

ON THE GENERALIZED FERMAT EQUATION $x^{13} + y^{13} = z^n$

ALEX J. BEST, SANDER R. DAHMEN, AND NUNO FREITAS

ABSTRACT. Let $n \in \mathbb{Z}_{\geq 2}$. We study the generalized Fermat equation

$$x^{13} + y^{13} = z^n, \quad x, y, z \in \mathbb{Z}, \quad \gcd(x, y, z) = 1.$$

Using a combination of techniques, including the modular method, classical descent, unit sieves, and Chabauty and Mordell–Weil sieve methods over number fields, we show that for $n = 5$ all its solutions (a, b, c) are trivial, i.e. satisfy $abc = 0$. Under the assumption of GRH, we also show that for $n = 7$ there are only trivial solutions. Furthermore, we provide partial results towards solving the equation for general $n \in \mathbb{Z}_{\geq 2}$, in particular that any solution (a, b, c) with $13 \mid c$ is trivial.

1. INTRODUCTION

Let $p, q, r \in \mathbb{Z}_{\geq 2}$ and consider the generalized Fermat equation

$$(1.1) \quad x^p + y^q = z^r, \quad x, y, z \in \mathbb{Z}, \quad \gcd(x, y, z) = 1.$$

See e.g. [2] for an overview, or [19] for a list of solved cases.

In this work, we study (1.1) with exponent triple $(13, 13, p)$, i.e.

$$(1.2) \quad x^{13} + y^{13} = z^p, \quad x, y, z \in \mathbb{Z}, \quad \gcd(x, y, z) = 1$$

(where still $p \in \mathbb{Z}_{\geq 2}$). It suffices to restrict to prime exponent p . The equation has been solved for $p = 2$ in [3] and $p = 3$ in [4], and prior to this work for no other prime exponent p . Our main focus will be on the cases $p = 5$ and $p = 7$, though several partial results will be given for other prime exponents p as well. We will also treat the equation for all p under a natural divisibility condition. Our main result is as follows.

Theorem 1.1. *Let $p \in \{5, 7\}$ and assume GRH if $p = 7$. Then the only solutions to the generalized Fermat equation*

$$(1.3) \quad x^{13} + y^{13} = z^p, \quad x, y, z \in \mathbb{Z}, \quad \gcd(x, y, z) = 1,$$

are the trivial solutions $(\pm 1, \mp 1, 0)$, $(\pm 1, 0, \pm 1)$, and $(0, \pm 1, \pm 1)$.

Date: October 15, 2025.

2020 Mathematics Subject Classification. Primary 11D41; Secondary 11F80, 11G05, 11G10, 11G30.

Key words and phrases. Fermat equations, modularity, Galois representations, Chabauty.

The first two named authors were supported by NWO Vidi grant 639.032.613.

We thank the Max Planck Institute for Mathematics in Bonn for its hospitality on several occasions, which enabled the last two named authors to collaborate on this paper.

Solving generalized Fermat equations (with unit coefficients) seems to be grinding to a halt. This work illustrates how combining and strengthening a variety of modern techniques can overcome difficulties and thereby still push the boundary of completely resolved interesting GFE's.

It is natural to distinguish between two cases of solutions (a, b, c) to (1.2), namely $13 \nmid c$ and $13 \mid c$. The latter case can be handled for any exponent, meaning we will prove the following theorem.

Theorem 1.2. *For all integers $n \geq 2$, the equation*

$$(1.4) \quad x^{13} + y^{13} = z^n, \quad x, y, z \in \mathbb{Z}, \quad \gcd(x, y, z) = 1$$

has no non-trivial solutions (a, b, c) such that $13 \mid c$ (or equivalently $13 \mid a + b$).

The outline of this paper is as follows. In Section 2, we prove Theorem 1.2 by Hilbert modular methods with a multi-Frey approach. In doing so, we extend the general applicability of a Frey curve studied in [6], which could be of independent interest in other contexts. In Section 3, we reduce the resolution of (1.2) in case $13 \nmid c$ for a fixed prime p to determining rational points on many hyperelliptic curves. We introduce strong ‘unit sieves’ in Section 4, to reduce the amount of hyperelliptic curves (per prime p) from the previous section that need to be considered. First, without the modular methods, we reduce to two hyperelliptic curves. Next, with the modular method, we reduce further to one curve. For $p = 5$ and $p = 7$ (assuming GRH for the latter), we use Chabauty methods in Section 5 to determine all rational points on the final hyperelliptic curve left, thereby completing the proof of Theorem 1.1. Finally, we look back, and discuss in Section 6 the (non-)applicability of alternative methods, illustrating the complementarity of our methods used.

Notation and conventions. For a number field F we denote its ring of integers by $\mathcal{O}_F$.

Let ζ be a primitive 13-th root of unity and let $L = \mathbb{Q}(\zeta)$. Let K be the cubic subfield of L . Explicitly, let $\rho := \zeta + \zeta^{-1} + \zeta^5 + \zeta^{-5}$, then $K = \mathbb{Q}(\rho)$ and $\rho^3 + \rho^2 - 4\rho + 1 = 0$. Note that K is totally real, with a fundamental system of units for its ring of integers given by ρ and $1 - \rho$.

2. A MULTI-FREY APPROACH TO THEOREM 1.2

In [6], the authors study in great detail two Frey curves (originally introduced in [15, 16]) associated with the Fermat-type equations of the form

$$(2.1) \quad x^{13} + y^{13} = dz^p.$$

More precisely, one Frey curve $E_{a,b}$ is defined over $\mathbb{Q}(\sqrt{13})$ and the other $F_{a,b}$ is defined over the totally real cubic subfield K of $L = \mathbb{Q}(\zeta)$; see [6, §7] for definitions and various properties. The exposition in *loc. cit.* is oriented towards the case $d = 3$, but most of the constructions and results there apply for $d = 1$, including the definitions of the Frey curves, as these are built from factors of the left hand side of (2.1). Moreover, in *loc. cit.* there is the underlying condition that all primes $\ell \mid d$ satisfy $\ell \not\equiv 1 \pmod{13}$, which is clearly true for $d = 1$.

Let $\mathfrak{q}_{13}$ be the unique prime in K above 13. Note that 2 is inert in both $\mathbb{Q}(\sqrt{13})$ and K .

The purpose of this section is to prove Theorem 1.2, for which we have two proofs. The more direct proof follows an application of the modular method using only the Frey curve $F_{a,b}/K$. This requires elimination of Hilbert newforms at levels $2\mathfrak{q}_{13}$ and $2^3\mathfrak{q}_{13}$, which makes the proof computationally heavy. The less direct proof, which we will give below, uses the multi-Frey technique combining both $E_{a,b}$ and $F_{a,b}$. The reasons for opting to present the less direct proof are the following:

- (i) Some of the results in [6, §7.1] do not apply directly to our main case of interest, i.e. $d = 1$ (and $13|c$, equivalently $13|a+b$) in (2.1), because they rely on the additional assumption $3|a+b$ or $3|d$, which we do not have. Thus our proof requires establishing some properties of $E_{a,b}$ with arguments independent of d , expanding the usefulness of this Frey curve.
- (ii) In the part of the argument that uses $F_{a,b}$, we only need to do elimination of newforms at level $2\mathfrak{q}_{13}$, reducing significantly the computational time of the proof. Furthermore, the more interesting parts of the elimination step in the more direct proof occurs at the level $2\mathfrak{q}_{13}$ and so it is also present in the proof we give below.

