New York Journal of Mathematics

New York J. Math. **12** (2006) 193–217.

On Pillai's Diophantine equation

Yann Bugeaud and Florian Luca

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.

Contents

1. Introduction 193
2. Results 194
3. Preparations 195
4. Preliminary results 196
5. Proof of Theorem 2.1 203
6. The ABC conjecture and the equation $a^{x_1} - a^{x_2} = b^{y_1} - b^{y_2}$ 206
7. Comments and remarks 216
References 216

1. Introduction

Let a, b and c be nonzero integers with $a \geq 2$ and $b \geq 2$. As noticed by Pólya [16], 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 [9] in the case $a = 2$, $b = 3$, and to Pillai [15] 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 $6^4 - 3^4 = 6^5 - 3^8 = 1215$.)

Received December 21, 2004.

Mathematics Subject Classification. 11D61, 11D72, 11D45.

Key words and phrases. Diophantine equations, applications of linear forms in logarithms and the Subspace Theorem, ABC conjecture.

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.

ISSN 1076-9803/06

Further results on Equation (1) are due to Shorey [21], Le [10] (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 [20] and to Bennett [1, 2]. We direct the reader to [23, 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 [20] 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 [11]. Luca's result is the following.

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. The second author also thanks Andrew Granville for enlightening conversations.

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 [11]. 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*

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

Our basic tool is the following simplified version of a result of Schlickewei (see [18], [19]), 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 $\{L_{1,\mu}, \ldots, L_{N,\mu}\}$ 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 $\mathbf{x} = (x_1, \ldots, x_N) \in \mathbb{Z}^N \backslash \{0\}$ to the inequality*

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

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 [8] 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 [24], and for linear forms in complex logarithms, due to Matveev [12].

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,*

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

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

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

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 nondegenerate 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., [6] 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* $z = s + c_0 > 1$ *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 nondegenerate. 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 nondegenerate; 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 and if x is a positive rational number with bounded denominator, then $Q(x)$ is a rational number whose numerator has the property that its largest prime factor tends to infinity with x (see, e.g., [23]). 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 (note that the denominator of z divides A which is fixed). 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. □

We now resume the proof of Theorem 4.2. We rewrite Equation (7) 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 $q = dq_1^m$, $A = A_1 A_0^m$, $B = B_1 B_0^m$, 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

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

when M is sufficiently large. Since $B_0 q_1$ is in $\mathcal{S}$, Ridout's Theorem [17] 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 $A_0(mz-1) - mB_0 c_1 q_1^{y_1} = 0$, which gives $z = s + c_0$, where $s = c_1 B_0 q_1^{y_1}/A_0$, 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 $q = dq_1^m, A = A_1 A_0^m, B = B_1 B_0^m$, we get

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

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 $z = c_1 q_1^{y_1} B_0/A_0 = s \in \mathcal{S}$, 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

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

From Equation (12), it follows that we may write $B = B_2 B_3$, $q = q_2 q_3$,

$$z - 1 = B_2 q_2^{y_2} u \qquad \text{and} \qquad \frac{z^{m-1}-1}{z-1} = B_3 q_3^{y_2} v,$$

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 $Bq^{y_2} = B_2 B_3 (q_2 q_3)^{y_2} \ll z^{m-1-\delta}$. We now get that

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

and again with the notations $q = dq_1^m,\ A = A_1 A_0^m,\ B = B_1 B_0^m$ 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

$$B_3 q_3^{y_2} v = \frac{z^{m-1} - 1}{z - 1} = \frac{(B_2 q_2^{y_2} u + 1)^{m-1} - 1}{B_2 q_2^{y_2} u} = \sum_{k=1}^{m-1} \binom{m-1}{k} (B_2 q_2^{y_2} u)^{k-1},$$

which can be rewritten as

$$-(m-1)D^{m-2} = -B_3 q_3^{y_2} v D^{m-2} + \sum_{k=2}^{m-1} \binom{m-1}{k} B_2^{(k-1)} q_2^{(k-1)y_2} u^{k-1} D^{m-2}. \tag{15}$$

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

$$\begin{aligned} x_1 &= B_3 q_3^{y_2} v D^{m-2}, \quad \text{and} \\ x_k &= B_2^{(k-1)} q_2^{(k-1)y_2} u^{k-1} D^{m-2}, \quad k = 2, \dots, m-1. \end{aligned}$$

It is clear that $x_i \in \mathbb{Z}$ for $i = 1, \ldots, N$. We may also enlarge $\mathcal{P}$ in such a way as to contain all the primes $p \le m$. Clearly,

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

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

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

Thus,

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

We now observe that

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

therefore inequality (16) implies that

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

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

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

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 an 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

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

and

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

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 nondegenerate, 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

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

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. □

5. Proof of Theorem 2.1

We follow the method of proof of Theorem 1 from [11].

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 [11], based on a result of Shorey and Stewart from [22], 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

$$b_p \leq \log(a^2 - 1) + O(\log(x_1 - x_2)) \ll \log a + \log x_1 \ll (\log a)(\log x_1).$$

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 nondegenerate. 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, as in [14].

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

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

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

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

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

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

Consequently,

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

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 [6]), we get that

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

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

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

it suffices to show that $z - \phi(g) \gg z$. If $g < z$, then $z - \phi(g) \ge z - g \ge z/2$. 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 [11] shows that if we write $p(m)$ for the smallest prime factor of m, then $p(z)|b(b-1)$. Hence, $p(z) \ll 1$, so

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

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. The *ABC* conjecture and the equation $a^{x_1} - a^{x_2} = b^{y_1} - b^{y_2}$

In this section, we discuss conditional results. Bennett [1] conjectured that there exist only finitely many triples of positive integers (a, b, c) with a and b coprime such that the Diophantine equation $a^x - b^y = c$ has two positive integer solutions (x, y). Note that if (a, b, c) is such a triple, then there exists $(x, y) \ne (x_1, y_1)$ such that

$$a^x - b^y = c = a^{x_1} - b^{y_1}.$$

Thus, we are led to a nontrivial solution $(x, y) \ne (x_1, y_1)$ of the equation

$$a^x - a^{x_1} = b^y - b^{y_1}. \tag{24}$$

In Theorem 2 in [11], it is shown that the ABC-conjecture implies that there are only finitely many positive integer solutions (a, b, x, x_1, y, y_1) with a and b coprime and $(x, y) \ne (x_1, y_1)$, subject to the additional restriction that both a and b are primes. We point out that an equation related to (24), namely $x^p - x = y^q - y$, was treated by Mignotte and Pethő in [13]. For example, it is shown there that if $2 \le p < q$ and $q \ge 4$ are fixed, then the above equation has only finitely many rational solutions (x, y). Further, the ABC conjecture is used there to suggest that perhaps the above equation has only finitely many integer solutions in all four unknowns (x, y, p, q) with $2 \le p < q$.

