho}_{W_0',p}$.*

Proof. According to [6, Remark 4.6], we have $p > 10^7$. Besides, it follows from conductor computations (recalled above and in Section 3 of [4]) and [6, Lemma 4.4] that we have $\upsilon_2(ab) = 1$ and $\overline{\rho}_{W,p} \cong \overline{\rho}_{W_0,p}$ or $\overline{\rho}_{W,p} \cong \overline{\rho}_{W_0',p}$ according to whether 5 divides $a+b$ or not.

The curve W_0 has bad additive reduction at 2 with potentially multiplicative reduction. On the other hand, from $\upsilon_2(ab) = 1$ and Lemma 1, it follows that $\upsilon_2(j(W)) \geq 0$. Therefore if I_2 denotes an inertia subgroup at 2, then $\#\overline{\rho}_{W,p}$ belongs to $\{2, 3, 4, 6, 8, 24\}$, while by the theory of Tate curves we have $\#\overline{\rho}_{W_0,p}(I_2) = 2$, or $2p$. In particular, it follows from Version 1 of the image of inertia argument explained in Section 3 that $\overline{\rho}_{W,p} \ncong \overline{\rho}_{W_0,p}$ and $5 \nmid a + b$ as claimed.

Alternatively, we can argue as follows: Suppose $5 \mid a + b$ and $\overline{\rho}_{W,p} \cong \overline{\rho}_{W_0,p}$. Then it follows that $\overline{\rho}_{W,p} \otimes \chi \cong \overline{\rho}_{W\otimes\chi,p} \cong \overline{\rho}_{W_0\otimes\chi,p} \cong \overline{\rho}_{W_0,p} \otimes \chi$, where $W \otimes \chi$ and $W_0 \otimes \chi$ are the twists of W and W_0, respectively, by the quadratic character $\chi = \chi_{-1}$ associated to the quadratic field $\mathbb{Q}(\sqrt{-1})$. Now, the trace of Frobenius at 3 of $W_0 \otimes \chi$ is $a_3(W_0 \otimes \chi) = -1$, whereas the possible traces of Frobenius at 3 of $W \otimes \chi$ are $a_3(W \otimes \chi) = 1, \pm 2$. Hence, $p \leq 3$, a contradiction. □

4.2. **The modular method over $\mathbb{Q}(\sqrt{5})$.** In [23], the modular method was applied with the multi-Frey technique using two Frey $\mathbb{Q}$-curves defined over $\mathbb{Q}(\sqrt{5})$ to solve (1.3) for a set of prime exponents with Dirichlet density 3/4. At the time, the purpose of using $\mathbb{Q}$-curves was to guarantee their modularity. It is now known that elliptic curves over real quadratic fields are modular (see [27]), and therefore we can work directly over $\mathbb{Q}(\sqrt{5})$, largely simplifying the arguments.

We now sharpen the relevant results from [23] in the language of Hilbert modular forms.

Let a, b be coprime integers. Using the notation in the beginning of this section, we consider the two elliptic curves defined over $\mathbb{Q}(\sqrt{5})$ by the following equations:

$$\begin{aligned} E_{a,b} &: \quad y^2 = x^3 + 2(a+b)x^2 - \bar{\omega}\psi_5(a,b)x, \\ F_{a,b} &: \quad y^2 = x^3 + 2(a-b)x^2 + \left(\frac{-3(\omega - \bar{\omega})}{10} + \frac{1}{2}\right)\psi_5(a,b)x. \end{aligned}$$

These two curves were denoted $E_{(a,b)}$ and $F_{(a,b)}$ in [23], respectively. Their standard invariants are given by the following identities:

$$c_4(E_{a,b}) = -2^4\left(\bar{\omega}\psi_5(a,b) + 2^2\omega\bar{\psi}_5(a,b)\right), \tag{4.1}$$

$$c_6(E_{a,b}) = -2^6(a+b)\left(\bar{\omega}\psi_5(a,b) - 2^3\omega\bar{\psi}_5(a,b)\right), \tag{4.2}$$

$$\Delta(E_{a,b}) = 2^6\bar{\omega}\phi_5(a,b)\psi_5(a,b), \tag{4.3}$$

and

(4.4)

$$c_4(F_{a,b}) = 2^4\left(\left(\frac{-3}{10}(\omega - \bar{\omega}) + \frac{1}{2}\right)\psi_5(a,b) + 2^2\left(\frac{3}{10}(\omega - \bar{\omega}) + \frac{1}{2}\right)\bar{\psi}_5(a,b)\right),$$

(4.5)

$$c_6(F_{a,b}) = 2^6(a-b)\left(\left(\frac{-3}{10}(\omega - \bar{\omega}) + \frac{1}{2}\right)\psi_5(a,b) - 2^3\left(\frac{3}{10}(\omega - \bar{\omega}) + \frac{1}{2}\right)\bar{\psi}_5(a,b)\right),$$

(4.6)

$$\Delta(F_{a,b}) = 2^6\left(\frac{-3}{10}(\omega - \bar{\omega}) + \frac{1}{2}\right)^2\left(\frac{3}{10}(\omega - \bar{\omega}) + \frac{1}{2}\right)\phi_5(a,b)\psi_5(a,b).$$

We now determine the conductors of $E_{a,b}$ and $F_{a,b}$. For simplicity, let us write $E = E_{a,b}$ and $F = F_{a,b}$ and denote by N_E and N_F the conductors of the curves E and F, respectively.

Lemma 2. *Let C be one of the curves E or F and let $\mathfrak{q}$ be a prime ideal in $\mathbb{Q}(\sqrt{5})$ of residual characteristic $\ell \neq 2, 5$. Then C has bad reduction at $\mathfrak{q}$ if and only if*

$\ell \mid \phi_5(a,b)$. Moreover in that case, we have $\ell \equiv 1 \pmod 5$ and

$$\upsilon_{\mathfrak{q}}(c_4(C)) = 0 \quad \text{and} \quad \upsilon_{\mathfrak{q}}(\Delta(C)) = 2\upsilon_{\mathfrak{q}}(\psi_5(a,b)) + \upsilon_{\mathfrak{q}}(\bar{\psi}_5(a,b)).$$

In particular, C has bad multiplicative reduction at $\mathfrak{q}$, and hence $\upsilon_{\mathfrak{q}}(N_C) = 1$.

Proof. Recall that $\phi_5(a,b) = \psi_5(a,b)\bar{\psi}_5(a,b)$ with $\psi_5(a,b)$, $\bar{\psi}_5(a,b)$ coprime outside 5 ([23, Proposition 3.1]). If C has bad reduction at $\mathfrak{q}$ with $\mathfrak{q}$ above $\ell \neq 2, 5$, then by formulas (4.1)-(4.3) and (4.4)-(4.6), we have that $\mathfrak{q}$ divides $\psi_5(a,b)\phi_5(a,b) = \psi_5(a,b)^2\bar{\psi}_5(a,b)$ and $\mathfrak{q} \nmid c_4(C)$. Hence $\ell \mid \phi_5(a,b)$. Conversely, if $\ell \mid \phi_5(a,b)$, then any prime ideal $\mathfrak{q}$ above ℓ divides $\psi_5(a,b)\bar{\psi}_5(a,b)$. In particular, we have $\mathfrak{q} \mid \Delta(C)$ and $\mathfrak{q} \nmid c_4(C)$.

Hence the result with the congruence $\ell \equiv 1 \pmod 5$ coming from [23, Lemma 2.2]. □

Let $\mathfrak{q}_2$ and $\mathfrak{q}_5$ be the unique primes in $\mathbb{Q}(\sqrt{5})$ above 2 and 5, respectively. Since 2 is inert in $\mathbb{Q}(\sqrt{5})$ we will write simply 2 for $\mathfrak{q}_2$.

Lemma 3. *We have the following valuations:*

$$\upsilon_2(N_E) = \upsilon_2(N_F) = 6, \tag{4.7}$$

$$\upsilon_{\mathfrak{q}_5}(N_E) = 0 \text{ when } 5 \nmid a+b \text{ and } \upsilon_{\mathfrak{q}_5}(N_E) = 2 \text{ when } 5 \mid a+b, \tag{4.8}$$

$$\upsilon_{\mathfrak{q}_5}(N_F) = 2 \text{ when } 5 \nmid a+b \text{ and } \upsilon_{\mathfrak{q}_5}(N_F) = 0 \text{ when } 5 \mid a+b. \tag{4.9}$$

Proof. We give the details of our computations only for the curve F, the case of E being similar, but simpler. The given model for F is integral at 2, and we have $(\upsilon_2(c_4(F)), \upsilon_2(\Delta(F))) = (4,6)$ (see formulas (4.4) and (4.6)). Therefore, according to [38, Tableau IV], we are either in Case 3 or in Case 4 of Tate's classification. To decide which case actually occurs, we then apply Proposition 1 of [38] with, in its notation, $t = 0$ and $r = 1 + \bar{\omega}$ or $r = 1$ according to whether ab is even or odd, respectively. Let us denote by a_2 and a_4 the coefficients of x^2 and x in the right-hand side of the equation defining F, respectively. Then, we have $\upsilon_2(a_4 + ra_2 + r^2) = 1$ and we conclude that we are in Case 3 of Tate's classification. In particular, we have $\upsilon_2(N_E) = 6$.

For the conductor valuation at $\mathfrak{q}_5$, we first notice that the given model for F is integral at $\mathfrak{q}_5$ if and only if 5 divides $a+b$. In that case we have $\upsilon_{\mathfrak{q}_5}(\phi_5(a,b)) = 2$ and $\upsilon_{\mathfrak{q}_5}(\psi_5(a,b)) = 1$. In particular, the curve F has good reduction at $\mathfrak{q}_5$, and therefore $\upsilon_{\mathfrak{q}_5}(N_F) = 0$. If 5 does not divide $a+b$, then we have $(\upsilon_{\mathfrak{q}_5}(c_4(F)), \upsilon_{\mathfrak{q}_5}(\Delta(F))) = (-1,-3)$. A change of variables over $\mathbb{Q}(\sqrt{5})$ then gives an integral model for F whose c_4 and Δ invariants have respective valuations 3 and 9 at $\mathfrak{q}_5$. According to [38, Tableau I], we have $\upsilon_{\mathfrak{q}_5}(N_F) = 2$. □

In [23], the work of Ellenberg on $\mathbb{Q}$-curves (see [25, Proposition 3.2]) was used to establish that the mod p Galois representations attached to $E_{a,b}$ and $F_{a,b}$ are irreducible for $p = 11$ and $p \geq 17$. We establish here an irreducibility result without using the fact that $E_{a,b}$ and $F_{a,b}$ are $\mathbb{Q}$-curves.

Proposition 2. *Let $p \geq 7$ be a prime number. Then, $\overline{\rho}_{E,p}$ and $\overline{\rho}_{F,p}$ are irreducible when $5 \nmid a+b$ and $5 \mid a+b$ respectively.*

Proof. Let $p \geq 7$ be a prime, and put $C = E$ or $C = F$.

