Functiones et Approximatio
46.1 (2012), 133–145
doi: 10.7169/facm/2012.46.1.10

PERFECT POWERS GENERATED BY THE TWISTED FERMAT CUBIC

Jonathan Reynolds

Abstract: On the twisted Fermat cubic, an elliptic divisibility sequence arises as the sequence of denominators of the multiples of a single rational point. It is shown that there are finitely many perfect powers in such a sequence whose first term is greater than 1. Moreover, if the first term is divisible by 6 and the generating point is triple another rational point then there are no perfect powers in the sequence except possibly an lth power for some l dividing the order of 2 in the first term.

Keywords: Elliptic divisibility sequence; perfect powers; Fermat equation.

1. Introduction

A divisibility sequence is a sequence

$$W_1, W_2, W_3, \dots$$

of integers satisfying $W_n | W_m$ whenever $n|m$. The arithmetic of these has been and continues to be of great interest. Ward [41] studied a large class of recursive divisibility sequences and gave equations for points and curves from which they can be generated (see also [32]). In particular, Lucas sequences can be generated from curves of genus 0. Although Ward did not make such a distinction, sequences generated by curves of genus 1 have become exclusively known as elliptic divisibility sequences [20, 21, 24, 25] and have applications in Logic [11, 17, 18] as well as Cryptography [38]. See [36, 37] for background on elliptic curves (genus-1 curves with a point). Let $d \in \mathbb{Z}$ be cube-free and consider the elliptic curve

$$C : u^3 + v^3 = d.$$

It is sometimes said that C is a twist of the Fermat cubic. The set $C(\mathbb{Q})$ forms a group under the chord and tangent method: the (projective) point $[1, -1, 0]$ is

The author is supported by a Marie Curie Intra European Fellowship (PIEF-GA-2009-235210)

2010 Mathematics Subject Classification: primary: 11G05; secondary: 11D41

the identity and inversion is given by reflection in the line $u = v$. Suppose that $C(\mathbb{Q})$ contains a non-torsion point P. Then we can write, in lowest terms,

$$mP = \left(\frac{U_m}{W_m}, \frac{V_m}{W_m}\right). \tag{1}$$

The sequence (W_m) is a (strong) divisibility sequence (see Proposition 3.3 in [22]). Three particular questions about divisibility sequences have received much interest:

- How many terms fail to have a primitive divisor?
- How many terms are prime?
- How many terms are a perfect power?

A primitive divisor is a prime divisor which does not divide any previous term.

1.1. Finiteness

Bilu, Hanrot and Voutier proved that all terms in a Lucas sequence beyond the 30th have a primitive divisor [3]. Silverman showed that finitely many terms in an elliptic divisibility sequence fail to have to have a primitive divisor [34] (see also [39]). The Fibonacci and Mersenne sequences are believed to have infinitely many prime terms [7, 8]. The latter has produced the largest primes known to date. In [9] Chudnovsky and Chudnovsky considered the likelihood that an elliptic divisibility sequence might be a source of large primes; however, (W_m) coming from the twisted Fermat cubic has been shown to contain only finitely many prime terms [21]. Gezer and Bizim have described the squares in some periodic divisibility sequences [23]. Using modular techniques inspired by the proof of Fermat's Last Theorem, it was finally shown in [6] that the only perfect powers in the Fibonnaci sequence are 1, 8 and 144. We will show:

Theorem 1.1. *If $W_1 > 1$ then there are finitely many perfect powers in (W_m).*

The proof of Theorem 1.1 uses the divisibility properties of (W_m) along with a modular method for cubic binary forms given in [2]. For elliptic curves in Weierstrass form similar results have been shown in [29]. In the general case, allowing for integral points, Conjecture 1.1 in [2] would give that there are finitely many perfect powers in (W_m).

