Publ. Math. Debrecen
88/1-2 (2016), 131–138
DOI: 10.5486/PMD.2016.7282

Number of solutions to $a^x + b^y = c^z$

By REESE SCOTT (Somerville) and ROBERT STYER (Villanova)

Abstract. For relatively prime integers a and b both greater than one and odd integer c, there are at most two solutions in positive integers (x, y, z) to the equation $a^x + b^y = c^z$. There are an infinite number of (a, b, c) giving exactly two solutions.

1. Introduction

This paper deals with the problem of finding an upper bound on the number of solutions in positive integers x, y, and z to the equation

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

for integers a, b, and c, all greater than 1 with $\gcd(a, b) = 1$. Although there is much previous work on this problem, realistically low bounds on the number of solutions to (1.1) have been obtained only for the special case in which one of x, y, or z is constant; results for this special case are obtained using lower bounds on linear forms in logarithms (e.g., [6], [1]). For the more general case in which all of x, y, and z are variable, MAHLER [8] used his p-adic analogue of the method of Thue–Siegel to prove that (1.1) has only finitely many solutions (x, y, z) (see [7]). LATER, GELFOND [3] made Mahler's result effective. As pointed out by the anonymous referee of this paper, the existence of a bound on the number of solutions, independent of a, b, and c, follows from a result of BEUKERS and SCHLICKEWEI [2]. HIRATA-KOHNO [4] used [2] to obtain a bound of 2^{36} (the referee believes Hirata-Kohno may have later announced a bound of 200, apparently unpublished).

Mathematics Subject Classification: 11D61.
Key words and phrases: exponential Diophantine equation.

Le [7] dealt with the general case when all of x, y, and z are variable with c odd:

Theorem A ([7]). *If $2 \nmid c$ then (1.1) has at most $2^{\omega(c)+1}$ solutions (x, y, z) where $\omega(c)$ is the number of distinct prime factors of c. Moreover, all solutions (x, y, z) of (1.1) satisfy $z < (2ab \log(2eab))/\pi$.*

We give a brief outline of a proof of Theorem A, which differs somewhat from Le's proof, but will allow us to establish some notation for our own variant of Theorem A. We distinguish four parity classes for x and y:

Class 1: $2 \mid x$ and $2 \mid y$. Class 2: $2 \nmid x$ and $2 \mid y$. Class 3: $2 \mid x$ and $2 \nmid y$. Class 4: $2 \nmid x$ and $2 \nmid y$.

For each parity class we define D to be the least integer such that $\frac{a^x b^y}{D}$ is a square for any choice of x and y in the parity class. If (x, y, z) is a solution to (1.1) with x and y in a given parity class, we say that the solution (x, y, z) is in that parity class. We then define the integer $\gamma(x, y, z)$ in $\mathbb{Q}(\sqrt{-D})$:

$$\gamma(x, y, z) = a^x - b^y + 2\sqrt{-a^x b^y}. \tag{1.2}$$

The norm of $\gamma(x, y, z)$ is c^{2z}. Let $C_D = \{\mathfrak{c}_1\overline{\mathfrak{c}_1}, \mathfrak{c}_2\overline{\mathfrak{c}_2}, \ldots, \mathfrak{c}_g\overline{\mathfrak{c}_g}\}$ be the set of all factorizations of $[c]$ into two ideals in $\mathbb{Q}(\sqrt{-D})$ such that, for $1 \le i \le g$, no $\mathfrak{c}_i$ is divisible by a principal ideal with a rational integer generator. $g = 2^{\omega(c)-1}$. For any (x, y, z), $[\gamma(x, y, z)]$ must be divisible by exactly one of the ideals $\mathfrak{c}_1$, $\overline{\mathfrak{c}_1}$, $\mathfrak{c}_2$, $\overline{\mathfrak{c}_2}$, $\ldots$, $\mathfrak{c}_g$, $\overline{\mathfrak{c}_g}$. We say that the solution (x, y, z) to (1.1) is *associated* with the ideal factorization $\mathfrak{c}_k\overline{\mathfrak{c}_k}$ when either $\mathfrak{c}_k$ or $\overline{\mathfrak{c}_k}$ divides $[\gamma(x, y, z)]$, where $\mathfrak{c}_k\overline{\mathfrak{c}_k} \in C_D$. It is an old result (see Lemma 2 of Section 2) that there is at most one solution (x, y, z) associated with a given ideal factorization in C_D (with one easily handled exception). Since $g = 2^{\omega(c)-1}$ and there are four parity classes as defined above, we obtain the result in the first sentence of Theorem A. The result in the second sentence of Theorem A follows from a result in Hua [5].

