JOURNAL
de Théorie des Nombres
de BORDEAUX
*anciennement Séminaire de Théorie des Nombres de Bordeaux*

Reese SCOTT et Robert STYER

**Bennett's Pillai theorem with fractional bases and negative exponents allowed**

Tome 27, n° 1 (2015), p. 289-307.

<http://jtnb.cedram.org/item?id=JTNB_2015__27_1_289_0>

*Journal de Théorie des Nombres*
*de Bordeaux* **27** (2015), 289–307

# Bennett's Pillai theorem with fractional bases and negative exponents allowed

par Reese SCOTT et Robert STYER

Résumé. Bennett a démontré que si $a$, $b$ et $c$ sont des nombres entiers positifs avec $a \geq 2$ et $b \geq 2$, l'équation $a^x - b^y = c$ n'admet au plus que deux nombres entiers positifs $x$ et $y$, comme solution. Nous pouvons généraliser ceci en choisissant $a$, $b$ et $c$ dans l'ensemble des nombres rationnels positifs permettant à $x$ et $y$ d'être des nombres entiers, positifs, négatifs ou nuls. Il n'y a quand même, au plus, que deux solutions à l'exception de deux case où l'équation a exactement trois solutions.

Abstract. Bennett has proven: If $a$, $b$, and $c$ are positive integers with $a, b \geq 2$, then the equation $a^x - b^y = c$ has at most two solutions in positive integers $x$ and $y$. Here we generalize this by allowing $a$, $b$, and $c$ to be positive rational numbers and, further, allowing $x$ and $y$ to be any integers, positive, negative, or zero. There are still at most two solutions except for two designated cases.

## 1. Introduction

In [3], Bennett proves

**Theorem A.** *If $a$, $b$, and $c$ are positive integers with $a, b \geq 2$, then the equation*

$$a^x - b^y = c \tag{1.1}$$

*has at most two solutions in positive integers $x$ and $y$*

and conjectures

**Conjecture.** *There are exactly eleven choices of $(a, b, c)$ such that (1.1) has two solutions.*

(Bennett's formulation of Theorem A actually reads "If $a$, $b$, and $c$ are nonzero integers with $a, b \geq 2 \ldots$", but since any case with negative $c$ is equivalent to a case with positive $c$, we take $c$ positive to simplify the formulations of Theorems 1 and 2 below.)

Manuscrit reçu le 1er août 2013, accepté le 2 janvier 2014.
*Mots clefs.* Pillai's equation, Exponential Diophantine equations.
*Mathematics Subject Classification.* 11D61.

Equation (1.1) of Theorem A is generally known as the Pillai equation; brief histories are given in [3] and [14], but see [18] for a much more extended history.

The purpose of this paper is to generalize Theorem A by allowing $a$, $b$, and $c$ to be any positive rational numbers (with $a \neq 1$, $b \neq 1$) and, further, allowing $x$ and $y$ to be any integers, positive, negative, or zero; there are still at most two solutions except for two designated cases, though an infinite number of choices of $(a, b, c)$ such that (1.1) has exactly two solutions.

The first step towards these generalizations is the following:

**Theorem 1.** *If $a$, $b$, and $c$ are positive integers with $a, b \geq 2$, then the equation*

$$a^x - b^y = c \tag{1.2}$$

*has at most two solutions in* nonnegative *integers $x$ and $y$ except for $(a, b, c) = (2, 5, 3)$, which has solutions $(x, y) = (2, 0)$, $(3, 1)$, $(7, 3)$, and no further solutions.*

We will use Theorem 1 in the proof of the following:

**Theorem 2.** *Let $A \neq 1$, $B \neq 1$, and $C$ be positive rational numbers. Then the equation*

$$A^x - B^y = C \tag{1.3}$$

*has at most two solutions $(x, y)$ where $x$ and $y$ are any integers, positive, negative, or zero, except when $(A, B, C : x_1, y_1; x_2, y_2; x_3, y_3)$ is $(2^u, 5^v, 3 : 7u, 3v; 3u, v; 2u, 0)$ or $(\left(\frac{2^n-1}{2^n}\right)^u, (1/2)^v, \frac{2^{n-1}-1}{2^{n-1}} : 2u, 2nv; u, nv; 0, (n-1)v)$ where $u, v \in \{1, -1\}$, $n > 1$ is a positive integer, and $(x_i, y_i)$ is a solution $(x, y)$ to (1.3) for $1 \leq i \leq 3$, taking $x_1 > x_2 > x_3$; in these cases there are exactly three solutions.*

*There are an infinite number of choices of $A$, $B$, $C$ giving exactly two solutions $(x, y)$ to* (1.3).

Before proceeding, we note several infinite families giving exactly two solutions to (1.3). We first list several infinite families in which $x$ and $y$ are both positive:

$$A = \frac{u(u^n \pm v^n)}{u^{n+1} \pm v^{n+1}}, B = \frac{v(u^n \pm v^n)}{u^{n+1} \pm v^{n+1}} \tag{1.4}$$

for given positive integers $u$ and $v$ with $u > v$, which gives the solutions $(x_1, y_1) = (n, n+1)$ and $(x_2, y_2) = (n+1, n)$ when all of the $\pm$ in (1.4) are plus, and also gives the solutions $(x_1, y_1) = (n, n)$ and $(x_2, y_2) = (n+1, n+1)$ when all of the $\pm$ in (1.4) are minus;

$$A = \frac{2^{n-1} \pm 1}{2^n}, B = \frac{1}{4}, (x_1, y_1) = (1, 1), (x_2, y_2) = (2, n) \tag{1.5}$$

where $n$ is an integer with $n \geq 2$ when we take the upper sign in $A$ and $n \geq 3$ when we take the lower sign in $A$;

$$A = \frac{2uv + u^2}{u^2 + uv + v^2}, B = \frac{u^2 - v^2}{u^2 + uv + v^2}, (x_1, y_1) = (1, 3), (x_2, y_2) = (3, 1), \tag{1.6}$$

where $u$ and $v$ are positive integers with $u > v$ (a similar parameterization produces an infinite family with $(x_1, y_1) = (1, 1)$ and $(x_2, y_2) = (3, 3)$).

Finally, we can obtain further examples of infinite families (with positive $x$ and $y$) by noting that, for certain fixed choices of $(x_1, y_1, x_2, y_2)$, the equation

$$A^{x_1} - B^{y_1} = A^{x_2} - B^{y_2} \tag{1.7}$$

can be converted to a Weierstrass equation (using, e.g., Connell [9], pages 105 and 115) which can be used to show (using, e.g., [13, Theorem 1] or [15]) that (1.7) has an infinite number of solutions in positive rational numbers $A \neq 1$ and $B \neq 1$. In this way we can show the following (see [16] for details):

*Let $S_1$ be the set of all quadruples of positive integers $(x_1, y_1, x_2, y_2)$ with the following properties:*

- $x_1 < x_2$, $y_1 \neq y_2$,
- $\max(x_2, y_1, y_2) \leq 4$,
- *if* $\max(x_2, y_1, y_2) = 4$, *then* $\min(x_2, \max(y_1, y_2)) < 3$,