Here, we remove both the restrictions that a and b are coprime, as well as the arithmetic restrictions that a and b are prime in Equation (24), and we prove the following result.

Theorem 6.1. *The ABC conjecture implies that the diophantine equation*

$$a^{x_1} - a^{x_2} = b^{y_1} - b^{y_2} \tag{25}$$

has only finitely many positive integer solutions $(a, b, x_1, x_2, y_1, y_2)$ *with* $a > 1,\ b > 1,\ x_1 \ne x_2$ *and* $a^{x_1} \ne b^{y_1}$.

Recall that the ABC conjecture asserts that for every $\varepsilon > 0$ there exists a constant C_ε depending on ε such that whenever

$$A + B = C$$

with nonzero integers $A,\ B$ and C such that A and B are coprime, then

$$\max\{|A|, |B|, |C|\} \le C_\varepsilon \left(\prod_{p | ABC} p \right)^{1+\varepsilon}.$$

Proof. We may assume that $x_1 > x_2$ and that $a > b$ (in particular, $a \geq 3$). We then also get that $y_1 > y_2$. We may further assume that $\gcd(x_1, x_2) = 1$ and that $\gcd(y_1, y_2) = 1$. Indeed, for if say $\gcd(x_1, x_2) = d$, we may then write $z_1 = x_1/d$, $z_2 = x_2/d$ and $a_1 = a^d$, and note that $(a_1, b, z_1, z_2, y_1, y_2)$ is also a solution in positive integers of the given equation, and it satisfies as well the conditions $a_1 > 1$, $z_1 \neq z_2$ and $a_1^{z_1} \neq b^{y_1}$.

Note also that $x_1 \neq y_1$, for if $x_1 = y_1$, then

$$\begin{aligned}\max\{a^{x_2}, b^{y_2}\} &> |a^{x_2} - b^{y_2}| = |a^{x_1} - b^{x_1}| = |a-b|(a^{x_1-1} + \cdots + b^{x_1-1}) \\ &\geq a^{x_2} + b^{y_2},\end{aligned}$$

which is a contradiction.

Further, since

$$b^{y_1} > b^{y_1} - b^{y_2} = a^{x_1} - a^{x_2} \geq a^{x_1}\left(1 - \frac{1}{a}\right) > \frac{a^{x_1}}{2} > a^{x_1-1} > b^{x_1-1},$$

we get that $y_1 > x_1 - 1$, and since $y_1 \neq x_1$, we have $y_1 > x_1$. Thus, y_1 is the largest one of all four exponents.

We shall first show that $x_1 = O(1)$, later that $y_1 = O(1)$ and finally that a is $O(1)$.

Step 1. $x_1 = O(1)$.

Let p be a prime dividing both a and b, and put $p^{r_p} \parallel a$ and $p^{s_p} \parallel b$. It is then clear that the order at which p divides the left-hand side of Equation (25) is $p^{r_p x_2}$, while the order at which p divides the right-hand side of the same equation is $p^{s_p y_2}$. Identifying those orders we get

$$r_p x_2 = s_p y_2,$$

showing that there exists a positive integer t_p such that $r_p = t_p y_2/\gcd(x_2, y_2)$ and $s_p = t_p x_2/\gcd(x_2, y_2)$. Setting

$$c = \prod_{p \mid \gcd(a,b)} p^{t_p},$$

we get $a = a_0 c^{y_2/\gcd(x_2,y_2)}$ and $b = b_0 c^{x_2/\gcd(x_2,y_2)}$, where now a_0 and b_0 are coprime and free of primes p dividing c. Inserting the above expressions for a and b in Equation (25) and cancelling in both sides a factor of $c^{x_2 y_2/\gcd(x_2,y_2)}$, we get

$$a_0^{x_1} c^{y_2(x_1-x_2)/\gcd(x_2,y_2)} - a_0^{x_2} = b_0^{y_1} c^{x_2(y_1-y_2)/\gcd(x_2,y_2)} - b_0^{y_2}, \tag{26}$$

which we rewrite as

$$a_0^{x_2}\left(a_0^{x_1-x_2} c^{y_2(x_1-x_2)/\gcd(x_2,y_2)} - 1\right) = b_0^{y_2}\left(b_0^{y_1-y_2} c^{x_2(y_1-y_2)/\gcd(x_2,y_2)} - 1\right). \tag{27}$$

Since a_0 and b_0 are coprime, we deduce the existence of a positive integer D (note that one of a_0, b_0 or c is larger than 1 so the two sides of the above equation are nonzero) such that both equations

$$\begin{aligned} a_0^{x_1-x_2} c^{y_2(x_1-x_2)/\gcd(x_2,y_2)} - 1 &= D b_0^{y_2} \\ b_0^{y_1-y_2} c^{x_2(y_1-y_2)/\gcd(x_2,y_2)} - 1 &= D a_0^{x_2} \end{aligned} \tag{28}$$

are satisfied. In the sequel, ε denotes a very small positive real number. We now apply the ABC conjecture to each of the above equations (28) (note that the coprimality conditions are satisfied as in both cases one of the terms is -1), getting

$$Db_0^{y_2} \ll (a_0b_0cD)^{1+\varepsilon} \qquad \text{and} \qquad Da_0^{x_2} \ll (a_0b_0cD)^{1+\varepsilon},$$

which, after multiplying them side by side and cancelling a factor of D^2, lead to the inequality

$$a_0^{x_2}b_0^{y_2} \ll D^{2\varepsilon}(a_0b_0c)^3. \tag{29}$$

We now rewrite Equation (26) as

$$a_0^{x_1}c^{y_2(x_1-x_2)/\gcd(x_2,y_2)} - b_0^{y_1}c^{x_2(y_1-y_2)/\gcd(x_2,y_2)} = a_0^{x_2} - b_0^{y_2}, \tag{30}$$

