On the generalized Pillai equation $\pm a^x \pm b^y = c$

revised 26 June 2009

Reese Scott

Robert Styer (correspondence author), Dept. of Mathematical Sciences, Villanova University, 800 Lancaster Avenue, Villanova, PA 19085–1699, phone 610–519–4845, fax 610–519–6928, robert.styer@villanova.edu

Abstract We show that the equation $\pm a^x \pm b^y = c$ (where the $\pm$ signs are independent) has at most two solutions (x, y) for given integers a and b both greater than one and c greater than zero, except for listed specific cases. For any prime $a > 5$ and $b = 2$, we show that there are at most two values of c allowing more than one solution to this equation, not counting trivial rearrangements; further restricting a to be a non-Wieferich prime,we improve this result: we show that there are no values of c allowing more than one solution, apart from designated exceptional cases. Finally, we give all solutions to the equation $|a^{x_1} - b^{y_1}| = |a^{x_2} - b^{y_2}|$ for $b = 2$ or 3 and prime a not a base-b Wieferich prime.

§1: Introduction. In this paper, we consider the equation

$$(-1)^u a^x + (-1)^v b^y = c, \tag{i}$$

where a, b, x, and y are positive integers, and u, $v \in \{0, 1\}$. In Section 2, we treat this equation for all a and b greater than one. In Section 3, we treat (i) with both a and b restricted to prime values.

Equation (i) is a generalized form of the familiar Pillai equation

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

which has been treated by many authors from the standpoint of considering the number of solutions (x, y) for given (a, b, c). Bennett [Be] gives a history of these results, and then improves them by showing there are at most two solutions to (ii). In Section 2 of this paper, we show that there are also at most two solutions (x, y, u, v) to (i), although here there are a number of completely specified exceptional cases allowing three or more solutions: see Theorem 1, which generalizes Theorem 1.1 of [Be] and, in a different direction, also generalizes Theorem 7 of [Sc-St].

In handling equation (ii) for the case $\gcd(a, b) = 1$, Bennett uses several inequalities which do not apply to (i), so we use a different method; however, we still use a theorem of Mignotte [Mi] as used by Bennett, and also some auxiliary results (Lemma 1 and Lemma 5) closely paralleling auxiliary results which are found in Section 4 of [Be] but which are not used by Bennett in proving (ii) has at most two solutions. The case $\gcd(a, b) > 1$ is more complicated for (i) than for (ii) and requires a different approach than [Be] (see Lemma 7 and Theorem 4).

Bennett finds eleven (a, b, c) giving exactly two solutions (x, y) to (ii), and conjectures these are the only such (a, b, c). For (i), however, there are three infinite families of (a, b, c) giving exactly two solutions (x, y, u, v), in addition to which we find 58 other such (a, b, c); see the remark following the statement of Theorem 1.

In Section 3, we treat (i) with a and b prime. We first ask which c allow more than one solution (x, y, u, v) to (i) for given odd prime a and $b = 2$. To avoid trivial rearrangements, we consider only the case of two

solutions (x_1, y_1, u_1, v_1) and (x_2, y_2, u_2, v_2) for which $x_1 \leq x_2$ and $y_1 \leq y_2$. Pillai [Pi] and Stroeker and Tijdeman [St-T] found all such c when $\{a, b\}$ equals $\{3, 2\}$. The methods of Pillai, which are elementary congruence methods which are not generalizable, can be used, along with Theorem 4 of [Sc], to show that for $\{a, b\}$ equal to $\{5, 2\}$, there are exactly three such c. When a is a Fermat or Mersenne prime greater than 5, and $b = 2$, it follows from Observation 8 below that there are exactly two such c. Generalizing these results, we prove there are at most two such c for any prime $a > 5$ when $b = 2$ (see Theorem 5). We then show that if we add the additional restriction that a not be a Wieferich prime, we can significantly improve this result: we prove there are no such c for any odd prime a when $b = 2$, apart from designated exceptional cases (see Theorem 6).

Finally, we give a complete list (not counting trivial rearrangements) of all solutions $(a, b, c, x_1, y_1, x_2, y_2)$ to the equation

$$|a^{x_1} - b^{y_1}| = |a^{x_2} - b^{y_2}| = c \tag{iii}$$

for a prime, $a > b$, $b = 2$ or 3, and a not a base-b Wieferich prime (see Theorem 7). It is easily seen that, under these restrictions, the list given in Theorem 7 shows that the only (a, b, c) satisfying (iii) are

$$(3, 2, 1), (5, 2, 3), (3, 2, 5), (13, 3, 10), (3, 2, 13), (11, 2, 7), (5, 3, 2), (3, 2, 7), (F, 2, F - 2) \tag{iv}$$

where F is a Fermat prime greater than 5. The (a, b, c) given in (iv) were shown by Cris Crawford [Sc] to be the only (a, b, c) yielding solutions to (iii) with a prime, b prime, and both a^x and b^y less than 2^{32}. Recently the second author ran a similar search for all $a, b < 25000$ with a^x and b^y less than 10^{20}, finding no other solutions with a and b prime [St1].

Mo De Ze and R. Tijdeman [M-T] have shown that, for a and b primes less than 200, if (i) has two solutions (x_1, y_1) and (x_2, y_2) with $x_1 \leq x_2$ and $y_1 \leq y_2$, we must have $\max\{a^{x_2}, b^{y_2}\} \leq 2^{15}$. They obtain a similar result for the equation $a^x b^y \pm a^z \pm b^w \pm 1 = 0$. Other specific results on various exponential Diophantine equations with prime bases have been given by many authors, see for example [A], [B-F], [Ha], [N], [Sc-St], [U], and [W]. In particular, Le [Le1] conjectured that the equation $p^x + q^y = r^z$, where p, q, and r are distinct primes, has at most one solution in positive integers (x, y, z) with $\min\{x, y, z\} > 1$. In [Le2], Le restates this conjecture. Le's conjecture can be easily proven using results in [Cao], [Sc], and [Sc-St]: by Theorem 6 of [Sc], we can assume that $q = 2$ and that the equation has at most two solutions; by the result in [Cao], if the equation has two solutions with $x, z > 1$, both solutions must have $2 \nmid x$; by Lemma 6 of [Sc], one solution must have y odd and the other must have y even, which is impossible modulo 3 unless $p = 3$; Lemma 2 of [Sc-St] then gives $r = 5$, so that, noting that $3 + 2 = 5$, Theorem 6 of [Sc] completes the proof.

§**2:** Let x and y be positive integers, and take u and $v \in \{0, 1\}$. In this section we consider the number of solutions (x, y, u, v) to the equation

$$(-1)^u a^x + (-1)^v b^y = c \tag{1}$$

for integers a and b greater than one and c greater than zero. Our main result is the following:

Theorem 1 For integers a and b both greater than one and $c > 0$, (1) has at most two solutions (x, y, u, v) except when (a, b, c) or (b, a, c) is:
$(3, 2, 5)$ which gives four solutions,

$(3,2,1)$, $(3,2,7)$, $(3,2,11)$, $(3,2,13)$, $(4,3,13)$, or $(5,2,3)$ which each give three solutions, or a member of the infinite family $(4,2,3\cdot 4^k)$, $k=1,2,3,\ldots$, each member of which gives three solutions.

Note: Since, for any solution, x and y uniquely determine u and v, we will refer to a solution (x,y) rather than a solution (x,y,u,v). Also, when $a=b$, we consider the solution (x,y) to be the same as the solution (y,x). (It is not hard to see that the existence of two solutions when $a=b$ implies (25) or (26) below, but this is not needed here.)

Remark: The question remains: for which (a,b,c) does (1) have exactly two solutions (x,y)? There are three infinite families of such (a,b,c) discussed in the Comments following Lemmas 2, 6, and 7. There are also two trivial infinite families of such (a,b,c): the first of these consists of those cases in which $a^{x_1}=b^{y_2}$ and $a^{x_2}=b^{y_1}$; the second consists of those cases in which $a=b=2$ and $x_i=y_j$ for some $1\le i,j\le 2$. If all these infinite families are excluded from consideration, and if we consider (b,a,c) the same as (a,b,c) and disregard duplications due to a or b being a perfect power, then there are still at least 58 anomalous cases of (a,b,c) giving exactly two solutions to (1). These are the only anomalous solutions with terms less than 10^{20} when $a,b<25000$ (see [Be, (1.2)] and [St1]). Noting that, from any (a,b,c) for which (1) has two solutions (x_1,y_1) and (x_2,y_2) such that $x_2=2x_1$, we can derive a new (a,b,c) by using $a^{2x_1}\pm a^{x_1}=(a^{x_1}\pm 1)^2\mp(a^{x_1}\pm 1)$, and disregarding rearrangements of terms, we can reduce the number of anomalous cases from 58 to 14 (see [St1]).

Theorem 1 is an immediate consequence of Theorems 2, 3, and 4 below. We will need the following lemmata:

Lemma 1 For a and b positive integers with $a>2$, $b>1$, and $\gcd(a,b)=1$, there exists a pair of positive integers (x,y) such that $b^y\pm 1=la^x, \gcd(l,a)=1$. Let n be the least such y and let m be the corresponding x. Then if N and M are positive integers with $M>m$ and $b^N\equiv\pm 1 \bmod a^M$ (where the $\pm$ is independent of the $\pm$ above), then

$$n\frac{a^{M-m}}{2^{g+h-1}}\mid N,$$

where $g=1$ and $h=0$, unless $a\equiv 2 \bmod 4$ and $m=1$ in which case g is the largest integer such that $2^g\mid b\pm 1$ (where the $\pm$ is chosen to maximize g) and h is the largest integer such that $2^h\mid n$.

Proof: This lemma closely parallels Lemma 4.1 of [Be] (note here $m=1$ is possible), and can be proven in the same way, except when $a\equiv 2 \bmod 4$ and $m=1$. For this case, we outline a straightforward elementary proof: suppose that y, w, and l are positive integers such that

$$b^y\pm 1=la^{w+1}, \gcd(l,a)=1. \tag{2}$$

Then the $\pm$ in (2) must be minus, and, if $\min(w)$ is the least possible value of w, then

$$\min(w)=g+h \tag{3}$$

where g and h are defined as in the formulation of the lemma. $y_0=2n(a/2)^{g+h}$ is the least value of y such that (2) holds with $w=g+h$. And $y_i=y_0a^i$ is the least value of y satisfying (2) with $w=g+h+i$. Since $a^{g+h+i+1}\mid b^y-1$ implies $y_i\mid y$, the lemma holds.

