Journal of Number Theory 132 (2012) 998–1015

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Perfect powers in elliptic divisibility sequences

Jonathan Reynolds [1,2]

Mathematisch Instituut, Universiteit Utrecht, Postbus 80.010, 3508 TA Utrecht, Netherlands

ARTICLE INFO

Article history:
Received 22 January 2011
Revised 2 August 2011
Accepted 4 September 2011
Available online 6 February 2012
Communicated by Michael A. Bennett

MSC:
11G05
11D41

Keywords:
Diophantine equations
Modular methods
Elliptic divisibility sequences

ABSTRACT

It is shown that there are finitely many perfect powers in an elliptic divisibility sequence whose first term is divisible by 2 or 3. For Mordell curves the same conclusion is shown to hold if the first term is greater than 1. Examples of Mordell curves and families of congruent number curves are given with corresponding elliptic divisibility sequences having no perfect power terms. The proofs combine primitive divisor results with modular methods for Diophantine equations.

1. Introduction

By combining modular techniques, inspired by the proof of Fermat's Last Theorem, with other highly nontrivial methods, it was finally shown in [10] that the only perfect powers in the Fibonnaci sequence are 1, 8 and 144. Fibonnaci is just one example of an infinite sequence (h_m) of integers

$$\ldots, h_{-2}, h_{-1}, h_0, h_1, h_2, \ldots$$

satisfying $h_m \mid h_n$ whenever $m \mid n$ and, up to sign,

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2$$

E-mail address: J.M.Reynolds@uu.nl.

[1] The author is supported by a Marie Curie Intra European Fellowship (PIEF-GA-2009-235210).
[2] The author thanks Gunther Cornelissen, Sander Dahmen and Shaun Stevens for helpful comments.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2011.09.013

for all $m, n \in \mathbb{Z}$, where $h_2 h_3 \neq 0$. Gezer and Bizim [27] have recently described the squares in some of these sequences but (h_m) was first studied in general by Ward [49] and is related to a Weierstrass equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \tag{1.1}$$

with integer coefficients. See [43,44] for background on Weierstrass equations and elliptic curves. The non-singular rational points on the projective closure of the curve defined by (1.1) form a group $E_{ns}(\mathbb{Q})$ and for $P \in E_{ns}(\mathbb{Q})$ different from the identity we can write

$$\big(x(P), y(P)\big) = \left(\frac{A_P}{B_P^2}, \frac{C_P}{B_P^3}\right), \tag{1.2}$$

where $A_P, B_P, C_P \in \mathbb{Z}$ and $\gcd(A_P C_P, B_P) = 1$. Let (h_m) be a sequence of integers as above with $h_0 = 0$ and $h_1 = 1$. Building on work of Ward, Shipsey [39] has given a formula for a Weierstrass equation (1.1) such that $h_m = \psi_m(0,0)$, where ψ_m is the mth division polynomial (see Section 3.2) and $h_m = \pm B_{m(0,0)}$ if $\gcd(a_3, a_4) = 1$. For example, up to sign, $(0,0)$ on

$$y^2 + xy + y = x^3 - 2x^2$$

generates the Fibonacci sequence $(B_{m(0,0)})$. In [49] Ward calls (h_m) an elliptic divisibility sequence; however, as in the Fibonacci case, the Weierstrass equation for (h_m) may have a singular point and so not define an elliptic curve.

Let $E/\mathbb{Q}$ be an elliptic curve and (1.1) a Weierstrass equation for E. Via the work of Everest [21,23], Ingram [29], Silverman [31,41] et al., it has now become conventional to use the following

Definition 1.1. Let $P \in E(\mathbb{Q})$ be a non-torsion point. For $m \in \mathbb{N}$ take B_{mP}, as in (1.2), to be positive and denote it by B_m. The sequence (B_m) is an *elliptic divisibility sequence*.

In the current paper, we are interested in analogues for elliptic divisibility sequences (in the sense of Definition 1.1) to the result for Fibonacci numbers. There are certainly perfect powers in some elliptic divisibility sequences. For example,

$$E\colon\ y^2 + xy = x^3 + x^2 - 7x + 5$$

with $P = (2, -3)$ gives $B_m = 1$ for $m = 1, 2, 3, 4, 7$ and $B_{12} = 2^7$. However, the following theorem shows that one can often prove that there are only finitely many perfect powers in such sequences.

Theorem 1.2. *. Let (B_m) be an elliptic divisibility sequence, generated by a non-torsion point $P \in E(\mathbb{Q})$, whose first term is divisible by 2 or 3. There are finitely many perfect powers in (B_m). Moreover, if $B_m = z^l$ for some integer z and prime l then l can be effectively bounded in terms of (1.1) and P.*

The proof of Theorem 1.2 combines a recent Frey–Hellegouarch construction for Klein forms by Bennett and Dahmen [3] with a primitive divisor result due to Silverman [41]. The method of proof is so flexible that it also allows one in certain concrete cases to completely determine the set of all perfect power terms, as was done for the Fibonacci sequence (see Proposition 1.5 and Example 1.9 below). The condition that only 2 or 3 divides the first term is because higher primes, such as 5, do not give a Klein form as in Definition 3.7.

Siegel [40] proved that there are finitely many (non-zero) $P \in E(\mathbb{Q})$ with $B_P = 1$. In [24] it is shown that for fixed $l > 1$, there are finitely many (non-zero) $P \in E(\mathbb{Q})$ with $B_P = z^l$ for some $z \in \mathbb{Z}$. Since their denominator is a perfect power, perhaps it is reasonable to give the following

Definition 1.3. Call $P \in E(\mathbb{Q})$ *power integral* if P is not the identity and B_P (as in (1.2)) is equal to a perfect power.

Note that 1 is a perfect power and so power integral points can be thought of as a generalization of the integral points. A lot of work has been done to make Siegel's theorem effective [2,11,25,28,34] and there are many techniques which can find all of the integral points for large classes of elliptic curves [26,35,46,47]. For certain curves we are now able to find all of the power integral points.

1.1. Mordell curves

Theorem 1.2 can be strengthened considerably for Mordell curves.

Theorem 1.4. *Let $D \in \mathbb{Z}$ be non-zero and $E\colon y^2 = x^3 + D$. There are finitely many perfect powers in an elliptic divisibility sequence (B_m) whose first term is greater than* 1. *As in Theorem* 1.2, *the bound for the possible prime exponent is effective.*

By utilizing the proofs of the theorems above in a specific case we are able to find the Mordell curve of smallest conductor with non-zero rank and no power integral points.

Proposition 1.5. *The elliptic curve $E\colon y^2 = x^3 + 11$ has no power integral points.*

In the general case, allowing for integral points, we expect the following to hold.

Conjecture 1.6. *Let $D \in \mathbb{Z}$ be non-zero and $E\colon y^2 = x^3 + D$. For l a sufficiently large prime, if B_P (as in* (1.2)) *is an lth power then $B_P = 1$.*

At the end of Section 5 it is explained that Conjecture 1.6 would follow from the Frey–Mazur conjecture [16].

1.2. Congruent number curves

A much studied class of elliptic curves is the congruent number curves $E_N\colon y^2 = x^3 - N^2x$, where $N \geqslant 1$ is an integer. Let p be an odd prime and a, b non-negative integers. For $N = 2^a p^b$, a simple algorithm for the determination of the integral points in $E_N(\mathbb{Q})$ has been given in [20] and [19]. In this case we are able to find all power integral points in $2E_N(\mathbb{Q})$; in fact they are all integral.

Theorem 1.7. *Let $N = 2^a p^b$. If $P \in 2E_N(\mathbb{Q})$ is power integral then $N = 2^a 3^b$ and $P = (c^2 25, c^3 35)$, where a, b are odd, $a \geqslant 3$ and $c = \pm 2^{(a-3)/2} 3^{(b-1)/2}$.*

In Section 6 Theorem 1.7 is proven using Fermat's Last Theorem, due to Wiles [50], along with the first variants by Ribet [38], Darmon and Merel [17].

