# Asymptotic Fermat's Last Theorem for a family of equations of signature (2, 2n, n)

# ASYMPTOTIC FERMAT'S LAST THEOREM FOR A FAMILY OF EQUATIONS OF SIGNATURE $(2, 2n, n)$

PEDRO-JOSÉ CAZORLA GARCÍA

Abstract. In this paper, we study the integer solutions of a family of Fermat-type equations of signature $(2, 2n, n)$, $Cx^2 + q^k y^{2n} = z^n$. We provide an algorithmically testable set of conditions which, if satisfied, imply the existence of a constant $B_{C,q}$ such that if $n > B_{C,q}$, there are no solutions $(x, y, z, n)$ of the equation. Our methods use the modular method for Diophantine equations, along with level lowering and Galois theory.

## 1. Introduction

1.1. **Historical background.** At the beginning of the 17th century, Fermat wrote in the margin of a copy of *Arithmetica* that he had proved that the exponential Diophantine equation

$$x^n + y^n = z^n \tag{1}$$

had no solutions $(x, y, z, n) \in \mathbb{Z}^4$ with $n > 2$ and $xyz \neq 0$. Fermat's alleged proof of this fact was never found and the resolution of (1) became one of the biggest problems in the history of mathematics, known as *Fermat's Last Theorem.*

In 1995, Wiles [28] proved the Modularity Theorem for semistable elliptic curves, which, along with Ribet's Level Lowering Theorem [25], finished the proof of Fermat's Last Theorem more than three centuries after its initial statement.

After Wiles's proof of Fermat's Last Theorem, several generalisations of (1) have been studied. For example, the equation

$$Ax^p + By^q = Cz^r, \tag{2}$$

where $A$, $B$ and $C$ are given integers, is called a *Fermat-type equation* of signature $(p, q, r)$. After the proof of Fermat's Last Theorem, many researchers (see [2, 4, 5, 19], among many others) have used the modular methodology pioneered by Wiles in order to study Fermat-type equations over $\mathbb{Q}$.

More recently, this methodology has also been used to study (2) over number fields $K$. In this setting, we are interested in solutions where $x$, $y$ and $z$ are elements of the ring of integers of $K$, which we will denote by $\mathcal{O}_K$.

One of the most relevant results on Fermat-type equations over number fields is due to Freitas and Siksek [12]. They showed that for 5/6 of real quadratic fields

*Date*: April 23, 2024.

2010 *Mathematics Subject Classification.* Primary 11D61, Secondary 11D41, 11F80, 11F11.

*Key words and phrases.* Exponential Diophantine equation, Fermat equations, Galois representations, Frey–Hellegouarch curve, asymptotic Fermat's Last Theorem, modularity, level lowering.

$K = \mathbb{Q}(\sqrt{d})$, ordered by the value of $d$, there exists a constant $B_K$, depending only on $K$, such that if $p > B_K$ is prime, the equation

$$x^p + y^p = z^p$$

has no solutions $(x, y, z) \in \mathcal{O}_K^3$ satisfying $xyz \neq 0$. This is called the *asymptotic Fermat's Last Theorem* (AFLT) *for* $K$. For a general totally real number field $K$, they give an algorithmically testable criterion which, if satisfied, implies the Asymptotic Fermat's Last Theorem for $K$. Shortly afterwards, Deconinck [11] proved an analogous result for the equation

$$Ax^p + By^p = Cz^p,$$

where $A, B, C \in \mathcal{O}_K$ are fixed and odd. In this situation, the constant implied by AFLT depends on $A$, $B$ and $C$, as well as on the number field $K$.

Other researchers have extended this line of work to Fermat-type equations of signatures $(p, p, 2)$ and $(p, p, 3)$. For example, Işik, Kara and Özman [13, 14] have studied the Diophantine equations

$$x^p + y^p = z^2, \quad 2 \mid y, \tag{3}$$

and

$$x^p + y^p = z^3, \quad 3 \mid y, \tag{4}$$

over totally real number fields $K$ with narrow class number $h_K^+ = 1$. For these fields, they show that there is a constant $B_K$ such that, if $p > B_K$, there are no solutions $(x, y, z, p) \in \mathcal{O}_K^3 \times \mathbb{Z}$ to either (3) or (4). Finally, this work was extended by Mocanu [24], who showed the same results under a weaker assumption.

1.2. **The main results.** In this paper, we adapt these techniques to approach a different problem. We note that all the previously mentioned literature considers solutions of **one** exponential Diophantine equation over infinitely many number fields. However, we shall consider solutions to a family of **infinitely many** exponential Diophantine equations of signature $(2, 2n, n)$ over the rationals. The family of Fermat-type equations that we will consider is the following:

$$Cx^2 + q^k y^{2n} = z^n, \quad \gcd(Cx, qy, z) = 1, \quad 2 \mid z, \tag{5}$$

where $C, q$ and $k$ are fixed positive integers, with $C$ squarefree and $q \geq 3$ a prime. This equation is relevant because, to the best of our knowledge, there are no results on AFLT for Fermat-type equations of signature $(p, p, 2)$ unless $C = 1$ or $C = 2$ (see [15, 16, 20, 21] for some of the existing results if $C = 1$ or $C = 2$), even over $\mathbb{Q}$. Since solutions of (5) are also solutions of

$$Cx^2 + q^k y^n = z^n, \quad \gcd(Cx, qy, z) = 1,$$

studying (5) gives information about a Fermat-type equation of signature $(n, n, 2)$ with $C \neq 1, 2$.

In addition, we note that (5) is a generalisation of the Lebesgue–Nagell equation, which has been widely studied in the literature (for example, see [3, 5, 6] or [22] for an exposition of the history of the Lebesgue–Nagell equation) to three variables $x, y$ and $z$.

We now proceed to give the definition of AFLT for (5), which is the following:

**Definition 1.** (AFLT for (5)) We say that Asymptotic Fermat's Last Theorem (AFLT) holds for (5) if there is a constant $B_{C,q}$, depending only on $C$ and $q$, such that if $p$ is a prime number with $p > B_{C,q}$, then there are no solutions $(x, y, z, n) \in \mathbb{Z}^4$ to (5) with $n = p$.

We remark that Definition 1 is stronger than some of the definitions of AFLT used in previous literature, in the sense that $B_{C,q}$ does not depend on $k$.

*Remark* 2. If the constant in Definition 1 exists, then there is a different constant $B'_{C,q}$ such that if $n$ is composite and $n > B'_{C,q}$, there are no solutions $(x, y, z, n) \in \mathbb{Z}^4$ of (5). Indeed, suppose that Definition 1 holds. Let

$$D = \{4, 6, 9\} \cup \{p \geq 5 \text{ prime} \mid p < B_{C,q}.\}$$

Any solution $(x, y, z, n) \in \mathbb{Z}^4$ of (5) with $n$ composite necessarily has $m \mid n$ for some $m \in D$, so we write $n = mt$ for some $t \geq 1$. The existence of such a solution $(x, y, z, n)$ of (5) clearly means that $(x', y', z') = (x, y^t, z^t)$ is a solution of

$$C(x')^2 + q^k(y')^{2m} = (z')^m. \tag{6}$$

A specialisation of a result of Darmon and Granville (see [10, Theorem 2]) yields that there are finitely many solutions of (6) for any $m \in D$. Then we can define

$$m' = \max\{s \geq 1 \mid \text{there exists } m \in D, (x, y, z) \in \mathbb{Z}^3$$
$$\text{such that } (x, y^s, z^s) \text{ is a solution of (6)}\} \cup \{1\}.$$

By our previous discussion, the set above is finite and, therefore, $m' < \infty$. By definition of $m'$, it follows that any solution $(x, y, z, n) \in \mathbb{Z}^4$ with $n$ composite satisfies

$$n < \max\{9, B_{C,q}\} \cdot m',$$

and so it suffices to take $B'_{C,q} = \max\{9, B_{C,q}\} \cdot m'$. However, we emphasise that the constant $m'$ can only be made effective by explicitly resolving (5), which is beyond the scope of this paper.