Lemma 2 If a and b are relatively prime positive integers greater than one, then, if (1) has three solutions (x_1,y_1), (x_2,y_2), and (x_3,y_3), we cannot have either $x_i=x_j$ or $y_i=y_j$ for $i\ne j$ with i and $j\in\{1,2,3\}$ except when $\{a,b\}$ is $\{3,2\}$ or $\{5,2\}$.

Proof: Assume $\{a, b\}$ is not $\{3, 2\}$ or $\{5, 2\}$ and assume the three solutions referred to in the lemma exist. Suppose $x_1 = x_2$ and, without loss of generality, take $y_1 < y_2$. Then we must have either

$$b^{y_2} - a^{x_1} = a^{x_1} - b^{y_1} = c > 0 \tag{4}$$

or

$$b^{y_2} - a^{x_1} = a^{x_1} + b^{y_1} = c > 0. \tag{5}$$

It is easily seen that no other combination of signs allows $x_1 = x_2$ except for the combinations given in (4) and (5). In either case, we have

$$2a^{x_1} = b^{y_1}(b^h \pm 1) \tag{6}$$

where $h = y_2 - y_1$. From (6) we see that $b^{y_1} = 2$ and $a^{x_1} = 2^h \pm 1$. Since we have assumed $(a, b) \neq (3, 2)$, it is a familiar elementary result that we must have $x_1 = 1$, so that $a = 2^h \pm 1$ and $c = 2^h \mp 1$. Here the upper signs correspond to (4) and the lower signs to (5). We must have

$$a^{x_3} - 2^{y_3} = c > 0 \tag{7}$$

since $a^{x_3} + 2^{y_3} = c$ is impossible, and $2^{y_3} - a^{x_3} = c$ violates Theorem 4 of [Sc] (recall $a > 5$). We see that if (4) holds, then, using $a = 2^h + 1$ with $c = 2^h - 1$ and considering (7) modulo 8, we must have $y_3 = 1$ which is a duplicate solution. On the other hand, if (5) holds, consideration of (7) modulo 8 requires x_3 even so that $a^{x_3} \geq (2^h - 1)^2 > 2^{h+1} + 1 = 2^h + c$, so that $y_3 > h$. But this is impossible modulo 2^{h+1}. The same argument holds when we reverse the roles of a and b.

Comment: Using (6), it is easy to construct infinite families (a, b, c) giving exactly two solutions to (1). Here we are not restricting a and b to be relatively prime.

We are now ready to prove

Theorem 2 For integer $c > 0$ and relatively prime integers $a \geq 24333$ and $b \geq 2$, (1) has at most two solutions (x, y).

Proof: Assume (1) has three solutions (x_1, y_1), (x_2, y_2), and (x_3, y_3) with $a \geq 24333$, and, recalling Lemma 2, take $x_1 < x_2 < x_3$. From the work of Leveque [Lev] and Cassels [Cas], it follows that we can take $c > 1$. Let $Y = \max\{y_2, y_3\}$ and let $y = \min\{y_2, y_3\}$. Now let $\Lambda = |x_3 \log a - Y \log b|$ and let $G = \max\{x_3/\log b, Y/\log a\}$. Applying a theorem of Mignotte [Mi] as given in Section 3 of [Be], and using in Mignotte's formula the parameters chosen by Bennett in Section 6 of [Be], we see that we must have either

$$G < 2409.08 \tag{8}$$

or

$$\log \Lambda > -22.997\,(\log G + 2.405)^2 \log a \log b. \tag{9}$$

Now combining the solutions (x_2, y_2) and (x_3, y_3) we obtain

$$\mid a^{x_3} - b^Y \mid = \pm a^{x_2} \pm b^y = c_1$$

where the $\pm$ signs are independent. Note that the sign in the absolute value on the left must be minus since $x_3 > x_2$ and $Y > y$. It is not hard to see that $c_1 \leq c$. Let $d = \min\{a^{x_3}, b^Y\}$. We see that $\Lambda = \log(1 + c_1/d) < c_1/d \leq c/d$. If (9) holds, we have

$$\log d < \log c + 22.997\,(\log G + 2.405)^2 \log a \log b. \tag{10}$$

Now $\Lambda = \log(1 + c_1/d) \leq \log c$ so that, adding Λ to both sides of (10) and dividing through by $\log a \log b$, we see that (10) implies

$$G < 2\frac{\log c}{\log a \log b} + 22.997\left(\log G + 2.405\right)^2. \tag{11}$$

We now consider the equation

$$a^{x_2}(a^{x_3-x_2} \pm 1) = b^y(b^{Y-y} \pm 1), \tag{12}$$

which is derived by combining the solutions (x_2, y_2) and (x_3, y_3). By Lemma 2 we must have $x_2 > m$ where m is defined as in Lemma 1, since it is easily seen that m is the lowest possible value of any x. Let $w = x_2 - m$. By Lemma 1 we have $na^w/2^{g+h-1}$ divides $Y - y$. Using (3) we see that $Y > n(2(a/2)^w)$. Now $b^n \geq a^m - 1$. From this we derive $n > 0.99999(\log a/\log b)m$, using the fact that $a \geq 24333$. Thus we have $Y = 0.99999(\log a/\log b)k_1 m(2(a/2)^w)$, where k_1 is a real number greater than 1. Therefore, for each of the two possible choices for G, we have

$$G = 0.99999km(2(a/2)^w)/\log b \tag{13}$$

where k is a real number greater than or equal to 1 (clearly $k > 1$ but we allow equality for later purposes).

Now suppose $c > 2a^{x_2}$. Then we must have both b^{y_1} and b^{y_2} greater than $c/2$. Let $t = \min\{y_1, y_2\}$ and let $T = \max\{y_1, y_2\}$. Then we have

$$a^{x_1}(a^{x_2-x_1} \pm 1) = b^t(b^{T-t} \pm 1).$$

Thus, $c/2 < b^t \leq a^{x_2-x_1} \pm 1 < a^{x_2}$, which contradicts $c > 2a^{x_2}$. Thus we can take $c < 2a^{x_2}$, so that

$$2\frac{\log c}{\log a \log b} < 2\left(\frac{\log 2}{\log a \log b} + \frac{w+m}{\log b}\right). \tag{14}$$

Using (14) we see that (11) implies

$$G < 2\left(\frac{\log 2}{\log a \log b} + \frac{w+m}{\log b}\right) + 22.997\left(\log G + 2.405\right)^2. \tag{15}$$

Assume $a > b$. Fixing a and b, we recall (13) and view (15) as an inequality in the variables k, m, and w, noting that k, m and w are all greater than or equal to 1. We see that if (15) holds for any k, m, and w, it must also hold for $k = m = w = 1$. Thus, for fixed a and b, (15) implies

$$\frac{0.99999a}{\log b} < 6 + 22.997\left(\log\left(\frac{0.99999a}{\log b}\right) + 2.405\right)^2. \tag{16}$$

Now both (16) and (8) imply

$$\frac{0.99999a}{\log b} < 2409.08,$$

which is impossible for $a > b$ and $a \geq 24333$. And if $b > a \geq 24333$, the above proof works with the roles of a and b reversed.

For Theorem 3 below, we will need a few more lemmata:

Lemma 3 Let $a > 1$ and $b > 1$ be relatively prime integers. For $1 \leq i \leq t$, let p_i be one of the t distinct prime divisors of a. Let $p_i^{g_i} || b^{n_i} \pm 1$, where n_i is the least number such that $p_i | b^{n_i} \pm 1$ (when $p_i = 2$ we choose the sign to maximize g_i).

Write

$$S = \sum_i g_i \log(p_i)/\log(a).$$

Then, if

$$a^x | b^y \pm 1, \tag{17}$$

where the $\pm$ sign is independent of the above, we must have

$$a^{x-S} | y.$$

Proof: Let $a = \prod_i p_i^{\alpha_i}$. If (17) holds, then for each i, $p_i^{x\alpha_i} | b^y \pm 1$, so that $p_i^{x\alpha_i - g_i} | y$ (in the case $x\alpha_i < g_i$, $p_i^{x\alpha_i - g_i}$ is a fraction that evenly divides y). Thus, y is divisible by

$$\prod_i p_i^{x\alpha_i - g_i} = a^{x-S}.$$

Lemma 4 If $a > 2$ and $(a, b) \neq (3, 2)$, then, in the notation of Lemma 3,

$$S < \frac{a \log b}{2 \log a}.$$

Proof: We assume $a > 2$ and $(a, b) \neq (3, 2)$. Then if a is odd, $\prod_i p_i^{g_i} \leq b^{\phi(a)/2} + 1 \leq b^{(a-1)/2} + 1 < b^{a/2}$, verifying Lemma 4 when a is odd. If $a > 4$ is even, then $\prod_i p_i^{g_i} \leq b^{\phi(a/2)} < b^{a/2}$ verifying the lemma in this case also. Finally, when $a = 4$, define g so that $2^g || b \pm 1$, where the sign is chosen to maximize g. Then the lemma holds unless $\frac{g \log(2)}{\log(4)} \geq \frac{4 \log(b)}{2 \log(4)}$, that is, unless $2^g \geq b^2$, which is impossible.

Lemma 5 Let $a > 2$, $b > 1$, and $c > 0$ be integers with $(a, b) = 1$. If (1) has two solutions (x_1, y_1) and (x_2, y_2), with $x_1 \leq x_2$ and $y_1 \leq y_2$, and if further $a^{x_1} > c/2$, then

$$x_1 < S + k,$$

where S is defined as in Lemma 3, and $k = \frac{8.1 + \log\log a}{\log a}$ when $a < 5346$ and $k = 1.19408$ otherwise.

Proof: When $(a, b) = (3, 2)$, all cases in which (1) has more than one solution are given in [Pi] and the Corollary to Theorem 2 of [Sc-St]; when $(a, b) = (5, 2)$, the elementary methods of [Pi] along with the Corollary to Theorem 2 of [Sc-St] suffice to give all cases in which (1) has more than one solution. The lemma holds in all these cases, so we assume from here on that $(a, b) \neq (3, 2)$ or $(5, 2)$.