1.2. Uniformness

What is particularly special about sequences (W_m) coming from twisted Fermat cubics is that they have yielded uniform results as sharp as some of their genus-0 analogues mentioned above. It has been shown that all terms of (W_m) beyond the first have a primitive divisor [19] and, in particular, we will make use of the fact that the second term always has a primitive divisor $p_0 > 3$ (see Section 6.2 in [19]). The number of prime terms in (W_m) is also bounded independently of d [22] and, in particular, if P is triple a rational point then all terms beyond the first fail to be prime (see Theorem 1.2 in [22]). Similar results can be achieved for perfect powers. Indeed:

Theorem 1.2. *Suppose that W_1 is even and at all primes greater than 3, P has non-singular reduction (on a minimal Weierstrass equation for C). If W_m is an lth power for some prime l then*

$$l \leqslant \max\left\{\mathrm{ord}_2(W_1), (1+\sqrt{p_0})^2\right\},$$

where $p_0 > 3$ is any primitive divisor of W_2. Moreover, for fixed $l > \mathrm{ord}_2(W_1)$ the number of lth powers in (W_m) is bounded independently of d.

Although the conditions in Theorem 1.2 appear to depend heavily on the point, in the next theorem we exploit the fact that group $C(\mathbb{Q})$ modulo the points of non-singular reduction has order at most 3 for a prime greater than 3.

Theorem 1.3. *Suppose that $6 \mid W_1$ and $P \in 3C(\mathbb{Q})$ (or P has non-singular reduction at all primes greater than 3). If W_m is an lth power for some prime l then $l \mid \mathrm{ord}_2(W_1)$. In particular, if $\mathrm{ord}_2(W_1) = 1$ then (W_m) contains no perfect powers.*

The conditions in Theorem 1.3 are sometimes satisfied for every rational non-torsion point on C. For example, we have

Corollary 1.4. *The only solutions to the Diophantine equation*

$$U^3 + V^3 = 15W^{3l}$$

with $l > 1$ and $\gcd(U, V, W) = 1$ have $W = 0$.

2. Properties of elliptic divisibility sequences

In this section the required properties of (W_m) are collected.

Lemma 2.1. *Let p be a prime. For any pair $n, m \in \mathbb{N}$, if $\mathrm{ord}_p(W_n) > 0$ then*

$$\mathrm{ord}_p(W_{mn}) = \mathrm{ord}_p(W_n) + \mathrm{ord}_p(m).$$

Proof. See equation (10) in [22]. ■

Proposition 2.2. *For all $n, m \in \mathbb{N}$,*

$$\gcd(W_m, W_n) = W_{\gcd(m,n)}.$$

In particular, for all $n, m \in \mathbb{N}$, $W_n \mid W_{nm}$.

Proof. See Proposition 3.3 in [22]. ■

Theorem 2.3 ([19]). *If $m > 1$ then W_m has a primitive divisor.*

3. The modular approach to Diophantine equations

For a more thorough exploration see [13] and Chapter 15 in [10]. 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 $K_f = \mathbb{Q}(c_2, c_3, \cdots)$ 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 [12], implemented on `MAGMA` [4] 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 pth coefficient of f and $a_p(E) = p + 1 - \#E(\mathbb{F}_p)$.*

Proof. This is due to Taylor and Wiles [40, 42] in the semi-stable case. The proof was completed by Breuil, Conrad, Diamond and Taylor [5]. ■

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 $a_p(E) = p + 1 - \#E(\mathbb{F}_p)$.*

Proof. See Chapter 8 of [16]. ■

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*

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

Suppose that the Galois representation

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

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

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

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

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

Proof. This arose from combining modularity with level-lowering results by Ribet [30, 31]. The strengthening in the case $\mathcal{O}_f = \mathbb{Z}$ is due to Kraus and Oesterlé [27]. A detailed exploration is given, for example, in Chapter 2 of [13]. ■

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 [35]). In particular, only primes of bad reduction divide N and if E has multiplicative reduction at p then $p \mid\mid N$.

Corollary 3.5. *Keeping the notation of Proposition 3.3, if p is a prime such that $p \nmid lN_0$ and $p \mid N$ then*

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

Proof. See Theorem 37 in [13]. ■

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 [42] but there are now constructions for other equations and we shall make use of those described below.