We can now present the main result of this paper, Theorem 3, which provides a set of algorithmically testable conditions which, if satisfied, imply AFLT for (5).

**Theorem 3.** *Let $C \geq 1$ be a squarefree integer, $q \geq 3$ a prime number and $k \geq 0$ an integer and consider the following Diophantine equation:*

$$Cx^2 + q^k y^{2n} = z^n, \quad \gcd(Cx, qy, z) = 1, \quad 2 \mid z.$$

*Suppose that the Diophantine equation*

$$Ct^2 + q^\gamma = 2^m \tag{7}$$

*has no solutions $(t, \gamma, m) \in \mathbb{Z}^3$ with $m > 6$ and $\gamma \geq 0$ with $\gamma \equiv k \pmod 2$. Suppose furthermore that any of the following hypotheses hold:*

*(a) The exponent $k$ is odd.*

*(b) The exponent $k$ is even, and $-C$ is not a square modulo $q$.*

*(c) The exponent $k$ is even, $q \not\equiv 7 \pmod 8$ and there are no solutions $(t, \gamma, m) \in \mathbb{Z}^3$ to the following equation:*

$$Ct^2 + 1 = q^\gamma 2^m, \quad m > 6, \quad \gamma \geq 0. \tag{8}$$

(d) *The exponent $k$ is even, $q \equiv 7 \pmod 8$, (8) has no solutions and there are no solutions $(t, \gamma, m) \in \mathbb{Z}^3$ to*

$$Ct^2 + 2^m = q^\gamma, \quad m > 6 \text{ even}, \quad \gamma > 0 \text{ odd}. \tag{9}$$

*Then AFLT holds for (5) and the constant $B_{C,q}$ can be explicitly computed.*

We note that, in order to prove Theorem 3, it suffices to do so under the assumption that $0 \leq k < 2n$. Indeed, let us write $k = 2nk_1 + k_2$, with $k_1 \geq 0$ and $0 \leq k_2 < 2n$. Then any solution $(x_0, y_0, z_0, n_0)$ of (5) gives rise to a solution $(x_0, y_0q^{k_1}, z_0, n_0)$ of

$$Cx^2 + q^{k_2}y^{2n} = z^n,$$

and, since $k \equiv k_2 \pmod 2$, the conditions in Theorem 3 are well defined if we replace $k$ by $k_2$. For this reason, we shall assume that $0 \leq k < 2n$ for the remainder of the paper.

In addition, we emphasise that the determination of whether any of the hypotheses in Theorem 3 are satisfied can be done in a computationally effective manner. For this purpose, we provide the reader with `Magma` code in the GitHub repository https://shorturl.at/hoxW8. We will explain the computations in Section 7, allowing us to prove the following result.

**Theorem 4.** *Let $1 \leq C \leq 70$ be a squarefree integer and $3 \leq q < 100$ be a prime number. By reducing (5) modulo 8, we see that $Cq^k \equiv 7 \pmod 8$. Then AFLT holds for 268 out of the 330 pairs in this range. In addition, Table 1 contains the number of pairs satisfying the conditions in Theorem 3, as well as the total number of pairs for each value of $k \pmod 2$.*

| $k \pmod 2$ | *#Pairs $(C, q)$* | *# Pairs satisfying the conditions in Theorem 3* |
|---|---|---|
| *0* | *158* | *131* |
| *1* | *172* | *137* |
| ***TOTAL*** | *330* | *268* |

Table 1. Number of pairs satisfying the conditions in Theorem 3.

The structure of the paper is as follows. In Section 2, we present the modular method for Diophantine equations and characterise under what conditions it fails to prove AFLT for (5). In Sections 3 and 4, we will use "image of inertia" arguments and Galois theory respectively to build upon this characterisation. In Section 5, we put the previous results together to show that the failure of AFLT implies the existence of an elliptic curve $E$ of a particular form. In Section 6, we finish the proof of Theorem 3 by relating the curve $E$ to the existence of solutions to certain Diophantine equations. Finally, on Section 7, we show that checking the conditions in Theorem 3 is a computationally effective process and prove Theorem 4.

**Acknowledgements** The author would like to thank Gareth Jones, Diana Mocanu and Lucas Villagra-Torcomián for their comments on a draft version of the paper and for useful conversations.

## 2. The Frey–Hellegouarch curve and the modular method

In this section, we present the Frey–Hellegouarch that we shall use to achieve a bound on the exponent $n$. An excellent expository article on the modular method and its applications can be found in [26].

We highlight that, due to the fact that $z$ is even, there is only one Frey–Hellegouarch curve to consider, allowing for a uniform treatment of all cases. If $z$ were odd, the number of cases to consider would grow significantly and, consequently, we would not be able to get a result like Theorem 3. We refer the reader to Remark 7 for a more detailed discussion on why this is the case.

We suppose that there exists a solution $(x, y, z, p)$ to (5) with $z$ even and $n = p \geq 7$ a prime number. Following Bennett and Skinner [2], we can associate the following elliptic curve to the solution:

$$F = F(x, z, p) : Y^2 + XY = X^3 + \frac{Cx - 1}{4} X^2 + \frac{Cz^p}{64} X. \tag{10}$$

We shall call $F$ the *Frey–Hellegouarch curve associated to* $(x, y, z, p)$. By [2, Lemma 2.1], the minimal discriminant of $F$ is given by

$$\Delta_F = -2^{-12} C^3 q^k (yz)^{2p}, \tag{11}$$

and conductor given by

$$N = \begin{cases} 2C^2 q \operatorname{Rad}_{2,q}(yz), & \text{if } k \neq 0, \\ 2C^2 \operatorname{Rad}_2(yz), & \text{if } k = 0. \end{cases} \tag{12}$$

where $\operatorname{Rad}_{2,q}(yz)$ denotes the product of all prime numbers dividing $yz$ except 2 and $q$, and similarly for $\operatorname{Rad}_2(yz)$. By the Modularity Theorem [28], the curve $F$ corresponds to a rational modular form of weight 2 and level $N$. However, we remark that the level $N$ depends on our solutions and, therefore, is not explicit.

In order to be able to work with newforms of an explicit level, we will need to combine the Modularity Theorem with Ribet's Level Lowering Theorem [25]. We shall do so by applying [26, Theorem 13] (which is a combination of [2, Lemmas 3.2 and 3.3]). By this result, it follows that either $yz = \pm 1$, or there exists a newform $f$ of weight 2, trivial Nebentypus character and level given by

$$N' = \begin{cases} 2C^2 q & \text{if } k \neq 0, p, \\ 2C^2 & \text{if } k = 0, p, \end{cases} \tag{13}$$

such that

$$\overline{\rho}_p(F) \cong \overline{\rho}_p(f), \tag{14}$$

where $\overline{\rho}_p$ denotes the mod-$p$ Galois representations associated to $F$ and $f$ respectively. We note that, since $z$ is even, $yz \neq \pm 1$. Consequently, (14) holds.

Given a prime number $\ell$, we define $a_\ell(F) := \ell + 1 - \#F(\mathbb{F}_\ell)$. Similarly, we let $c_\ell$ be the $\ell-$th coefficient in the Fourier cusp expansion of $f$, we let $K_f$ be the number field generated by all Fourier coefficients of $f$, and we let $\mathcal{O}_{K_f}$ be its ring of integers. Then, by [26, Propositions 5.1 and 5.2], (14) is equivalent to

$$\begin{cases} a_\ell(F) \equiv c_\ell \pmod{\mathfrak{p}} & \text{if } \ell \neq p, \quad \ell \nmid N, \\ c_\ell \equiv \pm(\ell + 1) \pmod{\mathfrak{p}} & \text{if } \ell \neq p, \quad \ell \nmid N', \quad \ell \mid N, \end{cases} \tag{15}$$

where $\mathfrak{p}$ is some prime ideal of $\mathcal{O}_{K_f}$ above $p$. In addition, if $f$ is a rational newform, the condition $\ell \neq p$ can be removed in both cases. The following proposition, which is [26, Proposition 9.1], allows us to bound $p$ in some instances by exploiting (15).

