On Pillai's Diophantine equation

Yann Bugeaud
Université Louis Pasteur
UFR de mathématiques
7 rue René Descartes, 67084 Strasbourg, France
bugeaud@math.u-strasbg.fr

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58180, Morelia, Michoacán, México
fluca@matmor.unam.mx

November 5, 2005

Abstract

Let a, b, A, B and c be fixed nonzero integers. We prove several results on the number of solutions to Pillai's Diophantine equation $Aa^x - Bb^y = c$ in positive unknown integers x and y.

1 Introduction

Let a, b and c be nonzero integers with $a \geq 2$ and $b \geq 2$. As noticed by Pólya [13], it follows from a theorem of Thue that the Diophantine equation

$$a^x - b^y = c, \qquad \text{in positive integers } x,\ y \tag{1}$$

has only finitely many solutions. If, moreover, a and b are coprime and c is sufficiently large compared with a and b, then (1) has at most one solution. This is due to Herschfeld [6] in the case $a = 2$, $b = 3$, and to Pillai [12] in the general case (Pillai also claimed that (1) can have at most one solution even if a and b are not coprime. This is incorrect, however, as shown by the example $6^4 - 3^4 = 6^5 - 3^8 = 1215$.)

Further results on equation (1) are due to Shorey [18], Le [7] (both papers are concerned with the more general equation $Aa^x - Bb^y = c$, in positive integers x, y) and, more recently, to Scott and Styer [17] and to Bennett [1, 2]. We direct the reader to [20, 1] for more references.

In view of Pólya's result, the above quoted theorem of Pillai can be rephrased as follows.

Theorem 1.1. *Let $a \geq 2$ and $b \geq 2$ be coprime integers. Then the Diophantine equation*

$$a^{x_1} - a^{x_2} = b^{y_1} - b^{y_2}, \tag{2}$$

in positive integers x_1, x_2, y_1, y_2 with $x_1 \neq x_2$ has at most finitely many solutions.

In (2), the bases a and b are fixed. Scott and Styer [17] allowed a to be a variable, under some additional, mild assumptions. A particular case of their Theorem 2 can be formulated as follows.

Theorem 1.2. *The Diophantine equation*

$$a^{x_1} - a^{x_2} = 2^{y_1} - 2^{y_2}, \tag{3}$$

in positive integers a, x_1, x_2, y_1, y_2 with $x_1 \neq x_2$ and a prime has no solution, except for four specific cases, or unless a is a sufficiently large Wieferich prime.

Since we still do not know whether or not infinitely many Wieferich primes exist, Theorem 1.2 does not imply that (3) has only finitely many solutions. Such a result has been recently established by Luca [8].

Theorem 1.3. *Let b be a prime number. The Diophantine equation*

$$a^{x_1} - a^{x_2} = b^{y_1} - b^{y_2}, \tag{4}$$

in positive integers a, x_1, x_2, y_1, y_2 with $a \neq b$ prime and $x_1 \neq x_2$ has only finitely many solutions.

The proof of Theorem 1.3 uses a broad variety of techniques from Diophantine approximation, ranging from Ridout's Theorem to the theory of linear forms in logarithms.

In the present paper, our aim is to generalize Theorem 1.3 in two directions. First, we remove the assumption 'b is prime' and we allow b to be any fixed positive integer. Secondly, under some mild coprimality conditions, we also allow arbitrary coefficients which need not be fixed, but whose prime factors should be in a fixed finite set of prime numbers.

Acknowledgments. We thank the referee for useful suggestions. This paper was written during a visit of the second author at the Université Louis Pasteur in Strasbourg in September 2004. He warmly thanks the Mathematical Department for its hospitality. Both authors were supported in part by the joint Project France-Mexico ANUIES-ECOS M01-M02.

2 Results

Let $\mathcal{P} = \{p_1, \ldots, p_t\}$ be a fixed, finite set of prime numbers. We write $\mathcal{S} = \{\pm p_1^{\alpha_1} \ldots p_t^{\alpha_t} : \alpha_i \geq 0,\ i = 1, \ldots, t\}$ for the set of all nonzero integers whose prime factors belong to $\mathcal{P}$. This notation will be kept throughout this paper.

Our main result is the following extension of Theorem 1.3.

Theorem 2.1. *Let b be a fixed nonzero integer. The Diophantine equation*

$$A(a^{x_1} - a^{x_2}) = B(b^{y_1} - b^{y_2}), \tag{5}$$

in positive integers $A,\ B,\ a,\ x_1,\ x_2,\ y_1,\ y_2$ has only finitely many solutions $(A,\ B,\ a, x_1, x_2, y_1, y_2)$ with $x_1 \neq x_2$, a prime, $A,\ B \in \mathcal{S}$ and $\gcd(Aa, Bb) = 1$.

We display two immediate corollaries concerning equation (1).

Corollary 2.2. *Let b be a fixed positive integer. There exists a positive constant a_0 depending only on b and $\mathcal{S}$ such that for any nonzero integer c, for any prime $a \geq a_0$, and for every positive integers $A,\ B$ in $\mathcal{S}$ coprime to c, the equation*

$$Aa^x - Bb^y = c,$$

in positive integers $x,\ y$ has at most one solution.

Corollary 2.3. *Let b be a fixed positive integer. There exists a positive constant c_0 depending only on b and $\mathcal{S}$ such that for any prime $a \geq 2$, and for any integer $c \geq c_0$ coprime to a, and for every coprime integers $A,\ B$ in $\mathcal{S}$, the equation*

$$Aa^x - Bb^y = c,$$

in positive integers $x,\ y$ has at most one solution.

Besides the introduction of the coefficients A and B, the important new point in Corollary 2.2 (resp. Corollary 2.3) is that the constant a_0 (resp. c_0) does not depend on c (resp. a).

The proof of Theorem 2.1 follows the same general lines as that of Theorem 1 from [8]. However, there are many additional difficulties since b is no longer prime and since the coefficients A, B are not even fixed. To overcome some of these difficulties, we are led to use the Schmidt Subspace Theorem instead of Ridout's Theorem.

We have tried to clearly separate the different steps of the proof of Theorem 2.1 and to point out where our assumptions on a and b are needed. A short discussion on possible extensions to our theorem is given in Section 6.

Throughout this paper, we use the symbols 'O', '$\ll$', '$\gg$', '$\asymp$' and 'o' with their usual meaning (we recall that $A \ll B$ and $B \gg A$ are equivalent to $A = O(B)$ and that $A \asymp B$ means that both $A \gg B$ and $B \gg A$ hold).