Theorem 1.8. *Let $N = 2^a p$, where $a = 0$ or* 1. *Suppose that $P \in E_N(\mathbb{Q})$ has*

$$x(P) \in -\mathbb{Q}^{*2}$$

and

$$x(P) + N \in p\mathbb{Q}^{*2}.$$

Then there are no perfect powers in the elliptic divisibility sequence generated by P.

Theorem 1.8 is proven using Theorem 1.7 along with an equation recently solved by Bennett, Ellenberg and Ng [4].

Example 1.9. There are no perfect powers in the elliptic divisibility sequence generated by $(-(60/41)^2, -455700/41^3)$ on $E_5\colon y^2 = x^3 - 25x$.

Let $N = 2^a p$, where $a = 0$ or 1. Points belonging to two cosets in $E_N(\mathbb{Q})/2E_N(\mathbb{Q})$ have been considered above. The remaining cases lead to equations which currently appear unresolvable in general. As the next example shows, there can be power integral points on E_N which are not integral. However, in the example N is equal to the odd terms of a sequence (C_m) and, since these odd terms form an elliptic divisibility sequence, there are conjectured to be finitely many possibilities with N prime [22]. This, along with Theorem 1.7 and Theorem 1.8, suggests that the number of power integral points in $E_N(\mathbb{Q})$ which are not integral could be uniformly bounded.

Example 1.10. For $(-1, 1)$ on $y^2 = x^3 - 2x$ and m odd write

$$m(-1,1) = \left(-\frac{A_m^2}{B_m^2}, \frac{A_m C_m}{B_m^3}\right).$$

We get a power integral point on $E_{C_m}\colon y^2 = x^3 - C_m^2 x$ given by $x(P) = -(C_m A_m)^2/B_m^4$. Moreover, C_m is prime for $m = 3, 7$ and 23.

2. Properties of elliptic divisibility sequences

In this section the required properties of elliptic divisibility sequences are collected.

Lemma 2.1. *Let (B_m) be an elliptic divisibility sequence.*

(i) *Let p be a prime. There exists a smallest positive integer m_0 such that $p \mid B_{m_0}$. Moreover, for every $m \in \mathbb{N}$,*

$$p \mid B_m \quad \Longleftrightarrow \quad m_0 \mid m.$$

(ii) *Let p be an odd prime. For any pair $n, m \in \mathbb{N}$, if $\operatorname{ord}_p(B_n) > 0$ then*

$$\operatorname{ord}_p(B_{mn}) = \operatorname{ord}_p(B_n) + \operatorname{ord}_p(m).$$

(iii) *For any pair $n, m \in \mathbb{N}$, if $2 \mid B_n$ then*

$$\operatorname{ord}_2(B_{mn}) = \operatorname{ord}_2(B_n) + \operatorname{ord}_2(m)$$

if a_1 is even and

$$\left|\operatorname{ord}_2(B_{mn}) - \left(\operatorname{ord}_2(B_n) + \operatorname{ord}_2(m)\right)\right| \leqslant \epsilon$$

otherwise, where the constant ϵ depends only on E and P.

(iv) *For all $m, n \in \mathbb{N}$,*

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

Proof. See [41] and Section 4 in Chapter IV of [45]. □

Lemma 2.2. *Assume that the given Weierstrass equation for E has a_1 even. For a prime p suppose that $m_0 = p$ in Lemma 2.1. Write $m = p^e m'$ where $p \nmid m'$. If B_m is an lth power then so is $B_{m'}$. Moreover, $p \nmid B_{m'}$.*

Proof. By Lemma 2.1, if a prime q divides $B_{m'}$ then $q \neq p$ and

$$\operatorname{ord}_q(B_m) = \operatorname{ord}_q(B_{m'}) + \operatorname{ord}_q\left(p^e\right) = \operatorname{ord}_q(B_{m'})$$

so the result follows. □

Definition 2.3. A prime $p \mid B_m$ such that $p \nmid B_{m'}$ for any $m' < m$ is called a *primitive divisor* of B_m.

Theorem 2.4 *(Silverman). For all but finitely many $m \in \mathbb{N}$, B_m has a primitive divisor. Moreover, if B_m does not have a primitive divisor then m is bounded by an effectively computable constant which depends only on the Weierstrass equation and the non-torsion point generating (B_m).*

Proof. See Section 2 of [41] or Chapter V of [45]. □

Remark 2.5. For certain minimal Weierstrass equations the number of terms without a primitive divisor has been uniformly bounded (see [29–31]).

3. The modular approach to Diophantine equations

For a more thorough exploration see [15] and Chapter 15 in [13]. As is conventional, in what follows all newforms shall have weight 2 with a trivial character at some level N and shall be thought of as a q-expansion

$$f = q + \sum_{n \geqslant 2} c_n q^n,$$

where the field $K_f = \mathbb{Q}(c_2, c_3, \ldots)$ is a totally real number field. The coefficients c_n are algebraic integers and f is called *rational* if they all belong to $\mathbb{Z}$. For a given level N, the number of newforms is finite. The modular symbols algorithm [14], implemented on MAGMA [8] by William Stein, shall be used to compute the newforms at a given level.

Theorem 3.1 *(Modularity theorem). Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. Then there exists a newform f of level N such that $a_p(E) = c_p$ for all primes $p \nmid N$, where c_p is the pth coefficient of f and $a_p(E) = p + 1 - \#\tilde{E}(\mathbb{F}_p)$.*

Proof. This is due to Taylor and Wiles [48,50] in the semi-stable case. The proof was completed by Breuil, Conrad, Diamond and Taylor [9]. □

The modularity of elliptic curves over $\mathbb{Q}$ can be seen as a converse to

Theorem 3.2 *(Eichler–Shimura). Let f be a rational newform of level N. There exists an elliptic curve $E/\mathbb{Q}$ of conductor N such that $a_p(E) = c_p$ for all primes $p \nmid N$, where c_p is the pth coefficient of f and $a_p(E) = p + 1 - \#\tilde{E}(\mathbb{F}_p)$.*

Proof. See Chapter 8 of [18]. □

Given a rational newform of level N, the elliptic curves of conductor N associated to it via the Eichler–Shimura theorem shall be computed using MAGMA.

Proposition 3.3. *Let $E/\mathbb{Q}$ be an elliptic curve with conductor N and minimal discriminant $\Delta_{\min}$. Let l be an odd prime and define*

$$N_0(E,l) := N/\prod_{\substack{\text{primes } p\|N \\ l\mid \operatorname{ord}_p(\Delta_{\min})}} p.$$

Suppose that the Galois representation

$$\rho_l^E : \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{Aut}\big(E[l]\big)$$

is irreducible. Then there exists a newform f of level $N_0(E,l)$. Also there exists a prime $\mathcal{L}$ lying above l in the ring of integers $\mathcal{O}_f$ defined by the coefficients of f such that

$$c_p \equiv \begin{cases} a_p(E) \bmod \mathcal{L} & \text{if } p \nmid lN, \\ \pm(1+p) \bmod \mathcal{L} & \text{if } p \parallel N \text{ and } p \nmid lN_0, \end{cases}$$

where c_p is the pth coefficient of f. Furthermore, if $\mathcal{O}_f = \mathbb{Z}$ then

$$c_p \equiv \begin{cases} a_p(E) \bmod l & \text{if } p \nmid N, \\ \pm(1+p) \bmod l & \text{if } p \parallel N \text{ and } p \nmid N_0. \end{cases}$$

Proof. This arose from combining modularity with level-lowering results by Ribet [36,37]. The strengthening in the case $\mathcal{O}_f = \mathbb{Z}$ is due to Kraus and Oesterlé [33]. A detailed exploration is given, for example, in Chapter 2 of [15]. □

Remark 3.4. Let $E/\mathbb{Q}$ be an elliptic curve with conductor N. Note that the exponents of the primes in the factorization of N are uniformly bounded (see Section 10 in Chapter IV of [42]). In particular, only primes of bad reduction divide N and if E has multiplicative reduction at p then $p \parallel N$.