**Proposition 2.1.** *Suppose that $(x, y, z, p) \in \mathbb{Z}^4$ is a solution to (5) with $n = p \geq 7$ prime. Let $f$ be a newform of weight 2 and level $N'$ as in (13), with field of coefficients $K_f$ and such that $\overline{\rho}_p(F) \cong \overline{\rho}_p(f)$. Then, for any prime number $\ell \nmid N'$, we define*

$$B'_\ell(f) = \mathrm{Norm}_{K_f/\mathbb{Q}}\left((\ell+1)^2 - c_\ell^2\right) \prod_{\substack{|a|<2\sqrt{\ell} \\ 2|a}} \mathrm{Norm}_{K_f/\mathbb{Q}}(a - c_\ell),$$

*and*

$$B_\ell(f) = \begin{cases} B'_\ell(f) & \text{if } f \text{ is rational.} \\ \ell B'_\ell(f) & \text{otherwise.} \end{cases}$$

*Then $p \mid B_\ell(f)$.*

*Remark* 5. We remark that, as long as $B_\ell(f) \neq 0$ for all newforms of weight 2 and level $N'$, we will be able to explicitly find a constant $B_{C,q}$ such that any solutions $(x, y, z, p)$ of (5) with $n = p$ prime necessarily satisfy that $p < B_{C,q}$, thereby proving AFLT for (5). Consequently, our aim is to characterise those newforms $f$ for which $B_\ell(f) = 0$.

As stated in the remarks following [26, Proposition 9.1], if $B_\ell(f) = 0$, $f$ is necessarily a rational newform and therefore corresponds to an elliptic curve $E$ via the Modularity Theorem. In this instance, we shall write $\overline{\rho}_p(F) \cong \overline{\rho}_p(E)$ to mean $\overline{\rho}_p(F) \cong \overline{\rho}_p(f)$. We also note that in this case $c_\ell = a_\ell(E) := \ell + 1 - \#E(\mathbb{F}_\ell)$.

In addition, if $B_\ell(f) = 0$, we know that $E$ is isogenous to a curve $E'$ with a $\mathbb{Q}-$rational point of order 2. In this case, it is still true that

$$\overline{\rho}_p(F) \cong \overline{\rho}_p(E').$$

This fact allows us to prove the following lemma.

**Lemma 2.2.** *Suppose that AFLT does not hold for (5). Then there exists an elliptic curve $E$ of conductor $N'$ with a model of the form*

$$E : Y^2 = X(X^2 + AX + B), \tag{16}$$

*for certain integers $A, B$ and satisfying*

$$\overline{\rho}_p(F) \cong \overline{\rho}_p(E).$$

*In addition, the invariants of the minimal model of $E$ are given by*

$$c_4 = A^2 - 3B,$$

$$c_6 = \frac{A(9B - 2A^2)}{2},$$

*and*

$$\Delta = \frac{B^2(A^2 - 4B)}{2^8}. \tag{17}$$

*Proof.* By our discussion in Remark 5, Proposition 2.1 will succeed in bounding $p$ unless there is an elliptic curve $E$ of conductor $N'$ with a point of order 2 satisfying $\overline{\rho}_p(F) \cong \overline{\rho}_p(E)$. Up to isomorphism, we can assume that $E$ has the following model:

$$E : Y^2 = X(X^2 + A'X + B'), \tag{18}$$

for certain $A', B' \in \mathbb{Z}$. By directly applying the formulas in [27, Chapter 3], we find that this model has invariants given by

$$c_4' = 16({A'}^2 - 3B'),$$

$$c_6' = 2^5 A'(9B' - 2{A'}^2),$$

and

$$\Delta' = 2^4 {B'}^2({A'}^2 - 4B').$$

Suppose that $\ell \neq 2$ is a prime for which the model (18) is not minimal. Therefore, it follows that $\ell^{12} \mid \Delta'$ and $\ell^4 \mid c_4'$. Consequently, $\ell^4 \mid {A'}^2 - 3B'$ and either

$$\ell^7 \mid {B'}^2 \quad \text{or} \quad \ell^6 \mid ({A'}^2 - 4B'),$$

by the pigeonhole principle. In both cases, we can see that $\ell^4 \mid B'$ and $\ell^2 \mid A'$. Then we can replace $(A', B')$ by

$$(A, B) = \left(\frac{A'}{\ell^2}, \frac{B'}{\ell^4}\right)$$

in (18) and obtain an isomorphic model. After finitely many iterations, this procedure will yield a model which is minimal at $\ell$.

Finally, let us consider the case $\ell = 2$. Since $2 \mid c_4'$, $2 \mid \Delta'$, and 2 is a prime of multiplicative reduction for $E$, it follows that (18) cannot be a minimal model at 2. Consequently, there is another model of $E$ with invariants given by

$$c_4'' = c_4'/2^4 = {A'}^2 - 3B',$$

$$c_6'' = c_6'/2^6 = \frac{A'(9B' - 2{A'}^2)}{2},$$

$$\Delta'' = \Delta'/2^{12} = \frac{{B'}^2({A'}^2 - 4B')}{2^8}.$$

If this model is minimal at 2, we may take $A = A'$ and $B = B'$ and finish the proof. Otherwise, we have that $2^6 \mid c_6''$ and $2^4 \mid c_4''$, and by exploting a similar argument to the case where $\ell \neq 2$, we may see that $2^4 \mid B'$ and $2^2 \mid A'$ and iterately replace $(A', B')$ by $(A'/2^2, B'/2^4)$ until we attain a minimal model. □

## 3. An image of inertia argument

If AFLT does not hold for (5), Lemma 2.2 gives the existence of an elliptic curve $E$ of conductor $N'$ such that $\overline{\rho}_p(F) \cong \overline{\rho}_p(E)$. In this case, we can see whether the image of the two Galois representation agree for some inertia subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. A very useful result in this direction is the following theorem due to Bennett and Skinner, which is [26, Theorem 13(e)] and follows directly from [2, Theorem 2.1(d)].

**Theorem 6.** *(Bennett-Skinner) Let $(x, y, z, p)$ be a solution to (5) with $n = p \geq 7$ prime. Let $F$ be the Frey–Hellegourch curve (10), and let $E$ be an elliptic curve such that*

$$\overline{\rho}_p(F) \cong \overline{\rho}_p(E).$$

*Then the denominator of the $j-$invariant of $E$ is not divisible by any odd primes $\ell \mid C$ except possibly $\ell = p$.*

With the use of Theorem 6, we are able to expand on the result of Lemma 2.2, giving rise to the following characterisation. For this, we let $\ell$ be a prime number and we let $\nu_\ell(\cdot)$ denote the standard $\ell-$adic valuation.

