JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Abdulmuhsin ALFARAJ

On the Finiteness of Perfect Powers in Elliptic Divisibility Sequences

Tome 35, nº 1 (2023), p. 247-258.

https://doi.org/10.5802/jtnb.1244

Le Journal de Théorie des Nombres de Bordeaux *est membre du Centre Mersenne pour l'édition scientifique ouverte*
http://www.centre-mersenne.org/
e-ISSN : 2118-8572

Journal de Théorie des Nombres de Bordeaux **35** (2023), 247–258

On the Finiteness of Perfect Powers in Elliptic Divisibility Sequences

par Abdulmuhsin ALFARAJ

Résumé. Nous prouvons qu'il n'existe qu'un nombre fini de puissances parfaites dans les suites de divisibilité elliptiques générées par un point non entier sur une courbe elliptique de la forme $y^2 = x(x^2 + b)$, où b est un entier positif non nul. Nous y parvenons en utilisant la modularité des courbes elliptiques sur les corps quadratiques réels.

Abstract. We prove that there are finitely many perfect powers in elliptic divisibility sequences generated by a non-integral point on elliptic curves of the form $y^2 = x(x^2 + b)$, where b is any positive integer. We achieve this by using the modularity of elliptic curves over real quadratic number fields.

1. Introduction

We start by explaining what we mean by an elliptic divisibility sequence.

Definition 1.1. Let $E/\mathbb{Q}$ be an elliptic curve given in Weierstrass form. Let $P \in E(\mathbb{Q})$ be a non-torsion point. For all $m \in \mathbb{N}$, we can write

$$mP = \left(A_m/B_m^2, C_m/B_m^3\right),$$

where A_m, B_m, C_m are integers, $B_m \neq 0$, and $\gcd(A_m, B_m) = \gcd(C_m, B_m) = 1$. We say that $\{B_m\}$ is the elliptic divisibility sequence generated by P.

In this paper we prove the finiteness of perfect powers in elliptic divisibility sequences generated by a non-integral point in a new class of elliptic curves.

Theorem 1.2. *Let $\{B_m\}$ be an elliptic divisibility sequence generated by a non-integral point on any elliptic curve over $\mathbb{Q}$ of the form*

$$E \,:\, y^2 = x(x^2 + b),$$

where b is a positive integer. Then there are finitely many perfect powers in $\{B_m\}$.

Manuscrit reçu le 17 décembre 2021, révisé le 28 avril 2022, accepté le 21 mai 2022.
2020 *Mathematics Subject Classification.* 11B83, 11D61, 11G05.
Mots-clefs. Modular methods, Elliptic divisibility sequences, Perfect powers.

We prove this using the so-called modular approach, which is inspired by the proof of Fermat's last theorem, along with utilizing the properties of elliptic divisibility sequences. The modular method was first used to study integer solutions to special classes of Diophantine equations, and it mainly relies on the modularity theorem and Ribet's level-lowering theorem. Recently, Freitas, Le Hung, and Siksek [10] proved that elliptic curves over real quadratic number fields are modular. Moreover, Fujiwara [13], Jarvis [15] and Rajaei [17] proved level lowering theorems for Hilbert eigenforms. The former (i.e. the theorems) can be regarded as generalisations of Ribert's level lowering theorem. This allowed us to apply the modular method when working with equations which have coefficients in real quadratic fields, which was a main part of our proof.

The study of the finiteness of perfect powers in sequences first started with the Fibonacci sequence and the Lucas sequence. By utilizing modular methods along with other techniques, Bugeaud, Mignotte and Siksek [3] proved that the only perfect powers in the Fibonacci sequence and the Lucas sequence are $\{0, 1, 8, 144\}$ and $\{1, 4\}$, respectively. This motivated the study of perfect powers in other special sequences, such as elliptic divisibility sequences. Everest and King [8] showed that, when assuming certain conditions on the generating point, the corresponding elliptic divisibility sequence contains only a finite number of elements that are powers of primes. In [9], Everest, Reynolds, and Stevens showed that the number of perfect powers of a fixed exponent in an elliptic divisibility sequence is finite by invoking Faltings' theorem. If the first term of the sequence is divisible by 2 or 3, or if the sequence arises from a Mordell curve where the first term is greater than 1, Reynolds [18] has shown that there are only finitely many terms that are perfect powers in both of these cases by using the modular approach.

Outline of the paper. We start by collecting some relevant results about elliptic curves in Section 2. In Section 3, we state some properties of elliptic divisibility sequences. In Section 4 we briefly cover results on the modularity of elliptic curves over quadratic number fields along with a level-lowering theorem. Finally, we prove Theorem 1.2 in Section 5.

2. Elliptic Curves

In this section we collect some relevant results about elliptic curves over number fields. The primary aim of this section is to provide sufficient conditions to check if a defining equation of an elliptic curve is minimal at a prime ideal, and to identify its type of reduction modulo a prime ideal.

Let E be an elliptic curve over some field K. We say that E/K is given in Weierstrass form if the elliptic curve is defined by the equation

$$E \,:\, y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_1, a_2, a_3, a_4, a_6 \in K$. We define the quantities Δ and c_4 as in III.1 in [19].