Corollary 3.5. *Keeping the notation of Proposition* 3.3, *if p is a prime such that $p \nmid N_0$ and $p \mid N$ then*

$$l < (1+\sqrt{p})^{2[K_f:\mathbb{Q}]}.$$

Proof. See Theorem 37 in [15]. □

Applying Proposition 3.3 to carefully constructed Frey curves has led to the solution of many Diophantine problems. The most famous of these is Fermat's Last theorem [50] but there are now constructions for other equations and we shall make use of those described below.

3.1. Recipes for Diophantine equations with signature $(l,l,3)$

Consider the equation

$$Ax^l + By^l = Cz^3,$$

with non-zero pairwise coprime terms and $l \geqslant 5$ prime. Assume any prime q satisfies $\operatorname{ord}_q(A) < l$, $\operatorname{ord}_q(B) < l$ and $\operatorname{ord}_q(C) < 3$. Without lost of generality also assume that $Ax \not\equiv 0 \bmod 3$ and $By^l \not\equiv 2 \bmod 3$. Construct the Frey curve

$$E_{x,y}\colon\ Y^2 + 3CzXY + C^2By^lY = X^3.$$

(We use the notation $E_{x,y}$ since z depends on x and y.)

Theorem 3.6. *(See Bennett, Vatsal and Yazdani [5].) The conductor $N_{x,y}$ of $E_{x,y}$ is given by*

$$N_{x,y} = 3^{\alpha} \operatorname{rad}_3(ABxy) \operatorname{rad}_3(C)^2,$$

where

$$\alpha = \begin{cases} 2 & \text{if } 9 \mid (2 + C^2By^l - 3Cz), \\ 3 & \text{if } 3 \parallel (2 + C^2By^l - 3Cz), \\ 4 & \text{if } \operatorname{ord}_3(By^l) = 1, \\ 3 & \text{if } \operatorname{ord}_3(By^l) = 2, \\ 0 & \text{if } \operatorname{ord}_3(By^l) = 3, \\ 1 & \text{if } \operatorname{ord}_3(By^l) \geqslant 4, \\ 5 & \text{if } 3 \mid C. \end{cases}$$

Suppose that $E_{x,y}$ does not correspond to one of the equations

$$\begin{aligned} 1 \cdot 2^5 + 27 \cdot (-1)^5 &= 5 \cdot 1^3, \\ 1 \cdot 2^7 + 3 \cdot (-1)^7 &= 1 \cdot 5^3, \\ 2 \cdot 1^2 + 27 \cdot (-1)^5 &= 25 \cdot (-1)^3, \quad \text{or} \\ 2 \cdot 1^7 + 3 \cdot (-1)^7 &= (-1)^3. \end{aligned}$$

Then there exists a newform of level

$$N_0 = 3^{\beta} \operatorname{rad}_3(AB) \operatorname{rad}_3(C)^2,$$

where

$$\beta = \begin{cases} 2 & \text{if } 9 \mid (2 + C^2By^l - 3Cz), \\ 3 & \text{if } 3 \parallel (2 + C^2By^l - 3Cz), \\ 4 & \text{if } \operatorname{ord}_3(By^l) = 1, \\ 3 & \text{if } \operatorname{ord}_3(By^l) = 2, \\ 0 & \text{if } \operatorname{ord}_3(B) = 3, \\ 1 & \text{if } \operatorname{ord}_3(By^l) \geqslant 4 \text{ and } \operatorname{ord}_3(B) \neq 3, \\ 5 & \text{if } 3 \mid C. \end{cases}$$

3.2. Frey–Hellegouarch curves for Klein forms

Let E be an elliptic curve defined over $\mathbb{Q}$ with Weierstrass coordinate functions x, y. For any integer $n \in \mathbb{Z}$, the nth *division polynomial* of E is the polynomial $\psi_n \in \mathbb{Q}[x, y] \subset \mathbb{Q}(E)$ as given on p. 39 of [7]. In particular,

$$\begin{aligned} \psi_2^2 &= 4x^3 + b_2x^2 + 2b_4x + b_6, \\ \psi_3 &= 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8, \end{aligned}$$

$\psi_n^2 \in \mathbb{Q}[x]$ and there exists $\theta_n \in \mathbb{Q}[x]$ such that the x-coordinate of the multiplication by n map is given by

$$[n]x = \frac{\theta_n}{\psi_n^2}. \tag{3.1}$$

Definition 3.7. Associate to $\psi_2^2(x)$ and $\psi_3(x)$ the homogeneous polynomials:

$$K_n^E(x, y) = \begin{cases} \psi_2^2(x/y)y^3 & \text{for } n = 2, \\ \psi_3(x/y)y^4 & \text{for } n = 3. \end{cases}$$

The notion of a Klein form arose from Klein's classification [32] of the finite subgroups of $\mathrm{Aut}_{\bar{\mathbb{Q}}}(\mathbb{P}_1)$. For our purposes it is enough to note that any separable cubic binary form in $\mathbb{Q}[x, y]$ is a Klein form and that a separable quartic

$$\alpha_0 x^4 + \alpha_1 x^3 y + \alpha_2 x^2 y^2 + \alpha_3 x y^3 + \alpha_4 y^4 \in \mathbb{Q}[x, y]$$

is a Klein form precisely when

$$12\alpha_0\alpha_4 - 3\alpha_1\alpha_3 + \alpha_2^2 = 0. \tag{3.2}$$

Lemma 3.8. *Let E be an elliptic curve defined over $\mathbb{Q}$. Then $K_2^E(x, y)$ and $K_3^E(x, y)$ are Klein forms.*

Proof. Since the multiplication by n map is separable (see Chapter III of [43]), $K_n^E(x, y)$ is separable. A small calculation checks that the coefficients of $K_3^E(x, y)$ satisfy (3.2). □

For S a fixed finite set of primes, let

$$\mathbb{Z}_S := \left\{x \in \mathbb{Q}\colon \operatorname{ord}_p(x) \geqslant 0 \text{ for all } p \notin S\right\}$$

and let $\mathbb{Z}_S^*$ be the set of units in $\mathbb{Z}_S$. Let F be a Klein form with integer coefficients of degree $k \in \{3, 4, 6, 12\}$ ($k = 3$ or 4 is enough for our purposes). The *index* of F is $n = 6 - 12/k$. Denote by Δ_F the discriminant of F and let S_F be the set of primes which divide $n\Delta_F$. In [3,15] Bennett and Dahmen construct a Frey–Hellegouarch curve for the Diophantine equation

$$F(A, B) = uC^l, \tag{3.3}$$

where $\gcd(A, B) = 1$, $C \neq 0$, l is prime and $u \in \mathbb{Z}_{S_F}^*$. Define

$$H(x, y) = \frac{1}{(k-1)^2}\begin{vmatrix} F_{xx} & F_{xy} \\ F_{xy} & F_{yy} \end{vmatrix}$$

and the Jacobian determinant of F and H by

$$G(x, y) = \frac{1}{k-2}\begin{vmatrix} F_x & F_y \\ H_x & H_y \end{vmatrix},$$

where F_x, F_y, etc., refer to corresponding partial derivatives. Then

$$4H(A, B)^3 + G(A, B)^2 = d_n F(A, B)^n,$$

where $d_2 = -27\Delta_F$ and $d_3 = 2^8\sqrt{-\Delta_F/27}$ are integers. So

$$E_{A,B}\colon\ Y^2 = X^3 + 3H(A,B)X + G(A,B)$$

has discriminant $-2^4 \cdot 3^3 d_n F(A,B)^2$.