**Proposition 3.1.** *Suppose that AFLT does not hold for (5) and let $E$ be the elliptic curve given in (16). Then, for all primes $r \mid C$, we have that $\nu_r(B) = \nu_r(A^2 - 4B)$.*

*Proof.* By Lemma 2.2, the $j-$invariant of $E$ is given by

$$j(E) = \frac{c_4^3}{\Delta} = \frac{2^8(A^2 - 3B)^3}{B^2(A^2 - 4B)}.$$

Let $r \mid C$ be a prime satisfying that $\nu_r(B) \neq \nu_r(A^2 - 4B)$. If $r = p$, we have that $p < C$, and so AFLT holds for (5) with $B_{C,q} = C$. If $r \neq p$, $r$ does not divide the denominator of $j(E)$ by Theorem 6. Consequently

$$3\nu_r(A^2 - 3B) \geq 2\nu_r(B) + \nu_r(A^2 - 4B). \tag{19}$$

Since $\nu_r(B) \neq \nu_r(A^2 - 4B)$, standard properties of $r-$adic valuations yield that

$$\nu_r(A^2 - 3B) = \nu_r((A^2 - 4B) + B) = \min\{\nu_r(B), \nu_r(A^2 - 4B)\},$$

while

$$2\nu_r(B) + \nu_r(A^2 - 4B) > 3\min\{\nu_r(B), \nu_r(A^2 - 4B)\}.$$

This gives a contradiction with (19). Consequently, $\nu_r(B) = \nu_r(A^2 - 4B)$ and the proposition follows. □

## 4. Using Galois theory to provide local information

Our aim in this section is to find conditions under which Proposition 2.1 can be refined. A key ingredient about the Frey–Hellegouarch curve $F$ that we use in the proof of Lemma 2.2 is the fact that $F(\mathbb{Q})$ always has a point of order 2, $(0, 0)$ and, consequently, $F(\mathbb{F}_\ell)$ has a point of order 2 for all primes $\ell$ of good reduction. For a subset of these primes, it happens that $F(\mathbb{F}_\ell)$ has a subgroup of order 4 and this fact can be exploited to improve upon Proposition 2.1 in order to obtain a bound for $p$.

Our aim is to characterise under what conditions such a prime $\ell$ fails to exist, and we shall do so in this section. In order to do this, we need to prove certain facts about the Frey–Hellegouarch curve $F$, and we do so in the following subsection.

4.1. **Some computations on the Frey curve.** Let $F'$ be any curve which is isogenous to $F$ via a rational isogeny of degree $2^m$ (note that the case $m = 0$ means that $F(\mathbb{Q})$ and $F'(\mathbb{Q})$ are isomorphic). The aim of this subsection is to show that $F'(\mathbb{Q})$ can never have a subgroup of order 4. We shall do that in three steps, corresponding to Lemmas 4.1 and 4.2, where we show that this fact is true for $F$, and Lemma 4.3, where we show the same for all $F' \ncong F$.

**Lemma 4.1.** *The Frey-Hellleguarch curve $F$ never has full $2-$torsion over $\mathbb{Q}$.*

*Proof.* Following [27, Exercise 3.7] and the expression for $F$ given in (10), we see that the roots of the $2-$division polynomial of $F$ are given by the expression

$$2Y + X = 0,$$

or, equivalently,

$$X = -2Y.$$

Substituting into (10) and simplifying, we get

$$-8Y^3 + CxY^2 - \frac{Cz^p}{32}Y = 0.$$

The root $Y = 0$ corresponds to the $2-$torsion point $(0, 0)$. If $F(\mathbb{Q})$ had additional $2-$torsion points, there would be other rational roots. This would mean that

$$C^2x^2 - Cz^p \geq 0.$$

But since $(x, y, z, p)$ is a solution to (5), we see that

$$C^2x^2 - Cz^p = -Cq^ky^{2p},$$

which is clearly negative. Consequently, the only point of order 2 in $F(\mathbb{Q})$ is $(0, 0)$. □

**Lemma 4.2.** *The group $F(\mathbb{Q})$ never has a point of order 4.*

*Proof.* Suppose that there exists a point $(X_0, Y_0) \in F(\mathbb{Q})$ of order 4. By Lemma 4.1, the only $\mathbb{Q}-$rational point of order 2 is $(0, 0)$, so it follows that

$$[2](X_0, Y_0) = (0, 0).$$

Consequently, the tangent line to $F$ at $(X_0, Y_0)$ passes through $(0, 0)$. Algebraically, this condition is equivalent to

$$2(Y_0^2 + X_0Y_0) = 3X_0^3 + \frac{Cx - 1}{2}X_0^2 + \frac{Cz^p}{64}X_0. \tag{20}$$

Since $(X_0, Y_0) \in F(\mathbb{Q})$, the left-hand side of the previous expression can be replaced by

$$2\left(X_0^3 + \frac{Cx - 1}{4}X_0^2 + \frac{Cz^p}{64}X_0\right),$$

and, consequently, it can be seen that (20) amounts to

$$X_0(X_0^2 - Cz^p/64) = 0.$$

Since $(X_0, Y_0)$ has order 4, it is clear that $(X_0, Y_0) \neq (0, 0)$ and, consequently

$$X_0^2 = \frac{Cz^p}{64},$$

but this is not possible since $C$ is squarefree and $\gcd(C, z) = 1$, so $\sqrt{Cz^p}$ is not a rational number. $\square$

These two lemmas show that $F(\mathbb{Q})$ does not have a subgroup of order 4. We can use them to prove that the same is true for curves which are isogenous to $F$ via a rational $2^m-$isogeny in the following lemma.

**Lemma 4.3.** *Let $F$ be the Frey–Hellegouarch curve* (10) *and let $m \geq 1$ be an integer. Let $F'$ be an elliptic curve which is isogenous to $F$ via a rational isogeny of degree $2^m$. Then $F'(\mathbb{Q})$ does not have a subgroup of order* 4.

*Proof.* By Lemmas 4.1 and 4.2, $F(\mathbb{Q})$ has only one subgroup of order $2^m$ with $m \geq 1$, and this is the subgroup generated by the point $(0, 0)$. Consequently, there is only one possible isogenous curve $F'$ to consider. By [27, Example III.4.5], this curve has a model given by

$$F' : V^2 = U^3 - \frac{Cx}{2}U^2 - \frac{Cq^k y^{2p}}{16}U,$$

and so it suffices to see that $F'(\mathbb{Q})$ does not have a subgroup of order 4. Firstly, we see that it does not have full $2-$torsion, as this would imply that

$$\frac{C^2x^2 + Cq^k y^{2p}}{4} = \frac{Cz^p}{4}$$

is a rational square. But this is not true since $C$ is squarefree and $\gcd(C, z) = 1$ by assumption.

Finally, we can see that $F'(\mathbb{Q})$ has no point of order 4 by mimicking the approach in Lemma 4.2. Indeed, we recall that $(0, 0)$ is the unique rational point of order 4 in $F'(\mathbb{Q})$. Consequently, if $(U_0, V_0) \in F'(\mathbb{Q})$ is a point of order 4, it follows that $[2](U_0, V_0) = (0, 0)$, and, after performing some computations, we find that

$$U_0^2 + \frac{Cq^k y^{2p}}{16} = 0,$$

which clearly has no solutions since $Cq^k y^{2p} > 0$. Consequently, $F'(\mathbb{Q})$ has no subgroup of order 4. $\square$

With this lemma, we can prove the following corollary, which will be useful in Section 4.2.

**Corollary 4.4.** *Suppose that AFLT does not hold for* (5)*, and let $E$ the elliptic curve given in Lemma 2.2. Then no curve isogenous to $E(\mathbb{Q})$ has a subgroup of order* 4.

