

## POWERS IN RECURRENCE SEQUENCES: PELL EQUATIONS

MICHAEL A. BENNETT

**ABSTRACT.** In this paper, we present a new technique for determining all perfect powers in so-called Pell sequences. To be precise, given a positive nonsquare integer  $D$ , we show how to (practically) solve Diophantine equations of the form

$$x^2 - Dy^{2n} = 1$$

in integers  $x, y$  and  $n \geq 2$ . Our method relies upon Frey curves and corresponding Galois representations and eschews lower bounds for linear forms in logarithms. Along the way, we sharpen and generalize work of Cao, Af Ekenstam, Ljunggren and Tartakowsky on these and related questions.

### 1. INTRODUCTION

Many problems in number theory may be reduced to finding the intersection of two sequences of positive integers, the philosophy being, barring local obstructions, that the finiteness of this intersection should depend solely upon how quickly the two sequences grow. In several situations, such statements may be made more precise, often by appealing to results from the theory of Diophantine approximation. For example, if we choose the two sequences to be a nondegenerate binary linear recurrence sequence and the sequence of perfect powers of integers, then we have the following

**Theorem 1.1** (Pethő [18], Shorey and Stewart [21]). *Let  $h$  be a nonzero integer and let  $u_n$  be the  $n$ th term of a nondegenerate binary recurrence sequence. If*

$$hx^q = u_n,$$

*for integers  $x$  and  $q$  larger than one, then the maximum of  $x, q$  and  $n$  is less than an effective constant (depending only upon  $h$  and the recurrence sequence).*

This result rests upon lower bounds for linear forms in logarithms of algebraic numbers (i.e. Baker's method).

To quantify this statement for a given recurrence can be rather difficult. For example, if we consider the Fibonacci sequence

$$F = \{0, 1, 1, 2, 3, 5, 8, 13, \dots\}$$

and write

$$P = \{1, 4, 8, 9, 16, 25, 27, \dots\}$$

---

Received by the editors July 20, 2003 and, in revised form, December 4, 2003.

2000 *Mathematics Subject Classification.* Primary 11D41; Secondary 11D45, 11B37.

*Key words and phrases.* Pell sequences, perfect powers, Thue equations.

This work was supported in part by a grant from NSERC.

for the sequence of positive perfect powers, then the only terms in common are 1, 8 and 144. Surprisingly, this result was only recently proven (see [7]; the proof is along similar lines to the work outlined here, only with additional highly nontrivial complications).

In this paper, we will consider a related problem, specifically that of determining the perfect powers that arise in so-called Pell sequences. Despite being, it must be confessed, of apparently rather specialized interest, one encounters a surprisingly rich literature on the subject. An early result along these lines is one of Ljunggren [14] which states that the Diophantine equation

$$(1.1) \quad x^2 - Dy^{2n} = 1$$

has, for  $n$  and  $D$  fixed integers with  $n \geq 2$ , at most two solutions in positive integers  $x$  and  $y$ , at least provided we do not have  $D = m^2 - 1$  for some  $m \in \mathbb{N}$ . To be somewhat more precise, one has

**Theorem 1.2** (Ljunggren [14]). *If  $D$  is a nonsquare positive integer such that  $D \neq m^2 - 1$  for any integer  $m$ , and  $n \geq 2$  is an integer, then the Diophantine equation (1.1) has at most two solutions in positive integers  $x$  and  $y$ . If there are two solutions, these correspond to the fundamental solution and its square or fourth power.<sup>1</sup>*

In fact, Ljunggren proved a stronger result if  $n \in \{2, 3\}$  (extending the above conclusion to include  $D$  of the form  $D = m^2 - 1$ ). The state of the art in case  $n = 2$  is a theorem of Walsh [28]. Before we state this, we define some quantities of which we will have later need. Suppose that  $D$  is a positive nonsquare integer and let  $u_1$  and  $v_1$  be the smallest positive integers such that

$$(1.2) \quad u_1^2 - Dv_1^2 = 1.$$

We call  $(u_1, v_1)$  the *fundamental solution* to the equation  $u^2 - Dv^2 = 1$ . Further define sequences of integers  $\{u_k\}$  and  $\{v_k\}$  by

$$u_k + v_k\sqrt{D} = \left(u_1 + v_1\sqrt{D}\right)^k.$$

We have

**Theorem 1.3** (Walsh [28]). *Let  $D$  be a positive nonsquare integer. Then there are at most two pairs of positive integers  $(x, y)$  such that*

$$(1.3) \quad x^2 - Dy^4 = 1.$$

*If there are two such solutions, say  $(x_1, y_1)$  and  $(x_2, y_2)$  with  $y_1 < y_2$ , then  $y_1^2 = v_1$  and  $y_2^2 = v_2$ , except if  $D = 1785$  or  $D = 16 \cdot 1785$ , in which case  $y_1^2 = v_1$  and  $y_2^2 = v_4$ .*

*If only one solution in positive integers  $(x, y)$  exists to equation (1.3), then  $y^2 = v_m$  where  $v_1 = mv^2$  for  $m$  a squarefree integer with either  $m = 1$  or  $m$  prime.*

This result provides an efficient algorithm for solving (1.1) in case  $n = 2$ . The computational difficulty, should one arise, lies in the calculation of the fundamental unit of  $\mathbb{Q}(\sqrt{D})$  and in factoring  $v_1$ . As we have nothing of consequence to add to this situation, we will restrict our attention to (1.1) with  $n \geq 3$ . We begin by sharpening Theorem 1.2:

---

<sup>1</sup>It will be evident later in this section what is meant here.

**Theorem 1.4.** *If  $n$  and  $D$  are fixed positive integers with  $n \geq 3$  and  $D$  nonsquare, then (1.1) has at most two solutions in positive integers  $x$  and  $y$ . If there are two solutions  $(x_1, y_1)$  and  $(x_2, y_2)$  with  $y_2 > y_1$ , then, if  $u_1$  and  $v_1$  are the smallest positive integers with  $u_1^2 - Dv_1^2 = 1$ , we have*

$$(x_1, y_1^n) = (u_1, v_1) \quad \text{and} \quad (x_2, y_2^n) = (2u_1^2 - 1, 2u_1v_1).$$

Our main interest in this paper, however, is when  $n \geq 2$  is also treated as a variable. Earlier work in the special case when  $D = 2$  is due to Pethő [19] (see also Cohn [9]):

**Theorem 1.5** (Pethő [19], Cohn [9]). *The Diophantine equation*

$$x^2 - 2y^{2n} = \pm 1$$

*has only the solutions  $(x, y, n) = (1, 1, n)$  and  $(239, 13, 2)$  in positive integers  $x, y$  and  $n \geq 2$ .*

We prove the following result, which provides an explicit bound upon (prime) exponents of Pell powers, for arbitrary  $D$ :

**Theorem 1.6.** *Let  $D$  be a positive nonsquare integer and write  $R$  for the radical of  $D$ , i.e.*

$$R = \prod_{p|D} p.$$

*If there exist positive integers  $x$  and  $y$  with  $y > 1$  and prime  $n$ , satisfying (1.1), then either*

$$D = 2^{2n-2}a^{2n} - 1 \quad \text{and} \quad y = 2a,$$

*for some integer  $a$ , or*

$$n < (2eR)^{2R^3}.$$

We note that the upper bound for  $n$  in Theorem 1.6 is, for a given  $D$ , typically inferior to comparable results in the literature based upon lower bounds for linear forms in logarithms of algebraic numbers. To be precise, if we apply a theorem of Mignotte [16], after reducing the problem to consideration of suitable Thue equations (see Section 2 of this paper), we obtain an upper bound for  $n$  in (1.1) of order  $\log D$ . Similarly, a general result for powers in recurrence sequences due to Pethő [20] yields a bound for  $n$  in terms of the fundamental unit in  $\mathbb{Q}(\sqrt{D})$ . What is (debatably!) interesting about our result, then, is that our bound on  $n$  depends solely on  $R$ , the radical of  $D$  (see also Theorem 1 of [27]), and that our proof does not use linear forms in logarithms, but rather relies upon results from the theory of Frey curves and modular forms. Further, as we shall observe in Sections 6 and 7, for many values of  $D$ , we are able to deduce much sharper estimates for  $n$ .