*and let $S_2 = \{(1, 1, 4, 4), (2, 2, 4, 4), (3, 3, 4, 4), (3, 4, 4, 3)\}$. Then, if $(x_1, y_1, x_2, y_2) \in S_1 \cup S_2$, there are an infinite number of choices of $(A, B)$ satisfying* (1.7) *(so that we have an infinite family of cases giving two solutions to* (1.3)*) except for two choices of $(x_1, y_1, x_2, y_2)$: $(1, 2, 2, 3)$ and $(2, 1, 3, 2)$, for which there are no solutions to* (1.7) *with $A \neq 1$, $B \neq 1$.*

When at least one of $x_1x_2$ and $y_1y_2$ is negative, and $x_1y_1x_2y_2 \neq 0$, the same approach as above can be used to find infinite families of cases of exactly two solutions to (1.3). For example, a case similar to (1.5) is

$$A = \frac{2^n + 1}{2}, B = 4, (x_1, y_1) = (1, -1), (x_2, y_2) = (2, n - 1) \tag{1.8}$$

where $n \geq 2$ is an integer. Also, examples of quadruples $(x_1, y_1, x_2, y_2)$ generating infinite families of $(A, B)$ satisfying (1.7) are given by $(x_1, y_1, x_2, y_2) = (1, 1, 2, -2))$, $(1, -2, 2, 1)$, and $(1, -1, 2, 1)$, corresponding to the Weierstrass equations $y^2 = x^3 + x^2 + T$ where $T = 64$, $-64$, and $-16x$, respectively, and also by $(x_1, y_1, x_2, y_2) = (1, -2, 2, 2)$, corresponding to the Weierstrass equation $y^2 + 18xy + 32y = x^3 - 56x^2 - 16x + 896$.

When $x_1y_1x_2y_2 = 0$ we consider the equation

$$A^r - A^s + 1 = B^n \tag{1.9}$$

where $n$ is a positive integer and $r$ and $s$ are integers (the pair $(A, B)$ in (1.9) may correspond to the pair $(B, A)$ in (1.3)). When either $n = 1$ or $rs = 0$, (1.9) is trivially easy to satisfy, so we consider $n \geq 2$ and $rs \neq 0$. For certain choices of $(n, r, s)$ such that $\max(n, |r|, |s|) \leq 4$, we can use elliptic functions as above (or even simpler methods) to show there are an infinite number of $(A, B)$ satisfying (1.9). But when any of $n$, $r$, or $s$ is not bounded, known results appear to be limited to very specific cases: an old result on the Nagell-Ljunggren equation $(x^t - 1)/(x - 1) = y^q$, given in [8, Section 2], can be used to handle the case $(r, s) = (2, 1)$ with $n \geq 2$ when $A$ and $B$ are positive integers; Luca [11] and Szalay [17] handle the case $n = 2$ with $r > s > 0$ when $A$ is a prime integer. We will use the main result of [11] (given as Proposition 4.1 in the Appendix of this paper) in the proof of Theorem 1 in the next section.

## 2. Proof of Theorem 1:

Before using lower bounds on linear forms in logarithms in the proof of Theorem 1, we need to justify the use of $a \geq 6$ as in [3] by first proving Theorem 1 for the case $a$ prime. In [3], Bennett handles Theorem A for the case $a$ prime by using results from [14], but this will not work here since we are allowing the exponents $x$ and $y$ to be zero. Instead, we will use a result of Luca [11] on the equation $p^r \pm p^s + 1 = z^2$, where $p$, $r$, $s$, and $z$ are positive integers with $p$ prime. Although the proof in [11] is long and not elementary, we can provide a short elementary proof (see the Appendix of this paper). Thus, the proofs of both Theorem A and Theorem 1 are elementary when $a$ is prime, but use a theorem of Mignotte [12] on lower bounds on linear forms in logarithms when $a$ is composite.

We now deal with the case $a$ prime:

**Lemma 2.1.** *For integers $b > 1$, $c > 0$, and positive prime $a$, equation (1.2) has at most two solutions in* nonnegative *integers $(x, y)$, except for $(a, b, c) = (2, 5, 3)$, which has solutions $(x, y) = (2, 0)$, $(3, 1)$, $(7, 3)$, and no further solutions.*

(Note that there are an infinite number of $(a, b, c)$ giving two solutions to (1.2), even when $a$ is restricted to prime values as in Lemma 2.1: set $b = a^{x_2} - a^{x_1} + 1$; or set $b^2 = a^{x_2} - a^{x_1} + 1$ with $a = 2$ and $x_2 = 2x_1 - 2$.)

*Proof.* We apply Theorem 3 of [14] which states that, when $a$ is prime and the parity of $y$ is fixed, Equation (1.1) has at most one solution in positive integers $(x, y)$ except for the following five exceptional $(a, b, c; x_1, y_1, x_2, y_2)$: $(3, 2, 1; 1, 1, 2, 3)$, $(2, 3, 5; 3, 1, 5, 3)$, $(2, 3, 13; 4, 1, 8, 5)$, $(2, 5, 3; 3, 1, 7, 3)$,

$(13, 3, 10; 1, 1, 3, 7)$. Noting that none of these five exceptional cases has a further solution with $2 \mid y > 0$ (use congruences modulo 3 or modulo 8), we see that, if (1.2) has more than two solutions in nonnegative integers $x$ and $y$ when $a$ is prime, we must have exactly one solution with $y = 0$ and exactly two further solutions. If these two further solutions are among the five exceptional cases, a solution with $y = 0$ occurs only when $(a, b, c) = (2, 5, 3)$, in which case the three solutions are $(2, 0)$, $(3, 1)$, $(7, 3)$. So from here on we exclude the five exceptional cases of Theorem 3 of [14] so that we can assume that we have three solutions $(x_1, y_1)$, $(x_2, y_2)$, $(x_3, y_3)$ with $y_1 = 0$ and $2 \not| y_2 - y_3$. Without loss of generality, assume $2 \mid y_2 = 2t$ for some integer $t$. Then we have a solution to the equation

$$b^{2t} + c = a^{x_2},$$

as well as a solution to the equation

$$1 + c = a^{x_1}.$$

Now we apply Theorem 4 of [14] which states that, if $a = 2$, Equation (1.1) has at most one solution in positive integers $x$ and $y$ except when $(a, b, c; x_1, y_1, x_2, y_2)$ is one of $(2, 3, 5; 3, 1, 5, 3)$, $(2, 3, 13; 4, 1, 8, 5)$, $(2, 5, 3; 3, 1, 7, 3)$. Applying this result to the solutions $(x_2, y_2)$ and $(x_3, y_3)$ and noting that all three cases just listed have already been excluded, we see that $a$ must be an odd prime. Combining the above two equations, we get

$$a^{x_2} - a^{x_1} + 1 = b^{2t},$$

contradicting the main theorem of [11] (see the Theorem in the introduction of [11], noting that $p > 2$ is intended; see also Proposition 4.1 in the Appendix of the present paper) unless $(a, b, c) = (3, 5, 2)$ or $(5, 11, 4)$. Considering each of these two cases modulo 3, we see that neither case allows a solution to (1.2) with $y$ odd, so neither case has a third solution. □

We are now ready to prove Theorem 1 itself.

*Proof of Theorem 1.* By Lemma 2.1, we can assume $a \geq 6$.