*Proof.* Assume for contradiction that some curve in the isogeny class of $E(\mathbb{Q})$ has a subgroup of order 4, and let $F$ be the Frey–Hellegouarch curve (10). By Lemma 4.3, it follows that no curve isogenous to $F$ via a rational $2^m-$isogeny has a subgroup of order 4. Then, by [18, Problem I (bis) and Theorem 1], there exists a prime number $\ell$ such that $\ell \nmid N$, $4 \nmid \#F(\mathbb{F}_\ell)$ and $4 \mid \#E(\mathbb{F}_\ell)$. If we define the sets

$$A_\ell = \{a \in \mathbb{Z} \mid |a| < 2\sqrt{\ell}, \quad a \equiv \ell + 3 \pmod 4\}, \tag{21}$$

and

$$B_\ell = \{b \in \mathbb{Z} \mid |b| < 2\sqrt{\ell}, \quad b \equiv \ell + 1 \pmod 4\}, \tag{22}$$

then the Hasse–Weil bounds, along with the previous discussion, yield that

$$a_\ell(F) \in A_\ell \quad \text{and} \quad a_\ell(E) \in B_\ell.$$

By (15), we have that

$$p \mid \prod_{\substack{a \in A_\ell \\ b \in B_\ell}} (a - b) \prod_{b \in B_\ell} (b^2 - (\ell + 1)^2). \tag{23}$$

Since $A_\ell$ and $B_\ell$ are clearly disjoint, $a - b \neq 0$ for any $a \in A_\ell, b \in B_\ell$. In addition, we also have that $\pm(\ell+1) - b \neq 0$ for any $b \in B_\ell$ by the Hasse–Weil bounds. Thus, (23) means that $p$ divides a non-zero number. This is a contradiction with the fact that AFLT does not hold and, consequently, it follows that no curve in the isogeny class of $E(\mathbb{Q})$ has a subgroup of order 4. □

4.2. **A Galois theory sieve.** After Corollary 4.4, we are left with the case where $E(\mathbb{Q})$ has no subgroup of order 4. In order to find a bound $B_{C,q}$ for the exponent in this situation, it is sufficient to find a prime number $\ell \nmid N$ satisfying the following two properties:

- The group $F(\mathbb{F}_\ell)$ has a subgroup of order 4.
- The group $E(\mathbb{F}_\ell)$ does not have a subgroup of order 4.

In this case, a similar argument to that of the proof of Corollary 4.4 allows to find an upper bound $B_{C,q}$ for $p$, therefore proving AFLT for (5). Consequently, if AFLT does not hold, such a prime $\ell$ cannot exist. In Proposition 4.5, we find necessary conditions for the non-existence of these primes.

**Proposition 4.5.** *Suppose that AFLT does not hold for* (5)*, let $F$ be the Frey-Hellegouarch curve* (10) *and $E$ be the elliptic curve given by Lemma 2.2. Let $s \in \{0, 1\}$ satisfy $k \equiv s \pmod 2$. Then all primes $\ell \nmid N$ satisfy at least one of the following conditions:*

*(i) $-Cq^s$ is not a square modulo $\ell$.*

*(ii) $A^2 - 4B$ is a square modulo $\ell$.*

*(iii) $B$ is a square modulo $\ell$.*

The proof of Proposition 4.5 uses the following proposition, which is proved in [6, Proposition 6.4] and [7, Proposition 6.4].

**Proposition 4.6.** *Let $E$ be an elliptic curve defined over $\mathbb{Q}$ with discriminant $\Delta$, and let $\ell$ be a prime of good reduction for $E$. Furthermore, assume that $E$ has at least one $\mathbb{Q}-$rational point of order 2. Then the reduced curve has full 2-torsion over $\mathbb{F}_\ell$, if, and only if,the reduced discriminant $\Delta$ is a square mod $\ell$.*

*Proof of Proposition 4.5.* Suppose for contradiction that there is a prime $\ell$ not satisfying any of the three conditions (i), (ii) or (iii). By (11), the discriminant of the Frey–Hellegouarch curve $F$ is

$$\Delta = -2^{-12} C^3 q^k (yz)^{2p},$$

which, up to multiplication by rational squares, is equivalent to $-Cq^s$. Similarly, (17) yields that, up to multiplication by a rational square, the discriminant of $E$ is equivalent to $A^2-4B$. Then, Proposition 4.6, along with the fact that conditions (i) and (ii) are not satisfied, yields that $F(\mathbb{F}_\ell)$ has full $2-$torsion while $E(\mathbb{F}_\ell)$ does not.

In order to apply the methodology that we outlined at the beginning of this subsection, it remains to see that $E(\mathbb{F}_\ell)$ has no points of order 4. Let $(x_0, y_0) \in E(\mathbb{F}_\ell)$ be a point of order 4. Since the only $\mathbb{F}_\ell-$rational point of order 2 is $(0,0)$, we have that $[2](x_0,y_0)=(0,0)$. By the duplication formula for elliptic curves (see [27, Group Law Algorithm 2.3]), we have that

$$(x_0,y_0) \in \left\{ \left(\sqrt{B}, \pm\sqrt{B}\sqrt{A+2\sqrt{B}}\right), \left(-\sqrt{B}, \pm\sqrt{B}\sqrt{A-2\sqrt{B}}\right) \right\}. \tag{24}$$

Since condition (iii) is not satisfied, none of these points are $\mathbb{F}_\ell-$rational. Consequently, $E(\mathbb{F}_\ell)$ has no subgroup of order 4 while $F(\mathbb{F}_\ell)$ does and so, by defining $A_\ell$ and $B_\ell$ as in (21) and (22) respectively, we may exploit a similar argument to that of the proof of Corollary 4.4 to obtain an upper bound for $p$. Consequently, AFLT holds for (5), which is a contradiction with our hypotheses. □

## 5. Finding all possibilities for $E$

In order to prove Theorem 3, we want to exploit Lemma 2.2 and Propositions 3.1 and 4.5 to find a list of possibilities for the coefficients $A$ and $A^2-4B$ in the curve $E$. To do this, we need the following lemma, which is a consequence of Chebotarev's Density Theorem.

**Lemma 5.1.** *Let $x, y, z \in \mathbb{Q}$ be rational numbers satisfying the following conditions:*

- *Neither $x$ nor $y$ are rational squares.*
- *The number $z$ is not equivalent to either $x$ or $y$ up to multiplication by rational squares.*

*Then there exists a prime number $\ell$ such that $x$ and $y$ are non-squares modulo $\ell$ and $z$ is a square modulo $\ell$.*

*Proof.* Let $K=\mathbb{Q}(\sqrt{x}, \sqrt{y}, \sqrt{z})$. Then our conditions on $x, y$ and $z$ show that there exist an element $\sigma \in \operatorname{Gal}(K/\mathbb{Q})$ with $\sigma(\sqrt{x})=-\sqrt{x}$, $\sigma(\sqrt{y})=-\sqrt{y}$ and $\sigma(\sqrt{z})=\sqrt{z}$.

By Chebotarev's density theorem [8] (also stated in Section 3 of [23]), there is a positive density of primes $\ell$ such that the Frobenius of $K/\mathbb{Q}$ at $\ell$ is equal to $\sigma$. This condition is equivalent to $x$ and $y$ being non-squares modulo $\ell$ and $z$ being a square modulo $\ell$, as desired. □

The possible values for $B$ and $A^2-4B$ will be different depending on the parity of $k$. For simplicity, we separate our argument in two propositions.

**Proposition 5.2.** *Suppose that $k$ is odd in* (5). *Suppose furthermore that there does not exist an elliptic curve $E$ given by*

$$E: Y^2 = X(X^2+AX+B),$$

*where $A, B \in \mathbb{Z}$ satisfy one of the following conditions:*

*(A) Either we have that*

$$B = -q^{\gamma_1} \prod_{r|C \ prime} r^{\beta_r},$$

$$A^2 - 4B = 2^{\alpha_2} \prod_{r|C \ prime} r^{\beta_r},$$

*with $\alpha_2 > 8$, $\beta_r = 1, 3$ for all $r \mid C$ prime and $\gamma_1$ odd, or*

*(B) We have that*

$$B = 2^{\alpha_1} \prod_{r|C \ prime} r^{\beta_r},$$

$$A^2 - 4B = -q^{\gamma_2} \prod_{r|C \ prime} r^{\beta_r},$$

*with $\alpha_1 > 4$, $\beta_r = 1, 3$ for all $r \mid C$ prime and $\gamma_2$ odd.*

*Then AFLT holds for* (5).