Proof of Theorem 1.2. It suffices to prove Theorem 1.2 for all $n = p$ a prime number. For $p = 2$ and $p = 3$ it follows, respectively, from [3, Theorem 1.1] and [4, Theorem 1.5]. For $p = 13$, it follows from Fermat's Last Theorem; in fact, Kummer's classical 19-th century work suffices for this, as 13 is a regular prime ($L = \mathbb{Q}(\zeta)$ even has trivial class group). So we can and will assume $n = p \geq 5$ prime and $p \neq 13$ for the rest of this section.

Suppose that (a, b, c) is a primitive solution to (1.4) with exponent p . Let $E = E_{a,b}$ over $\mathbb{Q}(\sqrt{13})$ be the Frey curve attached to (a, b, c) as defined in [6, p. 8666]. We denote by $\rho_{E,p}$ the p -adic Galois representation attached to E and by $\bar{\rho}_{E,p}$ the mod p reduction of $\rho_{E,p}$, i.e., the p -torsion Galois representations attached to E .

Proposition 2.1. *The representation $\bar{\rho}_{E,p}$ is irreducible.*

Proof. Set $M = \mathbb{Q}(\sqrt{13})$ and recall that 2 is inert in M . Let M_2 be the completion of M at 2 and M_2^{un} its maximal unramified extension. Let also $I_2 \subset G_M$ be an inertia subgroup at 2.

For $p \geq 7$ the result follows directly from [6, Proposition 8], so we are left with $p = 5$.

Suppose that $\bar{\rho}_{E,5}$ is reducible, that is,

$$\bar{\rho}_{E,5} \simeq \begin{pmatrix} \theta & \star \\ 0 & \theta' \end{pmatrix} \quad \text{with} \quad \theta, \theta' : G_M \rightarrow \mathbb{F}_5^* \quad \text{satisfying} \quad \theta\theta' = \chi_5,$$

where χ_5 is the mod 5 cyclotomic character. Thus the order of $\bar{\rho}_{E,5}(I_2)$ divides $80 = 2^4 \cdot 5$.

From the proof of [15, Proposition 3.3] we know that E has potentially good reduction at 2 and $v_2(\Delta_m) = 4$ where Δ_m is the discriminant of a minimal model for E . Let N/M_2^{un} be the extension of minimal degree over which E/M_2 acquires good reduction. Denote by $e(E)$ the degree of N/M_2^{un} . By Neron–Ogg–Shafarevich we know that $\rho_{E,5}(I_2) \simeq \text{Gal}(N/M_2^{\text{un}})$ has order $e(E)$.

Since $v_2(\Delta_m) \not\equiv 0 \pmod{3}$ it follows from [17, Théorème 3] that $3 | e(E)$ and $e(E) | 24$. Moreover, since $5 \nmid e(E)$, reduction modulo 5 preserves the order of $\rho_{E,5}(I_2)$, thus $\bar{\rho}_{E,5}(I_2)$ also has order $e(E)$, giving a contradiction because $3 \nmid 80$. $\square$

Proposition 2.2. *Assume $p \geq 5$ and $p \neq 13$. Then we have*

$$(2.2) \quad \bar{\rho}_{E,p} \simeq \bar{\rho}_{Z,p}$$

where the elliptic curve Z equals $E_{1,-1}$, $E_{1,0}$, or $E_{1,1}$.

Proof. For $p = 11$ and $p \geq 17$ this follows directly from [6, Proposition 9]. For $p = 7$ the same proposition includes the additional possibility that $\bar{\rho}_{E,p} \simeq \bar{\rho}_{g,\mathfrak{p}_7}$ for a Hilbert newform g over $\mathbb{Q}(\sqrt{13})$ of parallel weight 2, trivial character, level $2^3 \cdot 13$, with field of coefficients $\mathbb{Q}(\sqrt{2})$, and a choice of prime $\mathfrak{p}_7$ above 7 in this field. However, as explained in Remark 7.4 of *loc. cit* and proved in [5, Proposition 6.1] we have $\bar{\rho}_{g,\mathfrak{p}_7} \simeq \bar{\rho}_{E_{1,-1},7}$ which is already among the cases in the statement, completing the proof for $p = 7$ as well.

Note that the conclusion of [6, Proposition 9] also holds for $p = 5$ under the additional hypothesis $3 \mid a+b$ which we do not have. This hypothesis is there to guarantee irreducibility of $\bar{\rho}_{E,5}$ via [6, Proposition 8] and consequently apply level lowering [6, Lemma 7]. In our setting, we have irreducibility of $\bar{\rho}_{E,5}$ by Proposition 2.1 and everything else in *loc. cit* applies exactly the same, yielding the result for $p = 5$. $\square$

We remark that all the results above did not use the assumption $13 \mid a+b$ in Theorem 1.2.

Theorem 2.3. *Let (a, b, c) be a solution to (1.4) with exponent $p \geq 5$, $p \neq 13$.*

If $13 \mid a+b$ then $4 \mid a+b$.

Proof. Let $E = E_{a,b}$ be the Frey curve associated with (a, b, c) .

From Proposition 2.2, we know that $\bar{\rho}_{E,p} \simeq \bar{\rho}_{Z,p}$, where Z is $E_{1,-1}$, $E_{1,0}$ or $E_{1,1}$.

Let K^+ be the maximal totally real subfield of $L = \mathbb{Q}(\zeta)$ and π denote the unique prime ideal in K^+ above 13. From [15, Proposition 3.1], the base change curves $E_{1,0}/K^+$ and $E_{1,1}/K^+$ have bad additive reduction at π while $E_{1,-1}/K^+$ has good reduction at π . Furthermore, $E_{a,b}/K^+$ also has good reduction at π because $13 \mid a+b$. Therefore, for $Z = E_{1,0}$ and $Z = E_{1,1}$, restricting the isomorphism $\bar{\rho}_{E,p} \simeq \bar{\rho}_{Z,p}$ to G_{K^+} gives a contradiction because $\bar{\rho}_{E,p}|_{G_{K^+}}$ is unramified at π whilst $\bar{\rho}_{Z,p}|_{G_{K^+}}$ ramifies at π . We conclude that $\bar{\rho}_{E,p} \simeq \bar{\rho}_{E_{1,-1},p}$. Now the proof of part (B) in [6, Theorem 7] applies exactly the same to conclude $4 \mid a+b$.

(The argument in the proof of [6, Theorem 7] part (B) is purely local at 2 and so independent of the condition $3 \mid d$ in *loc. cit*; indeed, this condition is used there only to guarantee $\bar{\rho}_{E,p} \simeq \bar{\rho}_{E_{1,-1},p}$, which we established independently of d .) $\square$

To complete the proof of Theorem 1.2 we will now work with the Frey curve $F = F_{a,b}/K$ as defined in [6, p. 8669]. The results in *loc. cit* regarding $F_{a,b}$ are stated for general d (in particular, independently of $3 \mid d$) and apply in our setting directly.