3.1. A Frey curve for cubic binary forms

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 [2] a Frey curve is given for the Diophantine equation

$$F(a,b) = dc^l, \tag{2}$$

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

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

where

$$\begin{aligned} a_2 &= t_1a - t_2b, \\ a_4 &= t_0t_2a^2 + (3t_0t_3 - t_1t_2)ab + t_1t_3b^2, \\ a_6 &= t_0^2t_3a^3 - t_0(t_2^2 - 2t_1t_3)a^2b + t_3(t_1^2 - 2t_0t_2)ab^2 - t_0t_3^2b^3. \end{aligned}$$

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

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

Theorem 3.6 ([2]). *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 $F(a,b)$ the equation (3) is minimal, the elliptic curve $E_{a,b}$ has multiplicative reduction and $l \mid \mathrm{ord}_p(\Delta_{min}(E_{a,b}))$.*

3.2. Recipes for Diophantine equations with signature (l,l,l)

The following recipe due to Kraus [28] is taken from [10]. Consider the equation

$$Ax^l + By^l + Cz^l = 0,$$

with non-zero pairwise coprime terms and $l \geqslant 5$ prime. Setting $R = ABC$ assume that any prime q satisfies $\mathrm{ord}_q(R) < l$. Without lost of generality also assume that $By^l \equiv 0 \mod 2$ and $Ax^l \equiv -1 \mod 4$. Construct the Frey curve

$$E_{x,y} : Y^2 = X(X - Ax^l)(X + By^l).$$

The conductor $N_{x,y}$ of $E_{x,y}$ is given by

$$N_{x,y} = 2^\alpha \,\mathrm{rad}_2(Rxyz),$$

where

$$\alpha = \begin{cases} 1, & \text{if } \mathrm{ord}_2(R) \geqslant 5 \text{ or } \mathrm{ord}_2(R) = 0, \\ 1, & \text{if } 1 \leqslant \mathrm{ord}_2(R) \leqslant 4 \text{ and } y \text{ is even}, \\ 0, & \text{if } \mathrm{ord}_2(R) = 4 \text{ and } y \text{ is odd}, \\ 3, & \text{if } 2 \leqslant \mathrm{ord}_2(R) \leqslant 3 \text{ and } y \text{ is odd}, \\ 5, & \text{if } \mathrm{ord}_2(R) = 1 \text{ and } y \text{ is odd}. \end{cases}$$

Theorem 3.7 (Kraus [28]). *The Galois representation*

$$\rho_l^{x,y} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E_{x,y}[l])$$

is irreducible and $N_0(E_{x,y}, l)$ in Proposition 3.3 is given by

$$N_0 = 2^\beta \,\mathrm{rad}_2(R),$$

where

$$\beta = \begin{cases} 1, & \textit{if } \mathrm{ord}_2(R) \geqslant 5 \textit{ or } \mathrm{ord}_2(R) = 0, \\ 0, & \textit{if } \mathrm{ord}_2(R) = 4, \\ 1, & \textit{if } 1 \leqslant \mathrm{ord}_2(R) \leqslant 3 \textit{ and } y \textit{ is even}, \\ 3, & \textit{if } 2 \leqslant \mathrm{ord}_2(R) \leqslant 3 \textit{ and } y \textit{ is odd}, \\ 5, & \textit{if } \mathrm{ord}_2(R) = 1 \textit{ and } y \textit{ is odd}. \end{cases}$$

4. Proof of Theorem 1.1

Proof of Theorem 1.1. Assume that $W_1 > 1$ and W_m is an lth power for some prime l. Firstly we will use the Frey curve for cubic binary forms constructed in Section 3.1 and prove the existence of a prime divisor p to which Corollary 3.5 can be applied, giving a bound for l. Let S be the set of primes dividing $27d$. By assumption, W_1 is divisible by a prime q. Lemma 2.1 gives that

$$l \leqslant \mathrm{ord}_q(W_m) = \mathrm{ord}_q(W_1) + \mathrm{ord}_q(m).$$

Using Theorem 2.3 (or that there are only finitely many solutions to a Thue-Mahler equation), let l be large enough so that W_n is divisible by a prime $p \notin S$, where

$$n = q^{l-\mathrm{ord}_q(W_1)}.$$

Note that we can choose this lower bound for l and p independently of m. Then, using Proposition 2.2, $p \mid W_m$. Now construct a Frey curve $E_{U,V}$ for the Diophantine equation

$$U_m^3 + V_m^3 = dW^l$$

as in Section 3.1 (in our case $F(x, y) = x^3 + y^3$) and consider the Galois representation

$$\rho_l : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E_{U,V}[l]).$$

Using Theorem 3.6, choose l larger than some constant so that p divides the conductor of $E_{U,V}$ exactly once and the primes dividing N_0 in Proposition 3.3 belong to S. Since there are finitely many newforms of level N_0, Corollary 3.5 bounds l. Finally, for fixed l there are finitely many solutions by Theorem 1 in [14]. ■