Combining Theorems 1.4 and 1.6, we have

**Corollary 1.7.** *Let  $D$  be a positive nonsquare integer. Then the number of solutions to (1.1) in positive integers  $x, y$  and  $n$  with  $y, n \geq 2$  is bounded effectively solely in terms of  $R$ , the radical of  $D$ .*

It is unclear whether this dependence upon the radical of  $D$  is intrinsic or merely an artifice of our method. It may be that the number of powers in a Pell sequence is absolutely bounded, independent of  $D$ .

This paper is organized as follows. In Section 2, we translate the problem to consideration of binomial Thue inequalities and state a basic bound for the number

of solutions to such equations. In Section 3, we derive a precise and explicit result for solutions to equations of the shape

$$2^{2t}a^{2n} - Db^{2n} = 1,$$

sharpening and generalizing Af Ekenstam [11], Ljunggren [14] and Tartakowsky [25]. Our Proposition 3.2 strengthens the main result of Cao [8]. Section 4 is devoted to the proof of Theorem 1.4. In Section 5, we turn our attention to Frey curves and related Galois representations, corresponding to solutions of (1.1). These techniques enable us to prove Theorem 1.6. Section 6 contains some corollaries of these results which permit an easy solution of (1.1) for many values of  $D$ . Finally, in Section 7, we apply our method to completely solve (1.1) for all  $D \leq 100$ .

## 2. THE DIOPHANTINE INEQUALITY $|Aa^n - Bb^n| \leq 2$

If we rewrite equation (1.1) as

$$(x-1)(x+1) = Dy^{2n},$$

then we immediately obtain solutions to a Diophantine inequality of the form

$$(2.1) \quad |Aa^n - Bb^n| \leq 2,$$

for suitable positive integers  $A$  and  $B$ . An easy consequence of classical work of Thue [26] and Siegel [22], in conjunction with lower bounds for linear forms in two logarithms, is that the more general inequality

$$|Aa^n - Bb^n| \leq C,$$

where  $A, B$  and  $C$  are fixed nonzero integers and  $n \geq 3$ , has at most one solution in positive integers  $a$  and  $b$ , except for finitely many exceptional triples  $(A, B, n)$ . This set of exceptions is effectively computable and has cardinality depending only upon  $C$ . Unfortunately, current estimates make it very difficult to explicitly find these exceptional triples, given  $C$ . In the case of interest  $C = 2$ , however, this is a recent theorem of the author's, shamelessly reproduced here:

**Theorem 2.1** ([3]). *If  $A, B$  and  $n$  are integers with  $AB \neq 0$  and  $n \geq 3$ , then inequality (2.1) has at most one solution in positive integers  $(a, b)$ .*

The proof of this theorem follows similar lines to that of the analogous statement in [1], with the additional twist that equations of the shape  $a^n - 3b^n = 2$  are handled via the theory of Frey curves and modular forms.

## 3. THE DIOPHANTINE EQUATION $|Aa^n - Bb^n| = 1$

The main result of the preceding section provides precise information on the number of solutions in integers to the given Diophantine inequality, without answering the question of where such a solution should occur, if one does indeed exist. In the case where  $n$  is even, with certain restrictions upon  $A$  and  $B$ , we can in fact be rather more concrete:

**Theorem 3.1.** *Let  $t, n$  and  $D$  be integers with  $n \geq 2$ ,  $D$  positive and nonsquare, and  $(t, n, D) \neq (0, 2, 7140)$ . If there exist positive integers  $a$  and  $b$  such that*

$$(3.1) \quad 2^{2t}a^{2n} - Db^{2n} = 1,$$

*then*

$$u_1 = 2^t a^n \quad \text{and} \quad v_1 = b^n,$$

where  $u_1$  and  $v_1$  are the smallest positive integers such that  $u_1^2 - Dv_1^2 = 1$ . If  $(t, n, D) = (0, 2, 7140)$ , then (3.1) has precisely one solution in positive integers, corresponding to

$$u_2 = 239^2 \quad \text{and} \quad v_2 = 26^2.$$

In case  $t = 0$ , this is an extension of a result of Tartakowsky [25] (actually, he only provides a proof of a weaker version of this in case  $n = 2$ ; full details for larger  $n$  are available in the thesis of Af Ekenstam [11]). If  $t = n - 1$ , this is noted without proof by Ljunggren (as Theorem II of [14]).

*Proof.* If  $n = 2$  and  $t = 0$ , then, via Tartakowsky [25], we may assume that  $a^2 = u_i$  and  $b^2 = v_i$ , for  $i = 1$  or  $i = 2$ . In the latter case, it follows that  $a^2 = 2u_1^2 - 1$  and  $b^2 = 2u_1v_1$ . The second of these equations implies the existence of integers  $m$  and  $n$  for which either  $u_1 = 2m^2, v_1 = n^2$  or  $u_1 = m^2, v_1 = 2n^2$ . The first of these, together with  $a^2 = 2u_1^2 - 1$  is a contradiction modulo 4. The second implies the equation  $a^2 - 2m^4 = -1$ . A result of Ljunggren [13] thus leads to the conclusion that  $(a, m) = (1, 1)$  or  $(239, 13)$ . Since  $u_1 > 1$ , we are necessarily in the second case, whence

$$4Dn^4 = 169^2 - 1 = 2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 17.$$

It follows that  $n = 1, v_1 = 2$  and  $D = 7140$ , as claimed. If, however,  $n = 2$  and  $t = 1$ , Theorem 3.1 is an immediate consequence of Corollary 1.3 of Bennett and Walsh [6].

For larger values of  $n$ , we begin with an observation. If  $\epsilon = u + v\sqrt{D}$ , where  $u$  and  $v$  are positive integers for which  $u^2 - Dv^2 = 1$ , then if  $p$  is an odd positive integer and we write

$$E_k = \frac{\epsilon^k - \epsilon^{-k}}{\epsilon - \epsilon^{-1}},$$

it is readily verified that

$$(3.2) \quad \left(E_{\frac{p+1}{2}} - E_{\frac{p-1}{2}}\right) \left(E_{\frac{p+1}{2}} + E_{\frac{p-1}{2}}\right) = E_p,$$

$$(3.3) \quad (u+1) \left(E_{\frac{p+1}{2}} - E_{\frac{p-1}{2}}\right)^2 - (u-1) \left(E_{\frac{p+1}{2}} + E_{\frac{p-1}{2}}\right)^2 = 2,$$

$$(3.4) \quad (u+1) \left(E_{\frac{p+1}{2}} - E_{\frac{p-1}{2}}\right)^2 + (u-1) \left(E_{\frac{p+1}{2}} + E_{\frac{p-1}{2}}\right)^2 = \epsilon^p + \epsilon^{-p}.$$

