SOME EXTENSIONS OF THE MODULAR METHOD AND FERMAT EQUATIONS OF SIGNATURE $(13, 13, n)$

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

ABSTRACT. We provide several extensions of the modular method which were motivated by the problem of completing previous work to prove that, for any integer $n \geq 2$, the equation

$$x^{13} + y^{13} = 3z^n$$

has no non-trivial primitive solutions. In particular, we present four elimination techniques which are based on: (1) establishing reducibility of certain residual Galois representations over a totally real field; (2) generalizing image of inertia arguments to the setting of abelian surfaces; (3) establishing congruences of Hilbert modular forms without the use of often impractical Sturm bounds; and (4) a unit sieve argument which combines information from classical descent and the modular method.

The extensions are of broader applicability and provide further evidence that it is possible to obtain a complete resolution of a family of generalized Fermat equations by remaining within the framework of the modular method. As a further illustration of this, we complete a theorem of Anni-Siksek to show that, for $\ell, m \geq 5$, the only primitive solutions to the equation $x^{2\ell} + y^{2m} = z^{13}$ are trivial.

1. Introduction

In [4], it was shown that it is possible to get an optimal result for a family of generalized Fermat equations, specifically $x^5 + y^5 = 3z^n$ for $n \geq 2$ an integer, using a refined modular method with the multi-Frey approach over totally real fields. These methods were also applied to the equation

$$(1.1) \qquad\qquad x^{13} + y^{13} = 3z^p,$$

where p is prime, but failed for $p = 7$; this failure is due to the presence of five specific Hilbert modular forms after level lowering which the authors were not able to eliminate. Four of the obstructing forms are newforms of weight 2 defined over the real cubic subfield of $\mathbb{Q}(\zeta_{13})$, the cyclotomic field of 13th root of unity, whose level is the unique ideal of norm $2808 = 2^3 \cdot 3^3 \cdot 13$. The remaining one, which is the most relevant to us, is denoted by g; it is a newform defined over $\mathbb{Q}(\sqrt{13})$ of parallel weight 2, level $\mathfrak{N} = (2^3 13)$ and field of coefficients $\mathbb{Q}(\sqrt{2})$ appearing in [4, Proposition 9].

The techniques in this paper provide extensions of the modular method which were initially motivated by the problem of eliminating these five obstructing forms, but are of broader applicability. In particular, we successfully treat the remaining case $p = 7$ of equation (1.1).

Our first step is to reduce the resolution of (1.1) for $p = 7$ to the problem of dealing with the form g. For this, we consider the Frey curve $F = F_{a,b}$ defined in [4, §7.2]. The refined elimination technique from [4, §7.3] applied to F shows that the obstruction to the modular method arises from the four obstructing newforms defined over the real cubic subfield of $\mathbb{Q}(\zeta_{13})$, with level of norm 2808. We are then able to show that each of these forms has a reducible mod $\mathfrak{p}$ representation for some prime $\mathfrak{p} \mid 7$ (see Proposition 3.2). Since the mod 7 representation attached to F is irreducible by assumption, this allows us to discard these four forms (see Sections 2 and 4). However, establishing the reducibility property for the four obstructing forms requires a bit of care since the usual approach, which involves using the Sturm bound, is not computationally feasible in the setting of Hilbert modular forms.

The remaining obstructing form g arises for the Frey curve $E = E_{a,b}$ defined in [4, §7.1], more specifically, when trying to prove [4, Theorem 7] for $p = 7$. We will introduce three different methods for discarding this form.

The first method eliminates g by extending an 'image of inertia argument' to the setting of abelian surfaces. For this, we will combine modularity of an abelian surface with the study of the inertial types of g at suitable primes.

The second method is to show that g is congruent modulo 7 to the Hilbert newform associated to the Frey curve corresponding to the trivial solution $(1, -1, 0)$; see also [4, Remark 7.4]. In general, the proof of such congruences requires computing Hecke eigenvalues up to the Sturm bound, which is often not practical for Hilbert modular forms, as is the case in our situation. Instead, we exploit a multiplicity one phenomenon for the residual Galois representations attached to the Hilbert newforms in our situation, to establish the desired congruence.

The third method is based on combining the study of units in classical descent with local information coming from the modular method together with restrictions on the solutions coming from the multi-Frey approach in [4].

As a consequence, we obtain a complete resolution of the generalized Fermat equations in (1.1). More precisely, we establish the following result.

Theorem 1.1. *For all integers $n \geq 2$, there are no integer solutions (a, b, c) to the equation*
$$x^{13} + y^{13} = 3z^n$$
such that $abc \neq 0$ and $\gcd(a, b, c) = 1$.

An integer solution (a, b, c) to (1.1) is said to be a primitive solution if $\gcd(a, b, c) = 1$, and trivial if $abc = 0$.

It is natural to wonder whether one could use Chabauty methods to solve (1.1) for $p = 7$ by determining the rational points on the hyperelliptic curves associated with (1.1) from the constructions in [13]. This would necessitate computing the 2-Selmer groups of Jacobians of genus 3 hyperelliptic curves of the form $y^2 = x^7 + a$, where a belongs to the maximal totally real sextic subfield F of the field $\mathbb{Q}(\zeta_{13})$. Because some values of a which need to be treated are not seventh powers in F, such calculations would require working over the extensions $F(\sqrt[7]{a})$

which are of absolute degree 42. Even under GRH, this would be extremely challenging with current methods. Moreover, it would only lead to a conditional resolution of (1.1).

The computations required to support the proof of our theorems were performed using Magma [5], mainly the Hilbert Modular Forms Package (see [16, 28]). The program and output transcript files are available at [3] (see Read_Me.txt for a description of the files). The Dokchister-Doris package for computing the conductor of genus 2 curves is available at [22].

2. THE ELIMINATION STEP AWAY FROM REDUCIBLE PRIMES

In this section, we recall the elimination step of the modular method and discuss ways in which it can fail to yield a contradiction. The discussion will center on equation (1.1) for convenience, but the same principles apply more generally.

Let (a, b, c) be a primitive solution to (1.1) and $E_{a,b}/K$ a Frey curve attached to it, where K is a totally real number field. Also, let $\overline{\rho}_{E_{a,b},p}$ be the mod p representation attached to $E_{a,b}$. By assumption $\overline{\rho}_{E_{a,b},p}$ is an irreducible representation which is modular. An application of standard results on level lowering implies that there is a Hilbert newform f of level $\mathfrak{N}$ and weight 2, with field of coefficients $\mathbb{Q}_f$, such that

$$(2.1) \qquad \overline{\rho}_{E_{a,b},p} \simeq \overline{\rho}_{f,\mathfrak{p}}$$

where $\mathfrak{p} \mid p$ is a prime in $\mathbb{Q}_f$ and $\overline{\rho}_{f,\mathfrak{p}}$ the mod $\mathfrak{p}$ representation attached to f. In practice, the level $\mathfrak{N}$ is a concrete ideal dividing the conductor of $E_{a,b}$, independent of (a, b, c) and of 'small' norm. So the new subspace $S_2(\mathfrak{N})^{\mathrm{new}}$ of Hilbert cusp forms of level $\mathfrak{N}$, weight 2 and trivial character is accessible via the Hilbert Modular Forms package in Magma [5].

Given $f \in S_2(\mathfrak{N})^{\mathrm{new}}$, a candidate newform, a crucial step in the modular method consists of showing that the isomorphism (2.1) does not occur for *any* prime $\mathfrak{p}$ of $\mathbb{Q}_f$ above p. We say that we *have eliminated the form f for the exponent p* if we can successfully complete that step. By eliminating all the newforms in $S_2(\mathfrak{N})^{\mathrm{new}}$, we obtain a contradiction to the fact that $\overline{\rho}_{E_{a,b},p}$ is modular, thus solving (1.1) for the exponent p.

By taking traces at Frobenius elements on both sides of (2.1) one gets

$$(2.2) \qquad a_{\mathfrak{q}}(E_{a,b}) \equiv a_{\mathfrak{q}}(f) \pmod{\mathfrak{p}} \text{ for all primes } \mathfrak{q} \nmid p \cdot \mathrm{cond}(E_{a,b}),$$

where $a_{\mathfrak{q}}(f)$ is the Hecke eigenvalue of f at $\mathfrak{q}$, and $a_{\mathfrak{q}}(E_{a,b})$ the trace of Frobenius of E at $\mathfrak{q}$.

Let $q \neq p$ be a rational prime coprime to the level $\mathfrak{N}$ of f. Suppose that $E_{a,b}$ has good reduction at each prime ideal $\mathfrak{q}$ dividing q in K, and define the quantity

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

Note that (2.2) implies the exponent p divides $qB_q(E_{a,b}, f)$. Suppose instead that $E_{a,b}$ has multiplicative reduction at a prime $\mathfrak{q} \mid q$. Then, the isomorphism (2.1) implies that the form f satisfies level raising conditions, hence we have the congruence:

$$(2.3) \qquad a_\mathfrak{q}(f) \equiv \pm(\mathrm{Norm}(\mathfrak{q}) + 1) \pmod{\mathfrak{p}}.$$

In the elimination step, we find rational primes q such that, for all a, b mod q not both zero, the Frey curve $E_{a,b}$ has either good reduction at all $\mathfrak{q} \mid q$ or multiplicative reduction at all $\mathfrak{q} \mid q$. Then, for a newform $f \in S_2(\mathfrak{N})^{\mathrm{new}}$, we define

$$A_q(f) := q \prod_{(0,0) \neq (a,b) \in \mathbb{F}_q^2} B_q(E_{a,b}, f) \cdot \prod_{\mathfrak{q} \mid q} \mathrm{Norm}(a_\mathfrak{q}(f)^2 - (\mathrm{Norm}(\mathfrak{q}) + 1)^2),$$

where the first part accounts for the possibility of E having good reduction at q whilst the second product for the case of multiplicative reduction. The quantity $A_q(f)$ is independent of p, so once we find one prime q such that $A_q(f) \neq 0$, we have eliminated f for large p. For most f, trying a few auxiliary primes often suffices to find such a q. This is then enough to eliminate f for all exponents $p \nmid A_q(f)$. Furthermore, by using several primes $q_1, \ldots, q_s$, we eliminate f for all $p \nmid \gcd(A_{q_1}(f), \ldots, A_{q_s}(f))$.

For a given newform f, the elimination step leads to a set of primes P_f, which cannot be excluded by this process. This set usually consists of a few small primes, but it can also be empty or equal to the set of the prime numbers; the latter only occurs when all the auxiliary primes we tried gave $A_q(f) = 0$.

In [4, §7.3], four of the authors introduced the following refined elimination technique to deal with the remaining primes in P_f. The key observation of this refinement is that (2.2) and (2.3) imply $p \mid A_q(f)$ but the converse is not true. So, for the primes $p \in P_f$, they test for the congruences (2.2) and (2.3), which result from the isomorphism (2.1), directly. In other words, for each prime $\mathfrak{p} \mid p$ in $\mathbb{Q}_f$, they check the following congruences by direct computations:

(i) for all $\mathfrak{q} \mid q$ of good reduction for $E_{a,b}$ we have $a_\mathfrak{q}(f) \equiv a_\mathfrak{q}(E_{a,b}) \pmod{\mathfrak{p}}$;
(ii) for all $\mathfrak{q} \mid q$ of multiplicative reduction for $E_{a,b}$, we have $a_\mathfrak{q}(f) \equiv \pm(\mathrm{Norm}(\mathfrak{q}) + 1) \pmod{\mathfrak{p}}$;

This can be done as long as we can factor the primes $p \in P_f$ in the field $\mathbb{Q}_f$. If (i) and (ii) fail for $\mathfrak{p} \mid p$ then we have eliminated the pair $(f, \mathfrak{p})$. Excluding all such pairs then eliminates f for the exponent p. In [4, §7.3], this refinement allowed for the resolution of (1.1) for $p = 5, 11$.