Let us denote by $\overline{\rho}_{C,p}^{ss}$ the semi-simplification of the representation $\overline{\rho}_{C,p}$. Suppose $\overline{\rho}_{C,p}^{ss} \cong \theta \oplus \theta'$ with the characters θ, θ' satisfying $\theta\theta' = \chi_p$, where χ_p denotes the mod p

cyclotomic character. By [29, Lemma 6.3] for instance, we have that θ and θ' are unramified outside p and the additive primes of C. Furthermore, θ and θ' have the same conductor away from p. The unit group of K is generated by $\{-1, \epsilon\}$ where $\epsilon^2 - \epsilon - 1 = 0$. In the notation of [28], we compute $B = -2^6 \cdot 5$. From the first paragraph of the proof of [28, Theorem 1] we thus conclude that exactly one of θ, θ' ramifies at (the primes above) p. Let us therefore assume that θ is unramified at p.

Under the assumptions of the proposition, the only additive prime for C is 2 and it satisfies $\mathrm{Norm}(2) = 4$. It follows from $\upsilon_2(N_C) = 6$ and [31, Theorem 1.5] that level lowering at 2 cannot occur. Therefore, from the conductor computations above (see Lemmas 2 and 3) it follows that the conductor of θ is 2^3.

The Ray class group of $\mathbb{Q}(\sqrt{5})$ of modulus $2^3\infty_1\infty_2$ (where ∞_1 and ∞_2 denote the two real places) is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$. In particular, if $I_2 \subset G_{\mathbb{Q}(\sqrt{5})}$ denotes an inertia subgroup at 2, then $\theta|_{I_2}$ is of order 1 or 2. Thus either C or a quadratic twist C' of C has a 2-torsion point defined over $\mathbb{Q}(\sqrt{5})$. Therefore the torsion subgroup of C or C' has order divisible by $2p$ with $p \geq 7$. From [10, Theorem 6], we see that this is impossible. □

Since $E_{a,b}$ and $F_{a,b}$ are defined over a real quadratic field, they are modular by the main result of [27]. This completes Step 3 of the modular method.

4.3. **Bounding the exponent.**

We are now in position to study equation (1.2) with $r = 5$. Suppose that there exists an integer c such that (a, b, c) is a non-trivial primitive solution to equation (1.2) with $r = 5$ and $p \geq 7$ and assume that all the prime factors ℓ of d satisfy $\ell \not\equiv 1 \pmod 5$. Write $E = E_{a,b}$ and $F = F_{a,b}$.

The following lemma summarizes Step 4 of the modular method as applied to E and F.

Lemma 4. *There exist a Hilbert newform f over $\mathbb{Q}(\sqrt{5})$ of parallel weight 2, trivial character, and level 2^6 and a prime ideal $\mathfrak{p}$ above p in the coefficient field of f such that*

$$\overline{\rho}_{f,\mathfrak{p}} \cong \overline{\rho}_{F,p} \quad \text{or} \quad \overline{\rho}_{f,\mathfrak{p}} \cong \overline{\rho}_{E,p},$$

according to whether 5 divides $a + b$ or not.

Proof. Let $\mathfrak{q}$ be a prime ideal in $\mathbb{Q}(\sqrt{5})$ of bad reduction for E or F with residual characteristic $\ell \neq 2, 5$. According to Lemma 2 and [23, Lemma 2.2], the reduction is multiplicative and, by our assumption on d, the valuation of the minimal discriminant at $\mathfrak{q}$ is $\delta\upsilon_\ell(a^5 + b^5) = \delta(\upsilon_\ell(d) + p\upsilon_\ell(c)) = \delta p\upsilon_\ell(c)$, where $\delta = 1$, 2 when $\mathfrak{q}$ divides $\bar{\psi}_5(a, b)$ or $\mathfrak{q}$ divides $\psi_5(a, b)$ respectively. In particular, it is divisible by p. We conclude from Lemma 3 that the Artin conductor of the mod p representations of F and E is 2^6 according to whether 5 divides $a + b$ or not.

The rest of the proof follows by applying level lowering for Hilbert modular forms (see [30], [32], [39]), with irreducibility coming from Proposition 2 above. □

Let $q \neq 2, 5$ be a rational prime such that $q \not\equiv 1 \pmod 5$ and let $\mathfrak{q}$ be a prime in $\mathbb{Q}(\sqrt{5})$ above q. It follows from Lemma 2 that for any integers x, y with $(x, y) \neq (0, 0)$ and $0 \leq x, y \leq q - 1$, both elliptic curves $E_{x,y}$ and $F_{x,y}$ have good reduction at $\mathfrak{q}$. Moreover if x, y are defined by $(a, b) \equiv (x, y) \pmod q$ and $0 \leq x, y \leq q - 1$, then $a_{\mathfrak{q}}(E_{a,b}) = a_{\mathfrak{q}}(E_{x,y})$.

The result below follows from Lemma 4 and our definitions here and in Section 2.

Proposition 3. *There exists a Hilbert newform f over $\mathbb{Q}(\sqrt{5})$ of parallel weight 2, trivial character, and level 2^6 such that for any prime $q \neq 2, 5$ with $q \not\equiv 1 \pmod 5$, there exists $(x,y) \in \{0,\dots,q-1\}^2 \smallsetminus \{(0,0)\}$ such that we have $p \mid qB_q(E_{x,y}, f)$ or $p \mid qB_q(F_{x,y}, f)$, respectively if $5 \nmid a+b$ or $5 \mid a+b$.*

The following summarizes part of Step 5 of the modular method as applied to the Frey elliptic curves E and F.

Proposition 4.

(1) *If $5 \nmid a+b$ and $p \geq 7$, then $\overline{\rho}_{E,p}$ is isomorphic to the mod p representation of one of the curves*

$$E_{1,0}, \quad E_{1,0}\otimes\chi_{-1}, \quad E_{1,0}\otimes\chi_{2}, \quad E_{1,0}\otimes\chi_{-2}, \quad E_{1,1}, \quad E_{1,1}\otimes\chi_{2}.$$

(2) *If $5 \mid a+b$ and $p \geq 11$, then $\overline{\rho}_{F,p}$ is isomorphic to the mod p representation of one of the curves*

$$F_{1,-1} \quad \text{or} \quad F_{1,-1}\otimes\chi_2,$$

where χ_D denotes the quadratic character corresponding to the field $\mathbb{Q}(\sqrt{D})$.

Proof. Using [5], we do the following: we compute all the newforms over $\mathbb{Q}(\sqrt{5})$ of level 2^6, parallel weight 2, and trivial character. For each such newform h, we compute $q\mathcal{E}_q(h)$ and $q\mathcal{F}_q(h)$ for all primes $q \leq 30$ as above where $\mathcal{E}_q(h)$ (resp. $\mathcal{F}_q(h)$) is the product of all $B_q(E_{x,y}, h)$ (resp. $B_q(F_{x,y}, h)$) over the pairs $(x,y) \not\equiv (0,0)$ of integers in the range $\{0,\dots,q-1\}$.

Suppose $5 \nmid a+b$. From the previous proposition it follows that, for each h, if p does not divide the gcd of all $q\mathcal{E}_q(h)$ we can discard h for that p. This allows us to discard all except 6 newforms for $p \geq 7$; we identify the remaining 6 newforms with twists of the Frey elliptic curves $E_{1,0}$ and $E_{1,1}$.

Suppose $5 \mid a+b$. From the previous proposition it follows that, for each h, if p does not divide the gcd of all $q\mathcal{F}_q(h)$ we can discard h for that p. For $p \geq 11$, this allows us to discard all except 2 newforms which correspond to $F_{1,-1}$ and its quadratic twist by 2. We also note for later use that $p \geq 7$ works for all except three other newforms f, all of them satisfying $a_3(f) = 4$. □

4.4. **Proof of Theorem 1.** We will now prove Theorem 1 under the slightly more general situation where d is divisible by 3 but not by any prime $\ell \equiv 1 \pmod 5$.

From $3 \mid d$ and [23, Lemma 2.2], it follows that $3 \mid a+b$. This imposes a very strong restriction on the value of the trace of Frobenius of $E_{a,b}$ at (the unique prime ideal above) 3 in $\mathbb{Q}(\sqrt{5})$. Namely, the elliptic curve $E_{a,b}$ reduces modulo 3 to the curve defined by $y^2 = x^3 - \bar{\omega}^2 x$. Hence, we have $a_3(E_{a,b}) = 6$.

Note that the elliptic curves $E_{x,y}$ that appear in part (1) of Proposition 4 satisfy $x+y \not\equiv 0 \pmod 3$. Therefore, for $p \geq 7$, one may hope to discard them by computing their trace of Frobenius at 3. Indeed, we find that the a_3 coefficient of the curves $E_{1,0}$, $E_{1,0}\otimes\chi_{-1}$, $E_{1,0}\otimes\chi_2$, $E_{1,0}\otimes\chi_{-2}$, $E_{1,1}$, and $E_{1,1}\otimes\chi_2$ is 4. We have thus proved the following result.

Proposition 5. *If $p \geq 7$ and d is divisible by 3 but not by any prime $\ell \equiv 1 \pmod 5$, then we necessarily have $5 \mid a+b$.*

Remark 4.10. The previous type of argument does not always work. For instance, when $r = 7$ and $d = 3$ in equation (1.2), the condition $3 \mid a+b$ does not distinguish

$E_{0,1}$ and $E_{1,-1}$ by traces of Frobenius at 3, where $E_{a,b}$ is the Frey elliptic curve in the last paragraph of [26, p. 630].

To prove Theorem 1 it now suffices to notice that the cases $p = 2$, $p = 3$, and $p = 5$ follow from [2, Theorem 1.1], [3, Theorem 1.5], and [24, Théorème IX], respectively. Hence we can assume $p \geq 7$. Applying Propositions 1 and 5 concludes the proof.

Remark 4.11. Note we cannot improve on the result in [23] for $r = 5$ and $d = 2$ since we do not have the condition $3 \mid a + b$ to eliminate the curves in Proposition 4(1). Furthermore, the additional use of the Frey elliptic curve $W_{a,b}$ also does not help because $W_{1,1}$ is an elliptic curve without complex multiplication.

5. Partial results for $x^5 + y^5 = dz^p$ with $d = 1, 2$

It is sometimes possible to resolve equation (1.2) by assuming additional q-adic conditions to avoid the obstructing trivial solutions. In this section we provide such examples regarding the equation

$$x^5 + y^5 = dz^p, \quad \text{where } d \in \{1, 2\}. \tag{5.1}$$

First note that the conditions on c of Theorem 4 can easily be translated into divisibility conditions on $a+b$. More precisely, Theorem 4 follows from the following two theorems.

Theorem 5. *Assume $d = 1, 2$. Then, for all primes p, there are no non-trivial primitive solutions (a, b, c) to* (5.1) *satisfying $5 \mid a + b$.*

Theorem 6. *Assume $d = 1$ (resp. $d = 2$). Then, for all primes p, there are no non-trivial primitive solutions to* (5.1) *satisfying $2 \mid a + b$ (resp. $4 \mid a + b$).*

We want to emphasize that in the proof of Theorem 5, using the multi-Frey technique we are able to force a Frey curve to have multiplicative reduction at 3.

These results, and their proofs, should illustrate clearly to the reader that the obstruction to solving (5.1) with $d = 1$ (resp. $d = 2$) is that none of the Frey curves we use are sensitive to the trivial solutions $\pm(1, 0, 1), \pm(0, 1, 1)$ (resp. $\pm(1, 1, 1)$).