Proposition 3.9. *(See [3].) There exists $t \in \{\pm 1, \pm 3\}$ such that for all primes $p \notin S_F$ we have that the quadratic twist*

$$E^{(t)}_{A,B}\colon\ Y^2 = X^3 + 3H(A,B)t^2X + G(A,B)t^3$$

is semistable at p and

$$\operatorname{ord}_p\big(\Delta_{\min}\big(E^{(t)}_{A,B}\big)\big) = n\operatorname{ord}_p\big(F(A,B)\big).$$

Proof. This is Proposition 4.2 of [3]. □

Proposition 3.10. *(See [3].) Let $l > 163$ in (3.3) and let t be as in Proposition 3.9. Denote by $N_{A,B}$ the conductor of $E^{(t)}_{A,B}$. Then the Galois representation*

$$\rho_l^{A,B} : \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{Aut}\big(E^{(t)}_{A,B}[l]\big)$$

is modular of level

$$N_0 = \prod_{p \in S_F} p^{\operatorname{ord}_p(N_{A,B})}. \tag{3.4}$$

In particular, there exists a newform f of level N_0.

Proof. This is Proposition 8.1 in [3]. □

3.3. A similar Frey curve for cubic forms

The Frey curve already given in Section 3.2 can be seen as sufficient; however, for ease of reference we give a construction from [6].

Let

$$F(x,y) = t_0a^3 + t_1^2y + t_2xy^2 + t_3y^3 \in \mathbb{Z}[x,y]$$

be a separable cubic binary form. In [6] a Frey curve is given for the Diophantine equation

$$F(a,b) = dc^l, \tag{3.5}$$

where $\gcd(a,b) = 1$, $d \in \mathbb{Z}$ is fixed and $l \geqslant 7$ is prime. Define a Frey curve $E_{a,b}$ by

$$E_{a,b}\colon\ y^2 = x^3 + a_2x^2 + a_4x + a_6, \tag{3.6}$$

where

$$a_2 = t_1 a - t_2 b,$$
$$a_4 = t_0 t_2 a^2 + (3t_0 t_3 - t_1 t_2)ab + t_1 t_3 b^2,$$
$$a_6 = t_0^2 t_3 a^3 - t_0\big(t_2^2 - 2t_1 t_3\big)a^2 b + t_3\big(t_1^2 - 2t_0 t_2\big)ab^2 - t_0 t_3^2 b^3.$$

Then $E_{a,b}$ has discriminant $16\Delta_F F(a,b)^2$. Consider the Galois representation

$$\rho_l^{a,b} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}\big(E_{a,b}[l]\big).$$

Theorem 3.11. *(See [6].) Let S be the set of primes dividing $2d\Delta_F$. There exists a constant $\alpha(d,F) \geqslant 0$ such that if $l > \alpha(d,F)$ and $c \neq \pm 1$ then*:

- *the representation $\rho_l^{a,b}$ is irreducible*;
- *at any prime $p \notin S$ dividing $F(a,b)$ Eq.* (3.6) *is minimal, the elliptic curve $E_{a,b}$ has multiplicative reduction and $l \mid \mathrm{ord}_p(\Delta_{\min}(E_{a,b}))$.*

Proof. This is Theorem 2.3 and Lemma 2.4 in [6]. □

4. Proof of Theorem 1.2

Proof of Theorem 1.2. Let $n = 2$ or 3 and let S be the set of primes dividing $n\Delta_E$. Assume that B_m is an lth power. Note that by Theorem 1.1 in [24] it is enough to bound l in terms of the Weierstrass equation (1.1) for E and P. To do this we shall derive an equation of the form (3.3) and prove the existence of a prime divisor p_0 to which Corollary 3.5 can be applied.

Using Theorem 2.4, fix $e_0 \geqslant 1$ such that

- $B_{n^{e_0}}$ is divisible by a prime $p_0 \nmid n\Delta_E$,
- $p_0 \nmid B_{n^e}$ for all $0 \leqslant e < e_0$.

Note that e_0 does not depend on m. From Lemma 2.1, since $\mathrm{ord}_n(B_1) > 0$,

$$\mathrm{ord}_n(B_m) - \big(\mathrm{ord}_n(B_1) + \mathrm{ord}_n(m)\big) = O(1).$$

Hence, since $l \mid \mathrm{ord}_n(B_m)$, we can assume that l is large enough so that

$$\mathrm{ord}_n(m) \geqslant e_0. \tag{4.1}$$

For $Q \in E(\mathbb{Q})$, using (3.1) gives

$$\frac{A_{nQ}}{B_{nQ}^2} = \frac{\theta_n(A_Q/B_Q^2)}{\psi_n^2(A_Q/B_Q^2)} = \frac{B_Q^{2n^2}\theta_n(A_Q/B_Q^2)}{B_Q^2\,\psi_n^2(A_Q/B_Q^2)B_Q^{2(n^2-1)}}, \tag{4.2}$$

where

$$\psi_n^2\big(A_Q/B_Q^2\big)B_Q^{2(n^2-1)} = \begin{cases} K_2^E(A_Q, B_Q^2) & \text{if } n = 2, \\ (K_3^E(A_Q, B_Q^2))^2 & \text{if } n = 3 \end{cases}$$

(see Definition 3.7). Since θ_n is monic and the leading coefficient of ψ_n^2 is n^2, B_Q is coprime with the numerator of (4.2) and if B_{nQ} is an lth power then B_Q is a power of n multiplied by an lth power. Write $m = n^{\mathrm{ord}_n m}m'$ with $n \nmid m'$. From (4.1) it follows that $B_{n^{e_0}m'}$ is a power of n multiplied by an

lth power. Write $Q = n^{e_0-1}m'P$ then $n^{e_0}m'P = nQ$. The primes which divide the numerator and the denominator of (4.2) also divide the discriminant Δ_E (see [1]). So

$$K_n^E\big(A_Q, B_Q^2\big) = uC^l, \tag{4.3}$$

where $u \in \mathbb{Z}_S^*$. Moreover, $p_0 \nmid B_Q$ (since $\gcd(B_Q, B_{n^{e_0}}) = B_{n^{e_0-1}}$) and so $C \in \mathbb{Z}$ is divisible by p_0. In characteristic away from n the multiplication by n map is separable (see Chapter III of [43]) so the set of primes which divide the discriminant of K_n^E is equal to S. Applying Proposition 3.10 shows that there exists a newform f of level N_0 (as in (3.4)). It follows that there are finitely many choices for f. We have $p_0 \nmid lN_0$ and $p_0 \mid N_{A_Q,B_Q}$ (see Proposition 3.9 and denote the conductor of the appropriately twisted Frey curve by N_{A_Q,B_Q}) so Corollary 3.5 bounds l. □

Remark 4.1. Note that $K_n^E(A_Q, B_Q^2)$, as in (4.3), does not belong to $\mathbb{Z}_S^*$ so Proposition 8.1 in [3] along with Silverman's primitive divisor theorem proves the existence of an effectively computable bound for l which depends only on the Weierstrass equation (1.1) for E and P. However, keeping in mind that $p_0 \nmid lN_0$, in practice a much better bound is obtained by computing the newforms at level N_0 and applying Proposition 3.3 directly.

Remark 4.2. Let S be a finite set of fixed primes and let (B_m) be an elliptic divisibility sequence whose first term is divisible by 2 or 3. The results in Section 3.2 hold with the primes in S added to S_F. Using this the proof above can be extended to show that there are finitely many terms in (B_m) equal to a perfect power multiplied by an S-unit.

