GLASNIK MATEMATIČKI
Vol. 59(79)(2024), 299 – 312

ON A CONJECTURE CONCERNING THE NUMBER OF SOLUTIONS TO $a^x + b^y = c^z$, II

Maohua Le, Reese Scott and Robert Styer
Lingnan Normal College, China, Villanova University, USA

Abstract. Let a, b, c be distinct primes with $a < b$. Let $N(a,b,c)$ denote the number of positive integer solutions (x,y,z) of the equation $a^x + b^y = c^z$. In a previous paper [16] it was shown that if (a,b,c) is a triple of distinct primes for which $N(a,b,c) > 1$ and (a,b,c) is not one of the six known such triples then (a,b,c) must be one of three cases. In the present paper, we eliminate two of these cases (using the special properties of certain continued fractions for one of these cases, and using a result of Dirichlet on quartic residues for the other). Then we show that the single remaining case requires severe restrictions, including the following: $a = 2$, $b \equiv 1 \bmod 48$, $c \equiv 17 \mod 48$, $b > 10^9$, $c > 10^{18}$; at least one of the multiplicative orders $u_c(b)$ or $u_b(c)$ must be odd (where $u_p(n)$ is the least integer t such that $n^t \equiv 1 \bmod p$); 2 must be an octic residue modulo c except for one specific case; $2 \mid v_2(b-1) \le v_2(c-1)$ (where $v_2(n)$ satisfies $2^{v_2(n)} \parallel n$); there must be exactly two solutions (x_1, y_1, z_1) and (x_2, y_2, z_2) with $1 = z_1 < z_2$ and either $x_1 \ge 28$ or $x_2 \ge 88$. These results support a conjecture put forward in [28] and improve results in [16].

1. Introduction

Let $\mathbb{P}$ be the set of positive rational prime numbers. We consider $N(a,b,c)$, the number of solutions in positive integers (x,y,z) to the equation

$$a^x + b^y = c^z, a, b, c \in \mathbb{Z}^+, b > a > 1, \gcd(a,b) = 1. \tag{1.1}$$

This paper will continue the discussion of a conjecture on (1.1) found in [16, Conjecture 1.7].

There is much previous work on various types of exponential Diophantine equations with prime bases (see, for example, [1,3,6,10,11,14,20,22,24–26,30,

2020 *Mathematics Subject Classification.* 11D61.

Key words and phrases. Ternary purely exponential Diophantine equation, upper bound for number of solutions.

31]). Most such work deals with the familiar Pillai equation $c^z - b^y = a$, taking c and b prime. In 1985 the first author [14] obtained some early results on (1.1) and conjectured that (1.1) with a, b, c prime has at most one solution in positive integers (x, y, z) with $\min(x, y, z) > 1$. This conjecture is restated in [15] and proven in the introduction to [27]; it is also included in Theorem 1.2 below. Still unproven is the following conjecture.

Conjecture 1.1. *For a, b, and c distinct primes with $a < b$, we have $N(a, b, c) \leq 1$, except for*

(i) $N(2, 3, 5) = 2$, $(x, y, z) = (1, 1, 1)$ *and* $(4, 2, 2)$,
(ii) $N(2, 3, 11) = 2$, $(x, y, z) = (1, 2, 1)$ *and* $(3, 1, 1)$,
(iii) $N(2, 5, 3) = 2$, $(x, y, z) = (1, 2, 3)$ *and* $(2, 1, 2)$,
(iv) $N(2, 7, 3) = 2$, $(x, y, z) = (1, 1, 2)$ *and* $(5, 2, 4)$,
(v) $N(3, 5, 2) = 3$, $(x, y, z) = (1, 1, 3)$, $(1, 3, 7)$, *and* $(3, 1, 5)$,
(vi) $N(3, 13, 2) = 2$, $(x, y, z) = (1, 1, 4)$ *and* $(5, 1, 8)$.

In [26] it is shown that the more general equation

$$(-1)^u p^x + (-1)^v q^y = r^z, p, q, r \in \mathbb{P}, x, y, z, \in \mathbb{Z}^+, u, v \in \{0, 1\}$$

with $(p, q, r) \neq (2, 2, 2)$ has at most two solutions (x, y, z, u, v) except when (p, q, r) is a permutation of one of the following: $(5, 3, 2)$ which has seven solutions, $(7, 3, 2)$ which has four solutions, $(11, 3, 2)$ which has three solutions, $(13, 3, 2)$ which has three solutions. But improving this to at most one solution (with listed exceptions) has not been accomplished, even when (u, v) is fixed at $(0, 0)$.

