The product of like-indexed terms in binary recurrences

F. Luca and P.G. Walsh

November 29, 2006

Abstract

In recent work by Hajdu and Szalay, Diophantine equations of the form $(a^k-1)(b^k-1)=x^2$ were completely solved for a few pairs (a,b). In this paper, a general finiteness theorem for equations of the form $u_kv_k=x^n$ is proved, where u_k and v_k are terms in certain types of binary recurrence sequences. Also, a unified computational approach for solving equations of the type $(a^k-1)(b^k-1)=x^2$ is described, and this approach is used to completely solve such equations for almost all (a,b) in the range $1<a<b\leq 100$. In the final section of this paper, it is shown that the *abc* conjecture implies much stronger results on these types of Diophantine problems.

2000 Mathematics Subject Classification: 11D41,11B39

1 Introduction

There is a wealth of literature pertaining to the study of the arithmetical properties of terms in binary linear recurrences. In this paper we attempt to consider the question of comparative results among pairs of such sequences. This type of question was raised in recent work of Szalay [15], and Hajdu and Szalay [7], wherein Diophantine equations such as

$$(a^k-1)(b^k-1)=x^2,$$

for fixed integers (a,b), were completely solved. In particular, all solutions (k,x) were determined for the particular values $(a,b)\in\{(2,3),(2,5),(2,6)\}$. Although the methods in these papers are relatively elementary, the results lead one to believe that there is a general theory lurking, as the arithmetic nature of terms in distinct sequences seem to behave in somewhat of an independent manner.

It is the purpose of this paper to prove some general finiteness theorems along these lines, and also to exhibit specific procedures for solving equations exactly of the type described above. Moreover, we hope to raise several outstanding questions in such a way as to motivate further research on these problems.

The paper is divided into three parts. In the first part of this paper, we prove a general finiteness theorem for the product of like-indexed terms in two binary recurrences to be the n-th power of an integer. In the second part of the paper, we describe a method to completely solve Diophantine equations of the form $(a^k-1)(b^k-1)=x^2$. We conclude with some discussion on open problems, and connections of this topic to the *abc* conjecture.

2 A Finiteness Theorem

Let $a_1, b_1, c_1, d_1, a_2, b_2, c_2, d_2$ denote non-zero integers. Define two sequences $\{u_k\}$ and $\{v_k\}$ by

$$u_k = c_1 a_1^k + d_1 b_1^k, \quad v_k = c_2 a_2^k + d_2 b_2^k.$$

To avoid degenerate cases, we assume that $|a_i| > |b_i|$ for $i = 1$ and 2.

Theorem 2.1 *Let $n > 1$ denote a positive integer, and let e denote an n-th power free integer. Let a_i, b_i, c_i, d_i denote non-zero integers for $i = 1, 2$. If $n > 2$, then the equation*

$$u_k v_k = e x^n \tag{2.1}$$

has only finitely many positive integer solutions (k, x). If $n = 2$, then (2.1) has only finitely many positive integer solutions (k, x), except in one of the following two cases:

1. $a_2 b_1 = a_1 b_2$ *and* $c_2 d_1 = c_1 d_2$.
2. $a_2 b_1 = -a_1 b_2$ *and* $c_2 d_1 = \pm c_1 d_2$.

An immediate consequence of Theorem 2.1 is the following special case, which provided the motivation for much of this work.

Corollary 2.1 *Let $a > 1$ and $b > 1$ denote distinct integers, and let $n > 1$ be an integer. Then the equation*

$$(a^k - 1)(b^k - 1) = x^n$$

has finitely many solutions in integers (k, x).

The proof of Theorem 2.1 uses an ineffective result of Corvaja and Zannier [5] concerning polynomial values in linearly recurrence sequences with positive integer roots. We remark that this result is based on the subspace theorem, thereby rendering our result ineffective. We begin by recalling the notation and the result from [5] which is relevant for our purposes.

Let $\mathcal{A}$ be the set of all functions $f : \mathbf{N} \to \mathbf{Q}$ such that either $f = 0$ identically, or there exist $r \geq 1$ distinct positive integers $\alpha_1 > \alpha_2 \ldots > \alpha_r > 0$, and non-zero rational numbers $\beta_1, \beta_2, \ldots, \beta_r$, such that

$$f(n) = \sum_{i=1}^{r} \beta_i \alpha_i^n, \tag{2.2}$$

for all positive integers n. For a given non-zero $f \in \mathcal{A}$ of the form (2.2), r is the *rank* of f, and we denote it by rank(f). The integers α_i $(i = 1, 2, \ldots, r)$ are the *roots* of f. The rational numbers β_i $(i = 1, 2, \ldots, r)$ are the *coefficients* of f.

For a non-zero $f \in \mathcal{A}$ its rank, roots and coefficients are uniquely determined. Also, $\mathcal{A}$ is a subring of the ring of all the rational valued functions defined on $\mathbf{N}$. $\mathcal{A}$ consists of all sequences of rational numbers which satisfy some linear recurrence with integer coefficients, and whose characteristic polynomial has distinct roots which are positive integers. We shall make use of the following result from [5] (Corollary 1, page 320).

Lemma 2.1 *Let f be a non-zero element in $\mathcal{A}$ and let $n \geq 2$ be a fixed integer. If there exists a rational number e such that the diophantine equation*

$$f(k) = ex^n$$

has infinitely many integer solutions (k, x) with $k > 0$, then there exists $j \in \{0, 1, \ldots, n-1\}$, and an element $h \in \mathcal{A}$, such that if one denotes by g the element of $\mathcal{A}$ given by

$$g(k) := f(kn + j), \quad (k \in \mathbf{N}) \tag{2.2}$$

then $g = eh^n$.

We proceed with the proof of Theorem 2.1. Let $\{u_k\}$ and $\{v_k\}$ be the sequences in question, and assume that (2.1) has infinitely many solutions (k, x). We first reduce to the case that the integers a_1, a_2, b_1, b_2 are all positive. To see that this can be done, consider the subsequences

$$u_{2k} = c_1(a_1^2)^k + d_1(b_1^2)^k, \quad v_{2k} = c_2(a_2^2)^k + d_2(b_2^2)^k,$$

and

$$u_{2k+1} = c_1a_1(a_1^2)^k + d_1b_1(b_1^2)^k, \quad v_{2k+1} = c_2a_2(a_2^2)^k + d_2b_2(b_2^2)^k.$$

If (2.1) has infinitely many solutions, then infinitely many solutions must exist within one of these two subsequences. The roots (a_i^2, b_i^2) of these subsequences are clearly positive.