Supposing that there exist positive integers  $a$  and  $b$  with  $2^{2t}a^{2n} - Db^{2n} = 1$ , we thus have, for  $u_1$  and  $v_1$  as in (1.2),

$$(3.5) \quad 2^t a^n + b^n \sqrt{D} = (u_1 + v_1 \sqrt{D})^m$$

for some positive integer  $m$ . Let us assume first that there exists an odd prime  $p$  dividing  $m$ . Define

$$\epsilon = a_1 + b_1 \sqrt{D} = (u_1 + v_1 \sqrt{D})^{m/p}.$$

Then

$$(3.6) \quad 2^t a^n + b^n \sqrt{D} = (a_1 + b_1 \sqrt{D})^p.$$

Expanding via the binomial theorem and equating coefficients, we have that

$$2^t a^n = a_1 \cdot a_2, \quad b^n = b_1 \cdot b_2,$$

where  $a_2$  and  $b_2$  are odd integers with

$$\gcd(a_1, a_2), \gcd(b_1, b_2) \in \{1, p\}$$

and neither  $a_2$  nor  $b_2$  divisible by  $p^2$ . Further, if  $p \mid a_1$ , then  $p^2 \nmid a_2$  and similarly for  $b_1, b_2$ . It follows that either  $b_1 = s^n$  or

$$(3.7) \quad a_1 = 2^t r^n \quad \text{and} \quad b_1 = p^{n-1} s^n,$$

for  $r$  and  $s$  positive integers. In the first of these cases,  $E_p = (b/s)^n$  and so, from (3.2) and since the two factors on the left-hand side of (3.2) are coprime,

$$E_{\frac{p+1}{2}} - E_{\frac{p-1}{2}} = P^n \quad \text{and} \quad E_{\frac{p+1}{2}} + E_{\frac{p-1}{2}} = Q^n,$$

for some positive integers  $P$  and  $Q$ . Equation (3.3) thus yields

$$(a_1 + 1)P^{2n} - (a_1 - 1)Q^{2n} = 2$$

and so, via Theorem 2.1,  $P = Q = 1$ , contradicting  $p > 1$ . In case (3.7), we have  $E_p = py_0^n$  for some positive integer  $y_0$  and so (3.2) implies that

$$E_{\frac{p+1}{2}} \pm E_{\frac{p-1}{2}} = pP^n \quad \text{and} \quad E_{\frac{p+1}{2}} \mp E_{\frac{p-1}{2}} = Q^n,$$

for  $P$  and  $Q$  positive integers. Applying (3.3) and (3.4), we thus have either

$$(a_1 + 1)p^2 P^{2n} - (a_1 - 1)Q^{2n} = 2, \quad (a_1 + 1)p^2 P^{2n} + (a_1 - 1)Q^{2n} = 2^{t+1}a^n$$

or

$$(a_1 + 1)Q^{2n} - (a_1 - 1)p^2 P^{2n} = 2, \quad (a_1 + 1)Q^{2n} + (a_1 - 1)p^2 P^{2n} = 2^{t+1}a^n.$$

It follows that

$$2(a_1 \pm 1)Q^{2n} \mp 2 = 2^{t+1}a^n$$

and so, since  $a_1 = 2^t r^n$ ,

$$|(2^t r^n \pm 1)Q^{2n} - 2^t a^n| = 1.$$

Applying Theorem 2.1, we have  $Q = 1$ ,  $a = r$ , again a contradiction.

We are thus left to treat (3.5) with  $m = 2^\alpha$  for  $\alpha$  a nonnegative integer. The desired result will follow directly, if we can show that  $\alpha = 0$ . If  $\alpha > 0$ , then  $m$  and hence  $b$  are necessarily even, whereby  $t = 0$ . To derive a contradiction, we will appeal to the following

**Proposition 3.2.** *If  $D$  is a positive nonsquare integer and  $n \geq 3$ , then the equation  $x^n = u_{2k}$ , where  $x$  and  $k$  are positive integers, implies that*

$$D = 6083, \quad n = 3, \quad k = 1, \quad x = 23.$$

*Proof of Proposition 3.2.* If we have  $x^n = u_{2k} = 2u_k^2 - 1$ , then it follows from Proposition 8.1 of [4] and the fact that  $u_1 > 1$ , that  $u_k = 78$ . Since  $Dv_k^2 = u_k^2 - 1$  for a positive integer  $v_k$ , we thus have  $D = 6083$ ,  $n = 3$ ,  $k = 1$  and  $x = 23$ , as claimed.  $\square$

It follows, then, that  $\alpha = 1$ ,  $m = 2$ ,  $D = 6083$  and  $n = 3$ . Since 156 is not a cube, this contradicts (3.5), completing the proof of Theorem 3.1.  $\square$

## 4. SHARPENING LJUNGGREN

We will now proceed with the proof of Theorem 1.4. If we have a solution in positive integers  $(x, y)$  to (1.1), we may write

$$(4.1) \quad x + y^n \sqrt{D} = u_k + v_k \sqrt{D} = \left( u_1 + v_1 \sqrt{D} \right)^k$$

for  $k \in \mathbb{N}$ . We begin by showing that, given  $n$  and  $D$ , there is at most a single odd value of  $k$  for which (4.1) holds. Suppose the contrary, i.e. that there exist positive integers  $x_i, y_i$  and  $k_i$  with

$$(4.2) \quad x_i + y_i^n \sqrt{D} = \left( u_1 + v_1 \sqrt{D} \right)^{k_i}, \quad i \in \{1, 2\},$$

and  $k_1 < k_2$  odd. We may further suppose that  $k_1$  is the smallest odd positive integer such that a relation of the form (4.1) holds with  $k = k_1$ . Then, a standard argument (see e.g. Ljunggren [14]) implies that  $k_1$  divides  $k_2$ . Writing  $k_2 = pk_1$ , where  $p$  is an odd integer, and setting  $\epsilon = u_{k_1} + v_{k_1} \sqrt{D}$ , we thus have

$$E_p = (y_2/y_1)^n.$$

It follows from (3.2) that there exist positive integers  $a$  and  $b$  with

$$E_{(p+1)/2} + E_{(p-1)/2} = b^n \quad \text{and} \quad E_{(p+1)/2} - E_{(p-1)/2} = a^n,$$

whereby, from (3.3),

$$(x_1 + 1)a^{2n} - (x_1 - 1)b^{2n} = 2.$$

Applying Theorem 2.1, we conclude that  $a = b = 1$  and so  $p = 1$ , contradicting  $k_2 > k_1$ .

Next, let us consider solutions to (4.1) in even integers  $k$ . We have the following, completing the proof of Theorem 1.4. Note that much of our argument is essentially available in Ljunggren [14].