5. The Mordell curves $y^2 = x^3 + D$

Proof of Theorem 1.4. Write $D = d^2D'$, where D' is square free. Suppose that $P \in E(\mathbb{Q})$ with $x(P) \neq 0$ and $B_P = z^l$ for some prime l. Factorizing over $K = \mathbb{Q}(\sqrt{D'})$,

$$A_P^3 = C_P^2 - Dz^{6l} = \big(C_P + d\sqrt{D'}z^{3l}\big)\big(C_P - d\sqrt{D'}z^{3l}\big).$$

If $D' = 1$ then $C_P + dz^{3l} = ua^3$ and $C_P - dz^{3l} = vb^3$, where $a, b \in \mathbb{Z}$ are coprime, u, v divide $2d$ and uv is a cube. Subtracting the two factors gives

$$2dz^{3l} = ua^3 - vb^3. \tag{5.1}$$

In general the ring of T-integers

$$\mathcal{O}_{KT} := \big\{x \in K\colon \operatorname{ord}_{\mathfrak{p}}(x) \geqslant 0 \text{ for all } \mathfrak{p} \notin T\big\}$$

is a principal ideal domain for some finite set T of prime ideals. Include in T the primes in $\mathcal{O}_K$ dividing $2d\sqrt{D'}$. Using Dirichlet's unit theorem, $\mathcal{O}_{KT}^*/\mathcal{O}_{KT}^{*3}$ is a finite set. Hence, if $D' \neq 1$ then

$$C_P + d\sqrt{D'}z^{3l} = \big(u + \sqrt{D'}v\big)\big(a + b\sqrt{D'}\big)^3,$$

where $a, b \in \mathbb{Z}$ are coprime and there are finitely many choices for $u, v \in \mathbb{Q}$. Subtracting the two conjugate factors gives

$$dz^{3l} = va^3 + 3ua^2b + 3D'vab^2 + uD'b^3. \tag{5.2}$$

Now suppose that (B_m) is an elliptic divisibility sequence generated by a point on E. Multiplying through by the denominators of u, v in (5.1) or (5.2) gives an equation

$$F(a, b) = dc^l$$

as in (3.5) with $c^l = B_m^3$. Note that u and v are non-zero in (5.1) and at least one of u, v is non-zero in (5.2); it follows that the cubic forms considered are separable. Construct a Frey curve $E_{a,b}$ as in (3.6). Let S be the set of primes dividing $2d\Delta_F$.

Assume that $n \mid B_1$ and $n > 1$ is prime. Using the Siegel–Mahler theorem about finiteness of S-integral points on elliptic curves, fix $e_0 \geqslant 1$ such that $B_{n^{e_0}}$ is divisible by a prime $p_0 \notin S$. Note that e_0 does not depend on m. From Lemma 2.1, since $\operatorname{ord}_n(B_1) > 1$,

$$\operatorname{ord}_n(B_m) - \big(\operatorname{ord}_n(B_1) + \operatorname{ord}_n(m)\big) = O(1).$$

Hence, since $l \mid \operatorname{ord}_n(B_m)$, we can assume l is large enough so that

$$\operatorname{ord}_n(m) \geqslant e_0.$$

Then $B_{n^{e_0}} \mid B_m$ and, in particular, $p_0 \mid B_m$. Applying Theorem 3.11, Proposition 3.3 and Corollary 3.5 with $p = p_0$ gives that l is bounded. (Note that p_0 divides the conductor of the Frey curve but not the level of the newform.) The finiteness claim follows from Theorem 1.1 in [24]. □

Proof of Proposition 1.5. Let $D \in \mathbb{Z}$ be square-free. For $P \in 2E(\mathbb{Q})$ write $P = 2Q$. Using the duplication formula,

$$\frac{A_P}{B_P^2} = \frac{A_Q(A_Q^3 - 8DB_Q^6)}{4B_Q^2(A_Q^3 + DB_Q^6)} = \frac{A_Q(A_Q^3 - 8DB_Q^6)}{4B_Q^2C_Q^2}. \tag{5.3}$$

Any prime dividing C_Q and $A_Q^3 - 8DB_Q^6$ also divides $3D$. Suppose that B_P is an lth power and that B_Q is even. Since D is square-free, $\gcd(A_Q, C_Q) = 1$ so only 3 can divide both C_Q and the numerator of (5.3). If $\gcd(3, C_Q) = 1$ then C_Q and $2B_Q$ must be an lth powers.

Note that $E(\mathbb{Q}) = \langle(-7/4, 19/8)\rangle$. Let $P = m(-7/4, 19/8)$ for some $m \geqslant 1$ and denote B_P, as in (1.2), by B_m. Assume that B_P is an lth power. Using Lemma 2.2 we can assume that $3 \nmid B_P$ and $3 \nmid m$. From Lemma 2.1,

$$\operatorname{ord}_2(B_m) = \operatorname{ord}_2(B_1) + \operatorname{ord}_2(m) = 1 + \operatorname{ord}_2(m) \geqslant l \tag{5.4}$$

so m is even. Thus $P = 2Q$ for some $Q \in E(\mathbb{Q})$. By (5.3) it follows that C_Q and $2B_Q$ are lth powers. To continue the proof, we need the following lemma.

Lemma 5.1. *If $l > 2$ then 13, 19 and 619 divide B_Q. Also $7 \mid A_Q$ but $7 \nmid B_Q C_Q$.*

Proof. If $l > 2$ then (5.4) gives that $m = 4m'$ thus $Q = 2m'(-7/4, 19/8)$ for some $m' \geqslant 1$ so $B_2 \mid B_Q$ and, in particular, $19 \mid B_Q$. Using Lemma 2.1 again,

$$\operatorname{ord}_{19}(B_Q) = \operatorname{ord}_{19}(B_2) + \operatorname{ord}_{19}\big(m'\big) = 1 + \operatorname{ord}_{19}\big(m'\big) \geqslant l$$

so $\operatorname{ord}_{19}(m') > 0$ and, in particular, $13 \mid B_Q$. Similarly, $B_{13} \mid B_Q$ so $619 \mid B_Q$.

Since $7 \mid B_3$ and $\gcd(B_P, B_3) = 2$, we have that $7 \nmid B_P$ so, from (5.3), $7 \nmid B_Q C_Q$. Reducing the equation $C_Q^2 - 11B_Q^6 = A_Q^3$ modulo 7 shows that $A_Q \equiv 0 \bmod 7$. □

Assume that $l \geqslant 5$. Consider the $(l, l, 3)$ triple given by

$$C_Q^2 - 11B_Q^6 = A_Q^3,$$

where the three terms are pairwise coprime. As in Theorem 3.6 construct a Frey Curve

$$E_Q\colon Y^2 + 3A_QXY - 11B_Q^6Y = X^3$$

with conductor $N_Q = 3^\alpha \cdot 11\,\mathrm{rad}_3(C_Q B_Q)$, where $\alpha = 2$ or 3. The Galois representation $\rho_l^{E_Q}$: $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E_Q[l])$ arises from a cuspidal newform f of weight 2 and level $N_0 = 2 \cdot 3^\alpha \cdot 11$. This newform is one of

$$\begin{aligned}
f_1 &= q - q^2 + q^4 + 2q^7 - q^8 + q^{11} + \cdots,\\
f_2 &= q - q^2 + q^4 + 4q^5 - 2q^7 - q^8 - 4q^{10} - q^{11} + \cdots,\\
f_3 &= q - q^2 + q^4 - 2q^5 - 4q^7 - q^8 + 2q^{10} + q^{11} + \cdots,\\
f_4 &= q + q^2 + q^4 + 2q^7 + q^8 - q^{11} + \cdots,\\
f_5 &= q + q^2 + q^4 + 2q^7 + q^8 + q^{11} + \cdots,
\end{aligned}$$