Let us now discuss one way in which the argument above can fail. Suppose for some form f and a prime $\mathfrak{p}_0 \mid p \in P_f$ in $\mathbb{Q}_f$, the mod $\mathfrak{p}_0$ representation is reducible and, moreover, it satisfies $\overline{\rho}_{f,\mathfrak{p}_0}^{ss} \simeq \chi_p \oplus 1$, where χ_p is the mod p cyclotomic character. Then, this form satisfies $a_\mathfrak{q}(f) \equiv \mathrm{Norm}(\mathfrak{q}) + 1 \pmod{\mathfrak{p}_0}$, and therefore congruence (ii) holds with $\mathfrak{p} = \mathfrak{p}_0$. Thus we are unable to eliminate the pair $(f, \mathfrak{p}_0)$ using the refined elimination technique.

However, we note that the isomorphism (2.1) was obtained via level lowering theorems, which require the representations involved to be residually irreducible. So, in testing for the congruences (i) and (ii), we only need to consider those pairs $(f, \mathfrak{p})$, where $\mathfrak{p} \mid p$ is a prime in $\mathbb{Q}_f$ such that $\overline{\rho}_{f,\mathfrak{p}}$ is irreducible. This allows us to circumvent the reducibility issue raised in the previous paragraph. We will see in Section 3 that one of the reasons why equation (1.1) does not follow directly from the methods in [4], for $p = 7$, is the presence of reducible pairs $(f, \mathfrak{p}_0)$.

4

We note that this idea of avoiding reducible primes $\mathfrak{p}_0$ appeared in the work of Bugeaud-Mignotte-Siksek [7], where they work with classical forms over $\mathbb{Q}$. In that setting, a practical Sturm bound is available, allowing them to prove isomorphism of the form $\overline{\rho}_{f,\mathfrak{p}_0}^{ss} \simeq \chi_p \oplus 1$. For our purpose, due to the lack of practical Sturm bounds for Hilbert modular forms, we will establish the existence of our reducible pairs $(f, \mathfrak{p}_0)$ using base change arguments.

3. A REDUCIBILITY RESULT FOR HILBERT MODULAR FORMS

In this section, we let $K = \mathbb{Q}(b)$ be the real cubic subfield of $\mathbb{Q}(\zeta_{13})$, where $b^3 + b^2 - 4b + 1 = 0$. We let $\mathfrak{q}_{13}$ be the unique ramified prime in K, which lies above 13. We note that 2 and 3 are inert in K.

Let $\mathfrak{N} = 2 \cdot 3 \cdot \mathfrak{q}_{13}$, and write $S_2(\mathfrak{N})^{\mathrm{new}}$ for the new subspace of Hilbert cusp forms of level $\mathfrak{N}$, weight 2 and trivial character. For $f \in S_2(\mathfrak{N})^{\mathrm{new}}$ we let $\mathbb{Q}_f$ denote the field of coefficients of f. For a newform f and $\mathfrak{p} \mid p$ a prime in $\mathbb{Q}_f$, write $\overline{\rho}_{f,\mathfrak{p}} : G_K \to \mathrm{GL}_2(\mathbb{F}_\mathfrak{p})$ the mod $\mathfrak{p}$ representation attached to f. Recall that $\overline{\rho}_{f,\mathfrak{p}}$ can ramify only at primes dividing $\mathfrak{N}$ and p.

For certain newforms $f \in S_2(\mathfrak{N})^{\mathrm{new}}$, we will establish the reducibility of $\overline{\rho}_{f,\mathfrak{p}}$, where $\mathfrak{p} \mid 7$ is a ramified prime in $\mathbb{Q}_f$. We remark that, for cubic fields (or higher degree fields), there are no effective Sturm bounds available in the literature. Furthermore, even in the quadratic case, such effective bounds are too large to be of any practical use (see Section 6).

Instead, we present a method for establishing reducibility in certain situations when the residual representation is a base change from $\mathbb{Q}$. The method is presented in the particular case of interest, but could apply in other similar settings.

The space $S_2(\mathfrak{N})^{\mathrm{new}}$ has dimension 181, and decomposes into 15 Hecke constituents as:

$$(3.1) \qquad 181 = 1 + \underbrace{1 + 1 + 1} + 3 + 6 + 6 + 12 + 15 + 18 + 18 + 21 + 24 + 27 + 27.$$

More specifically, there are:

1. Four newforms with rational Hecke eigenvalues. One of them corresponds to the base change of the elliptic curve with Cremona label 78a1. The other three correspond to non base change elliptic curves over K which are permuted by the action of $\mathrm{Gal}(K/\mathbb{Q})$.
2. One newform with Hecke eigenvalues in the real cubic field $\mathbb{Q}(\zeta_7)^+ \subset \mathbb{Q}(\zeta_7)$.
3. Ten newforms whose Hecke eigenvalue fields have degrees $6, 12, 15, 18, 21, 24$ or 27. For each of the fields $\mathbb{Q}_f$, there is a *unique* subfield E such that $\mathbb{Q}_f$ is a ray class field of degree 3 over E. We have summarized the structure of these Hecke eigenvalue fields in Table 1. When $[\mathbb{Q}_f : \mathbb{Q}] \leq 21$, we have given a generator for the conductor $\mathfrak{f}_{\mathbb{Q}_f}$ of $\mathbb{Q}_f/E$, and its factorization. For $[\mathbb{Q}_f : \mathbb{Q}] > 21$, only the the factorization is provided.

Let σ be a generator for $\mathrm{Gal}(K/\mathbb{Q})$. Let f be a newform in a Hecke constituent in $S_2(\mathfrak{N})^{\mathrm{new}}$, and d_f the dimension of this constituent. By cyclic base change and Shimura [43], there exists a newform $f^\sigma \in S_2(\mathfrak{N})^{\mathrm{new}}$ such that $\mathbb{Q}_{f^\sigma} = \mathbb{Q}_f$ and

$$a_\mathfrak{q}(f^\sigma) = a_{\mathfrak{q}^\sigma}(f), \text{ for all primes } \mathfrak{q} \text{ of } K,$$

so that $\mathrm{Gal}(K/\mathbb{Q})$ acts on the Hecke constituents. Since $[K : \mathbb{Q}] = 3$ the orbits of this action are either of size 1 or 3. The Hecke constituents of dimension 1 split into two orbits under this action: there is one orbit of size 1 which corresponds to the base change of the elliptic

5

TABLE 1. The Hecke eigenvalue fields for the newforms in $S_2(\mathfrak{N})^{\mathrm{new}}$ over the cubic subfield K of $\mathbb{Q}(\zeta_{13})^+$ which are a cubic extension of a unique subfield.

	$[\mathbb{Q}_f : \mathbb{Q}] = 6$
E	$\mathbb{Q}(w) := \mathbb{Q}[x]/(x^2 - x - 7)$
$\mathfrak{f}_{\mathbb{Q}_f}$	$(2w + 2) = \mathfrak{p}_2\mathfrak{p}_7$

	$[\mathbb{Q}_f : \mathbb{Q}] = 6$
E	$\mathbb{Q}(w) := \mathbb{Q}[x]/(x^2 - x - 1)$
$\mathfrak{f}_{\mathbb{Q}_f}$	$(-8w + 6) = \mathfrak{p}_2\mathfrak{p}_{19}$

	$[\mathbb{Q}_f : \mathbb{Q}] = 12$
E	$\mathbb{Q}(w) := \mathbb{Q}[x]/(x^4 + 2x^3 - 9x^2 - 12x - 3)$
$\mathfrak{f}_{\mathbb{Q}_f}$	$(-w^2 - 3w + 3) = \mathfrak{p}_2\mathfrak{p}_7$

	$[\mathbb{Q}_f : \mathbb{Q}] = 15$
E	$\mathbb{Q}(w) := \mathbb{Q}[x]/(x^5 - 47x^3 - 105x^2 + 70x + 1)$
$\mathfrak{f}_{\mathbb{Q}_f}$	$(1/8(-3w^4 - w^3 + 138w^2 + 369w + 9)) = \mathfrak{p}_2$

	$[\mathbb{Q}_f : \mathbb{Q}] = 18$
E	$\mathbb{Q}(w) := \mathbb{Q}[x]/(x^6 - x^5 - 58x^4 - 79x^3 + 856x^2 + 2865x + 2495)$
$\mathfrak{f}_{\mathbb{Q}_f}$	$(-8w^5 + 32w^4 + 363w^3 - 425w^2 - 5425w - 7264) = \mathfrak{p}_2\mathfrak{p}_{31}$

	$[\mathbb{Q}_f : \mathbb{Q}] = 18$
E	$\mathbb{Q}(w) := \mathbb{Q}[x]/(x^6 - 28x^4 - 2x^3 + 104x^2 + 104x + 28)$
$\mathfrak{f}_{\mathbb{Q}_f}$	$(1/2(-w^4 + 2w^3 + 26w^2 - 48w - 40)) = \mathfrak{p}_2\mathfrak{p}_7$

	$[\mathbb{Q}_f : \mathbb{Q}] = 21$
E	$\mathbb{Q}(w) := \mathbb{Q}[x]/(x^7 + x^6 - 58x^5 + 172x^4 + 84x^3 - 744x^2 + 512x + 144)$
$\mathfrak{f}_{\mathbb{Q}_f}$	$(1/8(-17w^6 - 77w^5 + 726w^4 - 296w^3 - 2904w^2 + 2144w + 592)) = \mathfrak{p}_2\mathfrak{p}_7\mathfrak{p}_7'$

	$[\mathbb{Q}_f : \mathbb{Q}] = 24$
E	$\mathbb{Q}(w) := \mathbb{Q}[x]/(x^8 + 3x^7 - 53x^6 - 84x^5 + 1018x^4 + 190x^3 - 6992x^2 + 5440x + 5060)$
$\mathfrak{f}_{\mathbb{Q}_f}$	$\mathfrak{p}_2\mathfrak{p}_7$

	$[\mathbb{Q}_f : \mathbb{Q}] = 27$
E	$\mathbb{Q}(w) := \mathbb{Q}[x]/(x^9 + 2x^8 - 96x^7 - 99x^6 + 2894x^5 + 1462x^4 - 32500x^3 + 2240x^2 + 119964x - 102212)$
$\mathfrak{f}_{\mathbb{Q}_f}$	$\mathfrak{p}_2\mathfrak{p}_7\mathfrak{p}_{13}$

	$[\mathbb{Q}_f : \mathbb{Q}] = 27$
E	$\mathbb{Q}(w) := \mathbb{Q}[x]/(x^9 - x^8 - 90x^7 + 106x^6 + 2878x^5 - 4048x^4 - 38316x^3 + 61316x^2 + 172200x - 284688)$
$\mathfrak{f}_{\mathbb{Q}_f}$	$\mathfrak{p}_2\mathfrak{p}_{1153}$

curve with Cremona label $78a1$; the other orbit of size 3, underlined in (3.1), corresponds to a set of 3 elliptic curves permuted by $\mathrm{Gal}(K/\mathbb{Q})$.

Assume that $d_f \geq 3$. Then, since the number of Hecke constituents of dimension $d_f \geq 3$ is at most 2, we conclude these constituents must be fixed by the action of $\mathrm{Gal}(K/\mathbb{Q})$. Thus, f and f^σ belong to the same constituent. However, a quick inspection of the first few Hecke eigenvalues shows that f is not a base change. Therefore, there exists a non-trivial element $\tau \in \mathrm{Gal}(\mathbb{Q}_f/E)$ such that

$$a_{\mathfrak{q}}(f^\sigma) = a_{\mathfrak{q}^\sigma}(f) = \tau(a_{\mathfrak{q}}(f)), \text{ for all primes } \mathfrak{q} \text{ of } K.$$

Lemma 3.1. *For $d = 6, 12, 18, 21, 24$ or 27, let $S_d \subset S_2(\mathfrak{N})^{\mathrm{new}}$ be the unique Hecke constituent of dimension d containing a newform $f = f_d$ with $7 \mid \mathrm{Norm}(\mathfrak{f}_{\mathbb{Q}_f})$, where $\mathfrak{f}_{\mathbb{Q}_f}$ is as in Table 1. Then, for every prime $\mathfrak{p}_0 \mid \gcd(\mathfrak{f}_{\mathbb{Q}_f}, (7))$, we have $\mathrm{Norm}(\mathfrak{p}_0) = 7$, and $\mathfrak{p}_0$ totally ramifies in $\mathbb{Q}_f/E$.*

Proof. This follows from a computation in `Magma`. $\qquad\square$

Proposition 3.2. *For $d = 12, 21, 24$ or 27, let $f \in S_d$ and $\mathfrak{p}_0$ in $\mathbb{Q}_f$ be as in Lemma 3.1. Suppose that $\overline{\rho}_{f,\mathfrak{p}_0}$ ramifies at all the primes dividing the level $\mathfrak{N}$. Then, $\overline{\rho}_{f,\mathfrak{p}_0}$ is reducible.*

Proof. Let f and $\mathfrak{p}_0$ be as in the statement. Suppose that $\overline{\rho}_{f,\mathfrak{p}_0}$ is irreducible.