We now reduce to the case that $(a_1, b_1) = (a_2, b_2) = 1$. Let $D_1 = (a_1, b_1)$, $D_2 = (a_2, b_2)$, and consider the sequences

$$u'_k = c_1\left(\frac{a_1}{D_1}\right)^k + d_1\left(\frac{b_1}{D_1}\right)^k, v'_k = c_2\left(\frac{a_2}{D_2}\right)^k + d_2\left(\frac{b_2}{D_2}\right)^k.$$

Then (2.1) is equivalent to the equation

$$(D_1D_2)^k u'_k v'_k = ex^n.$$

Let j denote a congruence class (mod n) for which there are infinitely many solutions (k, x) to (2.1) with $k \equiv j \pmod{n}$. Define $D = (e, (D_1D_2)^j)$, $e_1 = e/D$, $f = (D_1D_2)^j/D$, and l to be the minimal positive integer such that $l^n = ff_1$ for some positive integer f_1. It follows that e_1f_1 is n-th power free, and that there are infinitely many solutions to the equation

$$u'_k v'_k = (e_1f_1)x^n.$$

We can therefore replace $\{u_k\}, \{v_k\}$ if necessary by $\{u'_k\}, \{v'_k\}$, and henceforth assume that $(a_1, b_1) = (a_2, b_2) = 1$. A similar argument shows that we may assume $(c_1, d_1) = (c_2, d_2) = 1$.

Finally, by eliminating terms of the respective sequences if necessary, and some changes in sign as required, there is no loss of generality in assuming that $u_k > 0$ and $v_k > 0$ for all $k \geq 1$, $e > 0$, and that every solution of (2.1) has $x > 0$.

Under the assumption of the existence of infinitely many solutions to (2.1), we deduce from Lemma 2.1 that there exists an element $j \in \{0, 1, \ldots, n-1\}$, and an element $h \in \mathcal{A}$, such that if we denote by

$$g(k) = u_{kn+j}v_{kn+j},$$

then $g = eh^n$. It follows that

$$u_{kn+j} = c_1a_1^j(a_1^n)^k + d_1b_1^j(b_1^n)^k$$

and

$$v_{kn+j} = c_2 a_2^j (a_2^n)^k + d_2 b_2^j (b_2^n)^k.$$

Upon replacing each pair (a_i, b_i) by (a_i^n, b_i^n), and each pair (c_i, d_i) by $(c_i a_i^j, d_i b_i^j)$, we see that every positive integer input k leads to a solution of (2.1). We note that this replacement leaves a_i and b_i coprime, but not c_i and d_i. To deal with this, we simply replace (c_i, d_i) by $c_i/(c_i, d_i), d_i/(c_i, d_i)$, which has only the affect of altering the value of e. Therefore, we will assume that $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2, e$ are integers such that $a_1, a_2, b_1, b_2, c_1, c_2, e$ are all positive, $(a_1, b_1) = (a_2, b_2) = (c_1, d_1) = (c_2, d_2) = 1$, and that for every positive integer k there exists an integer x such that $u_k v_k = ex^n$.

For the proof of Theorem 2.1, we henceforth assume that $a_i,\ b_i,\ c_i$ are positive integers, $e > 0$, $(a_i,\ b_i) = (c_i,\ d_i) = 1$ for $i = 1,\ 2$, and that there exists an element $f \in \mathcal{A}$ such that

$$(c_1 a_1^k + d_1 b_1^k)(c_2 a_2^k + d_2 b_2^k) = ef(k)^n \tag{2.3}$$

holds for all $k \geq 0$.

Let $\mathcal{P}$ denote the set of prime numbers. Then $\mathcal{A}$ is isomorphic to $\mathbf{Q}[X_p]_{p\in\mathcal{P}}$, and an explicit isomorphism between these rings is given by extending the map

$$p^n \xrightarrow{\psi} X_p \qquad \text{for all } p \in \mathcal{P}$$

multiplicatively and additively to obtain a ring isomorphism $\psi : \mathcal{A} \longrightarrow \mathbf{Q}[X_p]_{p\in\mathcal{P}}$.

We now interpret (2.3) in $\mathbf{Q}[X_p]_{p\in\mathcal{P}}$ (via ψ). If we define $A_i = \psi(a_i^n)$ and $B_i = \psi(b_i^n)$ for $i = 1,\ 2$, then

$$(c_1 A_1 + d_1 B_1)(c_2 A_2 + d_2 B_2) = eF^k,$$

where $F = \psi(f)$.

For an arbirary positive integer m and an arbitrary $p \in \mathcal{P}$ we let $\alpha_p(m)$ denote the exact power to which the prime p divides m. Since

$$m := \prod_{p\in\mathcal{P}} p^{\alpha_p(m)}$$

is the prime factor factorization of m (where all but finitely many of the $\alpha_p(m)$ are zero),

$$M := \psi(m^n) = \prod_{p\in\mathcal{P}} X_p^{\alpha_p(m)}.$$

We now introduce an ordering on the set of all monomials in $\mathbf{Q}[X_p]_{p\in\mathcal{P}}$ which reflects the total ordering on $\mathbf{N}$; i.e., if M_1 and M_2 are monomials in $\mathbf{Q}[X_p]_{p\in\mathcal{P}}$ then we define $M_1 > M_2$ if $\psi^{-1}(M_1) > \psi^{-1}(M_2)$ (with the convention that $\psi^{-1}(M_1) > \psi^{-1}(M_2)$ provided that $m_1 > m_2$). With these notations, since $a_i > b_i$ for $i = 1,\ 2$, it follows that $A_i > B_i$ for $i = 1,\ 2$.

For a given monomial M in $\mathbf{Q}[X_p]_{p\in\mathcal{P}}$ let us denote by $\mathrm{supp}(M)$ its *support*, i.e. the set of indeterminates on which M effectively depends. That is, if

$$M := \prod_{p\in\mathcal{P}} X_p^{\beta_p},$$

then

$$\mathrm{supp}(M) := \{p \mid \beta_p > 0\}.$$

The condition that $\gcd(a_i,\ b_i) = 1$ can now be translated in $\mathbf{Q}[X_p]_{p\in\mathcal{P}}$ into the condition

$$\operatorname{supp}(A_i) \cap \operatorname{supp}(B_i) = \emptyset \ \text{ for } i = 1,\ 2.$$

After all of these considerations, Theorem 2.1 will be proved provided that we can establish the following equivalent proposition.

Proposition.