In this paper we will show that, for a given (a, b, c), any solution (x, y, z) must occur in one of at most two parity classes of x and y. We then show that any solution in a given parity class must be associated with one of at most two ideal factorizations in C_D, regardless of the number of distinct primes dividing c. We also show that if solutions occur in two parity classes, then any solution in a given parity class must be associated with the same ideal factorization in C_D as any other solution in the same parity class. With these results we obtain:

Theorem 1. *For relatively prime integers a and b both greater than one and odd integer c, there are at most two solutions in positive integers (x, y, z) to (1.1); any solution (x, y, z) must satisfy $z < ab/2$.*

There are an infinite number of such (a, b, c) giving exactly two solutions.

(The bound on z follows from Theorem 3 of [10]. The infinite family $(a, b, c : x_1, y_1, z_1; x_2, y_2, z_2) = (2, 2^m - 1, 2^m + 1 : 1, 1, 1; m + 2, 2, 2)$ suffices to verify that there are an infinite number of (a, b, c) giving exactly two solutions.)

The result that there are at most two solutions to (1.1) in the special case in which either x or y is a fixed constant (usually 1) has been obtained by BENNETT [1] using lower bounds on linear forms in logarithms when $\gcd(a, b) = 1$ and using elementary methods when $\gcd(a, b) > 1$. Theorem 1 above provides an elementary proof of Bennett's result for the case c odd.

2. Proof of Theorem 1

Throughout this proof we assume that c is an odd integer and that a and b are relatively prime integers greater than 1. We also assume throughout this proof that (1.1) has solutions (x_1, y_1, z_1), (x_2, y_2, z_2), ..., (x_n, y_n, z_n) such that there is no integer greater than 1 dividing all of x_1, x_2, ..., x_n, and no integer greater than 1 dividing all of y_1, y_2, ..., y_n, where $n > 1$. Note that this assumption (which may involve redefining a and b) does not affect the number of solutions (x, y, z), or the value of D corresponding to a given solution, or the value of any $\gamma(x, y, z)$. We will prove Theorem 1 by using four lemmas, for the first of which we need two definitions: let $u(m)$ be the least integer t such that $m^t \equiv 1 \bmod c$; let $v_2(m)$ be the integer w such that $2^w \| m$.

Lemma 1. *For a given (a, b, c), all solutions (x, y, z) to (1.1) occur in at most two parity classes of x and y. If (1.1) has solutions in two different parity classes, we must have one of the following: Class 1 with Class 4; Class 2 with Class 3; Class 4 with Class 3 (in which case $u(a)$ is odd); or Class 4 with Class 2 (in which case $u(b)$ is odd).*

PROOF. If (1.1) has solutions in more than one parity class, we can, switching the roles of a and b if necessary, let (x_1, y_1, z_1) be any solution with x_1 odd and let (x_2, y_2, z_2) be any solution with x_2 even. Assume first $v_2(u(a^{x_1})) > 1$. Then we must have, noting $a^x \equiv -b^y \bmod c$ for every solution (x, y, z),

$$v_2(u(a^{x_1})) = v_2(u(b^{y_1})), v_2(u(a^{x_2})) < v_2(u(a^{x_1})), v_2(u(b^{y_2})) < v_2(u(b^{y_1})).$$

Note that, for any solution (x, y, z) to (1.1), we cannot have $v_2(u(b^y)) > v_2(u(b^{y_1}))$ so y_1 must be odd (otherwise $2 \mid y_i$ for every i, $1 \le i \le n$). So we see that $2 \mid x - y$ for any solution. Thus when $v_2(u(a^{x_1})) > 1$, only Class 1 and Class 4 are possible.