3 Preparations

In this Section, we review some standard notions of Diophantine approximation.

For a prime number p and a nonzero rational number x, we denote by $\mathrm{ord}_p(x)$ the order at which p appears in the factorization of x.

Let $\mathcal{M} = \{2, 3, 5, \dots\} \cup \{\infty\}$ be all the places of $\mathbb{Q}$. For a nonzero rational number x and a place μ in $\mathcal{M}$, we let the *normalized μ-valuation of x*, denoted by $|x|_\mu$, be $|x|_\mu = |x|$ if $\mu = \infty$, and $|x|_\mu = p^{-\mathrm{ord}_p(x)}$ if $\mu = p$ is finite.

These valuations satisfy the *product formula*

$$\prod_{\mu \in \mathcal{M}_{\mathbb{L}}} |x|_\mu = 1, \qquad \text{for all } x \in \mathbb{Q}^*.$$

Our basic tool is the following simplified version of a result of Schlickewei (see [15], [16]), which is commonly known as the Schmidt Subspace Theorem.

Lemma 3.1. *Let $\mathcal{P}'$ be a finite set of places of $\mathbb{Q}$ containing the infinite place. For any $\mu \in \mathcal{P}'$, let $\{L_{1,\mu}, \dots, L_{N,\mu}\}$ be a set of linearly independent linear forms in N variables with coefficients in $\mathbb{Q}$. Then, for every fixed $0 < \varepsilon < 1$, the set of solutions $\mathbf{x} = (x_1, \dots, x_N) \in \mathbb{Z}^N \setminus \{0\}$ to the inequality*

$$\prod_{\mu \in \mathcal{P}'} \prod_{i=1}^{N} |L_{i,\mu}(\mathbf{x})|_\mu < \max\{|x_i| \ : \ i = 1, \dots, N\}^{-\varepsilon} \tag{6}$$

is contained in finitely many proper linear subspaces of $\mathbb{Q}^N$.

Let $\mathcal{P}$ and $\mathcal{S}$ be as in Section 2. An $\mathcal{S}$*-unit* x is a nonzero rational number such that $|x|_w = 1$ for every finite valuation w stemming for a prime outside $\mathcal{P}$. We shall need the following version of a theorem of Evertse [5] on $\mathcal{S}$-unit equations.

Lemma 3.2. *Let $a_1, \ldots, a_N$ be nonzero rational numbers. Then the equation*

$$\sum_{i=1}^{N} a_i u_i = 1$$

in $\mathcal{S}$-unit unknowns u_i for $i = 1, \ldots, N$, and such that $\sum_{i \in I} a_i u_i \neq 0$ for each nonempty proper subset $I \subset \{1, \ldots, N\}$, has only finitely many solutions.

Finally, we will need lower bounds for linear forms in p-adic logarithms, due to Yu [21], and for linear forms in complex logarithms, due to Matveev [9].

Lemma 3.3. *Let p be a fixed prime and $a_1, \ldots, a_N$ be fixed rational numbers. Let $x_1, \ldots, x_N$ be integers such that $a_1^{x_1} \ldots a_N^{x_N} \neq 1$. Let $X \geq \max\{|x_i| : i = 1, \ldots, N\}$, and assume that $X \geq 3$. Then,*

$$\operatorname{ord}_p \left(a_1^{x_1} \ldots a_N^{x_N} - 1 \right) \ll \log X,$$

where the constant implied by $\ll$ depends only on $p, N, a_1, \ldots, a_N$.

Lemma 3.4. *Let $a_1, \ldots, a_N$ be fixed rational numbers and, for $1 \leq i \leq N$, let $A_i \geq 3$ be an upper bound for the numerator and for the denominator of a_i, written in its lowest form. Let $x_1, \ldots, x_N$ be integers such that $a_1^{x_1} \ldots a_N^{x_N} \neq 1$. Let*

$$X \geq \max \left\{ \frac{|x_N|}{\log A_i} + \frac{|x_i|}{\log A_N} : i = 1, \ldots, N-1 \right\},$$

and assume that $X \geq 3$. Then,

$$\log |a_1^{x_1} \ldots a_N^{x_N} - 1| \gg -(\log A_1) \ldots (\log A_n)(\log X),$$

where the constant implied by $\gg$ depends only on N.

4 Preliminary Results

Let $\mathcal{P}$ and $\mathcal{S}$ be as in Section 2.

We start with the following result regarding the size of the coefficient A in equation (5).

Lemma 4.1. *Assume that the Diophantine equation*

$$A(a^{x_1} - a^{x_2}) = B(q^{y_1} - q^{y_2}) \tag{7}$$

admits infinitely many positive integer solutions $(A,\ B,\ a,\ q,\ x_1,\ x_2,\ y_1,\ y_2)$ *such that* A, B, q *in* $\mathcal{S}$*,* $x_1 > x_2$*,* $y_1 > y_2$*,* $a > 1$*, and* $\gcd(Aa, Bq) = 1$*. Let* M *be the common value of the number appearing in either side of equation* (7)*. We then have* $A = M^{o(1)}$ *as* $\max\{A, B, q, x_1, x_2, y_1, y_2\}$ *tends to infinity.*

Proof. Let $q = \prod_{p\in\mathcal{P}} p^{z_p}$ and let $Z = \max\{3, z_p : p \in \mathcal{P}\}$. Assume that $p^{a_p}||A$. Since Aa and Bq are coprime, it follows that $p^{a_p}|(q^{y_1-y_2} - 1)$. By Lemma 3.3, we have that

$$a_p \ll \log(Zy_1).$$

Since this is true for all $p \in \mathcal{P}$, it follows that

$$\begin{aligned} \log A &= \sum_{p\in\mathcal{P}} a_p \log p \ll \log(Zy_1) \ll \log(q^{y_1}) \left(\frac{\log(Zy_1)}{Zy_1}\right) \\ &\ll (\log M)\left(\frac{\log(Zy_1)}{Zy_1}\right). \end{aligned} \tag{8}$$

Thus, it suffices to show that $Zy_1 \to \infty$ when $M \to \infty$. Suppose, on the contrary, that Zy_1 remains bounded for infinitely many solutions. Then, we may assume that q and y_1 are fixed, and, since $y_1 > y_2$, we may assume that y_2 is fixed as well. Since $Aa^{x_2}|q^{y_1-y_2} - 1$, it follows that we may further assume that a and A are fixed. It then follows that the largest prime factor of $a^{x_1-x_2} - 1$ remains bounded. However, $(a^n - 1)_{n\geq 1}$ is a non-degenerate binary recurrent sequence, and it is known that $P(a^n - 1)$ tends to infinity with n (in fact, by the well-known properties of primitive divisors to Lucas sequences, see e.g. [4] and [3], $P(a^n - 1) \geq n + 1$ holds for all $a > 1$ and $n \geq 7$). Hence, $x_1 - x_2$ is bounded as well, contradicting the fact that M tends to infinity. □

We can now present the following theorem.