5.1. Proof of Theorem 5.

The cases $p = 2$ and $p = 3$ follow from [2, Theorem 1.1] and [3, Theorem 1.5], respectively. It follows from Fermat's Last Theorem and the main theorem of [20] that the result holds for $p = 5$. Hence we can assume $p \geq 7$.

Let (a, b, c) be a putative non-trivial primitive solution to equation (5.1) with $d = 1, 2$, exponent $p \geq 7$, and $5 \mid a + b$.

By part (2) of Proposition 4 we have $\overline{\rho}_{F_{a,b},p} \cong \overline{\rho}_{A,p}$, where $A = F_{1,-1}$ or $F_{1,-1} \otimes \chi_2$ when $p \geq 11$. Furthermore, from its proof it follows that for $p = 7$ we can have $\overline{\rho}_{F,p} \cong \overline{\rho}_{A,p}$ or $\overline{\rho}_{F,p} \cong \overline{\rho}_{f,p}$, where f is one of the other three possible Hilbert newforms over $\mathbb{Q}(\sqrt{5})$ of parallel weight 2, trivial character, and level 2^6.

The traces of Frobenius at 3 of these five newforms satisfy $a_3(A) = a_3(f) = 4$. Using `Magma` to compute $a_3(F_{a,b})$ shows that $3 \mid a+b$ (if not, then $a_3(F_{a,b}) \in \{-2, 6\}$ and we get that $p \mid 6$, which is not the case). This means the curve $W = W_{a,b}$ from Section 4.1 has multiplicative reduction at 3 (see Lemma 1). Note that this is another instance of using the multi-Frey technique.

From [4, Proposition 3.1] we have that the representation $\overline{\rho}_{W,p}$ is irreducible. A standard application of the modular method with W (which follows from Propositions 3.3 and 3.4 of [4]) gives that $\overline{\rho}_{W,p} \cong \overline{\rho}_{g,p}$, where g is a rational newform of weight 2, trivial Nebentypus, and level $2^4 \cdot 5^2$, $2^3 \cdot 5^2$, or $2 \cdot 5^2$ for $d = 1$ and $2^4 \cdot 5^2$, $2 \cdot 5^2$ for $d = 2$, respectively. All newforms in these spaces correspond to (isogeny classes of) elliptic curves over $\mathbb{Q}$. Since level lowering is happening at the prime 3, we must have that $p \mid (3+1)^2 - a_3(g)^2$. By the Hasse bound and our assumption, it implies that $p = 7$ and $a_3(g) = \pm 3$.

We then notice using [16] that there are four newforms g of these levels for which we have $a_3(g) = \pm 3$. Moreover they all correspond to elliptic curves with potentially good reduction at 5 and whose minimal discriminant has valuation 2 or 8 at 5. According to [41, p. 312] it follows that $\#\overline{\rho}_{g,7}(I_5) = 3$ or 6, where I_5 is an inertia subgroup at 5.

On the other hand, since $5 \mid a + b$, the curve W has potentially multiplicative reduction at 5 (see Lemma 1). Hence by the theory of Tate curves, we have $\#\overline{\rho}_{W,7}(I_5) = 2$ or 14. According to Version 1 of the image of inertia argument explained in Section 3, this gives the desired contradiction.

5.2. **Proof of Theorem 6.** As in the previous proof, the result is known for $p \leq 5$. Let (a, b, c) be a putative non-trivial primitive solution to equation (5.1) with $d = 1$ and $2 \mid a + b$ (resp. $d = 2$ and $4 \mid a + b$) for $p \geq 7$.

In the case $d = 1$, the condition $2 \mid a + b$ implies that in fact $8 \mid a + b$, because $2 \mid c$, $p \geq 7$, and $2 \nmid \phi_5(a, b)$, where we recall $a^5 + b^5 = (a + b)\phi_5(a, b) = dc^p$; in the case $d = 2$, the condition $4 \mid a + b$ also implies that in fact $8 \mid a + b$. So we now assume $8 \mid a + b$.

By Theorem 5, we may assume $5 \nmid a + b$, and then invoking part (1) of Proposition 4 we deduce that $\overline{\rho}_{E,p} \cong \overline{\rho}_{A,p}$ where $A = E_{1,0}$, $E_{1,0} \otimes \chi_{-1}$, $E_{1,0} \otimes \chi_2$, $E_{1,0} \otimes \chi_{-2}$, $E_{1,1}$, or $E_{1,1} \otimes \chi_2$.

The result now follows from Version 2 of the image of inertia argument (see Section 3). Indeed, from $\overline{\rho}_{E,p} \cong \overline{\rho}_{A,p}$ we know that the inertial field at 2 of E and A must be the same. By Proposition 6 below and the assumption $8 \mid a + b$, we see this is not possible, as desired.

Write $L_{a,b} = L_{E_{a,b}}$ for the inertial field at 2 corresponding to the Frey elliptic curve $E_{a,b}$ (i.e., the field fixed by the kernel of $\overline{\rho}_{E_{a,b},m}(I_2)$ for any $m \geq 3$ coprime to 2). Respectively, for any integers x, y, we write $L_{x,y,D}$ for the inertial field at 2 corresponding to the curve $E_{x,y} \otimes \chi_D$.

Proposition 6. *Suppose (a, b, c) is a non-trivial primitive solution to (5.1) satisfying $8 \mid a + b$. Then $L_{a,b} \neq L_{1,0}$, $L_{1,0,-1}$, $L_{1,0,2}$, $L_{1,0,-2}$, $L_{1,1}$, $L_{1,1,2}$.*

Proof. This is verified using [5] by considering a suitable subfield M of the 3-division field of Z over $\mathbb{Q}(\sqrt{5})$, where $Z = E_{1,0}$, $E_{1,0} \otimes \chi_{-1}$, $E_{1,0} \otimes \chi_2$, $E_{1,0} \otimes \chi_{-2}$, $E_{1,1}$, or $E_{1,1} \otimes \chi_2$, with the property that Z has good reduction at a prime above 2 of M, but $E_{a,b}$ does not have good reduction at this prime above 2 of M if $8 \mid a + b$. It turns out that we can take M to be the subfield generated by the x and y coordinates of a choice of a 3-torsion point of Z.

We have the following two cases:

(a) For $Z = E_{1,1}, E_{1,1} \otimes \chi_2$, the choice of M has degree 4 over $\mathbb{Q}(\sqrt{5})$. Let $\mathfrak{q}'$ be the unique prime above 2 of M with ramification index 4.

(b) For $Z = E_{1,0}, E_{1,0} \otimes \chi_{-1}, E_{1,0} \otimes \chi_2, E_{1,0} \otimes \chi_{-2}$, the choice of M has degree 8 over $\mathbb{Q}(\sqrt{5})$. Let $\mathfrak{q}'$ be the unique prime above 2 of M with ramification index 8.

We remark that the full 3-division field of Z has degree 8 and 48 over $\mathbb{Q}(\sqrt{5})$ in cases (a) and (b), respectively. Thus, the choice of the smaller subfield M makes the computation feasible in case (b).

To show that $E_{a,b}$ does not have good reduction at the prime $\mathfrak{q}'$ of M if $8 \mid a+b$, we note that $v_{\mathfrak{q}'}(\Delta) = 24$ and 48 in cases (a) and (b), respectively.

Consider now $E' = E_{a',b'}$ and suppose that the reduction type of E' is either II, II^*, or I_0^* and we have that both $v_{\mathfrak{q}'}(a-a')$ and $v_{\mathfrak{q}'}(b-b')$ are $\geq 6 \cdot 4 = 24$. By [1, Lemma 2.1], the reduction type of E and E' at $\mathfrak{q}'$ are the same, and hence the conductor exponents at $\mathfrak{q}'$ of E and E' are the same.

In other words, if $(a,b) \equiv (a',b') \pmod{2^4}$, then the conductor exponent at $\mathfrak{q}'$ of $E_{a,b}$ is the same as that of $E_{a',b'}$, provided the reduction type of $E_{a',b'}$ is II, II^*, or I_0^*. Assuming $8 \mid a+b$ and using [5], it is thus shown that $E_{a,b}/M$ has conductor exponent $\neq 0$ at the prime of M above 2, whereas Z/M has good reduction at the prime of M above 2. □

6. A result on the second case

In this section, we prove Theorem 3. The following proposition is known to experts, but we have not been able to find a suitable reference for it, so we include a proof.

Proposition 7. *Let f be a (classical) newform of weight 2, trivial character, and level N. Let p be an odd prime not dividing N, and let a_p denote the p-th Fourier coefficient of f. Then, a necessary condition for the existence of a congruence between the p-adic Galois representation attached to f and the one attached to a newform g of level pN, trivial character, and weight 2 is*

$$a_p \equiv \pm 1 \pmod{p}. \tag{6.1}$$

Proof. Denote by $\rho_{f,p}$ and $\rho_{g,p}$ the restrictions to $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ of the respective global p-adic Galois representations attached to f and g. Then f congruent to g modulo p implies in particular that the semisimplifications of the residual local representations $\bar{\rho}_{f,p}^{ss}$ and $\bar{\rho}_{g,p}^{ss}$ of, respectively, $\rho_{f,p}$ and $\rho_{g,p}$ are isomorphic. We assume $p > 2$. Since $\rho_{g,p}$ is semistable non-crystalline of weight 2, $\bar{\rho}_{g,p}^{ss}$ is reducible and isomorphic to $\chi_p \mathrm{unr}(\mu) \oplus \mathrm{unr}(\mu)$ for some mod p unit μ and where χ_p denotes the mod p cyclotomic character (this is the case $k = 2$ of [9, Théorème 1.2]). Thus, the same holds for $\bar{\rho}_{f,p}^{ss}$. By [8, Théorème 6.7] (a theorem that puts together results of Deligne, Serre, Fontaine, and Edixhoven) this forces a_p to be congruent to ± 1 modulo p. □

Using the above proposition, we now prove Theorem 3.

The cases $p = 2$ and $p = 3$ follow from [2, Theorem 1.1] and [3, Theorem 1.5], respectively. It follows from Fermat's Last Theorem and the main theorem of [20] that the result holds for $p = 5$. Hence we can assume $p \geq 7$.

We know (see [4, Proposition 3.1]) that the mod p Galois representation attached to the Frey elliptic curve W is irreducible, for every $p \geq 7$. By level lowering, we have a congruence modulo p between the Frey elliptic curve W and some weight 2 newform of level $N = 50$, 200, or 400. Since we are assuming that p divides c, level raising at p mod p is happening for this specific newform. This implies in particular that the necessary condition in Proposition 7 must hold.

All newforms in these spaces correspond to (isogeny classes of) elliptic curves over $\mathbb{Q}$, and we consider the cases when:

(1) the elliptic curve does not have a rational 2-torsion point or
(2) the elliptic curve has a rational 2-torsion point.

Case 1. For all such elliptic curves, it can be checked (using [16] for instance) that the coefficient a_3 equals ±1 or ±3. Then we easily conclude using the congruence between these values and $0, \pm2, \pm4$ that this cannot happen for $p > 7$. We are using the fact that the Frey elliptic curve W has a rational 2-torsion point, and we are covering both the cases of W having good or multiplicative reduction at 3. For $p = 7$, the congruence forces $a_3 = \pm3$. We then quickly verify using [16] that none of the curves of level $N \in \{50, 200, 400\}$ satisfy both $a_3 = \pm3$ and $a_7 \equiv \pm1 \pmod 7$.