Theorem 1.1 of [3] (Theorem A of this paper) handles the case when the exponents $x$ and $y$ are restricted to positive integers only, so we can assume from here on that (1.2) has exactly three solutions $(x_1, y_1)$, $(x_2, y_2)$, and $(x_3, y_3)$ with

$$0 = y_1 < y_2 < y_3, 1 \leq x_1 < x_2 < x_3. \tag{2.1}$$

(2.1) shows that $\gcd(a, c) = 1$ so that $\gcd(a, b) = 1$. Up to a point, the methods of Bennett in handling the case $\gcd(a, b) = 1$ in the proof of Theorem 1.1 of [3] apply even when $y_1 = 0$; in particular, we can use $\frac{x_3}{\log b} < 5309$, which is Equation (3.6) of [3], to derive the following two inequalities:

$$y_3 < 5309 \log(a) \tag{2.2}$$

and

$$a^{x_2-x_1} \le 5309 \tag{2.3}$$

(see page 904 of [3]). Also (as in page 905 of [3]) we can assume that $x_3/y_3 = p_r/q_r$ where $p_r/q_r = \frac{a_r p_{r-1}+p_{r-2}}{a_r q_{r-1}+q_{r-2}}$ is the $r$-th convergent in the simple continued fraction

$$\frac{\log(b)}{\log(a)} = [a_0; a_1, a_2, a_3, \dots] \tag{2.4}$$

where the $a_i$ are the partial quotients of the continued fraction. Letting $a_{r+1}$ be the $(r+1)$-th partial quotient in (2.4), we can use $a_{r+1} > \frac{b^{y_3}\log a}{cy_3} - 2$, which is Equation (3.9) of [3]. Then, using $b^{y_2} > c$ (since $a^{x_1}(a^{x_2-x_1}-1) = b^{y_2}-1$ and $a^{x_1} > c$) we can assume (after (3.9) of [3])

$$a_{r+1} > \frac{b^{y_3-y_2}\log(a)}{y_3} - 2. \tag{2.5}$$

Note that these results do not require $y_1 > 0$. But when $y_1 = 0$, we cannot immediately get a bound on $b$ as in [3], so instead we obtain a bound on $x_1$ so that we can use (2.3) to obtain a bound on $x_2$, allowing us to use the solution $(x_2, y_2)$to obtain a bound on $b$. To do this requires several new steps.

We first show $y_2 \mid y_3$. We have

$$a^{x_1}(a^{x_2-x_1}-1) = b^{y_2}-1 \tag{2.6}$$

and

$$a^{x_1}(a^{x_3-x_1}-1) = b^{y_3}-1. \tag{2.7}$$

Let $g_1 = \gcd(x_2-x_1, x_3-x_1)$ and $g_2 = \gcd(y_2, y_3)$. Since $a^{g_1}-1$ divides both sides of (2.6) and (2.7), there must be a least number $j$ such that $a^{x_1}(a^{g_1}-1) \mid b^j - 1$, and $j$ must divide $g_2$, so that

$$b^{g_2} - 1 = a^{x_1}(a^{g_1}-1)w \tag{2.8}$$

where $w$ is a positive integer. But then, since $(b^{g_2}-1)/a^{x_1}$ divides both $a^{x_2-x_1}-1$ and $a^{x_3-x_1}-1$, there must be a least number $k$ such that $(a^{g_1}-1)w \mid (a^k-1)$ where $k \mid g_1$, so that $(a^{g_1}-1)w \mid (a^{g_1}-1)$, giving $w = 1$. So now (2.8) shows that taking $(x, y) = (x_1+g_1, g_2)$ gives a solution to (1.2), so that $g_2$ equals one of $y_1$, $y_2$, or $y_3$. But $g_2 = y_3 > y_2$ contradicts the definition of $g_2$. Also, $g_2 \ne y_1 = 0$. So $g_2 = y_2 \mid y_3$.

So we can take $y_2 = 1$ (replacing $b^{y_2}$ by $b$, so that $y_3$ in the new notation corresponds to $y_3/y_2$ in the old notation), giving

$$b = a^{x_2} - a^{x_1} + 1. \tag{2.9}$$

Next we find lower bounds on $y_3$ and $x_3$. From (2.9) we derive

$$\log(b) = x_2\log(a) + \log\left(1 - \frac{1}{a^{x_2-x_1}}\right) + \log\left(1 + \frac{1}{a^{x_2}-a^{x_1}}\right)$$

so that

$$\frac{\log(b)}{\log(a)} = x_2 - \frac{1}{u}$$

where $u > a^{x_2-x_1}\log(a)/2$ (using $\mid \log(1-z) \mid < 2z$ for $0 < z < 0.7968$). Recalling (2.4) we have

$$a_0 = x_2 - 1, a_1 = 1, a_2 = \lfloor u - 1 \rfloor \tag{2.10}$$

where $\lfloor u-1 \rfloor$ is the greatest integer less than or equal to $u-1$. Since $x_3/y_3$ is a convergent $p_r/q_r$ of (2.4) with $r$ odd (since $a^{x_3} > b^{y_3}$), we derive from (2.10) (noting $r = 1$ is impossible)

$$y_3 > \frac{a^{x_2-x_1}\log(a)}{2} \tag{2.11}$$

and

$$x_3 > \frac{a^{x_2-x_1}\log(a)x_2}{2} - 1. \tag{2.12}$$

From (2.12) we derive (using $a \geq 6$)

$$x_3 > 5x_1. \tag{2.13}$$

Next we derive an upper bound on $x_1$.

Assume first $2x_1 \geq x_2$. Using (2.9) we have

$$\begin{aligned} a^{x_3} &= b^{y_3} + c \\ &= (a^{x_2} - a^{x_1} + 1)^{y_3} + a^{x_1} - 1 \\ &= G + \frac{y_3(y_3-1)}{2}a^{2x_1}(a^{x_2-x_1}-1)^2 + y_3a^{x_2} - (y_3-1)a^{x_1} \end{aligned} \tag{2.14}$$

where $G$ is an integer divisible by $a^{3x_1}$. Then, by (2.13), we must have $y_3 - 1 = ha^{x_2-x_1}$ for some integer $h$, so that, letting $\lambda = 0$ or 1 according as $a$ is odd or even, (2.14) becomes

$$a^{x_3} = G + \frac{y_3h}{2^{1-\lambda}}(a^{x_2-x_1}-1)^2\frac{a^{x_1+x_2}}{2^\lambda} + (y_3-h)a^{x_2}$$

where $\frac{y_3h}{2^{1-\lambda}}$ is an integer. Thus,

$$\frac{a^{x_1}}{2^\lambda} \mid y_3 - h > 0, \tag{2.15}$$

which, with (2.2), gives

$$a^{x_1} < 2^\lambda 5309\log(a). \tag{2.16}$$

If, on the other hand, $2x_1 < x_2$, then (2.3) implies $a^{x_1} < 5309$ which implies (2.16). So we can use (2.16) to get a bound on $x_1$ in terms of $a$.

