

Sketch for Theorem 6 with a composite

revised 22 Dec 2007

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

Section 1

In this section we seek specific results on the generalized Pillai equation

$$|a^x \pm b^y| = c \quad (1)$$

with a and b either prime or composite. In some of the results obtained we bound b .

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

$$\pm a^{x_1} \pm b^{y_1} = \pm a^{x_2} \pm b^{y_2} = c > 0, 1 \leq x_1 \leq x_2, 1 \leq y_1 \leq y_2, \quad (2)$$

where the \pm signs are independent and $(x_1, y_1) \neq (x_2, y_2)$. Clearly (2) can be rewritten as one of the following four types:

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

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

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

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

Lemma 1 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

$$a^x | b^y \pm 1, \quad (3)$$

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 (3) 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 2 If $a > 2$ and $(a, b) \neq (3, 2)$, then, in the notation of Lemma 1,

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

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 2 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 3 Let $a > 2$, $b > 1$, and $c > 0$ be relatively prime integers. If (2) has a solution and if further $a^{x_1} > c/2$, then

$$x_1 < S + k,$$

where S is defined as in Lemma 1, and $k = \frac{\log 3294.5 + \log \log a}{\log a}$ when $a < 5346$ and $k = 1.19407$ 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]; the lemma holds in all these cases, so we assume from here on that $(a, b) \neq (3, 2)$.

If $y_1 = y_2$, then, using (6) of [Sc-St2] with the roles of a and b reversed, we see that $x_1 = 1$; so we can take $y_1 < y_2$. Following closely the method of proof in Bennett's Proposition 4.4 [Be], assume there are two solutions to (1) with $a^{x_1} > c/2$, $y_2 > y_1$, 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. 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

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

and so Lemma 1 implies that $y_2 - y_1 \geq a^{x_1-S}$. Thus,

$$y_2 > a^{k_1}.$$

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 2 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

$$\frac{G}{5.2595} \geq \frac{y_2}{5.2595 \log a} > \frac{2 \log c}{\log a \log b} \quad (4).$$

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], we see that we must have either

$$G < 3294.5 \quad (5)$$

or

$$\log \Lambda > -24.2 (\log G + 2.4)^2 \log a \log b. \quad (6)$$

First assume $c > 1$. Assume (6) holds. Then, in the same way we derived (11) of [Sc-St2] (here $c_1 = c$), we obtain

$$G < 2 \frac{\log c}{\log a \log b} + 24.2 (\log G + 2.4)^2. \quad (7)$$

Using (4) we obtain

$$G < 29.882 (\log G + 2.4)^2,$$

which implies $G < 3294.5$. So, no matter which of (5) or (6) holds, we have

$$3294.5 > G \geq \frac{y_2}{\log a} > \frac{a^{k_1}}{\log a},$$

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 (7) by

$$G < \frac{\log 2}{\log a \log b} + 24.2 (\log G + 2.4)^2. \quad (8)$$

From (8) we again derive

$$\frac{a^{k_1}}{\log a} < 3294.5,$$

impossible since $k_1 \geq k$.

NOTE: INSERT LEMMA 4

The following generalizes Observation 8 of [Sc-St2] to include composite values of a .

Lemma 5 : If $M > 3$ is a Mersenne number with $M = 2^u - 1$, then the only solutions to (2) with $a = M$ are

$$M + 2 = 2^{u+1} - M = c_1, \quad (6a)$$

$$M + 2^u = 2^{2u} - M^2 = c_2. \quad (6b)$$

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

$$F - 2 = 2^{v+1} - F = c_3, \quad (6c)$$

$$F + 2^v = F^2 - 2^{2v} = c_4. \quad (6d)$$

Proof of Lemma 5: In what follows we refer to a solution to (2) with $b = 2$. It is easy to see that, for $b = 2$, (2a), (2b), (2c), and (2d) require $y_1 < y_2$.

By Lemma 4, $x_1 = 1$.

If (2a) has a solution with $a = 2^n \pm 1$ with x_2 odd, then we must have $y_1 > n$; but, by Theorem 4 of [Sc-St], $2^{y_1} < a^{x_1} = a$, contradiction. If (2a) has a solution with $a = 2^n + 1$ and x_2 even, we have $y_1 = n$, so that $c = 1$ in (2), which is impossible for $a > 3$. If (2a) has a solution with $a = 2^n - 1$ and x_2 even, we have $y_1 = 1$, $a^{x_2} - a^{x_1} \equiv 6 \pmod{8}$, $2 \mid x_1 = 1$, contradiction. Thus, there are no Type I solutions to (2) when $a = 2^n \pm 1$.