5. Proof of Theorem 1.2

Proof of Theorem 1.2. Assume that W_m is an lth power. We will derive an (l, l, l) equation (9) which does not depend on d and use the Frey curve given Section 3.2. Then, similarly to the proof of Theorem 1.1, the existence of a prime divisor p_0 will be shown which bounds l via Corollary 3.5. Since $2 \mid W_1$, by Lemma 2.1,

$$l \leqslant \mathrm{ord}_2(W_m) = \mathrm{ord}_2(W_1) + \mathrm{ord}_2(m).$$

Assume that $l > \mathrm{ord}_2(W_1)$. Then $\mathrm{ord}_2(m) > 0$ so $m = 2m'$ for some m'.

A Weierstrass equation for C is

$$y^2 = x^3 - 2^4 3^3 d^2, \tag{4}$$

with coordinates $x = 2^2 3d/(u + v)$ and $y = 2^2 3^2 d(u - v)/(u + v)$. Write $x(mP) = A_m/B_m^2$ and $y(mP) = C_m/B_m^3$ in lowest terms.

Lemma 5.1 (see Corollary 3.2 in [22]). *Let $p = 2$ or 3. then $p \mid W_m$ if and only if $p \nmid A_m$.*

The discriminant of (4) is $-2^{12}3^9d^4$ so, since d is cube free, it is minimal at any prime larger than 3 (see Remark 1.1 in Chapter VII [36]). Note that the group of points with non-singular reduction is independent of the choice of minimal Weierstrass equation. The projective equation of (4) is

$$Y^2Z = X^3 - 2^4 3^3 d^2 Z^3.$$

Let $p > 3$ be a prime dividing d. By assumption, the partial derivatives

$$\frac{\partial C}{\partial X} = -3X^2, \qquad \frac{\partial C}{\partial Y} = 2YZ \qquad \text{and} \qquad \frac{\partial C}{\partial Z} = Y^2 + 2^4 3^4 d^2 Z^2 \tag{5}$$

do not vanish simultaneously at $P = [A_1B_1, C_1, B_1^3]$ over the field $\mathbb{F}_p$. Hence, noting that $2 \nmid A_m$ from Lemma 5.1 and that non-singular points form a group, we have

$$\gcd(A_m^3, C_m^2) \mid 3^{3+2\operatorname{ord}_3(d)} \tag{6}$$

for all m.

The inverses of the birational transformation are given by $u = (2^2 3^2 d + y)/6x$ and $v = (2^2 3^2 d - y)/6x$. Thus

$$\frac{U_m}{W_m} = \frac{2^2 3^2 d B_m^3 + C_m}{6A_mB_m} \qquad \text{and} \qquad \frac{V_m}{W_m} = \frac{2^2 3^2 d B_m^3 - C_m}{6A_mB_m}. \tag{7}$$

The assumptions made restrict the cancellation which can occur in (7) and, up to cancellation, if W_m is an lth power then so is A_m. More precisely, since W_m is an lth power and $2 \mid W_m$, Lemma 5.1 and (6) give that A_m is an lth power multiplied by a power of 3. Using the duplication formula,

$$\frac{A_m}{B_m^2} = \frac{A_{m'}(A_{m'}^3 + 8(2^4 3^3 d^2)B_{m'}^6)}{4B_{m'}^2(A_{m'}^3 - 2^4 3^3 d^2 B_{m'}^6)} = \frac{A_{m'}(A_{m'}^3 + 8(2^4 3^3 d^2)B_{m'}^6)}{4B_{m'}^2 C_{m'}^2}. \tag{8}$$

Again, cancellation in (8) is restricted so $A_{m'}$ is also an l power multiplied by a power of 3. Write

$$m = 2^{\operatorname{ord}_2(m)} n.$$

It follows that $A_n = 3^e A^l$,

$$A_n^3 + 8(2^4 3^3 d^2)B_n^6 = 3^f \bar{A}^l$$

and $C_n = \pm 3^g C^l$. Combining with $C_n^2 = A_n^3 - 2^4 3^3 d^2 B_n^6$ gives

$$3^f \bar{A}^l + 2^3 3^{2g} C^{2l} = 3^{2+3e} A^{3l}. \tag{9}$$

Note that, by dividing (9) through by an appropriate power of 3, we can assume that 3 divides at most one of the three terms.