Case 2. The fact that mod p we have level raising at p forces the necessary condition in Proposition 7 to hold: $a_p \equiv \pm1 \pmod p$. For an elliptic curve, this is equivalent to implying that $a_p = \pm1$ by the Hasse bound. But all curves in case 2 have a rational 2-torsion point; thus all their coefficients a_q for $q \nmid N$ are even. This gives a contradiction.

Remark 6.2. As pointed out to us by the referee, instead of Proposition 7, we could have used [36, Proposition 3(iii)] because f and g correspond to elliptic curves over $\mathbb{Q}$. However, the more general Proposition 7 may be useful in other applications of the modular method when level lowering results in a newform with non-rational Fourier coefficients.

7. A multi-Frey approach to the equation $x^{13} + y^{13} = 3z^p$

Let ζ_{13} be a primitive 13-th root of unity. In this section, we will use the following factorization and notation:

$$x^{13} + y^{13} = (x+y)\phi_{13}(x,y) = (x+y)\psi_{13}(x,y)\bar{\psi}_{13}(x,y), \tag{7.1}$$

where

$$\begin{aligned}\psi_{13}(x,y) &= (x+\zeta_{13}y)(x+\zeta_{13}^4y)(x+\zeta_{13}^3y)(x+\zeta_{13}^{12}y)(x+\zeta_{13}^9y)(x+\zeta_{13}^{10}y)\\ &= x^6 + \frac{1}{2}(w-1)x^5y + 2x^4y^2 + \frac{1}{2}(w+1)x^3y^3 + 2x^2y^4 + \frac{1}{2}(w-1)xy^5 + y^6\end{aligned}$$

and $\bar{\psi}_{13}(x,y)$ are the two degree 6 irreducible factors of $\phi_{13}(x,y)$ over $\mathbb{Q}(w)$, where $w \in \mathbb{Q}(\zeta_{13})$ satisfies $w^2 = 13$.

7.1. The modular method over $\mathbb{Q}(\sqrt{13})$.

We will now prove the following theorem by sharpening the methods in [22] plus a refined image of inertia argument.

Theorem 7. *Let (a,b,c) be a non-trivial primitive solution to equation* (1.2) *with $r = 13$, $p \geq 5$, $p \neq 7, 13$, and d such that all its prime factors ℓ satisfy $\ell \not\equiv 1 \pmod{13}$. If 3 divides d, then we have*

(A) *$13 \mid a + b$ and*
(B) *$4 \mid a + b$.*

Before entering the proof of this result, we first introduce tools from [22] which are valid beyond the setting of the theorem. Write $\zeta = \zeta_{13}$ and define

$$A_{x,y} = \alpha(x^2 + (\zeta + \zeta^{-1})xy + y^2), \quad B_{x,y} = \beta(x^2 + (\zeta^3 + \zeta^{-3})xy + y^2),$$
$$C_{x,y} = \gamma(x^2 + (\zeta^4 + \zeta^{-4})xy + y^2),$$

where

$$\alpha = \zeta^4 + \zeta^{-4} - \zeta^3 - \zeta^{-3}, \qquad \beta = \zeta + \zeta^{-1} - \zeta^4 - \zeta^{-4}, \qquad \gamma = \zeta^3 + \zeta^{-3} - \zeta - \zeta^{-1}$$

all have norm 13^2. We note that $A_{x,y}$, $B_{x,y}$, $C_{x,y}$ are polynomials with coefficients in (the maximal totally real subfield of) $\mathbb{Q}(\zeta)$ satisfying $A_{x,y} + B_{x,y} + C_{x,y} = 0$.

Suppose now that a, b are coprime integers. Let us denote by $E_{a,b}$ the short Weierstrass model of the elliptic curve $Y^2 = X(X - A_{a,b})(X + B_{a,b})$ given by

$$E_{a,b} : y^2 = x^3 + a_4(a,b)x + a_6(a,b),$$

where

$$\begin{aligned} a_4(a,b) &= 3^3 \left(A_{a,b}B_{a,b} + A_{a,b}C_{a,b} + B_{a,b}C_{a,b}\right), \\ a_6(a,b) &= -3^3 \left(2A_{a,b}^3 + 3A_{a,b}^2 B_{a,b} - 3A_{a,b}B_{a,b}^2 - 2B_{a,b}^3\right). \end{aligned}$$

This curve (in a slightly different short model) was first considered in [22], where it is denoted E_0. We then verify that $E_{a,b}$ is defined over $\mathbb{Q}(\sqrt{13})$. Its standard invariants are given by the following identities:

$$\begin{aligned} c_4(E_{a,b}) &= -2^4 \cdot 3 \cdot a_4(a,b) = -2^4 \cdot 3^4 \left(A_{a,b}B_{a,b} + A_{a,b}C_{a,b} + B_{a,b}C_{a,b}\right), \\ \Delta(E_{a,b}) &= 2^4 \cdot 3^{12} \left(A_{a,b}B_{a,b}C_{a,b}\right)^2 = 2^4 \cdot 3^{12} \cdot 13 \cdot \psi_{13}(a,b)^2. \end{aligned}$$

We now determine the conductor of $E_{a,b}$. For simplicity, let us write $E = E_{a,b}$ and N_E for its conductor.

Lemma 5. *Let $\mathfrak{q}$ be a prime ideal in $\mathbb{Q}(\sqrt{13})$ of residual characteristic $\ell \neq 2, 13$. Then E has bad reduction at $\mathfrak{q}$ if and only if $\mathfrak{q}$ divides $\psi_{13}(a,b)$. Moreover, in that case, we have*

$$\ell \equiv 1 \pmod{13}, \qquad \upsilon_{\mathfrak{q}}(c_4(E)) = 0 \quad \textit{and} \quad \upsilon_{\mathfrak{q}}(\Delta(E)) = 2\upsilon_{\mathfrak{q}}(\psi_{13}(a,b)).$$

In particular, E has bad multiplicative reduction at $\mathfrak{q}$, and hence $\upsilon_{\mathfrak{q}}(N_E) = 1$.

Proof. Recall that as elements of $\mathbb{Q}(\zeta)$, $A_{a,b}$, $B_{a,b}$, and $C_{a,b}$ are relatively prime outside 13.

Let us first assume that $\ell \neq 3$. It follows from the formulas above that if E has bad reduction at $\mathfrak{q}$, then $\mathfrak{q}$ divides $\psi_{13}(a,b)$ and $\mathfrak{q}$ does not divide $c_4(E)$. Conversely if $\mathfrak{q} \mid \psi_{13}(a,b)$, then $\mathfrak{q}$ divides $(A_{a,b}B_{a,b}C_{a,b})^2 = 13 \cdot \psi_{13}(a,b)^2$ and $\mathfrak{q}$ does not divide $c_4(E)$. Hence the equivalence. Moreover, we have $\upsilon_{\mathfrak{q}}(\Delta(E)) = 2\upsilon_{\mathfrak{q}}(\psi_{13}(a,b))$, and the congruence $\ell \equiv 1 \pmod{13}$ follows from [22, Section 2].

It remains to show that E has good reduction at the prime ideals in $\mathbb{Q}(\sqrt{13})$ above 3. Let $\mathfrak{q}$ be such a prime. From [22, Section 2], we have that $\mathfrak{q}$ does not divide $\psi_{13}(a,b)$. Therefore, we have $(\upsilon_{\mathfrak{q}}(c_4(E)), \upsilon_{\mathfrak{q}}(\Delta(E))) = (\geq 4, 12)$, and the defining model of E is not minimal at $\mathfrak{q}$ ([38, Tableau I]). A change of variables then shows that E has good reduction at $\mathfrak{q}$, as claimed. □

The following lemma follows from a similar statement for the curve E_0 in [22, Proposition 3.3].

Lemma 6. *We have*

$$\upsilon_w(N_E) = 2 \quad \textit{and} \quad \upsilon_2(N_E) = s \qquad \textit{where } s = 3, 4.$$

Moreover, when $a + b$ is even, $s = 3$ if $4 \mid a + b$ and $s = 4$ if $4 \nmid a + b$.

The next proposition gives us the required irreducibility of the mod p representation of E.

Proposition 8. *Let $p \geq 7$ be a prime number. Then the representation $\overline{\rho}_{E,p}$ is irreducible.*

Moreover, if 3 divides $a+b$, then $\overline{\rho}_{E,5}$ is also irreducible.

Proof. We note that the proof of [28, Theorem 3] applies in our situation, thereby proving the proposition for $p = 11$ and $p \geq 17$. Assume therefore that $p \in \{5, 7, 13\}$.

We note that 3 splits in $\mathbb{Q}(\sqrt{13})$ and let $\mathfrak{q}_1$, $\mathfrak{q}_2$ be the primes above it with $w + 1 \in \mathfrak{q}_1$ (and $w - 1 \in \mathfrak{q}_2$). By Lemma 5, the primes $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are primes of good reduction of E. Since $a, b \in \mathbb{Z}$ we can check that the pairs of traces of Frobenius at these primes $(a_{\mathfrak{q}_1}(E), a_{\mathfrak{q}_2}(E))$ satisfy

$$(a_{\mathfrak{q}_1}(E), a_{\mathfrak{q}_2}(E)) \in \{(-3,-1), (-1,-3), (-1,1)\}.$$

Moreover, the case $(-3,-1)$ occurs precisely when $3 \mid a+b$. Therefore, we can compute the corresponding pairs of characteristic polynomials of

$$(\overline{\rho}_{E,p}(\mathrm{Frob}_{\mathfrak{q}_1}), \overline{\rho}_{E,p}(\mathrm{Frob}_{\mathfrak{q}_2})),$$

which are given by

$$(x^2 - a_{\mathfrak{q}_1}(E)x + 3, x^2 - a_{\mathfrak{q}_2}(E)x + 3). \tag{7.2}$$

Now suppose that $\overline{\rho}_{E,p}$ is reducible. Then, for any prime $\mathfrak{q}$ in $\mathbb{Q}(\sqrt{13})$ of good reduction of E, the characteristic polynomial of $\overline{\rho}_{E,p}(\mathrm{Frob}_{\mathfrak{q}})$ must factor over $\mathbb{F}_p$ into two linear polynomials. In particular, this holds for $\mathfrak{q} = \mathfrak{q}_1, \mathfrak{q}_2$.

For $p = 5$, 7, and 13, we check that each of the pairs of polynomials in (7.2) always contains one polynomial that does not factor over $\mathbb{F}_p$ except when $p = 5$ and $(a_{\mathfrak{q}_1}(E), a_{\mathfrak{q}_2}(E)) = (-1, 1)$. This proves the proposition for $p \geq 7$. Finally, assume $3 \mid a + b$. In that case, we already observed that $(a_{\mathfrak{q}_1}(E), a_{\mathfrak{q}_2}(E)) = (-3,-1) \neq (-1,1)$. We conclude that $\overline{\rho}_{E,5}$ is irreducible, finishing the proof. □

We note that modularity of $E_{a,b}$ is guaranteed by [27], hence completing Step 3 of the modular method.