Following closely the method of proof in Bennett's Proposition 4.4 [Be], assume there are two solutions to (1) with $a^{x_1} > c/2$, $y_2 \geq y_1$, and $x_2 \geq x_1 = S + k_1$ with $k_1 \geq k$, where k is defined for each a as in the formulation of this lemma. If $y_1 = y_2$, then, using (6) with the roles of a and b reversed, we see that $x_1 = 1$; so we can take $y_1 < y_2$. From the equation

$$a^{x_1}(a^{x_2 - x_1} \pm 1) = b^{y_1}(b^{y_2 - y_1} \pm 1)$$

it follows that

$$b^{y_2 - y_1} \equiv \pm 1 \bmod a^{x_1}$$

and so Lemma 3 implies that $y_2 - y_1 \geq a^{x_1 - S}$. Thus,

$$y_2 > a^{k_1}. \tag{18}$$

On the other hand, $c < 2a^{x_1}$, so

$$\log c < x_1 \log a + \log 2 = (S + k_1) \log a + \log 2.$$

So now we have

$$\frac{y_2 \log b}{\log c} > \frac{a^{k_1} \log b}{(S + k_1) \log a + \log 2}.$$

From Lemma 4 we have

$$S < \frac{a \log b}{2 \log a}$$

and so

$$\frac{y_2 \log b}{\log c} > \frac{a^{k_1}}{\left(\frac{a}{2 \log a} + \frac{k_1}{\log b}\right) \log a + \frac{\log 2}{\log b}} > 10.519$$

where the second inequality follows from $k_1 \geq k$, $a \geq 3$, and $b \geq 2$. Let

$$G = \max\left\{\frac{x_2}{\log b}, \frac{y_2}{\log a}\right\}.$$

Then we have

$$\frac{G}{5.2595} \geq \frac{y_2}{5.2595 \log a} > \frac{2 \log c}{\log a \log b} \tag{19}.$$

Now let $\Lambda = |x_2 \log a - y_2 \log b|$. Applying a theorem of Mignotte as given in Section 3 of [Be], and using in Mignotte's formula the parameters chosen by Bennett in the proof of Proposition 4.4 of [Be] (recall $(a, b) \neq (3, 2)$ or $(5, 2)$), we see that we must have either

$$\log G \leq 8.1 \tag{20}$$

or

$$\log \Lambda > -24.2 \left(\log G + 2.4\right)^2 \log a \log b. \tag{21}$$

First assume $c > 1$. Assume (21) holds. Then, in the same way we derived (11) in the proof of Theorem 2 (here $c_1 = c$), we obtain

$$G < 2 \frac{\log c}{\log a \log b} + 24.2 (\log G + 2.4)^2. \tag{22}$$

Using (19) we obtain

$$G < 29.8815 (\log G + 2.4)^2,$$

which implies $\log G < 8.1$. So, no matter which of (20) or (21) holds, we have from (18)

$$e^{8.1} \geq G \geq \frac{y_2}{\log a} > \frac{a^{k_1}}{\log a},$$

which is impossible since $k_1 \geq k$.

Now assume $c = 1$, so that $\Lambda < \log 2$. Proceeding as with $c > 1$, it is easily seen we can replace (22) by

$$G < \frac{\log 2}{\log a \log b} + 24.2 (\log G + 2.4)^2. \tag{23}$$

From (23) we again derive

$$\frac{a^{k_1}}{\log a} < e^{8.1},$$

impossible since $k_1 \geq k$.

Lemma 6 Let $a > 1$, $b > 1$, and $c_1 > 0$ be relatively prime integers. Suppose (1) has two solutions (x, y) and $(2x, 2y)$, for a, b and $c = c_1$, so that (1) also has two solutions $(x, 2y)$ and $(2x, y)$, for a, b, and $c = c_2$, where c_2 is a positive integer. Then if $\max\{a^x, b^y\} > 4$, (1) does not have three solutions for a, b, and $c = c_1$, nor for a, b, and $c = c_2$.

Proof: Assume that (1) has two solutions (x, y) and $(2x, 2y)$ for a, b, and $c = c_1$, where a, b, and c_1 are as in the statement of the lemma. Assume, without loss of generality, that $a^x > b^y$, and take $a^x > 4$. We must have

$$a^{2x} - b^{2y} = a^x + b^y,$$

since no other combination of signs is possible. Thus, $a^x - b^y = 1$, so that we can assume $\min\{x, y\} = 1$ by the recent result of Mihailescu ([Me], [Mih]); note that the case $a^x = 9$ is easily handled by elementary methods, e.g., Theorem 7 of [Sc-St].

Assume first $y = 1$. Suppose that (1) has three solutions for either $c = c_1$ or $c = c_2$, where $c_2 = a^x + b^{2y}$ as in the statement of the lemma. Let the third solution be (x_3, y_3). Write $T = \max\{x, x_3\}$ and let $t = \min\{x, x_3\}$. Then we have

$$b \mid a^T \pm a^t = a^t(a^{T-t} \pm 1).$$

Since $a^x - 1 = b$, we must have $x|T - t$ (note $a^x \neq 4$), so that x divides both T and t, so that $x|x_3$. In the same way we can show that when $x = 1$, $y|y_3$.

So we have $x \mid x_3$ and $y \mid y_3$. Since $c_1 = a^x + b^y$ and $c_2 = a^x + b^{2y}$, we cannot have $a^{x_3} + b^{y_3} = c$ where $c = c_1$ or c_2. Now let $A = a^x$, and let $B = b^y$. Then we must have two solutions (X, Y) to the equation

$$|A^X - B^Y| = c,$$

where $c = c_1$ or c_2. Now, since $A - B = 1$, we can apply Theorem 1.1 of [Be1] to see that $(B, c) = (2, 1)$, $(2, 5)$, $(2, 7)$, $(2, 13)$, $(2, 23)$, or $(3, 13)$. Since we are taking $A > 4$, this concludes the proof of the lemma.

Comment: For any $a > 1$, $b > 1$, $x > 0$, $y > 0$ such that $|a^x - b^y| = 1$, we have two values of c such that (a, b, c) gives two solutions to (1), so we have an infinite family of (a, b, c) giving two solutions. Lemma 6 shows that no member of this infinite family has three solutions unless the set $\{a, b\} = \{3, 2\}$ or $\{4, 3\}$.

Theorem 3 For integer $c > 0$ and relatively prime integers a and b with $1 < a, b < 24333$, (1) has at most two solutions (x, y) except when (a, b, c) is:
$(3, 2, 5)$ which gives four solutions,
$(3, 2, 1)$, $(3, 2, 7)$, $(3, 2, 11)$, $(3, 2, 13)$, $(4, 3, 13)$, or $(5, 2, 3)$ which each give three solutions. (For $a > b$; if $a < b$ then reverse the appropriate entries.)

Proof: We eliminate from consideration cases in which both a and b are primes or prime powers, since the theorem holds in such cases by Theorem 7 of [Sc-St].

Suppose for some relatively prime $a > 2$ and $b > 1$ both less than 24333, we have three solutions (x_1, y_1), (x_2, y_2), and (x_3, y_3). Recalling Lemma 2, we can take $x_1 < x_2 < x_3$. Let $Y = \max\{y_2, y_3\}$ and let $y = \min\{y_2, y_3\}$. Then combining the solutions (x_2, y_2) and (x_3, y_3) by eliminating c, and rearranging terms if $y_3 < y_2$, we obtain

$$\pm a^{x_3} \pm b^Y = \pm a^{x_2} \pm b^y = c_1 > 0, \tag{24}$$

where the signs are all independent. As in the proof of Theorem 2, we obtain $2a^{x_2} > c \geq c_1$, so that we can apply Lemma 5 to (24) to obtain a bound on x_2, and hence x_1, for any given $\{a, b\}$.

Let $t = \min\{y_1, y_2\}$ and let $T = \max\{y_1, y_2\}$. For any set of choices of x_1 and x_2, we can find all possible corresponding t since $b^t || a^{x_2 - x_1} \pm 1$. And, for any set of choices of x_1, x_2, and t, we can find all possible corresponding T since $b^T = \pm a^{x_1} \pm b^t + a^{x_2}$. Thus, for any choice of relatively prime a and b, we can use a computer program [St1] to find all possible (x_1, x_2, t, T). For convenience, we take $b > a > 2$ and handle $b = 2$ separately. The (a, b) for which this computer search finds some (x_1, x_2, t, T) must include all (a, b) for which (1) has three solutions. We use Lemmas 2 and 6 to eliminate members of infinite families from consideration. Recall we have eliminated from consideration pairs in which both a and b are primes or prime powers. We find that the only remaining pair (a, b) that gives two solutions which could potentially produce a third solution is $(91, 2)$.

When $a = 91$ and $b = 2$, we have $91 - 2 = 91^2 - 2^{13} = 89$ and $91^2 + 2 = 91 + 2^{13} = 8283$. If $c = 89$, we cannot have a third solution of the form $a^x - b^y = c$, by Theorem 1.1 of [Be]. Clearly also a third solution cannot be of the form $a^x + b^y = c$. A solution of the form $b^y - a^x = c$ is ruled out by consideration modulo 3. If $c = 8283$, again we can rule out a third solution of the form $a^x + b^y = c$. A solution of the form $a^x - b^y = c$ is ruled out by consideration modulo 7, and a solution of the form $b^y - a^x = c$ is ruled out by consideration modulo 8. This completes the proof.

In what follows, let $[a_1, a_2, \ldots, a_n]$ denote an *unordered* n-tuple of elements which may or may not be distinct.

For Theorem 4 which follows we will need:

Lemma 7 Suppose (1) has two solutions (x_1, y_1) and (x_2, y_2) such that either

$$[a^{x_1}, b^{y_1}, a^{x_2}, b^{y_2}] = [3^{D+1}, 3^D, 3^D, 3^D] \tag{25}$$

or

$$[a^{x_1}, b^{y_1}, a^{x_2}, b^{y_2}] = [2^{D+2}, 2^{D+1}, 2^D, 2^D], \tag{26}$$

where D is a positive integer. Then (1) has no third solution except when (a, b, c) is $(4, 2, 3 \cdot 4^k)$ or $(2, 4, 3 \cdot 4^k)$ where k runs through the positive integers; this exceptional case has exactly three solutions to (1).

Proof: When (25) holds, we must have

$$c = 2 \cdot 3^D = 3^{D+1} - 3^D = 3^D + 3^D \tag{27}$$

since no other choice of signs is possible in arranging the terms a^{x_1}, b^{y_1}, a^{x_2}, and b^{y_2}. We can let $a = 3^i$ and $b = 3^j$. Let m and n be positive integers with $m \geq n$. Then it is easily checked that there are no solutions (m, n) to the equation $2 \cdot 3^D = 3^m \pm 3^n$ except for $(m, n) = (D + 1, D)$ or (D, D). Thus if there is a third solution (x_3, y_3) to (1) when (25) holds, we must have

$$(ix_3, jy_3) = (jy_k, ix_k) = (R, S) \tag{28}$$

where $k = 1$ or 2 and $[R, S] = [D+1, D]$ or $[D, D]$.