Let $p_0 > 3$ be a primitive divisor of W_2. Using Proposition 2.2, $p_0 \mid W_{2n}$ and, since n is odd, $p_0 \mid \bar{A}C$. Now follow the recipe given in Section 3.2. The conductor of the Frey curve for (9) is

$$N_{\bar{A},C} = 2^3 3^\delta \operatorname{rad}_3(\bar{A}CA)$$

and $N_0 = 2^3 3^\delta$ in Theorem 3.7, where $\delta = 0$ or 1. There is one newform

$$f = q - q^3 - 2q^5 + q^9 + 4q^{11} + \cdots$$

of level $N_0 = 24$. Moreover, f is rational. Since $p_0 \mid N_{\bar{A},C}$ and $p_0 \nmid N_0$,

$$l < (1 + \sqrt{p_0})^2$$

by Corollary 3.5. Finally, for fixed $l > 1$ there are finitely many solutions to (9) (see Theorem 2 in [14]) and they are independent of d. ■

6. Proof of Theorem 1.3

Proof of Theorem 1.3. As in the proof of Theorem 1.2, consider $x(P) = A_P/B_P^2$ and $y(P) = C_P/B_P^3$ on the Weierstrass equation

$$y^2 = x^3 - 2^4 3^3 d^2$$

for C. Since P is triple another rational point, a prime of bad reduction greater 3 does not divide A_P (see Section 3 in [19]). Thus the partial derivatives (5) do not vanish simultaneously at P and so at all primes greater than 3, P has non-singular reduction on a minimal Weierstrass for C.

Now follow the proof of Theorem 1.2 up to (8). Factorizing over $\mathbb{Z}[\sqrt{-3}]$ gives

$$A_n^3 = C_n^2 + 2^4 3^3 d^2 B_n^6 = (C_n + 2^2 3 d B_n^3 \sqrt{-3})(C_n - 2^2 3 d B_n^3 \sqrt{-3}).$$

We have

$$C_n + 2^2 3 d B_n^3 \sqrt{-3} = (-1 + \sqrt{-3})^s (a + b\sqrt{-3})^3 / 2^{s+3},$$

where $s = 0, 1$ or 2 and a, b are integers of the same parity. If $s = 0$ then

$$2^3 (C_n + 2^2 3 d B_n^3 \sqrt{-3}) = a(a^2 - 9b^2) + 3b(a^2 - b^2)\sqrt{-3},$$

so

$$2^3 C_n = a(a^2 - 9b^2), \tag{10}$$
$$2^5 d B_n^3 = b(a^2 - b^2), \tag{11}$$
$$2^2 A_n = a^2 + 3b^2. \tag{12}$$

If $s = 1$ then

$$\begin{aligned} 2^4 C_n &= -a^3 + 9ab^2 - 9a^2 b + 9b^3, \\ 2^6 3 d B_n^3 &= a^3 - 3a^2 b - 9ab^2 + 3b^3, \\ 2^2 A_n &= a^2 + 3b^2. \end{aligned}$$

If $s = 2$ then

$$\begin{aligned} 2^5 C_n &= -2a^3 + 18a^2 b + 18ab^2 - 18b^3, \\ 2^7 3dB_n^3 &= -2a^3 - 6a^2 b + 18ab^2 + 6b^3, \\ 2^2 A_n &= a^2 + 3b^2. \end{aligned}$$

By Lemma 5.1, $6 \nmid A_n$ so we are in the case $s = 0$.