Let $A_i,\ B_i$ be monomials in $\mathbf{Q}[X_p]_{p\in\mathcal{P}}$ and $c_i,\ d_i$ be integers for $i = 1,\ 2$. Assume that $\gcd(c_i,\ d_i) = 1$, $A_i > B_i$ and $\operatorname{supp}(A_i) \cap \operatorname{supp}(B_i) = \emptyset$ for $i = 1,\ 2$. If there exist integers e and k with $k \geq 2$ and a polynomial $F \in \mathbf{Q}[X_p]_{p\in\mathcal{P}}$ such that

$$(c_1A_1 + d_1B_1)(c_2A_2 + d_2B_2) = eF^k, \tag{2.4}$$

then $k = 2$, $e = 1$, $c_1 = c_2$, $d_1 = d_2$, $A_1 = A_2$, and $B_1 = B_2$.

Proof. Let

$$U := \operatorname{supp}(A_1) \cup \operatorname{supp}(A_2) \cup \operatorname{supp}(B_1) \cup \operatorname{supp}(B_2).$$

It is clear that U is finite and that

$$c_iA_i + d_iB_i \in \mathbf{Q}[X_p]_{p\in U}.$$

By (2.4), we also get that $F \in \mathbf{Q}[X_p]_{p\in U}$. Since $\gcd(c_i,\ d_i) = 1$ for $i = 1,\ 2$, it follows that $e = e_1^k$ for some positive integer e_1, and that the polynomial e_1F belongs to $\mathbf{Z}[X_p]_{p\in U}$. Thus, we may assume that (2.4) holds with $e = 1$ and with $F \in \mathbf{Z}[X_p]_{p\in U}$.

We now use the fact that $\mathbf{Z}[X_p]_{p\in U}$ is a unique factorization domain to conclude that there exist $t \geq 0$ distinct irreducible polynomials $Q_1,\ \ldots,\ Q_t$, positive integers $\gamma_1,\ \ldots,\ \gamma_t$, $\delta_1,\ \ldots,\ \delta_t$ satisfying $\gamma_i+\delta_i = k$ for all $i = 1,\ \ldots,\ t$, and two polynomials G_1 and G_2 for which

$$c_1A_1 + d_1B_1 = \prod_{i=1}^{t} Q_i^{\gamma_i}G_1^k,\ \ c_2A_2 + d_2B_2 = \prod_{i=1}^{t} Q_i^{\delta_i}G_2^k. \tag{2.5}$$

It suffices to show that (2.5) implies that $k = 2,\ G_1 = G_2 = 1$, for this would entail $\gamma_i = \delta_i = 1$ for all $i = 1,\ \ldots,\ t$; i.e. that $c_1A_1 + d_1B_1 = c_2A_2 + d_2B_2$, and the statement of the proposition then follows immediately by identifying the largest and smallest monomials and their coefficients.

We first observe that

$$\operatorname{supp}(A_1) \cup \operatorname{supp}(B_1) = \operatorname{supp}(A_2) \cup \operatorname{supp}(B_2). \tag{2.6}$$

To see this, assume that there exists $q \in \operatorname{supp}(A_1)\cup\operatorname{supp}(B_1)$ with $q \notin \operatorname{supp}(A_2)\cup\operatorname{supp}(B_2)$. Suppose, for example, that $q \in \operatorname{supp}(A_1)$. Setting $X_q = 0$ in the first relation of (2.5), we obtain $\prod_{i=1}^{t} Q_i\Big|_{X_q=0}$ divides d_1B_1. In particular, it follows that there exist nonzero integers m_i, monomials $M_i \in \mathbf{Z}[X_p]_{p\in U}$, and polynomials $H_i \in \mathbf{Z}[X_p]_{p\in U}$ for $i = 1,\ 2,\ \ldots,\ t$, such that

$$Q_i = m_iM_i + X_qH_i \qquad \text{for all } i = 1,\ \ldots,\ t \tag{2.7}$$

and such that $\prod_{i=1}^{t} M_i$ divides B_1. We now use the second relation of (2.5) together with (2.6) and (2.7), with $X_q = 0$, to see that $\prod_{i=1}^{t} M_i$ divides $c_2A_2 + d_2B_2$. This implies that $M_i = 1$ for all $i = 1,\ \ldots,\ t$.

Now noticing that, in fact, $c_2A_2 + d_2B_2$ does not depend on X_q, it also follows that $H_i = 0$ for all $i = 1, \ldots, t$, and therefore $Q_i = m_i$ for $i = 1, \ldots, t$. Thus, $m_i = \pm 1$ for $i = 1, \ldots, t$, and

$$c_2A_2 + d_2B_2 = \pm G_2^k. \tag{2.8}$$

However, it is easy to see that this is impossible. Indeed, pick $q_1 \in \mathrm{supp}(A_2) \cup \mathrm{supp}(B_2)$ and set $X_p = 1$ for all $p \in U - \{q_1\}$. Equation (2.8) shows that a polynomial of one variable, X_{q_1}, of the form $c_2X_{q_1}^{\alpha_1} + d_2$ (or $c_2 + d_2X_{q_1}^{\alpha_1}$, according to whether $q_1 \in \mathrm{supp}(A_2)$ or $q_1 \in \mathrm{supp}(B_2)$) is a perfect power of another polynomial (again, of one variable, X_{q_1}), which is not possible since a polynomial of this form cannot have multiple roots (notice that its roots are non-zero while the only root of its derivative is zero).

Thus,

$$U = \mathrm{supp}(A_1) \cup \mathrm{supp}(B_1) = \mathrm{supp}(A_2) \cup \mathrm{supp}(B_2).$$

We can now finish the argument by induction on the cardinality $l := |U|$. If $l = 1$, it then follows that both $c_1A_1 + d_1B_1$ and $c_2A_2 + d_2B_2$ are polynomials of one variable, both of the form $cX_p^{\alpha} + d$. From what we have said before, such polynomials cannot have multiple roots, therefore $G_1 = G_2 = 1$, and $\gamma_i = \delta_i = 1$ for all $i = 1, \ldots, t$, which takes care of this case.

Assume that $l > 1$ and, by induction, that the proposition holds whenever $|U| < l$. Choose $q_1 \in U$, let r be any prime number larger than $\max(c_1, c_2, d_1, d_2)$, and set $X_{q_1} := r$ in relations (2.5). We treat only the case $q_1 \in \mathrm{supp}(A_1) \cap \mathrm{supp}(A_2)$, as the other three instances can be dealt with similarly. Write

$$A_1 = X_{q_1}^{\alpha_1}A_1', \quad A_2 = X_{q_1}^{\alpha_2}A_2',$$

where A_1' and A_2' are monomials which do not contain q_1 in their support. An application of the induction hypothesis shows that

$$c_1r^{\alpha_1}A_1' + d_1B_1 = c_2r^{\alpha_2}A_2' + d_2B_2.$$

By comparing the coefficients and using the fact that r does not divide $c_1c_2d_1d_2$, it follows that $c_1r^{\alpha_1} = c_2r^{\alpha_2}$, $d_1 = d_2$, $B_1 = B_2$, and $A_1' = A_2'$. Hence, $c_1 = c_2$, and $\alpha_1 = \alpha_2$. As $A_1' = A_2'$ and $\alpha_1 = \alpha_2$ imply that $A_1 = A_2$, the proof of the induction step is complete, which completes the proof of the Proposition, and consequently of Theorem 2.1.