A more recent result is the following, easily derived from [16, Lemma 1.2, Theorem 1.4, Theorem 1.5, Corollary 1.6, and Theorem 1.8].

Theorem 1.2. *Let a, b, c be distinct primes with $a < b$. If $(a, b, c) = (2, 3, 5)$, $(2, 3, 11)$, $(2, 5, 3)$, $(2, 7, 3)$, $(3, 5, 2)$ or $(3, 13, 2)$, equation* (1.1) *has only the solutions given in the above conjecture. Except for these six cases, if equation* (1.1) *has more than one solution, we must have $(a, b, c) = (2, p, q)$ for some odd primes $p > 10^9$ and $q > 10^{18}$, and there must be exactly two solutions (x_1, y_1, z_1) and (x_2, y_2, z_2) as follows:*

$$2^{x_1} + p^{y_1} = q, 2 \mid x_1, 2 \mid y_1, \tag{1.2}$$

and

$$2^{x_2} + p^{y_2} = q^{z_2}, 2 \mid x_2, 2 \nmid y_2, 2 \nmid z_2 > 1. \tag{1.3}$$

(1.3) follows from $p \equiv 1 \bmod 3$, shown in [16] using a result of Bennett [4, Theorem 1.1.], and a result of Bauer and Bennett [2, Corollary 1.7]. Using $p \equiv 1 \bmod 3$ leads to the following theorem ([16, Theorem 1.5]).

Theorem 1.3. *Let a, b, c be distinct primes with $a < b$. If* (1.1) *has more than one solution and is not one of the six exceptional cases of Theorem 1.2,* *then we must have* $(a, b, c) = (2, p, q)$ *for some odd primes* p *and* q *satisfying one of the following conditions:*

$$\begin{aligned} p &\equiv 13 \bmod 24, \quad q \equiv 5 \bmod 24, \\ p &\equiv 13 \bmod 24, \quad q \equiv 17 \bmod 24, \\ p &\equiv 1 \bmod 24, \quad q \equiv 17 \bmod 24. \end{aligned}$$

The purpose of this paper is to first eliminate two of the cases in Theorem 1.3 and then show that the single remaining case implies severe restrictions on p and q. We use the following notation.

- If $2^t \parallel n$, we write $v_2(n) = t$.
- If t is the least positive integer such that $n^t \equiv 1 \bmod p$ for some prime p, we write $u_p(n) = t$.

We prove the following improvement on Theorem 1.3.

Theorem 1.4. *Let* a, b, c *be distinct primes with* $a < b$. *If* (1.1) *has more than one solution and is not one of the six exceptional cases of Theorem 1.2, then we must have* $(a, b, c) = (2, p, q)$ *for some odd primes* p *and* q *satisfying all of the following conditions.*

(i) $p \equiv 1 \bmod 48$, $q \equiv 17 \bmod 48$, $2 \mid v_2(p-1) \leq v_2(q-1)$.

(ii) At least one of the multiplicative orders $u_p(q)$ *and* $u_q(p)$ *must be odd.*

(iii) 2 *is an octic residue modulo* q, *that is,* 2 *is congruent to an eighth power modulo* q, *except when* $v_2(p-1) = v_2(q-1) = 4$.

A further restriction is given by the following theorem.

Theorem 1.5. *In equations* (1.2) *and* (1.3), *the following must hold.*

(i) Either $x_1 \geq 28$ *or* $x_2 \geq 88$.

(ii) If $27 \geq v_2(p-1) = v_2(q-1)$, *then* $x_2 \geq 88$; *and if* $87 \geq v_2(p-1)$ *and* $v_2(p-1) < v_2(q-1)$, *then* $x_1 \geq 28$.

Theorem 1.4 and Theorem 1.5 combine with Theorem 1.2 to give information on cases with a, b, c distinct primes (other than the six known cases) in which (1.1) might have more than one solution. We hope this new information might eventually lead to a proof of the above conjecture.

This conjecture is a special case of the following conjecture given in [28].