Assume $13 \mid a+b$. From Theorem 2.3 we have $4 \mid a+b$.

From lemmas 8, 9, 10, 11 and Theorem 8 of [6] it follows that $\bar{\rho}_{F,p}$ is irreducible and

$$\bar{\rho}_{F,p} \simeq \bar{\rho}_{f,\mathfrak{p}},$$

where f is a Hilbert newform over K of parallel weight 2, trivial character, level $2\mathfrak{q}_{13}$, and $\mathfrak{p}$ a prime above p in the field of coefficients of f . We compute this space using Magma [8].

There are four newforms, say f_1, f_2, f_3 and f_4 , in the space. The forms f_1, f_2 have rational coefficients and the forms f_3, f_4 have cubic coefficients fields. Furthermore, the form f_3 is the form denoted by $\mathfrak{f}_{11}$ in [5, §8] and its field of coefficients $\mathbb{Q}_{f_3}$ is the maximal totally real subfield of $\mathbb{Q}(\zeta_7)$. Let $\mathfrak{p}_7$ denote the unique prime in $\mathbb{Q}_{f_3}$ above 7.

Using **Magma** and standard trace comparisons at the auxiliary primes $q = 5, 7, 11$ eliminates the four newforms for all exponents p except for f_1 and f_3 when $p = 7$. In other words, it could still be possible that $\bar{\rho}_{F,7} \simeq \bar{\rho}_{f_1,7}$ or $\bar{\rho}_{F,7} \simeq \bar{\rho}_{\mathfrak{f}_{11},\mathfrak{p}_7}$. We claim that both $\bar{\rho}_{f_1,7}$ and $\bar{\rho}_{\mathfrak{f}_{11},\mathfrak{p}_7}$ are reducible. Therefore the previous isomorphisms cannot happen because $\bar{\rho}_{F,7}$ is irreducible.

We now prove the claim. Let W be the base change to K of the elliptic curve with Cremona label 26b1. The conductor of W is $2\mathfrak{q}_{13}$ and W is modular because K is cubic and totally real [14]. Thus either f_1 or f_2 correspond to W via modularity and comparing the trace of Frobenius at $3\mathcal{O}_K$ shows that f_1 corresponds to W . This curve has a 7-torsion point over K (in fact over $\mathbb{Q}$) therefore $\bar{\rho}_{f_1,7}$ is reducible. Finally, the representation $\bar{\rho}_{f_3,\mathfrak{p}_7}$ is also reducible by [5, Proposition 8.3], establishing the claim.

Remark 2.4. We note that we actually have $\bar{\rho}_{f_1,7} \simeq \bar{\rho}_{f_3,\mathfrak{p}_7}$ allowing for a variation of the proof of the claim. Indeed, the previous isomorphism follows from an application of the socle method in [5, §6]. Therefore, the claim follows if we show that any of the two representations is reducible, which we can do by using either of the arguments in the proof.

3. REDUCTION TO HYPERELLIPTIC CURVES

Fix an odd prime p . In this section we will reduce the resolution of our main equation of interest (1.2) to determining points on finitely many hyperelliptic curves of genus $(p-1)/2$ over the cubic number field K .

The polynomial $x^{13} + y^{13} \in \mathbb{Z}[x, y]$ factorizes over $\mathbb{Q}$ as

$$x^{13} + y^{13} = (x + y)\phi_{13}$$

where $\phi_{13} = \frac{x^{13} + y^{13}}{x + y} \in \mathbb{Z}[x, y]$ is the two variable 13-th cyclotomic polynomial. Over K we get a further factorization of the form

$$x^{13} + y^{13} = F \cdot \sigma(F) \cdot \sigma^2(F) \cdot (x + y)$$

where $F \in \mathcal{O}_K[x, y]$ is homogeneous of degree 4 and σ is a generator for $\text{Gal}(K/\mathbb{Q})$. Explicitly, we will choose

$$F := x^4 + \rho x^3 y + (\rho^2 + \rho - 1)x^2 y^2 + \rho x y^3 + y^4.$$

As this binary form is symmetric, one readily finds convenient identities for it. Namely, define binary forms

$$G := x + y, \quad H := x^2 + \frac{1}{5}(-2\rho^2 + 8)xy + y^2$$

and constant

$$d := \frac{1}{4\rho^2} = \left(\frac{\rho^2 + \rho - 4}{2}\right)^2, \quad \text{noting } 1 + d = (\rho^2 - \rho + 1) \left(\frac{\rho^2 + \rho - 5}{2}\right)^2.$$

Then we have the identity

$$(3.1) \quad (1 + d)H^2 = F + dG^4.$$

Now let $(a, b, c) \in \mathbb{Z}^3$ be a solution to (1.2). Since a, b are coprime, we have (see e.g. [12, Lemma 2.2]) the elementary properties that

$$\gcd(a + b, \phi_{13}(a, b)) \in \{1, 13\}$$

and

$$(3.2) \quad \gcd(a + b, \phi_{13}(a, b)) = 13 \Leftrightarrow 13 \mid c \Leftrightarrow 13 \mid a + b \Leftrightarrow 13 \mid \phi_{13}(a, b) \Leftrightarrow 13 \parallel \phi_{13}(a, b).$$

If the solution satisfies $13 \nmid a + b$, then by classical descent, we have

$$F(a, b) = ez_1^p \text{ and } G(a, b) = z_2^p$$

for certain $e, z_1, z_2 \in \mathcal{O}_K$ with e a unit (and actually $z_2 \in \mathbb{Z}$ nonzero). Writing

$$Y' := \frac{H(a, b)}{z_2^{2p}}, \quad X' := \frac{z_1}{z_2^4},$$

we see that specializing (3.1) at (a, b) and dividing by z_2^{4p} , we arrive at

$$C'_{p,e} : (1 + d)Y'^2 = eX'^p + d.$$

This defines a hyperelliptic curve $C'_{p,e}$ of genus $(p - 1)/2$. Via rescaling $(X', Y') \mapsto (X, Y) := (X_0 X', Y_0 Y')$ where

$$(3.3) \quad X_0 := 4(\rho^2 - \rho + 1), \quad Y_0 := 2^{p-1}(\rho^2 - \rho + 1)^{(p+1)/2}(\rho^2 + \rho - 5),$$

it is isomorphic to the curve given by the $\mathcal{O}_K$ -integral model

$$(3.4) \quad C_{p,e} : Y^2 = eX^p + 4^{p-1}(\rho^2 - \rho + 1)^p \rho^{-2}.$$

For later reference, we note the relation

$$(3.5) \quad \frac{(X')^p}{(Y')^2} = \frac{(X/X_0)^p}{(Y/Y_0)^2} = \frac{F(a, b)}{eH(a, b)^2}.$$

Determining $C_{p,e}(K)$ for all units $e \in \mathcal{O}_K^*$ up to p -th powers solves (1.2) for the case $13 \nmid a + b$. Note (for any p, e) that $C_{p,e}(K)$ is never empty, as it contains the point at infinity, denoted ∞ .