Next we obtain an upper bound on $a$. Assume $a \geq 241$. Then from (2.16) we get $x_1 = 1$, so that using (2.3) we get $x_2 = 2$. In this case, noting that (2.15) holds when $2x_1 \geq x_2$, we have

$$y_3 - \frac{y_3 - 1}{a} = \frac{ja}{2^\lambda} \tag{2.17}$$

for some positive integer $j$. From (2.17) we get

$$y_3 = \frac{\frac{ja^2}{2^\lambda} - 1}{a - 1} = a + 1 + t\frac{a^2}{2^\lambda} \tag{2.18}$$

where $t = \frac{j - 2^\lambda}{a-1}$ must be an integer since $y_3$ is an integer and $\gcd(a, a-1) = 1$. If $t \leq 0$ then (2.18) contradicts (2.11) since $a \geq 241$; if $t > 0$ then (2.18) implies $a^2/2^\lambda < y_3 < 5309 \log(a)$ which is impossible for $a \geq 241$. So we must have

$$a < 241. \tag{2.19}$$

Now for each $a < 241$, we use (2.16) to find all possible $x_1$ and then use (2.3) to find all possible $x_2$. We then find $b$ using (2.9) and then examine the numbers $q_i$, which are the denominators of the convergents in the simple continued fraction expansion of $\log(b)/\log(a)$. $y_3 = q_r$ for some $r$. If (1.2) has three solutions when $a \geq 6$, we must have some $q_r$ and $q_{r+1}$ such that

$$q_r < 5309 \log(a) \tag{2.20}$$

and

$$q_{r+1} > \frac{b^{q_r - 1} \log(a)}{q_r} - 2 \tag{2.21}$$

where (2.20) follows from (2.2) and (2.21) follows from (2.5), noting $q_{r+1} > a_{r+1}$. For convenience in calculation we actually use

$$q_r \leq \lfloor 5309 \log(240) \rfloor = 29096 \tag{2.22}$$

and

$$q_{r+1} > \frac{2b^d}{a} - 2, d = \frac{a \log(a)}{2} - 1 \tag{2.23}$$

where (2.23) is derived from replacing $q_r$ in (2.21) by $\frac{a \log(a)}{2}$, recalling (2.11). We find no cases satisfying both (2.22) and (2.23). □

## 3. Proof of Theorem 2

We will use two elementary lemmas.

**Lemma 3.1.** *Let $R$, $S$, $M$, and $t_1$ be positive integers such that $\gcd(R, S) = 1$ and $M \mid R^{t_1} - S^{t_1}$. Let $t_0$ be the least positive integer such that $M \mid R^{t_0} - S^{t_0}$. Then $t_0 \mid t_1$.*

*Proof.* Let $t_1 = st_0 + r$, $0 \le r < t_0$. Since $R^{t_0} \equiv S^{t_0} \bmod M$ and $R^{t_1} \equiv S^{t_1} \bmod M$, we must have $R^r \equiv S^r \bmod M$. Since $t_0$ is the least positive value of $t$ such that $R^t \equiv S^t \bmod M$, we must have $r = 0$ so that $t_0 \mid t_1$. □

**Lemma 3.2.** *If $R$, $S$, $t_1$, and $t_2$ are positive integers with $\gcd(R, S) = 1$, $R > S$, $t_1 > t_2$, $t_2 \mid t_1$, and each prime dividing $R^{t_1} - S^{t_1}$ also divides $R^{t_2} - S^{t_2}$, then $t_1 = 2$, $t_2 = 1$, and $R + S = 2^\alpha$ for some integer $\alpha > 1$.*

*Proof.* Assume $R^{t_1} - S^{t_1}$ is divisible only by primes which divide $R^{t_2} - S^{t_2}$. Considering the binomial expansion $((R^{t_2} - S^{t_2}) + (S^{t_2}))^p$ where $p$ is a prime dividing $t_1/t_2$ (noting that $R^{pt_2} - S^{pt_2} \mid R^{t_1} - S^{t_1}$), we find $t_1 = 2t_2$ with $R^{t_2} + S^{t_2} = 2^\alpha$ for some integer $\alpha > 1$, which requires $t_2$ odd, $R + S = 2^\alpha$, $t_2 = 1$. (See also the stronger result in [7, Theorem V].) □

For Lemma 3.3 which follows, we will need some notation. For each solution $(x, y)$ to (1.3) we write

$$A^x = \frac{u_x}{v_x}, B^y = \frac{u_y}{v_y}$$

where $u_x$ and $v_x$ are relatively prime positive integers, and $u_y$ and $v_y$ are relatively prime positive integers. Let $C = c/d$ where $c$ and $d$ are relatively prime positive integers. We have

$$u_x v_y - u_y v_x = \frac{c}{d} v_x v_y. \tag{3.1}$$

Let $p^k \parallel d$ for some prime $p$ and integer $k \ge 0$. Then there are just three possible types of solutions which we will call Type X, Type Y, and Type E:

- we say that a solution $(x, y)$ to (1.3) is 'Type X for $p$' when
$$p^k \parallel v_x, p^k \not\mid v_y; \tag{3.2}$$
- we say that a solution $(x, y)$ to (1.3) is 'Type Y for $p$' when
$$p^k \parallel v_y, p^k \not\mid v_x; \tag{3.3}$$
- we say that a solution $(x, y)$ to (1.3) is 'Type E for $p$' when, for some integer $q$,
$$p^q \parallel v_x, p^q \parallel v_y, q \ge k. \tag{3.4}$$

Now write

$$A = \frac{a}{g}, B = \frac{b}{h}$$

where $a$, $b$, $g$, $h$ are positive integers such that $\gcd(a, g) = 1$, $\gcd(b, h) = 1$, and neither $a/g$ nor $b/h$ equals 1. As before, take $C = c/d$. We can rewrite (1.3) as

$$\left(\frac{a}{g}\right)^x - \left(\frac{b}{h}\right)^y = \frac{c}{d}. \tag{3.5}$$

**Observation 3.1.** *If (3.5) has more than one solution for which both $x$ and $y$ are positive, then, for any prime $p$, $p \mid g \iff p \mid h$.*

*Proof.* Suppose there is a prime $p_h$ such that $p_h \mid h$ but $p_h \nmid g$. Then any solution to (3.5) with both $x > 0$ and $y > 0$ must be Type Y for $p_h$, so that, by (3.3), there is at most one such solution. Similarly, if there is a prime $p_g$ such that $p_g \mid g$ but $p_g \nmid h$, there can be at most one solution with $x$ and $y$ positive. □

Now we are ready to state

**Lemma 3.3.** *Suppose that, for positive integers $a$, $b$, $g$, $h$, $c$, $d$ with $g > 1$, (3.5) has two solutions $(x_1, y_1)$ and $(x_2, y_2)$ with $\min(x_1, y_1, x_2, y_2) > 0$, taking $x_1 > x_2$. If both the solutions $(x_1, y_1)$ and $(x_2, y_2)$ are Type E with $q > k$ for every prime dividing $g$, then (3.5) has no further solution $(x, y)$ where $x$ and $y$ are any integers, positive, negative, or zero, except when $(a, g, b, h, c, d : x_1, y_1; x_2, y_2; x_3, y_3) = (2^n - 1, 2^n, 1, 2, 2^{n-1} - 1, 2^{n-1} : 2, 2n; 1, n; 0, n - 1)$ where $n > 1$ is a positive integer.*