and put $\{M_-,\ M_+\} = \{y_2(x_1-x_2)/\gcd(x_2,y_2),\ x_2(y_1-y_2)/\gcd(x_2,y_2)\}$, where $M_- \le M_+$. Note first that $1 \le M_- < M_+$. Indeed, if not then $x_2y_1 = x_1y_2$; hence, $x_2/x_1 = y_2/y_1$, and since $\gcd(x_2,x_1) = \gcd(y_2,y_1) = 1$, we get that $x_2 = y_2$ and $x_1 = y_1$, which we have already seen to be impossible. Note also that both sides of Equation (30) are nonzero, for if $a_0^{x_2} = b_0^{y_2}$, we then have $a^{x_2} = b^{y_2}$; hence, $a^{x_1} = b^{y_1}$, which is impossible. Equation (30) immediately implies that $c^{M_-} \mid (a_0^{x_2} - b_0^{y_2})$, so $c^{M_-} \le |a_0^{x_2} - b_0^{y_2}|$, and further, after cancelling a factor of c^{M_-} from both sides of Equation (30), we get a relation of the type

$$A - B = C, \tag{31}$$

where $C = |a_0^{x_2} - b_0^{y_2}|/c^{M_-}$, and

$$(A,B) = (a_0^{x_1}c^{M_+-M_-}, b_0^{y_1}),\ \text{or}\ (a_0^{x_1}, b_0^{y_1}c^{M_+-M_-}),$$

according to whether $y_2(x_1-x_2)/\gcd(x_2,y_2) = M_+$, or M_-, respectively. We can now apply the ABC conjecture to Equation (31) (note that the above A and B are coprime), getting that

$$\max\{a_0^{x_1}, c^{M_+-M_-}, b_0^{y_1}\} \ll \left(a_0b_0c\frac{|a_0^{x_2} - b_0^{y_2}|}{c^{M_-}}\right)^{1+\varepsilon} \ll (a_0b_0(a_0^{x_2}b_0^{y_2}))^{1+\varepsilon}, \tag{32}$$

where we used the fact that $M_- \ge 1$ and $|a_0^{x_2} - b_0^{y_2}| \le a_0^{x_2}b_0^{y_2}$. Inserting estimate (29) into (32), we get

$$\max\{a_0^{x_1}, b_0^{y_1}, c^{M_+-M_-}\} \ll (a_0b_0c)^5D^{3\varepsilon}. \tag{33}$$

Using Equations (28), and inequalities (29) and (33), we get

$$\begin{aligned} D^2 &\ll (a_0^{x_1-x_2}b_0^{y_1-y_2}c^{M_++M_-}) \\ &= (a_0^{x_1}b_0^{y_1}c^{M_+-M_-})\left(\frac{c^{2M_-}}{a_0^{x_2}b_0^{y_2}}\right) \\ &\le (a_0^{x_1}b_0^{y_1}c^{M_+-M_-})a_0^{x_2}b_0^{y_2} \\ &\le (a_0b_0c)^{18}D^{11\varepsilon}, \end{aligned}$$

leading to

$$D \ll (a_0b_0c)^{10}. \tag{34}$$

Let $L = \max\{a_0, b_0, c\}$.

Assume that $L = b_0$. Then, $D \ll b_0^{30}$, and now inequality (33) shows that

$$b_0^{y_1} \ll (a_0b_0c)^5D^{3\varepsilon} \ll b_0^{15+90\varepsilon} \ll b_0^{16},$$

and since $b_0 > 1$ (because $L = b_0$ and $a \geq 3$), we get that y_1 is bounded. Hence, all four exponents $x_1,\ x_2,\ y_1$ and y_2 are bounded in this case.

Assume now that $L = c$. Then, $D \ll c^{30}$. Further, inequality (33) shows that

$$c^{M_+ - M_-} \ll (a_0 b_0 c)^5 D^{3\varepsilon} \ll c^{15+90\varepsilon} \ll c^{16}.$$

Since also c^{M_-} divides $|a_0^{x_2} - b_0^{y_2}|$, we have that, by inequality (29),

$$c^{M_-} \leq |a_0^{x_2} - b_0^{y_2}| \leq a_0^{x_2} b_0^{y_2} \ll (a_0 b_0 c)^3 D^{2\varepsilon} \ll c^{9+60\varepsilon} \ll c^{10},$$

therefore

$$c^{M_+} \ll c^{26}. \tag{35}$$

We may also assume that c is as large as we wish, otherwise Equation (25) becomes just a nondegenerate $\mathcal{S}$-unit equation (recall that we have assumed that $c = \max\{a_0, b_0, c\}$), and therefore it has only finitely many solutions. So, if c is larger than the constant implied in inequality (35), then $M_+ \leq 27$. This shows now that each one of the four numbers $x_1 - x_2,\ y_1 - y_2,\ x_2/\gcd(x_2, y_2)$ and $y_2/\gcd(x_2, y_2)$ is at most 27. From Equations (28), we get

$$\begin{aligned} c^{(x_1-x_2)(y_1-y_2)x_2y_2/\gcd(x_2,y_2)^2} &= \left(\frac{Db_0^{y_2}+1}{a_0^{x_1-x_2}}\right)^{x_2(y_1-y_2)/\gcd(x_2,y_2)} \\ &= \left(\frac{Da_0^{x_2}+1}{b_0^{y_1-y_2}}\right)^{y_2(x_1-x_2)/\gcd(x_2,y_2)}. \end{aligned}$$

The last equality above leads to the conclusion that

$$D \mid a_0^{(x_1-x_2)(y_1-y_2)x_2/\gcd(x_2,y_2)} - b_0^{(x_1-x_2)(y_1-y_2)y_2/\gcd(x_2,y_2)}.$$