When (26) holds, we must have

$$c = 2^{D+1} = 2^{D+2} - 2^{D+1} = 2^D + 2^D \tag{29}$$

or

$$c = 3 \cdot 2^D = 2^{D+2} - 2^D = 2^{D+1} + 2^D \tag{30}$$

since no other choice of signs is possible in arranging the terms a^{x_1}, b^{y_1}, a^{x_2}, and b^{y_2}. We can let $a = 2^i$ and $b = 2^j$.

Then it is easily checked that there are no solutions (m, n) to the equation $2^{D+1} = 2^m \pm 2^n$ except for $(m, n) = (D+2, D+1)$ or (D, D), and also there are no solutions to the equation $3 \cdot 2^D = 2^m \pm 2^n$ except for $(m, n) = (D+2, D)$ or $(D+1, D)$. Thus if there is a third solution (x_3, y_3) to (1) when (26) holds, we must have (28) with $[R, S] = [D+2, D+1]$, $[D, D]$, $[D+2, D]$, or $[D+1, D]$.

Since (x_3, y_3) and (x_k, y_k) are different solutions to (1), (28) implies $R \neq S$, $i \neq j$, $i \mid \gcd(R, S)$, and $j \mid \gcd(R, S)$, so that $\gcd(R, S) > 1$. Thus, considering all the $[R, S]$ possible from either (25) or (26), we see that we must have $[R, S] = [D+2, D]$ where D is even, so that $\max\{i, j\} = 2$ and

$$[a, b] = [4, 2], c = 3 \cdot 2^D \tag{31}$$

which is the exceptional case in the statement of the lemma. There is no fourth solution to (1) in this exceptional case since $\gcd(D+1, D) = 1$.

Comment: From (29) we see that $(a, b, c) = (4, 2, 2^{2k+1})$ gives exactly two solutions to (1). Also, infinite families of the type mentioned in the Comment following Lemma 2 can be derived from (27) and (30).

Theorem 4 Let a and b be positive integers with $\gcd(a, b) > 1$. Then (1) has at most two solutions unless $\{a, b\}$ is $\{4, 2\}$ and $c = 3 \cdot 4^k$ where k is a positive integer.

Proof: After Lemma 7, we can assume that (1) does not have two solutions (x_1, y_1) and (x_2, y_2) such that either (25) or (26) holds.

Let p be any prime dividing $\gcd(a, b)$, and let h, i, and j be positive integers such that $a = p^i a_0$, $b = p^j b_0$ and $c = p^h c_0$, where a_0, b_0, and c_0 are all relatively prime to p. Then any solution to (1) must fall into one of three types:

$$\text{Type X} : xi > yj = h,$$

$$\text{Type Y} : yj > xi = h,$$

$$\text{Type E} : xi = yj \leq h \text{ when } p > 2, \text{ or } xi = yj < h \text{ when } p = 2.$$

A Type X equation may be written, for some positive integer r,

$$\pm p^{h+r} {a_0}^{(h+r)/i} \pm p^h {b_0}^{h/j} = c. \tag{32}$$

A Type Y equation may be written, for some positive integer s,

$$\pm p^h {a_0}^{h/i} \pm p^{h+s} {b_0}^{(h+s)/j} = c. \tag{33}$$

A Type E equation may be written, for some positive integer $d \leq h$,

$$\pm p^d {a_0}^{d/i} \pm p^d {b_0}^{d/j} = c. \tag{34}$$

Suppose (1) has a solution of Type X and a solution of Type E. Then, combining (32) and (34), we see that

$$p^{h+r} {a_0}^{(h+r)/i} \leq p^h {b_0}^{h/j} + p^d {a_0}^{d/i} + p^d {b_0}^{d/j}. \tag{35}$$

Assume $a_0 \geq {b_0}^{i/j}$. Then ${a_0}^{(h+r)/i} \geq {b_0}^{h/j} \geq {b_0}^{d/j}$. Also, clearly, ${a_0}^{(h+r)/i} \geq {a_0}^{d/i}$. Thus,

$$p^h {b_0}^{h/j} + p^d {a_0}^{d/i} + p^d {b_0}^{d/j} \leq \left(\frac{1}{p^r} + \frac{1}{p^{h+r-d}} + \frac{1}{p^{h+r-d}} \right) p^{h+r} {a_0}^{(h+r)/i}. \tag{36}$$

Equality holds in (36) only when $a_0 = b_0 = 1$. When $p > 2$, (36) contradicts (35) unless $p = 3$, $r = 1$, $h = d$, and equality holds in both (35) and (36); but then $a_0 = b_0 = 1$ and (35) implies (25) which has been excluded. When $p = 2$, recalling the definition of Type E, we see that $h + r - d \geq 2$, so that (36) contradicts (35) here also unless $r = h - d = 1$ and equality holds in both (35) and (36); but then $a_0 = b_0 = 1$ and (35) implies (26) which was excluded. Thus, if (1) has a solution of Type X and a solution of Type E, we must have $a_0 < {b_0}^{i/j}$.

Similarly, if (1) has a solution of Type Y and a solution of Type E, the same argument (with the roles of a_0 and b_0 as well as i and j reversed) shows that $b_0 < {a_0}^{j/i}$. Thus, if (1) has three solutions, at least two of the solutions must be of the same type.

Now assume (1) has two solutions (x_1, y_1) and (x_2, y_2), both of Type E. Then, since $ix = jy$ for both solutions,

$$\frac{x_1}{y_1} = \frac{x_2}{y_2} = \frac{j}{i} \tag{37}$$

so that the two solutions cannot both be of the form $a^x - b^y = c$, by (3.1) of [Be]. Similarly, the two solutions cannot both be of the form $b^y - a^x = c$. Also, we cannot have one of the solutions of the form $a^x - b^y = c$ and the other of the form $b^y - a^x = c$, since the former requires $y/x < \log a / \log b$ and the latter requires $y/x > \log a / \log b$. Further, clearly we cannot have both solutions of the form $a^x + b^y = c$, since each of the exponents of one solution would be greater than the corresponding exponents of the other solution. Thus, if (1) has two solutions of Type E, we must have, for some positive integers d and f,

$$a^{d/i} + b^{d/j} = c \tag{38}$$

and

$$a^{f/i} - b^{f/j} = \pm c. \tag{39}$$

Note that $p^d || a^{d/i}$, $p^d || b^{d/j}$, $p^f || a^{f/i}$, and $p^f || b^{f/j}$. Now let $A = a^{(d,f)/i}$, let $B = b^{(d,f)/j}$, let $D = d/(d,f)$ and let $F = f/(d,f)$. Then (38) becomes

$$A^D + B^D = c \tag{40}$$

and (39) becomes

$$A^F - B^F = \pm c. \tag{41}$$

Taking $A > B$ and noting $A - B > 1$, and $F > D$, we see that $(A - B)(A^{F-1} + A^{F-2} * B + \cdots + B^{F-1}) > A^{F-1} + B^{F-1} \geq A^D + B^D$ (similarly when $B > A$). Thus, we cannot have two solutions to (1) both of Type E.

So now if (1) has three solutions, we can assume, without loss of generality, that it has two solutions of Type X. Call these solutions (x_1, y_1) and (x_2, y_2). From (32), we see that $y_1 = y_2$, so that $x_1 \neq x_2$. Take $x_1 < x_2$, and.let $r_1 = x_1 i - h$ and $r_2 = x_2 i - h$. Using (32) and combining the solutions (x_1, y_1) and (x_2, y_2) by eliminating c and rearranging terms, we obtain

$$2p^h {b_0}^{h/j} = p^{h+r_1} {a_0}^{(h+r_1)/i} \left(p^{r_2-r_1} {a_0}^{(r_2-r_1)/i} \pm 1\right). \tag{42}$$

If $p > 2$ then p^{h+1} divides the right side but not the left side of (42). So we must have $p = 2$ and $r_1 = 1$; indeed, our total argument thus far shows that $\gcd(a, b)$ must be a power of 2. Further, $a_0 = 1$, otherwise (42) requires that a and b have a common odd factor. Thus, a is a power of 2. Dividing both sides of (42) by 2^{h+1} we get

$${b_0}^{h/j} = {b_0}^{y_1} = 2^{r_2-1} \pm 1. \tag{43}$$

If $b_0 = 1$, then $r_2 = 2$ and $r_1 = 1$, so that (42) implies (26), which has been excluded. So we can take $b_0 > 1$. It is a familiar elementary result that (43) requires $y_1 = 1$ unless $b_0 = 3$, in which case $y_1 = 2$ is also possible.

Now suppose (1), in addition to having the two Type X solutions, has a third solution (x_3, y_3). Assume first $y_3 > y_1$. Then the solution (x_3, y_3) must be of Type Y, so that $a^{x_3} = 2^h$. Noting that $a^{x_1} = 2^{h+1}$, and combining the solutions (x_1, y_1) and (x_3, y_3), we obtain

$$b^{y_3} \pm b^{y_1} \leq 2^{h+1} + 2^h$$

from which we get

$$b^{y_1}(b-1) \leq 2^{h+1} + 2^h. \tag{44}$$

Dividing both sides of (44) by 2^h, we get

$${b_0}^{y_1}(b-1) \leq 3,$$

which is impossible for $b_0 > 1$.

Now suppose $y_3 = y_1$. Any solution of (1) must take one of three forms: $a^x - b^y = c$, $b^y - a^x = c$, or $a^x + b^y = c$. If $y_1 = y_2 = y_3$, we clearly cannot have any two of the three solutions of (1) of the same form. But $b^y - a^x = c$ requires $b^y > c$, while $a^x + b^y = c$ requires $b^y < c$.

So we must have $y_3 < y_1$, which requires $b_0 = 3$, $y_1 = 2$, $y_3 = 1$, $b = 2^{h/2}3$, $a^{x_3} = 2^{h/2}$, and $a^{x_1} = 2^{h+1}$, from which we get

$$2^h 3^2 \pm 2^{h/2} 3 = 2^{h+1} \pm 2^{h/2}, \tag{45}$$

which is impossible since (45) simplifies to $7 \cdot 2^{h/2} = 4$ or $7 \cdot 2^{h/2} = 2$. This completes the proof of Theorem 4.

§**3** In this section we first treat the following problem: for given odd prime a and $b = 2$, find all $c > 0$ such that (1) has two solutions. We bound the number of such c. Later we show that, under the additional restriction that a not be a Wieferich prime, there are no such c apart from certain exceptional cases.