Conjecture 1.6. *Let* $N(a, b, c)$ *be the number of solutions in positive integers* (x, y, z) *to the equation*

$$a^x + b^y = c^z, a, b, c \in \mathbb{Z}^+, b > a > 1, \gcd(a, b) = 1, \tag{1.4}$$

with a, b, c *not perfect powers.*

If $N(a, b, c) > 1$, *then* (a, b, c) *must be one of the following.*

(i) $N(2, 2^r - 1, 2^r + 1) = 2$, $(x, y, z) = (1, 1, 1)$ *and* $(r + 2, 2, 2)$, *where* r *is a positive integer with* $r \geq 2$, $r \neq 3$.

(ii) $N(2, 3, 11) = 2$, $(x, y, z) = (1, 2, 1)$ *and* $(3, 1, 1)$.

(iii) $N(2,3,35)=2$, $(x,y,z)=(3,3,1)$ *and* $(5,1,1)$.
(iv) $N(2,3,259)=2$, $(x,y,z)=(4,5,1)$ *and* $(8,1,1)$.
(v) $N(2,5,3)=2$, $(x,y,z)=(1,2,3)$ *and* $(2,1,2)$.
(vi) $N(2,5,133)=2$, $(x,y,z)=(3,3,1)$ *and* $(7,1,1)$.
(vii) $N(2,7,3)=2$, $(x,y,z)=(1,1,2)$ *and* $(5,2,4)$.
(viii) $N(2,89,91)=2$, $(x,y,z)=(1,1,1)$ *and* $(13,1,2)$.
(ix) $N(2,91,8283)=2$, $(x,y,z)=(1,2,1)$ *and* $(13,1,1)$.
(x) $N(3,5,2)=3$, $(x,y,z)=(1,1,3)$, $(1,3,7)$, *and* $(3,1,5)$.
(xi) $N(3,10,13)=2$, $(x,y,z)=(1,1,1)$ *and* $(7,1,3)$.
(xii) $N(3,13,2)=2$, $(x,y,z)=(1,1,4)$ *and* $(5,1,8)$.
(xiii) $N(3,13,2200)=2$, $(x,y,z)=(1,3,1)$ *and* $(7,1,1)$.

An effective upper bound for $N(a,b,c)$ was first given by A. O. Gel'fond [8] (Mahler [17] had earlier shown that the number of solutions was finite, using his p-adic analogue of the Diophantine approximation method of Thue-Siegel, but his method is ineffective). A straightforward application of an upper bound on the number of solutions of binary S-unit equations due to F. Beukers and H. P. Schlickewei [5] gives $N(a,b,c) \leq 2^{36}$. The following more accurate upper bounds for $N(a,b,c)$ have been obtained in recent years.

(i) (R. Scott and R. Styer, [28]) If $2 \nmid c$ then $N(a,b,c) \leq 2$.
(ii) (Y. Z. Hu and M. H. Le, [12]) If $\max\{a,b,c\} > 5 \cdot 10^{27}$, then $N(a,b,c) \leq 3$.
(iii) (Y. Z. Hu and M. H. Le, [13]) If $2 \mid c$ and $\max\{a,b,c\} > 10^{62}$, then $N(a,b,c) \leq 2$.
(iv) (T. Miyazaki and I. Pink, [18]) If $2 \mid c$ and $\max\{a,b,c\} \leq 10^{62}$, then $N(a,b,c) \leq 2$ except for $N(3,5,2)=3$.

More recently, Miyazaki and Pink ([19]) have begun work on improving $N(a,b,c) \leq 2$ to $N(a,b,c) \leq 1$ under certain conditions, including some specific results such as $c \notin \{2,3,5,6,17,257,65537\}$ when $N(a,b,c) > 1$ except for cases (i), (v), (vii), (x), and (xii) of Conjecture 1.6 ($c \neq 6$ has not previously been shown even for the more specific Pillai equation mentioned above).

Nevertheless, the problem of establishing $N(a,b,c) \leq 1$ with a finite number of specified exceptions remains open. This open question is addressed by the Conjecture 1.6

In Sections 3 and 4 we show that the first two cases given in Theorem 1.3 are impossible, and then, in Section 5, we prove Theorem 1.4 and Theorem 1.5 In Section 6, we consider (1.3) in the context of the *abc* conjecture.