The case $e = 1$ is of special interest to us, and we write $C_p := C_{p,1}$ and $C'_p := C'_{p,1}$. We see that also $(1, \pm 1)$ is contained in $C'_p(K)$. So that

$$(3.6) \quad \{(X_0, \pm Y_0), \infty\} \subset C_p(K).$$

We note that the trivial solutions (a, b, c) with $ab = 0$ (i.e. $(\pm 1, 0, \pm 1)$ and $(0, \pm 1, \pm 1)$) give rise to the point (X_0, Y_0) . Conversely, any potential solution (a, b, c) to (1.2) that gives rise to one of the three rational points in (3.6), can readily be checked using (3.5) (with the LHS being $1 + d$ for the point at infinity), to be a trivial solution with $ab = 0$.

Now, the possible units e can be restricted by unit sieves, as explained in Section 4 below. A ‘surviving’ unit ϵ by the sieve gives rise to a unit $e := \text{Norm}_{L/K}(\epsilon)$ here. We employ a first sieve, introduced in Section 4.2, for all primes $5 \leq p \leq 47$, $p \neq 13$. It turns out that for every such prime p , it remains to consider only two units up to p -th powers. These include $e = 1$ due to trivial solutions, and another ‘extraneous’ unit; see (4.9) for the latter. Explicitly, for $p = 5$, it suffices to consider the two units:

$$e \in \{1, (\rho(1 - \rho))^{-1}\}.$$

And for $p = 7$, it suffices to consider the two units:

$$e \in \{1, (\rho(1 - \rho))^3\}.$$

A further unit sieve, given in Section 4.3, will eliminate the extraneous unit for $p = 5, 7$ as well as for several larger primes p . We will discuss K -rational points on C_p (i.e. the $e = 1$ case) for $p = 5, 7, 11$ in Section 5. There we will completely determine $C_p(K)$ for $p = 5$ and (assuming GRH) for $p = 7$, which then finished the proof of Theorem 1.1.

4. THE UNIT SIEVE

Throughout this section, let p denote a rational prime with $p \neq 2, 3, 13$. The arguments in this section are inspired by the sieves in [12, §4] and [5, §7]. The key difference is that here we will work locally at p , which is one of the exponents in (1.2), whilst in *loc. cit.* all primes used in the sieve are different from the exponents. This allows us to work modulo p^2 , resulting in a highly effective sieve.

4.1. Factorization and extraneous unit. Suppose (a, b, c) is a solution to (1.2). We have the factorization in $\mathcal{O}_L$,

$$(4.1) \quad a^{13} + b^{13} = (a + b)\phi_{13}(a, b) = (a + b) \prod_{k=1}^{12} (a + \zeta^k b) = c^p.$$

We recall from [16, §2.1] several elementary facts regarding (4.1). Let $\mathfrak{p}_{13}$ be the unique prime in L above 13 and denote by $v_{\mathfrak{p}_{13}}$ its associated valuation satisfying $v_{\mathfrak{p}_{13}}(13) = 12$. Since a, b are coprime, the integers $a + b$ and $\phi_{13}(a, b)$ are coprime away from 13 and if $13 \mid a + b$ then $13 \parallel \phi_{13}(a, b)$. Furthermore, the factors $a + \zeta^k b$ for $1 \leq k \leq 12$ are pairwise coprime away from $\mathfrak{p}_{13}$, and satisfy $v_{\mathfrak{p}_{13}}(a + \zeta^k b) = 1$ when $13 \mid a + b$. Moreover, all primes $\ell \neq 13$ dividing $\phi_{13}(a, b)$ satisfy $\ell \equiv 1 \pmod{13}$.

Therefore, from (4.1) and classical descent, we have

$$(4.2) \quad a + \zeta b = \begin{cases} \epsilon \gamma^p & \text{if } 13 \nmid a + b \\ \epsilon(1 - \zeta) \gamma^p & \text{if } 13 \mid a + b, \end{cases}$$

for some $\epsilon \in \mathcal{O}_L^*$ and $\gamma \in \mathcal{O}_L$; and also (recalling $p \neq 2$),

$$(4.3) \quad a + b = \begin{cases} \delta^p & \text{if } 13 \nmid a + b \\ 13^{pj-1} \delta^p & \text{if } 13 \mid a + b, \end{cases}$$

for some $\delta \in \mathbb{Z}$ and $j \geq 1$.

Moreover, if $p \mid \phi_{13}(a, b)$ (and hence $p \mid a^{13} + b^{13}$) then $p \equiv 1 \pmod{13}$. From now on assume, next to $p \neq 2, 3, 13$, that $p \not\equiv 1 \pmod{13}$. Then $p \nmid \phi_{13}(a, b)$, and consequently $\mathfrak{p} \nmid a + \zeta^k b$ for $1 \leq k \leq 12$ and all primes $\mathfrak{p} \mid p$ in L . Let $p\mathcal{O}_L = \mathfrak{p}_1 \cdots \mathfrak{p}_s$ be the prime factorization of the prime p in L . We can reduce (4.2) modulo $\mathfrak{p}_i^2$, and from $\mathfrak{p}_i \nmid a + \zeta b$ it follows that $a + \zeta b \pmod{\mathfrak{p}_i^2}$ is invertible in $\mathcal{O}_L/\mathfrak{p}_i^2$. Since the order of the unit group of $\mathcal{O}_L/\mathfrak{p}_i^2$ is divisible by p , the condition of being a p -th power mod $\mathfrak{p}_i^2$ is nontrivial (note that working only mod $\mathfrak{p}_i$ would give a trivial condition).

By inspection, we easily spot the following solutions to (4.2) with $\gamma = \pm 1$:

- (i) $(a, b) = \pm(1, 0)$ with $\epsilon = 1$;
- (ii) $(a, b) = \pm(0, 1)$ with $\epsilon = \zeta$;
- (iii) $(a, b) = \pm(1, 1)$ with $\epsilon = 1 + \zeta$;
- (iv) $(a, b) = \pm(1, -1)$ with $\epsilon = 1$.

Note that (i), (ii), and (iii) correspond to the case $13 \nmid a + b$, and (iv) corresponds to the case $13 \mid a + b$.

Of course, replacing (ϵ, γ) by $(-\epsilon, -\gamma)$ in each case above will also give solutions. But clearly, in (4.2) we only need to consider ϵ up to p -th powers. We have $pk \equiv 1 \pmod{13}$ for some $k \in \mathbb{Z}$ (since $p \neq 13$), which implies $\zeta = (\zeta^k)^p$. So we see that the unit ϵ in solutions (i) and (ii) are the same up to p -th powers; also ϵ and $-\epsilon$ are the same modulo p -th powers.

In the case that $13 \mid a + b$, solution (iv) of course also satisfies (4.3) (with $\delta = 0$). There seems no a priori reason, for general p , to expect any other unit than $\epsilon = 1$ (up to p -th powers) from solution (iv) to survive the sieve modulo p^2 below.