Let K be a number field and $\mathcal{O}_K$ be its ring of integers. Let $v_\mathfrak{p}$ be the discrete valuation of K with respect to the prime ideal $\mathfrak{p}$. We write $K_\mathfrak{p}$ for the completion of K at $v_\mathfrak{p}$, $\mathcal{O}_\mathfrak{p}$ for its ring of integers, $\mathfrak{p}$ for the maximal ideal of $\mathcal{O}_\mathfrak{p}$, and $k_\mathfrak{p} = \mathcal{O}_\mathfrak{p}/\mathfrak{p}$, the residue field of $\mathcal{O}_\mathfrak{p}$. We say that a Weierstrass equation for E/K is minimal at $\mathfrak{p}$ if $v_\mathfrak{p}(\Delta)$ is minimal subject to the condition that $a_1, a_2, a_3, a_4, a_6 \in \mathcal{O}_\mathfrak{p}$.

Remark 2.1. Suppose we are given a Weierstrass equation of E/K with coefficients in $\mathcal{O}_\mathfrak{p}$. If $v_\mathfrak{p}(\Delta) < 12$ or $v_\mathfrak{p}(c_4) < 4$, then the equation is minimal at $\mathfrak{p}$ (Remark VII.1.1 in [19]).

Proposition 2.2 (VII.5.1 in [19])**.** *Let E/K be an elliptic curve given by a minimal Weierstrass equation for E at some $\mathfrak{p}$. Then*

1. *E has good reduction at $\mathfrak{p}$ if and only if $v_\mathfrak{p}(\Delta) = 0$;*
2. *E has multiplicative reduction at $\mathfrak{p}$ if and only if $v_\mathfrak{p}(\Delta) > 0$ and $v_\mathfrak{p}(c_4) = 0$;*
3. *and E has additive reduction at $\mathfrak{p}$ if and only if $v_\mathfrak{p}(\Delta) > 0$ and $v_\mathfrak{p}(c_4) > 0$.*

We say that E has semistable reduction at $\mathfrak{p}$ if it has either good or multiplicative reduction at $\mathfrak{p}$. We warn the reader that this terminology is used exclusively for multiplicative reduction in [19].

Definition 2.3. We define the conductor of E/K to be

$$\mathcal{N} = \prod_{\mathfrak{p} \text{ prime ideal}} \mathfrak{p}^{f_\mathfrak{p}(E)},$$

where for all primes $\mathfrak{p}$ not dividing 2 or 3,

$$f_\mathfrak{p}(E) = \begin{cases} 0 & \text{if } E \text{ has good reduction at } \mathfrak{p}, \\ 1 & \text{if } E \text{ has multiplicative reduction at } \mathfrak{p}, \\ 2 & \text{if } E \text{ has additive reduction at } \mathfrak{p}; \end{cases}$$

and for $\mathfrak{p}$ dividing 2 or 3, $f_\mathfrak{p}(E)$ is defined similarly, except for when E has additive reduction; in which case, $f_\mathfrak{p}(E)$ may have values greater than 2.

Remark 2.4. By Theorem IV.10.4 in [21], for all primes $\mathfrak{p}$, $f_\mathfrak{p}(E)$ has a bound depending only on the number field K.

3. Elliptic Divisibility Sequences

In this section we state some properties of elliptic divisibility sequences that we will be using in the proof of Theorem 1.2.

First, we note that our definition of an elliptic divisibility sequence is the one used by Silverman in [14], and by Everest in [8]. The term elliptic divisibility sequence was also used by Ward in [24] to define a closely related class of sequences satisfying certain recurrence relations. In this paper, we work with Definition 1.1 of an elliptic divisibility sequence.

We say that an element of a sequence of integers has a primitive divisor if it is divisible by a prime p that does not divide any element preceding it.

Example 3.1. Consider the elliptic curve

$$E \,:\, y^2 = x(x^2+5)$$

over $\mathbb{Q}$. The Mordell–Weil group of $E(\mathbb{Q})$ has rank 1, with generator $P = (20, 90)$, and torsion subgroup equal to the idenitity and the 2-torsion point $(0, 0)$. Consider the elliptic divisibility sequence $\{B_m\}$ generated by mP. Using the computer algebra package Magma [2], we computed the following multiples of P

$$2P = \left(\frac{6241}{36^2}, \frac{543599}{36^3}\right), \quad 3P = \left(\frac{700217780}{19679^2}, \frac{29468421431730}{19679^3}\right),$$
$$\text{and} \quad 4P = \left(\frac{933424765104001}{39139128^2}, \frac{10846791171022019729184 1}{39139128^3}\right).$$

Thus, the first 4 elements of the sequence are $B_1 = 1$, $B_2 = 36$, $B_3 = 19679$, and $B_4 = 39139128$. Note that the primitive divisors of B_2 are $\{2, 3\}$, of B_3 are $\{11, 1789\}$, and of B_4 are $\{7, 79, 983\}$.