We are now in position to study equation (1.2) with $r = 13$. Suppose that there exists an integer c such that (a, b, c) is a non-trivial primitive solution to (1.2) with $r = 13$ and $p \geq 5$ and assume that all the prime factors ℓ of d satisfy $\ell \not\equiv 1 \pmod{13}$. Write again $E = E_{a,b}$.

The following lemma summarizes Step 4 of the modular method.

Lemma 7. *We have*

$$\overline{\rho}_{E,p} \cong \overline{\rho}_{f,\mathfrak{p}},$$

where $\mathfrak{p}$ is a prime in $\overline{\mathbb{Q}}$ of residual characteristic p and f is a Hilbert newform over $\mathbb{Q}(\sqrt{13})$ of parallel weight 2, trivial character, and level

$$N_f = 2^s w^2, \qquad \text{where } s = 3, 4.$$

Moreover, when $a+b$ is even, $s = 3$ if $4 \mid a+b$ and $s = 4$ if $4 \nmid a+b$.

If in addition we have that 3 divides $a+b$, then the above also holds for $\overline{\rho}_{E,5}$.

Proof. Let $\mathfrak{q}$ be a prime ideal in $\mathbb{Q}(\sqrt{13})$ of bad reduction for E with residual characteristic $\ell \neq 2, 13$. According to Lemma 5 and Section 2 of [22], the reduction is multiplicative, and, by our assumption on d, the valuation of the minimal discriminant at $\mathfrak{q}$ is $2v_{\mathfrak{q}}(\psi_{13}(a,b)) = 2v_\ell(a^{13} + b^{13}) = 2v_\ell(d) + 2pv_\ell(c) = 2pv_\ell(c)$. In particular, it is divisible by p. We conclude from Lemma 6 that the Artin conductor of the mod p representations of E is $2^s w^2$ where s is the valuation at 2 of the conductor of N_E (computed in Lemma 6).

The rest of the proof follows by applying level lowering for Hilbert modular forms (see [30], [32], [39]), with irreducibility coming from Proposition 8 above. □

The following summarizes part of Step 5 of the modular method as applied to the Frey elliptic curve E.

Proposition 9. *Assume $p \geq 7$ and $p \neq 13$. Then, we have*

$$\overline{\rho}_{E,p} \cong \overline{\rho}_{Z,p}, \tag{7.3}$$

where Z is one of the elliptic curves

$$E_{1,-1}, \qquad E_{1,0}, \qquad or \qquad E_{1,1}.$$

In the case $p = 7$, we have an additional possibility that $\overline{\rho}_{E,p} \cong \overline{\rho}_{g,\mathfrak{p}_7}$ for a Hilbert newform g over $\mathbb{Q}(\sqrt{13})$ of parallel weight 2, trivial character, and level $2^3 w^2$, with field of coefficients $\mathbb{Q}(\sqrt{2})$, and a choice of prime $\mathfrak{p}_7$ above 7 in this field.

If in addition 3 divides $a + b$, then we also have $\overline{\rho}_{E,5} \cong \overline{\rho}_{Z,5}$ for Z as above.

Proof. Using [5], we compute the Hilbert newforms given by the previous lemma and we apply the same method as in Section 4.3 to bound the exponent p. More precisely, for $p \geq 5$, $p \neq 13$ we eliminate all the forms except those corresponding to the three elliptic curves in the statement and another form g which cannot be eliminated for $p = 7$.

Under the assumption $3 \mid a + b$, the previous lemma applies for $p = 5$ and the computations of this proof also, so the last statement follows. □

Remark 7.4. The form g in Proposition 9 cannot be eliminated for the exponent $p = 7$, even using 'many' auxiliary primes $q \neq 2, 13$. This failure appears to have the following explanation.

Let $\sqrt{2} + 3 \in \mathfrak{p}_7$ and $\sqrt{2} + 4 \in \mathfrak{p}'_7$ be the two primes above 7 in $\mathbb{Q}(\sqrt{2})$. By comparing traces of Frobenius mod $\mathfrak{p}'_7$, we promptly check that $\overline{\rho}_{E,7} \not\cong \overline{\rho}_{g,\mathfrak{p}'_7}$. For the prime $\mathfrak{p}_7$, the traces of $\overline{\rho}_{g,\mathfrak{p}_7}$ and $\overline{\rho}_{E_{1,-1},7}$ at Frobenius elements for primes $\mathfrak{q}$ in $\mathbb{Q}(\sqrt{13})$ of norm up to 5000 are the same, which suggests that $\overline{\rho}_{g,\mathfrak{p}_7} \cong \overline{\rho}_{E_{1,-1},7}$. If we could show this congruence, then the form g can be removed and the proof of Theorem 7 below also holds for $p = 7$.

However, to actually have this conclusion, we need to compare traces up to a 'Sturm bound' [15], which unfortunately turns out to be too large to be computationally feasible.

Proof of Theorem 7. Suppose (a, b, c) is a non-trivial primitive solution to (1.4) with $p \geq 5$ and $p \neq 7, 13$. Write $E = E_{a,b}$. From Proposition 9, we know that $\overline{\rho}_{E,p} \cong \overline{\rho}_{Z,p}$, where Z is $E_{1,-1}$, $E_{1,0}$, or $E_{1,1}$.

Again let $\mathfrak{q}_1$ and $\mathfrak{q}_2$ be the primes in $\mathbb{Q}(\sqrt{13})$ dividing 3 with $w + 1 \in \mathfrak{q}_1$. Both $\mathfrak{q}_i$ are primes of good reduction for E and Z; since $3 \mid d$, we have $3 \mid a + b$ and $a_{\mathfrak{q}_1}(E) = -3$ (see the proof of Proposition 8).

On the other hand, for $Z = E_{1,0}$ or $Z = E_{1,1}$, we have $a_{\mathfrak{q}_1}(Z) = -1$. Therefore we have $a_{\mathfrak{q}_1}(E) \not\equiv a_{\mathfrak{q}_1}(Z) \pmod{\mathfrak{p}}$ and we conclude that $\overline{\rho}_{E,p} \cong \overline{\rho}_{E_{1,-1},p}$.

We now prove (A). Let K^+ be the maximal totally real subfield of $\mathbb{Q}(\zeta_{13})$ and let π denote the prime ideal in K^+ above 13. From [22, Proposition 3.1], when

$13 \nmid a+b$ (or equivalently $13 \nmid c$), the curve Z/K^+ has good reduction at π and E/K^+ has bad additive reduction. The conclusion follows from version 2 of the image of inertia argument.

We now prove (B). Consider the base change of $E_{a,b}$ to the field M, where $M = \mathbb{Q}(\sqrt{13})(x,y)$, and (x,y) is a 3-torsion point of $Z = E_{1,-1}$ whose coordinates satisfy:

$$x^4 + (11232w - 56160)x^2 + (-2111616w + 8671104)x + 105131520w - 399499776 = 0,$$
$$y^2 = x^3 + a_4(1,-1)x + a_6(1,-1).$$

The extension M has degree 8 over $\mathbb{Q}(\sqrt{13})$. Let $\mathfrak{q}'$ be the unique prime of M of ramification index 8 above the prime 2 of $\mathbb{Q}(\sqrt{13})$. Then $v_{\mathfrak{q}'}(\Delta(E)) = 32 + 8v_2(a+b) \le 40$.

Consider now $E' = E_{a',b'}$ and suppose that the reduction type of E' is either II or I_0^* and we have that both $v_{\mathfrak{q}'}(a-a')$ and $v_{\mathfrak{q}'}(b-b')$ are $\ge 6\cdot 4 = 24$. By [1, Lemma 2.1], the reduction type of E and E' at $\mathfrak{q}'$ are the same, and hence the conductor exponents at $\mathfrak{q}'$ of E and E' are the same.

In other words, if $(a,b) \equiv (a',b') \pmod{2^3}$, then the conductor exponent at $\mathfrak{q}'$ of $E_{a,b}$ is the same as that of $E_{a',b'}$, provided the reduction type of $E_{a',b'}$ is II or I_0^*. Assuming $4 \nmid a+b$ and using [5], it is thus shown that $E_{a,b}/M$ has conductor exponent ≥ 4 at the prime of M above 2, whereas Z/M has conductor exponent 2 at the prime of M above 2. The conclusion follows from Version 3 of the image of inertia argument. We note that the full 3-division field of Z has degree 48 over $\mathbb{Q}(\sqrt{13})$, whereas our choice of M has degree 8 over $\mathbb{Q}(\sqrt{13})$, making the computation faster. □

7.2. The modular method over the real cubic subfield of $\mathbb{Q}(\zeta_{13})$. In [26], several Frey elliptic curves are attached to equation (1.2); in particular, for $r = 13$ one of them is $E_{a,b}$ from the previous section. In this section we will use another Frey elliptic curve adapted from a construction in [26] defined over a cubic field.

Let K^+ be the maximal (degree 6) totally real subfield of $\mathbb{Q}(\zeta_{13})$ and write K for its cubic subfield. Write $\zeta = \zeta_{13}$ and define

$$A_{x,y} = \alpha(x+y)^2, \quad B_{x,y} = \beta(x^2 + (\zeta+\zeta^{-1})xy + y^2), \quad C_{x,y} = \gamma(x^2 + (\zeta^8+\zeta^{-8})xy + y^2),$$

where

$$\alpha = \zeta^8 + \zeta^{-8} - \zeta - \zeta^{-1}, \qquad \beta = 2 - \zeta^8 - \zeta^{-8}, \qquad \gamma = \zeta + \zeta^{-1} - 2$$

all have norm 13^2. We note that $A_{x,y}$, $B_{x,y}$, $C_{x,y}$ are polynomials with coefficients in K^+ satisfying $A_{x,y} + B_{x,y} + C_{x,y} = 0$.

Let a, b be coprime integers such that $a + b \not\equiv 0$. We consider the Frey elliptic curve given by the short Weierstrass equation

$$F_{a,b} \; : \; y^2 = x^3 + a_4'(a,b)x + a_6'(a,b),$$

where

$$\begin{aligned} a_4'(a,b) &= 3^3 \cdot 13^2 \left(A_{a,b}B_{a,b} + A_{a,b}C_{a,b} + B_{a,b}C_{a,b}\right), \\ a_6'(a,b) &= -3^3 \cdot 13^3 \left(2A_{a,b}^3 + 3A_{a,b}^2 B_{a,b} - 3A_{a,b}B_{a,b}^2 - 2B_{a,b}^3\right). \end{aligned}$$

This curve is (up to a rational isomorphism) the quadratic twist by 13 of the curve defined by equation (13) with $(k_1,k_2) = (1,5)$ in [26].

We then verify that $F_{a,b}$ is defined over K. Its standard invariants are given by the following identities:

$$\begin{aligned} c_4(F_{a,b}) &= -2^4\cdot 3\cdot a_4'(a,b) = -2^4\cdot 3^4\cdot 13^2\left(A_{a,b}B_{a,b}+A_{a,b}C_{a,b}+B_{a,b}C_{a,b}\right),\\ \Delta(F_{a,b}) &= 2^4\cdot 3^{12}\cdot 13^6\left(A_{a,b}B_{a,b}C_{a,b}\right)^2. \end{aligned}$$

We now determine the conductor of $F_{a,b}$. For simplicity, let us write $F = F_{a,b}$ and N_F for its conductor.