Suppose we have

$$\pm a^{x_1} \pm b^{y_1} = \pm a^{x_2} \pm b^{y_2} = c > 0 \tag{46}$$

where the $\pm$ signs are all independent. Then we also have

$$\pm a^{x_1} \pm b^{y_2} = \pm a^{x_2} \pm b^{y_1} = c_1 > 0. \tag{47}$$

Since (47) is simply a rearrangement of (46), from here on we consider only the following revision of the above problem: for odd prime a and $b = 2$, find all $c > 0$ such that (1) has two solutions (x_1, y_1) and (x_2, y_2) with $x_1 \leq x_2$ and $y_1 \leq y_2$.

Theorem 5 Let x and y be positive integers, and $u, v \in \{0, 1\}$. When a is a prime greater than 5, there are at most two $c > 0$ such that

$$(-1)^u a^x + (-1)^v 2^y = c \tag{48}$$

has two solutions (x_1, y_1) and (x_2, y_2) with $x_1 \leq x_2$ and $y_1 \leq y_2$. (As in Section 2, we refer to a solution (x, y) rather than a solution (x, y, u, v).)

Theorem 5 is a consequence of Lemma 10 below along with the remark following the proof of the Corollary to Theorem 2 of [Sc-St].

Before proceeding we will need a few preliminaries. Suppose we have, for odd $a > 1$ with a not necessarily prime,

$$\pm a^{x_1} \pm 2^{y_1} = \pm a^{x_2} \pm 2^{y_2} = c > 0, 1 \leq x_1 \leq x_2, 1 \leq y_1 \leq y_2, \tag{49}$$

where the $\pm$ signs are independent and $(x_1, y_1) \neq (x_2, y_2)$. Clearly (49) can be rewritten as one of the following four types:

$$\text{Type 1 :} a^{x_1}(a^{x_2-x_1} - 1) = 2^{y_1}(2^{y_2-y_1} - 1) \tag{50}$$

$$\text{Type 2 :} a^{x_1}(a^{x_2-x_1} - 1) = 2^{y_1}(2^{y_2-y_1} + 1) \tag{51}$$

$$\text{Type 3 :} a^{x_1}(a^{x_2-x_1} + 1) = 2^{y_1}(2^{y_2-y_1} - 1) \tag{52}$$

$$\text{Type 4 :} a^{x_1}(a^{x_2-x_1} + 1) = 2^{y_1}(2^{y_2-y_1} + 1) \tag{53}$$

It is easy to see that all four types require $y_1 < y_2$.

In Lemmas 8 and 9 which follow, we consider (49) restricted to Types 2, 3, or 4; we will write (49a) to indicate this restriction. In these lemmas, a is not necessarily prime.

Lemma 8 In (51), $4 \not| \, x_2 - x_1$.

Proof: If $4 | x_2 - x_1$, then 5 divides the left side of (51). But also 3 divides the left side of (51). But 15 cannot divide the right side of (51).

Lemma 9 When $a > 3$ is odd and (49a) holds, we must have $x_1 = m$, where m is defined as in Lemma 1 for $b = 2$. When $a = 3$, $x_1 = 1$ or 2.

Proof: Suppose, for odd $a > 1670$, (49) holds with $x_1 > m$. We have

$$|a^{x_2} - 2^{y_2}| = \pm a^{x_1} \pm 2^{y_1} = c$$

where the $\pm$ signs are independent. Note that the sign in the absolute value on the left must be minus since $x_2 \geq x_1$ and $y_2 > y_1$. Note that it is a familiar elementary result that we can take $c > 1$, since here $a > 1670$ and $b = 2$. Let $\Lambda = |x_2 \log a - y_2 \log 2|$ and let $G = \max\{x_2/\log 2, y_2/\log a\}$. As in the proof of Theorem 2, we apply the theorem of Mignotte as given in Section 3 of [Be] using the parameters chosen by Bennett in Section 6 of [Be], and find that if (8) does not hold, we must have (11) with $b = 2$. Defining n as in Lemma

1, we have $na^w < y_2$, where $w = x_1 - m$. Taking $a > 1670$, we derive $n > 0.9999(\log a/\log 2)m$, from which we derive, as in the proof of Theorem 2,

$$G = 0.9999km\frac{a^w}{\log 2}$$

where $k \geq 1$. Note that here we do not have to consider the case $2|a$.

Suppose $c < 2a^{x_1}$. Then we can proceed as in the proof of Theorem 2 (here with $a \geq 1671$ rather than 24333) to obtain

$$0.9999\frac{a}{\log 2} < 2409.08,$$

from which it follows $a \leq 1670$, contradicting $a > 1670$.

To complete the proof of this lemma for the case $a > 1670$, it remains to show that $c < 2a^{x_1}$ when (49a) holds. By Lemma 8, $y_1 \leq s + 1$, where s is the greatest integer such that $2^s|a \pm 1$. Since $x_1 > m$, $a^{x_1} \geq a^2 > 2(a+1) \geq 2^{s+1} \geq 2^{y_1}$, so that $a^{x_1} > c/2$.

Now suppose $3 < a < 1670$ and (49a) holds with $x_1 > m$. We write (49a) in the form

$$a^{x_1}(a^{x_2-x_1} \pm 1) = 2^{y_1}(2^{y_2-y_1} \pm 1). \tag{54}$$

By Lemma 1, we must have $a|y_2 - y_1$. Also, since we have excluded Type 1 from consideration, at least one of the $\pm$ signs in (54) must be plus, so that there is an infinite set S of primes which cannot divide both sides of (54). Using these facts, we proceed with a computer search: for each $a < 1670$, we find a prime which must divide the right side of (54), and use this prime to obtain a congruence restriction on $x_2 - x_1$; we then find a prime that must divide the left side of (54), and use it to obtain a congruence restriction on $y_2 - y_1$; continuing back and forth this way, we obtain ever stronger congruence restrictions on $x_2 - x_1$ and $y_2 - y_1$, eventually showing that one side of (54) must be divisible by a prime in S, giving a contradiction. This is the method referred to as "bootstrapping" in [St] and is used by many authors to handle specific equations. This method cannot be relied on in general, but it does work for $a < 1670$, showing that there are no cases of (49a) with $x_1 > m$ when $3 < a < 1670$. When $a = 3$, the same method (but with $3^2|y_2 - y_1$) is used by Pillai [Pi, Lemmas 5, 6, 7] to show that $x_1 \leq 2$.

For the final results of this paper, we need to make a few observations. In all of these observations except Observation 8, a is not necessarily prime.

Observation 1: If $a > 3$, there is at most one c yielding a solution of a given type to (49a) when the parity of x_2 is pre-chosen.

Proof of Observation 1: Recalling Lemma 8, we see that, in (51), (52), and (53), the parity of $x_2 - x_1$ determines y_1. Since x_1 is pre-chosen by Lemma 9, c is determined.

Observation 2: When $a \equiv 7 \bmod 8$ we cannot have either (51) or (53).

Proof of Observation 2: If $a \equiv 7 \bmod 8$, then a is divisible by either a prime $p \equiv 7 \bmod 8$, or by both a prime $q \equiv 3 \bmod 8$ and a prime $r \equiv 5 \bmod 8$. If n is any positive integer, then $p \nmid 2^n + 1$ and $qr \nmid 2^n + 1$. Thus the observation holds.

Observation 3: In a Type 3 solution to (49), we cannot have $a \equiv 1 \bmod 8$. Also, we cannot have $2|x_2 - x_1$ unless $a = 2^n - 1$ for some integer n.

Proof of Observation 3: If, in (52), we have either $a \equiv 1 \bmod 8$ or 2 dividing both x_1 and x_2, we must have the left side of (52) congruent to 2 modulo 8, which requires $y_1 = 1$ and $y_2 = 2$, impossible for $a > 1$. And if 2 divides neither x_1 nor x_2, then any odd prime q dividing $a+1$ requires the left side of (52) to be congruent to -2 modulo q, and since we must have $y_1 = 1$, $q|2^{y_2}$, impossible.

Observation 4: In a Type 4 solution to (49), we must have $a \equiv 3 \bmod 8$ and $2 \not| \, x_2 - x_1$, except when $a = 2^n + 1$ for some integer n.

Proof of Observation 4: Assume $a \neq 2^n + 1$ for some integer n. Any odd prime q dividing $a - 1$ requires the left side of (53) to be congruent to 2 modulo q, so we cannot have $y_1 = 1$. Therefore, $2 \not| \, x_2 - x_1$ and $a \equiv 3 \bmod 4$, and by Observation 2, $a \equiv 3 \bmod 8$.

Observation 5: In a Type 2 solution to (49), we cannot have $3 < a \equiv 3 \bmod 8$ when m as in Lemma 9 is odd.

Proof of Observation 5: Suppose (51) has a solution with $3 < a \equiv 3 \bmod 8$ and m odd. Lemma 9 gives x_1 odd, consideration modulo 8 gives x_2 odd, and Lemma 8 gives $x_2 - x_1 \equiv 2 \bmod 4$ so that $y_1 = 3$. Thus, we can write (51) in the following form:

$$a^{x_1} \left(\frac{a^{(x_2-x_1)/2} + 1}{4} \right) \left(\frac{a^{(x_2-x_1)/2} - 1}{2} \right) = 2^{y_2-3} + 1 \tag{55}$$

Since $a > 3$, and $a \equiv 3 \bmod 8$ divides both sides of (55), we must have $y_2 > y_2 - 3 \geq 5$ so that (51) implies

$$a^{x_1}(\pm 8) \equiv 8 \bmod 32,$$

so that

$$a^{x_1}(\pm 1) \equiv 1 \bmod 4. \tag{56}$$

We must have the lower sign in (56), so $a^{x_2-x_1} - 1 \equiv -8 \bmod 32$. This requires $a^{(x_2-x_1)/2} \equiv -5$ or 11 modulo 32, so that

$$\frac{a^{(x_2-x_1)/2} - 1}{2} \equiv 5 \bmod 8.$$

But this requires that both sides of (55) be divisible by a prime congruent to 5 or 7 modulo 8, which is impossible: a prime 7 modulo 8 cannot divide the right side of (55), and, considering (55) modulo 3 gives $2 \not| \, y_2 - 3$, so that a prime 5 modulo 8 cannot divide the right side of (55).

Observation 6: If $a \equiv 2 \bmod 3$, then there is at most one c giving a Type 2 solution to (49) and at most one c giving a Type 4 solution to (49).

Proof of Observation 6: In (51) or (53), a determines the parity of $y_2 - y_1$, and when $a \equiv 2 \bmod 3$, $y_2 - y_1$ determines the parity of $x_2 - x_1$; since x_1 is determined by Lemma 9, Observation 1 applies to show that there is at most one c giving a Type 2 solution and at most one c giving a Type 4 solution.