Theorem 3.2 (Silverman [20])**.** *Let $\{B_m\}$ be an elliptic divisibility sequence. Then, the number of elements in $\{B_m\}$ not having a primitive divisor is finite.*

Elliptic divisibility sequences satisfy certain divisibility properties as the name suggests.

Proposition 3.3 (Lemma IV.3.1 & Corollary IV.4.5 in [22])**.** *Let $\{B_m\}$ be an elliptic divisibility sequence generated by a non-torsion point on some elliptic curve over $\mathbb{Q}$ given by an integral Weierstrass equation.*

(i) *Let p be an odd prime, and n, $m \in \mathbb{N}$. If $v_p(B_n) > 0$, then*

$$v_p(B_{nm}) = v_p(B_n) + v_p(m).$$

Suppose that $p = 2$ and $2 \mid a_1$, the coefficient in the Weiestrass equation. If $v_2(B_n) > 0$, then

$$v_2(B_{nm}) = v_2(B_n) + v_2(m).$$

(ii) $\{B_m\}$ *is a strong divisibility sequence, i.e., for all* n, $m \in \mathbb{N}$,

$$\gcd(B_m, B_n) = B_{\gcd(m,n)}.$$

Note that for the elliptic curve we are considering in Theorem 1.2, we have that $a_1 = 0$. Thus, the condition $2 \mid a_1$ is satisfied.

As a consequence of Theorem 3.2 and Proposition 3.3, we have the following lemma which will be a crucial step in proving Theorem 1.2. It says that whenever the first element of the sequence has a prime divisor, and given a finite set of primes, any element of the sequence that is an ℓ-th power for a prime ℓ large enough will have a prime divisor outside this finite set.

Lemma 3.4. *Let* $\{B_m\}$ *be an elliptic divisibility sequence generated by a non-torsion point on some elliptic curve over* $\mathbb{Q}$ *given by an integral Weierstrass equation, where* $2 \mid a_1$. *Suppose that* B_1 *is divisible by some prime number* q. *Let* T *be a finite set of prime numbers. There exists a positive integer* k *and a prime* $p \notin T$ *such that if* B_m *is an* ℓ*-th power for some prime* $\ell > k$, *then* $p \mid B_m$.

Proof. By Theorem 3.2, all but finitely many elements of $\{B_m\}$ have primitive divisors. Since T is a finite set of primes, we can always choose a large enough positive integer k such that the element $B_{q^{k-v_q(B_1)}}$ has a primitive divisor p not contained in T.

Let B_m is an ℓ-th power for some prime $\ell > k$. Since $q|B_1$, Proposition 3.3 implies that

$$\ell \le v_q(B_m) = v_q(B_1) + v_q(m) \implies v_q(m) \ge k - v_q(B_1),$$

that is, $q^{k-v_q(B_1)} \mid m$. Thus, by Proposition 3.3, we have

$$p \mid B_{q^{k-v_q(B_1)}} = B_{\gcd(q^{k-v_q(B_1)},m)} = \gcd(B_{q^{k-v_q(B_1)}}, B_m).$$

Therefore, $p \mid B_m$. □

4. Modularity and Level-Lowering

Let K be a totally real number field, and denote the absolute Galois group of K by $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. Let E be an elliptic curve over K, and write $\rho_{E,p}$ for the Galois representation arising from the action of G_K on the p-adic Tate module $T_p(E)$. We say that E is modular if there exists a Hilbert cuspidal eigenform $\mathfrak{f}$ of parallel weight 2 with rational Hecke eigenvalues such that the L-function of $\mathfrak{f}$ is equal to the Hasse–Weil L-function of E. Another way to express this is that there exists an isomorphism of compatible systems of Galois representations $\rho_{E,p} \cong \rho_{\mathfrak{f},p}$ where $\rho_{\mathfrak{f},p}$ is the Galois representation associated to $\mathfrak{f}$ by Eichler and Shimura [7] for $K = \mathbb{Q}$, and by Carayol [4, 5], Blasius and Rogawski [1], Wiles [25] and Taylor [23] for any totally real number field K.

Theorem 4.1 (Freitas, Le Hung, & Siksek [10])**.** *Let E be an elliptic curve over a real quadratic number field. Then E is modular.*

Denote by

$$\bar{\rho}_{E,p} : G_K \longrightarrow \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$$

the representation giving the action of G_K on $E[p]$, the p-torsion of E. Let $\mathfrak{f}$ be Hilbert eigenform $\mathfrak{f}$ over K. We denote by $\mathbb{Q}_\mathfrak{f}$ the number field generated by the eigenvalues $a_\mathfrak{q}(\mathfrak{f})$ at all prime ideals $\mathfrak{q}$ of $\mathcal{O}_K$.

The following theorem, stated in [11], is a useful summary of level lowering results of Fujiwara [13], Jarvis [15] and Rajaei [17] in the context of modular elliptic curves.

