Reprinted from JOURNAL OF NUMBER THEORY
All Rights Reserved by Academic Press, New York and London

Vol. 44, No. 2, June 1993
Printed in Belgium

On the Equations $p^x - b^y = c$ and $a^x + b^y = c^z$

REESE SCOTT

93 Russell Avenue, Watertown, Massachusetts 02172

Communicated by M. Pohst

Received November 26, 1990; revised October 2, 1991

This paper is a response to a problem in [R. K. Guy, "Unsolved Problems in Number Theory," Springer-Verlag, New York, 1981] (see Introduction). The main results are the following: The equation $p^x - b^y = c$, where p is prime, and $b > 1$ and c are positive integers, has at most one solution (x, y) when y is odd, except for five specific cases, and at most one solution when y is even. The equation $p^n - q^m = p^N - q^M$, where p and q are primes, has no solutions (n, m, N, M) unless $(p/q) = (q/p) = 1$, except for four specific cases. The equation $|p^x - q^y| = c$ has at most two solutions except for three specific cases. The equation $a^x + b^y = p^z$, where $a > 1$, $b > 1$, $(a, b) = 1$, and p is prime, has at most two solutions when p is odd and at most one solution when $p = 2$ except for two specific cases. © 1993 Academic Press, Inc.

INTRODUCTION

In section D9, p. 87, of [5], Richard Guy writes:

"Hugh Edgar asks how many solutions (m, n) does $p^m - q^n = 2^h$ have, for primes p, q and integer h. At most one? Only finitely many?"

The question is a specific case of the following problem:

How many solutions (m, n) does

$$|p^m - q^n| = c \tag{1}$$

have, for primes p, q and integer c? (We take $m, n > 0$.)

The finiteness of the number of solutions to Eq. (1) for a given choice of (p, q, c) follows from a result of Pillai [9].

There are three choices of (p, q, c) (taking $p > q$) which each yield exactly three solutions to Eq. (1): $(3, 2, 1)$, $(5, 2, 3)$, $(3, 2, 5)$. Theorem 5 of this paper shows that all other choices of (p, q, c) yield at most two solutions. In particular, the choice $p = F$, $q = 2$, $c = F - 2$ yields exactly two solutions when F is a Fermat prime 17 or greater.

Cris Crawford has confirmed by computer that, aside from trivial

0022-314X/93 $5.00

rearrangements, the only (p, q, c) yielding two or more solutions to Eq. (1) with p^m and $q^n < 2^{32}$ 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), (17, 2, 15), (257, 2, 255), (65537, 2, 65535). We conjecture that these eleven (p, q, c) are the only (p, q, c) giving more than one solution to Eq. (1), not counting the four trivial rearrangements (3, 2, 23), (5, 2, 123), (5, 3, 22), and (11, 2, 117). Note that in none of these cases is $c = 2^h$, $h > 1$.

Pillai's result [9] shows that the equation

$$a^x - b^y = c, \tag{2}$$

where $a > 1$, $b > 1$, and $c > 0$ are any integers, has only finitely many solutions (x, y). When c is sufficiently great with respect to a and b, he showed [10] there is at most one solution. LeVeque [8] and Cassels [1] showed that, for $c = 1$, there is at most one solution to Eq. (2), except when $a = 3$ and $b = 2$. For any c, if a is prime, Eq. (2) has at most one solution with y even and at most one solution with y odd, except for five specific choices of (a, b, c) each yielding exactly two solutions (see Theorem 3 of this paper).

Pillai [9] also gave the more general result that

$$ra^x - sb^y = c \tag{3}$$

has only finitely many solutions. Styer [15] has shown that when a and b are primes and Eq. (3) holds, then, if $a \leqslant 13$, $b \leqslant 13$, $r \leqslant 50$, $s \leqslant 50$, $c \leqslant 1000$, we must have $x, y \leqslant 18$.

Many results on Eq. (2) have been obtained for specific (a, b, c), particularly when $(a, b) = (2, 3)$ or $(3, 2)$. (An account of such results, as well as a clear presentation of more general results, is given in [12, pp. 50–55].) Pillai [10] noted Herschfeld's result [7] that there exists $d_0 > 0$ such that $|d| > d_0$ implies $3^x - 2^y = d$ has at most one solution, and conjectured [11] that this $d_0 = 13$. Stroeker and Tijdeman [14] prove Pillai's conjecture using Baker's method, noting that Pillai's conjecture does not yield to classical methods as do other specific cases handled by Pillai. Pillai's conjecture is also proven as a specific case of Theorem 4, corollary, of this paper.

In addition to treating the above equations in order to respond to Edgar's question, we handle the same question when h is a variable: we derive an easy, practical method to obtain all solutions (x, y, z) to $a^x + b^y = c^z$ where c is odd or equal to 2, noting there are at most two solutions if c is prime and at most one solution when $c = 2$, except for two specific cases. Nagell [19], Makowski [17, 18], and others have found solutions for specific a, b, c. Whether or not c is prime, we can obtain bounds on z which depend only on a and b and which are, in general, not excessively large, sometimes equaling the highest z actually occurring in a given case (see Theorem 2 of this paper).

RESULTS

We will need a few elementary lemmata, which establish properties of numbers b_i defined as follows:

Let $\alpha = a_1 + b_1\sqrt{d}$, where a_1, b_1, d are non-zero integers, $(a_1, b_1) = 1$, d square-free, $(N(\alpha), 2d) = 1$, and let $\alpha^i = a_i + b_i\sqrt{d}$ for every i. Note $(a_i, b_i) = 1$, $a_i \neq 0$, $b_i \neq 0$.