**Proposition 4.1.** *If  $D$  is a positive nonsquare integer and  $n \geq 3$ , then the equation  $y^n = v_{2j}$ , where  $y$  and  $j$  are positive integers, implies that  $j = 1$ .*

*Proof of Proposition 4.1.* If  $y^n = v_{2j}$  for a positive integer  $j$ , then

$$y^n = 2u_j v_j,$$

whereby there exist positive integers  $a$  and  $b$  such that either

$$u_j = 2^{n-1}a^n, \quad v_j = b^n$$

or

$$u_j = a^n, \quad v_j = 2^{n-1}b^n.$$

In the first case, we have

$$2^{2n-2}a^{2n} - Db^{2n} = 1,$$

while, in the second,

$$a^{2n} - 2^{2n-2}Db^{2n} = 1.$$

Applying Theorem 3.1 immediately implies Proposition 4.1 in the first case. In the second, we have that

$$a^n = u_1^+ \quad \text{and} \quad b^n = v_1^+,$$

for  $u_1^+$  and  $v_1^+$  the smallest positive integers satisfying

$$(u_1^+)^2 - 2^{2n-2}D(v_1^+)^2 = 1.$$

Since

$$u_1^+ + v_1^+ 2^{n-1} \sqrt{D} = (u_1 + v_1 \sqrt{D})^{2^s}$$

for some nonzero integer  $s$ , it follows that either  $s = 0$  (completing the proof of Proposition 4.1) or  $s \geq 1$ . In the latter case,  $j$  must be even and hence there exists a positive integer  $m$  with

$$y^n = v_{4m} = 4u_m v_m (2u_m^2 - 1).$$

It follows that

$$(4.3) \quad 4u_m(2u_m^2 - 1) = A^n$$

for some  $A \in \mathbb{N}$  and hence  $2u_m^2 - 1 = B^n$  for an integer  $B > 1$ . Once again applying Proposition 8.1 of [4],  $u_m = 78$ . Since 312 is not a perfect  $n$ th power for any  $n > 1$ , this contradicts (4.3).  $\square$

## 5. FROM PELL POWERS TO GALOIS REPRESENTATIONS

We now proceed with the main preoccupation of this paper – to find, given  $D$  alone, all powers in the associated Pell sequence; i.e., integers  $x, y$  and  $n \geq 2$  satisfying (1.1). While we have previously appealed to results from the theory of Galois representations and modular forms implicitly (e.g. in the application of Theorem 2.1), here we will do so in an explicit manner.

If we view a solution to (1.1) as a special case of the ternary equation

$$(5.1) \quad x^2 - Dy^{2n} = z^n$$

with  $z = 1$ , then the techniques of [4] (building upon those of [10]) allow us to treat such equations for certain  $D$  and suitably large prime  $n$ . In general, we cannot expect to solve (5.1) for arbitrary  $D$ , without additional arithmetic information. In the context of Pell powers, this is provided by classical work of Størmer [24] on primitive divisors of recurrence sequences.

Let us suppose that we have  $x^2 - Dy^{2n} = 1$  with, say,  $n \geq 7$  prime, and  $x, y$  integers with  $y > 1$ . Note that if  $D$  is even and not divisible by 8, then  $y$  is necessarily even. It follows that we are, without loss of generality, in one of the following situations:

- (i)  $D$  and  $y$  are odd;
- (ii)  $\nu_2(D) \in \{3, 4, 5\}$  and  $y$  is odd;
- (iii) either  $\nu_2(D) \geq 6$  or  $y$  is even, and  $x \equiv 1 \pmod{4}$ .

Here (and subsequently), we denote by  $\nu_p(x)$  the largest nonnegative integer  $k$  such that  $p^k$  divides an integer  $x$ .

As in [4], we consider the (Frey) elliptic curves

$$(5.2) \quad Y^2 = X^3 + 2xX^2 + Dy^{2n}X,$$

$$(5.3) \quad Y^2 = X^3 + xX^2 + \frac{Dy^{2n}}{4}X$$

and

$$(5.4) \quad Y^2 + XY = X^3 + \frac{(x-1)}{4}X^2 + \frac{Dy^{2n}}{64}X,$$

in cases (i), (ii) and (iii), respectively. For  $E$  one of these curves, we associate a Galois representation

$$\rho_n^E : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{F}_n)$$

on the  $n$ -torsion points  $E[n]$  of  $E$ . Via Lemma 3.3 of [4], this representation arises from a weight 2 cuspidal newform

$$f = f_E = \sum_{n=1}^{\infty} c_n q^n$$

of trivial character. The level  $N = N_f$  of this form is (see Lemmata 2.1 and 3.3 of [4]) one of  $R^*$ ,  $2R^*$ ,  $8R^*$  or  $32R^*$ , where

$$R^* = \begin{cases} R & \text{if } R \text{ is odd,} \\ R/2 & \text{if } R \text{ is even.} \end{cases}$$

Define, for a given nonsquare positive integer  $D$ , positive integers  $D_1$  and  $R$  by

$$D_1 = \prod_{p|D} p^{\delta_p} \quad \text{and} \quad R = \text{Rad}(D) = \prod_{p|D} p,$$

where

$$\delta_p = \begin{cases} 1 & \text{if } \nu_p(D) \text{ is odd,} \\ 2 & \text{if } \nu_p(D) \text{ is positive and even.} \end{cases}$$

In this way,  $D_1$  differs from  $D$  by a square factor. We note that  $D_1 < R^2$ . Now, let  $\epsilon_1$  be a unit in  $\mathbb{Q}(\sqrt{D_1})$ , corresponding to the minimal solution to the equation

$$(5.5) \quad u^2 - D_1 v^2 = 1$$

(i.e.  $\epsilon_1 = u_1^* + v_1^* \sqrt{D_1}$  where  $u_1^*$  and  $v_1^*$  are the smallest positive integers satisfying (5.5)). As usual, we will define  $u_k^*$  and  $v_k^*$  by

$$u_k^* + v_k^* \sqrt{D_1} = \left( u_1^* + v_1^* \sqrt{D_1} \right)^k.$$

We consider two cases separately. Either there exists a prime  $p$  with  $p \mid v_1^*$  and  $p$  coprime to  $2D_1$ , or there is no such prime. In the first case, from standard bounds on fundamental units in real quadratic fields (say due to Hua [12]), we have

$$(5.6) \quad p < \frac{\epsilon_1}{2} < \frac{1}{2} (4e^2 D_1)^{\sqrt{D_1}} < \frac{1}{2} (2eR)^{2R}.$$

Since  $p$  divides  $v_1^*$  and is coprime to  $2D_1$  (and hence to  $2D$ ), it follows that  $p$  is coprime to the conductor  $N$  of the newform  $f$  corresponding to our induced Frey curve  $E$  and that  $p$  divides  $y$ . We thus have

$$\text{trace } \rho_n^E(\text{Frob}_p) = \pm(1 + p)$$

and hence, via Proposition 4.3 of [4],

$$(5.7) \quad \text{Norm}_{K_f/\mathbb{Q}}(c_p \pm (p+1)) \equiv 0 \pmod{n},$$

where  $c_p$  is the  $p$ th Fourier coefficient of  $f$ . Here,  $K_f$  is the field of definition for the Fourier coefficients of  $f$ . Since, for each embedding  $\sigma$  of  $K_f$  in  $\mathbb{R}$ , we have

$$|\sigma(c_p)| \leq 2\sqrt{p}$$

(so that, in particular, the above norm is nonzero), it follows that

$$n \leq (p+1 + 2\sqrt{p})^{[K_f:\mathbb{Q}]} = (\sqrt{p}+1)^{2[K_f:\mathbb{Q}]}.$$

Now the degree of the extension  $K_f$  over  $\mathbb{Q}$  is bounded above by  $g_0^+(N)$ , the dimension of the space of weight 2, level  $N$  cuspidal newforms  $S_2^{\text{new}}(N)$ , of trivial

character, as a  $\mathbb{C}$ -vector space. Since  $R^*$  is odd and squarefree, it follows from, e.g., work of Martin [15] that

$$g_0^+(N) \leq g_0^+(32R^*) = \phi(R^*) < R^* \leq R,$$

where  $\phi$  denotes the Euler phi-function. Combining this with (5.6), we thus have

$$n \leq (p + 1 + 2\sqrt{p})^R < (2eR)^{2R^2}.$$

Let us next suppose that  $v_1^*$  has no prime divisor, coprime to  $2D$ . Then one of the following occurs:

- (i)  $v_1^* = 1$ ;
- (ii)  $v_1^*$  is even;
- (iii)  $v_1^*$  is composed entirely of odd prime divisors of  $D$ .