Suppose that W_m is a square. Then, from (8), $C_n = \pm C^2$, $2B_n = \pm B^2$ and $A_n = A^2$. Since $\gcd(a, b) \mid 2^2$, one of b or $a^2 - b^2$ is coprime with the odd primes dividing d. If it is b then multiplying (10) and (12) gives

$$\pm 2^5 (AC)^2 = a^5 - 6a^3 b^2 - 27ab^4$$

and, since b, up to sign, is either a square or 2 multiplied by a square, dividing by b^5 gives a rational point on the hyperelliptic curve

$$Y^2 = X^5 - 6X^3 - 27X$$

with non-zero coordinates; but computations implemented in `MAGMA` confirm that the Jacobian of the curve has rank 0 and, via the method of Chabauty, there are no such points. If $a^2 - b^2$ is coprime with the odd primes dividing d then multiplying with (12) gives a rational point on the elliptic curve

$$\pm Y^2 = X^4 + 2X^2 - 3$$

or on the elliptic curve

$$\pm 2^3 Y^2 = X^4 + 2X^2 - 3$$

with non-zero coordinates; but there are no such points.

Suppose that W_m is an lth power for some odd prime l. Then, from (8), C_n, $2B_n$ and A_n are lth powers. If a is odd then (10) gives $a = C^l$, $a^2 - 9b^2 = 2^3 \bar{C}^l$ and

$$C^{2l} - 2^3 \bar{C}^l = 9b^2. \tag{13}$$

If a is even then $a = 2C^l$, $a^2 - 9b^2 = 2^2 \bar{C}^l$ and

$$2^2 C^{2l} - 2^2 \bar{C}^l = 9b^2. \tag{14}$$

Thus, Theorem 15.3.4 in [10] (due to Bennett and Skinner [1], Ivorra [26] and Siksek [33]) and Theorem 15.3.5 in [10] (due to Darmon and Merel [15]) give that $l \leqslant 5$. If $l = 3$ then we have a rational point on the elliptic curve

$$Z^6 + X^3 = Y^2;$$

this curve has rank and gives a possible solution $\bar{C} = -1$, $a = C = \pm 1$ and $b = \pm 1$, but, from (11), we would have $B_n = 0$. If $l = 5$ then we have a rational point on the hyper elliptic curve

$$Y^2 = 8^e X^5 + 1,$$

where $e = 0$ or 1; but computations implemented in `MAGMA` confirm, via the method of Chabauty, that no such points give a required solution. ∎

References

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

[2] Nicolas Billerey, *Formes homogènes de degré 3 et puissances p-ièmes*, J. Number Theory **128** (2008), no. 5, 1272–1294.

[3] Yu. Bilu, G. Hanrot, and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine Angew. Math. **539** (2001), 75–122, With an appendix by M. Mignotte. MR 1863855 (2002j:11027).

[4] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265.

[5] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic).

[6] Yann Bugeaud, Maurice Mignotte, and Samir Siksek, *Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers*, Ann. of Math. (2) **163** (2006), no. 3, 969–1018.

[7] Chris Caldwell, *Mersenne primes: History, theorems and lists*, `http://primes.utm.edu/mersenne/index.html`.

[8] Chris Caldwell, *The prime pages: Fibonacci prime*, `http://primes.utm.edu/glossary/page.php?sort=FibonacciPrime`.

[9] D. V. Chudnovsky and G. V. Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests*, Adv. in Appl. Math. **7** (1986), no. 4, 385–434. MR 866702 (88h:11094)

[10] Henri Cohen, *Number theory. Vol. II. Analytic and modern tools*, Graduate Texts in Mathematics, vol. 240, Springer, New York, 2007.

[11] Gunther Cornelissen and Karim Zahidi, *Elliptic divisibility sequences and undecidable problems about rational points*, J. Reine Angew. Math. **613** (2007), 1–33.

[12] J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, 1997.

[13] Sander R. Dahmen, *Classical and modular methods applied to Diophantine equations*, Ph.D. thesis, University of Utrecht, 2008, `http://igitur-archive.library.uu.nl/dissertations/2008-0820-200949/UUindex.html`.

[14] Henri Darmon and Andrew Granville, *On the equations* $z^m = F(x,y)$ *and* $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. **27** (1995), no. 6, 513–543.

[15] Henri Darmon and Loïc Merel, *Winding quotients and some variants of Fermat's last theorem*, J. Reine Angew. Math. **490** (1997), 81–100.