If the right-hand side of the above divisibility relation is zero, we then get $a_0 = b_0 = 1$, therefore $a^{x_2} = b^{y_2}$; hence, $a^{x_1} = b^{y_1}$, which is impossible. Hence, the right-hand side of the above relation is nonzero, and since $M_+ \leq 27$, we get that

$$D \ll \max\{a_0, b_0\}^{729}.$$

Further, the ABC conjecture applied to the appropriate one of Equations (28) gives

$$c^2 \leq c^{M_+} \ll (Da_0b_0c)^{1+\varepsilon} \ll (Da_0b_0c)^{3/2}$$

giving

$$c \ll (Da_0b_0)^2 \ll (\max\{a_0, b_0\})^{1462}. \tag{36}$$

If $b_0 > a_0$, then inequality (33) gives

$$b_0^{y_1} \ll (a_0b_0c)^5 D^{3\varepsilon} \ll b_0^{7320+2187\varepsilon} \ll b_0^{7321},$$

which gives again the conclusion that all four exponents are bounded. Thus, we may assume that $a_0 > b_0$, and we get, from inequalities (33) and (36), that

$$a_0^{x_1} \ll (a_0b_0c)^5 D^{3\varepsilon} \ll a_0^{7320+2187\varepsilon} \ll a_0^{7321}, \tag{37}$$

giving that $x_1 = O(1)$. Note further that from estimate (36), we also deduce that

$$c^{y_2/\gcd(x_2,y_2)} \leq c^{27} \ll a_0^{39,474} \tag{38}$$

in this case, since we have established that $y_2/(x_2, y_2) \leq 27$.

Finally, let us assume that $L = a_0$. We then get that $D \ll a_0^{30}$, and now estimate (33) leads to

$$a_0^{x_1} \ll (a_0 b_0 c)^5 D^{3\varepsilon} \ll a_0^{15+90\varepsilon} \le a_0^{16}, \tag{39}$$

which gives $x_1 \ll 1$. Furthermore, from estimate (33), we also have that

$$c^{M_+ - M_-} \ll (a_0 b_0 c)^5 D^{3\varepsilon} \ll a_0^{15+90\varepsilon} \le a_0^{16},$$

while from relation (30) and estimate (29) we get

$$c^{M_-} \ll |a_0^{x_2} - b_0^{y_2}| \le a_0^{x_2} b_0^{y_2} \ll (a_0 b_0 c)^3 D^{2\varepsilon} \ll a_0^{3+60\varepsilon} \ll a_0^4,$$

which leads to the conclusion that $c^{M_+} \ll a_0^{20}$. Since $y_2/\gcd(x_2, y_2) \le M_+$, we deduce, in particular, that in both cases when $L = c$ and when $L = a_0$, inequality (38) holds.

Step 2. $y_1 = O(1)$.

From now on, we may assume that both x_1 and x_2 are fixed. We show that $y_1 = O(1)$. Note that in either case when $L = a_0$ or $L = c$, we have, by estimates (37), (39), and (38), that

$$\begin{aligned} a_0^{3\cdot 10^8} &> (a_0^{7321})^{40,000} \gg (a_0^{x_1})^{40,000} = (a_0 \cdot a_0^{39,474})^{x_1} \\ &\ge (a_0 \cdot c^{y_2/\gcd(x_2,y_2)})^{x_1} = a^{x_1} > a^{x_1} - a^{x_2} = b^{y_1} - b^{y_2} \gg b^{y_1}; \end{aligned}$$

hence, $b = a_0^{O(1/y_1)}$. Since $c \mid b$, we also have that $c = a_0^{O(1/y_1)}$. Hence, $b_0 c = a_0^{O(1/y_1)}$. From now on, we will assume that y_1 is so large so that $b_0 c < a_0$. In particular, we are in the case $L = a_0$.

Case 1. $x_2 \ge 2$.

Applying the ABC conjecture to the second equation (28), we get

$$D a_0^{x_2} \ll (D a_0 b_0 c)^{1+\varepsilon},$$

so

$$a_0^{x_2 - 1 - \varepsilon} \ll (b_0 c)^{1+\varepsilon} D^{\varepsilon} = a_0^{O(1/y_1)} D^{\varepsilon}. \tag{40}$$

Since clearly $D < a^{x_1} = a^{O(1)}$, we get

$$D \ll a^{O(1)} \le (a_0 c^{y_2})^{O(1)} = a_0^{O(1+y_2/y_1)} = a_0^{O(1)},$$

and now from inequality (40), we get that

$$a_0^{x_2 - 1 - \varepsilon} \ll a_0^{O(1/y_1 + \varepsilon)}.$$

The last inequality above leads to the conclusion that $y_1 \ll 1$, because $x_2 \ge 2$ and $\varepsilon > 0$ is arbitrarily small.

Case 2. $x_2 = 1$ but $x_1 \ge 3$.

Applying the ABC conjecture to the first of Equations (28), we get

$$a^{x_1 - 1} = (a_0 c^{y_2/\gcd(x_2,y_2)})^{x_1 - 1} \ll (a_0 b_0 c D)^{1+\varepsilon} = \left(a_0 b_0 c \frac{a^{x_1 - 1}}{b_0^{y_2}} \right)^{1+\varepsilon},$$

giving

$$b_0^{y_2} \ll (a_0 b_0 c)^{1+\varepsilon} a^{(x_1 - 1)\varepsilon} = a_0^{1 + O(1/y_1 + \varepsilon)} (a_0 c^{y_2})^{O(\varepsilon)} = a_0^{1 + O(1/y_1 + \varepsilon)}. \tag{41}$$

Now inequality (32) becomes

$$a_0^{x_1} \ll (a_0 b_0 |a_0 - b_0^{y_2}|)^{1+\varepsilon}.$$

If $a_0 > b_0^{y_2}$, we then get

$$a_0^{x_1 - 2(1+\varepsilon)} \ll b_0^2 = a_0^{O(1/y_1)},$$

which shows that $y_1 \ll 1$ if $\varepsilon > 0$ is small (because $x_1 \geq 3$), while if $b_0^{y_2} > a_0$, then, by estimate (41), we get

$$a_0^{x_1} \ll (a_0 b_0 b_0^{y_2})^{1+\varepsilon} \ll a_0^{2+O(1/y_1+\varepsilon)},$$

which again leads to the conclusion that $y_1 \ll 1$ if $\varepsilon > 0$ is sufficiently small, since $x_1 \geq 3$.

Case 3. $x_1 = 2$ and $x_2 = 1$.