Theorem 4.2. *Let K be a totally real number field, and E/K an elliptic curve of conductor $\mathcal{N}$. Let ℓ be a rational prime. For a prime ideal $\mathfrak{q}$ of K denote by $\Delta_\mathfrak{q}$ the discriminant of a local minimal model for E at $\mathfrak{q}$. Let*

$$\mathcal{M}_\ell := \prod_{\mathfrak{p}||\mathcal{N},\, \ell | v_\mathfrak{p}(\Delta_\mathfrak{p})} \mathfrak{p}, \quad \mathcal{N}_\ell := \frac{\mathcal{N}}{\mathcal{M}_\ell}.$$

Suppose the following

(i) *$\ell \geq 5$, the ramification index $e(\mathfrak{q}/\ell) < \ell - 1$ for all $\mathfrak{q} \mid \ell$, and $\mathbb{Q}(\zeta_l)^+ \not\subset K$;*
(ii) *E is modular;*
(iii) *$\bar{\rho}_{E,\ell}$ is irreducible;*
(iv) *E is semistable at all $\mathfrak{q} \mid \ell$;*
(v) *$\ell \mid v_\mathfrak{q}(\Delta_\mathfrak{q})$ for all $\mathfrak{q} \mid \ell$.*

Then, there is a Hilbert eigenform $\mathfrak{f}$ of parallel weight 2 that is new at level $\mathcal{N}_\ell$ and some prime ideal λ of the ring of integers of $\mathbb{Q}_\mathfrak{f}$ such that $\lambda \mid \ell$ and $\bar{\rho}_{E,\ell} \sim \bar{\rho}_{\mathfrak{f},\lambda}$.

Remark 4.3. Following the notation of Theorem 4.2, suppose that $\bar{\rho}_{E,\ell} \sim \bar{\rho}_{\mathfrak{f},\lambda}$. Let $\mathfrak{p}$ be a non-zero prime ideal in K. By comparing the traces of the images of Frobenius at $\mathfrak{p}$ in $\bar{\rho}_{E,\ell}$ and $\bar{\rho}_{\mathfrak{f},\lambda}$ we have the following.

(i) If $\mathfrak{p} \nmid \ell\mathcal{N}$, then $a_\mathfrak{p}(E) \equiv a_\mathfrak{p}(\mathfrak{f}) \mod \lambda$.
(ii) If $\mathfrak{p} \nmid \ell\mathcal{N}_\ell$ and $\mathfrak{p} \,||\, \mathcal{N}$, then $\pm(\mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{p}) + 1) \equiv a_\mathfrak{p}(\mathfrak{f}) \mod \lambda$.

We will be using the following result which shows that, under certain assumptions, (iii) in Theorem 4.2 is satisfied whenever ℓ is greater than some bound depending only the number field K.

Theorem 4.4 (Freitas & Siksek [12])**.** *Let K be a Galois totally real field. There is an effective constant C_K, depending only on K, such that the following holds. If $\ell > C_K$ is prime, and E is an elliptic curve over K which is semistable at all $\mathfrak{l} \mid \ell$, then $\bar{\rho}_{E,\ell}$ is irreducible.*

5. Proof of Theorem 1.2

To prove Theorem 1.2, the crucial step is to bound the exponent of any perfect power. To do that, we associate a specific Frey curve to any point mP with B_m a large enough ℓ-th power, and by using modularity and level lowering, we obtain a bound that only depends on the point P and the positive integer b. In fact, the proof provides an effective method to compute this bound explicitly.

We obtain Theorem 1.2 by combining the aforementioned bound on ℓ with a result by Everest, Reynolds and Stevens [9], which shows that there are only finitely many powers of a fixed exponent.

We start by proving a lemma that will allow us to associate an appropriate Frey curve to an equation obtained from substituting mP in the equation of E. The idea of this Frey curve construction was first considered in [6] in connection with the equation $x^4 + y^4 = z^p$, where p is a prime number.

Lemma 5.1. *Let ℓ be a prime, and let a, d, u, v, and w be non-zero integers. Suppose that a, d are positive, a is square-free, $\gcd(u, v) \mid ad$, and that*

$$v^2 - au^4 = dw^{4\ell}. \tag{5.1}$$

Then we can associate to (5.1) *the Frey curve*

$$F: \ Y^2 = X(X^2 + 4u\sqrt{a}X + 2\sqrt{a}(v + u^2\sqrt{a})), \tag{5.2}$$

over the number field $K = \mathbb{Q}(\sqrt{a})$, where $\Delta_F \neq 0$. Moreover, for all non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ such that $\mathfrak{p} \nmid 2ad$, the curve F is minimal at $\mathfrak{p}$, has semistable reduction at $\mathfrak{p}$, and $\ell \mid v_{\mathfrak{p}}(\Delta_F)$.