Recall from the discussion preceding Lemma 3.1 that for a non-trivial $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ there is $\tau \in \mathrm{Gal}(\mathbb{Q}_f/E)$ such that

$$a_{\mathfrak{q}^\sigma}(f) = \tau(a_{\mathfrak{q}}(f)), \text{ for all primes } \mathfrak{q}.$$

Since $\mathfrak{p}_0$ is totally ramified in $\mathbb{Q}_f/E$, and the residue field is $\mathbb{F}_{\mathfrak{p}_0} = \mathbb{F}_7$, $\tau : \mathbb{Q}_f \to \mathbb{Q}_f$ gives rise to the identity map $\mathbb{F}_7 \to \mathbb{F}_7$. It follows that

(3.2) $$a_{\mathfrak{q}^\sigma}(f) \equiv a_{\mathfrak{q}}(f) \pmod{\mathfrak{p}_0}, \text{ for all primes } \mathfrak{q}.$$

Let $\tilde{\sigma} \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be a lift for σ. Consider the conjugate representation $\overline{\rho}_{f,\mathfrak{p}_0}^\sigma$ which satisfies

$$\overline{\rho}_{f,\mathfrak{p}_0}^\sigma(\mathrm{Frob}_{\mathfrak{q}}) := \overline{\rho}_{f,\mathfrak{p}_0}(\mathrm{Frob}_{\mathfrak{q}^\sigma}) = \overline{\rho}_{f,\mathfrak{p}_0}(\tilde{\sigma}\,\mathrm{Frob}_{\mathfrak{q}}\,\tilde{\sigma}^{-1}).$$

(We note that these equalities are independent of the lift $\tilde{\sigma}$.) By Equation (3.2), we have

$$\mathrm{Tr}(\overline{\rho}_{f,\mathfrak{p}_0}^\sigma(\mathrm{Frob}_{\mathfrak{q}})) = a_{\mathfrak{q}^\sigma}(f) \equiv a_{\mathfrak{q}}(f) \equiv \mathrm{Tr}(\overline{\rho}_{f,\mathfrak{p}_0}(\mathrm{Frob}_{\mathfrak{q}})) \pmod{\mathfrak{p}_0},$$

for all primes $\mathfrak{q}$. Since $\overline{\rho}_{f,\mathfrak{p}_0}$ is irreducible (hence absolutely irreducible since $\mathfrak{p}_0 \nmid 2$), the representations $\overline{\rho}_{f,\mathfrak{p}_0}$ and $\overline{\rho}_{f,\mathfrak{p}_0}^\sigma$ are isomorphic. From [25, Theorem 2.14, Chapter III], we conclude that there is an irreducible representation $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_7)$ such that $\overline{\rho}|_{G_K} = \overline{\rho}_{f,\mathfrak{p}_0}$.

We will now determine the Serre level $N = N(\overline{\rho})$, the nebentypus $\epsilon(\overline{\rho})$ and Serre weight $k(\overline{\rho})$.

We have $k(\overline{\rho}) = 2$ because $\overline{\rho}|_{G_K} = \overline{\rho}_{f,\mathfrak{p}_0}$ is of parallel weight 2 and 7 is unramified in K.

Recall that 2 and 3 are inert in K, and that 13 is the only ramified prime in K. By assumption $\overline{\rho}_{f,\mathfrak{p}_0}$ ramifies at all primes $\mathfrak{q} \mid \mathfrak{N} = 2 \cdot 3 \cdot \mathfrak{q}_{13}$, hence $\overline{\rho}_{f,\mathfrak{p}_0}$ is a Steinberg representation at these primes (since $\mathfrak{q} \| \mathfrak{N}$). It follows that $\overline{\rho}$ is Steinberg at 2 and 3; thus $v_\ell(N(\overline{\rho})) = 1$ for $\ell = 2, 3$. At $\ell = 13$, the representation $\overline{\rho}$ is either Steinberg or a twist of Steinberg by a character χ of $G_{\mathbb{Q}}$ that becomes trivial over K. In the latter case, χ is of conductor 13^1 and the conductor

7

of $\overline{\rho}$ at 13 is 13^2. So twisting $\overline{\rho}$ by χ, if necessary, we can assume also that $\upsilon_{13}(N(\overline{\rho})) = 1$ since both $\overline{\rho}$ and $\overline{\rho} \otimes \chi$ restrict to $\overline{\rho}_{f,\mathfrak{p}_0}$. Thus $N(\overline{\rho}) = 2 \cdot 3 \cdot 13 = 78$.

Since $\overline{\rho}$ is Steinberg at $\ell = 2, 3, 13$ it follows that the nebentypus $\epsilon(\overline{\rho})$ is locally trivial at ℓ; thus $\epsilon(\overline{\rho}) = 1$ as there are no other ramified primes for $\overline{\rho}$.

From the above discussion and Khare-Wintenberger (Serre's conjecture) [30], $\overline{\rho}$ is modular ; hence, there is a classical newform h and a prime $\mathfrak{p} \mid 7$ in $\mathbb{Q}_h$ such that $\overline{\rho} \simeq \overline{\rho}_{h,\mathfrak{p}}$. it follows that there is a newform $h \in S_2(78)^{\text{new}}$ such that $\overline{\rho} \simeq \overline{\rho}_{h,\mathfrak{p}}$ for some prime $\mathfrak{p} \mid 7$ in $\mathbb{Q}_h$. There is only one such h, corresponding to the isogeny class of the elliptic curve W, with Cremona label $78a1$, whose trace of Frobenius at $q = 5$ is $a_5(W) = 2$. The prime 5 splits in K so, for $\mathfrak{q} \mid 5$, we must have the following congruences

$$\mathrm{Tr}(\overline{\rho}_{f,\mathfrak{p}_0}(\mathrm{Frob}_{\mathfrak{q}})) = \mathrm{Tr}(\overline{\rho}(\mathrm{Frob}_{\mathfrak{q}})) = \mathrm{Tr}(\overline{\rho}_{h,\mathfrak{p}}(\mathrm{Frob}_{\mathfrak{q}})) = \mathrm{Tr}(\overline{\rho}_{W,7}(\mathrm{Frob}_5)) \equiv 2 \pmod 7.$$

But we easily check that we have $\overline{\rho}_{f,\mathfrak{p}_0}(\mathrm{Frob}_{\mathfrak{q}}) \not\equiv 2 \pmod 7$.

This contradiction implies that $\overline{\rho}_{f,\mathfrak{p}_0}$ must be reducible, as desired.

$\square$

Remark 3.3. Let f be a newform in the unique Hecke constituent S_{18} such that 7 ramifies in $\mathbb{Q}_f$ (as described in Table 1). Then, one easily checks that $\overline{\rho}_{f,\mathfrak{p}}$ is irreducible for the unique prime $\mathfrak{p} \mid \mathfrak{f}_{\mathbb{Q}_f}$ above 7. By adapting the proof of Proposition 3.2, one can show that f is in fact congruent to the base change of one of the newforms in $S_2(78, \chi)^{\text{new}}$. In this case, we see that $\overline{\rho}_{f,\mathfrak{p}}$ is unramified at $\mathfrak{q}_{13}$.

Remark 3.4. Let $f \in S_2(\mathfrak{N})^{\text{new}}$ be a newform as in Proposition 3.2. Then, f appears in the cohomology of a Shimura curve. For $\mathfrak{q} = (2), (3)$ and $\mathfrak{q}_{13}$, we have $U_{\mathfrak{q}} f = \pm f$, where $U_{\mathfrak{q}}$ is the Hecke operator at $\mathfrak{q}$. We believe that the reducibility of $\overline{\rho}_{f,\mathfrak{p}}$ can be proved by generalising work of Martin [37] or of Ribet and Yoo [39, 45] on non-optimal levels for reducible representations to the setting of Shimura curves over totally real number fields.

4. REDUCTION TO THE PROBLEM OF ELIMINATING THE FORM g

We recall that in order to get a complete resolution of equation (1.1), it only remains to deal with the prime $p = 7$. There are five possible obstructing forms to this, four of which are described in Proposition 3.2 and Table 1; and the form g defined over $\mathbb{Q}(\sqrt{13})$ described in the introduction. The goal of this section is to explain how we discard the four forms in Proposition 3.2 by using the refined elimination technique described in Section 2. We then deal with g in three different ways in Sections 5, 6, and 7.

Since we are following the same strategy as in [4], a crucial step in solving (1.1) for $p = 7$ is to extend [4, Theorem 7] to the exponent $p = 7$. To this end, we must prove the following:

Theorem 4.1. *Let (a, b, c) be a non-trivial primitive solution to equation (1.1) for $p = 7$.*

Then $13 \mid a + b$ and $4 \mid a + b$.

From [4, Remark 7.4], Theorem 4.1 follows provided we can discard the form g. The following theorem reduces the resolution of (1.1) for $p = 7$ to the elimination of the form g by discarding the other four obstructing forms.

Theorem 4.2. *Assume Theorem 4.1. Then Theorem 1.1 holds.*

Proof of Theorem 4.2. It suffices to consider $x^{13} + y^{13} = 3z^n$ with $n = p$ a prime number.

The case $p \neq 7$ is precisely [4, Theorem 2], so we can assume $p = 7$.

Suppose (a, b, c) is a non-trivial primitive solution to equation (1.1) with $p = 7$. From Theorem 4.1 we can assume that $4 \mid a + b$ and $13 \mid a + b$.

Let $F = F_{a,b}$ be the Frey curve defined over K, which was introduced in [4, §7.2]. Note that $v_2(a + b) = v_2(3c^p) \geq 3$ and $3 \mid a + b$, therefore [4, Lemma 11] gives that $\overline{\rho}_{F,7} \cong \overline{\rho}_{f,\mathfrak{p}}$, for some $f \in S_2(\mathfrak{N})^{\mathrm{new}}$ and $\mathfrak{p} \mid 7$ in $\mathbb{Q}_f$.

The elimination technique described in Section 2, applied with the quantities $A_q(f)$ for the rational primes $q = 5, 7, 11, 17, 31$, shows that $\overline{\rho}_{F,7} \not\cong \overline{\rho}_{f,\mathfrak{p}}$ except when f is as in Proposition 3.2. To complete the proof of the theorem, we make use of the refinement explained in Section 2 to rule out the remaining four forms. To this end, let f be as in Proposition 3.2 (see also Table 1), and suppose that $\overline{\rho}_{F,7} \cong \overline{\rho}_{f,\mathfrak{p}}$, where $\mathfrak{p} \mid 7$ in $\mathbb{Q}_f$. Since $\overline{\rho}_{F,7}$ has conductor $\mathfrak{N}$, the same is true for $\overline{\rho}_{f,\mathfrak{p}}$. Furthermore, $\overline{\rho}_{f,\mathfrak{p}}$ is irreducible (because $\overline{\rho}_{F,7}$ is irreducible by [4, Theorem 8]) so by Proposition 3.2 we can assume that $\mathfrak{p}$ is unramified in $\mathbb{Q}_f$. Choosing a $q \neq 2, 3, 13$ satisfying $q \not\equiv 1 \pmod{13}$, we obtain from [4, Lemma 8] that

  (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 $a_{\mathfrak{q}}(f) \equiv \pm(\mathrm{Norm}(\mathfrak{q}) + 1) \pmod{\mathfrak{p}}$.