Here, Equations (28) become

$$\begin{aligned} a_0 c^{y_2} - 1 &= D b_0^{y_2} \\ b_0^{y_1 - y_2} c^{y_1 - y_2} - 1 &= D a_0. \end{aligned} \tag{42}$$

The ABC conjecture applied to the first of Equations (42) above gives

$$a_0 c^{y_2} \ll (a_0 b_0 c D)^{1+\varepsilon} < \left(a_0 b_0 c \frac{a_0 c^{y_2}}{b_0^{y_2}} \right)^{1+\varepsilon},$$

giving

$$b_0^{y_2} < b_0^{y_2(1+\varepsilon)} \ll (a_0 b_0 c)^{1+2\varepsilon} c^{\varepsilon y_2} = a_0^{1+O(1/y_1+\varepsilon)}. \tag{43}$$

On the other hand, rewriting Equation (25) as

$$(2a-1)^2 = 4b^{y_1} - (4b^{y_2} - 1),$$

and applying the ABC conjecture to the above equation we get

$$(a_0 c^{y_2})^2 = a^2 \ll (ab(b^{y_2}))^{1+\varepsilon} = (a_0 b_0 c b_0^{y_2} c^{2y_2})^{1+\varepsilon},$$

giving

$$a_0 \ll (b_0 c)^{1+2\varepsilon} b_0^{y_2(1+\varepsilon)} c_0^{2\varepsilon y_2} = b_0^{y_2} a_0^{O(1/y_1+\varepsilon)}, \tag{44}$$

and comparing estimates (43) and (44), we get

$$b_0^{y_2} = a_0^{1+O(1/y_1+\varepsilon)}.$$

The above estimate and the first equation (42) gives

$$a_0 c^{y_2} - 1 = D b_0^{y_2} = D a_0^{1+O(1/y_1+\varepsilon)},$$

so

$$D = c^{y_2} a_0^{O(1/y_1+\varepsilon)}. \tag{45}$$

Further,

$$b^{y_2} = b_0^{y_2} c^{y_2} = a_0^{1+O(1/y_1+\varepsilon)} c^{y_2} = (a_0 c^{y_2})^{1+O(1/y_1+\varepsilon)} = a^{1+O(1/y_1+\varepsilon)},$$

and since

$$a^2 \asymp a^2 - a = b^{y_1} - b^{y_2} \asymp b^{y_1},$$

we get that $b^{y_1/2} = a^{1+O(\varepsilon)}$ provided that a is sufficiently large with respect to ε. (Of course, if a is bounded, we then get only finitely many solutions). Hence, $y_2 = (y_1/2)(1 + O(1/y_1 + \varepsilon))$. We thus get that

$$M_- = \min\{y_1 - y_2,\ y_2\} = y_2(1 + O(1/y_1 + \varepsilon)).$$

Inequality (32) now gives

$$a_0^2 \ll \left(a_0 b_0 c \frac{|a_0 - b_0^{y_2}|}{c^{M_-}}\right)^{1+\varepsilon},$$

which together with the fact that $b_0^{y_2} = a_0^{1+O(1/y_1+\varepsilon)}$ gives

$$\begin{aligned} c^{y_2(1+O(1/y_1+\varepsilon))} &= c^{M_-} < c^{M_-(1+\varepsilon)} \ll (b_0 c)^{1+\varepsilon} a_0^{-1+\varepsilon} |a_0 - b_0^{y_2}|^{1+\varepsilon} \\ &= a_0^{O(1/y_1+\varepsilon)}, \end{aligned}$$

giving

$$c^{y_2} = a_0^{O(1/y_1+\varepsilon)}.$$

Thus, by (45), we also have

$$D = c^{y_2} a_0^{O(1/y_1+\varepsilon)} = a_0^{O(1/y_1+\varepsilon)}.$$

Subtracting the first equation (42) from the second one, and reducing the resulting equation modulo b^{M_-}, we get

$$a_0(c^{y_2} + D) \equiv 0 \pmod{b_0^{M_-}}.$$

Since a_0 and b_0 are coprime,

$$0 < c^{y_2} + D = a_0^{O(1/y_1+\varepsilon)},$$

while

$$b_0^{M_-} = (b_0^{y_2})^{1+O(1/y_1+\varepsilon)} = a_0^{1+O(1/y_1+\varepsilon)},$$

we get a contradiction if ε is sufficiently small and y_1 is sufficiently large. Thus, $y_1 \ll 1$.

Step 3. $a = O(1)$.

This part of the proof is unconditional and somewhat independent of the previous parts of the proof, which is why we record it as follows:

Theorem 6.2. *Assume that $x_1 > x_2 > 0$, $y_1 > y_2 > 0$ are fixed integers with $\gcd(x_1, x_2) = \gcd(y_1, y_2) = 1$ and $y_1 > x_1$. Then the diophantine equation*

$$a^{x_1} - a^{x_2} = b^{y_1} - b^{y_2} \tag{46}$$

has only finitely many positive integer solutions (a, b).

The case when $x_2 = y_2 = 1$ of Theorem 6.2 appears in [13]. Further, a partial result along the lines of Theorem 6.2 above appears as Proposition 3 on page 211 in [11]. However, the proof of that result in [11] uses the condition (imposed in that statement) that a and b are coprime, which is why we choose to give a complete and self-contained proof of Theorem 6.2 here.

Proof. It is easy to check that both curves $X^2-X=Y^3-Y$ and $X^2-X=Y^3-Y^2$ are elliptic, therefore there are only finitely many integer solutions (a,b) of Equation (46) when $(x_1,x_2,y_1,y_2)=(2,1,3,1)$ or $(2,1,3,2)$. From now on, we assume that $y_1\geq 4$. Further, when $x_1=2$, then $x_2=1$, and the given equation becomes

$$(2a-1)^2=4b^{y_1}-4b^{y_2}+1.$$

It is easy to check that the polynomial $g(Y)=4Y^{y_1}-4Y^{y_2}+1$ has only simple roots. Indeed, if z is a double root of g, then

$$z^{y_2-1}(y_1z^{y_1-y_2}-y_2)=\frac{g'(z)}{4}=0,$$

and since 0 is not a root of g, we get $z^{y_1-y_2}=y_2/y_1$. Furthermore, the relation $g(z)=0$ becomes $4z^{y_2}(z^{y_1-y_2}-1)=-1$, which implies that $4z^{y_2}(y_2/y_1-1)=-1$, therefore $4z^{y_2}=y_1/(y_1-y_2)$. Thus,

$$\left(\frac{y_1}{y_1-y_2}\right)^{y_1-y_2}=4^{y_1-y_2}(z^{y_1-y_2})^{y_2}=4^{y_1-y_2}\left(\frac{y_2}{y_1}\right)^{y_2}.$$

Since y_1 and y_2 are coprime, the above relation gives, by looking at the denominators, that y_1 is a power of 2 and that $y_1-y_2=1$. Now by looking at the numerators, we get that $y_2=y_1-1$ is an odd number, and that every prime factor of it divides y_1, which is obviously impossible.