Let us turn to the case $13 \nmid a + b$. When 2 is not a p -th power mod p^2 , the solution (iii) does not satisfy (4.3), so we do not expect the corresponding unit $\epsilon = 1 + \zeta$ to survive the sieve modulo p^2 below in general. However (up to p -th powers, as usual), next to the unit $\epsilon = 1$, there turns out to be a less obvious solution to (4.2) which will give rise to a unit ϵ_0 that will survive the sieve in general (in the case $13 \nmid a + b$ under consideration).

Indeed, to illustrate this for $p = 5$, we have

$$(4.4) \quad 13^2 - \zeta 13^2 = \epsilon_0 \gamma_0^5, \quad \text{where} \quad \gamma_0 := (1 - \zeta)^5, \quad \epsilon_0 := 13^2 / (1 - \zeta)^{24}.$$

Although the pair $(a, b) = (13^2, -13^2)$ does not satisfy $13 \nmid a + b$, this is not detectable when working modulo 25. This shows that for $a \equiv 13^2 \pmod{5^2}$ and $b \equiv -13^2 \pmod{5^2}$, the modulo 25 sieve can never discard the unit ϵ_0 ; trying to sieve at additional primes will also not eliminate this unit for the same reasons.

In the general case of exponent $p \geq 5$, considering still the case of solutions with $13 \nmid a + b$, we have that apart from the unit 1 there is always at least one other extraneous unit surviving the sieve as follows (all up to p -th powers of course). Note that we have the unit $\mu_0 := 13 / (1 - \zeta)^{12} \in \mathcal{O}_L^*$, and hence for every $k \in \mathbb{Z}$ the useful identity

$$(4.5) \quad \frac{\mu_0^k}{1 - \zeta} = \frac{13^k}{(1 - \zeta)^{12k+1}}.$$

For any $k \in \mathbb{Z}$ such that

$$(4.6) \quad 12k \equiv -1 \pmod{p},$$

which has a unique solution modulo p , we get of course that

$$\gamma_0 := (1 - \zeta)^{(12k+1)/p} \in \mathcal{O}_L.$$

Now the extraneous unit

$$(4.7) \quad \mu := \mu_0^k = \frac{13^k}{(1 - \zeta)^{12k}} \quad (\text{where } 12k \equiv -1 \pmod{p})$$

survives the unit sieve, since from (4.5) we see that

$$13^k - \zeta 13^k = \mu \gamma_0^p.$$

For later reference, we note that

$$(4.8) \quad \text{Norm}_{L/K}(\mu_0) = \text{Norm}_{L/K} \left(\frac{13}{(1-\zeta)^{12}} \right) = \left(\frac{13}{\text{Norm}_{L/K}(1-\zeta)^3} \right)^4 = (\rho(1-\rho))^{-8}.$$

For $j \in \mathbb{Z}$ with $j \equiv -8k \pmod{p}$, the condition (4.6) is equivalent to $3j \equiv 2 \pmod{p}$. For the norm (from L to K) of the extraneous unit $\mu = \mu_0^k$, up to p -th powers, we therefore get

$$(4.9) \quad \text{Norm}_{L/K}(\mu) = (\rho(1-\rho))^j \pmod{\mathcal{O}_K^{*p}}, \quad 3j \equiv 2 \pmod{p}.$$

In particular, for $p = 5$ we can take $j = -1$, and for $p = 7$ we can take $j = 3$.

4.2. The sieve without modular information. We recall that $p \neq 2, 13$ and $p \not\equiv 1 \pmod{13}$. Let $p\mathcal{O}_L = \mathfrak{p}_1 \cdots \mathfrak{p}_s$ be the factorization of p in L .

Case (I). We first apply the sieve in the case $13 \nmid a + b$.

Let $\mathcal{P}$ be the set of pairs (α, β) where $0 \leq \alpha \leq \beta \leq p^2 - 1$ such that at most one of α, β is a multiple of p , and $\alpha + \beta$ is a p -th power in $\mathbb{Z}/p^2\mathbb{Z}$; we assumed $\alpha \leq \beta$ by the symmetry in x, y of (1.2).

Let $M_i := (\mathcal{O}_L/\mathfrak{p}_i^2)^*$ and define $\epsilon_i := \epsilon_i(\alpha, \beta) = \alpha + \beta\zeta \pmod{\mathfrak{p}_i^2}$ for $(\alpha, \beta) \in \mathcal{P}$. Since α, β are not both divisible by p and $p \not\equiv 1 \pmod{13}$, the properties of ϕ_{13} mentioned in the paragraph following (4.1) guarantee that $\epsilon_i \in M_i$. Let $\bar{\epsilon}_i$ denote the canonical image of ϵ_i in M_i/M_i^p and consider

$$\begin{aligned} \phi : \mathcal{P} &\rightarrow \prod M_i/M_i^p \\ (\alpha, \beta) &\mapsto (\bar{\epsilon}_1, \dots, \bar{\epsilon}_s). \end{aligned}$$

We also have the standard reduction maps $\pi_i : \mathcal{O}_L^* \rightarrow M_i/M_i^p$, which give rise to a map

$$\begin{aligned} \pi : \mathcal{O}_L^*/\mathcal{O}_L^{*p} &\rightarrow \prod M_i/M_i^p \\ [\epsilon] &\mapsto (\pi_1(\epsilon), \dots, \pi_s(\epsilon)) \end{aligned}$$

where $[\epsilon] := \epsilon \pmod{\mathcal{O}_L^{*p}} \in \mathcal{O}_L^*/\mathcal{O}_L^{*p}$ and the map is well defined by the representative $\epsilon \in \mathcal{O}_L^*$. Note that for a solution (a, b, c) to (1.2) satisfying (4.2) for some γ, ϵ , there exists a pair $(\alpha, \beta) \in \mathcal{P}$ (congruent to (a, b) or (b, a) modulo p^2) such that

$$\phi(\alpha, \beta) = \pi([\epsilon]).$$

Using **Magma**, we explicitly construct both maps π and ϕ . As $\mathcal{P}$ is rather smaller (e.g. for $p = 5, 7$ of orders 62, 171 resp.) than $\mathcal{O}_L^*/\mathcal{O}_L^{*p}$ (e.g. for $p = 5, 7$ of orders $5^5 = 3125, 7^5 = 16807$ resp.), we do not compute the intersection $\pi(\mathcal{O}_L^*/\mathcal{O}_L^{*p}) \cap \phi(\mathcal{P})$. Instead, we simply compute the inverse image of $\phi(\mathcal{P})$ under π . In practice, we assert that $\#\ker(\pi) = 1$, and then for every $u \in \phi(\mathcal{P})$, we check whether there is a (necessarily unique) $\mathcal{E} \in \mathcal{O}_L^*/\mathcal{O}_L^{*p}$ such that $\pi(\mathcal{E}) = u$, and if so, store a representative ϵ for the class $\mathcal{E} = [\epsilon]$. The union of those ϵ is the output of the sieve.