By computing $a_{\mathfrak{q}}(F_{x,y})$ for each $\mathfrak{q} \mid q$ and all $x, y \in \{0, \dots, q-1\}$ not both zero, we eliminate f by checking that neither of the above congruences hold for all unramified primes $\mathfrak{p} \mid 7$ in $\mathbb{Q}_f$. Indeed, the auxiliary prime $q = 5$ suffices to eliminate all the four possible f. □

5. AN IMAGE OF INERTIA ARGUMENT WITH AN ABELIAN SURFACE

In this section, we give a proof of Theorem 4.1 based on generalizing an image of inertia argument to the setting of abelian surfaces.

From now on, we let $K = \mathbb{Q}(w)$ where $w^2 = 13$. We let $\mathcal{O}_K = \mathbb{Z}[u]$, with $u = \frac{1+w}{2}$, be the ring of integers of K. We consider the hyperelliptic curve C defined over K by

$$(5.1) \quad C : y^2 = (32u + 36)x^6 + (24u + 40)x^5 + (-u - 32)x^4 + (-16u + 8)x^3 + (17u - 28)x^2$$
$$+ (-6u + 16)x + 6u - 16,$$

and we denote its Jacobian by J.

Lemma 5.1. *The surface J has potentially good reduction at the primes (2) and (w), and we have $\mathrm{cond}(J) = \mathfrak{N}^2$, where $\mathfrak{N} = (2^3 w^2)$.*

Proof. We use Magma [5] to compute the odd part of the conductor of J, and the Dokchitser-Doris algorithm [21] to get the even part. This yields that $\mathrm{cond}(J) = \mathfrak{N}^2$.

Let $\mathfrak{q}$ be either of the primes (2) and (w) of K and consider C over $K_{\mathfrak{q}}$. By [35, Théorème 1 (V)], there is a stable model $\mathscr{C}$ of C over an extension F of $K_{\mathfrak{q}}$ such that the special fiber of $\mathscr{C}$ is a union of two elliptic curves intersecting at a single point.

9

Let $\mathcal{J}$ be the Néron model of the Jacobian of $\mathscr{C}$. By the discussion preceding [35, Proposition 2] and [35, Proposition 2(v)] itself, the special fibre of $\mathcal{J}$ is an abelian variety. Hence, J has potentially good reduction at the primes (2) and (w). $\qquad\square$

We record the following additional lemma for later, which also proves more concretely the assertion that J has potentially good reduction at (w). Let $K' = \mathbb{Q}(\zeta_{13} + \zeta_{13}^{-1})$ be the maximal totally real subfield of $\mathbb{Q}(\zeta_{13})$. Then K'/K is a cyclic extension ramified at (w) only. Let K'_w be the completion of K' at the unique prime above (w).

Lemma 5.2. *The surface J acquires good reduction over K'_w.*

Proof. Using `Magma` [5], the conductor exponent of J at the unique prime of K' above w is computed to be 0. $\qquad\square$

Let g be the Hilbert newform over K with parallel weight 2, trivial character and level $\mathfrak{N} = (2^3 w^2)$ listed in [4, Proposition 9]. Since $\mathrm{ord}_2(\mathfrak{N}) = 3$ is odd, the local component $\pi_{g,2}$ of the automorphic representation π_g attached to g is supercuspidal. Therefore, the Eichler-Shimura conjecture for totally real fields holds (see [38, Proposition 2.20.2] or [47, Theorem B]). Thus, there is an abelian surface A_g with RM by $\mathbb{Z}[\sqrt{2}]$ attached to g. The theorem below shows that A_g is isogenous to J.

Theorem 5.3. *Let C and J be given by* (5.1). *Then, we have the following:*

(1) $\mathrm{End}_K(J) = \mathbb{Z}[\sqrt{2}]$, *i.e. J is of GL_2-type with real multiplication (RM) by $\mathbb{Z}[\sqrt{2}]$;*

(2) *J is modular and corresponds to the Hecke constituent of the Hilbert newform g. In other words, J and A_g are isogenous.*

Proof. In [23, Theorem 17], there is an equation for the Humbert surface $\mathcal{H}_8$ of discriminant 8, which parametrizes principally polarized abelian surfaces with RM by $\mathbb{Z}[\sqrt{2}]$ (but where the action of $\mathbb{Z}[\sqrt{2}]$ by endomorphisms is forgotten), and is birational to a weighted projective space $\mathbf{P}^2_{r,s}$. It gives the Hilbert modular surface $Y_-(8)$ as a double-cover of $\mathbf{P}^2_{r,s}$ and this is a birational model of $Y_-(8)$ over $\mathbb{Q}$.

The point

$$(r', s') := \left(\frac{-20u - 24}{81}, \frac{-1456u + 3354}{81} \right)$$

determines the $\overline{K}$-isomorphism class of an abelian surface A whose Igusa-Clebsch invariants are given by

$$I'_2 := \frac{18112u - 38832}{81};$$

$$I'_4 := \frac{-112736u + 270660}{6561};$$

$$I'_6 := \frac{2386589920u - 5484934104}{531441};$$

$$I'_{10} := \frac{532320256u - 1222121472}{3486784401}.$$

The corresponding points in $Y_-(8)$ are still rational over K, hence by the modular interpretation of $Y_-(8)$, there is a choice of A in its $\overline{K}$-isomorphism class such that A is defined over K and A has RM by $\mathbb{Z}[\sqrt{2}]$.

For the last statement, here are some additional details. Let $\mathcal{O} = \mathbb{Z}[\sqrt{2}]$. The Hilbert modular surface $Y_-(8)$ in [23] is the coarse moduli space which parametrizes principally polarized abelian surfaces with real multiplication by $\mathbb{Z}[\sqrt{2}]$. Since A is principally polarized, A is the Jacobian of some genus 2 curve C' (the case of a canonically polarized product of two elliptic curves is ruled out as we already know A is $\overline{K}$-isomorphic to J). By the Torelli theorem, every automorphism of A with its polarization arises from $\pm\sigma$, where σ is an automorphism of C'. Since C' is isomorphic to C and the automorphism group of C is cyclic of order 2, the automorphism group of C' is cyclic of order 2. By Galois descent (see [20, §VI.3]), the obstruction to obtaining a representative moduli object defined over K corresponding to a K-rational point of $Y_-(8)$ is trivial.

Let I_2, I_4, I_6 and I_{10} be the Igusa-Clebsch invariants of the surface J, and $\alpha = -60u - 48$. Then, we have $I_{2i} = \alpha^{2i} I'_{2i}$ for $i = 1, 2, 3, 5$. This implies C and C' are isomorphic over K, since if they are given by

$$C : y^2 = a_6 x^6 + a_5 x^5 + a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0,$$
$$C' : y'^2 = a'_6 x'^6 + a'_5 x'^5 + a'_4 x'^4 + a'_3 x'^3 + a'_2 x'^2 + a'_1 x' + a'_0,$$

we have that

$$I_{2i}(C) = I_{2i} = \alpha^{2i} I'_{2i} = I_{2i}(C'),$$

and hence C is isomorphic to C' over K by the map

$$x = \alpha^2 x'$$
$$y = \alpha^6 y'.$$

Thus, the abelian surfaces A and J are isomorphic over K. Since A has RM by $\mathbb{Z}[\sqrt{2}]$, so does J. This gives one part of (1), namely that $\mathbb{Z}[\sqrt{2}]$ embeds into $\mathrm{End}_K(J)$. Using Magma, we can check $\mathrm{End}_{\overline{K}}(J)$ has rank 2 over $\mathbb{Z}$, giving the rest of (1).

Alternatively, one could compute the endomorphism ring $\mathrm{End}_K(J)$ using the algorithm in [12].

We now prove (2). Recall that 3 is inert in $\mathbb{Q}(\sqrt{2})$, and consider the 2-dimensional 3-adic Galois representation attached to J

$$\rho_{J,3} : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{GL}_2(\mathbb{Q}_3(\sqrt{2})).$$

Let $\bar{\rho}_{J,3}$ be the mod 3 reduction of this representation. By construction, $\bar{\rho}_{J,3}$ is odd. Since, J is principally polarized, and of GL_2-type, it follows from Ribet [40, Proposition 3.3] that, for $\mathfrak{q} \nmid 3\mathfrak{N}$, the characteristic polynomial at $\mathfrak{q}$ is of the form

$$\mathrm{charpoly}(\rho_{J,3}(\mathrm{Frob}_{\mathfrak{q}})) = x^2 - a_{\mathfrak{q}} x + \mathrm{Norm}(\mathfrak{q}),$$

where $\mathrm{tr}(\rho_{J,3}(\mathrm{Frob}_{\mathfrak{q}})) = a_{\mathfrak{q}} \in \mathbb{Q}(\sqrt{2})$, and $\mathrm{Norm}(\mathfrak{q})$ is the norm of $\mathfrak{q}$. By reduction modulo 3, we see that the image of $\bar{\rho}_{J,3}$ is contained in

$$\{u \in \mathrm{GL}_2(\mathbb{F}_9) : \det(u) \in \mathbb{F}_3^\times\}$$

11

and, since -1 is a square in $\mathbb{F}_9^\times$, the projective image lands in $\mathrm{PSL}_2(\mathbb{F}_9)$. By computing the orders of the conjugacy classes of $\bar\rho_{J,3}(\mathrm{Frob}_\mathfrak{q})$ for the primes $\mathfrak{q}$ above 17 and 53, we see that the projective image of $\bar\rho_{J,3}$ contains elements of orders $2, 4$ and 5. There is no proper subgroup of $\mathrm{PSL}_2(\mathbb{F}_9)$ which contains three elements with those orders, hence the projective image of $\bar\rho_{J,3}$ is $\mathrm{PSL}_2(\mathbb{F}_9)$. In particular, we see that the image of $\bar\rho_{J,3}$ contains $\mathrm{SL}_2(\mathbb{F}_9)$, so $\bar\rho_{J,3}$ is absolutely irreducible.

The prime 3 splits in K. Writing $(3) = v_1 v_2$, where $v_1 = (u-1)$ and $v_2 = (u)$, we get that

$$\mathrm{tr}(\rho_{J,3}(\mathrm{Frob}_{v_1})) = 2 \pm \sqrt{2}, \text{ and } \mathrm{tr}(\rho_{J,3}(\mathrm{Frob}_{v_2})) = \pm\sqrt{2}$$

by computing the Euler factors of the curve C at both places and factoring over $\mathbb{Q}(\sqrt{2})$. These traces are units modulo 3, so $\rho_{J,3}$ is ordinary at each $v \mid 3$. Further, since $5 \nmid \mathfrak{N}$, we see that $\bar\rho_{J,3}|_{I_5}$ is trivial, hence it has odd order. Since 3 and 5 have odd ramification indices in K, it follows that $\bar\rho_{J,3}$ satisfies the conditions of [24, Theorem 3.2 and Proposition 3.4]. Hence, it is modular.

We use [31, Theorem 3.5.5] to conclude that $\rho_{J,3}$, and hence J, is modular.

By local-global compatibility ([10, Théorème (A)]) and Lemma 5.1, the level of the Hilbert newform attached to J is $\mathfrak{N} = (2^3 w^2)$. There is a unique Hecke constituent of weight 2 and level $\mathfrak{N}$ whose Euler factors match those of the surface J, it is the one corresponding to the newform g. $\qquad\square$

The 'image of inertia argument' discards the possibility of the mod p representation of the Frey curve and that of a newform f being isomorphic by showing they have different image sizes at an inertia subgroup. This idea, originally from [33, p. 8], has been extensively applied and refined [2] (see [4, §3] for a description of two refinements) in the case of f corresponding to an elliptic curve. In its essence, this argument boils down to showing that the Frey curve and the newform f have different inertial types at some prime q dividing the level of f. Thus far, such inertia arguments have been restricted to the case of f corresponding to an elliptic curve because a method to explicitly determine the inertial types of a form f with non-rational coefficients has not been worked out in general.