We treat these cases in turn. In the first of them, we have  $D_1 = m^2 - 1$  for some integer  $m > 1$  and hence  $D = d^2(m^2 - 1)$  with  $d$  a positive integer. If  $d = 1$ , we may apply Theorem 1.4 to reach the desired conclusion. Since, by construction,  $D_1$  is cube-free (and hence  $m$  is even) and since every prime divisor of  $D$  divides  $D_1$ ,  $d$  is odd. If  $d > 1$  and  $q$  is a prime divisor of  $d$ , then  $v_q^*$  divides  $Dy^{2n}$  and so, via a classic result of Størmer [24] on primitive divisors of terms in recurrence sequences, there is an odd prime  $p$  dividing  $v_q^*$  and hence  $y$ , coprime to  $D$ . Arguing as previously, since

$$p \leq v_q^* < \frac{1}{2} \epsilon_1^q < \frac{1}{2} (2eR)^{2qR} < \frac{1}{2} (2eR)^{2R^2},$$

where the last inequality is a consequence of the fact that  $q \mid D$  (and hence  $q \leq R$ ), we have

$$n < (2eR)^{2R^3}.$$

Next suppose that  $v_1^*$  is even. If we further assume that  $n > R^{R^2}$ , then, from the upper bound for  $\epsilon_1$  in (5.6),  $\nu_2(v_1^*) < n$ . It follows that  $v_2^*$  necessarily divides  $Dy^{2n}$ , where  $D = d^2 D_1$ . Since  $v_2^* = 2u_1^* v_1^*$  and from  $(u_1^*)^2 - D_1 (v_1^*)^2 = 1$ , we have that  $u_1^*$  and hence  $y$  is divisible by a prime  $p$ , coprime to  $2D$ . We thus have

$$p < \frac{1}{2} (2eR)^{4R}$$

where, again, our corresponding Frey curve has multiplicative reduction at  $p$  (and hence congruence (5.7) is satisfied by the related modular form). Arguing as before, we obtain a bound of the shape

$$n < (2eR)^{4R^2}.$$

Finally, let us suppose that every prime divisor of  $v_1 > 1$  is an odd prime divisor of  $D$ . Let  $q$  be an odd prime dividing  $\gcd(v_1^*, D)$ . Assuming  $n > R^{R^2}$  guarantees that  $\nu_q(v_1^*) < n$  and, from

$$\nu_q(v_q^*) = \nu_q(v_1^*) + 1,$$

and properties of recurrence sequences, we have that  $y$  is divisible by every prime dividing  $v_q^*$ . By the aforementioned theorem of Størmer,  $v_m^*$  is divisible by a prime coprime to  $D_1$  for all  $m > 1$  and so there exists a prime  $p$  dividing  $v_q^*$  and  $y$ , coprime to  $2D_1$  and hence to  $N$ . We have

$$p \leq v_q^* < \frac{1}{2} (2eR)^{2qR} \leq \frac{1}{2} (2eR)^{2R^2}.$$

Arguing as previously, we conclude that

$$n \leq (p+1+2\sqrt{p})^{g_0^+(32R)} < (2eR)^{2R^3},$$

as desired. This completes the proof of Theorem 1.6.

## 6. SOME USEFUL PROPOSITIONS

Given  $D$ , actual application of the techniques of the preceding sections to completely solve (1.1) often turns out to be a routine matter. In practice, the upper bound for  $n$  in Theorem 1.6 is usually wildly pessimistic. As we shall see in this section, the situation is particularly nice if  $\gcd(v_1, 6) > 1$ . We begin with an easy corollary of Proposition 4.1:

**Proposition 6.1.** *If  $D$  is a positive nonsquare integer and  $x, y$  and  $n$  are positive integers satisfying (1.1), with  $y$  even and  $n \geq 3$ , then one of the following cases occurs:*

(i)  $v_1$  is even, whereby

$$\nu_2(v_1) \leq n \nu_2(y) \leq \nu_2(v_1) + 1.$$

If  $n \nu_2(y) = \nu_2(v_1) + 1$ , then there exist positive integers  $a$  and  $b$  such that

$$u_1 = a^n, \quad v_1 = 2^{n-1}b^n \quad \text{and} \quad y = 2ab.$$

(ii)  $v_1$  is odd, in which case there exist positive integers  $a$  and  $b$  such that

$$u_1 = 2^{n-1}a^n, \quad v_1 = b^n \quad \text{and} \quad y = 2ab.$$

*Proof.* Suppose, first, that  $v_1$  is even. The inequality  $\nu_2(v_1) \leq n \nu_2(y)$  is a trivial consequence of the fact that  $v_1$  divides  $y^n$ . If we have that  $n \nu_2(y) \geq \nu_2(v_1) + 1$ , then, writing  $y^n = v_j$  for some integer  $j$ , it follows that  $j$  is even and hence, from Proposition 4.1, equal to 2. This implies that  $2u_1v_1 = y^n$  whence  $n \nu_2(y) = \nu_2(v_1) + 1$  and the rest of part (i) of our claim follows immediately.

Next, suppose that  $v_1$  is odd while  $y$  is even. Then  $y^n = v_{2k}$  for  $k$  a positive integer whereby, again from Proposition 4.1,  $k = 1$ . The stated equalities for  $u_1$  and  $v_1$  thus follow from  $y^n = 2u_1v_1$  and the fact that  $v_1$  is odd.  $\square$

Analogous to Proposition 4.1, in case we are interested in solutions to (1.1) with  $y^n = v_j$  for  $j$  divisible by 3 rather than 2, is the following:

**Proposition 6.2.** *If  $D$  is a positive nonsquare integer and  $n \geq 3$ , then the equation  $y^n = v_{3k}$  has no solutions in positive integers  $y$  and  $k$ .*

*Proof.* Suppose that we have

$$y^n = v_{3k} = v_k(4u_k^2 - 1).$$

Since

$$\gcd(v_k, 4u_k^2 - 1) = \begin{cases} 3 & \text{if } 3 \mid v_k, \\ 1 & \text{otherwise,} \end{cases}$$

it follows that  $4u_k^2 - 1 = 3^\delta a^n$  for some integer  $a$ , where  $\delta \in \{0, 1\}$ . If  $\delta = 0$ , we have that both  $2u_k + 1$  and  $2u_k - 1$  are perfect  $n$ th powers, an immediate contradiction. If, however,  $\delta = 1$ , the equality  $(2u_k - 1)(2u_k + 1) = 3a^n$  implies the existence of positive integers  $b$  and  $c$  for which  $b^n - 3c^n = \pm 2$ . Theorem 2.1 yields  $b = c = 1$  and so  $u_k = 1$ , contradicting  $u_k^2 - Dv_k^2 = 1$  with  $D$  and  $v_k$  positive.  $\square$

From this result, we quickly obtain

**Proposition 6.3.** *If  $D$  is a positive nonsquare integer and  $x, y$  and  $n \geq 3$  are positive integers satisfying (1.1), with  $3 \mid y$ , then one of the following two cases occurs:*

- (i)  $3 \mid v_1$ , whence  $n\nu_3(y) = \nu_3(v_1)$ .
- (ii)  $3 \mid u_1$  and  $y$  is even (whereby the conclusions of Proposition 6.1 obtain).