We ran the sieve for all primes p in the range $5 \leq p \leq 43$, $p \neq 13$. For $p = 5$, after running the sieve, we have (up to 5-th powers) two surviving units:

$$\epsilon = 1 \quad \text{and} \quad \epsilon = -2\zeta^{11} - 4\zeta^{10} - 3\zeta^9 - 4\zeta^8 - 2\zeta^7 - 4\zeta^5 - 5\zeta^4 - \zeta^3 - \zeta^2 - 5\zeta - 4.$$

The second unit is indeed equal to $\mu = 13^2/(1-z)^{24}$ up to multiplication with a fifth power of a unit (the latter unit can be calculated to be $-2\zeta^{11}-2\zeta^{10}+\zeta^9-3\zeta^8-\zeta^7-\zeta^6-\zeta^5-\zeta^4-3\zeta^3+\zeta^2-2\zeta-2$).

Similarly, for all other primes in our range, we also have as output for our sieve that, up to p -th powers, there are only 2 units surviving, namely 1 and the extraneous unit.

Case (II). We now apply the sieve in the case $13 \mid a+b$. There are only two differences:

(a) Due to (4.3), the set $\mathcal{P}$ is the set of pairs (α, β) where $0 \leq \alpha \leq \beta \leq p^2 - 1$ such that at most one of α, β is a multiple of p , and $13(\alpha + \beta)$ is a p -th power in $\mathbb{Z}/p^2\mathbb{Z}$.

(b) Note that $(1 - \zeta)$ is invertible mod $\mathfrak{p}_i$. The map ϕ is defined instead using the quantities

$$\epsilon_i := (\alpha + \beta\zeta)(1 - \zeta)^{-1} \pmod{\mathfrak{p}_i^2}.$$

As before, with the help of **Magma** we apply the sieve to all primes $5 \leq p \leq 47$, $p \neq 13$. In this case, for all primes in our range, the only unit surviving the sieve is $\epsilon = 1$ (up to p -th powers), except when $p = 17$. For the latter prime, we get two units (including the trivial one of course) in (II). Presumably, the non-trivial unit can be eliminated by sieving at another prime. However, in light of the resolution when $13 \mid a+b$ in Theorem 1.2, we will not pursue this here.

4.3. The sieve with modular information. We will now eliminate the extraneous unit μ given in (4.7) for a range of primes p , including $p = 5, 7$. For this, we will combine modulo q information, for some auxiliary prime q , from the above sieve with that of the Frey curve $E_{a,b}/\mathbb{Q}(\sqrt{13})$ from Section 2.

Let $p = 5$ or 7 . We start by extracting modulo $q = 19$ information from the sieve. Since $p \nmid 19 - 1$, we let $\mathcal{P}$ be the set of pairs $(a, b) \neq (0, 0)$ with $0 \leq a \leq b \leq 18$. Note that 19 is inert in $L = \mathbb{Q}(\zeta)$ and let $M_1 := (\mathcal{O}_L/19\mathcal{O}_L)^*$. For the mod $q = 19$ situation, we consider the map

$$\begin{aligned} \phi : \mathcal{P} &\rightarrow M_1/M_1^p \\ (a, b) &\mapsto \overline{a + b\zeta} \pmod{19}. \end{aligned}$$

We also have, as before, the canonical map (for the newly defined M_1)

$$\pi : \mathcal{O}_L^*/\mathcal{O}_L^{*p} \rightarrow M_1/M_1^p.$$

Using **Magma**, we find that, for $p = 5$ and $p = 7$, the pairs in $\mathcal{P}$ satisfying $\phi(a, b) = \pi([\mu])$ are

$$\mathcal{L} = \{(a, 19 - a) \mid a \in \{1, 2, \dots, 9\}\}.$$

Now let (a, b, c) be a solution to (1.2) with $p = 5$ or $p = 7$ satisfying $13 \nmid a + b$. Assume that after descent it gives rise to the unit $\epsilon = \mu$ in (4.2). Thus $(a \bmod 19, b \bmod 19)$ (or the swapped pair) is in $\mathcal{L}$.

We now consider the Frey curve $E_{a,b}/\mathbb{Q}(\sqrt{13})$ attached to (a, b, c) . From Proposition 2.2 it follows that $\bar{\rho}_{E_{a,b,p}}$ is isomorphic to $\bar{\rho}_{E_{1,0,p}}$, $\bar{\rho}_{E_{1,1,p}}$ or $\bar{\rho}_{E_{1,-1,p}}$. Since $13 \nmid a + b$, from the proof of Theorem 2.3, we have $\bar{\rho}_{E_{a,b,p}} \not\cong \bar{\rho}_{E_{1,-1,p}}$, hence

$$\bar{\rho}_{E_{a,b,p}} \simeq \bar{\rho}_{E_{1,0,p}} \quad \text{or} \quad \bar{\rho}_{E_{a,b,p}} \simeq \bar{\rho}_{E_{1,1,p}}.$$

Note that 19 is inert in $\mathbb{Q}(\sqrt{13})$. Since $19 \not\equiv 1 \pmod{13}$ it follows from [6, Lemma 5] that $E_{a,b}$ has good reduction at 19 and by taking traces of Frobenius we obtain, respectively,

$$(4.10) \quad a_{19}(E_{a,b}) \equiv -9 \pmod{p} \quad \text{or} \quad a_{19}(E_{a,b}) \equiv 3 \pmod{p}.$$

On the other hand, for all $(a, b) \in \mathcal{L}$, we compute that

$$a_{19}(E_{a,b}) \equiv 0 \pmod{5} \quad \text{and} \quad a_{19}(E_{a,b}) \equiv 4 \pmod{7},$$

yielding a contradiction to both congruences in (4.10) for both $p = 5$ and $p = 7$. This eliminates the possibility of μ occurring after descent for these primes, as desired.

For the prime exponents $11 \leq p \leq 37$, $p \neq 13$, we apply a similar argument using an appropriate auxiliary prime q . More precisely, we take

$$(p, q) \in \{(11, 23), (17, 103), (19, 7), (23, 139), (29, 233), (31, 37), (37, 11)\}$$

with the improvement that, when $p \mid q - 1$, equation (4.3) allows us to take $\mathcal{P}$ to be the set of pairs $(a, b) \neq (0, 0)$ with $0 \leq a \leq b \leq q - 1$ and $a + b$ a p -th power in $\mathbb{Z}/q\mathbb{Z}$. The upshot is that also in this prime range, the extraneous unit is eliminated.

5. RATIONAL POINTS ON C_p

In this section, we will use variants of Chabauty's method to determine $C_p(K)$ for $p = 5$ and $p = 7$, where we assume GRH is the latter case. Subsequently, this will complete the proof of Theorem 1.1. We will also explore some partial results for $p = 11$ (assuming GRH again).