Now assume $v_2(u(a^{x_1})) = 1$ with $(a^{x_1})^{u(a^{x_1})/2} \not\equiv -1 \bmod c$. Then $v_2(u(b^{y_1})) = 1$ with $(b^{y_1})^{u(b^{y_1})/2} \not\equiv -1 \bmod c$. Note that, for any solution (x, y, z) to (1.1), $v_2(u(b^y)) > 1$ is impossible, so that y_1 must be odd. Then, since $u(b^y) = \frac{u(b)}{\gcd(u(b),y)}$ for any y, we have

$$b^{u(b)/2} \equiv b^{\frac{y_1}{\gcd(u(b),y_1)}\frac{u(b)}{2}} = (b^{y_1})^{u(b^{y_1})/2} \not\equiv -1 \bmod c.$$

$v_2(u(a^{x_2})) = 0$ so that $v_2(u(b^{y_2})) = 1$ with $(b^{y_2})^{u(b^{y_2})/2} \equiv -1 \bmod c$, so y_2 is odd and

$$b^{u(b)/2} \equiv (b^{y_2})^{u(b^{y_2})/2} \equiv -1 \bmod c,$$

a contradiction. So the case $v_2(u(a^{x_1})) = 1$ with $(a^{x_1})^{u(a^{x_1})/2} \not\equiv -1 \bmod c$ is impossible.

Now assume $v_2(u(a^{x_1}))=1$ with $(a^{x_1})^{u(a^{x_1})/2} \equiv -1 \bmod c$. Then $v_2(u(b^{y_1}))=0$ and we have

$$v_2(u(a^{x_2})) = 0, v_2(u(b^{y_2})) = 1.$$

Note that, for any solution (x, y, z) to (1.1), $v_2(u(b^y)) > 1$ is impossible, so y_2 must be odd. We see that $2 \nmid x - y$ for any solution. So when $v_2(u(a^{x_1})) = 1$ with $(a^{x_1})^{u(a^{x_1})/2} \equiv -1 \bmod c$, only Class 2 and Class 3 are possible.

If $v_2(u(a^{x_1})) = 0$, then $v_2((u(b^{y_1})) = 1$ and

$$v_2(u(a^{x_2})) = 0, v_2(u(b^{y_2})) = 1.$$

Note that, for any solution (x, y, z) to (1.1), $v_2(u(b^y)) > 1$ is impossible, so both y_1 and y_2 must be odd. So when $v_2(u(a^{x_1})) = 0$, only Class 4 and Class 3 are possible.

If we were to reverse the roles of a and b in the above proof, taking y_1 odd and y_2 even, then, considering each of the possible values of $v_2(u(b^{y_1}))$ and proceeding as in the preceding paragraphs, we would obtain the same results, except that when $v_2(u(b^{y_1})) = 0$ we must have Class 4 with Class 2. □

Lemma 2. *In a given parity class of x and y, there is at most one solution (x, y, z) to (1.1) associated with a given ideal factorization in C_D, except when $(a, b, c) = (3, 10, 13)$ or $(10, 3, 13)$.*

Proof. See [9, proof of Theorem 1 and the first paragraph of the proof of Theorem 2], noting that the only relevant instance of exception (iii) in Theorem 1 of [9] is given by $(a, b, c) = (3, 10, 13)$. □

Lemma 3. *If* (1.1) *has solutions in more than one parity class, then we must have one of the following:*
$a^{u(a)/2} \equiv b^{u(b)/2} \equiv -1 \mod c$,
$u(a)$ *is odd and* $b^{u(b)/2} \equiv -1 \bmod c$, *or*
$a^{u(a)/2} \equiv -1 \bmod c$ *and* $u(b)$ *is odd.*

PROOF. Assume (1.1) has two solutions (x_1, y_1, z_1) and (x_2, y_2, z_2) such that $2 \nmid x_1$ and $2 \mid x_2$. We have $a^{x_1} \equiv -b^{y_1} \bmod c$ and $a^{x_2} \equiv -b^{y_2} \bmod c$ so that $a^{|x_1 - x_2|} \equiv b^t \bmod c$ for some t such that $0 \le t < u(b)$. Let $L = \operatorname{lcm}(x_1, x_1 - x_2)$ so that L is odd. Then we have

$$a^L \equiv (-b^{y_1})^{L/x_1} \equiv (b^t)^{L/|x_1 - x_2|} \bmod c,$$

so that the congruence $b^q \equiv -1 \bmod c$ has a solution q. This requires $b^{u(b)/2} \equiv -1 \bmod c$.

Similarly, if (1.1) has two solutions (x_1, y_1, z_1) and (x_2, y_2, z_2) such that $2 \nmid y_1 - y_2$, we must have $a^{u(a)/2} \equiv -1 \bmod c$. Now Lemma 3 follows from Lemma 1. □

For the proof of Lemma 4 which follows, we use the following definition: we say that $h_1 + k_1\sqrt{-D} \equiv h_2 + k_2\sqrt{-D} \bmod c$ if $h_1 \equiv h_2 \bmod c$ and $k_1 \equiv k_2 \bmod c$.