*Proof.* If we have  $x^2 - Dy^{2n} = 1$  with  $n \geq \max\{\nu_3(v_1) + 1, 3\}$ , where  $3 \mid v_1$ , it follows that  $y^n = v_j$  with  $3^n$  dividing  $v_j$ . We thus have  $j = 3k$  for some integer  $k$ , whereby the result is immediate from Proposition 6.2. If 3 divides  $y$ , but not  $v_1$ , then  $y^n = v_k$  where  $k$  is even (if  $3 \mid u_1$ ) or divisible by 3 (if 3 fails to divide  $u_1$ ). In the first case, it follows that  $y$  is even. In the second, as before, we obtain a contradiction via Proposition 6.2.  $\square$

Notice, from  $u_1^2 - Dv_1^2 = 1$ , that  $v_1$  is necessarily even for all

$$D \equiv 1, 2, 4, 5, 6 \pmod{8},$$

while  $v_1$  is guaranteed to be divisible by 3 if  $D \equiv 1 \pmod{3}$ . We may thus apply at least one of Proposition 6.1 or 6.3 for at least 3/4 of all values of  $D$ . In these situations, complete determination of solutions to (1.1) is usually a trivial matter.

## 7. COMPUTATIONS

We now attempt to demonstrate that the techniques of the previous sections provide a practical method for determining all Pell powers in a given sequence. Specifically, we will prove the following

**Theorem 7.1.** *If  $1 \leq D \leq 100$ , then the only solutions to (1.1) in positive integers  $x, y$  and  $n$  with  $y, n \geq 2$  are with  $(x, y, n, D)$  in the following list:*

$$\begin{aligned} &(7, 2, 2, 3), (9, 2, 2, 5), (15, 2, 2, 14), (31, 2, 3, 15), (33, 2, 3, 17), \\ &(17, 2, 2, 18), (161, 6, 2, 20), (23, 2, 2, 33), (25, 2, 2, 39), (31, 2, 2, 60), \\ &(63, 2, 3, 62), (127, 2, 4, 63), (127, 4, 2, 63), (129, 2, 4, 65), (129, 4, 2, 65), \\ &(65, 2, 3, 66), (33, 2, 2, 68), (80, 3, 2, 79), (82, 3, 2, 83), (39, 2, 2, 95). \end{aligned}$$

*Proof.* We begin by tabulating the values of  $v_1$  for  $D < 100$  in Table 1. First consider the case  $n = 2$ . In this situation, we may appeal to Theorem 1.3; a number of elementary results are also applicable, at least for many  $D$  (see, for example, Theorem 8, Chapter 28 of Mordell [17]). From the above table, we encounter solutions with  $v_1 > 1$  square for

$$D \in \{5, 14, 18, 33, 39, 60, 65, 68, 79, 83, 95\}.$$

The only such solutions for which  $y^2 \neq v_1$  are with  $D = 3, 20$  and  $63$ . In each case, we have  $y^2 = v_2$ .

Let us now turn our attention to (1.1) with  $n \geq 3$  prime. In these cases, we will rely heavily upon Propositions 6.1 and 6.3. Applying the second of these for those  $D$  with  $3 \mid v_1$ , we obtain immediate contradictions unless  $27 \mid v_1$  (i.e. unless  $D \in \{67, 85\}$ , whence  $\nu_3(v_1) = 3$  and  $n = 3$ ). If  $(D, n) = (67, 3)$  and  $y$  is even, then part (ii) of Proposition 6.1 provides a contradiction. If, however,  $y$  is odd, the relation  $x^2 - 67y^6 = 1$  implies the existence of positive integers  $a$  and  $b$  for which

$$a^6 - 67b^6 = \pm 2,$$

TABLE 1.

| D  | $v_1$ | D  | $v_1$ | D  | $v_1$     | D  | $v_1$  | D  | $v_1$   |
|----|-------|----|-------|----|-----------|----|--------|----|---------|
| 2  | 2     | 23 | 5     | 43 | 531       | 62 | 8      | 82 | 18      |
| 3  | 1     | 24 | 1     | 44 | 30        | 63 | 1      | 83 | 9       |
| 5  | 4     | 26 | 10    | 45 | 24        | 65 | 16     | 84 | 6       |
| 6  | 2     | 27 | 5     | 46 | 3588      | 66 | 8      | 85 | 30996   |
| 7  | 3     | 28 | 24    | 47 | 7         | 67 | 5967   | 86 | 1122    |
| 8  | 1     | 29 | 1820  | 48 | 1         | 68 | 4      | 87 | 3       |
| 10 | 6     | 30 | 2     | 50 | 14        | 69 | 936    | 88 | 21      |
| 11 | 3     | 31 | 273   | 51 | 7         | 70 | 30     | 89 | 53000   |
| 12 | 2     | 32 | 3     | 52 | 90        | 71 | 413    | 90 | 2       |
| 13 | 180   | 33 | 4     | 53 | 9100      | 72 | 2      | 91 | 165     |
| 14 | 4     | 34 | 6     | 54 | 66        | 73 | 267000 | 92 | 120     |
| 15 | 1     | 35 | 1     | 55 | 12        | 74 | 430    | 93 | 1260    |
| 17 | 8     | 37 | 12    | 56 | 2         | 75 | 3      | 94 | 221064  |
| 18 | 4     | 38 | 6     | 57 | 20        | 76 | 6630   | 95 | 4       |
| 19 | 39    | 39 | 4     | 58 | 2574      | 77 | 40     | 96 | 5       |
| 20 | 2     | 40 | 3     | 59 | 69        | 78 | 6      | 97 | 6377352 |
| 21 | 12    | 41 | 320   | 60 | 4         | 79 | 9      | 98 | 10      |
| 22 | 42    | 42 | 2     | 61 | 226153980 | 80 | 1      | 99 | 1       |

a contradiction modulo 7. If, however,  $(D, n) = (85, 3)$ , then  $\nu_2(v_1) = 2$  and part (i) of Proposition 6.1 implies that 7749 is a perfect cube, again a contradiction. This completes the proof of Theorem 7.1 in case 3 divides  $v_1$ .

Next, we will treat those remaining values of  $D$  with even  $v_1$ . From Proposition 6.1, we may assume that  $\nu_2(v_1) \geq 2$ . If  $\nu_2(v_1) = 2$ , then part (i) of Proposition 6.1 implies the existence of integers  $a$  and  $b$  such that  $u_1 = a^3$  and  $v_1 = 4b^3$ , in each case a contradiction. If  $\nu_2(v_1) = 3$  (and hence  $n = 3$  and  $\nu_2(y) = 1$ ), we have

$$D \in \{17, 62, 66, 77, 89\}.$$

For the first three of these values, we have solutions to  $x^2 - Dy^6 = 1$  with  $y^3 = v_1$ . If there are additional solutions for these  $D$ , Theorem 1.4 thus implies that the corresponding  $u_1 = 4a^3$  for some integer  $a$ , contradicting the parity of  $v_1$ . If  $D = 77$ , the equation  $x^2 - 77y^6 = 1$  with  $\nu_2(y) = 1$  implies, after factoring, the existence of odd positive integers  $a$  and  $b$  with

$$(7.1) \quad Aa^6 - Bb^6 = \pm 1,$$

where

$$(A, B) \in \{(1, 1232), (7, 176), (11, 112), (16, 77)\}.$$

Modulo 7 or 9, we can discount all equations except

$$a^6 - 1232b^6 = 1,$$

which, via Theorem 3.1, has no positive integral solutions.