Lemma 8. *Let $\mathfrak{q}$ be a prime ideal in K of residual characteristic $\ell \neq 2,3,13$. If F has bad reduction at $\mathfrak{q}$, then $\ell \mid a^{13}+b^{13}$. If in addition $\ell \not\equiv 1 \pmod{13}$, then F has bad reduction at $\mathfrak{q}$ if and only if $\ell \mid a+b$. Moreover, if F has bad reduction at $\mathfrak{q}$, we have*

$$\upsilon_{\mathfrak{q}}(c_4(F)) = 0 \quad \textit{and} \quad \upsilon_{\mathfrak{q}}(\Delta(F)) = \delta\upsilon_\ell(a^{13}+b^{13}),$$

where $\delta = 2$ or 4 according to whether ℓ divides $\phi_{13}(a,b)$ or $a+b$, respectively. In particular, F has bad multiplicative reduction at $\mathfrak{q}$, and hence $\upsilon_{\mathfrak{q}}(N_F) = 1$.

Proof. Recall that $A = A_{a,b}$, $B = B_{a,b}$, $C = C_{a,b}$ are coprime outside 13 as elements of $\mathbb{Q}(\zeta)$. Moreover $(ABC)^2$ divides $13(a+b)^2(a^{13}+b^{13})^2$, and the quotient is coprime to $(ABC)^2$ away from 13 (see Section 2 of [22]). In particular, if F has bad reduction at $\mathfrak{q}$, then ℓ divides $a^{13}+b^{13}$ and $\mathfrak{q} \nmid c_4(F)$. If $\ell \not\equiv 1 \pmod{13}$, the equivalence holds since primes dividing $a^{13}+b^{13}$ not congruent to 1 modulo 13 automatically divide $a+b$ and hence A. Moreover, in that case, we have

$$\upsilon_{\mathfrak{q}}(\Delta(F)) = \upsilon_{\mathfrak{q}}\left((ABC)^2\right) = 4\upsilon_\ell(a+b) + 2\upsilon_\ell(\phi_{13}(a,b)).$$

The result then follows from the fact that $a+b$ and $\phi_{13}(a,b)$ are coprime outside 13. □

We now determine the valuation of N_F at the unique prime ideals above 2, 3, and 13. The two former prime numbers are inert in K, and we simply write 2 and 3 for the unique primes above them in K. We denote by $\mathfrak{q}_{13}$ the prime ideal above 13 in K.

Lemma 9. *We have the following valuations:*

$$\begin{aligned} \upsilon_{\mathfrak{q}_{13}}(N_F) &= \begin{cases} 1 & \textit{if } 13 \mid a+b,\\ 2 & \textit{if } 13 \nmid a+b; \end{cases}\\ \upsilon_3(N_F) &= \begin{cases} 0 & \textit{if } 3 \nmid a+b,\\ 1 & \textit{if } 3 \mid a+b; \end{cases}\\ \upsilon_2(N_F) &= \begin{cases} 0 & \textit{if } \upsilon_2(a+b) = 2,\\ 1 & \textit{if } \upsilon_2(a+b) \geq 3,\\ 3 & \textit{if } ab \equiv 0 \pmod 4,\\ 4 & \textit{if } \upsilon_2(a+b) = 1 \textit{ or } ab \equiv 2 \pmod 4. \end{cases} \end{aligned}$$

Proof. For simplicity, write $A = A_{a,b}$, $B = B_{a,b}$, and $C = C_{a,b}$. Let us denote by π_{13} the unique prime ideal in $\mathbb{Q}(\zeta)$ above 13. We first compute the valuation at π_{13} of $c_4(F)$ and $\Delta(F)$. Using the equalities $AB = \alpha\beta(a+b)^2\left((a+b)^2+\gamma ab\right)$ and $AC = \alpha\beta(a+b)^2\left((a+b)^2-\beta ab\right)$ we obtain

$$\upsilon_{\pi_{13}}(AC) = \upsilon_{\pi_{13}}(AB) = 24\upsilon_{13}(a+b) + \begin{cases} 6 & \text{if } 13 \mid a+b,\\ 4 & \text{if } 13 \nmid a+b. \end{cases}$$

Similarly, using $BC = \beta\gamma\big((a+b)^2 + \gamma ab\big)\big((a+b)^2 - \beta ab\big)$, we have

$$\upsilon_{\pi_{13}}(BC) = \begin{cases} 8 & \text{if } 13 \mid a+b, \\ 4 & \text{if } 13 \nmid a+b. \end{cases}$$

Therefore it follows that we have

$$(\upsilon_{\mathfrak{q}_{13}}(c_4(F)), \upsilon_{\mathfrak{q}_{13}}(\Delta(F))) = \begin{cases} (8, 23 + 12\upsilon_{13}(a+b)) & \text{if } 13 \mid a+b, \\ (\geq 7, 21) & \text{if } 13 \nmid a+b. \end{cases}$$

In particular, the defining model of F is not minimal at $\mathfrak{p}_{13}$ ([38, Tableau I]). After a change of variables, we obtain that if 13 divides $a+b$, then F has bad multiplicative reduction of type I_ν with $\nu = -1+12\upsilon_{13}(a+b)$. Therefore we have $\upsilon_{\mathfrak{q}_{13}}(N_F) = 1$. Otherwise, if 13 divides $a+b$, then F has bad additive reduction at $\mathfrak{q}_{13}$ and $\upsilon_{\mathfrak{q}_{13}}(N_F) = 2$.

We now deal with the prime ideal generated by 3. Neither B nor C is divisible by 3. In particular, if 3 does not divide $a+b$, then $(\upsilon_3(c_4(F)), \upsilon_3(\Delta(F))) = (\geq 4, 12)$ and the defining model of F is not minimal at 3 ([38, Tableau I]). After a change of variables, we obtain that F has good reduction at 3; hence $\upsilon_3(N_F) = 0$. Otherwise, if 3 divides $a+b$, then $(\upsilon_3(c_4(F)), \upsilon_3(\Delta(F))) = (4, 12 + 4\upsilon_3(a+b))$. Therefore, according to [38], after a change of variables, we obtain that F has bad multiplicative reduction of type I_ν with $\nu = 4\upsilon_3(a+b)$. Therefore we have $\upsilon_3(N_F) = 1$.

We finally compute the valuation at 2 of the conductor of F. Neither B nor C is divisible by 2. Therefore, we have

$$\upsilon_2(c_4(F)) = 4 + \upsilon_2(AB + AC + BC) \quad \text{and} \quad \upsilon_2(\Delta(F)) = 4 + 4\upsilon_2(a+b).$$

In particular, if $\upsilon_2(a+b) \geq 3$, then after a change of variables, we find that F has bad multiplicative reduction at 2 of type I_ν with $\nu = -8 + 4\upsilon_2(a+b)$; hence $\upsilon_2(N_F) = 1$. Similarly, if $\upsilon_2(a+b) = 2$, then F has good reduction at 2 and $\upsilon_2(N_F) = 0$.

It remains to deal with the case $\upsilon_2(a+b) \leq 1$. Assume first that 2 does not divide $a+b$. Then we have $ab \equiv 0 \pmod 2$ and $(\upsilon_2(c_4(F)), \upsilon_2(\Delta(F))) = (4, 4)$. Therefore, by [38, Tableau IV], we are in Case 3, 4, or 5 of Tate's classification and $\upsilon_2(N_F) = 4$, 3, or 2, respectively. We have

$$a_4'(a,b) \equiv -(\alpha\beta + \alpha\gamma + \beta\gamma + \alpha\beta\gamma ab) \pmod 4$$

and

$$a_6'(a,b) \equiv 2\alpha^3 + 3\alpha^2\beta - 3\alpha\beta^2 - 2\beta^3 + 3\alpha^2\beta\gamma ab \pmod 4.$$

In particular, we have $a_4'(a,b) \equiv \alpha\beta + \alpha\gamma + \beta\gamma \equiv r^2 \pmod 2$ and $a_6'(a,b) \equiv \alpha\beta\gamma \equiv t^2 \pmod 2$ with $r = t = \zeta + \zeta^{-1} + \zeta^2 + \zeta^{-2} + \zeta^3 + \zeta^{-3} + \zeta^5 + \zeta^{-5}$. According to [38, Proposition 1], one then verifies using the above congruences of $a_4'(a,b)$ and $a_6'(a,b)$ modulo 4 that we are in a case ≥ 4 of Tate's classification if and only if $ab \equiv 0 \pmod 4$. In that case, the congruence class (in the notation of [38]) of $b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 = -a_4'(a,b)^2 + 12ra_6'(a,b) + 6r^2a_4'(a,b) + 3r^4$ modulo 2^3 is independent of a, b such that $ab \equiv 0 \pmod 4$ (since then both $a_4'(a,b) \pmod 4$ and $a_6'(a,b) \pmod 2$ only depend on α, β, and γ). One then verifies that it has valuation 2. According to [38, Proposition 1] we are in Case 4 of Tate's classification; hence $\upsilon_2(N_F) = 3$.

Assume now that $\upsilon_2(a+b) = 1$. Then we have $(\upsilon_2(c_4(F)), \upsilon_2(\Delta(F))) = (4, 8)$ and by [38, Tableau IV], we are in Case 6, 7, or 8 of Tate's classification. We have

$$a_4'(a,b) \equiv \beta\gamma(4\alpha - 3\beta\gamma) \pmod 8 \quad \text{and} \quad a_6'(a,b) \equiv 2(\beta\gamma)^3 \pmod 4.$$

Since the congruence class (in the notation of [38]) of $b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 = -a_4'(a,b)^2 + 12ra_6'(a,b) + 6r^2a_4'(a,b) + 3r^4$ modulo 2^4 depends only on $a_4'(a,b) \pmod 8$, $a_6'(a,b) \pmod 4$, it is independent of a, b such that $v_2(a+b) = 1$. In particular, we can take $(a,b) = (1,1)$. Using Magma we check that the elliptic curve $F_{1,1}$ has conductor exponent 4 at 2. This means that for this specific curve we are in Case 6 of Tate's classification. In particular, the congruence equation in [38, Proposition 3(a)] has no solution for $(a,b) = (1,1)$ and hence for all a, b with $v_2(a+b) = 1$. It follows that $v_2(N_F) = 4$ when $v_2(a+b) = 1$. □

Write $E = E_{a,b}$ and $F = F_{a,b}$. The following illustrates a fundamental difference between the Frey elliptic curves E and F. Note that irreducibility of $\overline{\rho}_{E,p}$ followed by an application of [28, Theorem 3] which makes crucial use of the presence of explicit primes of good reduction of E. This was guaranteed by the fact that all the primes not dividing $2 \cdot 13$ of bad reduction of E must have residual characteristic congruent to 1 mod 13 (see Lemma 5). This is no longer the case for F due to the factor $a + b$ in $\Delta(F)$. Therefore, we can only apply [28, Theorem 2], which guarantees that $\overline{\rho}_{F,p}$ is irreducible when $p > (1 + 3^{18})^2$. This bound is insufficient for our purposes.