LEMMA 1. $k \mid i \Rightarrow b_k \mid b_i$.

The proof follows from inspection of the expansion of $(a_k + b_k\sqrt{d})^{i/k}$.

LEMMA 2. *If k is the lowest value of i such that $g \mid b_i$, then $g \mid b_s$ implies $k \mid s$.*

Proof. $g \mid b_s = a_k b_{s-k} + b_k a_{s-k}$ implies $g \mid b_{s-k}$, so that $s = 2k$ is the lowest value of $s > k$ such that $g \mid b_s$, $s = 3k$ is the lowest value of $s > 2k$ such that $g \mid b_s$, etc.

LEMMA 3. *If $t > 0$, or if $t = 0$ and $p \mid d$, and k is the lowest value of i such that $p^t g \mid b_i$, and $p^t \parallel b_k$, then pk is the lowest value of i such that $p^{t+1} g \mid b_i$. Unless $t = 0$ and $p = 3 \mid d$, $p^{t+1} \parallel b_{pk}$.*

Proof. By Lemma 2, it is enough to examine the expansion of $(a_k + b_k\sqrt{d})^{s/k}$ to see that p is the lowest value of s/k such that $p^{t+1} g \mid b_s$, and, when $t \geqslant 1$, $p^{t+1} \parallel b_{pk}$. If $t = 0$ and $p \mid d$, $p \nmid a_k$ (since $(N(\alpha), d) = 1$) so that $p \parallel b_{pk}$ unless $p = 3$.

LEMMA 4. *Lemmatta 1 – 3 also apply to numbers b_i defined as follows: Let $r > 1$ be any odd number, and let $\mathfrak{a}\bar{\mathfrak{a}}$ be some factorization of $[r]$ into conjugate ideals in $Q(\sqrt{-d})$, where d is square-free, $0 < d \neq 1$ or 3, $(-d/r) = 1$, $(r, d) = 1$, and there is no $t \in \mathbb{Z}$ such that $t > 1$ and $[t] \mid \mathfrak{a}$. Let z be the lowest number such that $\mathfrak{a}^z = [\alpha]$ where $\alpha = a_z + b_z\sqrt{-d}$ for some a_z, b_z in $\mathbb{Z}$, and write $\alpha^{i/z} = a_i + b_i\sqrt{-d}$, $\mathfrak{a}^i = [a_i + b_i\sqrt{-d}]$, for every i such that $z \mid i$. (Note $z \nmid i$ implies $\mathfrak{a}^i \neq [a + b\sqrt{-d}]$ for any integers a, b.)*

The Lemmata 1–3 clearly apply to $\alpha = a_z + b_z\sqrt{-d}$, since we have $a_z \neq 0$, $b_z \neq 0$, $d \neq 0$, d square-free, $(a_z, b_z) = 1$, $(N(\alpha), 2d) = 1$. The only difference is that here the subscripts i are all multiples of z.

LEMMA 5. *Lemmata 1–3 also apply to numbers b_i defined as follows:*

For $d \equiv 7 \bmod 8$, let $\mathfrak{p}_2\bar{\mathfrak{p}}_2$ be the factorization of $[2]$ into distinct prime ideals in $Q(\sqrt{-d})$. Let z be the lowest number such that $\mathfrak{p}_2^z$ is principal. Write

$$\mathfrak{p}_2^i = \left[\left(\frac{a_z + b_z\sqrt{-d}}{2}\right)^{i/z}\right] = \left[\frac{a_i + b_i\sqrt{-d}}{2}\right] \qquad \text{for every } i \text{ such that } z \mid i.$$

The proofs of Lemmata 1–3 remain essentially the same for b_i thus defined, although for the new proof of Lemma 1 we must note that $b_k \mid b_i \Leftrightarrow b_k \mid 2^{i/k-1}b_i$, and for Lemma 3 we note that $p^{t+1}g \mid b_s \Leftrightarrow p^{t+1}g \mid 2^{s/k-1}b_s$.

THEOREM 1. *Let R be a set of positive rational primes, let S be the set of all numbers greater than one all of whose prime divisors are in R, and let T be the set of all numbers in S divisible by every prime in R. Let P and Q be relatively prime square-free integers such that $PQ \in T$. Take $A \in S$, $B \in S$, $AB \in T$, $(A, B) = 1$, $(AB/P)^{1/2} \in \mathbb{Z}$. Then, for every prime $r \notin R$, there is at most one such pair of numbers A, B such that*

$$A + B = r^x, \tag{4}$$

where x is any positive integer, except for the following cases allowing exactly three, two, and two solutions respectively:

$$\text{(i)} \quad 3 + 5 = 2^3, \qquad 3^3 + 5 = 2^5, \qquad 3 + 5^3 = 2^7, \tag{5}$$

$$\text{(ii)} \quad 3 + 13 = 2^4, \qquad 3^5 + 13 = 2^8, \tag{6}$$

$$\text{(iii)} \quad 3\left(\frac{3^{N-1}-1}{8}\right) + \left(\frac{3^{N+1}-1}{8}\right) = \frac{3^N - 1}{2},$$
$$3^{2N+1}\left(\frac{3^{N-1}-1}{8}\right) + \left(\frac{3^{N+1}-1}{8}\right) = \left(\frac{3^N-1}{2}\right)^3, \qquad N \text{ odd}. \tag{7}$$