Observation 7: If $a \equiv 1 \bmod 3$, then a Type 4 solution to (49) is impossible, a Type 3 solution requires $a \equiv 7 \bmod 8$, and a Type 2 solution requires $a \equiv 1 \bmod 8$ or $\equiv 3 \bmod 8$.

Proof of Observation 7: Suppose $a \equiv 1 \bmod 3$ and either (52) holds or (53) holds. We must have $2|y_2$. If (53) holds, we must have $2|y_1$ so that $a \equiv 3 \bmod 4$, impossible when $2|y_2$ and $2|y_1$. If (52) holds, we must have (again, using consideration modulo 3), $2 \not| y_1$, so that $\left(\frac{2}{p}\right) = 1$ for every prime $p \mid a$; but $a \equiv 1 \bmod 8$

is impossible by Observation 3, so that $a \equiv 7 \bmod 8$. If (51) holds with $a \equiv 1 \bmod 3$, then consideration modulo 3 shows $2 \not| y_2 - y_1$, so that no primes congruent to 5 modulo 8 can divide either side of (51); and clearly no primes congruent 7 modulo 8 can divide either side of (51).

Observation 8: If $M > 3$ is a Mersenne prime with $M = 2^u - 1$, then the only solutions to (49) with $a = M$ are

$$M + 2 = 2^{u+1} - M = c_1, \tag{57}$$

$$M + 2^u = 2^{2u} - M^2 = c_2. \tag{58}$$

If $F > 5$ is a Fermat prime with $F = 2^v + 1$, then the only solutions to (49) with $a = F$ are

$$F - 2 = 2^{v+1} - F = c_3, \tag{59}$$

$$F + 2^v = F^2 - 2^{2v} = c_4. \tag{60}$$

Proof of Observation 8: If $a = M$ or $a = F$, Type 1 solutions to (49) are impossible by the Corollary to Theorem 2 of [Sc-St]. By Observation 2, when $a = M$, only Type 3 solutions to (49) are possible. By Observation 1, c_1 and c_2 are the only possible values for c in (49). If $a = F$, Observations 3 and 6 show that c_3 and c_4 are the only possible values of c in (49). By Theorem 1, the observation holds.

Observation 9: If, in (49a), we have $a > 3$, $x_1 = 1$, and $x_2 > 2$, then we cannot have both $2|x_2$ and $2|y_2$.

Proof of Observation 9: Let t be the greatest number such that $2^t|a \pm 1$. Suppose (49a) holds with $a > 3$, $x_1 = 1$, $2|x_2 > 2$, and $2|y_2$. By Lemma 8, $2^{y_1} \leq 2^{t+1} \leq 2(a+1)$. We have $a^2 < a^{x_2/2} + 2^{y_2/2} \leq a + 2^{y_1} \leq 3a+2$, impossible.

Lemma 10 If $a > 5$ is relatively prime to 6, there are at most two values of c for which (49a) holds, provided that we take a prime when $a \equiv 11 \bmod 24$ and m is even, where m is defined as in Lemma 1 for $b = 2$.

Proof: Suppose for a given a, we can show that only one of (51), (52), and (53) holds. Then Observation 1 applies to show that Lemma 10 holds for such a, since in (49a), $x_1 = m$ is prechosen by Lemma 9. We can use this to show that Lemma 10 holds for $a \equiv 7 \bmod 8$ and $a \equiv 1 \bmod 3$: Observation 2 handles $a \equiv 7 \bmod 8$ and, once $a \equiv 7 \bmod 8$ is handled, Observation 7 suffices to handle $a \equiv 1 \bmod 3$.

So if Lemma 10 fails to hold, we must have $a \equiv 5$, 11, or 17 mod 24. Observation 6 applies to show that there is at most one c giving a Type 2 solution and at most one c giving a Type 4 solution. Observation 3 and Observation 1 show that there is at most one c giving a Type 3 solution (recall we have already handled $a \equiv 7 \bmod 8$). Now Observation 3 applies to show that Lemma 10 holds for $a \equiv 17 \bmod 24$, and Observation 4 applies to show that Lemma 10 holds for $a \equiv 5 \bmod 24$. And, if $2 \not| m$ where m is defined as in Lemma 1, Observation 5 applies to show that Lemma 10 holds for $a \equiv 11 \bmod 24$.

To complete the proof of this lemma, it suffices to show that we cannot have (51) with prime $a \equiv 11 \bmod 24$ and m even. Suppose (51) holds for such a and m. Then considering (51) modulo a and modulo 3, and recalling Lemma 8, we see we must have $2|x_2$, $2|y_2$, and $y_1 = 3$. Thus,

$$a^{x_2/2} + 2^{y_2/2} < a^{x_1} + 2^3.$$

Suppose $x_2 > 2x_1$. Then

$$a^2 - a \leq a^{x_2/2} - a^{x_1} < 2^3 - 2^{y_2/2} \leq 4,$$

which is impossible. So $x_2 \leq 2x_1$. Let v be the least number such that $a|2^v + 1$. Now $a^{x_1} = a^m||2^v + 1$. $2 \not| v|y_2 - y_1$. Also $v|a - 1$ and so v divides both sides of (51). Let q be the least prime dividing v, and let t be the least number such that $q|2^t + 1$. Then $2 \not| t|y_2 - y_1$. Since $q \mid v \mid a - 1$, $q \neq 3$ and $t \geq 5$. $(t, v) = 1$, so $tv|y_2 - y_1 \geq 5v$. Recalling $x_2 \leq 2x_1$, we see that (51) implies

$$2^{y_2 - y_1} < a^{x_2} \leq a^{2x_1} \leq (2^v + 1)^2 < 2^{5v},$$

which is a contradiction.

This completes the proof of Lemma 10.

We can now easily obtain the following

Proof of Theorem 5:

Suppose for some prime a there exists a positive integer c such that (49) has a Type 1 solution. From (4) of [Sc-St], we see that $2 \not| x_2 - x_1$ and $2 \not| y_2 - y_1$, and from (6a) of [Sc-St] we see that $y_1 \geq 2$. From this we easily derive $a \equiv 1 \bmod 8$, and if s is the least number such that $a|2^s - 1$, then s is odd. (51) and (53) are impossible for such a; and (52) is impossible by Observation 3. Thus, any further solutions to (49) for such a must be of Type 1. But this is impossible by the comment following the corollary of Theorem 2 of [Sc-St].

Thus, if Theorem 5 fails to hold, all the solutions of (48) must be of Type 2, Type 3, or Type 4. But this violates Lemma 10, completing the proof of Theorem 5.

Now recall that p is a Wieferich prime if $p^2 \mid 2^p - 2$. In the theorem that follows, it will be seen that excluding Wieferich primes allows us to obtain a result much stronger than that of Theorem 5, showing that when a is a prime which is not Mersenne, Fermat, or Wieferich, there are no values of c satisfying (49) except when $a = 11$ or possibly when $a \equiv 1 \bmod 16$, in which cases there is exactly one such c.

Theorem 6 If a is prime, then any solution to (49) must be one of the equations listed in (A) or (B) below, except possibly when a is a Wieferich prime greater than 1.25×10^{15}, or when (49) is of the form $p + 2^{t+1} = p^k - 2^y$ where $p \equiv 1 \bmod 16$ is a prime greater than 10^8, $2^t||p - 1$, $2 \mid y - t$, and $k \leq 1669$ is a

positive integer $\equiv 3 \bmod 4$.

$$
\begin{aligned}
(A): \quad & 3-2=3^2-2^3=1 \\
& 2^3-3=2^5-3^3=5 \\
& 2^4-3=2^8-3^5=13 \\
& 2^3-5=2^7-5^3=3 \\
& 3+2^3=3^3-2^4=11 \\
& 3^2+2=3^3-2^4=11 \\
& 3+2=2^5-3^3=5 \\
& 3^2+2^2=2^8-3^5=13 \\
& 5+2=2^5-5^2=7 \\
& 2^2-3=3^2-2^3=1 \\
& 3^2-2^2=2^5-3^3=5 \\
& 5-2=2^7-5^3=3 \\
& 11-2^2=2^7-11^2=7 \\
(B): \quad & M+2=2^{u+1}-M \\
& M+2^u=2^{2u}-M^2 \\
& F-2=2^{v+1}-F \\
& F+2^v=F^2-2^{2v}
\end{aligned}
$$

where $M=2^u-1$ is a Mersenne prime greater than or equal to 3, and $F=2^v+1$ equals 9 or is a Fermat prime greater than or equal to 3.

Proof: It has been shown that $1093 \equiv 5 \bmod 8$ and $3511 \equiv 7 \bmod 8$ are the only Wieferich primes less than 1.25×10^{15} [Mc]. The Corollary to Theorem 2 of [Sc-St] shows that neither of these primes gives a Type 1 solution to (49). Since both these primes are congruent to 1 modulo 3, Observation 7 applies to show that any solution to (49) in which $a=1093$ or 3511 must be a Type 3 solution with $a=3511$. Observation 3 shows that $2 \not| x_2-x_1$, so that consideration modulo 16 gives $y_1=3$. But then $2^{y_2}=a^{x_2}+a^{x_1}+2^{y_1} \equiv 1+1+3 \equiv 0 \bmod 5$, impossible. So we can assume in what follows that a is not a Wieferich prime.

By the Corollary to Theorem 2 of [Sc-St], all Type I solutions in which a is not a Wieferich prime are listed in (A), and so we can eliminate Type 1 solutions to (49) from consideration.

For $a=3$, all Type 2, Type 3, and Type 4 solutions have been given by Pillai [Pi]. The elementary methods of [Pi] also suffice to give all the Type 2, Type 3, and Type 4 solutions when $a=5$. A considerably faster way to find all these solutions when $a=3$ or 5 is the application of Lemmas 8 and 9 to determine the possible x_1 and y_1 for each Type, followed by the application of the Corollary to Theorem 2 of [Sc-St] to determine all possible x_2 and y_2; the cases in which no (x_2, y_2) exists are easily handled by consideration modulo 8 or modulo 15. With either method, we find that the only instances of (49) with $a=3$ or 5 are either among the specific equations listed in (A), or among equations in (B) for which $M=3$ or $F=3$, 5, or 9. It follows from Observation 8 that the remaining Mersenne and Fermat primes have only the solutions listed in (B).

So we can assume from here on that a is not a Mersenne or Fermat prime, and hence also that $x_1=1$ (recall Lemma 9) and $x_2>1$ (recall (6)).