We shall establish here a much better irreducibility result, dealing first with the case $p = 5$ in full generality.

Lemma 10. *The representation $\overline{\rho}_{F,5}$ is irreducible.*

Proof. We proceed using explicit equations as in [17, Theorem 7]. Let j_F denote the j-invariant of F. Then

$$\begin{aligned} j_F - 1728 &= \eta G(a,b)^2/H(a,b)^2 \\ &= 13(\nu G(a,b)/H(a,b))^2, \end{aligned}$$

where G, H are degree-12 homogeneous monic polynomials in two variables with coefficients in K, and $\eta, \nu \in K$ [5]. If $\overline{\rho}_{F,5}$ is reducible, that is, F has a 5-isogeny over K, then we must have that

$$j_F - 1728 = \frac{(t^2 + 4st - s^2)^2(t^2 + 22st + 125s^2)}{s^5 t},$$

for some $u = t/s \in \mathbb{P}^1(K)$, following the argument in [5]. Thus, we obtain a K-rational point (u, v) on the elliptic curve

$$D : 13Y^2 = (X^2 + 22X + 125)X,$$

where

$$u = t/s, \qquad v = \nu \frac{G(a,b)}{H(a,b)} \frac{u}{u^2 + 4u - 1}.$$

The elliptic curve D has rank 1 over K and over $\mathbb{Q}$ and $D_{tors}(K) = D_{tors}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ [5]. This implies that $D(K) = D(\mathbb{Q})$; i.e., every K-rational point of D is in fact $\mathbb{Q}$-rational. Thus,

$$\nu \frac{G(a,b)}{H(a,b)} \in \mathbb{Q},$$

which in turn implies that $j_F - 1728 \in \mathbb{P}^1(\mathbb{Q})$. Put $N = \eta G(a,b)^2$, $M = H(a,b)^2$, and let σ be a non-trivial automorphism of K. Write $R = N\sigma(M)\sigma^2(M) = A_0(a,b) + A_1(a,b)z + A_2(a,b)z^2$ where $K = \mathbb{Q}(z)$ and A_0, A_1, A_2 are degree 12 homogeneous polynomials in two variables with coefficients in $\mathbb{Q}$. Since $j_F - 1728 \in \mathbb{P}^1(\mathbb{Q})$, then

R is rational, and this implies that $A_1(x,1)$ and $A_2(x,1)$ must have a common root. It can be verified that this is not the case for $a/b \in \mathbb{P}^1(\mathbb{Q})$, except for $a/b = -1$ [5]. □

Remark 7.5. The following example shows that in the previous proof of Lemma 10 it is essential to be working with j-invariants arising from the Frey elliptic curve F. Consider the elliptic curve over $\mathbb{Q}$ defined by

$$y^2 + (1+a)xy + ay = x^3 + ax^2, \qquad a = \frac{-10933}{144},$$

which has 10-torsion over $\mathbb{Q}$ and acquires full 2-torsion over $\mathbb{Q}(\sqrt{13})$. In particular, it also has 10-torsion over K and a $C_2 \times C_{10}$ torsion group over K^+.

Theorem 8. *Assume $p \geq 7$ and $p \neq 13$. If either $13 \mid a+b$ or $13 \nmid a+b$ and $p \neq 17, 37$, then $\overline{\rho}_{F,p}$ is irreducible.*

Proof. Suppose $\overline{\rho}_{F,p}$ is reducible; that is,

$$\overline{\rho}_{F,p} \sim \begin{pmatrix} \theta & \star \\ 0 & \theta' \end{pmatrix} \quad \text{with} \quad \theta, \theta' : G_K \to \mathbb{F}_p^* \quad \text{satisfying} \quad \theta\theta' = \chi_p.$$

We note that $K = \mathbb{Q}(z)$, where $z^3 + z^2 - 4z + 1 = 0$. According to the notation of [28, Theorem 1] we set $\epsilon_1 = z$ and $\epsilon_2 = 1 - z$, observe that the unit group of K is generated by $\{-1, \epsilon_1, \epsilon_2\}$, and compute $B = 5^3 \cdot 13$. Thus from the first paragraph of the proof of [28, Theorem 1] we conclude that for $p = 11$ and $p \geq 17$ exactly one of θ, θ' ramifies at p. Since 7 is inert in K and F is semistable at 7, it follows from [33, Lemma 1] also that only one of θ, θ' ramifies at $p = 7$.

The characters θ and θ' ramify only at p and additive primes of F; the latter are $\mathfrak{q}_{13}$ and 2 when $13 \nmid a+b$ and $4 \nmid a+b$ respectively (see Lemma 9). Furthermore, at an additive prime $\mathfrak{q}$ both θ, θ' have conductor exponent equal to $\upsilon_{\mathfrak{q}}(N_F)/2$; in particular, $\upsilon_2(N_F) \neq 3$.

Replacing F by a p-isogenous curve we can assume θ is unramified at p. Therefore, the possible conductors for θ are $2^s \mathfrak{q}_{13}^t$ with $s \in \{0, 2\}$ and $t \in \{0, 1\}$. Let ∞_1, ∞_2, and ∞_3 be the real places of K. The field K has narrow class number 1 and the Ray class groups for the modulus $2^2\infty_1\infty_2\infty_3$, $\mathfrak{q}_{13}\infty_1\infty_2\infty_3$, and $2^2\mathfrak{q}_{13}\infty_1\infty_2\infty_3$ are isomorphic to

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z}, \quad \text{and} \quad \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z},$$

respectively; hence θ has order $n = 1, 2$, or 4. Moreover the case $n = 4$ only occurs when θ ramifies at $\mathfrak{q}_{13}$. In particular, if $13 \mid a+b$, then F is semistable at $\mathfrak{q}_{13}$ and we have $n = 1$ or 2.

Suppose $n = 1, 2$. Thus either F or a quadratic twist F' of F has a p-torsion point defined over K. Note that F has full 2-torsion over K^+ which is a quadratic extension of K; hence it has at least one 2-torsion point over K (namely, the point with x-coordinate $-3 \cdot 13(A_{a,b} + 2B_{a,b})$). Thus, the quadratic twist F' also has a 2-torsion point over K, and we conclude that the K-torsion subgroup of F or F' has order divisible by $2p$ with $p \geq 7$. From [10, Theorem 5], we see that this is impossible.

In particular, this proves the result for all primes $p \equiv 3 \pmod 4$, because $n = 4$ does not divide the order of $\mathbb{F}_p^*$.

Suppose $n = 4$. Since K^+ is the field fixed by θ^2 (note θ^2 has conductor $\mathfrak{q}_{13}$) θ has order 2 over K^+. After a quadratic twist, now over K^+, we conclude that F has a p-torsion point defined over K^+. From [21] we see this is possible only for $p \le 19$ and $p = 37$. We conclude that $\overline{\rho}_{F,p}$ is irreducible for all $p \ge 7$ such that $p \ne 13, 17, 37$ (after discarding the primes $p \equiv 3 \pmod 4$). □

From Lemma 9 we know that $F_{a,b}$ is semistable at all primes dividing 3 in K. Thus, from [26, Theorem 6.3], it follows that $F_{a,b}$ is modular.

We now wish to use the Frey elliptic curve $F_{a,b}$ to solve our Fermat equations. Suppose that there exists an integer c such that (a,b,c) is a non-trivial primitive solution to (1.4) with $p \ge 5$. Write again $F = F_{a,b}$.

From the conductor computations coming from Lemmas 8 and 9, irreducibility results from Lemma 10 and Theorem 8, and level lowering again, we obtain the following lemma.

Lemma 11. *Assume $p \ge 5$, $p \not\equiv 13$. If $13 \nmid a+b$, assume further $p \not\equiv 17, 37$. Then, there exists a prime $\mathfrak{p}$ in $\overline{\mathbb{Q}}$ above p such that*

$$\overline{\rho}_{F,p} \cong \overline{\rho}_{f,\mathfrak{p}}, \tag{7.6}$$

where f is a Hilbert newform over K of parallel weight 2, trivial character, and level

$$N_f = 2^{\alpha_2} \cdot 3^{\alpha_3} \cdot \mathfrak{q}_{13}^{\alpha_{13}}.$$

Here, $\alpha_2 \in \{0,1,3,4\}$, $\alpha_3 \in \{0,1\}$, $\alpha_{13} \in \{1,2\}$ is the valuation (computed in Lemma 9) at 2, 3, and $\mathfrak{q}_{13}$ of N_F respectively.

We now comment on the sizes of the spaces occurring in Lemma 11. With `Magma`, we compute respectively the dimensions of the cuspidal and its new subspace at each level of the form $2^s \cdot 3 \cdot \mathfrak{q}_{13}^t$ with $s \in \{0,1,3,4\}$ and $t \in \{1,2\}$. For $t = 1$ and $t = 2$, we obtain

$s = 0$:	$33, 27$;	and	$s = 0$:	$425, 334$;
$s = 1$:	$295, 181$;		$s = 1$:	$3823, 2353$;
$s = 3$:	$18817, 11466$;		$s = 3$:	$244609, 148101$;
$s = 4$:	$150929, 91728$;		$s = 4$:	$1956865, 1184820$.

We see that for $s = 0$ and $s = 1$, the computations of the newforms are within reach of current implementations (indeed, we have already computed a larger space when studying the case of $r = 5$), but for $s = 3$ and $s = 4$, the dimensions are totally out of reach. Using the multi-Frey technique, we are able to prove Theorem 2 by computing only in the case $(s,t) = (1,1)$ (that is, in level $2 \cdot 3 \cdot \mathfrak{q}_{13}$).

7.3. **Proof of Theorem 2.** The case $p = 2$ follows from [2, Theorem 1.1], and the case $p = 3$ follows from [3, Theorem 1.5]. For exponent $p = 13$ the result follows from Theorem 2 in [42, Section 4.3].

Suppose (a,b,c) is a non-trivial primitive solution to (1.4) with $p \ge 5$, $p \ne 7, 13$. From Theorem 7 we can assume that $4 \mid a+b$ and $13 \mid a+b$. Moreover, we have $\upsilon_2(a+b) = \upsilon_2(3c^p) \ge 3$. Write $F = F_{a,b}$. Thanks to our assumptions, Lemma 11 applies with no further restrictions. In particular, we have that $\overline{\rho}_{F,p} \cong \overline{\rho}_{f,\mathfrak{p}}$, where f is a Hilbert newform over K of parallel weight 2, trivial character, and level $N_f = 2 \cdot 3 \cdot \mathfrak{q}_{13}$. (Note that the multi-Frey technique is implicit in this step because the proof of Theorem 7 uses the Frey elliptic curve E.)

The dimension of the new cuspidal subspace is 181. Using [5], we compute all the newforms f in these spaces and bound the exponent using the primes in K above rational primes $q = 5, 7, 11, 17, 31$ as usual using the norm of the difference between traces. This suffices to eliminate all but 4, 2 forms corresponding to the exponents $p = 5, 11$, respectively.