Further, if $C \in T$, $(C/P)^{1/2} \in \mathbb{Z}$, and $C + 1 = r^y > 3^2$ for some integer y, then (4) has a solution with A, B defined as above if and only if $2 \mid y$, in which case

$$x = \frac{y}{2} + 1, \qquad A = 2^{x-1} \pm 1, \qquad B = 2^{x-1} \mp 1 \qquad \text{when} \quad r = 2, \quad y > 4, \tag{8}$$

and

$$x = \frac{y}{2}, \qquad A = \frac{r^x \pm 1}{2}, \qquad B = \frac{r^x \mp 1}{2} \qquad \text{when} \quad r > 2. \tag{9}$$

Proof. Assume (4) has a solution (with A, B restricted as in the formulation of Theorem 1). Let $P_1P_2 = P$, $P_1 \leqslant P_2$, let $Q_1Q_2 = Q$, and

assume, without loss of generality, $P_1Q_1 \mid A$. Let $e = 1$ or 0 according as $r = 2$ or not. Then (4) is equivalent to the equations in ideals in $Q(\sqrt{-P})$

$$\left[\frac{P_1(A/P_1)^{1/2} \pm (B/P_2)^{1/2}\sqrt{-P}}{2^e}\right] = \mathfrak{a}_{P_1}\mathfrak{p}_r^{x-2e}$$

and

$$\left[\frac{(A-B)/2^e \pm 2^{1-e}(AB/P)^{1/2}\sqrt{-P}}{2^e}\right] = \mathfrak{p}_r^{2(x-2e)},$$

where $\mathfrak{a}_{P_1}^2 = [P_1]$ and $\mathfrak{p}_r\bar{\mathfrak{p}}_r = [r]$. Note $r = 2 \Rightarrow P \equiv 7 \bmod 8$. Let $\mathfrak{p}_r^z = [(a_z + b_z\sqrt{-P}/2^e]$, $a_z, b_z \in \mathbb{Z}$, where z is the lowest number for which such an equation is possible. Write $a_i + b_i\sqrt{-P}/2^e = ((a_z + b_z\sqrt{-P})/2^e)^{i/z}$ for every i such that $z \mid i$. If $P = 1$, $P_1 = P_2$, so we can assume without loss of generality $2 \mid B$, and choose $(a_z, b_z) = (a_1, b_1)$ such that $2 \mid b_z = b_1$. If $P = 3$, choose $(a_z, b_z) = (a_1, b_1)$ such that $a_1 \in \mathbb{Z}$, $b_1 \in \mathbb{Z}$, noting that if $(a_1 + b_1\sqrt{-3})^n\varepsilon = (c + d\sqrt{-3})$, where $c \in \mathbb{Z}$, $d \in \mathbb{Z}$, and ε is a unit, then $\varepsilon = \pm 1$ since $2 \nmid a_1 - b_1$. For all P (noting the restriction above when $P = 1$), the choice of $|a_z|$, $|b_z|$ is unique; the signs will not matter in what follows.

Let j be the lowest number such that $2^{1-e}Q \mid b_j$. $j \mid 2(x - 2e)$, by Lemma 2. $j \mid x - 2e \Rightarrow \mathfrak{a}_{P_1} \sim [1] \Rightarrow P_1 = 1$, in which case, by Lemma 1, $j \mid x - 2e \Rightarrow 2^{1-e}Q \mid (B/P)^{1/2} \Rightarrow A = 1$, which was excluded. So $j \nmid x - 2e$. Thus all solutions to (4) have $x = jt/2 + 2e$, where $2 \nmid t$.

Choose J such that $j \mid J \mid 2(x - 2e)$. $2 \nmid 2(x - 2e)/J = w$ (since $2 \nmid 2(x - 2e)/j$);

$$\left[\frac{P_1(A/P_1)^{1/2} \pm (B/P_2)^{1/2}\sqrt{-P}}{2^e}\right]$$
$$= \mathfrak{a}_{P_1}\mathfrak{p}_r^{J/2}\mathfrak{p}_r^{((w-1)/2)J}$$
$$= \left[\frac{P_1u + v\sqrt{-P}}{2^e}\right]\left[\frac{a_{((w-1)/2)J} + b_{((w-1)/2)J}\sqrt{-P}}{2^e}\right] \tag{10}$$

for some u, v such that $2u \in \mathbb{Z}$, $2v \in \mathbb{Z}$;

$$[P_1]\mathfrak{p}_r^J = \left[\frac{(P_1^2u^2 - Pv^2)/2^e + 2^{1-e}P_1uv\sqrt{-P}}{2^e}\right] = [P_1]\left[\frac{a_J + b_J\sqrt{-P}}{2^e}\right],$$

so $r > 2 \Rightarrow u \in \mathbb{Z}$, $v \in \mathbb{Z}$. (If $P = 3$, we can take u and v to be integers.) $j \mid J \mid 2(x - 2e)$, so $Puv \in T$. $(P_2, u) = (P_1, v) = 1$ since $(P, a_J) = 1$. By (10), noting $2^{1-e}Q \mid b_{((w-1)/2)J}$ when $w > 1$, and recalling $Q_1 \mid A$ and $Q_2 \mid B$, we get

$Q_1 | u$, $Q_2 | v$. $(Q_2, u) = (Q_1, v) = 1$. So $P_1u^2 + P_2v^2 = r^{j/2+2e}$ is a solution to (4) in which the set of primes dividing P_1u^2 is the set of primes dividing A (similarly for P_2v^2, B). Since we can take $J = j$ we get: all solutions to (4) are of form

$$A_t + B_t = r^{jt/2+2e} = r^{x_t}, \tag{11}$$

where $2 \nmid t$ and the set of primes dividing A_t is the same regardless of the value of t (assuming, without loss of generality, $(A_{t_1}, A_{t_2}) > 1$ for any $t_1 \neq t_2$). The lowest solution, if it exists, is at $t = 1$.