Proof. Factoring over $\mathcal{O}_K$, we have

$$(v + u^2\sqrt{a})(v - u^2\sqrt{a}) = dw^{4\ell}. \tag{5.3}$$

If $\mathfrak{q}$ is a non-zero a prime ideal of $\mathcal{O}_K$ that divides both $(v + u^2\sqrt{a})$ and $(v - u^2\sqrt{a})$, then $\mathfrak{q} \mid 2ad$, since $\gcd(u, v) \mid ad$. Thus, by the unique factorization of ideals into products of prime ideals, we obtain

$$(v + u^2\sqrt{a})\mathcal{O}_K = \mathfrak{b}_1\mathfrak{a}_1^\ell \quad \text{and} \quad (v - u^2\sqrt{a})\mathcal{O}_K = \mathfrak{b}_2\mathfrak{a}_2^\ell, \tag{5.4}$$

where $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{b}_1, \mathfrak{b}_2$ are ideals in $\mathcal{O}_K$, and $\mathfrak{b}_1\mathfrak{b}_2 \mid 2ad\mathcal{O}_K$. Now, notice that

$$(v + u^2\sqrt{a}) - (v - u^2\sqrt{a}) = 2u^2\sqrt{a}. \tag{5.5}$$

We associate the following Frey curve to a putative solution (u, v, w) of the equation (5.5):

$$F: \ Y^2 = X(X^2 + 4u\sqrt{a}X + 2\sqrt{a}(v + u^2\sqrt{a})),$$

where

$$\Delta_F = -2^9 a\sqrt{a}(v + u^2\sqrt{a})^2(v - u^2\sqrt{a}) \tag{5.6}$$

and

$$c_4 = 32\sqrt{a}(3v - 5u^2\sqrt{a}).$$

Suppose that $a \neq 1$. Since a is square free, $\sqrt{a}$ is irrational; hence, $\Delta_F \neq 0$. Now if $a = 1$ and $\Delta_F = 0$, then $dw^{4\ell} = (v + u^2\sqrt{a})(v - u^2\sqrt{a}) = 0$, contradicting that both d and w are non-zero. Therefore, Δ_F is non-zero.

Let $\mathcal{S}$ be the set of non-zero prime ideals in $\mathcal{O}_K$ dividing $2ad$. Now, if $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ that divides both Δ_F and c_4, then $\mathfrak{p}$ will either divide $(v + u^2\sqrt{a})$ and $(3v - 5u^2\sqrt{a})$, or $(v - u^2\sqrt{a})$ and $(3v - 5u^2\sqrt{a})$. If $\mathfrak{p}$ divides $(v + u^2\sqrt{a})$ and $(3v - 5u^2\sqrt{a})$, then it will divide

$$3(v + u^2\sqrt{a}) - (3v - 5u^2\sqrt{a}) = 8u^2\sqrt{a}$$

and

$$5(v + u^2\sqrt{a}) + (3v - 5u^2\sqrt{a}) = 8v$$

implying that $\mathfrak{p}$ divides both $2u\sqrt{a}$ and $2v$. Since $\gcd(u, v) \mid ad$, we have that $\mathfrak{p}$ divides $(2d\sqrt{a})\mathcal{O}_K$. A similar argument with the other pair also gives that $\mathfrak{p} \mid (2d\sqrt{a})\mathcal{O}_K$. Thus, if $\mathfrak{p}$ divides Δ_F and c_4, then $\mathfrak{p} \in \mathcal{S}$.

Therefore, by Remark 2.1, the curve F is minimal at all primes $\mathfrak{p} \notin \mathcal{S}$. Moreover, by Proposition 2.2, the curve F has good or multiplicative reduction at all primes $\mathfrak{p} \notin \mathcal{S}$. Also, if $\mathfrak{p} \notin \mathcal{S}$ and $\mathfrak{p} \mid \Delta_F$, then (5.4) and (5.6) imply that $\mathfrak{p}$ divides $\mathfrak{a}_1^\ell$ or $\mathfrak{a}_2^\ell$. Hence, $\ell \mid v_\mathfrak{p}(\Delta_F)$ for all $\mathfrak{p} \notin \mathcal{S}$. □

The next lemma shows that if ℓ in Lemma 5.1 is large enough, then we can apply level lowering to the Frey curve F. We note that the C_K appearing below is the effective constant, depending only on K, given by Theorem 4.4 for the Galois totally real field K under consideration. Note that this makes sense as K in Lemma 5.1 is either $\mathbb{Q}$ or a real quadratic number field, and in both cases K is a Galois totally real field.

Lemma 5.2. *Take the assumptions of Lemma 5.1. Let $\mathcal{N}$ be the conductor of F. If $\ell > max\{2ad, C_K, 5\}$, then there is a Hilbert eigenform $\mathfrak{f}$ of parallel weight 2 that is new at level $\mathcal{N}_\ell$ and a prime ideal λ of $\mathbb{Q}_\mathfrak{f}$ such that $\lambda \mid \ell$ and $\bar{\rho}_{F,\ell} \sim \bar{\rho}_{\mathfrak{f},\lambda}$.*

Proof. Recall the definitions

$$\mathcal{M}_\ell := \prod_{\mathfrak{p}||\mathcal{N},\, \ell|v_\mathfrak{p}(\Delta_\mathfrak{p})} \mathfrak{p}, \quad \mathcal{N}_\ell := \frac{\mathcal{N}}{\mathcal{M}_\ell},$$

in Theorem 4.2. Again, let $\mathcal{S}$ be the set of prime ideals in $\mathcal{O}_K$ dividing $2ad$. By Lemma 5.1, if $\mathfrak{p} \mid \mathcal{N}$ and $\mathfrak{p} \notin \mathcal{S}$, then $\mathfrak{p} \,||\, \mathcal{N}$ and $\ell \mid v_\mathfrak{p}(\Delta_F)$. Then $\mathcal{N}_\ell$ is a product of finitely many primes ideals that are contained in $\mathcal{S}$.