3 Computing all solutions of $(a^k - 1)(b^k - 1) = x^2$

Although the result of the previous section is ineffective, being based on the ineffective result of Corvaja and Zannier, there are subclasses of those sequences in Theorem 2.1 for which all solutions can be determined for the particular case $n = 2$. In particular, for a fixed pair of positive integers (a, b), and under certain mild hypotheses, we will demonstrate how one can determine all integer solutions (k, x) to the Diophantine equation

$$(a^k - 1)(b^k - 1) = x^2.$$

We demonstrate our method by computing all solutions for most pairs (a, b) satisfying $2 \le b < a \le 100$.

Theorem 3.1 *Let $2 \le b < a \le 100$ be integers. Assume that $(a-1)(b-1)$ is not a square, and that (a, b) is not in the set $\{(22, 2), (22, 4), (25, 3), (81, 5)\}$. If*

$$(a^k - 1)(b^k - 1) = x^2, \tag{3.1}$$

then $k = 2$.

Of the 4851 pairs (a, b) satisfying $2 \leq b < a \leq 100$, Theorem 3.1 is able to deal with 4749 of them. This is an improvement upon previous work of Szalay [15], wherein the particular case $(a, b) = (3, 2)$ was solved, and on work by Hajdu and Szalay [7], wherein the case $(a, b) = (6, 2)$ was solved. It is worth noting that a few of the pairs (a, b) left out in the statement of Theorem 3.1 can be dealt with using elementary methods. For example, as argued in [15], the pair $(5, 2)$ can be dealt with using congruence arguments. The same argument applies to the pair $(65, 2)$. We forego the details of these particular pairs since we do not have a method to solve (3.1) for almost all pairs (a, b) satisfying the property that $(a-1)(b-1)$ is a square. A new idea to deal with these pairs would be of interest. The remaining 4 pairs cannot be dealt with by our method since they have integral solutions at $k = 3$ or rational solutions at $k = -1$.

The proof of Theorem 3.1 will be accomplished in stages. We first state some general solvability results which will rule out 1670 of the 4749 pairs. For the remaining 3079 pairs, a computational method will be described to rule out solutions for odd values of k. The proof is completed by using a result of Cohn [3] and properties of solutions to Pell equations (see [9]) to rule out solutions for even values of k.

We state the following result from [16], which improved upon the work of Szalay [15], who dealt with the particular case $n = m$.

Lemma 3.1 *The equation*

$$(2^m - 1)(3^n - 1) = x^2$$

has no solutions in positive integers (m, n, x).

The following result improves upon Theorem 2 of [7].

Lemma 3.2 *The only positive integers* (a, m, n, x), *with* $m > n \geq 1$ *and* $m \geq 3$, *satisfying*

$$(a^m - 1)(a^n - 1) = x^2$$

are $(2, 6, 3, 21), (3, 5, 1, 22), (7, 4, 1, 120)$.

Proof. The assumption $m \geq 3$ is required, for if $m = 2$ and $n = 1$, then solutions exist for all a of the form $a = u^2 - 1$. Let $d = \gcd(m, n)$, then $\gcd(a^m - 1, a^n - 1) = a^d - 1$, and so (3.1) can be rewritten as

$$\left(\frac{a^m - 1}{a^d - 1}\right)(a^d - 1)^2\left(\frac{a^n - 1}{a^d - 1}\right) = x^2.$$

Let $m_1 = m/d$ and $n_1 = n/d$, then both $(a^{m_1 d} - 1)(a^d - 1)^{-1}$ and $(a^{n_1 d} - 1)(a^d - 1)^{-1}$ are squares. By a result of Ljunggren in [10], the only positive integer solutions of the Diophantine equation

$$\frac{y^k - 1}{y - 1} = z^2,$$

for $k \geq 3$, are $(y, k, z) = (3, 5, 11)$ and $(7, 4, 20)$. These lead to the last of the two solutions given in the statement, and leaves us only to deal with the case $m = 2d$ and $d > 1$. But in this case, it follows that $a^d + 1 = u^2$ for some integer u, and by the result of Chao Ko [8] on Catalan's equation, we see that the only possibility is the first solution given in the statement of the lemma.

We now proceed with the proof of Theorem 3.1. We will deal three cases separately; the first with k even, the second with k odd and ab not a square, and the last case covering the situation that k is odd and ab is a perfect square.

Case i: k is even.

We first note a result of Cohn [3], who proved that the only solution to the Diophantine equation $(x^4-1)(y^4-1)=z^2$ in positive integers $x>1, y>1$, is $(x,y)=(13,239)$. We will therefore assume that $k \equiv 2 \pmod 4$.

We verified computationally that for all $2 \le b < a \le 100$, and k in the range $4 < k < 200$, that (3.1) is not solvable. We will assume for the remainder of the proof that $k > 200$.

A solution to (3.1) with k even implies the existence of positive integers u, v, d, with $d > 1$ and squarefree, such that $(X,Y) = (b^{k/2}, u)$ and $(a^{k/2}, v)$ are solutions to the Pell equation

$$X^2 - dY^2 = 1.$$

Let $\epsilon_d = T + U\sqrt{d}$ correspond to the minimal solution (T,U) of this equation, and for $i \ge 1$, let $T_i + U_i\sqrt{d} = (T+U\sqrt{d})^i$. It follows that there are positive integers s and t, with $t > s \ge 1$ such that

$$T_t = a^{k/2},\ T_s = b^{k/2}.$$

We may assume without loss of generality that $\gcd(s,t)=1$, for if $g=\gcd(s,t)$, we could simply replace ϵ_d by ϵ_d^g. Note that since s and t are coprime, one of them must be odd. Much of this proof will be spent on proving the following.

Claim. If m is a positive integer for which

$$T_m = c^{k/2}$$

for some c satisfying $2 \le c \le 100$ and even $k > 200$, then m is a power of 2.

In the proof of this claim, we will use the fact that the sequence $\{T_i\}$ satisfies the property that if m_1 divides m_2 and m_2/m_1 is odd, then T_{m_1} divides T_{m_2}. For further properties of these sequences, the reader may wish to consult [9].