Theorem 4.2. *Let* $m > n > 0$ *be fixed positive integers. Then, the Diophantine equation*

$$A(z^m - z^n) = B(q^{y_1} - q^{y_2}) \tag{9}$$

has only finitely many positive integer solutions (A, B, z, q, y_1, y_2) *with* $z > 1$ *and* $A,\ B,\ q$ *in* $\mathcal{S}$ *such that* $\gcd(Az, Bq) = 1$.

Proof. We assume that the given equation has infinitely many solutions. We write again M for the common value of the two sides in equation (9). Thus, we assume that M tends to infinity. By Lemma 4.1, it follows that we may assume that $A = M^{o(1)}$. In particular, $A = z^{o(1)}$ because $M \asymp Az^m$, m is fixed and z tends to infinity. From equation (9), we now conclude that $z^{m(1+o(1))} \asymp Bq^{y_1}$. This observation will be used several times in the course of the present proof.

We now prove a Lemma about solutions of equation (9) of a certain type.

Lemma 4.3. *Let $c_0 \neq 1$ be a fixed rational number. Then there exist only finitely many solutions of equation* (9) *with $z = s + c_0$ and s a rational number which is a $\mathcal{S}$-unit.*

Proof. We assume again, for a contradiction, that we have infinitely many such solutions. Since z is an integer, it follows that the denominator of s is $\ll 1$. If $c_0 = 0$, it follows that $z \in \mathcal{S}$. In this case, equation (9) is the $\mathcal{S}$-unit equation

$$X_1 + X_2 + X_3 + X_4 = 0,$$

where $X_1 = Az^m,\ X_2 = -Az^n,\ X_3 = -Bq^{y_1}$ and $X_4 = -By^{y_2}$. Since $z > 1$ and $\gcd(Az, Bq) = 1$, it follows that it is non-degenerate. In particular, it can have only finitely many solutions (A, B, z, q, y_1, y_2). Assume now that $c_0 \neq 0$. Equation (9) can be rewritten as

$$Q(s) = q^{y_1}B/A - q^{y_2}B/A,$$

where $Q(s)$ is a polynomial in s whose constant term is $d_0 = c_0^n(c_0^{m-n} - 1) \neq 0$. Dividing both sides of the above equation by d_0 and rearranging some terms, it follows that the above equation can be rewritten as

$$\sum_{i=1}^{m+2} a_i X_i = 1, \tag{10}$$

where $a_1 = 1/d_0 \neq 0,\ a_2 = -1/d_0 \neq 0,\ a_i$ are fixed rational numbers for $i = 3, \ldots, m+2,\ X_1 = q^{y_1}B/A,\ X_2 = -q^{y_2}B/A$, and $X_i = s^{i-2}$ for $i \in \{3, \ldots, m+2\}$. Let $\mathcal{I} \subset \{1, 2, \ldots, m+2\}$ be the subset of those indices i such that $a_i \neq 0$. Equation (10) is an $\mathcal{S}$-unit equation in the variables X_i for $i \in \mathcal{I}$. Let $\mathcal{J}$ be the subset of $\mathcal{I}$ (which can be the full set $\mathcal{I}$) such that

$$\sum_{j \in \mathcal{J}} a_j X_j = 1 \tag{11}$$

is non-degenerate; i.e., has the property that if $\mathcal{K}$ is any nonempty proper subset of $\mathcal{J}$, then $\sum_{k\in\mathcal{K}} a_k X_k \neq 0$. It is clear that for each solution of equation (10) such a subset $\mathcal{J}$ exists. Since we have infinitely many solutions, we may assume that $\mathcal{J}$ is fixed. By Lemma 3.2, it follows that equation (11) admits only finitely many solutions $(X_j)_{j\in\mathcal{J}}$. If $1 \in \mathcal{J}$, then $q^{y_1}B/A$ takes only finitely many values, and since $\gcd(Bq, A) = 1$, it follows that A, B, q, y_1 are all bounded. Since $y_1 > y_2$, we get that y_2 is bounded as well. Hence, M is bounded in this case. If $i \in \mathcal{J}$ for some $i \geq 3$, it follows that s^{i-2} is bounded. Hence, z is bounded, which is a contradiction. Finally, if $\mathcal{J} = \{2\}$, then $-q^{y_2}B/A$ is fixed. Hence, we may assume that A, B, q, y_2 are all fixed. With $C = q^{y_2}B/A$, we get $z^m - z^n + C = q^{y_1}B/A$. One verifies immediately that if $m \geq 3$ or if $(m, n) = (2, 1)$ and $C \neq 1/4$, then the polynomial $R(z) = z^m - z^n + C$ has at least two distinct roots. It is known that if $Q(X) \in \mathbb{Q}[X]$ is a polynomial which has at least two distinct roots, then $Q(x)$ is a rational number whose denominator has the property that its largest prime factor tends to infinity with x (see e.g. [20]). This shows that the equation $R(z) = q^{y_1}B/A$ can have only finitely many solutions (z, y_1) in this case as well. Hence, it remains to look at the case $(m, n) = (2, 1)$ and $C = 1/4$. But since $\gcd(Bq, A) = 1$, this leads to $A = 4,\ B = 1,\ q = 1$, which is impossible because in this case $M = 0$; hence, $z = 1$, which is not allowed.

$\square$

We now resume the proof of Theorem 4.2. We rewrite the equation as

$$Az^n(z^{m-n} - 1) = Bq^{y_2}(q^{y_1-y_2} - 1). \tag{12}$$

Since z and q are coprime, it follows that Bq^{y_2} divides $z^{m-n} - 1$.