In this section, we will use the modularity in Theorem 5.3 to describe (see Theorem 5.6) the inertial type of the non-rational form g at the prime (2); this together with the local information at (w) given by Lemma 5.2 allows for a proof of Theorem 1.1.

Before proceeding we need some notation. Let $E = E_{1,-1}$ be the Frey curve attached to the trivial solution $(1, -1, 0)$ in [4, Section 7.1]; it admits a minimal model given by

$$E : y^2 = x^3 - ux^2 + (9u - 25)x - 17u + 49.$$

Let also J be as above and $\mathfrak{p}_7$ be the prime of $\mathbb{Q}(\sqrt{2})$ above 7 generated by $3 + \sqrt{2}$.

Let $K_2/\mathbb{Q}_2$ be the unique unramified quadratic extension and K_2^{un} its maximal unramified extension in a fixed algebraic closure of $\mathbb{Q}_2$. For an abelian variety A/K_2 with potentially good reduction, there is a minimal extension M_A/K_2^{un} where A obtains good reduction. By a result of Serre-Tate ([42, §2, Corollary 3]), we have $M_A = K_2^{un}(A[p])$ for any odd prime p.

We recall that the curve E has potentially good reduction at 2. By Lemma 5.1, the same is true for J; so $M_E = K_2^{un}(E[3])$ and $M_J = K_2^{un}(J[3])$.

Proposition 5.4. *We have $M_E = M_J$ and $\mathrm{Gal}(M_E/K_2^{un}) \cong \mathrm{SL}_2(\mathbb{F}_3)$.*

Proof. Computing the standard invariants of E, we find that they have the following valuations at (2):

$$(v_2(c_4(E)), v_2(c_6(E)), v_2(\Delta(E))) = (5, 5, 4).$$

Hence $v_2(j(E)) = 11$ and E has potentially good reduction at (2). It follows from [9, pp. 675, Corollaire] that E has semistability defect $e = 24$, hence $\mathrm{Gal}(M_E/K_2^{un}) \cong \mathrm{SL}_2(\mathbb{F}_3)$ by [32].

On the other hand, J also has potentially good reduction at (2) by Lemma 5.1, and as a byproduct, the Dokchitser-Doris algorithm [21] returns the totally ramified field $K_2(J[3])$ with a defining polynomial over K_2 of degree 24.

We check that E has good reduction over $K_2(J[3])$, so $M_E \subset M_J = K_2^{un}(J[3])$ by minimality. Since $[M_E : K_2^{un}] = 24 = [M_J : K_2^{un}]$ the result follows. $\qquad\square$

The following well known result will be of use for us; due to a lack of a clear reference we include a proof here.

Lemma 5.5. *Let K be a totally real field and $\mathfrak{q}$ a prime above 2 in K. Let $I_\mathfrak{q} \subset G_K$ be an inertia subgroup at $\mathfrak{q}$. Let h be a Hilbert modular form over K of level $\mathfrak{N}$ and field of coefficients $\mathbb{Q}_h$. Assume that $\mathfrak{q} \mid \mathfrak{N}$ and that h has a supercuspidal exceptional type at $\mathfrak{q}$.*

Then, for all primes p coprime to $6\mathfrak{N}$ and all primes $\mathfrak{P} \mid p$ in $\mathbb{Q}_h$, we have $\overline{\rho}_{h,\mathfrak{P}}(I_\mathfrak{q}) \simeq \mathrm{SL}_2(\mathbb{F}_3)$.

Proof. Let π_h be the automorphic representation attached to h, and $\pi_{h,\mathfrak{q}}$ the local component at $\mathfrak{q}$. Also, let $\sigma_{h,\mathfrak{q}} : W_\mathfrak{q} \to \mathrm{GL}_2(\mathbb{C})$ be the Weil representation attached to $\pi_{h,\mathfrak{q}}$ by the local Langlands correspondence (see [34]). Since $\pi_{h,\mathfrak{q}}$ is a supercuspidal exceptional representation, then $\sigma_{h,\mathfrak{q}}$ is an exceptional representation, which means that the projective image of $\sigma_{h,\mathfrak{q}}$ is either A_4 or S_4 (the A_5 case cannot occur since $W_\mathfrak{q}$ is solvable).

Let p be a rational prime coprime to $6\mathfrak{N}$ and $\mathfrak{P} \mid p$ a prime in $\mathbb{Q}_h$. Let $D_\mathfrak{q} \supset I_\mathfrak{q}$ be a decomposition group at $\mathfrak{q}$ in G_K. By local-global compatibility ([10, Théorème (A)]), the projective image of $\rho_{h,\mathfrak{P}}|_{D_\mathfrak{q}}$ in $\mathrm{PGL}_2(\overline{\mathbb{Q}}_p)$ is either A_4 or S_4, and $\rho_{h,\mathfrak{P}}|_{I_\mathfrak{q}}$ acts irreducibly [8, §42.1] (in loc. cit., supercuspidal exceptional representations are called primitive representations). Since $p \nmid 6$, the image of $\overline{\rho}_{h,\mathfrak{P}}|_{D_\mathfrak{q}}$ in $\mathrm{PGL}_2(\overline{\mathbb{F}}_p)$ is also A_4 or S_4, and $\overline{\rho}_{h,\mathfrak{P}}|_{I_\mathfrak{q}}$ acts irreducibly. A careful analysis of the proof of [18, Proposition 2.4] shows that it carries over to any finite local extension of $\mathbb{Q}_2$. In particular, this implies that the projective image of $\overline{\rho}_{h,\mathfrak{P}}|_{I_\mathfrak{q}}$ is equal to A_4. Therefore, the image of $\overline{\rho}_{h,\mathfrak{P}}|_{I_\mathfrak{q}} \subset \mathrm{SL}_2(\overline{\mathbb{F}}_p)$ is isomorphic to either A_4 or $\mathrm{SL}_2(\mathbb{F}_3)$; the result now follows since there is only one element of order 2 in $\mathrm{SL}_2(\overline{\mathbb{F}}_p)$ (for $p > 2$), hence no subgroup of $\mathrm{SL}_2(\overline{\mathbb{F}}_p)$ is isomorphic to A_4. $\qquad\square$

Theorem 5.6. *Let $\mathfrak{P} \mid 7$ in $F = \mathbb{Q}(\sqrt{2})$ be a prime. Then, we have*

$$M_J = K_2^{un}(J[7]) = K_2^{un}(J[\mathfrak{P}])$$

and, moreover,

$$\overline{\rho}_{g,\mathfrak{P}}|_{I_2} \cong \overline{\rho}_{E,7}|_{I_2}.$$

Here, I_2 denotes an inertia subgroup at (2) in G_K.

Proof. Let $\mathfrak{P}, \mathfrak{P}'$ be the two primes above 7 in $\mathbb{Q}(\sqrt{2})$. By [44, Theorem 4.3.1], we have that

$$J[7] = J[\mathfrak{P}] \times J[\mathfrak{P}'].$$

This means that the field $M_J = K_2^{un}(J[7])$ is the compositum of $K_2^{un}(J[\mathfrak{P}])$ and $K_2^{un}(J[\mathfrak{P}'])$, the fields cut out by $\overline{\rho}_{J,\mathfrak{P}}|_{I_2}$ and $\overline{\rho}_{J,\mathfrak{P}'}|_{I_2}$ respectively.

We will now show that these three fields have the same degree and the first statement follows. By Theorem 5.3, we have $\overline{\rho}_{J,\mathfrak{P}} \cong \overline{\rho}_{g,\mathfrak{P}}$ and $\overline{\rho}_{J,\mathfrak{P}'} \cong \overline{\rho}_{g,\mathfrak{P}'}$. By Proposition 5.4 and the discussion preceding it, we only need to show that the fields cut out by $\overline{\rho}_{g,\mathfrak{P}}|_{I_2}$ and $\overline{\rho}_{g,\mathfrak{P}'}|_{I_2}$ have degree $\#\operatorname{SL}_2(\mathbb{F}_3) = 24$.

Note that if $\rho_{g,\mathfrak{P}}|_{I_2}$ is reducible then the conductor exponent at 2 is either 1 (special representation) or even (because the determinant of $\rho_{g,\mathfrak{P}}$ is cyclotomic, and hence on restriction to inertia, the diagonal characters must be inverses of each other); therefore, $\rho_{g,\mathfrak{P}}|_{I_2}$ is irreducible and g has supercuspidal type at 2 which is not given by an induction from the unramified quadratic extension. We conclude that g is either supercuspidal induced from a ramified extension or exceptional. In the former case, then $\overline{\rho}_{g,\mathfrak{P}}|_{I_2}$ would have projective dihedral image; since the field cut out by $\overline{\rho}_{g,\mathfrak{P}}|_{I_2}$ is a Galois subextension of $K_2^{un}(J[7])/K_2^{un}$, which has Galois group $\operatorname{SL}_2(\mathbb{F}_3)$, and $\operatorname{SL}_2(\mathbb{F}_3)$ does not have any quotients which are dihedral, we conclude that g must have a supercuspidal exceptional type at 2. By Lemma 5.5, we obtain that the fields cut out by $\overline{\rho}_{g,\mathfrak{P}}|_{I_2}$ have degree $\#\operatorname{SL}_2(\mathbb{F}_3) = 24$ as required.

We now prove the last statement. From the first part of the theorem, Theorem 5.3 and Proposition 5.4, we have that M_J is the field cut out by both $\overline{\rho}_{g,\mathfrak{P}}|_{I_2}$ and $\overline{\rho}_{E,7}|_{I_2}$. Thus, $\overline{\rho}_{g,\mathfrak{P}}|_{I_2}$, and $\overline{\rho}_{E,7}|_{I_2}$ have the same kernel, and image $\operatorname{SL}_2(\mathbb{F}_3) \hookrightarrow \operatorname{SL}_2(\mathbb{F}_7) \subset \operatorname{GL}_2(\mathbb{F}_7)$. Therefore, it follows from [26, Lemma 2] that they are isomorphic representations. $\qquad\square$

Finally, we now show Theorem 4.1 using the information on the inertial types.

First proof of Theorem 4.1. Let (a, b, c) be a non-trivial primitive solution to equation (1.1) with $n = p = 7$.

Let $E_{a,b}$ be the Frey curve defined in [4, Section 7.1]. The proof of [4, Theorem 7] uses [4, Proposition 9] which asserts that $\overline{\rho}_{E_{a,b},p} \cong \overline{\rho}_{Z,p}$ where Z is one of $E_{1,-1}$, $E_{1,0}$, $E_{1,1}$. In the case $p = 7$, there is the additional possibility that $\overline{\rho}_{E_{a,b},7} \cong \overline{\rho}_{g,\mathfrak{P}}$ where $\mathfrak{P} \mid 7$ in $\mathbb{Q}(\sqrt{2})$. By [4, Remark 7.4] we have $\mathfrak{P} = \mathfrak{p}_7$.

Suppose Z is one of the three curves above, the arguments of [4, Theorem 7] still hold for $p = 7$. For instance, if $Z = E_{1,-1}$ and $4 \nmid a + b$, then it is shown that

(5.2) $$\overline{\rho}_{E_{a,b},p}|_{I_2} \not\cong \overline{\rho}_{Z,p}|_{I_2}.$$

To complete the proof, we only have to eliminate the possibility that $\overline{\rho}_{E_{a,b},7} \cong \overline{\rho}_{g,\mathfrak{p}_7}$.

By Theorem 5.3, we have $\overline{\rho}_{g,\mathfrak{p}_7} \cong \overline{\rho}_{J,\mathfrak{p}_7}$. The proof of [4, Theorem 7 (A)] then remains valid by simply replacing Z/K' with J/K'_w and using Lemma 5.2. This shows $13 \mid a + b$.