A *primitive* divisor of T_i is defined to be a prime p which divides T_i, but does not divide T_j for any $j < i$. By Theorem 24 of [2], T_i has a primitive divisor for all odd $i \ge 5$. Since $T_1 > 1$, T_1 has a primitive divisor. Also, since $T_3 = 4T_1^2 - 3$, it is easy to see that T_3 must have a primitive divisor as well. Thus, for each odd $i \ge 1$, T_i has a primitive divisor.

For the proof of the claim, let $m = 2^r l$, with $r \ge 0$ and l odd. Assume first that l is composite. If p and q are distinct primes dividing l, then T_m is divisible by $T_{2^r}, T_{2^r p}, T_{2^r q}, T_{2^r pq}$, and hence T_m is divisible by at least 4 primes. Therefore c is divisible by at least 4 primes, which implies that $c \ge 2*3*5*7 = 210$, which is not possible by our hypothesis. If l is divisible by p^2 for some odd prime p, then T_m is divisible by $T_{2^r}, T_{2^r p}, T_{2^r p^2}$. Since primitive divisors q of T_i are of the form $q \equiv \pm 1 \pmod i$, it follows that T_m, and hence c, is divisible by a product of primes as large as $2(2p-1)(2p^2-1)$, which is greater than 100 for $p \ge 3$. Therefore we conclude that if $l > 1$, then l must be prime.

Since T_{2^r} divides T_m,

$$T_{2^r}\left(\frac{T_m}{T_{2^r}}\right) = c^{k/2}.$$

Furthermore, by the binomial theorem, since l is prime, either T_{2^r} and $\frac{T_m}{T_{2^r}}$ are coprime, or their greatest common divisor is equal to l. The latter case occurs precisely when l divides T_{2^r}. We will complete the

proof of the claim that $l = 1$ by dealing with these two cases separately.

Assume that l does not divide T_{2^r}, then T_{2^r} and $\frac{T_m}{T_{2^r}}$ are coprime, and hence there exists a positive integer $c_1 > 1$ dividing c for which $T_{2^r} = c_1^{k/2}$. Using standard arguments involving the recurrence formulas satisfied by elements in the sequence $\{T_i\}$, it is not difficult to verify that for each $i > 1$,

$$(T_{2^r})^i < T_{2^r i} < 2^{i-1}(T_{2^r})^i. \tag{3.2}$$

Therefore,

$$c^{k/2} = T_m = T_{2^r l} > (T_{2^r})^l = (c_1^{k/2})^l,$$

and so

$$c_1^l < c \leq 100. \tag{3.3}$$

This forces $T_{2^r} = 2^{k/2}$, and either $l = 3$ or $l = 5$. If $l = 5$, then (3.3) shows that $c > 2^5 = 32$. But from (3.2),

$$c^{k/2} = T_{2^r 5} < 2^4 T_{2^r}^5 = 2^4 (32)^{k/2},$$

which implies that

$$c < 2^{8/k} 32 < 2^{8/200} 32 < 33,$$

a contradiction. Similarly, if $l = 3$, then $c > 2^3 = 8$, while (3.2) shows that

$$c^{k/2} = T_{2^r 3} < 2^2 T_{2^r}^3 = 2^2 (2^{k/2})^3,$$

which implies that

$$c < 2^{4/k} 8 < 2^{4/200} 8 < 9,$$

a contradiction.

We henceforth assume that l divides T_{2^r}. It follows from the binomial theorem that l properly divides T_m/T_{2^r}, and so $l^{k/2-1}$ divides T_{2^r}. Equation (3.2) shows that

$$c^{k/2} = T_m > (T_{2^r})^l > (l^{k/2-1})^l,$$

which simplifies to

$$100 \geq c > (l^{(k-2)/k})^l > l^{(98l)/200}.$$

This inequality can only hold if $l \leq 3$, and so either $l = 1$ or $l = 3$. If $l = 3$ we deduce from the divisibility properties of terms in the sequence $\{T_i\}$ that

$$T_{2^r} = (c_1^{k/2})/3$$

for some positive integer c_1. Using (3.2) once more, we obtain

$$c^{k/2} = T_m > (T_{2^r})^3 = (c_1^{3k/2})/27,$$

which implies that

$$c_1^3 < c(3^{6/k}) < 100(3^{6/200}) < 104,$$

and hence $c_1 = 3$. Therefore, $T_{2^r} = 3^{k/2-1}$, and so by (3.2)

$$c^{k/2} = T_m > (3^{k/2-1})^3,$$

which implies that

$$c > 27^{(k-2)/k} \geq 27^{198/200} > 26.$$

On the other hand, (3.2) also shows that

$$c^{k/2} = T_m < 4(T_{2^r})^3 = 4(27^{k/2-1}),$$

which implies that

$$c < 27^{(k-2)/k} 4^{2/k} < 27^{198/200} 4^{2/200} < 27.$$

This last contradiction shows that $l = 1$, completing the proof of the claim.

Recall that $t > s \geq 1$ are coprime integers with $T_t = a^{k/2}$ and $T_s = b^{k/2}$. From the above claim, we deduce that $s = 1$ and that t is a power of 2. From (3.2), we see that

$$a^{k/2} = T_t > T_1^t = (b^{k/2})^t,$$

and so

$$b^t < a \leq 100. \tag{3.4}$$

Since $b \geq 2$, it follows that $t = 2$ or $t = 4$. If $t = 2$, then since $T_2 = 2T_1^2 - 1$, we have that

$$a^{k/2} + 1^{k/2} = 2(b^2)^{k/2}.$$

Part (1) of the Main Theorem in [6] states that the equation $X^n + Y^n = 2Z^n$ has no integer solutions with $XYZ \neq 0$ for $n \geq 3$. Since $k \geq 6$, we see that $t = 2$ is not possible. Assume now that $t = 4$, then by (3.4), either $b = 2$ or $b = 3$, and $a > b^4$. However, (3.2) also shows that

$$a^{k/2} = T_4 < 2^3 T_1^4 = 2^3 b^{2k},$$

which is the same as

$$a < 2^{6/100} b^4. \tag{3.5}$$

If $b = 2$, (3.5) shows that $a < 17$, which is impossible since $a > b^4 = 16$. If $b = 3$, (3.5) shows that $a \leq 82$, which combined with $a > b^4 = 81$ yields $a = 82$. But this would mean that T_4 is even, which is impossible. This completes the proof in the case that k is even.

Case ii: k is odd and ab is not a square.