*Proof.* Assume (3.5) has two solutions $(x_1, y_1)$ and $(x_2, y_2)$ with

$$\min(x_1, y_1, x_2, y_2) > 0$$

such that both the solutions $(x_1, y_1)$ and $(x_2, y_2)$ are Type E with $q > k$ for every prime dividing $g > 1$. Let $x_1/y_1 = m/n$ where $m$ and $n$ are positive integers such that $\gcd(m, n) = 1$. Let $p$ be any prime such that $p^i \parallel g$ for some positive integer $i$. Then there must exist a positive integer $j$ such that $p^j \parallel h$ and

$$im = jn,$$

from which, using Observation 3.1, we derive the result that there exists a positive integer $w$ such that

$$g = w^n, h = w^m.$$

Since also $\frac{x_2}{y_2} = \frac{m}{n}$, we can write $x_1 = mt_1$, $y_1 = nt_1$, $x_2 = mt_2$, $y_2 = nt_2$, where $t_1$ and $t_2$ are positive integers, taking $t_1 > t_2$. Then, for $\nu$ in the set $\{1, 2\}$,

$$\left(\frac{a^m}{w^{mn}}\right)^{t_\nu} - \left(\frac{b^n}{w^{mn}}\right)^{t_\nu} = \frac{c}{d} \tag{3.6}$$

so that

$$(a^m)^{t_\nu} - (b^n)^{t_\nu} = c\left(\frac{w^{mnt_\nu}}{d}\right) \tag{3.7}$$

where

$$d \mid w^{mnt_\nu}. \tag{3.8}$$

From (3.8) we see that every prime dividing $d$ divides $g$ so that both of the solutions $(x_1, y_1)$ and $(x_2, y_2)$ are Type E with $q > k$ for every prime

dividing $d$, so that $\frac{w^{mnt_\nu}}{d}$ is an integer divisible by every prime dividing $d$. Thus, for every prime $p$,

$$p \mid (a^m)^{t_1} - (b^n)^{t_1} \iff p \mid (a^m)^{t_2} - (b^n)^{t_2}. \tag{3.9}$$

Now let $\gcd(a^m, b^n) = z$. Let $a_0 = a^m/z$ and $b_0 = b^n/z$ so that

$$z^t(a_0^t - b_0^t) = (a^m)^t - (b^n)^t \tag{3.10}$$

where $\gcd(a_0, b_0) = 1$ and $t$ can equal either $t_1$ or $t_2$. Since $\gcd(a, w) = \gcd(b, w) = 1$, we see from (3.7) that any prime dividing $z$ must divide $c$. If $z > 1$, let $p^v \parallel c$, where $p$ is a prime which divides $z$ and $v$ is a positive integer. Then also $p^v \parallel (a^m)^t - (b^n)^t$ for $t = t_1$ and for $t = t_2$. But, since $z^{t_2} < z^{t_1}$, by (3.10) we see that, if $v_1$ and $v_2$ are nonnegative integers such that $p^{v_1} \parallel a_0^{t_1} - b_0^{t_1}$ and $p^{v_2} \parallel a_0^{t_2} - b_0^{t_2}$, we must have

$$v_1 < v_2. \tag{3.11}$$

In what follows we allow $z = 1$ as well as $z > 1$.

Let $\prod_{\iota=1}^{\mu} p_\iota^{\alpha_\iota}$ be the prime factorization of $a_0^{t_1} - b_0^{t_1}$, and let $M = \prod_{\iota=1}^{\mu} p_\iota$. Let $t_0$ be the least positive integer such that $M \mid a_0^{t_0} - b_0^{t_0}$. Noting that (3.11) holds when $z > 1$, we see, using (3.9) and (3.10), that $M \mid a_0^{t_2} - b_0^{t_2}$, so $t_0 < t_1$. By Lemma 3.1, $t_0 \mid t_1$, so that Lemma 3.2 gives $t_1 = 2$, $t_2 = t_0 = 1$, and $a_0 + b_0 = 2^\alpha$, where $\alpha > 1$ is an integer. We get

$$a^m + b^n = 2^\alpha \tag{3.12}$$

by showing $z = 1$: noting that (3.11) holds when $z > 1$, we find (since $t_2 \mid t_1$)

$$z = 1, \gcd(a, b) = 1, a_0 = a^m, b_0 = b^n,$$

so that (3.12) holds.

Since $t_1 = 2$ and $t_2 = 1$, we have, recalling (3.6) ,

$$\left(\frac{a^m}{w^{mn}}\right) - \left(\frac{b^n}{w^{mn}}\right) = \left(\frac{a^m}{w^{mn}}\right)^2 - \left(\frac{b^n}{w^{mn}}\right)^2 = \frac{c}{d},$$

which requires

$$w^{mn} = a^m + b^n = 2^\alpha, \tag{3.13}$$

by (3.12). We have $\gcd(c, d) = 1$, $\gcd(a^m - b^n, a^m + b^n) = 2$, $\frac{c}{d} = \frac{a^m - b^n}{a^m + b^n}$, so that

$$d = \frac{a^m + b^n}{2} = \frac{w^{mn}}{2} = 2^{\alpha - 1}. \tag{3.14}$$

Note $\alpha - 1$ corresponds to $k$ in (3.2), (3.3), and (3.4) when $p = 2$.

Now suppose $(x_3, y_3)$ is a third solution to (3.5). Using (3.13) and (3.14) and noting $\alpha > 1$, we see that at least one of $x_3$ and $y_3$ is positive, so it suffices to consider two cases (according as $nx_3 = my_3$ or not):

*Case 1.* Equation (3.5) has three solutions $(x, y)$:$(2m, 2n), (m, n), (mt_3, nt_3)$, where $t_3 > 2$ is a positive integer.

*Case 2.* Equation (3.5) has three solutions $(x, y)$: $(2m, 2n)$, $(m, n)$, $(x_3, y_3)$, where $nx_3 \neq my_3$ and $\max(x_3, y_3) > 0$.

If Case 1 holds, then we have (3.6) with $\nu = 3$, so that the solution $(x_3, y_3)$ is Type E with $q > k$ for every prime dividing $w$, so that we can use the same reasoning as above to get $t_3 = 2$, a contradiction.

It remains to treat Case 2. In the notation of (3.2), (3.3), and (3.4), for the solution $(x_3, y_3)$ we have

$$v_x = w^{nx_3}, v_y = w^{my_3}. \tag{3.15}$$

Assume first $nx_3 > my_3$. Then $(x_3, y_3)$ must be Type X for 2, so that, using (3.2) with (3.15) and (3.14), we find

$$d = w^{nx_3} = \frac{w^{mn}}{2} = 2^{\alpha-1}, \tag{3.16}$$

which requires $w = 2$ and $n = 1$, so that (3.13) becomes $2^m = a^m + b$, which requires $a = 1$, $g = w^n = 2$, $b = 2^m - 1$, $h = w^m = 2^m$, $c/d = (1-b)/2^m \leq 0$, contradicting $c/d > 0$.

So we must have $my_3 > nx_3$, so that, using the same reasoning as above, (3.16) becomes

$$d = w^{my_3} = \frac{w^{mn}}{2} = 2^{\alpha-1}, \tag{3.17}$$

which requires $w = 2$ and $m = 1$, so that (3.13) becomes $2^n = a + b^n$, which requires

$$b = 1, h = w^m = 2, a = 2^n - 1, g = 2^n, \frac{c}{d} = \frac{a-1}{2^n} = \frac{2^{n-1}-1}{2^{n-1}}.$$

Since $w = 2$ and $m = 1$, (3.17) shows that the only possible third solution has $y_3 = n - 1$, which requires $x_3 = 0$, giving the exception in Lemma 3.3. □

*Proof of Theorem 2:* Assume (1.3) has three solutions $(x_1, y_1)$, $(x_2, y_2)$, $(x_3, y_3)$.