Since $\ell > 2ad$, ℓ is not divisible by any prime ideal in $\mathcal{S}$. Thus, for all $\mathfrak{p} \mid \ell$, F has semistable reduction at $\mathfrak{p}$ and $\ell \mid v_\mathfrak{p}(\Delta_F)$. Moreover, since $\ell > C_K$, Theorem 4.4 implies that $\bar{\rho}_{F,\ell}$ is irreducible.

Therefore, the following conditions are satisfied:

(i) $\ell \geq 5$, the ramification index for all primes of $\mathcal{O}_K$ lying above ℓ is ≤ 2, and $\mathbb{Q}(\zeta_\ell)^+ \not\subset K$;
(ii) F is modular, by Theorem 4.1 if $a \neq 1$, and by the Modularity Theorem if $a = 1$;
(iii) $\bar{\rho}_{F,\ell}$ is irreducible;
(iv) E is semistable at $\mathfrak{p}$ for all $\mathfrak{p} \mid \ell$;
(v) and $\ell \mid v_\mathfrak{p}(\Delta_F)$ for all $\mathfrak{p} \mid \ell$.

Hence, we may apply Theorem 4.2. □

Proof of Theorem 1.2. Write $mP = (A_m/B_m^2, C_m/B_m^3)$ in lowest terms, for all $m \geq 1$. If $A_m = 0$, then from the equation of the elliptic curve we deduce that $P = (0, 0)$, which is a 2-torsion point; but P is non-torsion. Thus, $A_m \neq 0$ and $C_m \neq 0$ for all $m \geq 1$. Suppose that $B_m = w_m^\ell$, for a prime number ℓ and an integer w_m. Since $B_1 > 1$ and $B_1 \mid B_m$ (by Proposition 3.3), we have $w_m > 1$ for all m. For a fixed ℓ, by Theorem 1.1 in [9], we can only have finitely many elements of the sequence that are ℓ-th powers. Thus, to prove the theorem it suffices to show that ℓ is bounded.

By substituting mP in the equation of the elliptic curve, we get an equation of the form

$$C_m^2 = A_m(A_m^2 + bw_m^{4\ell}),$$

where $\gcd(A_m, A_m^2 + bw_m^{4\ell}) \mid b$. Therefore, we can write

$$A_m = a_m u_m^2 \quad \text{and} \quad A_m^2 + bw_m^{4\ell} = a_m v_m^2,$$

where u_m, v_m, and a_m are positive integers, a_m is square-free, $a_m \mid b$, and $\gcd(u_m, v_m)$ divides b. Observe that $u_m v_m \neq 0$, since $C_m \neq 0$. Hence, we get the equation

$$v_m^2 - a_m u_m^4 = (b/a_m) w_m^{4\ell}. \tag{5.7}$$

Observe that (5.7) is (5.1) in Lemma 5.1 with $u = u_m$, $v = v_m$, $w = w_m$, $a = a_m$, $d = b/a_m$, and $2ad = 2b$. Then we can associate to (5.7) the Frey curve

$$F_m : \ Y^2 = X(X^2 + 4u_m\sqrt{a_m}X + 2\sqrt{a_m}(v_m + u_m^2\sqrt{a_m})),$$

over the number field $K_m = \mathbb{Q}(\sqrt{a_m})$, where $\Delta_{F_m} \neq 0$. Moreover, for all primes $\mathfrak{p}$ of $\mathcal{O}_{K_m}$ such that $\mathfrak{p} \nmid 2b$, F_m is minimal at $\mathfrak{p}$, F_m has semistable reduction at $\mathfrak{p}$, and $\ell \mid v_\mathfrak{p}(\Delta_{F_m})$.

Let $\mathcal{S}$ be the set of prime ideals in $\mathcal{O}_{K_m}$ dividing $2b$. Let T be the set of prime numbers lying under the prime ideals of $\mathcal{S}$. Then, by Lemma 3.4, there exists a positive integer k, depending only on B_1 and b, and a prime $p_0 \notin T$ such that if B_m is an ℓ-th power for some $\ell > k$, then $p_0 \mid B_m$. Now, for all $m \in \mathbb{N}$, $a_m \mid b$. Hence, for all B_m, there are only finitely many possible number fields K_m, which only depend on the constant b appearing in the

equation of E. Again, for any $m \in \mathbb{N}$, let C_{K_m} denote the corresponding effective bound given by Theorem 4.4. Set C to be the maximum of all the possible (finitely many) values of C_{K_m}.