We first assume that $m \geq 3$. If $n = m - 1$, then $Bq^{y_2}|(z - 1)$, which implies that $Bq^{y_2} \ll z$. Equation (9), after multiplying both sides of it by m^m, can be rewritten as

$$|A(mz - 1)^m - Bm^m q^{y_1}| = |Af(z) - Bm^m q^{y_2}|, \tag{13}$$

where $f(z)$ is a polynomial in z with integer coefficients and of degree $m-2$. We now write $q = dq_1^m,\ A = A_1A_0^m,\ B = B_1B_0^m$, where d, A_1, B_1 are mth power free. Clearly, since $A, B, q \in \mathcal{S}$ and m is fixed, d, A_1, B_1 can take only finitely many values. In what follows, we assume that d, A_1, B_1 are fixed. Equation (13) implies easily that

$$\Big|\frac{A_0(mz - 1)}{B_0 q_1^{y_1}} - m(dB_1/A_1)^{1/m}\Big| \ll \frac{Az^{m-2}}{Bq^{y_1}} \ll \frac{1}{z^2}, \tag{14}$$

when M is sufficiently large. Since B_0q_1 is in $\mathcal{S}$, Ridout's Theorem [14] tells us that the above inequality (14) can have only finitely many solutions (A_0, B_0, z, q_1, y_1) if $(dB_1/A_1)^{1/m}$ is not rational. Indeed, recall that — a particular version of — Ridout's Theorem says that if α is algebraic and irrational, then for every $\varepsilon > 0$, the Diophantine inequality

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{1+\varepsilon}}$$

has only finitely many integer solutions (p, q) with $q \in \mathcal{S}$. However, for us, if $dB_1/A_1 = c_1^m$ for some rational number m, then for large z the above inequality (14) leads to the conclusion that $A_0(mz-1) - mB_0c_1q_1^{y_1} = 0$, which gives $z = s + c_0$, where $s = c_1B_0q_1^{y_1}/A_0$, and $c_0 = 1/m \neq 1$. However, by Lemma 4.3, equation (9) can have only finitely many solutions of this type also.

We now assume that $m - n \geq 2$. If $n \geq 2$, then $Bq^{y_2} | z^{m-n} - 1$, therefore $Bq^{y_2} \leq z^{m-2}$. Hence,

$$|Az^m - Bq^{y_1}| = |Az^n - Bq^{y_2}| \ll z^{(m-2)+o(1)}.$$

With the notation $q = dq_1^m, A = A_1A_0^m, B = B_1B_0^m$, we get

$$\left|\frac{A_0z}{B_0q_1^{y_1}} - (dB_1/A_1)^{1/m}\right| \ll \frac{Az^{m-2}}{Bq^{y_1}} \ll \frac{1}{z^2},$$

and Ridout's Theorem implies once again that the above inequality can have only finitely many positive integer solutions (A_0, B_0, z, q_1, y_1) with $A_0, B_0, q_1 \in \mathcal{S}$ unless $dB_1/A_1 = c_1^m$ for a rational number c_1. If $dB_1/A_1 = c_1^m$, we then get for large z that $z = c_1q_1^{y_1}B_0/A_0 = s \in \mathcal{S}$, and equation (9) has only finitely many solutions of this type by Lemma 4.3.

We now assume that $n = 1$. We then write

$$z^{m-1} - 1 = (z-1)\left(\frac{z^{m-1}-1}{z-1}\right),$$

and note that

$$\gcd\left(z-1, \frac{z^{m-1}-1}{z-1}\right) \Bigm| m-1.$$

From equation (12), it follows that we may write $B = B_2B_3$, $q = q_2q_3$,

$$z - 1 = B_2q_2^{y_2}u \qquad \text{and} \qquad \frac{z^{m-1}-1}{z-1} = B_3q_3^{y_2}v,$$

where B_2, B_3, q_2, q_3 are positive integers and $u,\ v$ are positive rational numbers with bounded denominators. Let $\delta > 0$ be some small number to be fixed later. If either

$$u > z^{\delta} \qquad \text{or} \qquad v > z^{\delta},$$

then either

$$B_2 q_2^{y_2} < z^{1-\delta} \qquad \text{or} \qquad B_3 q_3^{y_2} \ll z^{m-2-\delta},$$

and in both cases we have that $Bq^{y_2} = B_2B_3(q_2q_3)^{y_2} \ll z^{m-1-\delta}$. We now get that

$$|Az^m - Bq^{y_1}| = |Az - Bq^{y_2}| \ll z^{m-1-\delta},$$

and again with the notations $q = dq_1^m,\ A = A_1A_0^m,\ B = B_1B_0^m$ we arrive at

$$\Big|\frac{A_0 z}{B_0 q_1^{y_1}} - (dB_1/A_1)^{1/m}\Big| \ll \frac{z^{m-1-\delta}}{Bq^{y_1}} \ll \frac{1}{z^{1+\delta+o(1)}} \ll \frac{1}{z^{1+\delta/2}}.$$

Here, we used the fact that δ is fixed and that $A = z^{o(1)}$. Since $\delta > 0$ is fixed, Ridout's Theorem implies once again that the above inequality can have only finitely many positive integer solutions (A_0, B_0, z, q_1, y_1) with $B_0, q_1 \in \mathcal{S}$ unless $dB_1/A_1 = c_1^m$ for some rational number c_1, and as we have already seen, when this last condition holds, then for large z, we get that $z = q_1^{y_1}B/A = s \in \mathcal{S}$, and there can be only finitely many solutions of this type by Lemma 4.3.

From now on, we consider only those solutions for which both inequalities

$$u < z^{\delta} \qquad \text{and} \qquad v < z^{\delta}$$

hold. Write $D \ll 1$ for the least common multiple of the denominators of u and v. Note that the greatest prime divisor of D is at most m. We now get

$$B_3 q_3^{y_2} v = \frac{z^{m-1}-1}{z-1} = \frac{(B_2q_2^{y_2}u+1)^{m-1}-1}{B_2q_2^{y_2}u} = \sum_{k=1}^{m-1}\binom{m-1}{k}\left(B_2q_2^{y_2}u\right)^{k-1},$$

which can be rewritten as

$$-(m-1)D^{m-2} = -B_3q_3^{y_2}vD^{m-2} + \sum_{k=2}^{m-1}\binom{m-1}{k}B_2^{(k-1)}q_2^{(k-1)y_2}u^{k-1}D^{m-2}. \tag{15}$$

We now apply Lemma 3.1 to (15). Put $N = m-1,\ \mathcal{P}' = \mathcal{P}\cup\{\infty\}$. Let $\mathbf{x} = (x_1, \ldots, x_N) \in \mathbb{Q}^N$. For all $\mu \in \mathcal{P}'$ and all $i = 1, \ldots, N$ we set