From now on, we assume that $x_1\geq 3$.

Write $f(X)=X^{x_1}-X^{x_2}$ and let $g(Y)=Y^{y_1}-Y^{y_2}$. Recall the following theorem due to Davenport, Lewis and Schinzel (see [7]).

Theorem 6.3. *Let $f(X)$ and $g(Y)$ be polynomials with integer coefficients of degrees >1. Let $D_f(\lambda)=\operatorname{disc}(f(X)-\lambda)$ and $D_g(\lambda)=\operatorname{disc}(g(Y)-\lambda)$. Assume further that there are at least $\lceil \deg(f)/2\rceil$ distinct roots of $D_f(\lambda)=0$ for which $D_g(\lambda)\neq 0$. Then, the polynomial $f(X)-g(Y)$ is irreducible over the complex numbers. Further, the genus of the curve given by the equation $f(X)=g(Y)$ is strictly positive except possibly when $\deg(f)=2$ or $\deg(f)=\deg(g)=3$. Apart from these possible exceptions, the equation $f(x)=g(y)$ has at most a finite number of integral solutions (x,y).*

In our case, one checks easily that all the roots λ of D_f are:

(i) $\lambda=0$ with multiplicity x_2-1,

(ii) $\lambda=-\zeta^{x_2}\cdot\left(\dfrac{x_1-x_2}{x_1}\right)\cdot\left(\dfrac{x_2}{x_1}\right)^{\frac{x_2}{x_1-x_2}}$, with $\zeta=e^{\frac{2\pi ik}{x_1-x_2}}$, $k=0,\ldots,x_1-x_2-1$.

The roots λ of D_g are obtained in the same way as at (i) and (ii) above by replacing the pair (x_1,x_2) with the pair (y_1,y_2). Since $\gcd(x_1,x_2)=\gcd(y_1,y_2)=1$, we see that all the nonzero roots of both D_f and D_g are simple roots. Hence, assuming that either $x_2<x_1/2$ or $y_2<y_1/2$ holds, we get that either $x_1-x_2\geq\lceil x_1/2\rceil$ or $y_1-y_2\geq\lceil y_1/2\rceil$ holds. Since we also have that $\deg(g)\geq 4$, we conclude that in this instance we may apply Theorem 6.3 above to our pair of polynomials $f(X)$ and $g(Y)$ and conclude that Equation (46) has only finitely many integer solutions (a,b) provided that we can show that the only common root of both D_f and D_g is $\lambda=0$. Let us assume that D_f and D_g have a nonzero common root,

say z. Using (ii) above, and identifying the absolute value of this nonzero common root, we get the diophantine equation

$$\left(1-\frac{x_2}{x_1}\right)\cdot\left(\frac{x_2}{x_1}\right)^{\frac{x_2/x_1}{1-x_2/x_1}}=\left(1-\frac{y_2}{y_1}\right)\cdot\left(\frac{y_2}{y_1}\right)^{\frac{y_2/y_1}{1-y_2/y_1}}. \tag{47}$$

The above equation can be rewritten as $h(u)=h(v)$, where $u=x_2/x_1,\ v=y_2/y_1$, and $h(z)$ is the function defined on $(0,1)$ and given by

$$h(z)=(1-z)z^{\frac{z}{1-z}}.$$

We shall first use the above equation to rule out some possible instances.

Case 1. *$u<1/2$ or $v<1/2$.*

In this case, it suffices to prove that the function $h(z)$ shown above is one-to-one in the interval $(0,1)$. Indeed, once we have proved this fact, then the equation $h(u)=h(v)$ will force $u=v$, and since both u and v are rational numbers in reduced form, we read that $x_1=y_1$ and $x_2=y_2$, which is a contradiction.

To prove the injectivity of $h(z)$ in $(0,1)$, note that with

$$k(z)=\log h(z)=\log(1-z)+\frac{z\log z}{1-z},$$

we have

$$\frac{dk}{dz}=\frac{\log z}{(1-z)^2}<0,\qquad \text{when } z\in(0,1),$$

which proves that $h(z)$ is one-to-one in $(0,1)$.

From now on, we assume that both $u\geq 1/2$ and $v\geq 1/2$ hold. Hence, $x_1\leq 2x_2$ and $y_1\leq 2y_2$. Since $x_1\geq 3$ and $y_1\geq 4$, we conclude that both $x_2\geq 2$ and $y_2\geq 2$. Furthermore, let us show that $y_2\geq 4$. Indeed, assume that $y_2\leq 3$. Since $y_1\geq 4$ and $\gcd(y_1,y_2)=1$, it follows that $y_2/y_1<1/2$ except when $y_1=5$. In this case, that is, in the case $(y_1,y_2)=(5,3)$, we can still have $(x_1,x_2)=(4,3),\ (3,2)$, and the Theorem 6.3 does not apply to those cases. However, one checks by hand that the two curves obtained in this way are irreducible and of genus >1, so we can have only finitely many solutions integer solutions (a,b) to the diophantine equation $f(a)=g(b)$ in these cases.

Case 2. *The final contradiction.*

From now on, we assume that both $u>1/2$ and $v>1/2$, that both x_2 and y_2 are at least 2, and that one of them is at least 4. To deal with these remaining cases, we use a finiteness criterion of Bilu and Tichy from [5]. We follow the presentation from [4]. To use the criterion, we need to define five kinds of *standard pairs of polynomials*. In what follows, α and β are nonzero rational numbers, $\mu,\ \nu$ and q are positive integers, ρ is a nonnegative integer and $\nu(X)\in\mathbb{Q}[X]$ is a nonzero polynomial, which may be constant.