Suppose there is a solution to (11) with $t > 1$. Then there is some prime $m \in R$ such that $m^2 | (A_tB_t/A_1B_1) = (b_{jt}/b_j)^2$ where $A_1 + B_1 = r^{j/2+2e}$. By Lemmata 2 and 3, $m | t$. Since we can take $J = jm$ in (10), we can take $t = m$ as a solution to (11) with $t > 1$. Since $2 \nmid (2(x-2e)/j)$ for any x satisfying (4), $m > 2$. By Lemma 3, if $m^n \| b_j$ and either $m > 3$ or $n > 0$, then $m^{n+1} \| b_{jm}$. Using the notation of (11), we get $(A_m, B_m) = (m^2A_1, B_1)$ or (A_1, m^2B_1) according as $m | A_1$ or $m | B_1$. Thus

$$(A_1 + B_1)m^2 = (r^{j/2+2e})m^2 > A_m + B_m = r^{jm/2+2e}, \tag{12}$$

$m^2 > r^{(j/2)(m-1)}$, $r = j = 2$, $m \leqslant 5$, $R = \{3, 5\}$, and (4) has three solutions: $(A, B, x) = (3, 5, 3)$, $(3^3, 5, 5)$, $(3, 5^3, 7)$. There are no further solutions since $\mathfrak{p}_2^i = [(1+\sqrt{-15})/2]^{i/2} = [(a_i + b_i\sqrt{-15})/2]$, $b_{18} \notin S$, $b_{30} \notin S$, $b_{50} \notin S$. Note: $P = 1$, 3, or 5 is impossible mod 8 when $r = 2$.

If $(r, R) \neq (2, \{3, 5\})$, we must have $m = 3$, $3 \nmid b_j$, $b_{3j} = \pm 3^N b_j = b_j(3a_j^2 - b_j^2P)/4^e$. Let $(K, D) = (A_1/3, B_1)$ or $(B_1/3, A_1)$ according as $3 | A_1$ or $3 | B_1$. $\pm 4^e \cdot 3^{N-1} = a_j^2 - b_j^2(P/3) = ((3K-D)/2^e)^2 - 4^{1-e}KD$, $\pm 16^e \cdot 3^{N-1} = (9K-D)(K-D)$. $9K - D \equiv K - D \bmod 8$, $9K - D = \pm 4^e$, $K - D = \pm 4^e \cdot 3^{N-1}$, $|K-D| \geqslant |9K-D|$, $K < D$, $8K = 4^e(3^{N-1} \pm 1)$, $K = 4^e(3^{N-1} \pm 1)/8$ where $\pm$ is $-$ if $e = 0$, $D = 4^e(3^{N+1} \pm 1)/8$ where $\pm$ is $-$ if $e = 0$. Using the notation of (11), $A_3B_3 = b_{3j}^2P/4^{1-e} = 3^{2N}b_j^2P/4^{1-e} = 3^{2N}A_1B_1$, $3^{2N+1}K = A_3$ or B_3. $r^{j/2+2e} = 4^e(3^N \pm 1)/2$ where $\pm$ is $-$ if $e = 0$. If $e = 0$, $2 \nmid N$ and we have (7). A third solution in this case requires $3^2j | 2x$, $(A_9, B_9) = (3^2A_3, B_3)$ or $(A_3, 3^2B_3)$, which is impossible as was (12) for $r > 2$. If $e = 1$, we have $2^{j/2+1} = 3^N + (-1)^g$, where $g = 1$ or 0. It is a familiar elementary result (see [13]) that we must have $(j/2+1, N, g) = (1, 1, 1)$, $(2, 1, 0)$, or $(3, 2, 1)$. But $x_1 = j/2 + 2 \geqslant 3$. So $(3K, D, x_1) = (3, 5, 3)$ or $(3, 13, 4)$. $(3, 5, 3)$ was handled above. $(3, 13, 4)$ has no third solution since $13 > 5$ and $3^2j | 2x - 4$ is impossible as was (12) for $D > 5$. (Proof of the non-existence of third solutions is also easily obtained by elementary congruence methods: see, for example, [6, pp. 200–201].)

Finally, suppose $C \in T$, $(C/P)^{1/2} \in \mathbb{Z}$, and $C + 1 = r^y$ for some y, and

suppose also that (4) has a solution. Let $1 + C = r^{jw/2+2e} = r^y$. If $2 \nmid (2(y-2e)/j) = w$,

$$\left[\frac{1 \pm (C/P)^{1/2}\sqrt{-P}}{2^e}\right] = \mathfrak{p}_r^{j/2}\mathfrak{p}_r^{((w-1)/2)j}$$

$$= \left[\frac{a_{j/2} + b_{j/2}\sqrt{-P}}{2^e}\right]\left[\frac{a_{((w-1)/2)j} + b_{((w-1)/2)j}\sqrt{-P}}{2^e}\right].$$

Treating this equation in the same manner as (10), we get $A_1 = 1$, contradiction. So $2 | w$, $2 | y$. Conversely, it is elementary that $2 | y$ ensures that (4) has the solution (8) or (9).