$L_i(\mathbf{x}) = x_i$ except for $(i,\mu) = (1,\infty)$, for which we put

$$L_{1,\infty} = -x_1 + \sum_{k=2}^{m-1} \binom{m-1}{k} x_k.$$

We evaluate the double product appearing at inequality (6) for our system of forms and points $\mathbf{x} = (x_1, \dots, x_N)$ given by $x_1 = B_3 q_3^{y_2} v D^{m-2}$ and $x_k = B_2^{(k-1)} q_2^{(k-1)y_2} u^{k-1} D^{m-2}$ for $k = 2, \dots, m-1$. It is clear that $x_i \in \mathbb{Z}$ for $i = 1, \dots, N$. We may also enlarge $\mathcal{P}$ in such a way as to contain all the primes $p \le m$. Clearly,

$$\prod_{\mu \in \mathcal{P}'} |L_k(\mathbf{x})|_\mu \le u^{k-1} \qquad \text{for } k \ge 2,$$

$$\prod_{\mu \in \mathcal{P}} |L_1(\mathbf{x})|_\mu \le \frac{1}{B_3 q_3^{y_2}},$$

and

$$|L_1(\mathbf{x})|_\infty = (m-1) D^{m-2}.$$

Thus,

$$\prod_{\mu \in \mathcal{P}'} \prod_{i=1}^{N} |L_i(\mathbf{x})|_\mu \le \frac{(m-1) D^{m-2} u^{N^2}}{B_3 q_3^{y_2}} \ll \frac{(z^\delta)^{m^2}}{z^{m-1-\delta}} = \frac{1}{z^{m-1-\delta(m^2+1)}}. \qquad (16)$$

We now observe that

$$\max\{|x_i| : i = 1, \dots, N\} = B_3 q_3^{y_2} v D^{m-2} \ll z^{m-2},$$

therefore inequality (16) implies that

$$\prod_{\mu \in \mathcal{P}'} \prod_{i=1}^{N} |L_i(\mathbf{x})|_\mu \ll (\max\{|x_i| : i = 1, \dots, N\})^{-\frac{m-1-\delta(m^2+1)}{m-2}}.$$

Choosing $\delta = \dfrac{m-1}{2(m^2+1)}$, we get that the inequality

$$\prod_{\mu \in \mathcal{P}'} \prod_{i=1}^{N} |L_i(\mathbf{x})|_\mu \ll (\max\{|x_i| : i = 1, \dots, N\})^{-\varepsilon}$$

holds with $\varepsilon = \dfrac{m-1}{2(m-2)}$. Lemma 3.1 now immediately implies that there exist only finitely many proper subspaces of $\mathbb{Q}^N$ such that each one of our points $\mathbf{x}$ lies on one of those subspaces. This leads to a equation of the form

$$\sum_{i=1}^{N} C_i x_i = 0,$$

with some integer coefficients C_i for $i = 1, \ldots, N$ not all zero, which is equivalent to

$$C_1 B_3 q_3^{y_2} v D^{m-2} + \sum_{k=2}^{m-1} C_k B_2^{k-1} q_2^{(k-1)y_2} u^{k-1} D^{m-2} = 0.$$

If $C_1 = 0$, then we divide by D^{m-2} and the above relation becomes $g(w) = 0$, where $w = B_2 q_2^{y_2} u$, and $g(X)$ is the nonzero polynomial

$$\sum_{k=2}^{m-1} C_k X^{k-1}.$$

Hence, w can take only finitely many values, and, since $w = z-1$, it follows that z can take only finitely many values. If $C_1 \neq 0$, then $w | C_1 B_3 q_3^{y_2} u D^{m-2}$. Further, the greatest common divisor of $w = z-1$ and $B_3 q_3^{y_2} v D^{m-2} = D^{m-2}(z^{m-1}-1)/(z-1)$ divides $D^{m-2}(m-1)$. Hence, this greatest common divisor is $O(1)$. It then follows that $w \ll C_1$. In particular, $w = z-1$ can take only finitely many values in this case as well.

This completes the discussion for the case when $m \geq 3$. We now deal with the case $(m,n) = (2,1)$. In this last case, we have

$$Az(z-1) = Bq^{y_2}(q^{y_1-y_2}-1).$$

Since Bq and Az are coprime, we get $z-1 = Bq^{y_2}\lambda$ for some positive integer λ. Hence,

$$\frac{q^{y_1-y_2}-1}{A\lambda} = z = Bq^{y_2}\lambda + 1,$$

therefore $q^{y_1-y_2} - AB\lambda^2 q^{y_2} = A\lambda + 1$. We let δ be some small positive number, and we show that the above equation has only finitely many solutions with $A\lambda < (Bq^{y_2})^{1-\delta}$. Indeed, assume that this is not the case. We then take $N = 2$, $\mathcal{P}' = \mathcal{P} \cup \{\infty\}$, and $L_{i,\mu}(X_1, X_2) = X_i$ for all $(i,\mu) \in \{1,2\} \times \mathcal{P}'$, except for $(i,\mu) = (2,\infty)$, case in which we put $L_{2,\infty}(X_1,X_2) = X_1 - X_2$.

It is easy to see that $L_{1,\mu}$ and $L_{2,\mu}$ are linearly independent for all $\mu \in \mathcal{P}'$. Taking $x_1 = q^{y_1 - y_2}$ and $x_2 = AB\lambda^2$, we get easily that

$$\prod_{i=1}^{2} \prod_{\mu \in \mathcal{P}'} |L_{i,\mu}(x_1, x_2)|_\mu = \frac{A\lambda + 1}{ABq^{y_2}} \ll \frac{1}{(Bq^{y_2})^\delta}.$$

Furthermore, since $A\lambda < (Bq^{y_2})^{1-\delta}$, it follows that

$$A\lambda^2 Bq^{y_2} \le (A\lambda)^2 (Bq^{y_2}) \le (Bq^{y_2})^{2(1-\delta)+1},$$

and

$$q^{y_1 - y_2} = AB\lambda^2 q^{y_2} + A\lambda + 1 \le 2AB\lambda^2 q^{y_2} \ll (Bq^{y_2})^{3-2\delta}.$$

Hence,

$$\prod_{i=1}^{2} \prod_{\mu \in \mathcal{P}'} |L_{i,\mu}(x_1, x_2)|_\mu \ll (\max\{x_1, x_2\})^{-\frac{\delta}{3-2\delta}}.$$