Lemma 4. *All solutions to* (1.1) *in a given parity class are associated with one of at most two ideal factorizations in the set* C_D. *If* (1.1) *has solutions in more than one parity class, then any two solutions in the same parity class must be associated with the same ideal factorization in the set* C_D.

PROOF. Let (x_1, y_1, z_1) and (x_2, y_2, z_2) be two solutions in the same parity class, with x_1 the least x occuring in any solution in the parity class and (x_2, y_2, z_2) any other solution in the parity class. We have

$$\gamma(x_1, y_1, z_1) = a^{x_1} - b^{y_1} + 2\sqrt{-a^{x_1} b^{y_1}} \tag{2.1}$$

and

$$\gamma(x_2, y_2, z_2) \equiv a^{x_2} - b^{y_2} + 2a^{(x_2 - x_1)/2} b^d \sqrt{-a^{x_1} b^{y_1}} \bmod c \tag{2.2}$$

where $d = hu(b) + (y_2 - y_1)/2$, where h is any integer such that $d \ge 0$ (we can take h to be the least such integer greater than or equal to zero so that $h = 0$ when $y_2 \ge y_1$). We have

$$a^{x_1} a^{x_2 - x_1} = a^{x_2} \equiv -b^{y_2} \equiv -b^{y_1} b^{2d} \bmod c. \tag{2.3}$$

Since $a^{x_1} \equiv -b^{y_1} \bmod c$, (2.3) gives

$$a^{x_2 - x_1} \equiv b^{2d} \bmod c. \tag{2.4}$$

Since a is prime to c, there exists an integer δ such that $0 \leq \delta < c$ and

$$a^{(x_2-x_1)/2}\delta \equiv b^d \bmod c. \tag{2.5}$$

(2.5) with (2.4) gives

$$\delta^2 \equiv 1 \bmod c. \tag{2.6}$$

Now consider all the solutions (x_i, y_i, z_i) to (1.1), regardless of parity class. $a^{x_i} \equiv -b^{y_i} \bmod c$ for every i, and there is no integer greater than 1 dividing all the x_i. So we can construct a linear combination of all the x_i to obtain

$$a \equiv \pm b^t \bmod c \tag{2.7}$$

where t is an integer such that $0 \leq t < u(b)$. So (2.5) becomes

$$\pm(b^t)^{(x_2-x_1)/2}\delta \equiv b^d \bmod c$$

so that $\delta \equiv \pm b^r \bmod c$ for some $0 \leq r < u(b)$. By (2.6), $b^{2r} \equiv 1 \bmod c$. This requires either $r = 0$ or $r = u(b)/2$. Recalling (2.4) we see that (2.2) becomes

$$\gamma(x_2, y_2, z_2) \equiv b^{2d}(a^{x_1} - b^{y_1}) \pm 2b^{2d}b^r\sqrt{-a^{x_1}b^{y_1}} \bmod c. \tag{2.8}$$

Write $\gamma_1 = \gamma(x_1, y_1, z_1)$ and write $\gamma_2 = \gamma(x_2, y_2, z_2)$, unless the $\pm$ in (2.8) is minus, in which case γ_2 is the conjugate of $\gamma(x_2, y_2, z_2)$. Let $\beta = a^{x_1} - b^{y_1} + 2b^r\sqrt{-a^{x_1}b^{y_1}}$. Since $\gcd(b, c) = 1$, (2.8) gives $c \mid \beta\overline{\beta}$. Let $\mathfrak{c}_k$ be the unique ideal such that $\mathfrak{c}_k\overline{\mathfrak{c}_k} \in C_D$ and $\mathfrak{c}_k \mid [\beta]$. $\mathfrak{c}_k$ contains both β and c, so by (2.8) it contains γ_2, so that $\mathfrak{c}_k \mid [\gamma_2]$, so that the solution (x_2, y_2, z_2) is associated with the ideal factorization $\mathfrak{c}_k\overline{\mathfrak{c}_k}$. Since either $r = 0$ or $r = u(b)/2$ ($r = u(b)/2$ is possible only when $2 \mid u(b)$), there are at most two possible values for β one of which must be γ_1, so there are at most two possible choices for $\mathfrak{c}_k$ one of which must be $\mathfrak{c}_h$ where $\mathfrak{c}_h \mid [\gamma_1]$. If $u(b)$ is odd, then $r = 0$ and $\beta = \gamma_1$, so $\mathfrak{c}_k = \mathfrak{c}_h$. If $2 \mid u(b)$ and $b^{u(b)/2} \equiv -1 \bmod c$, then either $\beta = \gamma_1$ (when $r = 0$) or $\beta = \overline{\gamma_1}$ (when $r = u(b)/2$), so that $\mathfrak{c}_k = \mathfrak{c}_h$ or $\mathfrak{c}_k = \overline{\mathfrak{c}_h}$. Now Lemma 4 follows from Lemma 3. □