To show that no solutions exist when $k > 3$ is odd, we first eliminate subsets of pairs (a, b) as follows. We first eliminate those pairs for which Lemma 3.1 and Lemma 3.2 have shown (3.1) to be unsolvable. We then eliminate those pairs (a, b) for which ab is a square, as this case will be dealt with separately in Case iii. Finally, we eliminate those pairs (a, b) for which one of a or b is even and the other satisfies the property of being one more than an odd multiple of an odd power of two, for in this case $(a^k - 1)(b^k - 1)$ is exactly divisible by an odd power of 2. Of the 4749 pairs (a, b) we intend to solve (for k odd at this point), there remain 3079 pairs. We noticed at the time of writing this paper that many more pairs could have been eliminated in this last way by eliminating instead all of those pairs for which $(a - 1)(b - 1)$ is properly divisible by an odd power of 2. This is a moot point since in the end we obtained the desired result.

To deal with these 3079 pairs, we select a *modulus* $A_1 = 2520$. A_1 has the property that 21 primes p exist for which $p-1$ divides A_1. For each of the 3079 pairs (a,b), each odd k satisfying $1 \le k \le A_1$, and each of the 21 primes p for which $p-1$ divides A_1, we compute

$$\Big(\frac{(a^k-1)(b^k-1)}{p}\Big). \tag{3.6}$$

A pair (a,b) is eliminated by this process if for each odd k in the range $1 \le k \le A_1$ there exists at least one prime, say q, of the 21 primes, for which

$$\Big(\frac{(a^k-1)(b^k-1)}{q}\Big) = -1.$$

A Mathematica program ran for about 24 hours and returned 1011 triples of the form (a,b,k) for which (3.6) evaluated to 0 or 1 for all 21 primes p.

We then selected a new modulus $A_2 = 48A_1$. From the 1011 triples (a,b,k) remaining from the previous step, we obtain $48 * 1011$ new triples, where a fixed triple (a,b,k) leads to 48 new triples by keeping (a,b) fixed, but adding multiples of A_1 to k.

We computed (3.6) for all of the $48 * 1011$ triples with respect to 16 new primes p for which $p-1$ divides A_2, but not A_1, and $p < 1000$. This computation took about 4 hours, and returned 51 triples (a,b,k) for which (3.6) evaluated to 0 or 1 for all of these new 16 primes.

For these remaining 51 triples, we computed (3.6) with respect to each of the remaining 15 primes p for which $p-1$ divides A_2 but not A_1, and for which $p > 1000$. Of these 51 triples, there remained 4 survivors:

$$(25,3,60479),(25,3,120959),(81,5,60479),(81,5,120959).$$

The two remaining cases $(a,b) = (25,3),(81,5)$ cannot be eliminated by this method because of the relations

$$\Big(\frac{1}{25}-1\Big)\Big(\frac{1}{3}-1\Big) = \Big(\frac{4}{5}\Big)^2,\ \Big(\frac{1}{81}-1\Big)\Big(\frac{1}{5}-1\Big) = \Big(\frac{8}{9}\Big)^2.$$

This completes the proof in the case that k is odd and ab is not a square.

Case iii: k is odd and ab is a perfect square.

The proof of Theorem 3.1 will be complete once we have shown that for all pairs (a,b), with ab a perfect square, and odd $k > 200$, (3.1) has no solutions.

We know from the result of Case i that a and b cannot be squares. Therefore, there exists a positive integer $d > 1$, and positive integers u, v, such that $a = du^2$ and $b = dv^2$. A solution to (3.1) implies the existence of a positive integer $D > 1$, and positive integers z, w such that $(X,Y) = (d^{(k-1)/2}u^k, z), (d^{(k-1)/2}v^k, w)$ are solutions to the quadratic equation

$$dX^2 - DY^2 = 1. \tag{3.7}$$

It is well known that if (3.7) is solvable, there exists a minimal solution $\eta = A\sqrt{d} + B\sqrt{D}$, and that all positive integer solutions (X,Y) come from $(X,Y) = (A_i, B_i)$, for i odd, where

$$\eta^i = A_i\sqrt{d} + B_i\sqrt{D}.$$

We therefore have that there exist positive odd integers $t > s \geq 1$ such that $A_t = d^{(k-1)/2}u^k$ and $A_s = d^{(k-1)/2}v^k$. Let $g = \gcd(s,t)$, then it is well known from the theory of these sequences (see [9] for example), that $\gcd(A_t, A_s) = A_g$. Therefore, $A_g = d^{(k-1)/2}y^k$, for some integer y.

We have shown that if A_t and A_s lead to a solution of (3.1), then so do A_t and A_g. Furthermore, by replacing η by η^g, we deduce that $A_{t/g}$ and A_1 lead to a solution of (3.1). We can therefore continue the proof under the assumption that $s = 1$.

Similar to (3.2) we have the following inequalities for i odd, which are easily proved by induction;

$$A_1^i < A_i < 2^{i-1}d^{(i-1)/2}A_1^i. \tag{3.8}$$

We use (3.8) to infer that

$$d^{(k-1)/2}u^k = A_t > A_1^t = (d^{(k-1)/2}v^k)^t.$$

Since $a \leq 100$, we deduce that

$$10 \geq \sqrt{a} = \sqrt{du^2} > d^{(k-1)/2k}u > d^{(t(k-1))/2k}v^t. \tag{3.9}$$

Since $d \geq 2$, (3.9) shows that $v = 1$, $A_1 = 2^{(k-1)/2}$, and either $(t,d) = (3,2), (3,3)$ or $(5,2)$.

We will complete the proof by dealing with $(t,d) = (5,2)$, as the other possibilities can be dealt with in exactly the same way. Once again from (3.8), using the fact that $v = 1$, we obtain

$$du^2 > (d^{(k-1)/2}u^k)^{2/k} = A_t^{2/k} = A_5^{2/k} > (A_1^5)^{2/k} = (2^{(k-1)/2})^{10/k} > 2^{(1980/400)} > 30.$$

Therefore, $a \geq 32$ since d divides a and $d = 2$ is even. On the other hand, using (3.8) once again shows that

$$du^2 = d^{2/k}(d^{(k-2)/2}u^k)^{2/k} < 2^{2/k}A_5^{2/k} < 2^{2/k}(2^4d^2A_1^5)^{2/k} = 2^{2/k}(2^4 \cdot 2^2 \cdot 2^{5(k-1)/2})^{2/k} = 2^{5+(9/k)} < 34.$$

Since $d = 2$ is even, we conclude that $du^2 = 32$. It follows that $u = 4$, and hence $A_5 = d^{(k-1)/2}u^k = 2^{(5k-1)/2}$. But this implies that A_5/A_1 is even, which is not possible. This completes the proof of Theorem 3.1.