By Observation 2 of [Sc-St2], (2b) has no solutions with $a = 2^n - 1$. If (2b) has a solution with $a = 2^n + 1$ and x_2 odd, then $(a + 1)/2 = 2^{n-1} + 1$ divides both sides of (2b), so that $y_2 - y_1$ must be an odd multiple of $n - 1$; but a also divides both sides of (2b), so that $y_2 - y_1$ must be an odd multiple of n , contradiction. If (2b) has a solution with $a = 2^n + 1$ and x_2 even, then $y_1 = n$, so that $c = c_4$; by Theorem 1 of [Sc-St2], the only possible case is given by (6d).

By Observation 3 of [Sc-St2], (2c) has no solutions with $a = 2^n + 1$. If (2c) has a solution with $a = 2^n - 1$ then we must have either $y_1 = 1$ or $y_1 = n$ according as x_2 is either odd or even, so that $c = c_1$ or c_2 ; but by Theorem 1 of [Sc-St2] the only possible cases are given by (6a) and (6b).

By Observation 2 of [Sc-St2], (2d) has no solutions with $a = 2^n - 1$. Any solutions with $a^n + 1$ must have $y_1 = 1$, so that $c = c_3$; by Theorem 1 of [Sc-St2], the only case is given by (6c). This completes the proof of Lemma 5.

Section 2

In this section we treat the equation

$$\pm a^x \pm b^y = \pm a^w \pm b^z \tag{1}$$

for relatively prime positive integers $a > b > 1$ such that the largest prime divisor of a is not a base- b Wieferich prime. We are concerned only with solutions (x, y, w, z) such that the pair (x, y) is distinct from the pair (w, z) . In what follows, we will always be dealing with (1) under these restrictions.

Theorem 1 If the greatest of the four terms in (1) is a power of 2, then (1) must be one of the equations in (A) or (B) below.

$$\begin{aligned} (A) : 2^3 - 3 &= 2^5 - 3^3 \\ 2^4 - 3 &= 2^8 - 3^5 \\ 2^3 - 5 &= 2^7 - 5^3 \\ 3 + 2 &= 2^5 - 3^3 \\ 3^2 + 2^2 &= 2^8 - 3^5 \\ 5 + 2 &= 2^5 - 5^2 \\ 3^2 - 2^2 &= 2^5 - 3^3 \\ 5 - 2 &= 2^7 - 5^3 \\ 11 - 2^2 &= 2^7 - 11^2 \end{aligned}$$

$$\begin{aligned}
(B) : M + 2 &= 2^{u+1} - M \\
M + 2^u &= 2^{2u} - M^2 \\
F - 2 &= 2^{v+1} - F
\end{aligned}$$

where $M = 2^u - 1$ and $F = 2^v + 1$.

Proof: Letting $x_1 = \min\{x, w\}$, $y_1 = \min\{y, z\}$, $x_2 = \max\{x, w\}$, $y_2 = \max\{y, z\}$, and $b = 2$, we rewrite (1) as

$$2^{y_2} - a^{x_2} = (-1)^g 2^{y_1} + (-1)^h a^{x_1} \quad (2)$$

where g and h are in the set $\{0, 1\}$. We cannot have $g = h = 1$. If $g = 0$ and $h = 1$, then, by Theorem 4 of [Sc], (1) must be one of the first three equations listed in (A) above. So we can assume $h = 0$ and write (2) as

$$2^{y_1} (2^{y_2 - y_1} - (-1)^g) = a^{x_1} (a^{x_2 - x_1} + 1). \quad (3)$$

Let m be defined as in Lemma 1 of [Sc-St2] for $b = 2$. By Lemma 9 of [Sc-St2], we must have $x_1 = m$. Let v be the least number such that $a | 2^v - (-1)^g$. Let the prime factorization of a be $a = \prod_i p_i^{\alpha_i} \prod_j q_j^{\beta_j}$, where for each i , $p_i^{\alpha_i} | 2^v - (-1)^g$, and for each j , $q_j^{\beta_j + 1} | 2^v - (-1)^g$. From (3) we see that we must have

$$v \prod_i p_i^{(m-1)\alpha_i} | y_2 - y_1 \quad (4)$$

and, for any q_j which is not a Wieferich prime,

$$q_j^{\beta_j} | v \quad (5)$$

and

$$q_j^{\beta_j} | r - 1 \quad (6)$$

where r is some prime divisor of a .

Now assume $m > 1$. Then, noting that $a \neq 2^n + 1$ for any integer n , we see that

$$2^v > a. \quad (7)$$

From (6) we see that, since $m > 1$, the largest prime divisor of a must be greater than or equal to 7. Also, by the restriction on a in (1), the largest prime divisor of a must be among the p_i . Combining this with (4) and (7), we obtain

$$k \frac{\log a}{\log 2} 7^{m-1} = y_2 \quad (8)$$

where $k \geq 1$.