*Proof.* Suppose that AFLT does not hold for (5). Then Lemma 2.2 yields the existence of a curve $E$ of conductor $N'$ as in (13). First, let us suppose that $p \neq k$, so that $N' = 2C^2q$. Then it follows that only 2, $q$ and the primes dividing $C$ can divide the discriminant $\Delta$ given in (17), so $B$ and $A^2 - 4B$ can be supported only on these primes.

In addition, since $2 \mid\mid N'$ and $q \mid\mid N'$, both 2 and $q$ are primes of multiplicative reduction for $E$ and therefore divide $\Delta$ while not dividing $c_4$. On the other hand, $C^2 \mid N'$ and so all primes $r$ dividing $C$ have additive reduction. Consequently, any such $r$ will divide both $c_4$ and $\Delta$. Since the expressions for $c_4$ and $\Delta$ are given in Lemma 2.2, we see that 2 and $q$ divide precisely one of $A^2 - 4B$ and $B$ while any prime $r \mid C$ divides both. In addition, by Proposition 3.1, we have that $\nu_r(B) = \nu_r(A^2 - 4B)$ for all $r \mid C$ prime.

Suppose that there exists a prime $\ell \nmid N$ such that $A^2 - 4B$ and $B$ are non-squares modulo $\ell$, while $-Cq$ is a square modulo $\ell$. Then Proposition 4.5 gives that AFLT holds for (5), which is a contradiction. By Lemma 5.1, such a prime $\ell$ will exist unless one of the following conditions are satisfied:

(a) The number $B$ is a rational square.

(b) The number $A^2 - 4B$ is a rational square.

(c) The number $B$ is equivalent, up to rational squares, to $-Cq$.

(d) The number $A^2 - 4B$ is equivalent, up to rational squares, to $-Cq$.

Let us consider each condition separately. If (a) is satisfied, this would mean that $\sqrt{B} \in \mathbb{F}_\ell$ for every prime number $\ell$. In addition, by the multiplicativity of the Legendre symbol, we have that

$$\left(\frac{A + 2\sqrt{B}}{\ell}\right)\left(\frac{A - 2\sqrt{B}}{\ell}\right) = \left(\frac{A^2 - 4B}{\ell}\right).$$

Consequently, at least one of the three previous Legendre symbols is equal to 1. If $A^2 - 4B$ is a square modulo $\ell$, the discriminant of the curve $E$ is a square modulo $\ell$ by (17) and so $E(\mathbb{F}_\ell)$ has full $2-$torsion by Proposition 4.6.

If either $A + 2\sqrt{B}$ or $A + 2\sqrt{B}$ are squares modulo $\ell$, at least two of the points of order 4 in (24) are defined over $\mathbb{F}_\ell$. In any case, $E(\mathbb{F}_\ell)$ has a subgroup of order 4 for all $\ell \nmid N'$. By [18, Theorem I], this means that there exists an elliptic curve $E'$ isogenous to $E$ and such that $E'(\mathbb{Q})$ has a subgroup of order 4. Then Corollary 4.4 yields that AFLT holds for (5).

Suppose now that condition (b) is satisfied. Then the discriminant $\Delta$ of $E$ is a square modulo $\ell$ for every prime number $\ell$. By Proposition 4.6, it follows that $4 \mid \#E(\mathbb{F}_\ell)$ for every prime number $\ell \nmid N'$. Then [18, Theorem I] yields that there exists a curve $E'$ isogenous to $E$ and such that $E'(\mathbb{Q})$ has a subgroup of order 4. Therefore, Corollary 4.4 gives that AFLT holds for (5).

Now, if condition (c) is satisfied, it follows that either

$$\begin{aligned} B &= -2^{\alpha_1} q^{\gamma_1} \prod_{r \mid C \text{ prime}} r^{\beta_r}, \\ A^2 - 4B &= \prod_{r \mid C \text{ prime}} r^{\beta_r}, \end{aligned} \tag{25}$$

with $\alpha_1 > 4$ even, $\beta_r$ odd for all $r \mid C$ prime and $\gamma_1 \equiv k \equiv 1 \pmod 2$, or

$$\begin{aligned} B &= -q^{\gamma_1} \prod_{r \mid C \text{ prime}} r^{\beta_r}, \\ A^2 - 4B &= 2^{\alpha_2} \prod_{r \mid C \text{ prime}} r^{\beta_r}, \end{aligned} \tag{26}$$

where $\alpha_2 > 8$, $\beta_r$ odd for all $r \mid C$ prime and $\gamma_1 \equiv k \equiv 1 \pmod 2$. We remark that $\alpha_1 > 4$ and $\alpha_2 > 8$ because 2 needs to divide the discriminant $\Delta$ given in (17). Now, the set of conditions (25) yield that $A^2 < 0$, while the set of conditions (26) correspond to case (A) in the statement of the Proposition.

Finally, suppose that condition (d) is satisfied. By a similar argument to the one in condition (c), case (B) in the proposition follows. In both situations, we have that the model for the curve $E$ in (18) is isomorphic to one where $\beta_r = 1$ or $\beta_r = 3$, and hence the proposition follows for $p \neq k$.

Assume now that $p = k$. In this case, we would have that $N' = 2C^2$. We deal with conditions (a) and (b) exactly as before. We note that, since $q \nmid N'$, it follows that $q \nmid B$ and $q \nmid A^2 - 4B$ and so conditions (c) and (d) cannot hold.

$\square$

*Remark* 7. A key ingredient in the proof of Proposition 5.2 is that 2 is a prime of multiplicative reduction for the Frey–Hellegouarch curve $F$ and therefore can only divide either $A^2 - 4B$ or $B$. In addition, as opposed to the rest of primes of additive reduction, it would be impossible to adapt Proposition 3.1 to relate $\nu_2(A^2 - 4B)$ and $\nu_2(B)$.

If we allow $z$ to be odd in (5), and as we mentioned at the beginning of Section 2, we would need to consider many more Frey–Hellegouarch curves. For some of these, 2 is a prime of additive reduction and, therefore, it is impossible to use the same arguments as in this paper.

If $k$ is even, the following proposition gives the possible values of $A^2-4B$ and $B$. Its proof is almost identical to that of Proposition 5.2, and we shall omit it.

**Proposition 5.3.** *Suppose that $k$ is even in* (5)*. Suppose furthermore that there does not exist an elliptic curve $E$ given by*

$$E : Y^2 = X(X^2 + AX + B),$$

*where $A, B \in \mathbb{Z}$ satisfy one of the following conditions:*

*(A') We have*

$$B = -2^{\alpha_1} \prod_{r|C} r^{\beta_r},$$

$$A^2 - 4B = q^{\gamma_2} \prod_{r|C \text{ prime}} r^{\beta_r},$$

*with $\alpha_1 > 4$ even, $\beta_r = 1, 3$ for all $r \mid C$ prime and $\gamma_2 \geq 0$, or*

*(B') We have*

$$B = -q^{\gamma_1} \prod_{r|C \text{ prime}} r^{\beta_r},$$

$$A^2 - 4B = 2^{\alpha_2} \prod_{r|C \text{ prime}} r^{\beta_r},$$

*with $\alpha_2 > 8$, $\beta_r = 1, 3$ for all $r \mid C$ prime and $\gamma_1 \geq 0$ even, or*

*(C') We have*

$$B = - \prod_{r|C \text{ prime}} r^{\beta_r},$$

$$A^2 - 4B = 2^{\alpha_2} q^{\gamma_2} \prod_{r|C \text{ prime}} r^{\beta_r},$$

*with $\alpha_2 > 8$, $\beta_r = 1, 3$ for all $r \mid C$ prime and $\gamma_2 \geq 0$, or*