A *standard pair of the first kind* is a pair of polynomials of the form

$$(X^q,\alpha X^\rho\nu(X)^q),$$

or switched, where $0\leq\rho<q,\ \gcd(\rho,q)=1$ and $\rho+\deg(\nu)>0$.

A *standard pair of the second kind* is $(X^2,(\alpha X^2+\beta)\nu(X)^2)$, or switched.

Denote by $D_\mu(X,\delta)$ the μth Dickson polynomial, defined by the functional equation $D_\mu(z+\delta/z) = z^\mu + (\delta/z)^\mu$, or by the explicit formula

$$D_\mu(X,\delta) = \sum_{i=0}^{\lfloor \mu/2 \rfloor} d_{\mu,i} X^{\mu-2i} \qquad \text{with} \qquad d_{\mu,i} = \frac{\mu}{\mu-i}\binom{\mu-i}{i}(-\delta)^i.$$

A *standard pair of the third kind* is a pair of polynomials of the form

$$(D_\mu(X,\alpha^\nu), D_\nu(X,\alpha^\mu)),$$

where $\gcd(\mu,\nu)=1$.

A *standard pair of the fourth kind* is $(\alpha^{-\mu/2}D_\mu(X,\alpha), -\beta^{-\nu/2}D_\nu(X,\beta))$, where $\gcd(\mu,\nu)=2$.

A *standard pair of the fifth kind* is $((\alpha X^2-1)^3,\ 3X^4-4X^3)$ (or switched).

The following theorem is the main result of [5]. It extends and completes Theorem 6.3.

Theorem 6.4. *Let $f(X),\ g(X) \in \mathbb{Q}[X]$ be nonconstant polynomials such that the equation $f(a)=g(b)$ has infinitely many integer solutions (a,b). Then $f=\phi\circ f_1\circ\kappa$ and $g=\phi\circ g_1\circ\lambda$, where $\kappa(X)\in\mathbb{Q}[X]$ and $\lambda(X)\in\mathbb{Q}[X]$ are linear polynomials, $\phi(X)\in\mathbb{Q}[X]$ and $(f_1(X),g_1(X))$ is a standard pair.*

We assume that the equation $f(a)=f(b)$ has infinitely many positive integer solutions (a,b), and we use the above Theorem 6.4 to reach a contradiction. Let us assume that $f=\phi\circ f_1\circ\kappa$ and $g=\phi\circ g_1\circ\lambda$. Since, $f(X)=X^{x_1}-X^{x_2}$ has $z=1$ as a simple root, we get that ϕ cannot be a perfect power of exponent >1 of another polynomial. Writing $\phi(X)=a_0(X-\alpha_1)^{\lambda_1}\dots(X-\alpha_t)^{\lambda_t}$ with $t\geq 1$ distinct roots $\alpha_1,\dots,\alpha_t$, where $\alpha_1=f_1(\kappa(0))$, and positive integers $\lambda_1,\dots,\lambda_t$, we get that

$$f(X)=X^{x_2}(X^{x_1-x_2}-1)=a_0(f_1(\kappa(X))-\alpha_1)^{\lambda_1}\dots(f_1(\kappa(X))-\alpha_t)^{\lambda_t}.$$

From the above remark, we have $\lambda_1=1$ if $t=1$. We now show that this must always be the case. Note that the roots of $f(X)$ are among the roots of $f_1(\kappa(X))-\alpha_i$ for $i=1,\dots,t$, and that if $t\geq 2$ and $i\neq j$, then $f_1(\kappa(X))-\alpha_i$ and $f_1(\kappa(X))-\alpha_j$ are coprime as polynomials. Hence, they do not share any root. Thus, since $\alpha_1=f_1(\kappa(0))$, we get that $z=0$ is a root of multiplicity x_2 of $(f_1(\kappa(X))-\alpha_1)^{\lambda_1}$, and that all other roots have multiplicity one, and are roots of unity of order x_1-x_2. Thus, when $t\geq 2$, we get at once that $\lambda_2=\dots=\lambda_t=1$, and that if $\lambda_1>1$, then $f_1(\kappa(X))-\alpha_1=\gamma X^d$ for some nonzero number γ, where $d=\deg(f_1)$. Identifying the multiplicity of the root $z=0$, we get $x_2=d\lambda_1$ and $x_1-x_2=(t-1)d$, giving that $d\mid\gcd(x_1,x_2)$. Thus, $d=1$, which is not allowed. In conclusion, even if $t>1$, we must then have $\lambda_1=\dots=\lambda_t=1$, therefore all the roots of ϕ are simple.

Assume now that (f_1,g_1) is a pair of the first or second kind. Then either $f_1(X)=X^q$ or $g_1(X)=X^q$. Assume say that $f_1(X)=X^q$. Then $f_1(\kappa(X))-\alpha_1=(\gamma X+\delta)^q-\delta^q$ and this polynomial has $z=0$ as a simple root if $\delta\neq 0$, and as root of multiplicity exactly $q=d=\deg(f)$ if $\delta=0$. The case of the simple root at $z=0$ is not convenient (because $x_2\geq 2$), and the remaining case leads to $d=x_2$, and $dt=x_1$, which is again impossible because it gives $x_2\mid x_1$. The case when $g_1(X)=X^q$ can be dealt with analogously.

Assume now that (f_1, g_1) is a pair of the third, fourth or fifth kind. We know that $\min\{x_2, y_2\} \geq 4$. Then either $f_1(\kappa(X)) - \alpha_1$ or $g_1(\lambda(X)) - \alpha_s$ has a root of multiplicity at least four, where $s \in \{1, \ldots, t\}$ is such that $\alpha_s = g_1(\lambda(0))$. But this implies that either $(f_1(\kappa(X)) - \alpha_1)' = f_1'(\kappa(X))\kappa'(X)$ or $(g_1(\lambda(X)) - \alpha_s)' = g_1'(\lambda(X))\lambda'(X)$ has a triple root. Since κ and λ are nonconstant linear polynomials, we conclude immediately that this last fact is equivalent to the fact that either $f_1'(X)$ has a triple root or $g_1'(X)$ has a triple root. It is clear that this is not so if (f_1, g_1) is a pair of the fifth kind. We now verify that the derivative of any Dickson polynomial does not have double roots, therefore it does not have triple roots either. Setting $x_1 = x/\sqrt{\delta}$, we easily get that $D_\mu(x, \delta) = \delta^\mu D_\mu(x_1, 1)$, therefore it is enough to verify our claim when $\delta = 1$. But since the roots $D_\mu(X, 1)$ are precisely $2\cos \pi k/m$ for $k = 0, \ldots, m-1$, which are all real and simple, it follows, by Rolle's Theorem, that the roots of its derivative $D_\mu'(X)$ are also real and simple.