Suppose now that $B_m = w_m^\ell$ where $\ell > \max\{k, 2b, C, p_0, 5\}$. Recall that $k, 2b, C$, and p_0 depend only on b and the point P generating $\{B_m\}$. Now, $\ell > k$ implies that $p_0 \mid w_m^\ell$, which in turn implies that $p_0 \mid \Delta_{F_m}$. If $\mathfrak{p} \mid p_0$, where $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_{K_m}$, then $\mathfrak{p} \notin \mathcal{S}$ and $\mathfrak{p} \nmid \ell$, since $p_0 \notin T$ and $\ell > p_0$. Let $\mathfrak{p}$ be any prime ideal of $\mathcal{O}_{K_m}$ that divides p_0. So, we have that $\mathfrak{p} \,||\, \mathcal{N}$, the conductor of F_m, and $\mathfrak{p} \nmid \ell\mathcal{N}_\ell$. Since $\ell > \max\{2b, C, 5\}$, by Lemma 5.2, there is a Hilbert eigenform $\mathfrak{f}$ over K_m of parallel weight 2 that is new at level $\mathcal{N}_\ell$ and some prime λ of $\mathbb{Q}_\mathfrak{f}$ such that $\lambda \mid \ell$ and $\bar{\rho}_{F,\ell} \sim \bar{\rho}_{\mathfrak{f},\lambda}$. Since $\mathfrak{p} \nmid \ell\mathcal{N}_\ell$ and $\mathfrak{p} \,||\, \mathcal{N}$, by Remark 4.3, we have that

$$\pm(\mathrm{Norm}_{K_m/\mathbb{Q}}(\mathfrak{p}) + 1) \equiv a_\mathfrak{p}(\mathfrak{f}) \mod \lambda.$$

This implies that

$$\ell \mid \mathrm{Norm}_{\mathbb{Q}_\mathfrak{f}/\mathbb{Q}}(\mathrm{Norm}_{K_m/\mathbb{Q}}(\mathfrak{p}) + 1 \pm a_\mathfrak{p}(\mathfrak{f})), \tag{5.8}$$

Now, Theorem 0.1 in [16] states that the Ramanujan–Petersson conjecture holds for a certain class of Hilbert modular forms. It is clear that the $\mathfrak{f}$ and $\mathfrak{p}$ we are considering satisfy the conditions of Theorem 0.1 in [16]. Therefore, we have that

$$|a_\mathfrak{p}(\mathfrak{f})| \le 2\sqrt{\mathrm{Norm}_{K_m/\mathbb{Q}}(\mathfrak{p})}.$$

Thus,

$$\begin{aligned}|\mathrm{Norm}_{K_m/\mathbb{Q}}(\mathfrak{p}) + 1 \mp a_\mathfrak{p}(\mathfrak{f})| &\ge \mathrm{Norm}_{K_m/\mathbb{Q}}(\mathfrak{p}) + 1 - 2\sqrt{\mathrm{Norm}_{K_m/\mathbb{Q}}(\mathfrak{p})} \\ &= \left(\sqrt{\mathrm{Norm}_{K_m/\mathbb{Q}}(\mathfrak{p})} - 1\right)^2 > 0.\end{aligned}$$

Hence, $\mathrm{Norm}_{\mathbb{Q}_\mathfrak{f}/\mathbb{Q}}(\mathrm{Norm}_{K_m/\mathbb{Q}}(\mathfrak{p}) + 1 \mp a_\mathfrak{p}(\mathfrak{f})) \neq 0$. Therefore, by (5.8), ℓ is bounded by $\mathrm{Norm}_{\mathbb{Q}_\mathfrak{f}/\mathbb{Q}}(\mathrm{Norm}_{K_m/\mathbb{Q}}(\mathfrak{p}) + 1 \mp a_\mathfrak{p}(\mathfrak{f}))$. Note that $\mathrm{Norm}_{K_m/\mathbb{Q}}(\mathfrak{p})$ is either p_0 or p_0^2, and p_0 only depends on B_1 and b. Moreover, $\mathcal{N}_\ell$ has finitely many possible values that only depend on $2b$; more precisely, $\mathcal{N}_\ell$ is a finite product of prime ideals belonging to $\mathcal{S}$, each of which has a bounded exponent by Remark 2.4. Thus, by noting that there are finitely many Hilbert eigenforms $\mathfrak{f}$ of any fixed level, we have that the set of Hilbert eigenforms $\mathfrak{f}$ with level equal to any $\mathcal{N}_\ell$ is finite. Therefore, for any B_m an ℓ-th power with $\ell > \max\{k, 2b, C, p_0, 5\}$, $\mathrm{Norm}_{\mathbb{Q}_\mathfrak{f}/\mathbb{Q}}(\mathrm{Norm}_{K_m/\mathbb{Q}}(\mathfrak{p}) + 1 \mp a_\mathfrak{p}(\mathfrak{f}))$ has finitely many possible values. By finding the maximum of these values, we obtain a bound on ℓ. □

Remark 5.3. The condition that the point P is non-integral was vital in our proof, since it allowed us to find the prime p_0 using Lemma 3.4. Also, if b was negative, then to follow the same methodology we would require the modularity of elliptic curves over imaginary quadratic number fields,

which is not known to be true yet. One might also be tempted to show that Theorem 1.2 holds for the more general equation $y^2 = x(x^2 + ax + b)$, with some additional assumptions, by attempting to adjust this proof. However, this does not appear to be viable as we won't be able to control the common divisors of the two factors on the left hand side of (5.3), which was necessary for the effectiveness of the level-lowering method, i.e., obtaining a finite number of possible levels $\mathcal{N}_\ell$ when varying ℓ.