Applying Lemma 3.1, it follows that once δ is fixed there are only finitely many choices for the ratio x_1/x_2. In particular, $q^{y_1 - 2y_2}/(AB\lambda^2)$ can take only finitely many values. Enlarging $\mathcal{P}$, if needed, it follows that we may assume that λ is also an $\mathcal{S}$-unit. In this case, the equation $q^{y_1 - y_2} - AB\lambda^2 q^{y_2} = A\lambda + 1$ becomes a $\mathcal{S}$-unit equation which is obviously non-degenerate, therefore it has only finitely many solutions $(A, B, q, \lambda, y_1, y_2)$. Hence, there are only finitely many solutions of equation (9) which satisfy the above property. From now on, we assume that $A\lambda > (Bq^{y_2})^{1-\delta}$ with some small δ. We now set $\delta = 1/2$ and get that

$$z = Bq^{y_2}\lambda + 1 \gg (Bq^{y_2})^{2-\delta} A^{-1} \ge (Bq^{y_2})^{3/2} z^{o(1)}.$$

Thus, $Bq^{y_2} \ll z^{2/3+o(1)} < z^{3/4}$. We now write again $q = dq_1^2$, $A = A_1 A_0^2$, $B = B_1 B_0^2$ and rewrite equation (9) as

$$|A_1(A_0(2z-1))^2 - 4dB_1 B_0^2 q_1^{2y_1}| = |4Bq^{y_2} - A| \ll z^{3/4},$$

which gives

$$\left| \frac{A_0(2z-1)}{B_0 q_1^{y_1}} - 2(dB_1/A_1)^{1/2} \right| \ll \frac{z^{3/4}}{Bq^{y_1}} \ll \frac{1}{z^{5/4}}.$$

Ridout's Theorem implies once again that the above inequality can have only finitely many positive integer solutions (A_0, B_0, z, q_1, y_1) with $q_1 \in \mathcal{S}$ unless $dB_1/A_1 = c_1^m$ with some rational number m. In this last case, for large z we get that $z = s + c_0$, where $s = c_1 q_1^{y_1} B_0/A_0 \in \mathcal{S}$ and $c_0 = 1/2 \neq 1$, and there are only finitely many solutions of this kind by Lemma 4.3. $\square$

5 Proof of Theorem 2.1

We follow the method of proof of Theorem 1 from [8].

We assume that b is not a perfect power of some integer and that $x_1 > x_2$. Thus, $y_1 > y_2$. We also assume that equation (5) has infinitely many positive integer solutions $(A, B, a, x_1, x_2, y_1, y_2)$ with a prime, A, B in $\mathcal{S}$, $\gcd(Aa, Bb) = 1$ and $x_1 > x_2$. We shall eventually reach a contradiction.

Note that, if $x_1 \ll 1$ holds for all such solutions, then the contradiction will follow from Theorem 4.2. Hence, it suffices to show that $x_1 \ll 1$. In Steps 1 to 3, we will establish that, if x_1 and y_1 are sufficiently large, then there exists $\delta > 0$, depending only on b, such that all the solutions of equation (5) have

$$\max\{x_2/x_1, y_2/y_1\} < 1 - \delta. \tag{17}$$

Then, in Step 4, we adapt the argument used at Step 4 of the proof of Theorem 1 from [8], based on a result of Shorey and Stewart from [19], to get that $x_1 \ll 1$.

We already know that $A = M^{o(1)}$. We shall show that $B = M^{o(1)}$ as well. Let $p^{b_p} || B$. Then $p^{b_p} | a^{x_1 - x_2} - 1$. It is known that $b_p \le \log(a^2 - 1) + O(\log(x_1 - x_2)) \ll \log a + \log x_1 \ll (\log a)(\log x_1)$. Hence,

$$\log B = \sum_{p \in \mathcal{P}} b_p \log p \ll (\log a)(\log x_1) = \log(a^{x_1}) \left(\frac{\log x_1}{x_1} \right),$$

therefore $B = M^{o(1)}$ because $A = M^{o(1)}$ and x_1 tends to infinity.

We now proceed in several steps.

Step 1. *The case a is fixed.*

In this case, equation (5) is a particular case of an $\mathcal{S}$-unit equation in four terms, which is obviously non-degenerate. In particular, there are only finitely many such solutions. These solutions are even effectively computable by using the theory of lower bounds for linear forms in logarithms, like in [11].

From now on, by Step 1, we may assume that $a > b^2$. Since

$$b^{2x_1} \ll \frac{1}{2} a^{x_1} < a^{x_1 - 1}(a - 1) \le a^{x_1} - a^{x_2} = (b^{y_1} - b^{y_2})B/A < b^{y_1(1+o(1))}, \tag{18}$$

we get that $x_1 < y_1$.

Moreover, inequality (18) shows that there are only finitely many solutions $(A, B, a, x_1, y_1, x_2, y_2)$ of equation (5) with bounded y_1, and so, from now on, we shall assume that y_1 is as large as we wish.

Step 2. *There exists a constant $\delta_1 > 0$ depending only b such that the inequality $y_2 < y_1(1-\delta_1)$ holds for large values of y_1.*

For positive integers m and r, with r a prime number, we write $\mathrm{ord}_r(m)$ for the exact order at which the prime r divides m. We write $b = \prod_{i=1}^{t} r_i^{\beta_i}$, where $r_1 < r_2 \cdots < r_t$ are distinct primes and β_i are positive integers for $i = 1, \ldots, t$. Rewriting equation (5) as

$$a^{x_2}(a^{x_1-x_2}-1) = b^{y_2}(b^{y_1-y_2}-1)B/A, \tag{19}$$

we recognize that $\beta_i y_2 \le \mathrm{ord}_{r_i}(a^{x_1-x_2}-1)$. Let f_i be the following positive integer: If r_i is odd, we then let f_i be the multiplicative order of a modulo r_i. If $r_i = 2$, and $x_1 - x_2$ is odd, we then let $f_i = 1$, and if $x_1 - x_2$ is even, we then let $f_i = 2$. Since $y_2 > 0$, it is clear that $f_i | x_1 - x_2$. We write $u_i = \mathrm{ord}_{r_i}(a^{f_i} - 1)$. We then have

$$\begin{aligned} \beta_i y_2 &\le \mathrm{ord}_{r_i}(a^{x_1-x_2}-1) \le u_i + \mathrm{ord}_{r_i}\left(\frac{x_1-x_2}{f_i}\right) \\ &\le u_i + \frac{\log(x_1-x_2)}{\log r_i} < u_i + \frac{\log y_1}{\log r_i}. \end{aligned} \tag{20}$$