THEOREM 2. *If A, B, P, Q, R, S, T are defined as in the formulation of Theorem* 1, *and either $r = 2$ or r is any odd integer (not necessarily prime), then, if* (4) *has a solution and is not one of the equations in* (5) *or* (6), *we must have*

$$(x-s)\left|\frac{3^{u+v}}{2}h(-P)\left\langle q_1 - \left(\frac{-P}{q_1}\right), \ldots, q_n - \left(\frac{-P}{q_n}\right)\right\rangle\right., \tag{13}$$

where $s = 2$ or 0 according as $r = 2$ or not, $u = 1$ or 0 according as $3 < P \equiv 3 \bmod 8$ or not, $v = 1$ or 0 according as (4) *is the exceptional case* (7) *or not, $h(-P)$ is the lowest h such that $\mathfrak{a}^h$ is principal for every ideal $\mathfrak{a}$ in $Q(\sqrt{-P})$, $\langle a_1, \ldots, a_n\rangle = L \cdot C \cdot M \cdot (a_1, \ldots, a_n)$, $q_1 \cdots q_n$ is the prime factorization of Q, and (a/q) is the familiar Legendre symbol unless $q = 2$, in which case $(a/q) = 0$.*

Proof. Suppose in the proof of Theorem 1, we allow r to be an odd composite prime to every prime in R. Then, to each solution of (4) there corresponds a specific factorization of $[r]$ into conjugate ideals $\mathfrak{p}_r\bar{\mathfrak{p}}_r$. The lowest solution corresponding to any such factorization has $x = j/2$, where j is defined as in the proof of Theorem 1 for $\mathfrak{p}_r$.

Thus, from the proof of Theorem 1, noting $x - s = j/2$ unless (4) is one of (5), (6), (7) and taking $q_1 < q_2 < \cdots < q_n$, we get

$$(x-s)\left|\frac{3^{u+v}}{2}h(-P)\left\langle 2^G, 2^H\left(q_1 - \left(\frac{-P}{q_1}\right)\right), q_2 - \left(\frac{-P}{q_2}\right), \ldots, q_n - \left(\frac{-P}{q_n}\right)\right\rangle\right.,$$

where $G = 1$ or 0 according as $2 | P$ or not, and $H = 1$ or 0 according as $q_1 = 2$ or not. But we can take $G = H = 0$, noting the following:

If $2 \nmid P$ and $r > 2$, $4 | b_{2z}$, where b_i is defined as in the proof of Theorem 1 and z is defined as in Lemma 4. If $2 | P$ and $2 | z$, then $2 | b_z$. And if $2 | P$ and $2 \nmid z$, $z | h(-P)/2$ when $P > 2$, and $n > 0$ when $P = 2$.

Theorems 1 and 2 supply an easy, usable method to find all (x, y, z) giving solutions to any equation $a^x + b^y = c^z$ with (a, b, c) given and c odd or equal to 2. (Note here z is any positive integer, not the z of Lemma 4.) If c is unknown instead of given, Theorem 2 provides a finite list of possible z. For each such $z > 1$, it is often possible to compute all the solutions (x, y, c) by well-known elementary or algebraic methods. For example, after Theorem 2, conventional methods suffice to show there is no $x \geqslant 1$, $y \geqslant 1$ such that $2^x + 3^y$ is a perfect power other than 5^2. (See also Theorem 6.)

We can directly derive from Theorem 2 the following

COROLLARY TO THEOREM 2. *Let R be a finite set of rational primes and let S be the set of all rational integers divisible by no primes other than those in R.*

If $A \in S$, $B \in S$, $(A, B) = 1$, and r is odd or equal to 2, then

$$A + B = r^x \text{ implies } x \text{ is in } M, \tag{14}$$

where M is a finite set of integers less than M_0, where M_0 is an effectively computable bound dependent only on R.

(Note: For specific R, after the methods of Theorem 2 have been used to find all possible values x can take in Eq. (14), elementary methods often suffice to show Eq. (14) implies $x = 1$, regardless of the value of r, except for a finite list of specific cases.)

The corollary follows directly from Theorem 2, except that to handle the case $A = 1$ or $B = 1$ we need to double the bound in (13) and note that, if T is the set of numbers divisible by every prime in a given finite set of primes and by no other primes, there are at most two solutions to $A + 1 = r^x$ for $A \in T$ and r fixed, and, if two solutions (A_1, x_1) and (A_2, x_2) exist, $x_1 = 1$ and $x_2 = 2$.

From Theorem 1 we can derive several theorems relating to Edgar's question:

THEOREM 3. *Let $b > 1$ and c be positive rational integers and let p be a positive rational prime. Then the equation*

$$p^x - b^y = c \tag{15}$$

has at most one solution (x, y), where x is any positive rational integer and y is any positive rational *odd* integer, except for the following five cases:

$$2 + 1 = 3, \qquad 2^3 + 1 = 3^2 \tag{16}$$

$$3 + 5 = 2^3, \qquad 3^3 + 5 = 2^5 \tag{17}$$

$$3 + 13 = 2^4, \qquad 3^5 + 13 = 2^8 \tag{18}$$

$$5 + 3 = 2^3, \qquad 5^3 + 3 = 2^7 \tag{19}$$

$$3 + 10 = 13, \qquad 3^7 + 10 = 13^3. \tag{20}$$

When y is any positive even *integer, there is at most one solution to Eq.* (15).

Proof. If $(p, b) > 1$, Eq. (15) has at most one solution, so we assume $(p, b) = 1$. It is shown in [1] by elementary methods that Eq. (15) has at most one solution when $c = 1$ unless $p = 3$, $b = 2$, in which case, as shown by elementary methods in [13], there are exactly two solutions, given by Eqs. (16).