Finally, we note that $\overline{\rho}_{g,\mathfrak{p}_7}|_{I_2} \cong \overline{\rho}_{E_{1,-1},7}|_{I_2}$ by Theorem 5.6, and that $\overline{\rho}_{E_{1,-1},7}|_{I_2} \not\cong \overline{\rho}_{E_{a,b},7}|_{I_2}$ by (5.2), for $4 \nmid a + b$. This shows that $4 \mid a + b$. $\qquad\square$

Remark 5.7. The obstruction to solving (1.1) comes from an abelian surface with real multiplication; namely, the surface A_g attached to the form g. The approach in this section relies crucially on the fact that A_g is isogenous over $\mathbb{Q}(\sqrt{13})$ to a principally polarized abelian surface with real multiplication, i.e. A_g is a $\mathbb{Q}(\sqrt{13})$-rational point on some Humbert surface. Hence, the methods in [17, §4.1.2] and [23, §7] can be applied to explicitly find a hyperelliptic curve C such that A_g is isogenous over $\mathbb{Q}(\sqrt{13})$ to the Jacobian J of C. There is thus a reasonable chance for the method in this section to succeed whenever the obstruction to the modular method for solving a Diophantine equation like the one in (1.1) is isogenous to a principally polarized abelian surface with real multiplication and reasonably-sized height.

Remark 5.8. Although we apply this generalized inertia argument to a situation with fixed exponent $p = 7$, the method described is also applicable to a setting with general exponent p (unlike the methods in Sections 6-7). This can be useful when working with certain Frey hyperelliptic curves as in the Darmon program for the Generalized Fermat equation [14].

For example, in forthcoming work [11], the equation $x^p + y^p = z^5$ is studied using a Frey hyperelliptic curve $C_5^- = C_5^-(a, b, c)$ constructed by Darmon (see [14, p. 425]), where (a, b, c) is a non-trivial primitive solution satisfying $2 \mid ab$, $5 \nmid ab$. The Jacobian $J_5^- = J_5^-(a, b, c)$ of C_5^- is defined over $\mathbb{Q}$ and becomes of GL_2-type over $F = \mathbb{Q}(\sqrt{5})$ with real multiplication by F. In applying the modular method in this case, one finds that it is not possible to rule out an isomorphism

$$\tag{5.3} \overline{\rho}_{J_5^-, \mathfrak{P}} \cong \overline{\rho}_{h, \mathfrak{P}}$$

by comparing traces of Frobenius at primes not dividing 10, where h is a certain Hilbert newform of parallel weight 2, trivial character, and level $(2^4 \mathfrak{r}^2)$ over F; here, $\mathfrak{P}$ is a prime above p, $\mathfrak{r}$ is the prime above 5 of F, and note that 2 is inert in F. By modularity and comparing a few traces, one checks that the Hilbert newform h corresponds to $J_5^-(8, -8, 0)$ twisted by the quadratic character associated to $F(\sqrt{2})$. Applying the Dokchitser-Doris algorithm [21], we deduce that $J_5^-(8, -8, 0)$ achieves good reduction over a degree 10 totally ramified extension of F_2^{un} (see [3]), so $\overline{\rho}_{h, \mathfrak{P}}(I_2)$ has order dividing 20 and divisible by 5. Moreover, it is shown in [11] that $J_5^-(a, b, c)$ has potentially multiplicative reduction at 2 when $2 \mid ab$, $5 \nmid ab$ for $p > 5$. Therefore, this implies that $\overline{\rho}_{J_5^-, \mathfrak{P}}$ is a quadratic twist of Steinberg at 2 and hence $\overline{\rho}_{J_5^-, \mathfrak{P}}(I_2)$ has order dividing $2p$. We thus obtain a contradiction to isomorphism (5.3) when $p > 5$.

6. A RESIDUAL MULTIPLICITY ONE ARGUMENT

In this section, we outline a proof of Theorem 4.1 based on establishing the mod 7 congruence mentioned in the introduction and described below; see also [4, Remark 7.4] for more details.

The natural attempt to use a Sturm bound such as the one in [19] fails because it necessitates the computation of Hecke eigenvalues for primes of $K = \mathbb{Q}(\sqrt{13})$ of norm at least 10^6, which is not computationally feasible.

The method we introduce for establishing $\overline{\rho}_{g, \mathfrak{p}_7} \cong \overline{\rho}_{f, 7}$ below, without the use of a Sturm bound, relies on a residual multiplicity one argument. It applies for more general f, g and p. For example, it has also been used in [15] to show the isomorphism of some residual mod 2

Galois representations arising from Hilbert modular forms over the maximal totally real subfield of $\mathbb{Q}(\zeta_{32})$, the cyclotomic field of 32nd root of unity.

Let $E = E_{1,-1}$ and $\mathfrak{p}_7$ be as in the previous section; in particular, we have $\mathbb{F}_{\mathfrak{p}_7} = \mathbb{F}_7$.

Let $S_2(\mathfrak{N})^{\text{new}}$ be the new subspace of Hilbert cusp forms of weight 2, trivial character, and level $\mathfrak{N} = (2^3 w^2)$. The elliptic curve E is modular by [27] and corresponds to a newform $f \in S_2(\mathfrak{N})^{\text{new}}$. Similarly, in Theorem 5.3, we prove that the surface J is modular and corresponds to the form $g \in S_2(\mathfrak{N})^{\text{new}}$. So, we have $\bar{\rho}_{f,7} \simeq \bar{\rho}_{E,7}$ and $\bar{\rho}_{g,\mathfrak{p}_7} \simeq \bar{\rho}_{J,\mathfrak{p}_7}$.

Let $D = \left(\frac{-1,-1}{K}\right)$ be the totally definite quaternion algebra over K ramified at both places at infinity only. Let $\mathcal{O}_D$ be a maximal order in D. Also, let $\widehat{D} = D \otimes \widehat{\mathbb{Z}}$, $\widehat{\mathcal{O}}_K = \mathcal{O}_K \otimes \widehat{\mathbb{Z}}$, and $\widehat{\mathcal{O}}_D = \mathcal{O}_D \otimes \widehat{\mathbb{Z}}$, where $\widehat{\mathbb{Z}}$ is the profinite completion of $\mathbb{Z}$. We fix an isomorphism $\left(\widehat{\mathcal{O}}_D\right)^\times \simeq \text{GL}_2(\widehat{\mathcal{O}}_K)$, and we define the compact open subgroup

$$U_0(\mathfrak{N}) := \left\{ \gamma \in \left(\widehat{\mathcal{O}}_D\right)^\times : \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod \mathfrak{N} \right\}.$$

We consider the space

$$S_2^D(\mathfrak{N}) = \left\{ f : D^\times \backslash \widehat{D}^\times / U_0(\mathfrak{N}) \to \mathbb{C} \right\}$$

which has an action of Hecke operators $T_\mathfrak{q}$ for $\mathfrak{q} \nmid \mathfrak{N}$. Let $\mathbb{T}_\mathfrak{N}$ be the Hecke algebra acting on $S_2^D(\mathfrak{N})$ which is generated by the operators $T_\mathfrak{q}$. There is a decomposition

$$S_2^D(\mathfrak{N}) = S_2^D(\mathfrak{N})^{\text{old}} \oplus S_2^D(\mathfrak{N})^{\text{new}}.$$

where the subspaces $S_2^D(\mathfrak{N})^{\text{old}}$ and $S_2^D(\mathfrak{N})^{\text{new}}$ are $\mathbb{T}_\mathfrak{N}$-stable, and $S_2^D(\mathfrak{N})^{\text{new}}$ is the orthogonal complement of $S_2^D(\mathfrak{N})^{\text{old}}$ under a certain inner product defined on $S_2^D(\mathfrak{N})$.

The $\mathbb{Z}$-submodule of $S_2^D(\mathfrak{N})$ given by

$$S_2^D(\mathfrak{N}, \mathbb{Z}) = \left\{ f : D^\times \backslash \widehat{D}^\times / U_0(\mathfrak{N}) \to \mathbb{Z} \right\},$$

is stable under $\mathbb{T}_\mathfrak{N}$ and generates $S_2^D(\mathfrak{N})$ over $\mathbb{C}$ (i.e. is an integral structure for $S_2^D(\mathfrak{N})$).

Let $S_2^D(\mathfrak{N}, \mathbb{Z})^{\text{new}}$ be the orthogonal projection of $S_2^D(\mathfrak{N}, \mathbb{Z})$ to $S_2^D(\mathfrak{N})^{\text{new}}$. Then $S_2^D(\mathfrak{N}, \mathbb{Z})^{\text{new}}$ is an integral structure for $S_2^D(\mathfrak{N})^{\text{new}}$; in particular, the matrices representing the action of the $T_\mathfrak{q}$ on $S_2^D(\mathfrak{N})^{\text{new}}$ have integer coefficients.

For any commutative ring with unity A, define

$$S_2^D(\mathfrak{N}, A) := S_2^D(\mathfrak{N}, \mathbb{Z}) \otimes A$$
$$S_2^D(\mathfrak{N}, A)^{\text{new}} := S_2^D(\mathfrak{N}, \mathbb{Z})^{\text{new}} \otimes A.$$

We recall that, since $[K : \mathbb{Q}] = 2$ is even, the Jacquet-Langlands correspondence implies that there is an isomorphism of Hecke modules $\text{JL} : S_2^D(\mathfrak{N}) \simeq S_2(\mathfrak{N})$, which maps $S_2^D(\mathfrak{N})^{\text{new}}$ onto $S_2(\mathfrak{N})^{\text{new}}$. We let $\phi = \text{JL}^{-1}(f)$ and $\psi = \text{JL}^{-1}(g)$.

Proposition 6.1. *Consider the residual representations*

$$\bar{\rho}_{g,\mathfrak{p}_7} : \text{Gal}(\overline{\mathbb{Q}}/K) \to \text{GL}_2(\mathbb{F}_7) \quad and \quad \bar{\rho}_{f,7} : \text{Gal}(\overline{\mathbb{Q}}/K) \to \text{GL}_2(\mathbb{F}_7).$$

Then, we have $\bar{\rho}_{g,\mathfrak{p}_7} \cong \bar{\rho}_{f,7}$.

16

Proof. Recall that the coefficient field of f is $\mathbb{Q}$ and that of g is $L = \mathbb{Q}(\sqrt{2})$. Let $\mathcal{O}_L = \mathbb{Z}[\sqrt{2}]$ and $\mathcal{O}_{L,\mathfrak{p}_7}$ be the completion of $\mathcal{O}_L$ at $\mathfrak{p}_7$. Let

$$\theta : S_2^D(\mathfrak{N}, \mathcal{O}_{L,\mathfrak{p}_7})^{\text{new}} \twoheadrightarrow S_2^D(\mathfrak{N}, \mathbb{F}_7)^{\text{new}}$$

be the natural reduction map.

Up to scaling, we may assume ϕ and ψ are elements in $S_2^D(\mathfrak{N}, \mathcal{O}_{L,\mathfrak{p}_7})^{\text{new}}$ and their reductions $\bar{\phi} = \theta(\phi)$ and $\bar{\psi} = \theta(\psi)$ are non-zero elements in $S_2^D(\mathfrak{N}, \mathbb{F}_7)^{\text{new}}$. Hence, $\bar{\phi}$ and $\bar{\psi}$ are eigenvectors of $T_\mathfrak{q}$ (mod 7) for all $\mathfrak{q} \nmid 7\mathfrak{N}$.

Let $\mathbb{T} \subseteq \text{End}_{\mathbb{F}_7}(S_2^D(\mathfrak{N}, \mathbb{F}_7)^{\text{new}})$ be the Hecke algebra generated by the operators $T_\mathfrak{q}$ (mod 7) for all primes $\mathfrak{q} \nmid 7\mathfrak{N}$, and $W_{\bar{\phi}}$ (resp. $W_{\bar{\psi}}$) be the $\mathbb{T}$-submodule generated by $\bar{\phi}$ (resp. $\bar{\psi}$) in $S_2^D(\mathfrak{N}, \mathbb{F}_7)^{\text{new}}$.