Acknowledgements. I would like to thank Samir Siksek for sharing his knowledge and for his guidance throughout my master's project at the University of Warwick, from which this paper was produced. I would also like to thank Daniel Loughran for his guidance and comments. Finally, I would like to thank the referee for the suggestions and comments.

References

[1] D. Blasius & J. D. Rogawski, "Motives for Hilbert modular forms", *Invent. Math.* **114** (1993), no. 1, p. 55-87.

[2] W. Bosma, J. Cannon & C. Playoust, "The Magma Algebra System I: The User Language", *J. Symb. Comput.* **24** (1997), no. 3-4, p. 235-265.

[3] Y. Bugeaud, M. Mignotte & S. Siksek, "Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers", *Ann. Math.* **163** (2006), no. 3, p. 969-1018.

[4] H. Carayol, "Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert", *Ann. Sci. Éc. Norm. Supér.* **19** (1986), no. 3, p. 409-468.

[5] ———, "Sur les représentations galoisiennes modulo attachées aux formes modulaires", *Duke Math. J.* **59** (1989), no. 3, p. 785-801.

[6] H. Darmon, "Serre's conjectures", in *Seminar on Fermat's last theorem*, CMS Conference Proceedings, vol. 17, American Mathematical Society, 1995, p. 135-153.

[7] F. Diamond & J. Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer, 2005, xv+436 pages.

[8] G. Everest & H. King, "Prime powers in elliptic divisibility sequences", *Math. Comput.* **74** (2005), no. 252, p. 2061-2071.

[9] G. Everest, J. Reynolds & S. Stevens, "On the denominators of rational points on elliptic curves", *Bull. Lond. Math. Soc.* **39** (2007), no. 5, p. 762-770.

[10] N. Freitas, B. V. Le Hung & S. Siksek, "Elliptic Curves over Real Quadratic Fields are Modular", *Invent. Math.* **201** (2015), no. 1, p. 159-206.

[11] N. Freitas & S. Siksek, "The Asymptotic Fermat's Last Theorem for Five-Sixths of Real Quadratic Fields", *Compos. Math.* **151** (2015), p. 1395-1415.

[12] ———, "Criteria for irreducibility of mod p representations of Frey curves", *J. Théor. Nombres Bordeaux* **27** (2015), no. 1, p. 67-76.

[13] K. Fujiwara, "Level optimisation in the totally real case", `https://arxiv.org/abs/math/0602586v1`, 2006.

[14] P. Ingram & J. H. Silverman, "Uniform estimates for primitive divisors in elliptic divisibility sequences", in *Number theory, analysis and geometry*, Springer, 2012, p. 243-271.

[15] F. Jarvis, "Correspondences on Shimura curves and Mazur's principle at p", *Pac. J. Math.* **213** (2004), no. 2, p. 267-280.

[16] R. Livné, "Communication networks and Hilbert modular forms", in *Applications of algebraic geometry to coding theory, physics and computation*, NATO Science Series II: Mathematics, Physics and Chemistry, vol. 36, Kluwer Academic Publishers, 2001, p. 255-270.

[17] A. Rajaei, "On the levels of mod ℓ Hilbert modular forms", *J. Reine Angew. Math.* **537** (2001), p. 33-65.

[18] J. Reynolds, "Perfect powers in elliptic divisibility sequences", *J. Number Theory* **132** (2012), no. 5, p. 998-1015.
[19] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer, 1986, xii+400 pages.
[20] ———, "Wieferich's criterion and the abc-conjecture", *J. Number Theory* **30** (1988), no. 2, p. 226-237.
[21] ———, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer, 1994, xiii+525 pages.
[22] M. Streng, "Elliptic divisibility sequences with complex multiplication", 2006, Master's thesis, Universiteit Utrecht.
[23] R. Taylor, "On Galois representations associated to Hilbert modular forms", *Invent. Math.* **98** (1989), no. 2, p. 265-280.
[24] M. Ward, "Memoir on elliptic divisibility sequences", *Am. J. Math.* **70** (1948), p. 31-74.
[25] A. J. Wiles, "On ordinary λ-adic representations associated to modular forms", *Invent. Math.* **94** (1988), no. 3, p. 529-573.

Abdulmuhsin Alfaraj
Department of Mathematical Sciences
University of Bath
Claverton Down
Bath, BA2 7AY
UK.
E-mail: abdulmuhsinalfaraj@hotmail.com
URL: https://sites.google.com/view/abdulmuhsinalfaraj/