Thus, after Theorem 1, it is enough to point out that Eqs. (20) give the only instance of the exceptional case of Theorem 1 for which $(3^{N-1} - 1)/8 = 1$.

Note that Theorem 3 shows that Edgar's equation

$$p^m - q^n = 2^h \tag{21}$$

has at most two solutions (m_1, n_1) and (m_2, n_2). $2 \nmid n_1 - n_2$.

We can strengthen Theorem 3 somewhat with two additional theorems:

THEOREM 4. *If $p > 0$ is prime and $b > 0$ is any integer, $p^{x_1} - b^{y_1} = p^{x_2} - b^{y_2} > 0$ has no solutions x_1, y_1, x_2, y_2 (where $x_1 < x_2$, $y_1 > 0$) unless*

(a) $(p, b, x_1, y_1, x_2, y_2) =$

$$(3, 2, 1, 1, 2, 3), \quad (2, 3, 3, 1, 5, 3), \quad (2, 3, 4, 1, 8, 5), \quad \text{or} \quad (2, 5, 3, 1, 7, 3) \tag{22}$$

or

(b) *$p > 2$ and $\operatorname{ord}_p b$ is odd, where $\operatorname{ord}_p b$ is the least t such that $b^t \equiv 1 \bmod p$.*

Proof. As in Theorem 3, we can take $b > 1$ and $(b, p) = 1$. If $p > 2$ and $\operatorname{ord}_p b$ is even, then

$$p^{x_1}(p^{x_2 - x_1} - 1) = b^{y_1}(b^{y_2 - y_1} - 1) \Rightarrow 2 \mid y_2 - y_1,$$

so that Theorem 3 suffices to show that $(p, b, x_1, y_1, x_2, y_2) = (3, 2, 1, 1, 2, 3)$.

If $p = 2$, let $2^t \| b - 1$. Then $2 \nmid y_2 - y_1$ would imply $2^t \| b^{y_2 - y_1} - 1$, so that $x_1 = t$, $2^t = 2^{x_1} > b^{y_1} > 2^t$, contradiction. So $2 \mid y_2 - y_1$, and Theorem 3 suffices to show that $(p, b, x_1, y_1, x_2, y_2)$ is one of the three remaining cases listed in (22) above.

Noting $(b/p) = -1 \Rightarrow 2 \mid \operatorname{ord}_p b$ for odd p, and letting $(b/2) = 1$ for any b, we get

COROLLARY TO THEOREM 4. *Let p and q be positive primes, $p < q$, and let n, m, N, M be positive integers.*

Then, unless $(p/q) = (q/p) = 1$, there are no solutions to the equation

$$p^n - q^m = p^N - q^M \tag{23}$$

except when (p, q, n, m, N, M) or (q, p, m, n, M, N) is one of the solutions listed in (22) above. (Note that here $p^n - q^m$ may be less than zero.)

Proof. After Theorem 4, it is enough to note that, when $p > 2$, $(p/q) \neq (q/p) \Rightarrow p \equiv q \equiv 3 \bmod 4 \Rightarrow 2 \mid (N-n) - (M-m) \Rightarrow 2 \mid N-n$, $2 \mid M-m$, so that Eq. (23) has no solutions in this case, by Theorem 3.

THEOREM 5. *The equation*

$$|p^x - q^y| = c, \tag{24}$$

where p and q are distinct positive primes and c is any positive integer, has at most three solutions x, y, where x and y are positive integers. There are exactly three specific choices of (p, q, c) (taking $p < q$) giving three solutions: $(2, 3, 1)$, $(2, 3, 5)$, $(2, 5, 3)$.

Proof. Suppose for some (p, q, c) the equations

$$p^n + c = q^m \tag{25}$$

and

$$q^k + c = p^h \tag{26}$$

both have solutions (n_1, m_1) and (h_1, k_1), respectively. Then $p^r(p^{R-r} + 1) = q^t(q^{T-t} + 1)$ where $r = \min(n_1, h_1)$, $R = \max(n_1, h_1)$, $t = \min(m_1, k_1)$, $T = \max(m_1, k_1)$, so that, if $q > 2$, the congruence

$$p^x \equiv -1 \bmod q \tag{27}$$

has a solution $x > 0$, and, if $p > 2$, the congruence

$$q^y \equiv -1 \bmod p \tag{28}$$

has a solution $y > 0$. Suppose also that (25) has a second solution (n_2, m_2) so that $p^{n_1}(p^{n_2-n_1} - 1) = q^{m_1}(q^{m_2-m_1} - 1)$, assuming, without loss of generality, $n_1 < n_2$. If $(q, p, m_1, n_1, m_2, n_2)$ is one of the solutions listed in (22), $2 \mid n_2 - n_1$. If $(q, p, m_1, n_1, m_2, n_2)$ is not listed in (22), then $q > 2$, so that $2 \mid n_2 - n_1$ since (27) has a solution. Similarly, the existence of a second solution to (26), (h_2, k_2), say, implies $2 \mid k_2 - k_1$ (when (25) also gives a solution).

Now, if (24) has three or more solutions, then either (25) and (26) both have solutions, or one of (25) and (26) has three solutions. In either case, either (25) has two solutions such that $2 \mid n_2 - n_1$ or (26) has two solutions such that $2 \mid k_2 - k_1$, so that two of the three (or more) solutions to (24) must be among the five specific cases of Theorem 3 ((16) through (20)).