4 Connections with the ABC conjecture

It is certainly the case that the results of this paper represent a small step towards the truth on the solvability of Diophantine equations of the type being considered. Not surprisingly, the *abc* conjecture shows that much stronger statements hold. In this section, we attempt to exhibit how far the above results are from the truth by proving a very strong Diophantine result under the hypothesis of the *abc* conjecture. For more on the *abc* conjecture and its consequences, the reader may wish to refer to the paper of Nitaj [12], that of Browkin [1], or that of Ribenboim [14].

The *abc* conjecture Given any $\epsilon > 0$, there exists $C = C(\epsilon) > 0$, depending only on ϵ, with the property that for all triples of positive integers a, b, c satisfying $(a,b,c) = 1$ and $c = a + b$, the inequality

$$c < C \cdot N(a,b,c)^{1+\epsilon}$$

holds, where $N(a,b,c)$ denotes the product of distinct primes dividing abc.

Theorem 4.1 *Let a, b, c, d, e be nonzero integers. Then the abc conjecture implies that the equation*

$$(ax^m + b)(cy^n + d) = ez^2 \tag{4.1}$$

has only finitely many solutions (x, y, z, m, n) satisfying $xyz \neq 0$, $dax^m \neq bcy^n$ and $\min(m, n) \geq 5$.

In particular, the *abc* conjecture shows that there are only finitely many positive integers (x, y, z, m, n), with $z > 0$, $x^m \neq y^n$, and $\min(m, n) \geq 5$, such that

$$(x^m - 1)(y^n - 1) = z^2. \tag{4.2}$$

If the exponent 2 in (4.1) is replaced by an integer $k > 2$, a much stronger statement can be derived from the *abc* conjecture. We will forego this endeavour, and content ourselves with a proof of Theorem 4.1.

It would be of interest to determine a heuristic argument which would indicate the Diophantine nature of the above problem in the case that $\min(m, n) < 5$. Even for the particular equation

$$(x^3 - 1)(y^3 - 1) = z^2,$$

we do not have any reason to believe that there should be only finitely many integer solutions, nor do we have an argument which suggests that there are infinitely many integer solutions.

Proof of Theorem 4.1

For the sake of simplicity we will prove only the case (4.2), as the coefficients appearing in (4.1) do not play a significant role in the proof. We will work with a non-trivial solution of equation (4.2) with $z > 0$. Assume that $x^m \neq y^n$, then not both x and y can be zero. If one of them, say x, is zero, then (4.2) reduces to $z^2 - y^m = 1$, which is a particular case of Catalan's equation (see [13]), which was solved by Chao Ko [8], and its only solution is $3^2 - 2^3 = 1$. We will assume for the remainder of the proof that $xy \neq 0$.

From (4.2) there exists a positive integer D such that

$$x^m - 1 = Du^2, \; y^n - 1 = Dv^2, \tag{4.3}$$

with u and v coprime positive integers, for if g divides both u and v, then D can be replaced by Dg^2.

In what follows, we fix $\varepsilon < 1$, and denote by $c_1, \; c_2, \; \ldots$ recursively defined constants depending on ε. We apply the *abc* conjecture to the first equation of (4.3) to obtain

$$|x|^m < c_1 N(xDu)^{1+\varepsilon}.$$

By replacing ε in this equation by $\varepsilon/(1+\varepsilon)$, and defining where $c_2 = c_1^{\varepsilon/(1+\varepsilon)}$, we see that

$$|x|^{m(1-\varepsilon)} < c_2 N(xDu) < c_2 |x||D|u. \tag{4.4}$$

Since

$$|D|u^2 = |x^m - 1| \leq 2|x|^m,$$

we get

$$u \leq \frac{\sqrt{2}|x|^{m/2}}{|D|^{1/2}}. \tag{4.5}$$

Combining (4.4) and (4.5) shows

$$|x|^{m(1-\varepsilon)} < c_3|x||D|\frac{|x|^{m/2}}{|D|^{1/2}} = c_3|D|^{1/2}|x|^{m/2+1}, \tag{4.6}$$

where $c_3 = c_2\sqrt{2}$. Inequality (4.6) implies that

$$|D| > c_4|x|^{m(1-2\varepsilon)-2}, \tag{4.7}$$

and so (4.5) now shows that

$$u < c_5|x|^{m\varepsilon+1}, \tag{4.8}$$

where $c_4 = c_3^{-2}$ and $c_5 = \sqrt{2}c_3 = 2c_2$.

A similar argument applied to the second equation in (4.3) gives

$$|D| > c_4|y|^{n(1-2\varepsilon)-2}, \tag{4.9}$$

and

$$v < c_5|y|^{n\varepsilon+1}, \tag{4.10}$$

respectively. Since $x^m \neq y^n$, it follows that $u \neq v$. We will assume without loss of generality that $u > v$. This implies that $|x|^m > |y|^n$.

Upon multiplying the first equation in (4.3) by v^2, the second equation by u^2, and eliminating the common term containing D from the two resulting equations, we find that

$$v^2x^m - u^2y^n = u^2 - v^2. \tag{4.11}$$

Let $d = \gcd(v^2x^m,\ u^2y^n,\ u^2 - v^2)$. Since u and v are assumed to be coprime, $d = \gcd(x^m,\ y^n,\ u^2 - v^2)$. Therefore, from (4.11), we determine that

$$v^2\frac{x^m}{d} - u^2\frac{y^n}{d} = \frac{u^2 - v^2}{d}. \tag{4.12}$$

Applying the *abc* conjecture to (4.12), we obtain

$$\max\Big(v^2\frac{|x|^m}{d},\ u^2\frac{|y|^n}{d}\Big) < c_1N\Big(u^2v^2\frac{x^my^n(u^2 - v^2)}{d^3}\Big)^{1+\varepsilon}. \tag{4.13}$$

Let N denote the radical appearing in the right side of (4.13), and observe that

$$N \leq N\Big(u^2v^2x^my^n\frac{(u^2 - v^2)}{d}\Big) \leq \frac{u^3v|xy|}{d}. \tag{4.14}$$

Combining (4.13) and (4.14) shows that

$$v^2\frac{|x|^m}{d} < N < c_1\Big(\frac{u^3v|xy|}{d}\Big)^{1+\varepsilon} < \frac{(u^3v|xy|)^{1+\varepsilon}}{d},$$

and thus

$$v^2|x|^m < c_1(u^3v|xy|)^{1+\varepsilon}. \tag{4.15}$$

In a similar manner, one obtains the inequality

$$u^2|y|^n < c_1(u^3v|xy|)^{1+\varepsilon}. \tag{4.16}$$

Combining (4.15) and (4.16) yields the inequality

$$|x|^m|y|^n < c_6u^{4+6\varepsilon}v^{2\varepsilon}|x|^{2+2\varepsilon}|y|^{2+2\varepsilon}, \tag{4.17}$$

where $c_6 = c_1^2$. Employing the bounds for u and v from (4.8) and (4.10), we get

$$|x|^m|y|^n < c_7|x|^{6+\varepsilon(8+10m)}|y|^{2+\varepsilon(4+2n)}, \tag{4.18}$$

where $c_7 = c_6c_5^{8+8\epsilon}$. Hence,

$$|x|^{m(1-10\varepsilon)-(6+8\varepsilon)}|y|^{n(1-2\varepsilon)-(2+4\varepsilon)} < c_7. \tag{4.19}$$