The remaining  $D$  with  $v_1$  even are  $D = 65$  (for which  $\nu_2(v_1) = 4$ ) and  $D = 41$  (with  $\nu_2(v_1) = 6$ ). In the first of these cases, Proposition 6.1 implies that  $n = 5$  and that  $u_1$  is a fifth power, contradicting  $u_1 = 129$ . If  $D = 41$ , the same proposition leads to the conclusion that either  $n = 7$  and  $v_1 = 64a^7$  for some integer  $a$  (contrary to  $v_1 = 320$ ), or that  $n = 3$ ,  $\nu_2(y) = 2$ . In the latter situation, factoring the equation

$x^2 - 41y^6 = 1$  leads to a solution in positive integers  $a$  and  $b$  to an equation of the form (7.1) with

$$(A, B) \in \{(1, 2^{10} \cdot 41), (41, 2^{10})\}.$$

Modulo 9, we are left with the equation

$$a^6 - 2^{10} \cdot 41y^6 = 1,$$

again contradicting Theorem 3.1. This completes the proof of Theorem 7.1, in case  $\gcd(v_1, 6) > 1$ .

It remains, then, to consider

$$D \in \{23, 27, 47, 51, 71, 96\}.$$

Note that, for these cases, we may assume  $\gcd(y, 6) = 1$ . Otherwise, part (ii) of Proposition 6.1 and part (ii) of Proposition 6.3 together imply that  $v_1$  is an odd perfect power. We will begin with  $D \in \{27, 96\}$ . Considering the Frey curves corresponding to a solution of (1.1) with  $n \geq 7$  prime (see Section 5), we find, from the fact that  $y$  is odd, that in each case  $N = 96$ . Since  $v_1 = 5$ , we have that  $5 \mid y$  and hence

$$\text{Norm}_{K_f/\mathbb{Q}}(c_5 \pm 6) \equiv 0 \pmod{n},$$

for a weight 2, level 96 cuspidal newform with trivial character. From Stein's Modular Forms Database [23], we have  $c_5 = 2$  for all such forms, contradicting  $n \geq 7$ . We are left to deal with  $n \in \{3, 5\}$ . In these cases, if  $D = 27$ , factoring  $x^2 - 27y^{2n} = 1$  and using the fact that  $y$  is odd implies that

$$a^{2n} - 27b^{2n} = \pm 2$$

for some integers  $a$  and  $b$ , a contradiction modulo 9 and 11, for  $n = 3$  and  $n = 5$ , respectively. If  $D = 96$ , we similarly have either

$$a^{2n} - 24b^{2n} = \pm 1 \quad \text{or} \quad 3a^{2n} - 8b^{2n} = \pm 1$$

with  $a$  and  $b$  odd integers. Modulo 8, we may suppose that

$$a^{2n} - 24b^{2n} = 1$$

which, via Theorem 3.1, has no solutions with  $n \geq 2$ .

Next, we consider  $D = 23$ . From the fact that  $y$  is odd, we are led to a weight 2 cuspidal newform of level  $N = 736$ . Stein's Database thus tells us that

| $c_3$    | $c_5$                                          | $F(\theta)$                                            |
|----------|------------------------------------------------|--------------------------------------------------------|
| $\theta$ | $\pm\theta - 1$                                | $\theta^2 \pm 2\theta - 1$                             |
| $\theta$ | $\pm\theta + 1$                                | $\theta^2 - 3$                                         |
| $\theta$ | $-\theta^2 \pm 3\theta$                        | $\theta^3 \mp 4\theta^2 + \theta \pm 4$                |
| $\theta$ | $\pm\frac{1}{2}\theta^3 \mp \frac{7}{2}\theta$ | $\theta^4 \mp 2\theta^3 - 9\theta^2 \pm 12\theta + 16$ |

where  $c_3 \equiv 0, \pm 2 \pmod{\nu}$  (since 3 fails to divide  $y$ ) and  $c_5 \equiv \pm 6 \pmod{\nu}$  (since  $5 \mid y$ ), for some prime  $\nu$  above  $n$ . Here, we list Fourier coefficients  $c_p$  for  $p = 3$  and 5 for each cuspidal newform at level 736, together with minimal polynomials  $F$  such that  $F(\theta) = 0$ . Congruence (5.7) leads to a contradiction for all prime  $n \geq 7$ , except for  $n = 23$  (where  $n \mid N$ , the level of our newform). We may thus suppose that  $n \in \{3, 5, 23\}$ . The equation  $x^2 - 23y^{2n} = 1$  with  $y$  odd leads to  $a^{2n} - 23b^{2n} = \pm 2$ , with  $a$  and  $b$  odd integers. Modulo 8, we may discount the minus sign. If we consider the equation  $a^{2n} - 23b^{2n} = 2$  modulo 7, 11 and 47, we deduce a series of contradictions for  $n = 3, 5$  and 23, respectively.

If  $D = 47$ , then  $N = 1504$  and we have  $v_1 = 7$ . In each case we have  $c_3 = \theta$ , where  $F(\theta) = 0$  for one of the following polynomials:

| $F(\theta)$                                                                                                        |
|--------------------------------------------------------------------------------------------------------------------|
| $\theta^4 \pm 2\theta^3 - 3\theta^2 \mp 4\theta + 1$                                                               |
| $\theta^5 - 11\theta^3 + 23\theta \mp 12$                                                                          |
| $\theta^6 \pm 4\theta^5 - 3\theta^4 \mp 20\theta^3 + 3\theta^2 \pm 24\theta - 8$                                   |
| $\theta^8 \pm 2\theta^7 - 19\theta^6 \mp 32\theta^5 + 105\theta^4 \pm 124\theta^3 - 184\theta^2 \mp 96\theta + 64$ |

From  $c_3 \equiv 0, \pm 2 \pmod{\nu}$  and the fact that  $n \geq 7$  is prime, if  $F(\theta) = \theta^4 \pm 2\theta^3 - 3\theta^2 \mp 4\theta + 1$ , we have that  $n = 13$ . Similarly, if  $F(\theta) = \theta^5 - 11\theta^3 + 23\theta \mp 12$ ,  $n = 11$ , while in all other cases, we derive a contradiction for all prime  $n \geq 7$ . This leaves us to deal with  $n \in \{3, 5, 11, 13, 47\}$ . Here, considering the equation  $a^{2n} - 47b^{2n} = \pm 2$  modulo 8, we may discard the minus sign, whereby we obtain a contradiction modulo 13, 11, 23, 53 and 283 for  $n = 3, 5, 11, 13$  and 47, respectively.

If  $D = 51$ , then  $N = 1632$  and  $v_1 = 7$ . Here from [23], we find that  $c_7 \in \{0, \pm 2\}$  except for forms with  $c_7$  as follows (where, as previously,  $F(\theta) = 0$ ):

| $c_7$                         | $F(\theta)$                          |
|-------------------------------|--------------------------------------|
| $\pm(2\theta + 4)$            | $\theta^2 + 3\theta - 2$             |
| $\pm(\theta^2 - 3\theta - 2)$ | $\theta^3 - 3\theta^2 - 4\theta + 4$ |

Since we have, from the fact that  $v_1 = 7$  divides  $y$ ,

$$\text{Norm}_{K_f/\mathbb{Q}}(c_7 \pm 8) \equiv 0 \pmod{n},$$

we contradict  $n \geq 7$  prime in all cases except for those forms with  $F(\theta) = \theta^3 - 3\theta^2 - 4\theta + 4$ , where we have  $n = 17$  or  $n = 31$ . It remains to eliminate the possible values  $n \in \{3, 5, 7, 17, 31\}$ . Arguing as previously, we deduce the existence of integers  $a$  and  $b$ , coprime to 6, with either

$$a^{2n} - 51b^{2n} = \pm 2 \quad \text{or} \quad 3a^{2n} - 17b^{2n} = \pm 2.$$

Modulo 8 and 17, we may thus suppose that

$$a^{2n} - 51b^{2n} = -2.$$

Working modulo 9, 11, 29, 103 and 311, we again arrive, in each case, at a contradiction.