Let $\mathbb{T}' \subseteq \mathbb{T}$ be the subalgebra generated by the Hecke operators $T_\mathfrak{q}$ for prime ideals $\mathfrak{q} \nmid 7\mathfrak{N}$ of norm up to 43, and S the socle of $S_2^D(\mathfrak{N}, \mathbb{F}_7)^{\text{new}}$ considered as a $\mathbb{T}'$-module, i.e. the sum of all simple $\mathbb{T}'$-submodules of $S_2^D(\mathfrak{N}, \mathbb{F}_7)^{\text{new}}$, which is semi-simple.

Since both $\bar{\phi}$ and $\bar{\psi}$ are eigenvectors for $\mathbb{T}'$, $W_{\bar{\phi}}$ and $W_{\bar{\psi}}$ are simple $\mathbb{T}'$-modules of dimension one over $\mathbb{F}_7$. Hence, $W_{\bar{\phi}}$ and $W_{\bar{\psi}}$ are contained in S. They are isomorphic as $\mathbb{T}'$-modules as for all prime ideals $\mathfrak{q} \nmid 7\mathfrak{N}$ of norm up to 43, we have that $a_\mathfrak{q}(f)$ (mod 7) $= a_\mathfrak{q}(g)$ (mod $\mathfrak{p}_7$) as elements in $\mathbb{F}_7$, where $a_\mathfrak{q}(u)$ denotes the eigenvalue of $T_\mathfrak{q}$ acting on an eigenvector $u \in S_2^D(\mathfrak{N})$.

Using `Magma` [5], we can compute the $\mathbb{T}'$-module S, which has dimension 348 over $\mathbb{F}_7$. There are 34 (non-isomorphic) simple constituents which have dimension one over $\mathbb{F}_7$, and each appears with multiplicity one. Thus, $W_{\bar{\phi}} = W_{\bar{\psi}}$ inside $S \subseteq S_2^D(\mathfrak{N}, \mathbb{F}_7)^{\text{new}}$. Since $W_{\bar{\phi}} = W_{\bar{\psi}}$ inside $S_2^D(\mathfrak{N}, \mathbb{F}_7)^{\text{new}}$ and both are $\mathbb{T}$-modules as well, we obtain that $a_\mathfrak{q}(f)$ (mod 7) $= a_\mathfrak{q}(g)$ (mod $\mathfrak{p}_7$) as elements of $\mathbb{F}_7$, for all prime ideals $\mathfrak{q} \nmid 7\mathfrak{N}$.

$\square$

Second proof of Theorem 4.1. The bulk of the argument of the proof of this theorem given in Section 5, including the identity (5.2), still applies.

Therefore, we only need to show that the isomorphism $\overline{\rho}_{E_{a,b},7} \cong \overline{\rho}_{g,\mathfrak{p}_7}$ is not possible. Suppose we have that $\overline{\rho}_{E_{a,b},7} \cong \overline{\rho}_{g,\mathfrak{p}_7}$. Then by Proposition 6.1, we have

$$\overline{\rho}_{E_{a,b},7} \cong \overline{\rho}_{g,\mathfrak{p}_7} \cong \overline{\rho}_{E_{1,-1},7}.$$

Now the arguments that eliminated $E_{1,-1}$ apply to eliminate g, thereby completing the proof.

$\square$

7. A UNIT SIEVE ARGUMENT

In this section, we give a proof of Theorem 4.1 based on combining the study of units in classical descent with local restrictions on the solutions coming from the multi-Frey approach in [4].

Let ζ be a primitive 13th root of unity. Suppose (a, b, c) is a nontrivial primitive solution to (1.1). We then have the factorization in $\mathbb{Z}[\zeta]$,

$$a^{13} + b^{13} = (a + b) \prod_{i=1}^{12} (a + \zeta^i b) = 3c^7.$$

The integers $a+b$ and $\frac{a^{13}+b^{13}}{a+b}$ are coprime away from 13 (see, e.g., [13, Lemma 2.1]). Let $\ell \not\equiv 1$ (mod 13) be a prime number dividing $a^{13}+b^{13}$. Since a and b are coprime, we have that $\ell \nmid ab$ and hence there exists an integer b' such that $bb' \equiv -1$ (mod ℓ). Therefore we have $(ab')^{13} \equiv 1$ (mod ℓ) and since $\ell \not\equiv 1$ (mod 13), it follows that ℓ divides $a + b$. In particular, we have that $3 \nmid a + \zeta b$. Furthermore, by classical descent, we have that

(7.1)
$$a + \zeta b = \begin{cases} \epsilon \beta^7 & \text{if } 13 \nmid a + b \\ \epsilon(1 - \zeta)\beta^7 & \text{if } 13 \mid a + b, \end{cases}$$

where ϵ is a unit of $\mathbb{Z}[\zeta]$ and $\beta \in \mathbb{Z}[\zeta]$. We only need to consider ϵ up to 7th powers, which means that there are initially $16,807$ possible choices for ϵ.

One can now reduce (7.1) modulo a prime $\mathfrak{q}$ of $\mathbb{Z}[\zeta]$ above the rational prime q. If q is such that the order of the multiplicative group of the residue field at $\mathfrak{q}$ is divisible by 7, the condition of being a 7th power is nontrivial.

The primes $q = 11, 17, 23, 29, 37, 41$ satisfy the condition above; moreover, we can obtain local information from the modular method: if $\overline{\rho}_{E_{a,b},7} \cong \overline{\rho}_{g,\mathfrak{p}_7}$, locally at q this congruence imposes constraints on the solutions (a, b) modulo q (in both cases of good or multiplicative reduction of $E_{a,b}$ at q) and hence on the unit ϵ.

Note we cannot obtain information from $q = 2$ in the same way, because 2 divides the level of g. However, since the multiplicative group of the residual field of K at $\mathfrak{q} = (2)$ has order a multiple of 7, this together with the assumption $4 \nmid a + b$ also imposes restrictions on ϵ.

Third proof of Theorem 4.1. We first note the condition $4 \nmid a + b$ is equivalent to $2 \nmid a + b$ for our equation. Now we sieve the set of possible units in the two cases of equation (7.1), assuming $2 \nmid a + b$ for a contradiction. More precisely, in both the cases $13 \nmid a + b$ and $13 \mid a + b$, using the primes $q = 2, 11, 19, 23$ the set of units which passes all local conditions is empty. Thus $4 \mid a + b$, as desired.

We will now prove that $13 \mid a + b$. From the above we can assume $4 \mid a + b$ and $13 \nmid a + b$ for a contradiction. Using the local information at the primes $q = 2, 11, 19, 23, 29, 41$, again the set of units which passes all local conditions is empty, concluding the proof. $\square$

Remark 7.1. This method of sieving units also appears in [13], in the context of reducing the number of hyperelliptic curves to be considered for Chabauty. However, only the primes q not dividing the level are considered there. In our case, we succeed without the need to apply Chabauty since we can sieve also at $q = 2$ which is a prime in the level. It should also be noted that the reason the unit $\epsilon = 1$ does not pass the local conditions from the modular method (unlike the situation in [13]) is because our original equation (1.1) does not have the trivial solutions $\pm(1, 0, 1), \pm(0, 1, 1)$ due to the coefficient 3.

8. A REMARK ON THE EQUATION $x^{2\ell} + y^{2m} = z^p$

To conclude this paper, we use the technique from Section 3 to complete the following result of Anni–Siksek [1].

Theorem 8.1 (Anni–Siksek). *Let $p = 3, 5, 7, 11$ or 13. Let $\ell, m \geq 5$ be primes, and if $p = 13$ suppose moreover that $m, \ell \neq 7$. Then the only primitive solutions to*

$$x^{2\ell} + y^{2m} = z^p$$

are the trivial ones $(x, y, z) = (\pm 1, 0, 1)$ and $(0, \pm 1, 1)$.

The proof of this theorem is a remarkable application of the modular method over totally real subfields of $\mathbb{Q}(\zeta_p)^+$. The extra conditions $m, \ell \neq 7$ for $p = 13$ are required due to the presence of a single Hilbert newform, denoted $\mathfrak{f}_{11}$ in *loc. cit*, which evades the elimination step.

Let $K \subset \mathbb{Q}(\zeta_{13})^+$ be the cubic field of Section 3. Recall that 2 is inert in K and that $\mathfrak{q}_{13}$ is the unique prime above 13. The newform $\mathfrak{f}_{11}$ belongs to $S_2(2 \cdot \mathfrak{q}_{13})^{\mathrm{new}}$, the new subspace of Hilbert cusp forms of level $2 \cdot \mathfrak{q}_{13}$, weight 2, and trivial character. It is the unique newform in this space with field of coefficients $\mathbb{Q}_{\mathfrak{f}_{11}} = \mathbb{Q}(\zeta_7)^+$ the real cubic subfield of the cyclotomic field of 7-th roots of unity, in which 7 is totally ramified. Let $\mathfrak{p}_0$ be the unique prime of $\mathbb{Q}_{\mathfrak{f}_{11}}$ above 7. The authors are not able to exclude the possibility that

$$(8.1) \qquad\qquad \overline{\rho}_{E',7} \simeq \overline{\rho}_{\mathfrak{f}_{11}, \mathfrak{p}_0},$$

where E' is the Frey curve defined in [1, pg. 10]; see [1, pg. 19] for further details. However, as observed in *loc. cit.*, numerical evidence strongly suggests that $\overline{\rho}_{\mathfrak{f}_{11}, \mathfrak{p}_0}^{ss} \simeq \chi_7 \oplus 1$ so, in particular, $\overline{\rho}_{\mathfrak{f}_{11}, \mathfrak{p}_0}$ is reducible. In Proposition 8.3, we show that this is indeed the case. This means that the isomorphism (8.1) cannot occur since $\overline{\rho}_{E',7}$ is irreducible. Therefore, since $\mathfrak{p}_0$ is the only prime in $\mathbb{Q}_{\mathfrak{f}_{11}}$ above 7, we have successfully completed the elimination step for the form $\mathfrak{f}_{11}$. This in turn allows us to remove the assumption that $m, \ell \neq 7$ for $p = 13$ in Theorem 8.1. Thus we have the following corollary.

Corollary 8.2. *Let $\ell, m \geq 5$ be primes. Then the only primitive solutions to*

$$x^{2\ell} + y^{2m} = z^{13}$$

are the trivial ones $(x, y, z) = (\pm 1, 0, 1)$ and $(0, \pm 1, 1)$.

We now complete the proof of this result by showing that $\overline{\rho}_{\mathfrak{f}_{11}, \mathfrak{p}_0}$ is indeed reducible.

Proposition 8.3. *The representation $\overline{\rho}_{\mathfrak{f}_{11}, \mathfrak{p}_0} : G_K \to \mathrm{GL}_2(\mathbb{F}_7)$ is reducible.*

Proof. Suppose $\overline{\rho}_{\mathfrak{f}_{11}, \mathfrak{p}_0}$ is irreducible for a contradiction.

The conductor of $\overline{\rho}_{\mathfrak{f}_{11}, \mathfrak{p}_0}$ is $\mathfrak{N}' = (1), (2), \mathfrak{q}_{13}$ or $2\mathfrak{q}_{13}$. From the irreducibility assumption on $\overline{\rho}_{\mathfrak{f}_{11}, \mathfrak{p}_0}$ and [6, Theorem 3.2.2] ,we conclude there exists a Hilbert newform $g \in S_2(\mathfrak{N}')^{\mathrm{new}}$ such that $\overline{\rho}_{\mathfrak{f}_{11}, \mathfrak{p}_0} \simeq \overline{\rho}_{g, \mathfrak{p}'}$ for some prime $\mathfrak{p}' \mid 7$ in the coefficient field $\mathbb{Q}_g$ of g.