Consider first the case in which $C$ is not an integer, so that $d > 1$ in (3.5). Let $p$ be any prime dividing $d$ with $p^k \parallel d$ for some positive integer $k$, and let

$$p^{i_1} \parallel v_{x_1}, p^{i_2} \parallel v_{x_2}, p^{i_3} \parallel v_{x_3}, p^{j_1} \parallel v_{y_1}, p^{j_2} \parallel v_{y_2}, p^{j_3} \parallel v_{y_3},$$

where $i_1$, $i_2$, $i_3$, $j_1$, $j_2$, $j_3$ are nonnegative integers and

$$A^{x_1} = \frac{u_{x_1}}{v_{x_1}}, B^{y_1} = \frac{u_{y_1}}{v_{y_1}}, A^{x_2} = \frac{u_{x_2}}{v_{x_2}}, B^{y_2} = \frac{u_{y_2}}{v_{y_2}}, A^{x_3} = \frac{u_{x_3}}{v_{x_3}}, B^{y_3} = \frac{u_{y_3}}{v_{y_3}},$$

where all fractions are in reduced form.

Assume first that $(x_1, y_1)$ is Type E for $p$, $(x_2, y_2)$ is Type X for $p$, and $(x_3, y_3)$ is Type Y for $p$. Then (3.2), (3.3), and (3.4) require

$$i_1 > i_2 > i_3 \geq 0, \tag{3.19}$$

which requires either $u_{x_1}/v_{x_1} > u_{x_2}/v_{x_2} > u_{x_3}/v_{x_3}$ or $u_{x_1}/v_{x_1} < u_{x_2}/v_{x_2} < u_{x_3}/v_{x_3}$ so that

$$\min\left(A^{x_1}, A^{x_2}, A^{x_3}\right) < A^{x_2} < \max\left(A^{x_1}, A^{x_2}, A^{x_3}\right). \tag{3.20}$$

Similarly (3.2), (3.3), and (3.4) require

$$j_1 > j_3 > j_2 \geq 0, \tag{3.21}$$

which requires

$$\min\left(B^{y_1}, B^{y_2}, B^{y_3}\right) < B^{y_3} < \max\left(B^{y_1}, B^{y_2}, B^{y_3}\right). \tag{3.22}$$

But now considering (1.3), we see that (3.20) requires

$$\min\left(B^{y_1}, B^{y_2}, B^{y_3}\right) < B^{y_2} < \max\left(B^{y_1}, B^{y_2}, B^{y_3}\right),$$

contradicting (3.22). So we cannot simultaneously have solutions of Type E, Type X, and Type Y for $p$.

From (3.2) and (3.3) we see that there is at most one solution which is Type X for $p$ and at most one solution which is Type Y for $p$. So now we see that at least two of the three solutions under consideration must be Type E for $p$. Now let $p_1$ be any prime distinct from $p$ such that $p_1^{k_1} \parallel d$ for some positive integer $k_1$. Using the same argument as above, we see that at least two of the three solutions under consideration must be Type E for $p_1$. Since the set of three solutions under consideration contains at least two solutions which are Type E for $p$ and at least two solutions which are Type E for $p_1$, it must contain at least one solution which is Type E for both $p$ and $p_1$. Now recalling (3.4) we see that without loss of generality we can assume that in (1.3) $A$ and $B$ are such that $A = a/g$ and $B = b/h$ with $pp_1 \mid g$ and $pp_1 \mid h$; indeed, $g$ and $h$ are each divisible by every prime dividing $d$. Take $x_1 > x_2 > x_3$. Then, noting that for every prime $p$ dividing $d$ at least two of the three solutions under consideration are Type E, we can use (3.2), (3.3), and (3.4) to see that the solutions $(x_1, y_1)$ and $(x_2, y_2)$ are both Type E for $p$ with $q > k$, where $p^k \parallel d$ with $k > 0$ and $\min(x_1, y_1, x_2, y_2) > 0$.

Now let $p_2$ be any prime dividing $g$ which does not divide $d$, where we are using the same $A = a/g$ and $B = b/h$ and the same $x_1 > x_2 > x_3$ as above, so that $\min(x_1, y_1, x_2, y_2) > 0$. Any solution to (1.3) must be Type E for $p_2$ since Type X and Type Y are impossible by (3.2) and (3.3). Since here we have $p_2^{k_2} \parallel d$ with $k_2 = 0$, we see that the solutions $(x_1, y_1)$ and $(x_2, y_2)$ are both Type E for $p_2$ with $q > k_2$ (noting $q > 0$ since $p_2 \mid g$). Thus we have shown that the solutions $(x_1, y_1)$ and $(x_2, y_2)$ are Type E with $q > k$ for every prime dividing $g > 1$ (so that every such prime also divides $h$), where $\min(x_1, y_1, x_2, y_2) > 0$. Now we can apply Lemma 3.3 to the solutions $(x_1, y_1)$ and $(x_2, y_2)$ to show that there can be no third solution to (1.3) when $d > 1$, except for the second exceptional case in the formulation of Theorem 2.

Now consider the case in which $C$ is an integer so that $d = 1$ in (3.5). This requires

$$v_x = v_y \tag{3.23}$$

for every solution $(x, y)$ to (1.3), since (3.1) must hold. Since $C \geq 1$, $A^x > 1$ for every solution to (1.3), so we can assume without loss of generality that $x$ is positive in any solution $(x, y)$ to (1.3). At most one solution to (1.3) has $y = 0$, and (3.23) shows that we can take $y > 0$ in any solution such that $y \neq 0$.

Now, if $v_x = 1$ in any solution $(x, y)$ to (1.3), then $v_x = v_y = 1$ for every solution, and we have the equivalent of (1.2) which is handled by Theorem 1, giving the first exceptional case in the formulation of Theorem 2.

If $v_x > 1$ for any solution $(x, y)$ to (1.3), then $v_x = v_y > 1$ for every solution, so that, taking $A = a/g$ and $B = b/h$ as in (3.5), we have $g > 1$ and $h > 1$. Let $p$ be any prime dividing $g$. Then, since $d = 1$, every solution $(x, y)$ to (1.3) must be Type E for $p$ with $q > k = 0$. Thus the conditions of Lemma 3.3 are met, and we can use Lemma 3.3 to show there is no third solution when $d = 1$ (except for the first exceptional case in the formulation of Theorem 2).

It remains to show there are an infinite number of choices of $A$, $B$, $C$ for which (1.3) has exactly two solutions $(x, y)$ by referring to the cases mentioned in the Introduction. □

## 4. Appendix: the equation $p^r \pm p^s + 1 = z^2$

In this appendix we give a short elementary proof of Proposition 4.1 below, which is proven in [11] using lower bounds on linear forms in logarithms, a deep result of Bennett and Skinner [5], and the well known result of Bilu, Hanrot, and Voutier [6].

**Proposition 4.1.** *(see the Theorem in the introduction of* [11]*) The only solutions to the equation*

$$p^r + (-1)^v p^s + 1 = z^2$$

*in positive integers* $(z, p, r, s)$ *and* $v \in \{0, 1\}$ *with* $r \neq s$ *and* $p$ *an odd prime are* $(z, p, r, s) = (5, 3, 3, 1)$, $(11, 5, 3, 1)$, *with* $v = 1$ *in both cases.*

The key to making Proposition 4.1 elementary is the use of Lemmas 4.1 and 4.2 below. Lemma 4.1 removes the need for the use of lower bounds on linear forms in logarithms and [5], greatly shortening the proof; then Lemma 4.2 immediately gives Proposition 4.1, bypassing the need for [6]. The clever use of continued fractions in [11] remains untouched.