The exponent of y in (4.19) is positive for $n \geq 3$ and ε small enough. Moreover, if $m \geq 7$ and ε is small enough, then (4.19) also shows that $\max(m,\ n,\ |x|,\ |y|)$ is bounded by a constant c_8. Thus, it remains to deal with the case in which $m \leq 6$. In order to do so, we first show that $|y|^n$ is not much smaller than $|x|^m$. Indeed, from the second equation in (4.3) and (4.7) we get

$$|y|^n \geq \frac{|y^n-1|}{2} = \frac{|D|v^2}{2} \geq \frac{|D|}{2} > c_9|x|^{m(1-2\varepsilon)-2}, \tag{4.20}$$

where $c_9 = c_4/2$. Hence,

$$|y| > c_9^{1/n}|x|^{\frac{m(1-2\varepsilon)-2}{n}}. \tag{4.21}$$

Using (4.21) with (4.19) shows that

$$c_{10}|x|^{m(1-10\varepsilon)-(6+8\varepsilon)+\frac{(m(1-2\varepsilon)-2)(n(1-2\varepsilon)-(2+4\varepsilon))}{n}} < c_7, \tag{4.22}$$

where

$$c_{10} = c_9^{\frac{n(1-2\varepsilon)-(2+4\varepsilon)}{n}}. \tag{4.23}$$

The exponent of c_9 from formula (4.23) is bounded from below when ε is small and $n \geq 3$. Indeed, if $\epsilon \leq 1/12$, then

$$\frac{n(1-2\varepsilon)-(2+4\varepsilon)}{n} \geq \frac{5n-14}{6n} \geq \frac{1}{18},$$

which shows that $c_{10} > c_9^{1/18}$ for ε small enough. Upon taking logarithms of both sides of (4.22), we obtain

$$\Big(m(1-10\varepsilon)-(6+8\varepsilon)+\frac{(m(1-2\varepsilon)-2)(n(1-2\varepsilon)-(2+4\varepsilon))}{n}\Big)\log|x| < c_{11}, \tag{4.24}$$

where $c_{11} = c_7c_9^{-1/18}$. We now determine a lower bound for the term appearing in parenthesis in front of the factor $\log|x|$ in inequality (4.24). Let $\varepsilon = 10^{-3}$. Then,

$$\frac{n(1-2\varepsilon)-(2+4\varepsilon)}{n} = \frac{.998n-2.004}{n} \geq .497 \qquad \text{for } n \geq 4.$$

Hence,

$$m(1-10\varepsilon)-(6+8\varepsilon)+\frac{(m(1-2\varepsilon)-2)(n(1-2\varepsilon)-(2+4\varepsilon))}{n} \geq$$

$$.99m - 6.008 + .497(.998m - 2) > 1.486m - 7.002. \tag{4.25}$$

The right hand side of (4.25) is strictly larger than 0 when $m \geq 5$, and so (4.25) implies that

$$(1.486m - 7.002)\log|x| < c_{11},$$

which leads to $\max(m,\ |x|) < c_{12}$. In particular, $|x|^m$ is bounded, and since $|x|^m > |y|^n$, it follows that $|y|$ and n are bounded as well.

Acknowledgement The authors gratefully acknowledge the suggestions by the referee, in particular for the simplification of the proof of Theorem 2.1.

References

[1] J. Browkin *The abc-Conjecture*, Number Theory, 75-105, Trends Math., Birkhäuser, Basel, 2000.

[2] R.D. Carmichael *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$ Annals of Math. **15** no. 1-2 (1915), 30-70.

[3] J.H.E. Cohn *Perfect Pell powers* Glasgow Math. J. **38** (1996), 19-20.

[4] J.H.E. Cohn. *The Diophantine equation* $x^4 - Dy^2 = 1$ *II.* Acta Arith. **78** (1997), 401-403.

[5] P. Corvaja and U. Zannier *Diophantine equations with power sums and Universal Hilbert Sets*, Indag. Math. N.S. **9**, 317-332.

[6] H. Darmon and L. Merel *Winding quotients and some variants of Fermat's last theorem*, J. Reine Angew. Math. **490** (1997), 81-100.

[7] L. Hajdu and L. Szalay *On the diophantine equations* $(2^n-1)(6^n-1) = x^2$ *and* $(a^n-1)(a^{kn}-1) = x^2$ *Period. Math. Hungar.* **40** (2000), 141-145.

[8] C. Ko *On the diophantine equation* $x^2 = y^n + 1$, $xy \neq 0$ Sci. Sinica **14** (1965), 457-460.

[9] D.H. Lehmer. *An extended theory of Lucas functions.* Ann. Math. **31** (1930), 419-448.

[10] W. Ljunggren *Some theorems on indeterminate equations of the form* $\frac{x^n-1}{x-1} = y^q$ (Norwegian) Norsk Mat. Tidsskr. **25** (1943), 17-20.

[11] F. Luca *Multiply perfect numbers in Lucas sequences with odd parameters* Publ. Math. Debrecen **58** (2001), 121-155.

[12] A. Nitaj *La conjecture abc. (The abc conjecture)* Enseign. Math., II. Ser. 42 (1996), 3-24.

[13] P. Ribenboim *Catalan's Conjecture: Are* 8 *and* 9 *the only consecutive powers?* Academic Press, Boston, 1994.

[14] P. Ribenboim *ABC Candies*, J. Number Theory **81** (2000), 48-60.

[15] L. Szalay *On the diophantine equation* $(2^n - 1)(3^n - 1) = x^2$ Publ. Math. Debrecen **57** (2000), 1-9.

[16] P.G. Walsh *On Diophantine equations of the form* $(x^m - 1)(y^n - 1) = z^2$ Tatra Mt. Math. Publ. **20** (2000), 1-3.

F. Luca
Instituto de Matemáticas UNAM
Campus Morelia
Ap. Postal 61-3 (Xangari)
CP 58 089
Morelia, Michoacan
Mexico
fluca@matmor.unam.mx

P.G Walsh
Department of Mathematics
University of Ottawa
585 King Edward St.
Ottawa, Ontario, Canada
K1N-6N5
gwalsh@mathstat.uottawa.ca