In its basic form, the method of Chabauty (and Coleman) considers an embedding of a genus at least two curve $C/\mathbb{Q}$ inside an abelian variety J (usually its Jacobian) $C \hookrightarrow J$ and studies the subsets of rational points inside these spaces. In the case where the rank of $J(\mathbb{Q})$ is less than the dimension of J , we can find nontrivial locally analytic ℓ -adic functions vanishing on all of $J(\mathbb{Q})$ and hence all of $C(\mathbb{Q}) \subseteq C(\mathbb{Q}_\ell) \cap J(\mathbb{Q})$. Pulling these functions back to the curve then results in an effective method to find the rational points (or at least a finite set of ℓ -adic points containing them), when the rank condition is met.

Many variants of these methods have been introduced, which can in some cases apply when the original rank condition is not satisfied. These generally work by considering similar set-ups coming from different constructions starting from the initial curve. They include elliptic curve Chabauty [9], quadratic Chabauty [1], Selmer group Chabauty [21], and, most importantly for us, number field Chabauty [20].

In this last variant, introduced by Siksek using ideas of Wetherell, we begin with a curve C defined over a number field F , and rather than considering $C(F) \rightarrow J(F)$ we consider $\text{Res}_{F/\mathbb{Q}} C(\mathbb{Q}) \rightarrow \text{Res}_{F/\mathbb{Q}} J(\mathbb{Q})$. This has the advantage of possibly working when $\text{rank}(J(F)) \leq [F : \mathbb{Q}](g - 1)$ (rather than $\text{rank}(J(F)) \leq g - 1$), although it may not always be successful.

With many Chabauty-like methods, the p -adic analysis suffices to give a bound on the number of rational points in each p -adic disk, though often this bound is not sufficient to determine the rational points exactly. Thus, the combination of Chabauty with some form of Mordell–Weil sieve [10] is what usually suffices to effectively determine the rational points on the curve.

Let $J_p := \text{Jac}(C_p)/K$ be the Jacobian of C_p .

5.1. The case $p = 5$. Recall the definition of X_0 and Y_0 in (3.3) and let

$$X_1 := 4\rho - 4, \quad Y_1 := 176\rho^2 - 288\rho + 96.$$

We will show that

$$(5.1) \quad C_5(K) = \{(X_0, \pm Y_0), (X_1, \pm Y_1), \infty\}.$$

With **Magma** we compute that J_5 has 2-Selmer rank equal to 2 and has trivial 2-torsion. Moreover, $[(X_0, Y_0) - \infty], [(X_1, Y_1) - \infty] \in J_5(K)$ provide 2 independent points of infinite order. So $\text{rank } J_5(K) = 2$ and we have explicit generators for a finite index subgroup. This puts us in a position to apply Siksek's Chabauty over number fields [20].

Using the implementation due to Siksek (which needs only minor updates to work with recent versions of **Magma**) we find that the set of primes above $p = 47$ the combination of Chabauty and the Mordell–Weil sieve are enough to prove that there is only one K -rational point in each of the residue disks around $\{(X_0, \pm Y_0), (X_1, \pm Y_1), \infty\}$, and that all other residue disks do not contain K -rational points. This shows that $C_5(K)$ is as claimed.

Finally, we need to check that the two ‘extra’ points $(X_1, \pm Y_1)$ do not correspond to solutions of (1.2). By (3.5), it suffices to show that the binary quartic form

$$F(x, y) - \frac{(X_1/X_0)^p}{(Y_1/Y_0)^2} H(x, y)^2$$

does not have a linear factor over K (or even $\mathbb{Q}$ actually). One readily checks that this is indeed the case by factorizing the form over K using **Magma**. (Perhaps surprisingly, it factorizes into two irreducible quadratic pieces over K .) This finalizes the proof of Theorem 1.1 for $p = 5$.

5.2. The case $p = 7$. Assume GRH. We will show that

$$(5.2) \quad C_7(K) = \{(X_0, \pm Y_0), \infty\}.$$

With **Magma**, we compute, using the GRH assumption for the underlying class group computations, that J_7 has 2-Selmer rank equal to 1 and has trivial 2-torsion. Moreover, $[(X_0, Y_0) - \infty] \in J_7(K)$ is a point of infinite order. So $\text{rank } J_7(K) = 1$ and we have an explicit generator for a finite index subgroup. This puts us in a position to apply ‘standard’ Chabauty. Performing this (e.g. using **Magma**) shows 5.2, thereby finalizing the proof of Theorem 1.1 for $p = 7$.

5.3. The case $p = 11$. Assume GRH again. For $p = 11$, we compute that J_{11} has 2-Selmer rank equal to 3 and has trivial 2-torsion. We were able to only find one independent point of infinite order on $J_{11}(K)$, namely $[(X_0, Y_0) - \infty]$. So $1 \leq \text{rank } J_{11}(K) \leq 3$. As C_{11} has K -rational points, and hence points everywhere locally, we find that if Sha is finite, then its order is a square (see e.g. [18, Corollaries 9 and 12]), and consequently $\text{rank } J_{11}(K) \in \{1, 3\}$. Perhaps Selmer group Chabauty [21] can deal with this case.

6. ALTERNATIVE METHODS

In this section we discuss the necessity of Chabauty and modular methods. We focus mainly on $p = 5$.

6.1. Chabauty methods for other cases. Assume $(a, b, c) \in \mathbb{Z}^3$ is a solution to (1.2) with $13|c$ (i.e. $13|a + b$). Similarly as in Section 3, we can reduce to finding rational points on hyperelliptic curves. Let the binary forms $F, G, H \in \mathcal{O}_K[x, y]$ and the constant $d \in K$ be as defined in Section 3, and choose $\pi_{13} := F(1, -1) = \rho^2 + 3\rho - 2$ as generator for the unique prime ideal in $\mathcal{O}_K$ lying above 13. A classical descent gives that

$$F(a, b) = \pi_{13} e z_1^p \text{ and } 13G(a, b) = z_2^p$$

for certain $e, z_1, z_2 \in \mathcal{O}_K$ with e a unit (and actually $z_2 \in \mathbb{Z}$).

Writing $Y' := H(a, b)/z_2^{2p}$ and $X' := z_1/z_2^4$ as before, we see that specializing (3.1) at (a, b) and dividing by z_2^{4p} , we arrive at

$$D'_{p,e} : (1 + d)Y'^2 = \pi_{13} e X'^p + \frac{d}{13^4}.$$

This defines a hyperelliptic curve $D'_{p,e}$ of genus $(p-1)/2$. Its equation could be conveniently rescaled again of course.

The case $e = 1$ is again of special interest to us, and we write $D'_p := D'_{p,1}$. We note that the trivial solutions (a, b, c) with $c = 0$ (i.e. $(\pm 1, \mp 1, 0)$) give rise to the point at infinity on D'_p . Let $p \neq 13$ be prime with $5 \leq p \leq 47$. As the basic (non-modular) sieve eliminates all units e , except $e = 1$ of course, we are left with determining $D'_p(K)$ in order to find the solutions (a, b, c) with $13|c$. Let us focus on the difficulties for $p = 5$.