*(D') We have*

$$B = 2^{\alpha_1} q^{\gamma_1} \prod_{r|C \text{ prime}} r^{\beta_r},$$

$$A^2 - 4B = - \prod_{r|C \text{ prime}} r^{\beta_r},$$

*with $\alpha_1 > 4, \beta_r = 1, 3$ for all $r \mid C$ prime and $\gamma_1 \geq 0$, or*

*(E') We have*

$$B = 2^{\alpha_1} \prod_{r|C \text{ prime}} r^{\beta_r},$$

$$A^2 - 4B = -q^{\gamma_2} \prod_{r|C \text{ prime}} r^{\beta_r},$$

*with $\alpha_1 > 4, \beta_r = 1, 3$ for all $r \mid C$ prime and $\gamma_2 \geq 0$ even, or*

*(F') We have*

$$B = q^{\gamma_1} \prod_{r \mid C \ prime} r^{\beta_r},$$
$$A^2 - 4B = -2^{\alpha_2} \prod_{r \mid C \ prime} r^{\beta_r},$$

*with $\alpha_2 > 8$ even, $\beta_r = 1, 3$ for all $r \mid C$ prime and $\gamma_1 \geq 0$.*

*Then AFLT holds for* (5).

## 6. Proof of Theorem 3

In this section, we prove Theorem 3 by studying the values for $B$ and $A^2 - 4B$ given in Propositions 5.2 and 5.3. We shall do this by relating the existence of these curves to the existence of solutions to certain Diophantine equations. This is compiled in the following proposition.

**Proposition 6.1.** *Suppose that AFLT does not hold for* (5). *Then one of the following three alternatives hold:*

*(i) There is a solution $(t, \gamma, m) \in \mathbb{Z}^3$ to the equation*

$$Ct^2 + q^\gamma = 2^m, \text{ with } m > 6 \text{ and } \gamma \geq 0 \text{ with } \gamma \equiv k \pmod 2,$$

*(ii) The exponent $k$ is even, $q \equiv 7 \pmod 8$ and there is a solution $(t, m, \gamma) \in \mathbb{Z}^3$ to the equation*

$$Ct^2 + 2^m = q^\gamma, \text{with } m > 6 \text{ even and } \gamma > 0 \text{ odd.} \tag{27}$$

*(iii) The exponent $k$ is even and there is a solution $(t, m, \gamma) \in \mathbb{Z}^3$ to the equation*

$$Ct^2 + 1 = 2^m q^\gamma, \text{with } m > 6 \text{ and } \gamma \geq 0. \tag{28}$$

*Proof.* First, let us suppose that either $k$ is odd or $k$ is even and alternatives $(B')$ or $(E')$ in Proposition 5.3 hold. Then we have that either

$$A^2 = 2^2 \left( 2^{\alpha_2 - 2} \prod_{r \mid C \text{ prime}} r^{\beta_r} - \prod_{r \mid C \text{ prime}} r^{\beta_r} q^{\gamma_1} \right),$$

or

$$A^2 = 2^{\alpha_1 + 2} \prod_{r \mid C \text{ prime}} r^{\beta_r} - \prod_{r \mid C \text{ prime}} r^{\beta_r} q^{\gamma_2},$$

where $\alpha_1 > 4$, $\alpha_2 > 8$, $\beta_r = 1, 3$ for all $r \mid C$ prime, and $\gamma_1, \gamma_2 \geq 0$ with $\gamma_1 \equiv \gamma_2 \equiv k \pmod 2$. Since $C$ is squarefree, both expressions can be rewritten as

$$A^2 = Cw^2(2^m - q^\gamma),$$

for certain integers $w > 0$, $m > 6$ and $\gamma \geq 0$ with $\gamma \equiv k \pmod 2$. Thus, it follows that

$$2^m - q^\gamma = Ct^2,$$

for certain integer $t > 0$. This corresponds to case (i) in the proposition. Suppose now that $k$ is even and that we are in cases $(A')$ or $(F')$ of Proposition 5.3. Then we have that either

$$A^2 = \prod_{r \mid C \text{ prime}} r^{\beta_r} \left( q^{\gamma_2} - 2^{\alpha_1 + 2} \right),$$

or

$$A^2 = 2^2 \prod_{r|C \text{ prime}} r^{\beta_r} \left(q^{\gamma_1} - 2^{\alpha_2 - 2}\right),$$

with $\beta_r = 1, 3$ for all $r \mid C$ prime, $\gamma_1, \gamma_2 > 0$, $\alpha_1 > 4$ even and $\alpha_2 > 8$ even. Hence, by similar reasoning, there is a solution $(t, m, \gamma) \in \mathbb{Z}^3$ of

$$Ct^2 + 2^m = q^\gamma, \tag{29}$$

with $m > 6$ even. Note that, in order for (5) to have a solution with $z$ and $k$ even, it follows that $C \equiv 7 \pmod 8$. From (29), we see that this implies that $q \equiv 7 \pmod 8$ and $\gamma$ is odd. This proves (27) and alternative (ii) of the proposition.

Finally, let us consider the remaining cases $(C')$ and $(D')$ of Proposition 5.3. In these cases, we have that

$$A^2 = 2^2 \prod_{r|C \text{ prime}} r^{\beta_r} \left(2^{\alpha_2 - 2} q^{\gamma_2} - 1\right),$$

$$A^2 = \prod_{r|C \text{ prime}} r^{\beta_r} \left(2^{\alpha_1 + 2} q^{\gamma_1} - 1\right),$$

with $\beta_r = 1, 3$ for all $r \mid C$ prime, $\alpha_1 > 4$, $\alpha_2 > 8$, $\gamma_1 \geq 0$ and $\gamma_2 \geq 0$. Once more, this is equivalent to the existence of an integral solution $(t, m, \gamma) \in \mathbb{Z}^3$ of

$$Ct^2 + 1 = 2^m q^\gamma,$$

where $m > 6$ and $\gamma \geq 0$, which proves (28) and alternative (iii) in the proposition. □

Theorem 3 is a direct consequence of the previous proposition, and the proof is immediate.

*Proof of Theorem 3.* In order to see that AFLT holds for (5), it suffices to see that none of the conditions (i), (ii) or (iii) in Proposition 6.1 are satisfied.

By the hypotheses in the Theorem, (7) does not have any solutions and so alternative (i) does not hold. Similarly, hypotheses (a), (b), (c) and (d) in Theorem 3 directly imply that alternatives (ii) and (iii) in Proposition 6.1 are not safisfied. Consequently, AFLT holds for (5), as we wanted to show.

□

## 7. Checking the conditions in Theorem 3

In order to computationally verify whether the conditions in Theorem 3 are met, we need to resolve three Diophantine equations ((7), (8) and (9)). This can be done by means of the `Magma` code available in https://shorturl.at/hoxW8, which we will briefly explain in this section.

For (7), the methods outlined by the author in [6] could be used to achieve a complete solution for the more general equation

$$Ct^2 + q^\gamma = w^m. \tag{30}$$

These methods involve the use of the modular methodology, along with lower bounds for linear forms in three logarithms and the resolution of Thue–Mahler equations.

However, solving (7) is, in practice, significantly easier than solving (30) since $w$ is restricted to be a power of 2. We note that (7) is a particular case of (5), and, therefore, we may then adapt the Frey–Hellegouarch curve (10) to (7) by setting $x = t$, $y = 1$ and $z = 2$. Then we realise that, by (12), $F$ has conductor equal to $N = 2C^2q$ if $\gamma \neq 0$ and equal to $N = 2C^2$ if $\gamma = 0$. In addition, the minimal discriminant is equal to

$$\Delta = -2^{2m-12}C^3q^{\gamma}.$$

If $N < 500,000$, we may get all elliptic curves of conductor $N$ from Cremona's tables ([9]) and recover $\gamma, m$ and subsequently $t$, just by inspecting its minimal discriminant.