Now let $\Lambda = y_2 \log 2 - x_2 \log a$, let $G = y_2 / \log a$, and let $c = a^{x_1} + (-1)^g 2^{y_1} = a^m + (-1)^g 2^{y_1}$. We see from (3) and from the fact that $a \neq 2^n \pm 1$ for any n that $1 < c < 2a^m$. Using a theorem of Mignotte [Mi] with parameters chosen by Bennett [Be, Section 6], we see that we must have either

$$G < 2409.08 \quad (9)$$

or

$$\log \Lambda > -22.997(\log G + 2.405)^2 \log a \log 2. \quad (10)$$

In exactly the same manner as in the proof of Theorem 2 in [Sc-St2], we obtain

$$G < 2 \frac{\log c}{\log a \log 2} + 22.997(\log G + 2.405)^2. \quad (11)$$

(Note that (11) corresponds to (11) in [Sc-St2].) Using (8), along with $G = y_2 / \log(a)$ and $c < 2a^m$, we find that we can view (11) as an inequality in the variables k and m . If (11) holds for $m \geq 6$ and $k \geq 1$ then it must hold for $m = 6$ and $k = 1$. But then both (11) and (9) require $7^5 < 2409.08 \log 2$, false. So we can assume $m < 6$ in which case both (11) and (9) require $G < 2409.08$, so that

$$x_2 / \log 2 < y_2 / \log a < 2409.08. \quad (12)$$

Let p be the largest prime dividing a , recalling that p must be among the p_i . Combining (4), (12), and (7), we obtain

$$p < 1670. \quad (13)$$

Assume that none of the primes q_j is a Wieferich prime. Then combining (4) and (5), we see that $y_2 > a$, so that (12) gives $a < 24333$. If $p > 547$, then we can use (4) and (12) to obtain

$$v < \frac{1670 \log a}{p \log 2} < 44. \quad (14)$$

There are only nine primes p in the range $547 < p < 1669$ which allow $v \leq 43$, and these can easily be shown to make (2) impossible since each requires the left side of (3) to be divisible by primes which cannot divide the right side of (3). Now we can use a computer search to show there are no cases of (2) with $m > 1$ and with none of the q_j Wieferich: we use $a < 24333$, $p < 547$, and $vp|y_2 - y_1$, and use the method called “bootstrapping” in [Sc-St, page 217] to find primes which must divide the left side of (3) but cannot all divide the right side of (3).

Now suppose at least one of the q_j is Wieferich. By (13), the only such Wieferich prime possible is 1093, and $1093|a$. Combining (4) and (5), we see that $y_2 > a/1093$ so that

$$\frac{a}{1093} \log 2 < 670 \log a$$

from which we obtain $a < 46491492$. Since $p \geq 1097$, we can use (4) and (12) to obtain $v < 39$, impossible when $1093|a$.

Thus we have $x_1 = m = 1$, and we can use the methods of the proof of Theorem 6 of [Sc-St2] to complete the proof.

Comment: The theorem we have just proven generalizes Theorem 6 of [Sc-St2] for the Type 3 and Type 4 cases. The Type 2 case can be handled just as easily the same way, requiring additional calculations which we have not yet done but which are just as practical as those in the above proof. The Type 1 case can also be handled in the same way, although here we must use $x_2 \leq 1669$ to arrive at a contradiction by the “bootstrapping” methods; as with the Type 2 case in Theorem 6 of [Sc-St2], the Type 1 case with a composite leaves open the possibility of cases with x_2 odd, which can be dealt with in a manner similar to the Type 2 case in Theorem 6 of [Sc-St2].

If we do not require the calculations to be practical, we can obtain the following, letting $x_1 = \min\{x, w\}$:

Theorem 2

Let B and W be fixed positive real numbers. Then, if (1) holds with $b < B$ and the highest prime dividing a is not a base- b Wieferich prime greater than W , we must have $x_1 = m = 1$, except for a finite number of effectively computable cases.

Sketch of Proof: Theorem 2 can be easily proven by essentially the same methods as the more specific Theorem 1 above, noting the following:

For any odd a we consider 2 a base- a Wieferich prime.

We divide the expression on the left of (4) by 2 whenever $a \equiv 2 \pmod{4}$.

In (8), we replace 7 by 3.

When $c > 2a^m$, we obtain a bound on c in (11) by using Lemmas 2 and 3 to get $c < b^{y_1}$ where $y_1 < \frac{b \log(a)}{2 \log(b)} + k$, with k defined as in Lemma 3 above.

With these changes, the proof of Theorem 2 essentially follows that of Theorem 1.

[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.

[Sc-St2] R. Scott and R. Styer, On the generalized Pillai equation $\pm a^x \pm b^y = c$, *Journal of Number Theory*, **118** (2006), pp. 236–265.