Let $p^x - q^y = c$ now represent one of the five specific cases of Theorem 3, with x_1, y_1 and x_2, y_2 representing the two solutions given by Theorem 3 to this specific case. Let "A" be the hypothesis that "there exists x_3, y_3 (distinct from (x_1, y_1) and (x_2, y_2)) such that $p^{x_3} - q^{y_3} = c$" and let "B" be the hypothesis that "$p^x - q^y = -c$ also has a solution." Note that "A" implies $2 \mid y_3$. Note also that "B" can hold for at most one pair x_1, y_1, since $p^x - q^y = -c$ can have no second solution x_2, y_2 with $2 \mid x_2 - x_1$ (by Theorem 3) or with $2 \nmid x_2 - x_1$ (by the first paragraph of this proof). "B" precludes "A" (again by the paragraph just cited).

Thus, to prove Theorem 5, it is enough to check each of the five specific cases of Theorem 3 and either find a solution satisfying "B," or prove there is no solution satisfying "B" or "A."

The specific cases given by (16), (17), and (19) have solutions satisfying "B" ($3 - 2^2 = -1$, $2^2 - 3^2 = -5$, $2 - 5 = -3$), so that each of these cases gives exactly three solutions to (24).

Equation (18) allows no solution satisfying "B" (since $3^n - 13 \equiv -2$ or $4 \bmod 8$, and $4 + 13 = 17$) or "A" (by Theorem 4). Equation (20) allows no solution satisfying "B" (since $13^n + 10 \equiv 2 \bmod 3$) or "$A$" (since $3^n + 10 \not\equiv 13^m \bmod 8$ if $2 \mid n$).

Finally, we prove

THEOREM 6. *If a and b are relatively prime integers greater than one, and if p is prime, then the equation*

$$a^x + b^y = p^z \tag{29}$$

has at most two solutions in positive integers (x, y, z) when $p \neq 2$, and at most one solution (x, y, z) when $p = 2$, except for two cases (taking $a < b$): $(a, b, p) = (3, 5, 2)$, which has exactly three solutions, and $(a, b, p) = (3, 13, 2)$, which has exactly two solutions.

Proof. We will use the following

LEMMA 6. *Equation (29) has at most one solution when the parities of x and y are preassigned, except for three choices of (a, b, p) (taking $a < b$): $(3, 5, 2)$, $(3, 13, 2)$, $(3, 10, 13)$.*

Lemma 6 follows directly from Theorem 1, noting that $(a, b, p) = (3, 10\ 13)$ is the only instance of (7) for which $(3^{N-1} - 1)/8 = 1$.

Consider first the case $p=2$. Taking congruences mod 8, we see that (29) has no solutions except in the following cases:

(i) $a \equiv b \equiv 7 \bmod 8$, in which case $2 \nmid x-y$.

(ii) One of a, b (say a) is congruent $\pm 3 \bmod 8$ while the other (say b) is congruent 7 mod 8, in which case $2 \mid x$ and $2 \nmid y$.

(iii) One of a, b (say a) is congruent 1 mod 8, while the other (say b) is congruent 7 mod 8, in which case $2 \nmid y$.

(iv) $a \equiv -b \equiv \pm 3 \bmod 8$, in which case $2 \nmid x$ and $2 \nmid y$.

By Lemma 6, cases (ii) and (iv) have at most one solution (x, y, z) unless $(a, b)=(3, 5)$ or $(3, 13)$, in which cases there are three and two solutions, respectively, by Theorem 1.

For case (i), let $2^s \| a+1$ and $2^t \| b+1$. $2^z > 1+b$, so $z > t$. If $2 \nmid y$, $b^y \equiv 2^t - 1 \bmod 2^{t+1}$, so $a^x \equiv 2^t + 1 \bmod 2^{t+1}$. If $2 \mid x$, $2^{s+1} \mid a^x - 1$. So $2 \nmid y$ implies $s < t$. Similarly, $2 \nmid x$ implies $t < s$. Thus case (i) has at most one solution, by Lemma 6.

For case (iii), let $2^s \| a-1$ and $2^t \| b+1$. $2 \nmid y$, so (as in the above) $a^x \equiv 2^t + 1 \bmod 2^{t+1}$. $s \leqslant t$. If $s=t$, $2 \nmid x$. If $s<t$, $2 \mid x$. Thus the parity of x, as well as that of y, is predetermined, and there is at most one solution, by Lemma 6.

Now consider the case $p>2$. Define $\operatorname{ord}_p r$ to be the least n such that $r^n \equiv 1 \bmod p$. It is elementary that $2 \mid \operatorname{ord}_p r$ if and only if there is an m such that $r^m \equiv -1 \bmod p$. Also easily derived is the result that $\operatorname{ord}_p s^n = \operatorname{ord}_p s/(\operatorname{ord}_p s, n)$.

Let $2^u \| \operatorname{ord}_p a$ and $2^v \| \operatorname{ord}_p b$, taking $u \leqslant v$. $v=0 \Rightarrow u=0 \Rightarrow 2 \nmid \operatorname{ord}_p a^x$ (for any x) $\Rightarrow (-a^x)^{\operatorname{ord}_p a^x} = -(a^x)^{\operatorname{ord}_p a^x} \equiv -1 \bmod p \Rightarrow 2 \mid \operatorname{ord}_p -a^x$. So if $v=0$ and there exist x, y such that $b^y \equiv -a^x \bmod p$, then $2 \mid \operatorname{ord}_p b = \operatorname{ord}_p -a^x (\operatorname{ord}_p b, y)$, contradiction.