For a positive integer m, we write $F_m(X) = \Phi_m(X) \in \mathbb{Z}[X]$ for the mth cyclotomic polynomial if $m \ge 3$ and $F_m(X) = X^m - 1$ for $m = 1, 2$. From the definition of f_i and u_i, we have that

$$r_i^{u_i} | F_{f_i}(a).$$

Let $\mathcal{F} = \{f_i : i = 1, \ldots, t\}$, and let $\ell = \#\mathcal{F}$. Observe that

$$\begin{aligned} M^{o(1)} b^{y_1} &= (b^{y_1} - b^{y_2})B/A = a^{x_2}(a^{x_1-x_2}-1) \ge a \prod_{f \in \mathcal{F}} F_f(a) \\ &= \prod_{f \in \mathcal{F}} \left(a^{1/\ell} F_f(a)\right). \end{aligned} \tag{21}$$

For $f \in \mathcal{F}$, we put $d_f = \deg(F_f)$. Hence, $d_f = f$ if $f \le 2$, and $d_f = \phi(f)$ otherwise, where ϕ is the Euler function. We now remark that

$$a^{1/\ell} F_f(a) \gg F_f(a)^{\frac{\ell d_f + 1}{\ell d_f}}. \tag{22}$$

Indeed, since $\ell \le t = \omega(b)$ is bounded, the above inequality is equivalent to

$$a^{d_f} \gg F_f(a).$$

Since all the roots of $F_f(X)$ are roots of unity, the above inequality is implied by

$$a^{d_f} \gg (a+1)^{d_f},$$

which is equivalent to

$$\left(1+\frac{1}{a}\right)^{d_f} \ll 1.$$

In turn, this last inequality follows from the fact that $d_f \le f$ together with the fact that $f_i | r_i - 1$ whenever $r_i > 2$ by Fermat's Little Theorem. Let $d = \max\{d_f : f \in \mathcal{F}\}$. Inequalities (21), (22) and (20) show that

$$\begin{aligned} b^{y_1(1+o(1))} &\gg \left(\prod_{f\in\mathcal{F}} F_f(a)\right)^{\frac{\ell d+1}{\ell d}} \gg \left(\prod_{i=1}^{t} r_i^{u_i}\right)^{\frac{\ell d+1}{\ell d}} \\ &\gg \left(\prod_{i=1}^{t} \frac{r_i^{\beta_i y_2}}{y_1}\right)^{\frac{\ell d+1}{\ell d}} \gg \frac{b^{\left(\frac{\ell d+1}{\ell d}\right) y_2}}{y_1^{2t}}, \end{aligned}$$

therefore

$$y_1(1+o(1)) > \left(\frac{\ell d+1}{\ell d}\right) y_2 - 2t \log y_1 + O(1),$$

and so,

$$y_2 < \left(\frac{\ell d}{\ell d+1}\right) y_1(1+o(1)) + O(\log y_1) = \left(\frac{\ell d}{\ell d+1}\right) y_1(1+o(1)),$$

which implies the assertion of Step 2 with $\delta_1 = 1/(2\ell d)$ once y_1 is sufficiently large.

Step 3. *There exists a constant $\delta_2 > 0$ depending only on b such that the inequality $x_2 < (1-\delta_2)x_1$ holds for large values of y_1.*

We look again at equation (19). We put $z = y_1 - y_2$, and we notice that, by Step 2, the inequality $z/y_1 \gg 1$ holds for all positive integer solutions of equation (5), with a a prime not dividing b, and $x_1 > x_2$. From equation (19), we learn that $x_2 = \mathrm{ord}_a(b^z - 1)$. We let g be the multiplicative order of b modulo a. It then follows that $a|\Phi_g(b)$. Furthermore, if we put $v = \mathrm{ord}_a(\Phi_g(b))$, we then have that

$$\begin{aligned} x_2 &= \mathrm{ord}_a\left(a^{x_2}(a^{x_1-x_2}-1)\right) = \mathrm{ord}_a\left(b^{y_2}(b^{y_1-y_2}-1)\right) - \mathrm{ord}_a(A) \\ &\leq \mathrm{ord}_a(b^z-1) = v + O\left(\frac{\log z}{\log a}\right). \end{aligned}$$

Consequently,

$$\frac{b^z-1}{a^{x_2}} \geq \frac{b^z-1}{z^{O(1)}\Phi_g(b)}.$$

Since $g|z$, and since

$$\Phi_z(m) = m^{\phi(z)+O(\tau(z))}$$

holds for all positive integers m, where $\tau(z)$ is the number of divisors of z (see [4]), we get that

$$\frac{b^z-1}{a^{x_2}} \geq b^{z-\phi(g)+O(\tau(z)+\log z)} = b^{z-\phi(g)+O(z^{1/2})},$$

where we used the well-known fact that $\tau(z) \ll z^{1/2}$. Note that since $z/y_1 \gg 1$ and since y_1 is as large as we wish, it follows that z_1 is as large as we wish. Since

$$b^{z-\phi(g)+O(\tau(z))} \leq \frac{b^z-1}{a^{x_2}} = M^{o(1)}\left(\frac{a^{x_1-x_2}-1}{b^{y_2}}\right) = b^{o(z)}\left(\frac{a^{x_1-x_2}-1}{b^{y_2}}\right),$$

it suffices to show that $z-\phi(g) \gg z$. If $g < z$, then $z-\phi(g) \geq z-g \geq z/2$. Thus, we may assume that $g = z$. Since the order of b modulo a is g, we get that $a \equiv 1 \pmod{g}$, therefore $z|a-1$. In particular, $z|b^{x_2}(b^z-1)$. The argument from the end of Step 3 of the proof of Theorem 1 in [8] shows that if we write $p(m)$ for the smallest prime factor of m, then $p(m)|b(b-1)$. Hence, $p(m) \ll 1$, therefore

$$z-\phi(g) = z-\phi(z) \geq z/p(z) \gg z,$$

which completes the proof of the assertion of Step 3.

The combination of Steps 2 and 3 shows that equation (17) holds with $\delta = \min\{\delta_1, \delta_2\}$.