If $N \geq 500,000$, the curve is not in Cremona's database. However, we let $m = 3a + b$, where $a \geq 0$ and $b \in \{0, 1, 2\}$. We also let $\gamma = 6c + d$, where $c \geq 0$ and $d \in \{0, \dots, 5\}$. Then it can then be checked that the point $(U, V)$ given by

$$(U, V) = \left(\frac{C \cdot 2^{a+b}}{q^{2c}}, \frac{C^2 \cdot 2^b \cdot t}{q^{3c}}\right)$$

is a rational point on the elliptic curve $E_{b,d}$ given by the expression

$$E_{b,d} : V^2 = U^3 - C^3 2^{2b} q^d.$$

Furthermore, it is clear that the only prime which can occur in the denominators of $U$ and $V$ is $q$ and, consequently, $(U, V)$ is a $\{q\}-$integral point. Therefore, it is sufficient to determine all $\{q\}-$integral points on the 18 curves $E_{b,d}$, where $b = 0, 1, 2$ and $d = 0, \dots, 5$. In our code, we do this with a combination of [17, Algorithm 4.2] and the built-in `Magma` function for computing $S-$integral points on elliptic curves.

An identical approach can be used for (9). For this, we let $m = 6a' + b'$, where $a' \geq 0$ and $b' \in \{0, \dots, 5\}$ and we let $\gamma = 3c' + d'$, with $c' \geq 0$ and $d' \in \{0, 1, 2\}$. Then the pair $(U', V')$ given by

$$(U', V') = \left(\frac{C \cdot q^{c'+d'}}{2^{2a'}}, \frac{C^2 \cdot q^{d'} \cdot w}{2^{3a'}}\right),$$

is a $\{2\}-$integral point on one of the 18 Mordell curves $F_{b',d'}$ given by

$$F_{b',d'} : (V')^2 = (U')^3 - C^3 \cdot 2^{b'} \cdot q^{2d'}.$$

These points can be computed in precisely the same way as before. Finally, for (8), it is sufficient to resolve the Ramanujan-Nagell type equation

$$u^2 + C = Cv,$$

where $u \in \mathbb{Z}$ and $v \in \mathbb{Z}$ is only supported on the primes 2 and $q$. This can be done by directly employing [17, Algorithm 6.2].

Finally, by combining all the aforementioned techniques, we can finish the proof of Theorem 4.

*Proof of Theorem 4.* If there are any solutions $(x, y, z, n)$ to (5), it is elementary to check that $Cq^k \equiv 7 \pmod 8$ by reducing (5) modulo 8. If $k$ is even, this condition is equivalent to $C \equiv 7 \pmod 8$ while if $k$ is odd, it is equivalent to $Cq \equiv 7 \pmod 8$.

For each suitable pair in the range $1 \leq C \leq 70$ and $3 \leq q < 100$, our `Magma` program uses the techniques in this section to check whether the conditions in Theorem 3 are satisfied. The results are shown in Table 1. □

## References

[1] K. Belabas, F. Beukers, P. Gaudry, H. Lenstra, W. McCallum, B. Poonen, S. Siksek, M. Stoll, M. Watkins, *Explicit Methods in Number Theory: Rational Points and Diophantine Equations*, Panoramas et synthèses **36**, Société Mathématique de France, Paris, 2012.

[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.

[3] M. A. Bennett and S. Siksek, *Differences between perfect powers: The Lebesgue–Nagell equation*, Transactions of the AMS, to appear, https://arxiv.org/abs/2109.09128.

[4] N. Billerey, I. Chen, L. Dieulefait, N. Freitas, *A multi-Frey approach to Fermat equations of signature $(r, r, p)$*, Transactions of AMS **371**(2019), pp. 8651–8677.

[5] Y. Bugeaud, M. Mignotte and S. Siksek, *Classical and modular approaches to exponential Diophantine equations II. The Lebesgue–Nagell equation*, Compositio Math. **142** (2006), 31–62.

[6] P. J. Cazorla-García, *On differences of perfect powers and prime powers*, available online on https://arxiv.org/abs/2312.09985.

[7] P. J. Cazorla-García and V. Patel, *On the generalised Lebesgue–Nagell equation*, in preparation.

[8] N. G. Chebotarev, *Die bestimmung der dichtigkeit einer menge von primzahlen, welche zu einer gegebenen substitutionsklasse gehören*, Mathematische Annalen, **95**, 191–228, 1926.

[9] J. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press (1997), `https://homepages.warwick.ac.uk/staff/J.E.Cremona/book/fulltext/index.html`.

[10] H. Darmon and A. Granville. On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. *Bull. London Math. Soc.*, 27(6):513–543, 1995.

[11] H. Deconinck, *On the generalized Fermat equation over totally real fields*, Acta Arithmetica **173**(3), 2016, 225–237.

[12] N. Freitas and S. Siksek, *The Asymptotic Fermat's Last Theorem for Five-Sixths of Real Quadratic Fields*, Compositio Mathematica **151** (2015), 1395–1415.

[13] E. Işik, E. Özman and Y. Kara, *On ternary Diophantine equations of signature $(p, p, 2)$ over some totally real number fields*, Turkish Journal of Mathematics **44**(4), 2020, 1197–1211.

[14] E. Işik, E. Özman and Y. Kara, *On ternary Diophantine equations of signature $(p, p, 3)$ over number fields*, Canadian Journal of Mathematics **75** (4), 2023, 1293–1313.

[15] W. Ivorra, *Sur les équations $x^p + 2^\beta y^p = z^2$ et $x^p + 2\beta y^p = 2z^2$*, Acta Arithmetica **108**(4), 2003, 327–338.

[16] W. Ivorra and A. Kraus, *Some results on the equations $ax^p + by^p = cz^2$*, Canadian Journal of Mathematics **58**, 2006, 115–156.

[17] R. von Känel and B. Matschke, *Solving S-unit, Mordell, Thue, Thue–Mahler and generalized Ramanujan–Nagell equations via Shimura–Taniyama conjecture*, Memoirs of the American Mathematical Society, **286** (1419), 2016.

[18] N. M. Katz, *Galois properties of torsion points on abelian varieties*, Inv. Math. **62**, 1981, 481–502.

[19] A. Kraus, *Sur l' ´équation $a^3 + b^3 = c^p$*, Experimental Mathematics **7** (1998), No. 1, 1–13.

[20] N. Kumar and S. Sahoo, *On the solutions of $x^p + y^p = 2^r z^p$, $x^p + y^p = z^2$ over totally real fields*, 2022, https://arxiv.org/abs/2207.10930.

[21] N. Kumar and S. Sahoo, *On the solutions of $x^2 = By^p + Cz^p$ and $2x^2 = By^p + Cz^p$ over totally real fields*, 2023, https://arxiv.org/abs/2301.09263.

[22] M. Le and G. Soydan, *A brief survey on the generalized Lebesgue–Ramanujan–Nagell equation*, Surveys in Mathematics and its Applications **15** (2020), 473–523.

[23] H. W. Lenstra, and P. Stevenhagen, *Chebotarev and his density theorem*, Mathematics Intelligencer, **18** (2), 26–37, 1995.

[24] D. Mocanu, *Asymptotic Fermat for signatures $(p,p,2)$ and $(p,p,3)$ over totally real fields*, Mathematika **68**(4), 1233–1257.

[25] K. A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.

[26] S. Siksek, *The modular approach to Diophantine equations*, pages 151–179 of [1].

[27] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer (2009).

[28] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

Department of Mathematics, University of Manchester, Manchester, United Kingdom, M13 9PY

*Email address*: `pedro-jose.cazorlagarcia@manchester.ac.uk`