So $v>0$, and there is an s such that $b^s \equiv -1 \bmod p$. If $-a^x \equiv b^y \bmod p$, $a^x \equiv b^{y+s} \bmod p$. If $2^t \| (x, \operatorname{ord}_p a)$, then $2^{u-t} \| \operatorname{ord}_p a/(\operatorname{ord}_p a, x) = \operatorname{ord}_p a^x = \operatorname{ord}_p b/(\operatorname{ord}_p b, y+s)$, so $2^{v-u+t} \| (\operatorname{ord}_p b, y+s)$.

$v>u$ implies $2 \mid y+s$, so the parity of y is predetermined when $v>u$. $v=u$ implies $y+s$ is odd or even according as $t=0$ or $t>0$, and $2 \mid \operatorname{ord}_p a$ if $v=u$, so the parity of x determines the parity of y when $v=u$. In either case, (29) has at most two solutions, by Lemma 6, unless $(a, b, p)=(3, 10, 13)$.

If $(a, b, p)=(3, 10, 13)$, $v=1>u=0$, so $2 \mid y+s=y+3$, $2 \nmid y$. If $2 \nmid x$, $(x, y, z)=(1, 1, 1)$ or $(7, 1, 3)$, by Theorem 1. If $2 \mid x$, $2 \mid z$ (using mod 10), $13^{z/2} - 3^{x/2} = 2^t$, where $t=1$ or $y-1$. Using mod 3, we get $2 \mid t$. Using mod 4, we get $2 \mid (x/2)$. By Lemma 6, the only solution to $13^{z/2} - 3^{x/2} = 2^t$ is $t=2$, $x=4$, $z=2$, which fails to satisfy (29).

Note Theorem 6 shows that there are at most two solutions to Eq. (21) even if h is unknown instead of given.

REFERENCES

Sources Relating to the Equation $p^x - b^y = c$.

1. J. W. S. CASSELS, On the equation $a^x - b^y = 1$, *Amer. J. Math.* **75** (1953), 159–162.
2. J. W. S. CASSELS, On the equation $a^x - b^y = 1$, II, *Proc. Cambridge Philos. Soc.* **56** (1960), 97–103.
3. J. W. S. CASSELS, On a class of exponential equations, *Ark. Mat.* **4** (1960), 231–233.
4. H. EDGAR, On a theorem of Suryanarayana, *in* "Proc. Wash. St. Univ. Conf., Number Theory, Pullman 1971," pp. 52–54.
5. R. K. GUY, "Unsolved Problems in Number Theory," Springer-Verlag, New York, 1981.
6. R. K. GUY, C. B. LACAMPAGNE, AND J. L. SELFRIDGE, Primes at a glance, *Math. Comp.* **48** (1987), 183–202.
7. A. HERSCHFELD, The equation $2^x - 3^y = d$, *Bull. Amer. Math. Soc. (N.S.)* **42**, No. 4 (1936), 231–234.
8. W. J. LEVEQUE, On the equation $a^x - b^y = 1$, *Amer. J. Math.* **74** (1952), 235–331.
9. S. S. PILLAI, On the inequality $0 < a^x - b^y \leqslant n$, *J. Indian Math. Soc. (1)* **19** (1931), 1–11.
10. S. S. PILLAI, On $a^x - b^y = c$, *J. Indian Math. Soc. (2)* **2** (1936), 19–122, Corr. **2**, 215.
11. S. S. PILLAI, On the equation $2^x - 3^y = 2^X + 3^Y$, *Bull. Calcutta Math. Soc.* **37** (1945), 15–20.
12. T. N. SHOREY AND R. TIJDEMAN, "Exponential Diophantine Equations," Cambridge Univ. Press, Cambridge, 1986.
13. W. SIERPINSKI, Sur une question concernant le nombre de diviseurs premiers d'un nombre natural, *Colloq. Math.* **6** (1958), 209–210.
14. R. J. STROEKER AND R. TIJDEMAN, "Diophantine Equations," pp. 321–369, Computational Methods in Number Theory, M. C. Tract 155, Centr. Math. Comp. Sci., Amsterdam, 1982.
15. R. STYER, Small two variable exponential diophantine equations, *Math. Comp.*, in press.

Sources Relating to the Equation $a^x + b^y = c^z$.

16. T. HADANO, On the Diophantine equation $a^x = b^y + c^z$, *Math. J. Okayama Univ.* **19**, No. 1 (1976/77), 25–29.
17. A. MAKOWSKI, On the diophantine equation $2^x + 11^y = 5^z$, *Nordisk Mat. Tidskr.* **7** (1959), 81, 96.
18. A. MAKOWSKI, On the equation $13^x - 3^y = 10$, *Math. Student* **28** (1960), 87.
19. T. NAGELL, Sur une classe d'équations exponentielles, *Ark. Mat.* **3** (1958), 569–582.
20. W. SIERPINSKI, On the equation $3^x + 4^y = 5^z$, *Wiadom. Math. (2)* **1** (1955/56), 194–195.
21. S. UCHIYAMA, On the Diophantine equation $2^x = 3^y + 13^z$, *Math. J. Okayama Univ.* **19**, No. 1 (1976/1977), 31–38.

Sources Relating to Theorem 1.

22. E. BENDER AND N. HERZBERG, Some diophantine equations related to the quadratic form $ax^2 + by^2$, *in* "Studies in Algebra and Number Theory" (G.-C. Rota, Ed.), pp. 219–272, Advances in Mathematics Supplementary Studies, Vol. 6, Academic Press, San Diego, 1979.
23. H. RUMSEY AND E. C. POSNER, On a class of exponential equations, *Proc. Amer. Math. Soc.* **15** (1964), 974–978.

Printed by Catherine Press, Ltd., Tempelhof 41, B-8000 Brugge, Belgium