for $\alpha = 2$ or (up to conjugacy) one of

$$\begin{aligned}
f_6 &= q - q^2 + q^4 - 2q^5 + q^7 - q^8 + 2q^{10} - q^{11} + \cdots\\
f_7 &= q - q^2 + q^4 + q^5 + 4q^7 - q^8 - q^{10} - q^{11} + \cdots\\
f_8 &= q - q^2 + q^4 - 3q^5 - 4q^7 - q^8 + 3q^{10} - q^{11} + \cdots\\
f_9 &= q - q^2 + q^4 - 2q^5 - q^7 - q^8 + 2q^{10} + q^{11} + \cdots\\
f_{10} &= q + q^2 + q^4 + 2q^5 - q^7 + q^8 + 2q^{10} - q^{11} + \cdots\\
f_{11} &= q + q^2 + q^4 - q^5 + 4q^7 + q^8 - q^{10} + q^{11} + \cdots\\
f_{12} &= q + q^2 + q^4 + 2q^5 + q^7 + q^8 + 2q^{10} + q^{11} + \cdots\\
f_{13} &= q + q^2 + q^4 + 3q^5 - 4q^7 + q^8 + 3q^{10} + q^{11} + \cdots\\
f_{14} &= q - q^2 + q^4 + \theta q^5 + 2q^7 - q^8 - \theta q^{10} + q^{11} + \cdots\\
f_{15} &= q + q^2 + q^4 + \theta q^5 + 2q^7 + q^8 + \theta q^{10} - q^{11} + \cdots
\end{aligned}$$

for $\alpha = 3$, where the last two are defined over a quadratic number field and $\theta^2 + 2\theta - 9 = 0$. Applying Proposition 3.3 with $p = 13$, 19, 619 gives $l = 5$ if $f = f_2$ and $l < 5$ (a contradiction) otherwise. If $f = f_2$ then applying Proposition 4.2 in [5] with $p = 5$ gives a contradiction; note that 5 is a prime of good reduction and f_2 is rational so the restriction $l \neq 5$ in the proposition can be removed.

To eliminate the possibilities of $l = 2$ or 3 consider the parameterizations given in (5.2) with $D = 11$. Then $K = \mathbb{Q}(\sqrt{11})$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt{11}]$ is a principal ideal domain with fundamental unit $10 + 3\sqrt{11}$. Also $2\sqrt{11} = (10 - 3\sqrt{11})\sqrt{11}(3 + \sqrt{11})^2$. It follows that $(u, v) = (1, 0), (10, 3), (10, -3), (199, 60)$ or $(199, -60)$.

If $(u, v) = (1, 0)$ then $C_Q = a(a^2 + 33b^2)$ and $B_Q^3 = b(3a^2 + 11b^2)$, where b is even (since $4 \mid B_Q^3$). Since $33 \nmid C_Q$, a is an lth power. Write $a = C^l$. Since $2 \mid b$ and $3 \nmid b$, $b = 2^{3(l-1)} B^{3l}$. Write $a^2 + 33b^2 = \bar{C}$ and $3a^2 + 11b^2 = \bar{B}$. Then

$$3C^{2l} + 2^{6(l-1)} 11 B^{6l} = \bar{B}^{3l}, \tag{5.5}$$

$$C^{2l} + 2^{6(l-1)} 33 B^{6l} = \bar{C}^l, \tag{5.6}$$

$$\bar{B}^{3l} - 3\bar{C}^l = 2^{6l-3} 11 B^{6l}, \tag{5.7}$$

$$\bar{C}^l - 3\bar{B}^{3l} = -8C^{2l}, \tag{5.8}$$

where the terms in each of the ternary equations are nonzero and pairwise coprime. If $l = 2$ then (5.7) becomes $-3\bar{C}^2 + (\bar{B}^2)^3 - 2^3 11(2B^2)^6 = 0$ and Proposition 6.5.9 in [12] gives a (non-zero) rational point on the elliptic curve given by $Y^2 = X^3 - 2376$, but there are no such points. If $l = 3$ then (5.8) becomes $\bar{C}^3 + 3(-\bar{B}^3)^3 + (2C^2)^3 = 0$ and Proposition 6.4.14 in [12] gives a (non-zero) rational point with non-zero coordinates on the elliptic curve given by $Y^2 = X^3 + 144$, but there are no such points.

For the other parameterizations details are given only for $(u, v) = (10, 3)$. The other cases are similar. Assume that $(u, v) = (10, 3)$. Then $A_Q = a^2 - 11b^2$,

$$B_Q^3 = 3a^3 + 30a^2b + 99ab^2 + 110b^3$$

and

$$C_Q = 10a^3 + 99a^2b + 330ab^2 + 363b^3.$$

Suppose that $l = 2$. Since C_Q and $2B_Q$ are squares, multiplying the two expressions gives a rational point on the hyperelliptic curve

$$F\colon\ Y^2 = 60X^6 + 1194X^5 + 9900X^4 + 43780X^3 + 108900X^2 + 144474X + 79860.$$

But computations implemented in MAGMA confirm that the Jacobian of F has rank 0 and, via the method of Chabauty, $F(\mathbb{Q})$ is empty. Finally, suppose that $l = 3$. By Lemma 5.1, $A_Q \equiv 0 \bmod 7$. Hence, $a/b \equiv 2$ or $5 \bmod 7$. Substituting these in the parametrization of B_Q^3 shows that $a/b \equiv 5 \bmod 7$, but this cannot be a solution if C_Q is a cube. This completes the proof of Proposition 1.5. □

By (5.1) and (5.2) we see that Conjecture 1.6 would follow from

Conjecture 5.2. *(See [6].) Let F be a separable homogeneous cubic binary form with integer coefficients, d a fixed integer $\geqslant 1$ and l a prime number. There exists a constant $C_{d,F} > 0$ depending only on d and F such that if $l > C_{d,F}$ and*

$$F(a, b) = dc^l$$

with $\gcd(a, b) = 1$ *then* $c = \pm 1$.

In [6] it is explained that Conjecture 5.2 would follow from the Frey–Mazur conjecture.

Remark 5.3. A more direct Frey curve for $C_P^2 = A_P^3 + DB_P^6$ with B_P an lth power is

$$E_P\colon\ Y^2 = X^3 - 3A_PX + 2C_P.$$

However, parametrizing as above highlights the connection with cubic binary forms and, as in the proof of Proposition 1.5, helps resolve specific cases.

6. The congruent number curves $y^2 = x^3 - (2^a p^b)^2 x$

Let E_N be the elliptic curve given by $y^2 = x^3 - N^2x$, where N is a congruent number. For a non-torsion point $P \in E_N(\mathbb{Q})$ there exist non-zero integers z_1, z_2, z_3 so that

$$\begin{aligned} A_P &= \alpha_1 z_1^2, \\ A_P + NB_P^2 &= \alpha_2 z_2^2, \\ A_P - NB_P^2 &= \alpha_3 z_3^2, \end{aligned}$$

where the α_i are square free. Note that $\alpha_1 \mid N$, $\alpha_2 \mid 2N$ and $\gcd(z_1^2, z_2^2) \mid N$. So, in particular, $\gcd(z_1, z_2) = 1$ if N is square free. We have

$$\alpha_2 z_2^2 - \alpha_1 z_1^2 = N B_P^2; \tag{6.1}$$

$$\alpha_1 z_1^2 - \alpha_3 z_3^2 = N B_P^2; \tag{6.2}$$

$$\alpha_2 z_2^2 - \alpha_3 z_3^2 = 2N B_P^2; \tag{6.3}$$

$$2\alpha_1 z_1^2 - \alpha_2 z_2^2 = \alpha_3 z_3^2. \tag{6.4}$$

Theorem 6.1. *Suppose that l is an odd prime, r is a non-negative integer and U, V, W are non-zero pairwise coprime integers with*

$$U^l + 2^r V^l + W^l = 0. \tag{6.5}$$

Then $r = 1$ and $(U, V, W) = \pm(-1, 1, -1)$.