Step 4. *The exponent x_1 is bounded.*

Recall that $A = M^{o(1)}$ and $B = M^{o(1)}$. It then follows from (17) that there exists a positive real number η such that

$$|AB^{-1}a^{x_1}b^{-y_1}-1| < a^{-\eta x_1}. \tag{23}$$

Write $AB^{-1} = p_1^{u_1} \dots p_t^{u_t}$. If x_1 is sufficiently large, then, for $1 \le j \le t$, we have $p_j^{|u_j|} \le a^{x_1}$; hence, $|u_j|/\log a \le 2x_1$. Furthermore, we have $y_1/\log a \ll_b x_1$. Applying Lemma 3.4, we get

$$\log |AB^{-1}a^{x_1}b^{-y_1} - 1| \gg -(\log a)(\log x_1),$$

where the constant implied in $\gg$ depends only on b and $\mathcal{P}$. Combined with (23), this gives an upper bound for x_1, in terms of b and $\mathcal{P}$. According to the observation made at the beginning of Section 5, this finishes the proof of our theorem.

6 Comments and Remarks

It would certainly be of interest to extend the results of this note in order to cover a wider class of equations of the same type as (5). For example, it would be interesting to relax the condition 'a is a prime', to, say, 'a is an integer' (or, even, to 'a has a bounded number of prime factors'), or to replace the condition 'b is fixed' by the condition 'b is an $\mathcal{S}$-unit'. We have not succeeded in proving any of such results. The most difficult point seems to lie in Step 3 of Section 5.

Furthermore, we stress that, as in [8], our results are ineffective, since they ultimately depend on the Schmidt Subspace Theorem. It would be very interesting to provide an effective version of even a weaker form of our main theorem.

Moreover, it would be nice to relax the coprimality condition occurring in Theorem 2.1. This, however, seems to be quite difficult.

We conclude by a short discussion on conditional results. Bennett [1] conjectured that there exist only finitely many triples of positive integers (a, b, c) with $\gcd(a, b, c) = 1$ such that the Diophantine equation $a^x - b^y = c$ has two solutions in positive integers x and y. In Theorem 2 in [8] it is shown that the ABC-conjecture implies that there are only finitely many such triples, subject to the additional restriction that both a and b are primes. However, a close investigation of the arguments in [8] shows that the fact that both a and b are primes is not used except for treating the case of the equation

$$z^2 - z = q^{y_1} - q^{y_2} \tag{24}$$

in positive integers (z, q, y_1, y_2) with z and q coprime. All solutions of this last equation are known if q is a prime (see Proposition 1 in [8]) but it is still an open question to decide whether (24) has only finitely many solutions if

q is allowed to be an arbitrary positive integer. Actually, it turns out that, if we assume the ABC-conjecture, then we get that equation (24) has at most finitely many solutions. This is exactly what we want to conclude that, under the ABC-conjecture, there exist only finitely many triples of positive integers (a, b, c) with $\gcd(a, b, c) = 1$ such that the Diophantine equation $a^x - b^y = c$ has two positive integer solutions (x, y). We close by pointing out that an equation related to (24), namely $x^p - x = y^q - y$, was treated by Mignotte and Pethő in [10]. For example, it is shown there that if $2 \leq p < q$ and $q \geq 4$ are fixed, then the above equation has only finitely many rational solutions (x, y). Further, the ABC conjecture is used to suggest that perhaps the above equation has only finitely many integer solutions in all four unknowns (x, y, p, q) with $2 \leq p < q$.

References

[1] M. A. Bennett, 'On some exponential equations of S.S. Pillai', *Canad. J. Math.* **53** (2001), 897–922.

[2] M. A. Bennett, 'Pillai's conjecture revisited', *J. Number Theory* **98** (2003), 228–235.

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

[4] R. D. Carmichael, 'On the numerical factors of arithmetic forms $\alpha^n \pm \beta^n$', *Ann. Math. (2)* **15** (1913), 30–70.

[5] J.-H. Evertse, 'The number of solutions of decomposable form equation', *Invent. Math.* **122** (1995), 559–601.

[6] A. Herschfeld , 'The equation $2^x - 3^y = d$,' *Bull. Amer. Math. Soc. (N. S.)* **42** no. 4 (1936), 231–234.

[7] Maohua Le, 'A note on the Diophantine equation $ax^m - by^n = k$', *Indag. Math. (N.S.)* **3** (1992), 185–191.

[8] F. Luca, 'On the diophantine equation $p^{x_1} - p^{x_2} = q^{y_1} - q^{y_2}$', *Indag. Math. (N.S.)* **14** (2003), 253–270.

[9] E. M. Matveev, 'An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II', *Izv. Ross. Akad.*

Nauk Ser. Mat. **64** (2000), 125–180. English transl. in *Izv. Math.* **64** (2000), 1217–1269.

[10] M. Mignotte, A. Pethő, 'On the Diophantine equation $x^p - x = y^q - y$', *Publ. Mat.* **43** (1999), 207–216.

[11] D. Z. Mo and R. Tijdeman, 'Exponential Diophantine equations with four terms', *Indag. Math. (N.S.)* **3** no. 1 (1992), 47–57.

[12] S. S. Pillai, 'On $a^x - b^y = c$', *J. Indian Math. Soc. (N.S.)* **2** (1936), 119–122.

[13] G. Pólya, 'Zur Arithmetische Untersuchung der Polynome', *Math. Z.* **1** (1918), 143–148.

[14] D. Ridout, 'Rational approximations to algebraic numbers', *Mathematika* **4** (1957), 125–131.

[15] W. M. Schmidt, *Diophantine Approximation*, Springer Verlag, LNM **785** (1980).

[16] W. M. Schmidt, *Diophantine Approximations and Diophantine Equations*, Springer Verlag, LNM **1467** (1991).

[17] R. Scott and R. Steyer, 'On $p^x - q^y = c$ and related three terms exponential Diophantine equations with prime bases', *J. Number Theory* **105** no. 2 (2004), 212–234.

[18] T. N. Shorey, 'On the equation $ax^m - by^n = k$', *Indag. Math.* **48** (1986), 353–358.

[19] T. N. Shorey, C. L. Stewart, 'Pure powers in recurrence sequences and some related diophantine equations', *J. Number Theory* **27** (1987), 324–352.

[20] T. N. Shorey and R. Tijdeman, *Exponential diophantine equations*, Cambridge U. Press, 1986.

[21] K. R. Yu, 'p-adic logarithmic forms and group varieties. II *Acta Arith.* **89** (1999) no. 4, 337–378.