Now suppose $x_2 = 2$. We can write (49) as

$$a^2 \pm a - 2^{y_2} \pm 2^{y_1} = 0, \tag{61}$$

where the $\pm$ signs are independent. Thus,

$$a = \frac{\mp 1 + \sqrt{2^{y_2+2} \mp 2^{y_1+2} + 1}}{2}.$$

All solutions (g, h, z) to the equation $2^g \pm 2^h + 1 = z^2$ have been found by Szalay [Sz] using a bound of Beukers [Bk]. A simpler shorter proof using a more recent bound of Bauer and Bennett [B-B] is found in [Sc1]. It follows from Szalay's result that, when $x_2 = 2$, the only possible prime value of $a > 5$ which is not Mersenne or Fermat is

$$a = 11 = \frac{-1 + \sqrt{2^9 + 2^4 + 1}}{2}$$

which corresponds to the final entry of (A).

So from here on we can assume the following: $x_1 = 1$, $x_2 > 2$, (49) is not one of the cases in (A) or (B), and a is not a Fermat or Mersenne prime.

Consider a Type 4 solution to (49). By Observation 4, we have x_2 even and $y_1 = 2$. Let $D = a - 4$. We have

$$\left(a^{x_2/2}\right)^2 + D = 2^{y_2}. \tag{62}$$

It follows from Corollary 1.7 of [B-B] that

$$y_2 < 3.8462 \frac{\log D}{\log 2},$$

so that

$$2^{y_2} < D^{3.8462}. \tag{63}$$

So now we have

$$(a-4)^{3.8462} = D^{3.8462} > 2^{y_2} > a^{x_2} \geq a^4,$$

which is impossible. Thus this theorem holds for the Type 4 case.

Now consider a Type 3 solution to (49). By Observation 3, we have $2 \nmid x_2 - x_1$ so that $2|x_2$. Suppose that $a \equiv 3 \bmod 8$ and recall $a = 3$ has already been excluded. Then $y_1 = 2$ and consideration modulo a shows that $2|y_2$; so we can apply Observation 9 to eliminate $a \equiv 3 \bmod 8$ from consideration. If $a \equiv 1 \bmod 3$, we must have $2|y_2$ and again we can use Observation 9, eliminating $a \equiv 1 \bmod 3$ from consideration. So we must have $a \equiv 5 \bmod 12$ or $a \equiv 23 \bmod 24$. Consider $a \equiv 5 \bmod 12$. Since we have shown a is not a Fermat prime, we can take $a \geq 29$. And, in (62) and (63), we can take $D = a + 2$. Thus we have

$$\left(\frac{31a}{29}\right)^{3.8462} \geq (a+2)^{3.8462} = D^{3.8462} > 2^{y_2} > a^{x_2} \geq a^4,$$

which is impossible. Now consider the case $a \equiv 23 \bmod 24$. In (62) and (63), we can take $D = a + 2^{y_1} < 2a$, noting a is not a Mersenne prime. Assume first $x_2 \geq 6$. Now we have

$$(2a)^{3.8462} > D^{3.8462} > 2^{y_2} > a^{x_2} \geq a^6,$$

which is again impossible. Now assume $x_2 = 4$. We could handle the case $x_2 = 4$ as above to obtain a bound on a, but this would require computer calculations to handle cases below that bound. Instead, we use an elementary argument. We have

$$2^{y_1}\left(2^{y_2-y_1}-1\right) = a\left(a^3+1\right). \tag{64}$$

Since 9 divides the right side of (64), we must have $6|y_2 - y_1$. Let v be the least number such that $a|2^v - 1$. $v|y_2 - y_1$ and $v|a-1$ so that $3 \not| v$. Since $a \equiv 7 \bmod 8$, $2 \not| v$. Putting this all together, we see that $6v|y_2 - y_1$, so that

$$2^{6v} \le 2^{y_2-y_1} < 2^{y_2} = a^4 + D < a^4 + 2a < 2^{4v} + 2^{v+1},$$

which is impossible. So our theorem holds for the Type 3 case.

Consider a Type 2 solution to (49). By Observations 2 and 5, we must have $a \equiv 1 \bmod 4$. If $3 \not| 2^{y_1} + 2^{y_2}$, then $a \equiv 2 \bmod 3$ and $2 \mid x_2$, so that the left side of (51) is congruent to 2 modulo 3, so that we must have $2|y_2$, and Observation 9 applies to give a contradiction; so $3 \mid 2^{y_1} + 2^{y_2}$. So we have

$$2 \not| y_2 - y_1 \text{ and } a \equiv 1 \bmod 4. \tag{65}$$

Let s be the least number such that $a \mid 2^s + 1$. By (51) and (65), $2 \not| s \ge 11$.

Assume first that $2 \mid x_2$ so that, by (51), $2^{y_1}||a-1$. Let d be the greatest odd divisor of $a-1$. $s \mid d$, so that in (63) we can take $D = a + 2^{y_1} < a + \frac{a}{11}$. (Note that Corollary 1.7 of [B-B] is proven for D any nonzero integer.) If $x_2 \ge 4$ we have

$$\left(\frac{12a}{11}\right)^{3.8462} > D^{3.8462} > 2^{y_2} \ge a^4 - D > a^4 - \frac{12a}{11}, \tag{66}$$

which is impossible since $a > 7$. Thus, we cannot have $2 \mid x_2$.

This leaves the following equation as the only possible instance of (49), where (49) is not one of the equations listed in (A) or (B), and a is not a Wieferich prime greater than 1.25×10^{15}:

$$a + 2^{y_1} = a^{x_2} - 2^{y_2} = c > 0, \tag{67}$$

where x_2 is odd. By Lemma 8, $x_2 \equiv 3 \bmod 4$ and 2^{y_1-1} is the greatest power of 2 dividing $a-1$. By (65), $y_1 - 1$ and y_2 are the same parity. x_1 and y_1 are determined, so that c is determined and we can use Theorem 2 of [Sc] to check by computer all values of a less than 10^8. By (65), $a \equiv 1 \bmod 8$. If $a \equiv 9 \bmod 16$ then, since $a + 1 \equiv 10 \bmod 16$ divides the left side of (51), we must have a prime 5 or 7 modulo 8 dividing both sides of (51), impossible when $2 \not| y_2 - y_1$. So $a \equiv 1 \bmod 16$. It remains to show that $x_2 = k \le 1669$. Let $\Lambda = |x_2 \log a - y_2 \log 2|$. As in the proof of Lemma 9, we again derive (11) with $b = 2$. Here $G = x_2/\log 2$ and $c = a + 2^{y_1} < \frac{5}{3}a$. Thus $x_2/\log 2 < 2409.08$ giving $k \le 1669$.

This completes the proof of Theorem 6.

The methods of Lemma 9 and Theorem 6 can be used also to handle certain cases of (1) when $b > 2$. In particular, for Theorem 7 below, we will need results on the following equation:

$$a^{x_1} + a^{x_2} = 3^{y_1} + 3^{y_2}, \tag{68}$$

where $a > 3$ is a prime, $1 \le x_1 \le x_2$, $1 \le y_1 \le y_2$, and $(x_1, y_1) \ne (x_2, y_2)$.

Lemma 11 When (68) holds, we must have $x_1 = m$, where m is defined as in Lemma 1 for $b = 3$.

Proof: Note (68) requires $x_1 < x_2$ and $y_1 < y_2$. Suppose, for prime $a \geq 2647$, (68) holds with $x_1 > m$. Let $c = |a^{x_2} - 3^{y_2}|$. Let $\Lambda = |x_2 \log a - y_2 \log 3|$ and let $G = \max\{x_2/\log 3, y_2/\log a\}$. As in the proofs of Theorem 2 and Lemma 9, we apply the theorem of Mignotte as given in Section 3 of [Be] using the parameters chosen by Bennett in Section 6 in [Be], and find that if $G \geq 2409.08$ then (11) holds with $b = 3$. Defining n as in Lemma 1, we have $n > \frac{m \log a}{\log 3}$. From this we get, as in the proofs of Theorem 2 and Lemma 9,

$$G = km\frac{a^w}{\log 3}$$

where $w = x_1 - m$ and $k \geq 1$.

Suppose first that $a^{x_1} > 3^{y_1}$. Then $c < a^{x_1}$ and we can proceed as in the proofs of Theorem 2 and Lemma 9 to obtain

$$\frac{a}{\log 3} < 2409.08, \tag{69}$$

from which it follows that $a < 2647$.

Now suppose $a^{x_1} < 3^{y_1}$. Let m_1 be the greatest number such that $3^{m_1}|a+1$ and let $w_1 = y_1 - m_1$. $3^{w_1}|x_2 - x_1$, by Lemma 1. Now $c < 3^{y_1} = 3^{m_1+w_1} \leq \frac{a+1}{2}(x_2 - x_1) < ax_2$ and $G = x_2/\log 3$, so that (11) becomes

$$G < 2\left(\frac{1}{\log 3} + \frac{\log G + \log\log 3}{\log a \log 3}\right) + 22.997\left(\log G + 2.405\right)^2,$$

from which we again obtain (69), so that again we have $a < 2647$.

So it remains to check for possible solutions of (68) with $x_1 > m$, a prime, and $3 < a < 2647$. A computer search similar to that used in Lemma 9 yields no such solutions. This completes the proof of Lemma 11.

We now define a base-3 Wieferich prime to be a prime p such that $p^2|3^p - 3$. Peter Montgomery [Mon] has shown has shown that 11 and 1006003 are the only base-3 Wieferich primes under 2^{32}.

Lemma 12 If a is not a base-3 Wieferich prime greater than 2^{32}, then the only solution (a, x_1, y_1, x_2, y_2) to (68) is $(a, x_1, y_1, x_2, y_2) = (5, 1, 1, 2, 3)$.

Proof: If $a \equiv 3 \bmod 4$, then, since $a|3^{y_2-y_1} + 1$, we must have $\left(\frac{3}{a}\right) = -1$. But similarly we must have $\left(\frac{a}{3}\right) = -1$, impossible. In particular, we cannot have $a = 11$ or 1006003, so we can exclude base-3 Wieferich primes from consideration.

After Lemma 11 we can assume $x_1 = 1$. Consideration modulo 3 shows $a \equiv 2 \bmod 3$ and $2 \mid x_2$.