Proof. The result is due to Wiles [50] for $r = 0$, Ribet [38] for $r \geqslant 2$, and Darmon and Merel [17] for $r = 1$. □

Lemma 6.2. *Suppose that r is a non-negative integer and U, V, W are non-zero pairwise coprime integers. If*

$$U^4 - 2^r V^4 + W^4 = 0 \tag{6.6}$$

then $r = 1$ and $|U| = |V| = |W| = 1$. There are no solutions to the equation

$$2^r U^4 - V^4 + W^4 = 0. \tag{6.7}$$

Proof. See, for example, Section 6.5 of [12]. □

Proof of Theorem 1.7. The only torsion points in $E_N(\mathbb{Q})$ are 2-torsion. If b is even then the rank of $E_N(\mathbb{Q})$ is zero (since it is zero when $b = 0$), so assume that b is odd. Assume that $P \in 2E_N(\mathbb{Q})$ is non-zero. The fundamental 2-descent map (see, for example, Section 8.2.3 in [12]) shows that:

$$A_P = z_1^2;$$
$$A_P - 2^a p^b B_P^2 = z_2^2;$$
$$A_P + 2^a p^b B_P^2 = z_3^2.$$

Suppose that p divides A_P exactly e times. Then e is even, $e < b$, and, by replacing A_P by A_P/p^e and b by $b - e$, we can assume that p does not divide A_P. Eqs. (6.2)–(6.4) become:

$$-2^a p^b B_P^2 = (z_2 - z_1)(z_2 + z_1);$$
$$2^a p^b B_P^2 = (z_3 - z_1)(z_3 + z_1);$$
$$2^{a+1} p^b B_P^2 = (z_3 - z_2)(z_3 + z_2).$$

Now $\gcd(z_j - z_i, z_j + z_i)$ divides $2z_j$ and $2^{a+1} p^b B_P^2$, so is a power of 2.

Suppose that B_P is a perfect power. Now p divides $z_2+(-1)^{s_1}z_1$ and $z_3+(-1)^{s_2}z_1$, where $s_1, s_2 \in \{0,1\}$. So p divides $z_3+(-1)^{s_3}z_2$, where $s_3 = s_1+s_2+1$. *Siegel's identity*:

$$(-1)^{s_3+1}\frac{z_2+(-1)^{s_1}z_1}{z_3+(-1)^{s_3}z_2} - \frac{z_3+(-1)^{s_2}z_1}{z_3+(-1)^{s_3}z_2} + 1 = 0$$

gives (6.5), (6.6) or (6.7). Thus

$$(-1)^{s_3+1}\frac{z_2+(-1)^{s_1}z_1}{z_3+(-1)^{s_3}z_2} = u \quad \text{and} \quad -\frac{z_3+(-1)^{s_2}z_1}{z_3+(-1)^{s_3}z_2} = v,$$

where $(u,v) = (1,-2), (-2,1)$ or $(-\frac{1}{2}, -\frac{1}{2})$. So

$$-2^a p^b B_P^2 = (-1)^{s_3+1}u\big(z_2+(-1)^{s_1+1}z_1\big)\big(z_3+(-1)^{s_3}z_2\big)$$

and

$$2^a p^b B_P^2 = -v\big(z_3+(-1)^{s_2+1}z_1\big)\big(z_3+(-1)^{s_3}z_2\big).$$

Dividing the two equations gives

$$\frac{u}{v} = (-1)^{s_3+1}\frac{z_3+(-1)^{s_2+1}z_1}{z_2+(-1)^{s_1+1}z_1}.$$

But

$$\frac{z_3+(-1)^{s_3}z_2}{z_2+(-1)^{s_1+1}z_1} - \frac{z_3+(-1)^{s_2+1}z_1}{z_2+(-1)^{s_1+1}z_1} = (-1)^{s_3},$$

thus $u \neq v$,

$$\frac{z_2+(-1)^{s_1+1}z_1}{z_3+(-1)^{s_3}z_2} = (-1)^{s_3}\frac{v}{v-u},$$

and

$$\left(\frac{z_2+(-1)^{s_1+1}z_1}{z_3+(-1)^{s_3}z_2}\right)\left(\frac{z_2+(-1)^{s_1}z_1}{z_3+(-1)^{s_3}z_2}\right) = \frac{uv}{u-v} = \frac{-2^a p^b B_P^2}{(z_3+(-1)^{s_3}z_2)^2}.$$

So

$$\frac{-uv}{2^a p^b (u-v)}$$

is a square. Hence $(u,v) = (1,-2)$, $p=3$, a is odd, $B_P = 1$ and

$$\big(z_3+(-1)^{s_3}z_2\big)^2 = 2^{a-1}3^{b+1}.$$

Thus

$$z_3 = \frac{1}{2}\big(z_3+(-1)^{s_3}z_2 + z_3 + (-1)^{s_3+1}z_2\big) = \pm\frac{1}{2}\left(2^{\frac{a-1}{2}}3^{\frac{b+1}{2}} + \frac{2^{a+1}3^b}{2^{\frac{a-1}{2}}3^{\frac{b+1}{2}}}\right)$$

and

$$A_P = z_3^2 - 2^a 3^b = 2^{a-3} 3^{b-1} 25.$$

From which it follows that $a \geqslant 3$ and P is as required. □

Proof of Theorem 1.8. Let $N = 2^a p$ where $a = 0$ or 1. Let $P \in E_N(\mathbb{Q})$ non-torsion point with $x(P) \in -\mathbb{Q}^{*2}$ and $x(P) + N \in p\mathbb{Q}^{*2}$. If m is even then the result follows from Theorem 1.7. If m is odd then the fundamental 2-descent map (see, for example, 8.2.3 in [12]) shows that $\alpha_1 = -1$ and $\alpha_2 = p$ so $\alpha_3 = -p$.

Now (6.3) becomes $z_2^2 + z_3^2 = 2^{a+1} B_P^2$ and (6.4) becomes $2z_1^2 + pz_2^2 = pz_3^2$ so

$$z_2^2 + 2p(z_1/p)^2 = z_3^2.$$

Corollary 6.3.6 in [12] with the particular solution $(1, 0, 1)$ gives $dz_2 = s^2 - 2pt^2$, $dz_1 = 2pst$, $dz_3 = s^2 + 2pt^2$ where s, t are coprime integers and $d \mid 2p$.

If $d = \pm 1$ then $|z_2| = s^2 - 2pt^2$, $|z_1| = 2pst$ and $|z_3| = s^2 + 2pt^2$. Since z_1 is even, $a = 0$ and substituting into (6.3) gives $(s^2 - 2pt^2)^2 + (s^2 + 2pt^2)^2 = 2B_P^2$ so

$$s^4 + 4p^2 t^4 = B_P^2.$$

Now applying Theorem 1 in [4] shows that B_P cannot be a perfect power.

If $d = \pm 2$ then $|z_2| = 2s^2 - pt^2$, $|z_1| = 2pst$ and $|z_3| = 2s^2 + pt^2$, where s, t are coprime integers. So $a = 0$ and substituting into (6.3) gives

$$4s^4 + p^2 t^4 = B_P^2.$$

So $4s^4 = B_P^2 - p^2 t^4 = (B_P + pt^2)(B_P - pt^2)$. Since $2 \nmid B_P$ and $p \nmid B_P$, we have $B_P + pt^2 = \pm 2s'^4$ and $B_P - pt^2 = \pm 2t'^4$ where s', t' are coprime and odd. Thus $\pm s'^4 \pm t'^4 = B_P$. Again applying Theorem 1 in [4] shows that if B_P is a perfect power then it is a square or a cube, but these remaining cases are well known (see 6.5.2 of [12] and 14.6.6 of [13]).

Finally, the cases $d = \pm p$ and $d = \pm 2p$ give the same two parametrizations already considered above. □

References

[1] Mohamed Ayad, Points S-entiers des courbes elliptiques, Manuscripta Math. 76 (3–4) (1992) 305–324.

[2] A. Baker, The Diophantine equation $y^2 = ax^3 + bx^2 + cx + d$, J. Lond. Math. Soc. 43 (1968) 1–9.

[3] Michael A. Bennett, Sander R. Dahmen, Klein forms and the generalized superelliptic equation, preprint available at http://www.staff.science.uu.nl/~dahme104/KleinForms.pdf, 2010.

[4] Michael A. Bennett, Jordan S. Ellenberg, Nathan C. Ng, The Diophantine equation $A^4 + 2^\delta B^2 = C^n$, Int. J. Number Theory 6 (2) (2010) 311–338.