For $\mathfrak{N}' = (1)$ and $\mathfrak{N}' = \mathfrak{q}_{13}$, we have $\dim S_2(\mathfrak{N}')^{\mathrm{new}} = 0$, so $\mathfrak{N}' = (2)$ or $2\mathfrak{q}_{13}$.

For $\mathfrak{N}' = (2)$, we have $\dim S_2(\mathfrak{N}')^{\mathrm{new}} = 1$. The unique newform corresponds to the isogeny class of the base change to K of the elliptic curve W with Cremona label $338b1$. From LMFDB [36, Elliptic Curves over $\mathbb{Q}$], we see that $\overline{\rho}_{W,7}$ is reducible, hence $\overline{\rho}_{\mathfrak{f}_{11},\mathfrak{p}_0} \not\simeq \overline{\rho}_{W,7}|_{G_K}$.

We conclude that $\overline{\rho}_{\mathfrak{f}_{11},\mathfrak{p}_0}$ ramifies at both (2) and $\mathfrak{q}_{13}$, that is $\mathfrak{N}' = 2\mathfrak{q}_{13}$.

Now, a similar argument to the one used in the proof of Proposition 3.2 shows that $\overline{\rho}_{\mathfrak{f}_{11},\mathfrak{p}_0}$ extends to an irreducible representation $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_7)$, and that there is a classical newform $h \in S_2(26)^{\mathrm{new}}$ such that $\overline{\rho} \simeq \overline{\rho}_{h,\mathfrak{p}}$ for some prime $\mathfrak{p} \mid 7$ in $\mathbb{Q}_h$. There are two newforms $h_1, h_2 \in S_2(26)^{\mathrm{new}}$, with rational coefficients, corresponding to the isogeny classes of the elliptic curves W_1 and W_2 with Cremona label $26a1$ and $26b1$ respectively.

The curve W_2 has a 7-torsion point, so $\overline{\rho}_{h_2,7}$ is reducible, hence $\overline{\rho} \not\simeq \overline{\rho}_{h_2,7}$.

Finally, we observe that $a_5(W_1) = -3$ for the prime 5, which is split in K. So, for a prime $\mathfrak{q} \mid 5$ in K, we have

$$\mathrm{Tr}(\overline{\rho}_{h_1,7}|_{G_K}(\mathrm{Frob}_{\mathfrak{q}})) = \mathrm{Tr}(\overline{\rho}_{W_1,7}(\mathrm{Frob}_5)) \equiv -3 \pmod{7}.$$

But, we easily check that $\mathrm{Tr}(\overline{\rho}_{\mathfrak{f}_{11},\mathfrak{p}_0}(\mathrm{Frob}_{\mathfrak{q}})) \equiv 6 \not\equiv -3 \pmod{\mathfrak{p}_0}$, showing that $\overline{\rho} \not\simeq \overline{\rho}_{h_1,7}$.

Since there are no other possible forms h we obtain the desired contradiction. $\qquad\square$

References

[1] S. Anni and S. Siksek, *Modular elliptic curves over real abelian fields and the generalized Fermat equation $x^{2\ell} + y^{2m} = z^p$*, Algebra & Number Theory **10** (2016), no.6, 1147–1172 8, 8

[2] M. A. Bennett and C. M. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math. **56** (2004), no. 1, 23–54. 5

[3] N. Billerey, I. Chen, L. Dembélé, L. Dieulefait, and N. Freitas, *Supporting* `Magma` *program files for this paper*, http://math.univ-bpclermont.fr/~billerey/Research/BCDDF/ 1, 5.8

[4] N. Billerey, I. Chen. L. Dieulefait, and N. Freitas, *A multi-Frey approach to Fermat equations of signature (r, r, p)*, Trans. Amer. Math. Soc. **371** (2019), no. 12, 8651–8677. 1, 1, 2, 2, 4, 4, 4, 5, 5, 5, 5, 6, 7

[5] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. J. Symbolic Comput. **24** (1997), no. 3–4, 235–265. Computational algebra and number theory (London, 1993). 1, 2, 5, 5, 6

[6] C. Breuil, and F. Diamond, *Formes modulaires de Hilbert modulo p et valeurs d'extensions entre caractères galoisiens*, Ann. Sci. Éc. Norm. Supér. (4) **47** (2014), no. 5, 905–974. 8

[7] Y. Bugeaud, M. Mignotte and S. Siksek *A multi-Frey approach to some multi-parameter families of Diophantine equations*, Canadian Journal of Mathematics **60** (2008), 491-519. 2

[8] C. J. Bushnell, G. Henniart, *The local Langlands conjecture for* GL(2), *Grundlehren der Mathematischen Wissenschaften* **335**, Springer-Verlag, Berlin, 2006. xii+347 pp. 5

[9] É. Cali, *Défaut de semi-stabilité des courbes elliptiques dans le cas non ramifié*, Canad. J. Math. **56** (2004), no 4, 673–698. 5

[10] H. Carayol, *Sur les représentations l-adiques associées aux formes modulaires de Hilbert*, Ann. Sci. École Norm. Sup. (4) **19** (1986), no. 3, 409–468. 5, 5

[11] I. Chen and A. Koutsianas, *A modular approach to Fermat equations of signature $(p, p, 5)$ using Frey hyperelliptic curves*, preprint. 5.8, 5.8

[12] E. Costa, N. Mascot, J. Sijsling, J. Voight, *Rigorous computation of the endomorphism ring of a Jacobian*, Math. Comp. **88** (2019), no. 317, 1303–1339. 5

[13] S. R. Dahmen, and S. Siksek, *Perfect powers expressible as sums of two fifth or seventh powers*, Acta Arith. **164** (2014), no. 1, 65–100. 1, 7, 7.1

[14] H. Darmon, *Rigid local systems, Hilbert modular forms, and Fermat's last theorem*, Duke Math. J. **102** (2000), no 3, 413–449. 5.8

[15] L. Dembélé, *An intriguing hyperelliptic Shimura curve quotient of genus* 16. To appear in Algebra and Number Theory. https://arxiv.org/pdf/1906.06772.pdf 6

[16] L. Dembélé, and J. Voight, *Explicit methods for Hilbert modular forms.* Elliptic curves, Hilbert modular forms and Galois deformations, 135–198, Adv. Courses Math. CRM Barcelona, Birkhäuser/Springer, Basel, 2013. 1

[17] L. Dembélé, and A. Kumar, *Examples of abelian surfaces with everywhere good reduction*, Math. Ann. **364** (2016), no. 3-4, 1365–1392. 5.7

[18] F. Diamond, *An extension of Wiles' results*, Modular forms and Fermat's last theorem (Boston, MA, 1995), 475–489, Springer, New York, 1997. 5

[19] J. Burgos Gil and A. Pacetti, *Hecke and Sturm bounds for Hilbert modular forms over real quadratic fields*, Math. Comp. **86** (2017), no. 306, 1949–1978. 6

[20] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Proc. Antwerpen Conference, vol. 2, Lecture Notes in Mathematics, Volume 349, 1973, pp. 143-316, Springer-Verlag. 5

[21] T. Dokchitser, C. Doris 3-*torsion and conductor of genus 2 curves*, Math. Comp. **88** (2019), no. 318, 1913–1927. 5, 5, 5.8

[22] C. Doris, Package for computing the conductor or genus 2 curves. Available at https://cjdoris.github.io/Genus2Conductor/#installation 1

[23] N. Elkies, and A. Kumar, *K3 surfaces and equations for Hilbert modular surfaces*, Algebra Number Theory **8** (2014), no. 10, 2297–2411. 5, 5.7

[24] J. Ellenberg, *Serre's conjecture over* $\mathbb{F}_9$, Ann. of Math. (2) **161** (2005), no. 3, 1111–1142. 5

[25] W. Feit, *The Representation Theory of Finite Groups*, North-Holland, Amsterdam-New York-Oxford, 1982. 3

[26] N. Freitas, *On the Fermat-type equation* $x^3 + y^3 = z^p$, Commentarii Mathematici Helvetici **91** (2016), 295–304. 5

[27] N. Freitas, B. Le Hung, S. Siksek, *Elliptic Curves over Real Quadratic Fields are Modular*, Inventiones Mathematicae **201** (2015), no. 1, 159–206. 6

[28] M. Greenberg, and J. Voight, *Computing systems of Hecke eigenvalues associated to Hilbert modular forms*, Math. Comp. **80** (2011), no. 274, 1071–1092. 1

[29] Haruzo Hida, *p-adic Automorphic Forms on Shimura Varieties*, Springer Monographs in Mathematics, Springer-Verlag, 2004.

[30] C. Khare, and J.-P. Wintenberger, *On Serre's conjecture for* 2-*dimensional mod p representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Ann. of Math. (2) **169** (2009), no. 1, 229–253. 3

[31] M. Kisin, *Moduli of finite flat group schemes, and modularity*, Ann. of Math. (2) **170** (2009), no. 3, 1085–1180. 5

[32] A. Kraus, *Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive*, Manuscripta Math. **69** (1990), no. 4, 353–385. 5

[33] A. Kraus, *Sur l'équation* $a^3 + b^3 = c^p$, Experimental Math. **7** (1998), no. 1, 1–13. 5

[34] P. Kutzko, *The Langlands conjecture for* GL_2 *of a local field*, Ann. of Math. (2) **112** (1980), no. 2, 381–412. 5

[35] Q. Liu, *Courbes stables de genre 2 et leur schéma de modules*, Math. Ann. **295** (1993), no. 2, 201–222. 5

[36] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, http://www.lmfdb.org, 2013. 8

[37] K. Martin, *The Jacquet-Langlands correspondence, Eisenstein congruences, and integral L-values in weight* 2, Math. Res. Lett. **24** (2017), no. 6, 1775–1795. 3.4

[38] J. Nekovář, *Level Raising and Anticyclotomic Selmer Groups for Hilbert Modular Forms of Weight Two*, Canad. J. Math. Vol. **64** (3), 2012, 588–668. 5

[39] K. Ribet, *Non-optimal levels of mod ℓ reducible Galois representations*, CRM Lecture notes, 2010. Available at http://math.berkeley.edu/~ribet/crm.pdf. 3.4

[40] K. Ribet, *Abelian varieties over* $\mathbb{Q}$ *and modular forms*, Modular curves and abelian varieties, 241–261, Progr. Math. **224**, Birkhäuser, Basel, 2004. 5

[41] J.-P. Serre, *Linear representations of finite groups*, Springer-Verlag, New York-Heidelberg, 1977. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.

[42] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Annals of Math. **88** (1968), no. 2, 492–517. 5

[43] Goro Shimura, *The special values of the zeta functions associated with Hilbert modular forms*, Duke Math. J. **45** (1978), no. 3, 637–679. 3

[44] J. Wilson, *Curves of genus 2 with real multiplication by a square root of 5*, PhD thesis, University of Oxford, 1998. 5

[45] H. Yoo, *Non-optimal levels of a reducible* mod ℓ *modular representation*, Trans. Amer. Math. Soc. **371** (2019), no. 6, 3805–3830. 3.4

[46] R. Taylor, *On Galois representations associated to Hilbert modular forms*, Invent. Math. **98** (1989), no. 2, 265–280.

[47] S. Zhang, *Heights of Heegner Points on Shimura Curves*, Annals of Math., Second Series, **153**, no. 1 (2001), 27–147. 5

Université Clermont Auvergne, CNRS, LMBP, F-63000 Clermont-Ferrand, France.

Email address: `nicolas.billerey@uca.fr`

Department of Mathematics, Simon Fraser University, Burnaby, BC V5A 1S6, Canada

Email address: `ichen@sfu.ca`

Department of Mathematics, University of Luxembourg, Maison du Nombre, Avenue de la Fonte, Esch-sur-Alzette L-4364, Luxembourg

Email address: `lassina.dembele@gmail.com`

Departament d'Algebra i Geometria, Universitat de Barcelona, G.V. de les Corts Catalanes 585, 08007 Barcelona, Spain

Email address: `ldieulefait@ub.edu`

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

Email address: `nuno.freitas@icmat.es`