Finally, let us suppose that  $D = 71$ . Then  $N = 2272$  and we have  $v_1 = 413$ . In each case we either have  $c_3 = \pm 1, \pm 3$ , or  $c_3 = \theta$  where  $F(\theta) = 0$  for  $F$  as follows:

| $F(\theta)$                                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------------------------------------------|
| $\theta^6 - 9\theta^4 \mp 2\theta^3 + 22\theta^2 \pm 6\theta - 13$                                                                                   |
| $\theta^8 \pm 4\theta^7 - 8\theta^6 \mp 40\theta^5 + 13\theta^4 \pm 112\theta^3 + 9\theta^2 \mp 56\theta + 9$                                        |
| $\theta^9 \pm 8\theta^8 + 12\theta^7 \mp 48\theta^6 - 135\theta^5 \pm 20\theta^4 + 265\theta^3 \pm 92\theta^2 - 127\theta \mp 52$                    |
| $\theta^{10} \pm 2\theta^9 - 20\theta^8 \mp 36\theta^7 + 133\theta^6 \pm 204\theta^5 - 323\theta^4 \mp 383\theta^3 + 159\theta^2 \pm 116\theta - 16$ |

In any case, the fact that  $c_3 \equiv 0, \pm 2 \pmod{\nu}$  leads, after some routine computation, to the conclusion that

$$n \in \{3, 5, 7, 13, 19, 59, 71, 397\}.$$

As before, considerations modulo 8 imply that

$$a^{2n} - 71b^{2n} = 2$$

for integers  $a$  and  $b$ , a contradiction modulo 7, 11, 29, 53, 191, 709, 569 and 2383, for  $n = 3, 5, 7, 13, 19, 59, 71$  and 397, respectively. This completes the proof of Theorem 7.1.  $\square$

#### ACKNOWLEDGMENTS

We thank the anonymous referee for numerous helpful suggestions.

#### REFERENCES

- [1] M.A. Bennett, Rational approximation to algebraic numbers of small height: the Diophantine equation  $|ax^n - by^n| = 1$ , *J. Reine Angew. Math.* 535 (2001), 1–49. MR2002d:11079
- [2] M.A. Bennett, Products of consecutive integers, *Bull. London Math. Soc.* 36 (2004), 683–694.
- [3] M.A. Bennett, The Diophantine inequality  $|ax^n - by^n| \leq 2$ , submitted for publication.
- [4] M.A. Bennett and C. Skinner, Ternary Diophantine equations via Galois representations and modular forms, *Canad. J. Math.* 56 (2004), 23–54.
- [5] M.A. Bennett, V. Vatsal and S. Yazdani, Ternary Diophantine equations of signature  $(p, p, 3)$ , *Compositio Math.*, to appear.
- [6] M.A. Bennett and P.G. Walsh, The Diophantine equation  $b^2x^4 - dy^2 = 1$ , *Proc. Amer. Math. Soc.* 127 (1999), 3481–3491. MR2000b:11025
- [7] Y. Bugeaud, M. Mignotte and S. Siksek, Classical and modular approaches to exponential Diophantine equations I: Fibonacci and Lucas perfect powers, preprint.
- [8] Z. Cao, On the Diophantine equation  $x^{2n} - Dy^2 = 1$ , *Proc. Amer. Math. Soc.* 98 (1986), no. 1, 11–16. MR87i:11035
- [9] J.H.E. Cohn, Perfect Pell powers, *Glasgow Math. J.* 38 (1996), 19–20. MR97b:11047
- [10] H. Darmon and L. Merel, Winding quotients and some variants of Fermat’s Last Theorem, *J. Reine Angew. Math.* 490 (1997), 81–100. MR98h:11076
- [11] A. Af Ekenstam, Contributions to the Theory of the Diophantine Equation  $Ax^n - By^n = C$ , Ph.D. Thesis, Uppsala, 1959.
- [12] L.K. Hua, On the least solution of Pell’s equation, *Bull. Amer. Math. Soc.* 48 (1942), 731–735. MR4:130f
- [13] W. Ljunggren, Zur Theorie der Gleichung  $x^2 + 1 = Dy^4$ , *Avh. Norske. vid. Akad.* 1, No. 5 (1942). MR8:6f
- [14] W. Ljunggren, A Diophantine equation with two unknowns, C.R. Dixième Congrès Math. Scandinaves 1946, 265–270. MR8:368i
- [15] G. Martin, Dimensions of spaces of cusp forms and newforms on  $\Gamma_0(N)$  and  $\Gamma_1(N)$ , preprint.
- [16] M. Mignotte, A note on the equation  $ax^n - by^n = c$ , *Acta Arith.* 75 (1996), 287–295. MR97c:11042
- [17] L. J. Mordell, Diophantine Equations, Academic Press, London, 1969. MR40:2600
- [18] A. Pethő, Perfect powers in second order linear recurrences, *J. Number Theory* 15 (1982), 5–13. MR84f:10024
- [19] A. Pethő, The Pell sequence contains only trivial perfect powers. Sets, graphs and numbers (Budapest, 1991), 561–568, Colloq. Math. Soc. János Bolyai, 60, North-Holland, Amsterdam, 1992. MR94e:11031
- [20] A. Pethő, Diophantine properties of linear recursive sequences. II, *Acta Math. Acad. Paedagog. Nyhzi. (N.S.)* 17 (2001), 81–96. MR2003d:11021
- [21] T. Shorey and C.L. Stewart, Pure powers in recurrence sequences and some related Diophantine equations, *J. Number Theory* 27 (1987), 324–352. MR89a:11024
- [22] C.L. Siegel, Die Gleichung  $ax^n - by^n = c$ , *Math. Ann.* 114 (1937), 57–68.
- [23] W. Stein, *The Modular Forms Database*, <http://modular.fas.harvard.edu/Tables> (2003).
- [24] C. Størmer, Quelques théorèmes sur l’équation de Pell  $x^2 - Dy^2 = \pm 1$  et leurs applications, *Christiania Videnskabs Selskabs Skrifter, Math. Nat. Kl.* 1897, No. 2, 48 pages.
- [25] W. Tartakowsky, Auflösung der Gleichung  $x^4 - py^4 = 1$ , *Bull. de l’Académie des Sciences URSS* 20 (1926), 310–324.
- [26] A. Thue, Berechnung aller Lösungen dewisser Gleichungen von der form  $ax^r - by^r = f$ , *Vidensk. Skrifter I*, No. 4, Kristiania, 1918.

- [27] J. Turk, Polynomial values and almost powers, *Michigan Math. J.* 29 (1982), 213–220. MR0654481 (83h:10040)
- [28] P.G. Walsh, An improved method for solving the family of Thue equations  $X^4 - 2rX^2Y^2 - sY^4 = 1$ , *Number theory for the millenium* (Urbana, IL, 2000), 375–383, A.K. Peters, Natick, MA, 2002. MR2003k:11052

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRITISH COLUMBIA, VANCOUVER, BRITISH COLUMBIA, CANADA V6T 1Z2

*E-mail address:* `bennett@math.ubc.ca`