This completes the proof of Theorem 6.2 and of Theorem 6.1 as well. □

□

7. Comments and remarks

It would certainly be of interest to extend the results of this paper 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 [11], 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.

References

[1] Bennett, Michael A. On some exponential equations of S.S. Pillai. *Canad. J. Math.* **53** (2001), 897–922. MR1859761 (2002g:11032), Zbl 0984.11014.

[2] Bennett, Michael A. Pillai's conjecture revisited. *J. Number Theory* **98** (2003), 228–235. MR1955415 (2003j:11030), Zbl 1045.11021.

[3] Bilu, Yu.; Hanrot, G.; Voutier, P. M. Existence of primitive divisors of Lucas and Lehmer numbers. With an appendix by M. Mignotte. *J. Reine Angew. Math.* **539** (2001), 75–122. MR1863855 (2002j:11027), Zbl 0995.11010.

[4] Bilu, Yu. F.; Brindza, B.; Kirschenhofer, P.; Pintér, Á.; Tichy, R. F. Diophantine equations and Bernoulli polynomials. With an appendix by A. Schinzell. *Compositio Math.* **131** (2002), 173–188. MR1898434 (2003a:11025), Zbl 1028.11016.

[5] Bilu, Yuri F.; Tichy, Robert F. The diophantine equation $f(x) = g(y)$. *Acta Arith.* **95** (2000), 261–288. MR1793164 (2001i:11031), Zbl 0958.11049.

[6] Carmichael, R. D. On the numerical factors of arithmetic forms $\alpha^n \pm \beta^n$. *Ann. Math. (2)* **15** (1913), 30–70. JFM 44.0216.01.

[7] Davenport, H.; Lewis, D. J.; Schinzel, A. Equations of the form $f(x) = g(y)$. *Quart. J. Math. Oxford* **12** (1961), 304–312. MR0137703 (25 #1152), Zbl 0121.28403.

[8] Evertse, Jan-Hendrik. The number of solutions of decomposable form equations. *Invent. Math.* **122** (1995), 559–601. MR1359604 (96i:11034), Zbl 0851.11019.

[9] Herschfeld, Aaron. The equation $2^x - 3^y = d$. *Bull. Amer. Math. Soc.* (N.S.) **42** no. 4 (1936), 231–234. Zbl 0014.00801, JFM 62.0134.02.
[10] Le, Maohua. A note on the Diophantine equation $ax^m - by^n = k$. *Indag. Math.* (N.S.) **3** (1992), 185–191. MR1168346 (93c:11016), Zbl 0762.11012.
[11] Luca, Florian. On the diophantine equation $p^{x_1} - p^{x_2} = q^{y_1} - q^{y_2}$. *Indag. Math.* (N.S.) **14** (2003), 207–222. MR2026815 (2004h:11024), Zbl 1080.11031.
[12] Matveev, E. M. 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. MR1817252 (2002e:11091), Zbl 1013.11043.
[13] Mignotte, M.; Pethő, A. On the Diophantine equation $x^p - x = y^q - y$. *Publ. Mat.* **43** (1999), 207–216. MR1697521 (2000d:11044), Zbl 0949.11022.
[14] Mo, De Ze; Tijdeman, R. Exponential Diophantine equations with four terms. *Indag. Math.* (N.S.) **3** no. 1 (1992), 47–57. MR1157518 (93d:11035), Zbl 0765.11018.
[15] Pillai, S.S. On $a^x - b^y = c$. *J. Indian Math. Soc.* (N.S.) **2** (1936), 119–122. Zbl 0014.39205.
[16] Pólya, G. Zur arithmetischen Untersuchung der Polynome. *Math. Z.* **1** (1918), 143–148. JFM 46.0240.04.
[17] Ridout, D. Rational approximations to algebraic numbers. *Mathematika* **4** (1957), 125–131. MR0093508 (20 #32), Zbl 0079.27401.
[18] Schmidt, Wolfgang M. Diophantine approximation. Lecture Notes in Mathematics, 785. *Springer, Berlin*, 1980. MR0568710 (81j:10038), Zbl 0421.10019.
[19] Schmidt, Wolfgang M. Diophantine approximations and Diophantine equations. Lecture Notes in Mathematics, 1467. *Springer-Verlag, Berlin*, 1991. MR1176315 (94f:11059), Zbl 0754.11020.
[20] Scott, Reese; Styer, Robert. 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. MR2040155 (2005a:11040).
[21] Shorey, T.N. On the equation $ax^m - by^n = k$. *Indag. Math.* **48** (1986), 353–358. MR0862765 (88a:11030), Zbl 0603.10019.
[22] Shorey, T. N.; Stewart, C. L. Pure powers in recurrence sequences and some related diophantine equations. *J. Number Theory* **27** (1987), 324–352. MR0915504 (89a:11024), Zbl 0624.10009.
[23] Shorey, T. N.; Tijdeman, R. Exponential diophantine equations. Cambridge Tracts in Mathematics, 87. *Cambridge University Press, Cambridge*, 1986. MR0891406 (88h:11002), Zbl 0606.10011.
[24] Yu, Kunrui. p-adic logarithmic forms and group varieties. II. *Acta Arith.* **89** (1999), no. 4, 337–378. MR1703864 (2000e:11097), Zbl 0928.11031.

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

Instituto de Matemáticas, Universidad Nacional Autónoma de México, C.P. 58089, Morelia, Michoacán, México
fluca@matmor.unam.mx

This paper is available via http://nyjm.albany.edu/j/2006/12-12.html.