Recalling the parenthetical comments immediately following the statement of Theorem 1, and noting that, when $(a, b, c) = (3, 10, 13)$, (1.1) has exactly two solutions (see, e.g., [9], last paragraph of the proof of Theorem 6), we see that Theorem 1 follows from Lemmas 1, 2, and 4.

3. Cases with exactly two solutions

We give the following conjecture, which allows c even as well as c odd:

Conjecture. *For integers a, b, and c all greater than one with $\gcd(a, b) = 1$, there is at most one solution in positive integers (x, y, z) to (1.1) except for the following (a, b, c) or (b, a, c):* $(5, 2, 3)$, $(7, 2, 3)$, $(3, 2, 11)$, $(3, 2, 35)$, $(3, 2, 259)$, $(3, 4, 259)$, $(3, 16, 259)$, $(5, 2, 133)$, $(3, 10, 13)$, $(89, 2, 91)$, $(91, 2, 8283)$, $(3, 5, 2)$, $(3, 13, 2)$, $(3, 13, 4)$, $(3, 13, 16)$, $(3, 13, 2200)$, *and* $(2^n - 1, 2, 2^n + 1)$ *for any positive integer $n \geq 2$.*

All (a, b, c) in the above list give exactly two solutions in positive integers x, y, and z except for $(a, b, c) = (3, 5, 2)$, which has three solutions. A computer search found no other (a, b, c) with $\gcd(a, b) = 1$ giving more than one solution in positive integers x, y, z to (1.1) in the ranges $a < 2500$, $b < 10000$ with $a^x < 10^{30}$, $b^y < 10^{30}$.

Except for $(5, 2, 3)$, $(7, 2, 3)$, and $(2^n - 1, 2, 2^n + 1)$, all the (a, b, c) in the list given in Conjecture 1 can be derived from the first six entries of Conjecture 1.2 of [1] which deals with the case in which one of x or y is constant.

References

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

[2] F. Beukers and H. P. Schlickewei, The equation $x + y = 1$ in finitely generated groups, *Acta Arith.* **78** (1996), 189–199.

[3] A. O. Gel'fond, Sur la divisibilité de la différence des puissances de deux nombres entires par une puissance d'un idéal premier, *Math. Sb.* (1940), 7–25.

[4] N. Hirata-Kohno, S-unit equations and integer solutions to exponential Diophantine equations, Analytic Number Theory and surrounding Areas 2006, *Kyoto RIMS Kokyuroku*, 2006, 92–97.

[5] L. K. Hua, Introduction to Number Theory, *Springer-Verlag, Berlin*, 1982.

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

[7] M. Le, An upper bound for the number of solutions of the exponential Diophantine equation $a^x + b^y = c^z$, *Proc. Japan Acad.* **75 Ser. A** (1999), 90–91.

[8] K. Mahler, Zur Approximation algebraischer Zahlen I: Über den grössten Primtailer binärer Formen., *Math. Ann.* **107** (1933), 691–730.

[9] R. Scott, On the equations $p^x - q^y = c$ and $a^x + b^y = c^z$, *J. Number Theory* **44** (1993), 153–165.

[10] R. Scott and R. Styer, On $p^x - q^y = c$ and related three term exponential Diophantine equations with prime bases, *J. Number Theory* **105** (2004), 212–234.

REESE SCOTT
86 BOSTON ST.
SOMERVILLE, MA 02143
USA

ROBERT STYER
DEPARTMENT OF MATHEMATICS
AND STATISTICS
VILLANOVA UNIVERSITY
800 LANCASTER AVENUE
VILLANOVA, PA 19085–1699
USA

E-mail: robert.styer@villanova.edu

(Received February 5, 2015; revised September 1, 2015)