[5] Michael A. Bennett, Vinayak Vatsal, Soroosh Yazdani, Ternary Diophantine equations of signature $(p, p, 3)$, Compos. Math. 140 (6) (2004) 1399–1416, MR 2098394 (2005i:11036).

[6] Nicolas Billerey, Formes homogènes de degré 3 et puissances p-ièmes, J. Number Theory 128 (5) (2008) 1272–1294.

[7] I.F. Blake, G. Seroussi, N.P. Smart, Elliptic Curves in Cryptography, London Math. Soc. Lecture Note Ser., vol. 265, Cambridge University Press, 2000.

[8] Wieb Bosma, John Cannon, Catherine Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. 24 (3–4) (1997) 235–265.

[9] Christophe Breuil, Brian Conrad, Fred Diamond, Richard Taylor, On the modularity of elliptic curves over **Q**: Wild 3-adic exercises, J. Amer. Math. Soc. 14 (4) (2001) 843–939, (electronic).

[10] Yann Bugeaud, Maurice Mignotte, Samir Siksek, Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers, Ann. of Math. (2) 163 (3) (2006) 969–1018.

[11] J. Coates, An effective p-adic analogue of a theorem of Thue. III. The Diophantine equation $y^2 = x^3 + k$, Acta Arith. 16 (1969/1970) 425–435.

[12] Henri Cohen, Number Theory, vol. I. Tools and Diophantine Equations, Grad. Texts in Math., vol. 239, Springer, New York, 2007.
[13] Henri Cohen, Number Theory, vol. II. Analytic and Modern Tools, Grad. Texts in Math., vol. 240, Springer, New York, 2007.
[14] J.E. Cremona, Algorithms for Modular Elliptic Curves, Cambridge University Press, 1997.
[15] Sander R. Dahmen, Classical and modular methods applied to Diophantine equations, PhD thesis, University of Utrecht, 2008, http://igitur-archive.library.uu.nl/dissertations/2008-0820-200949/UUindex.html.
[16] Henri Darmon, Serre's conjectures, in: Seminar on Fermat's Last Theorem, Toronto, ON, 1993–1994, in: CMS Conf. Proc., vol. 17, Amer. Math. Soc., Providence, RI, 1995, pp. 135–153.
[17] Henri Darmon, Loïc Merel, Winding quotients and some variants of Fermat's last theorem, J. Reine Angew. Math. 490 (1997) 81–100.
[18] Fred Diamond, Jerry Shurman, A First Course in Modular Forms, Grad. Texts in Math., vol. 228, Springer-Verlag, New York, 2005.
[19] Konstantinos A. Draziotis, Integer points on the curve $Y^2 = X^3 \pm p^k X$, Math. Comp. 75 (255) (2006) 1493–1505 (electronic).
[20] Konstantinos Draziotis, Dimitrios Poulakis, Practical solution of the Diophantine equation $y^2 = x(x + 2^a p^b)(x - 2^a p^b)$, Math. Comp. 75 (255) (2006) 1585–1593 (electronic).
[21] Graham Everest, Helen King, Prime powers in elliptic divisibility sequences, Math. Comp. 74 (252) (2005) 2061–2071 (electronic).
[22] Graham Everest, Valéry Mahé, A generalization of Siegel's theorem and Hall's conjecture, Experiment. Math. 18 (1) (2009) 1–9.
[23] Graham Everest, Victor Miller, Nelson Stephens, Primes generated by elliptic curves, Proc. Amer. Math. Soc. 132 (4) (2004) 955–963 (electronic).
[24] Graham Everest, Jonathan Reynolds, Shaun Stevens, On the denominators of rational points on elliptic curves, Bull. Lond. Math. Soc. 39 (5) (2007) 762–770.
[25] J.-H. Evertse, On equations in S-units and the Thue–Mahler equation, Invent. Math. 75 (3) (1984) 561–584.
[26] J. Gebel, A. Pethő, H.G. Zimmer, Computing integral points on elliptic curves, Acta Arith. 68 (2) (1994) 171–192.
[27] Betül Gezer, Osman Bizim, Squares in elliptic divisibility sequences, Acta Arith. 144 (2) (2010) 125–134.
[28] Robert Gross, Joseph Silverman, S-integer points on elliptic curves, Pacific J. Math. 167 (2) (1995) 263–288.
[29] Patrick Ingram, Elliptic divisibility sequences over certain curves, J. Number Theory 123 (2) (2007) 473–486.
[30] Patrick Ingram, A quantitative primitive divisor result for points on elliptic curves, J. Théor. Nombres Bordeaux 21 (3) (2009) 609–634.
[31] Patrick Ingram, Joseph H. Silverman, Uniform estimates for primitive divisors in elliptic divisibility sequences, in: D. Goldfeld, J. Jorgenson, P. Jones, D. Ramakrishnan, K.A. Ribet, J. Tate (Eds.), Number Theory, Analysis and Geometry, In Memory of Serge Lang, Springer, ISBN 978-1-4614-1259-5, 2012.
[32] Felix Klein, Lectures on the Icosahedron and the Solution of Equations of the Fifth Degree, revised ed., Dover Publications Inc., New York, NY, 1956, translated into English by George Gavin Morrice.
[33] A. Kraus, J. Oesterlé, Sur une question de B. Mazur, Math. Ann. 293 (2) (1992) 259–275.
[34] Serge Lang, Elliptic Curves: Diophantine Analysis, Grundlehren Math. Wiss., vol. 231, Springer-Verlag, Berlin, 1978.
[35] Attila Pethő, Horst G. Zimmer, Josef Gebel, Emanuel Herrmann, Computing all S-integral points on elliptic curves, Math. Proc. Cambridge Philos. Soc. 127 (3) (1999) 383–402.
[36] K.A. Ribet, On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms, Invent. Math. 100 (2) (1990) 431–476.
[37] Kenneth A. Ribet, Report on mod l representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, in: Motives, Seattle, WA, 1991, in: Proc. Sympos. Pure Math., vol. 55, Amer. Math. Soc., Providence, RI, 1994, pp. 639–676.
[38] Kenneth A. Ribet, On the equation $a^p + 2^\alpha b^p + c^p = 0$, Acta Arith. 79 (1) (1997) 7–16.
[39] R. Shipsey, Elliptic divisibility sequences, PhD thesis, Goldsmith's College (University of London), 2000, http://homepages.gold.ac.uk/rachel/#PhD.
[40] Carl Ludwig Siegel, Über einige Anwendungen Diophantischer Approximationen, Abh. Preussischen Akademie der Wissenshaften, 1929.
[41] Joseph H. Silverman, Wieferich's criterion and the *abc*-conjecture, J. Number Theory 30 (2) (1988) 226–237.
[42] Joseph H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Grad. Texts in Math., vol. 151, Springer-Verlag, New York, 1994.
[43] Joseph H. Silverman, The Arithmetic of Elliptic Curves, Grad. Texts in Math., vol. 106, Springer, 2009.
[44] Joseph H. Silverman, John Tate, Rational Points on Elliptic Curves, Undergrad. Texts Math., Springer-Verlag, New York, 1992.
[45] Marco Streng, Elliptic divisibility sequences with complex multiplication, Master's thesis, Universiteit Utrecht, 2006, http://www.warwick.ac.uk/.
[46] R.J. Stroeker, N. Tzanakis, Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms, Acta Arith. 67 (2) (1994) 177–196.
[47] R.J. Stroeker, N. Tzanakis, Computing all integer solutions of a genus 1 equation, Math. Comp. 72 (244) (2003) 1917–1933, (electronic).
[48] Richard Taylor, Andrew Wiles, Ring-theoretic properties of certain Hecke algebras, Ann. of Math. (2) 141 (3) (1995) 553–572.
[49] Morgan Ward, Memoir on elliptic divisibility sequences, Amer. J. Math. 70 (1948) 31–74.
[50] Andrew Wiles, Modular elliptic curves and Fermat's last theorem, Ann. of Math. (2) 141 (3) (1995) 443–551.