**Lemma 4.1.** *Let* $D \neq 1$ *be any squarefree integer, let* $u$ *be a positive integer, and let* $S$ *be the set of all numbers of the form* $r + s\sqrt{D}$, *where* $r$ *and* $s$ *are nonzero rational integers,* $(r, sD) = 1$, *and* $u|s$. *Let* $p$ *be any*

*odd prime number, and let $t$ be the least positive integer such that $\pm p^t$ is expressible as the norm of a number in $S$, if such $t$ exists. Then, if $\pm p^n$ is also so expressible, we must have $t|n$. (Note the $\pm$ signs in the statement of this lemma are independent.)*

Comment: We will use this lemma when $D > 0$ to bypass the problem of units.

*Proof.* Assume that for some $p$ and $S$, there exists $t$ as defined in the statement of the lemma. Then $p$ splits in $\mathbb{Q}(\sqrt{D})$; let $[p] = PP'$, where $P$ and $P'$ are prime ideals in $\mathbb{Q}(\sqrt{D})$. For each positive integer $k$ there exists an $\alpha$ in $S$ such that $P^{kt} = [\alpha]$. Now suppose $\pm p^{kt+g}$ equals the norm of some $\gamma$ in $S$ where $g$ is a positive integer with $g < t$. Since $P^{kt+g}$ must be principal, $P^g = [\beta]$ for some irrational integer $\beta \in \mathbb{Q}(\sqrt{D})$. Therefore, for some unit $\epsilon$, either $\gamma = \epsilon\alpha\beta$ or $\bar{\gamma} = \epsilon\alpha\beta$. $\epsilon\alpha\beta$ has integer coefficients and the norm of $\alpha$ is odd, so $\epsilon\beta$ has integer coefficients. Now $\alpha \in S$ and $\epsilon\alpha\beta \in S$, so that one can see that $\epsilon\beta \in S$, which is impossible by the definitions of $t$ and $g$. □

**Lemma 4.2.** *The equation*

$$(1 + \sqrt{-D})^r = m \pm \sqrt{-D} \tag{4.1}$$

*has no solutions with integer $r > 1$ when $D$ is a positive integer congruent to 2 mod 4 and $m$ is any integer, except for $D = 2$, $r = 3$.*

*Further, when $D$ congruent to 0 modulo 4 is a positive integer such that $1 + D$ is prime or a prime power, (4.1) has no solutions with integer $r > 1$ except for $D = 4$, $r = 3$.*

*Proof.* Assume (4.1) has a solution with $r > 1$ for some $m$ and even $D$. From Theorem 13 of [2], we see that $r$ is a prime congruent to 3 mod 4 and there is at most one such $r$ for a given $D$. Thus we obtain

$$(-1)^{\frac{D+2}{2}} = r - \binom{r}{3}D + \binom{r}{5}D^2 - \cdots - D^{\frac{r-1}{2}}. \tag{4.2}$$

If $r = 3$, (4.2) shows that $|D - 3| = 1$, giving the two exceptional cases of the Lemma. So from here on we assume $3 \nmid r$.

We will use two congruences:

Congruence 1 : $$(-1)^{\frac{D+2}{2}} \equiv \left(\frac{r}{3}\right)2^{r-1} \bmod D - 3$$

Congruence 2 : $$(-1)^{\frac{D+2}{2}} \equiv 2^{r-1} \bmod D + 1$$

Congruences 1 and 2 correspond to congruences (9e) and (9f) of Lemma 7 of [2] and can be derived by considering the expansions of $(1 + \sqrt{-3})^r$ and $(1 + 1)^r$ respectively. Noting that $r - 1 \equiv 2 \bmod 4$, from Congruence 1 we

see that $D-3$ cannot be divisible both by a prime 3 mod 4 and a prime 5 mod 8. So $D \equiv 2 \bmod 4$ implies $D \not\equiv 3 \bmod 5$. Now let $D+1=y$. If $D \equiv 1 \bmod 5$, $y^r \equiv 3 \bmod 5$; since $m^2+D=y^r$, $m^2 \equiv 2 \bmod 5$, impossible. If $D \equiv 2 \bmod 5$, $y^r \equiv 2 \bmod 5$, so that 5 divides $m$. But then we see from (4.1) that $5|m$ implies $3|r$, which we have excluded. Now $y^r$ is congruent to $-y$ modulo $y^2+1$ so that $m^2$ is congruent $-2y+1$ modulo $y^2+1$. So, using the Jacobi symbol, we must have

$$\begin{aligned} 1 = \left(\frac{-2y+1}{(y^2+1)/2}\right) &= \left(\frac{2y^2+2}{2y-1}\right) \\ &= \left(\frac{y+2}{2y-1}\right) \\ &= \left(\frac{-5}{y+2}\right). \end{aligned}$$

If $D \equiv 2 \bmod 4$, then $y \equiv 3 \bmod 4$ and the last Jacobi symbol in this sequence equals $\left(\frac{y+2}{5}\right) = \left(\frac{D+3}{5}\right)$, which has the value $-1$ when $D$ is congruent to 0 or 4 modulo 5. Thus, when $D \equiv 2 \bmod 4$ and $r \neq 3$, we have shown that there are no values of $D$ modulo 5 that are possible.

So we assume hereafter that $D \equiv 0 \bmod 4$. Write $D+1=p^n$ where $p$ is prime, and let $g$ be the least number such that $2^g \equiv -1 \bmod p$, noting Congruence 2. We see that $g|r-1$ and also $g|p-1|p^n-1=D$. Now (4.2) gives $-1 \equiv 1 \bmod g$ so that $g \leq 2$. Assume first that $n$ is odd. Since $4|D$, $p \equiv 1 \bmod 4$. In this case, we must have $g=2$, $p=5$. If $n$ is even, since we have $1+D=p^n$ and $m^2+D=p^{rn}$, we must have $2p^{rn/2}-1 \leq D=p^n-1$, giving $r<2$, impossible. So we have $n$ odd, $p=5$.

Since $n$ is odd, $D \equiv 4 \bmod 8$, and, since $\binom{r}{3}$ is odd, (4.2) gives $r \equiv 3 \bmod 8$. Now assume $r \equiv 2 \bmod 3$ and let $y=5^n=1+D$. Then $y^r \equiv y^2 \bmod y^3-1$, so that $m^2 \equiv y^2-y+1 \bmod y^2+y+1$, so that

$$\begin{aligned} 1 &= \left(\frac{y^2-y+1}{y^2+y+1}\right) \\ &= \left(\frac{-2y}{y^2+y+1}\right) \\ &= \left(\frac{-2}{y^2+y+1}\right) \end{aligned}$$

which is false since $y^2+y+1 \equiv 7 \bmod 8$. Thus we have $r \equiv 19 \bmod 24$ so that $y^r \equiv -y^7 \bmod y^{12}+1$, so that $m^2 \equiv -y^7-y+1 \bmod \frac{y^{12}+1}{2}$. Thus we

have

$$\begin{aligned}1 &= \left(\frac{-y^7-y+1}{(y^{12}+1)/2}\right) = \left(\frac{y^7+y-1}{(y^{12}+1)/2}\right) = \left(\frac{2(y^{12}+1)}{y^7+y-1}\right)\\ &= \left(\frac{y^{12}+1}{y^7+y-1}\right) = \left(\frac{y^6-y^5-1}{y^7+y-1}\right) = \left(\frac{y^7+y-1}{y^6-y^5-1}\right)\\ &= \left(\frac{y^5+2y}{y^6-y^5-1}\right) = \left(\frac{y^4+2}{y^6-y^5-1}\right) = -\left(\frac{y^6-y^5-1}{y^4+2}\right)\\ &= \left(\frac{2y^2-2y+1}{y^4+2}\right) = \left(\frac{y^4+2}{2y^2-2y+1}\right) = \left(\frac{7}{2y^2-2y+1}\right)\\ &= \left(\frac{2y^2-2y+1}{7}\right)\end{aligned}$$

which is possible only when $y$ is congruent to 1, 4, or 0 modulo 7. This is impossible since $y$ is an odd power of 5. This completes the proof of the lemma. □