Let $p = 5$. By a 2-Selmer group computation, the rank of the Jacobian of D'_5/K equals 0 or 1. Assuming finiteness of Sha, we get that the rank equals 1. If we could find a point of infinite order on the Jacobian, we of course get that the rank equals 1, and we could very likely apply (standard) Chabauty in practice to determine the K -rational points on the curve. However, a further search did not reveal a point of infinite order on the Jacobian. So we are not in a position to employ ‘basic’ Chabauty. Perhaps Selmer group Chabauty over number fields could be employed.

For the extraneous unit μ , by a 2-Selmer group computation, the rank of the Jacobian of $C_{5,\mu}/K$ equals 0 or 1. We find ourselves in a similar situation as with D'_5 .

6.2. Modular methods for other cases. In view of recent progress [7, 11] surrounding the Darmon program for the generalized Fermat equation [13], it is natural to wonder if we could replace the use of Chabauty methods in our proofs with an application of the multi-Frey modular method using higher dimensional Frey varieties. Recall that, in Theorem 1.2, we used the modular method with Frey curves to deal with the case $13|a + b$ of equation (1.3); in particular, this deals with the trivial solution $\pm(1, -1, 0)$. The Frey hyperelliptic curve $J = J_5^-(a, b, c)$ attached to Fermat equations of signature $(p, p, 5)$ is an excellent candidate for the complementary case, because it becomes singular when evaluated at the trivial solutions $\pm(1, 0, 1)$ and $\pm(0, 1, 1)$ (see [11, §5] for discriminant formula). However, a closer look at the proof of [11, Theorem 1.2] reveals at least one serious obstruction, namely, when $2|ab$ and

$5 \mid ab$ we do not have irreducibility of the mod $\mathfrak{p}$ representation $\bar{\rho}_{J,\mathfrak{p}}$. Unfortunately, our additional assumption $13 \nmid a + b$ does not help and so irreducibility can only be guaranteed conjecturally for large enough p via [13, Conjecture 4.1]. Additionally, we observe that the Frey hyperelliptic curve for signature $(13, 13, p)$ studied in [7] is non-singular when evaluated at $\pm(1, 0, 1)$ and $\pm(0, 1, 1)$, giving rise to obstructions in the elimination step; since this obstructing variety has CM, we only expect to complete the argument conjecturally for large p , assuming the large image conjecture [13, Conjecture 4.1].

REFERENCES

- [1] Jennifer S. Balakrishnan and Netan Dogra. Quadratic Chabauty and rational points. I: p -adic heights. *Duke Math. J.*, 167(11):1981–2038, 2018. [5](#)
- [2] Michael A. Bennett, Imin Chen, Sander R. Dahmen, and Soroosh Yazdani. Generalized Fermat equations: a miscellany. *Int. J. Number Theory*, 11(1):1–28, 2015. [1](#)
- [3] Michael A. Bennett and Chris M. Skinner. Ternary Diophantine equations via Galois representations and modular forms. *Can. J. Math.*, 56(1):23–54, 2004. [1](#), [2](#)
- [4] Michael A. Bennett, Vinayak Vatsal, and Soroosh Yazdani. Ternary Diophantine equations of signature $(p, p, 3)$. *Compos. Math.*, 140(6):1399–1416, 2004. [1](#), [2](#)
- [5] Nicolas Billerey, Imin Chen, Lassina Dembélé, Luis Dieulefait, and Nuno Freitas. Some extensions of the modular method and Fermat equations of signature $(13, 13, n)$. *Publ. Mat., Barc.*, 67(2):715–741, 2023. [2](#), [2](#), [2.4](#), [4](#)
- [6] Nicolas Billerey, Imin Chen, Luis Dieulefait, and Nuno Freitas. A multi-Frey approach to Fermat equations of signature (r, r, p) . *Trans. Am. Math. Soc.*, 371(12):8651–8677, 2019. [1](#), [2](#), [2](#), [2](#), [2](#), [2](#), [4.3](#)
- [7] Nicolas Billerey, Imin Chen, Luis Dieulefait, and Nuno Freitas. On Darmon’s program for the generalized Fermat equation. I. *J. Reine Angew. Math.*, 822:107–146, 2025. [6.2](#)
- [8] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993). [2](#)
- [9] Nils Bruin. Chabauty methods using elliptic curves. *J. Reine Angew. Math.*, 562:27–49, 2003. [5](#)
- [10] Nils Bruin and Michael Stoll. The Mordell-Weil sieve: proving non-existence of rational points on curves. *LMS J. Comput. Math.*, 13:272–306, 2010. [5](#)
- [11] Imin Chen and Angelos Koutsianas. A modular approach to Fermat equations of signature $(p, p, 5)$ using Frey hyperelliptic curves. Preprint, arXiv:2210.02316 [math.NT] (2022), 2022. [6.2](#)
- [12] Sander R. Dahmen and Samir Siksek. Perfect powers expressible as sums of two fifth or seventh powers. *Acta Arith.*, 164(1):65–100, 2014. [3](#), [4](#)
- [13] Henri Darmon. Rigid local systems, Hilbert modular forms, and Fermat’s last theorem. *Duke Math. J.*, 102(3):413–449, 2000. [6.2](#)
- [14] Maarten Derickx, Filip Najman, and Samir Siksek. Elliptic curves over totally real cubic fields are modular. *Algebra Number Theory*, 14(7):1791–1800, 2020. [2](#)
- [15] Luis Dieulefait and Nuno Freitas. Fermat-type equations of signature $(13, 13, p)$ via Hilbert cuspforms. *Math. Ann.*, 357(3):987–1004, 2013. [2](#), [2](#), [2](#)
- [16] Nuno Freitas. Recipes to Fermat-type equations of the form $x^r + y^r = Cz^p$. *Math. Z.*, 279(3-4):605–639, 2015. [2](#), [4.1](#)
- [17] Alain Kraus. Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive. *Manuscr. Math.*, 69(4):353–385, 1990. [2](#)
- [18] Bjorn Poonen and Michael Stoll. The Cassels-Tate pairing on polarized Abelian varieties. *Ann. Math.* (2), 150(3):1109–1149, 1999. [5.3](#)
- [19] Ashleigh Ratcliffe and Bogdan Grechuk. Generalized Fermat equation: a survey of solved cases. *Expo. Math.*, 43(4):59, 2025. Id/No 125688. [1](#)
- [20] Samir Siksek. Explicit Chabauty over number fields. *Algebra Number Theory*, 7(4):765–793, 2013. [5](#), [5.1](#)
- [21] Michael Stoll. Chabauty without the Mordell-Weil group. In *Algorithmic and experimental methods in algebra, geometry, and number theory*, pages 623–663. Cham: Springer, 2017. [5](#), [5.3](#)

ALEX J. BEST, UK

Email address: alex.j.best@gmail.com

SANDER R. DAHMEN, DEPARTMENT OF MATHEMATICS, VU AMSTERDAM, DE BOELELAAN 1111, 1081 HV AMSTERDAM, THE NETHERLANDS

Email address: s.r.dahmen@vu.nl

NUNO FREITAS, INSTITUTO DE CIENCIAS MATEMÁTICAS, CSIC, CALLE NICOLÁS CABRERA, 13–15, 28049 MADRID, SPAIN

Email address: nuno.freitas@icmat.es