[16] Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005.

[17] Kirsten Eisenträger and Graham Everest, *Descent on elliptic curves and Hilbert's tenth problem*, Proc. Amer. Math. Soc. **137** (2009), no. 6, 1951–1959.

[18] Kirsten Eisenträger, Graham Everest, and Alexandra Shlapentokh, *Hilbert's Tenth Problem and Mazur's Conjectures in Complementary Subrings of Number Fields*, `http://arxiv.org/abs/1012.4878`, 2010.

[19] Graham Everest, Patrick Ingram, and Shaun Stevens, *Primitive divisors on twists of Fermat's cubic*, LMS J. Comput. Math. **12** (2009), 54–81.

[20] Graham Everest and Helen King, *Prime powers in elliptic divisibility sequences*, Math. Comp. **74** (2005), no. 252, 2061–2071 (electronic).

[21] Graham Everest, Victor Miller, and Nelson Stephens, *Primes generated by elliptic curves*, Proc. Amer. Math. Soc. **132** (2004), no. 4, 955–963 (electronic).

[22] Graham Everest, Ouamporn Phuksuwan, and Shaun Stevens, *The uniform primality conjecture for the twisted fermat cubic*, `http://arxiv.org/abs/1003.2131`, 2010.

[23] Betül Gezer and Osman Bizim, *Squares in elliptic divisibility sequences*, Acta Arith. **144** (2010), no. 2, 125–134.

[24] Patrick Ingram, *Elliptic divisibility sequences over certain curves*, J. Number Theory **123** (2007), no. 2, 473–486.

[25] Patrick Ingram and Joseph H. Silverman, *Uniform estimates for primitive divisors in elliptic divisibility sequences*, to appear in a forthcoming memorial volume for Serge Lang, published by Springer-Verlag.

[26] Wilfrid Ivorra, *Sur les équations $x^p + 2^\beta y^p = z^2$ et $x^p + 2^\beta y^p = 2z^2$*, Acta Arith. **108** (2003), no. 4, 327–338. MR 1979902 (2004b:11036)

[27] A. Kraus and J. Oesterlé, *Sur une question de B. Mazur*, Math. Ann. **293** (1992), no. 2, 259–275.

[28] Alain Kraus, *Majorations effectives pour l'équation de Fermat généralisée*, Canad. J. Math. **49** (1997), no. 6, 1139–1161.

[29] Jonathan Reynolds, *Perfect powers in elliptic divisibility sequences*, `http://arxiv.org/abs/1101.2949`, 2011.

[30] K. A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), no. 2, 431–476.

[31] Kenneth A. Ribet, *Report on mod l representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math., vol. 55, Amer. Math. Soc., Providence, RI, 1994, pp. 639–676.

[32] R. Shipsey, *Elliptic divisibility sequences*, Ph.D. thesis, Goldsmith's College (University of London), 2000, `http://homepages.gold.ac.uk/rachel/#PhD`.

[33] Samir Siksek, *On the Diophantine equation $x^2 = y^p + 2^k z^p$*, J. Théor. Nombres Bordeaux **15** (2003), no. 3, 839–846. MR 2142239 (2005m:11049)

[34] Joseph H. Silverman, *Wieferich's criterion and the abc-conjecture*, J. Number Theory **30** (1988), no. 2, 226–237.

[35] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.

[36] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer, 2009.

[37] Joseph H. Silverman and John Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.

[38] Katherine Stange and Kristin Lauter, *The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences*, Selected Areas in Cryptography **5381** (2008), 309–327.

[39] Marco Streng, *Elliptic divisibility sequences with complex multiplication*, Master's thesis, Universiteit Utrecht, 2006, `http://www.warwick.ac.uk/~masjap/mthesis.pdf`.

[40] Richard Taylor and Andrew Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572.

[41] Morgan Ward, *Memoir on elliptic divisibility sequences*, Amer. J. Math. **70** (1948), 31–74.

[42] Andrew Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.

Address: Jonathan Reynolds: Mathematisch Instituut, Universiteit Utrecht, Postbus 80.010, 3508 TA Utrecht, Nederland.

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

Received: 5 April 2011