*Proof of Proposition 4.1.* First consider the case $v = 0$. We establish some notation by paraphrasing [11, Section 3]: When $v = 0$, we see that the only case in which solutions might exist is when $p \equiv 3 \bmod 4$ and $r - s$ is odd; choose $r$ odd and let $p^s + 1 = Du^2$, with $D$ square-free and $u > 0$ an integer. At this point we diverge from [11] and note that if $S$ is the set of all integers of the form $h + k\sqrt{D}$ with nonzero rational integers $h$ and $k$, $(h, kD) = 1$ and $u|k$, then $p^r$ and $-p^s$ are both expressible as the norms of numbers in $S$. Therefore Lemma 4.1 shows that $\pm p^d$ is expressible as the norm of a number in $S$, where $d$ divides both $r$ and $s$. Now to complete the treatment of the case $v = 0$, we return to the method of proof of [11]: $r$ is odd and $s$ is even, so we have $d \le s/2$. For some coprime positive integers $X$ and $Y$ such that $(X, p^s + 1) = 1$, we must have

$$X^2 - Y^2(p^s + 1) = \pm p^d. \tag{4.3}$$

(4.3) corresponds to (17) in [11]. Since $|p^d| < \sqrt{p^s + 1}$, $X/Y$ must be a convergent of the continued fraction for $\sqrt{p^s + 1}$. But then, since $p^s + 1$ is of the form $m^2 + 1$, we must have $p^d = \pm 1$, impossible.

So we must have $v = 1$. As in [11], we write $p^s - 1 = Du^2$, $D$ and $u$ positive integers and $D$ squarefree. Clearly, $p$ splits in $\mathbb{Q}(\sqrt{-D})$, and we can let $[p] = \pi_1\pi_2$ be its factorization into ideals. We can take

$$\pi_1{}^s = [1 + u\sqrt{-D}], \pi_1{}^r = [z \pm u\sqrt{-D}].$$

At this point we diverge from [11]: clearly $s$ is the least possible value of $n$ such that $p^n = h^2 + k^2u^2D$ for some relatively prime nonzero integers $h$

and $k$, so we can apply Lemma 4.1 to obtain $s|r$. Thus,

$$(1 + u\sqrt{-D})^{r/s} = (z \pm u\sqrt{-D})\epsilon$$

where $\epsilon$ is a unit in $\mathbb{Q}(\sqrt{-D})$. If $D = 1$ or 3, we note $2|u$ and $2 \not| z$, so that we must have $\epsilon = \pm 1$. Now Proposition 4.1 follows from Lemma 4.2. □

Posted on [16] are further simplifications to other proofs in [11] and in [17], which handles the case $2^r + (-1)^v 2^s + 1 = z^2$. ([16] has the same paper referenced in [4] as R. Scott, Elementary treatment of $p^a \pm p^b + 1 = x^2$.) We give a shorter proof of Szalay's result for the case $v = 0$, using a bound of Bauer and Bennett [1]; we also point out that the proof for the case $v = 1$ can be made elementary. An outline of a proof of the result for the case $v = 0$ was given by Mignotte; see the comments at the end of Section D10 of [10].

## References


[1] M. Bauer and M. Bennett, *Applications of the hypergeometric method to the generalized Ramanujan-Nagell equation*, Ramanujan J., **6**, (2002), 209–270.

[2] E. Bender and N. Herzberg, *Some Diophantine equations related to the quadratic form* $ax^2+by^2$,in Studies in Algebra and Number Theory, G.-C. Rota, Ed., pp. 219–272, Advances in Mathematics Supplementary Studies, **6**, Academic Press, San Diego, (1979).

[3] M. Bennett, *On some exponential equations of S. S. Pillai*, Canadian Journal of Mathematics, **53**, 5 (2001), 897–922.

[4] M. A. Bennett, Y. Bugeaud and M. Mignotte, *Perfect powers with few binary digits and related Diophantine problems. II*, Mathematical Proceedings of the Cambridge Philosophical Society, **153**, 3 (2012), 525–540.

[5] M. A. Bennett and C. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math. **56**, (2004), 23-54.

[6] Y. Bilu, G. Hanrot, 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.

[7] G. Birkhoff, H.S. Vandiver, *On the integral divisors of* $a^n - b^n$, Annals of Math., **5**, (1903-1904), 173-180.

[8] Y. Bugeaud, M. Mignotte, *L'équation de Nagell-Ljunggren* $\frac{x^n-1}{x-1} = y^q$, Enseign. Math., **48**, 2 (2002), 147–168.

[9] I. Connell, *Elliptic Curve Handbook*, dated February 1999, `http://www.math.mcgill.ca/connell` accessed 21 Nov 2012.

[10] R. K. Guy, *Unsolved Problems in Number Theory*, Third Edition, Springer, New York, (2004).

[11] F. Luca, *The Diophantine equation* $x^2 = p^a \pm p^b + 1$, Acta Arith., **112**, (2004), 87–101.

[12] M. Mignotte, *A corollary to a theorem of Laurent-Mignotte-Nesterenko*, Acta Arithmetica, **86**, (1998), 101–111.

[13] Z. Scherr, *The real topology of rational points on elliptic curves*, `http://www-personal.umich.edu/~zscherr/papers/rationalpoints.pdf` accessed 21 Nov 2012.

[14] R. Scott, *On the Equations* $p^x - b^y = c$ *and* $a^x + b^y = c^z$, Journal of Number Theory, **44**, 2 (1993), 153–165.

[15] T. Skolem,*Diophantische Gleichungen*, Chelsea Publishing Company, New York, NY (1950).

[16] R. Styer webpage `http://www.homepage.villanova.edu/robert.styer/ReeseScott/index.htm`

[17] L. Szalay, *The equation* $2^N \pm 2^M \pm 2^L = z^2$, Indag. Math., N.S., **13**, 1, (2002), 131–142.

[18] M. Waldschmidt, *Perfect powers: Pillai's works and their developments*, preprint arXiv:0908.4031, 27 Aug 2009.

Reese Scott
86 Boston St
Somerville, MA 02143-2014, USA

Robert Styer
Villanova University
800 Lancaster Avenue
Villanova, PA, USA
*E-mail*: robert.styer@villanova.edu
*URL*: http://www.homepage.villanova.edu/robert.styer/ReeseScott/index.htm