Let m_1 be the highest number such that $3^{m_1}|a + 1$. Let $w_1 = y_1 - m_1$. Since $3^{y_1}||a^{x_2-x_1} + 1$,

$$3^{w_1}||x_2 - x_1. \tag{70}$$

Suppose $a \equiv 1 \bmod 8$. Then consideration modulo 8 shows $2|y_1$ and $2|y_2$, so that, since we must have $2|x_2$,

$$2a^{x_2/2} < |a^{x_2/2} - 3^{y_2/2}|\left(a^{x_2/2} + 3^{y_2/2}\right) < \max\{a^{x_1}, 3^{y_1}\} < \max\{a, 3^{m_1}x_2\} < ax_2,$$

which is impossible for $a \geq 5$ and $x_2 \geq 2$.

So we must have $a \equiv 5 \bmod 8$, so consideration modulo 8 gives $2 \not| \, y_1$ and $2 \not| \, y_2$. Now $(a+1)/2 \equiv 3 \bmod 4$ so that m_1 must be odd, since otherwise there exists a prime $q > 3$ with $q \equiv 3 \bmod 4$ dividing both sides of (68), impossible since $y_2 - y_1$ is even. Since y_1 is odd, we have $2|w_1$ so that, in particular,

$$w_1 \neq 1, x_2 \neq 4. \tag{71}$$

We write (68) in the following form:

$$\left(a^{x_2/2}\right)^2 + (a^{x_1} - 3^{y_1}) = 3^{y_2}. \tag{72}$$

Let $D = |a^{x_1} - 3^{y_1}|$. We apply Corollary 1.7 of [B-B] to obtain

$$y_2 < 5.715 \frac{\log D}{\log 3}$$

so that we have

$$3^{y_2} < D^{5.715}. \tag{73}$$

Suppose first $3^{y_1} > a^{x_1} = a$. If $a = 5$, $3^{y_1} \geq 9$, so that $3|x_2 - x_1$, so that 7 divides both sides of (68), which is impossible since $2|y_2 - y_1$. So, since we have $a \equiv 2 \bmod 3$ and $a \equiv 5 \bmod 8$, we can take $a \geq 29$, $3^{y_1} \geq 81$. Then

$$\begin{aligned} a^{x_2} &= 3^{y_2} + 3^{y_1} - a = 3^{y_2} + D < D^{5.715} + D < 3^{5.715 y_1} + 3^{y_1} \\ &= 3^{5.715 y_1}\left(1 + 3^{-4.715 y_1}\right) < \left(3^{w_1} a\right)^{5.715}\left(1 + 3^{-4.715 y_1}\right) \\ &< \gamma \left(3^{w_1} a\right)^{5.715} = a^{(\log \gamma / \log a) + (\log 3 / \log a) 5.715 w_1 + 5.715}, \end{aligned}$$

where $\gamma < 1 + 10^{-8}$. Using (70), we obtain

$$3^{w_1} + 1 \leq x_2 < (\log 3 / \log a) 5.715 w_1 + 5.715 + (\log \gamma / \log a) < 2 w_1 + 5.72,$$

which is impossible for $w_1 \geq 2$. Using (71), we get $w_1 = 0$, contradicting $3^{y_1} > a$.

So $a > 3^{y_1}$ and $D < a$. Suppose $x_2 > 2$. Then by (71), $x_2 \geq 6$ and we have

$$a^6 \leq a^{x_2} = 3^{y_2} - D < D^{5.715} - D < a^{5.715} - a,$$

impossible.

So if (68) has a solution, we must have $x_1 = 1$ and $x_2 = 2$. We can write (68) in the form

$$a^2 + a - 3^{y_2} - 3^{y_1} = 0,$$

which we view as a quadratic equation in a to obtain

$$a = \frac{-1 + \sqrt{4\left(3^{y_2}\right) + 4\left(3^{y_1}\right) + 1}}{2}. \tag{74}$$

It follows from the results of Tzanakis and Wolfskill [T-W] and Le [Le] that the only solutions (z, y_1, y_2) to the equation $z^2 = 4\left(3^{y_2}\right) + 4\left(3^{y_1}\right) + 1$ are given by $(z, y_1, y_2) = (5, 1, 1)$, $(11, 1, 3)$, and $(2 \cdot 3^k + 1, k, 2k)$,

which give $a = 2$, $a = 5$, and $a = 3^k$. $a = 2$ and $a = 3^k$ are not under consideration here, and $a = 5$ gives the single solution specified in the statement of this lemma. This completes the proof.

For convenience in stating Theorem 7 below, we call a Wieferich prime greater than $1.25 \cdot 10^{15}$ a *large base-2 Wieferich prime*, and we call a base-3 Wieferich prime greater than 2^{32} a *large base-3 Wieferich prime.*

Combining Theorem 6 and Lemma 12, and using also Theorem 1 of [Sc-St] and Corollary 1.7 of [Be], we immediately obtain

Theorem 7 Let a be prime, $a > b$, $b = 2$ or $b = 3$, a not a large base-b Wieferich prime, $1 \le x_1 \le x_2$, $1 \le y_1 \le y_2$, and $(x_1, y_1) \ne (x_2, y_2)$. If there is a solution (a, x_1, y_1, x_2, y_2) to the equation

$$|a^{x_1} - b^{y_1}| = |a^{x_2} - b^{y_2}|, \tag{75}$$

then (75) must be one of the following equations:

$$\begin{aligned}
3 - 2 &= 3^2 - 2^3 \\
2^3 - 3 &= 2^5 - 3^3 \\
2^4 - 3 &= 2^8 - 3^5 \\
2^3 - 5 &= 2^7 - 5^3 \\
13 - 3 &= 13^3 - 3^7 \\
2^2 - 3 &= 3^2 - 2^3 \\
3^2 - 2^2 &= 2^5 - 3^3 \\
5 - 2 &= 2^7 - 5^3 \\
11 - 2^2 &= 2^7 - 11^2 \\
5 - 3 &= 3^3 - 5^2 \\
F - 2 &= 2^{v+1} - F
\end{aligned}$$

where $F = 2^v + 1$ is a Fermat prime greater than or equal to 3, or $F = 9$.

References:

[A] L. J. Alex, Diophantine equations related to finite groups, *Comm. Algebra*, **4**, no. 1 (1976), 77–100.

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

[Be] M. Bennett, On some exponential equations of S. S. Pillai, *Canadian Journal of Mathematics*, **53**, no. 5, (2001), 897–922.

[Be1] M. Bennett, Pillai's conjecture revisited, *J. of Number Theory*, **98** (2003), 228-235.

[Bk] F. Beukers, The generalized Ramanujan-Nagell equation 1, *Acta Arith.*, **38**, 1981, 389–410.

[B-F] J. L. Brenner and L. L. Foster, Exponential Diophantine Equations, *Pacific J. of Math.*, **101**, no. 2 (1982), 263–301.

[Cao] Z. F. Cao, On the Equation $x^2 + 2^m = y^n$ and Hugh Edgar's Problem. *Kexue Tongbau* [in Chinese], **31**, (7) (1986), pp. 555-556.

[Cas] J. W. S. Cassels, On the equation $a^x - b^y = 1$, *American Journal of Mathematics*, **75**, (1953), 159–162.

[Ha] T. Hadano, On the Diophantine equation $a^x + b^y = c^z$, *Math. J. Okayama Univ.*, **19**, no. 1 (1976/77), 25–29.

[Le] M. H. Le, The Diophantine equation $x^2 = 4q^n + 4q^m + 1$, Proc. Amer. Math. Soc., **106**, 3, 1989, 599–604.

[Le1] M. H. Le, On the Diophantine equation $a^x + b^y = c^z$, *J. Changchun Teachers College Ser. Nat. Sci.* **2** (1985), 50–62 (in Chinese).

[Le2] M. H. Le, A conjecture concerning the exponential Diophantine equation $a^x + b^y = c^z$, *Acta Arithmetica* **106.4** (2003), 345–353.

[Lev] W. J. Leveque, On the equation $a^x - b^y = 1$, *American Journal of Mathematics*, **74**, (1952), 325–331.

[Mc] Richard McIntosh, letter dated 15 Dec 2003 posted on the web at
http://www.loria.fr/∼zimmerma/records/Wieferich.status,
also see http://torch.cs.dal.ca/∼knauer/Wieferich

[Me] T. Metsänkylä, Catalan's Conjecture: Another old Diophantine problem solved, *Bull. Amer. Mat. Soc.* **41**, no. 1 (2003), 43–112.

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

[Mih] P. Mihailescu, A class number free criterion for Catalan's conjecture. *J. Number Theory* **99**, no. 2, (2003), 225–231.

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

[Mon] P. Montgomery, New solutions of $a^{p-1} \equiv 1 \bmod p^2$, *Math. Comp.*, **61**, no. 203 (1993), 361–363.

[N] T. Nagell, Sur une classe d'equations exponentielles, *Ark. Mat.*, **3**, (1958), 569–582.

[Pi] S. S. Pillai, On the equation $2^x - 3^y = 2^X + 3^Y$, *Bull. Calcutta Soc.*, **37**, (1945), 15-20.

[Sc] R. Scott, On the Equations $p^x - b^y = c$ and $a^x + b^y = c^z$, *Journal of Number Theory*, **44**, no. 2 (1993), 153-165.

[Sc1] R Scott, Elementary solution of $p^a \pm p^b + 1 = x^2$, preprint.

[Sc-St] R Scott and R. Styer, On $p^x - q^y = c$ and related three term exponential Diophantine equations with prime bases, *Journal of Number Theory*, **105** no. 2 (2004), 212–234.

[St-T] R. J. Stroeker and R. Tijdeman, Diophantine Equations, pp. 321-369, *Computational Methods in Number Theory*, MC Track 155, Central Math Comp Sci, Amsterdam, 1982.

[St] R. Styer, Small two variable exponential Diophantine equations, *Math. Comp.*, **60**, no. 202 (1993), 811-816.

[St1] R. Styer, http://www.homepage.villanova.edu/robert.styer/ReeseScott/index.htm, contains links to programs and data files.

[Sz] L. Szalay, The equation $2^N \pm 2^M \pm 2^L = z^2$, Indag. Math., N.S., **13**, no. 1, 2002, 131–142.

[T-W] N. Tzanakis, J. Wolfskill, The Diophantine equation $x^2 = 4q^{a/2} + 4q + 1$ with an application to coding theory, *J. of Number Theory*, **26**, (1987), 96–116.

[U] S. Uchiyama, On the Diophantine equation $2^x = 3^y + 13^z$, *Math. J. Okayama Univ.*, **19**, no. 1 (1976/77), 31–38.

[W] B. M. M. de Weger, Solving exponential Diophantine equations using lattice basis reduction algorithms, *J. Number Theory*, **26**, no. 3 (1987), 325–367.