For the remaining forms, we use the following refined elimination technique [5]. For each form, choosing a $q \neq 2, 3, 13$ and $q \not\equiv 1 \pmod{13}$, we obtain that if $\overline{\rho}_{F,p} \cong \overline{\rho}_{f,\mathfrak{p}}$ for some prime $\mathfrak{p} \mid p$ in the field of coefficients of f, then (by Lemma 8):

(i) either $q \nmid a+b$ and then for all $\mathfrak{q}$ above q, we have $a_{\mathfrak{q}}(f) \equiv a_{\mathfrak{q}}(F_{a,b}) \pmod{\mathfrak{p}}$

(ii) or $q \mid a+b$ and then for all $\mathfrak{q}$ above q, we have $a_{\mathfrak{q}}(f) \equiv \pm(N(\mathfrak{q})+1) \pmod{\mathfrak{p}}$.

By computing $a_{\mathfrak{q}}(F_{x,y})$ for each $\mathfrak{q} \mid q$ and all $x, y \in \{0, \ldots, q-1\}$ not both zero, we eliminate each form by checking that neither of the above congruences holds for that form.

Acknowledgments

We thank Christophe Breuil for discussions concerning Proposition 7. We also thank Peter Bruin for helpful conversations regarding Remark 7.5, Maarten Derickx and Michael Stoll for a conversation about [21], and Enrique Gonzalez Jimenez for helpful suggestions. We are grateful to the referee for a careful reading and helpful remarks.

References

[1] Michael A. Bennett, Imin Chen, Sander R. Dahmen, and Soroosh Yazdani, *On the equation* $a^3 + b^{3n} = c^2$, Acta Arith. **163** (2014), no. 4, 327–343, DOI 10.4064/aa163-4-3. MR3217670

[2] Michael A. Bennett and Chris M. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math. **56** (2004), no. 1, 23–54, DOI 10.4153/CJM-2004-002-2. MR2031121

[3] Michael A. Bennett, Vinayak Vatsal, and Soroosh Yazdani, *Ternary Diophantine equations of signature* $(p, p, 3)$, Compos. Math. **140** (2004), no. 6, 1399–1416, DOI 10.1112/S0010437X04000983. MR2098394

[4] Nicolas Billerey, *Équations de Fermat de type* $(5, 5, p)$ (French, with French summary), Bull. Austral. Math. Soc. **76** (2007), no. 2, 161–194, DOI 10.1017/S0004972700039575. MR2353205

[5] Nicolas Billerey, Imin Chen, Luis Dieulefait, and Nuno Freitas, supporting `Magma` program files for this paper, `http://people.math.sfu.ca/~ichen/xrrdp`.

[6] Nicolas Billerey and Luis V. Dieulefait, *Solving Fermat-type equations* $x^5 + y^5 = dz^p$, Math. Comp. **79** (2010), no. 269, 535–544, DOI 10.1090/S0025-5718-09-02294-7. MR2552239

[7] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language,* Computational algebra and number theory (London, 1993), J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. MR1484478

[8] Christophe Breuil, *Sur quelques représentations modulaires et p-adiques de* $\mathrm{GL}_2(\mathbf{Q}_p)$*. II* (French, with French summary), J. Inst. Math. Jussieu **2** (2003), no. 1, 23–58, DOI 10.1017/S1474748003000021. MR1955206

[9] Christophe Breuil and Ariane Mézard, *Multiplicités modulaires et représentations de* $\mathrm{GL}_2(\mathbf{Z}_p)$ *et de* $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ *en* $l = p$ (French, with English and French summaries), with an appendix by Guy Henniart, Duke Math. J. **115** (2002), no. 2, 205–310, DOI 10.1215/S0012-7094-02-11522-1. MR1944572

[10] Peter Bruin and Filip Najman, *A criterion to rule out torsion groups for elliptic curves over number fields*, Res. Number Theory **2** (2016), Art. 3, 13, DOI 10.1007/s40993-015-0031-5. MR3501016

[11] Yann Bugeaud, Florian Luca, Maurice Mignotte, and Samir Siksek, *Almost powers in the Lucas sequence* (English, with English and French summaries), J. Théor. Nombres Bordeaux **20** (2008), no. 3, 555–600. MR2523309

[12] Yann Bugeaud, Maurice Mignotte, and Samir Siksek, *Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers*, Ann. of Math. (2) **163** (2006), no. 3, 969–1018, DOI 10.4007/annals.2006.163.969. MR2215137

[13] Yann Bugeaud, Maurice Mignotte, and Samir Siksek, *Classical and modular approaches to exponential Diophantine equations. II. The Lebesgue-Nagell equation*, Compos. Math. **142** (2006), no. 1, 31–62, DOI 10.1112/S0010437X05001739. MR2196761

[14] Yann Bugeaud, Maurice Mignotte, and Samir Siksek, *A multi-Frey approach to some multi-parameter families of Diophantine equations*, Canad. J. Math. **60** (2008), no. 3, 491–519, DOI 10.4153/CJM-2008-024-9. MR2414954

[15] Jose Ignacio Burgos Gil and Ariel Pacetti, *Hecke and Sturm bounds for Hilbert modular forms over real quadratic fields*, Math. Comp. **86** (2017), no. 306, 1949–1978, DOI 10.1090/mcom/3187. MR3626544

[16] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, Cambridge, 1997. MR1628193

[17] Sander R. Dahmen, *A refined modular approach to the Diophantine equation* $x^2+y^{2n}=z^3$, Int. J. Number Theory **7** (2011), no. 5, 1303–1316, DOI 10.1142/S1793042111004472. MR2825973

[18] Sander R. Dahmen and Samir Siksek, *Perfect powers expressible as sums of two fifth or seventh powers*, Acta Arith. **164** (2014), no. 1, 65–100, DOI 10.4064/aa164-1-5. MR3223319

[19] Henri Darmon and Andrew Granville, *On the equations* $z^m = F(x,y)$ *and* $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. **27** (1995), no. 6, 513–543, DOI 10.1112/blms/27.6.513. MR1348707

[20] Henri Darmon and Loïc Merel, *Winding quotients and some variants of Fermat's last theorem*, J. Reine Angew. Math. **490** (1997), 81–100. MR1468926

[21] Martin Derickx, Sheldon Kamienny, William Stein, and Michael Stoll, *Torsion points on elliptic curves over number fields of small degree*, arXiv e-prints, July 2017.

[22] Luis Dieulefait and Nuno Freitas, *Fermat-type equations of signature* $(13,13,p)$ *via Hilbert cuspforms*, Math. Ann. **357** (2013), no. 3, 987–1004, DOI 10.1007/s00208-013-0920-7. MR3118622

[23] Luis Dieulefait and Nuno Freitas, *The Fermat-type equations* $x^5 + y^5 = 2z^p$ *or* $3z^p$ *solved through* $\mathbb{Q}$*-curves*, Math. Comp. **83** (2014), no. 286, 917–933, DOI 10.1090/S0025-5718-2013-02731-7. MR3143698

[24] G. Lejeune Dirichlet, *Mémoire sur l'impossibilité de quelques équations indéterminées du cinquième degré* (French), J. Reine Angew. Math. **3** (1828), 354–375, DOI 10.1515/crll.1828.3.354. MR1577706

[25] Jordan S. Ellenberg, *Galois representations attached to* $\mathbb{Q}$*-curves and the generalized Fermat equation* $A^4 + B^2 = C^p$, Amer. J. Math. **126** (2004), no. 4, 763–787. MR2075481

[26] Nuno Freitas, *Recipes to Fermat-type equations of the form* $x^r + y^r = Cz^p$, Math. Z. **279** (2015), no. 3-4, 605–639, DOI 10.1007/s00209-014-1384-5. MR3318242

[27] Nuno Freitas, Bao V. Le Hung, and Samir Siksek, *Elliptic curves over real quadratic fields are modular*, Invent. Math. **201** (2015), no. 1, 159–206, DOI 10.1007/s00222-014-0550-z. MR3359051

[28] Nuno Freitas and Samir Siksek, *Criteria for irreducibility of* $\operatorname{mod} p$ *representations of Frey curves* (English, with English and French summaries), J. Théor. Nombres Bordeaux **27** (2015), no. 1, 67–76. MR3346965

[29] Nuno Freitas and Samir Siksek, *Fermat's last theorem over some small real quadratic fields*, Algebra Number Theory **9** (2015), no. 4, 875–895, DOI 10.2140/ant.2015.9.875. MR3352822

[30] Kazuhiro Fujiwara, *Level optimization in the totally real case*, arXiv mathematics e-prints, February 2006.

[31] Frazer Jarvis, *Level lowering for modular mod* l *representations over totally real fields*, Math. Ann. **313** (1999), no. 1, 141–160, DOI 10.1007/s002080050255. MR1666809

[32] Frazer Jarvis, *Correspondences on Shimura curves and Mazur's principle at* p, Pacific J. Math. **213** (2004), no. 2, 267–280, DOI 10.2140/pjm.2004.213.267. MR2036920

[33] Alain Kraus, *Courbes elliptiques semi-stables et corps quadratiques* (French, with French summary), J. Number Theory **60** (1996), no. 2, 245–253, DOI 10.1006/jnth.1996.0122. MR1412962

[34] Alain Kraus, *Majorations effectives pour l'équation de Fermat généralisée* (French, with French summary), Canad. J. Math. **49** (1997), no. 6, 1139–1161, DOI 10.4153/CJM-1997-056-2. MR1611640

[35] Alain Kraus, *Sur l'équation* $a^3 + b^3 = c^p$ (French, with English and French summaries), Experiment. Math. **7** (1998), no. 1, 1–13. MR1618290

[36] A. Kraus and J. Oesterlé, *Sur une question de B. Mazur* (French), Math. Ann. **293** (1992), no. 2, 259–275, DOI 10.1007/BF01444715. MR1166121

[37] The LMFDB Collaboration, *The L-functions and modular forms database*, http://www.lmfdb.org, 2013.

[38] Ioannis Papadopoulos, *Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle* 2 *et* 3 (French, with French summary), J. Number Theory **44** (1993), no. 2, 119–152, DOI 10.1006/jnth.1993.1040. MR1225948

[39] Ali Rajaei, *On the levels of mod l Hilbert modular forms*, J. Reine Angew. Math. **537** (2001), 33–65, DOI 10.1515/crll.2001.058. MR1856257

[40] Kenneth A. Ribet, *On the equation $a^p + 2^\alpha b^p + c^p = 0$*, Acta Arith. **79** (1997), no. 1, 7–16, DOI 10.4064/aa-79-1-7-16. MR1438112

[41] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques* (French), Invent. Math. **15** (1972), no. 4, 259–331, DOI 10.1007/BF01405086. MR0387283

[42] Jean-Pierre Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ (French), Duke Math. J. **54** (1987), no. 1, 179–230, DOI 10.1215/S0012-7094-87-05413-5. MR885783

[43] Andrew Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551, DOI 10.2307/2118559. MR1333035

Université Clermont Auvergne, CNRS, LMBP, F-63000 Clermont-Ferrand, France
Email address: nicolas.billerey@uca.fr

Department of Mathematics, Simon Fraser University, Burnaby, British Columbia V5A 1S6, Canada
Email address: ichen@sfu.ca

Departament d'Algebra i Geometria, Universitat de Barcelona, G.V. de les Corts Catalanes 585, 08007 Barcelona, Spain
Email address: ldieulefait@ub.edu

Department of Mathematics, University of British Columbia, Vancouver, British Columbia V6T 1Z2 Canada
Email address: nunobfreitas@gmail.com