2. Preliminary Lemmas

Lemma 2.1 (Theorem 6 of [26]). *Let p, q be distinct odd positive primes. For a given positive integer k, the equation*

$$q^n - p^m = 2^k, m, n \in \mathbb{N},$$

has at most one solution in positive integers (m, n).

Lemma 2.2 (Theorem 1.1. of [4]). *Let c and b be positive integers. Then there exists at most one pair (z, y) of positive integers for which*

$$0 < |c^z - b^y| < \frac{1}{4}\max\{c^{z/2}, b^{y/2}\}.$$

Lemma 2.3. *If a prime p is of the form $a^2 + 64b^2$ for some integers a and b, then 2 is a quartic residue modulo p.*

Proof. A proof is found in [7] which is simpler than Gauss's earlier proof of a conjecture of Euler. □

Lemma 2.4. *For any prime $p \equiv 1 \bmod 16$, 2 is an octic residue modulo p if and only if $p = a^2 + 256b^2$ for some integers a and b.*

Proof. This lemma is found in Whiteman [33], who cites Reuschle [29] for the original statement of the lemma and Western [32] for the first proof. □

Lemma 2.5 (Theorem 1.8 of [16]). *Let a, b, c distinct primes with $a < b$. If (1.1) has more than one solution and is not one of the six exceptional cases given in Theorem 1.2, then $a = 2$, $b > 10^9$, and $c > 10^{18}$.*

3. $(p, q) \not\equiv (13, 5) \bmod 24$

The purpose of this section is to prove the following result.

Proposition 3.1. *If $p \equiv q \equiv 5 \bmod 8$, then the equation*

$$2^x + p^y = q^z, p, q \in \mathbb{P}$$

has at most one solution in positive integers (x, y, z).

We will use four lemmas.

Lemma 3.2. *Let D be a natural number which is not a perfect square. Let h, k, h_1, and k_1 be integers. Suppose the equation $h^2 - Dk^2 = -1$ is solvable, and that $h_1 + k_1\sqrt{D}$ is its fundamental solution. Let p be any prime dividing h_1. Then if $U^2 - DV^2 = 1$, we must have $p \mid V$.*

Proof. The lemma follows from [21, Theorem 106] and [24, Lemma 1]. □

For the next two lemmas we establish notation for the continued fraction for $\sqrt{D}$ and its convergents (the basic results on which this notation is based can be found in [23]). For any non-square positive integer D let

$$\sqrt{D} = [a_0, \overline{a_1, \dots, a_s}]$$

represent the continued fraction expansion of $\sqrt{D}$. Let $\frac{P_m}{Q_m}$ be the m-th convergent of $\sqrt{D}$ and let

$$k_m = (-1)^{m+1}(P_m^2 - DQ_m^2), \tag{3.1}$$

noting that (as shown in [23]) all the k_m are positive integers with

$$k_{ns+j} = k_j, j = 0, \dots, s-1, n \in \mathbb{Z}^+. \tag{3.2}$$

We are now ready to state the following lemma.

LEMMA 3.3 (Theorem 10.8.2 of [23]). *Let k be an integer. If $|k| < \sqrt{D}$ and (x, y) is a solution of $x^2 - Dy^2 = k$ with $\gcd(x, Dy) = 1$, then $\frac{|x|}{|y|}$ is a convergent of the continued fraction for $\sqrt{D}$.*

LEMMA 3.4. *If $|x^2 - Dy^2| < \sqrt{D}$ and $\gcd(x, Dy) = 1$, then $|x^2 - Dy^2| = k_m$ for some $m \le s-1$.*

PROOF. By Lemma 3.3, x/y is a convergent of the continued fraction for $[a_0, \overline{a_1, \dots, a_s}]$, so that (3.2) gives the lemma. □

The following lemma is obtained by direct calculation.

LEMMA 3.5. *If $D = p^{2n} + 4$ where $p, n \in \mathbb{Z}^+$ with $2 \nmid p$, then we have*

$$\sqrt{D} = [p^n, \overline{(p^n-1)/2, 1, 1, (p^n-1)/2, 2p^n}]. \tag{3.3}$$

$$\begin{aligned} &\frac{P_0}{Q_0} = \frac{p^n}{1}, \quad \frac{P_1}{Q_1} = \frac{(p^{2n} - p^n + 2)/2}{(p^n - 1)/2}, \quad \frac{P_2}{Q_2} = \frac{(p^{2n} + p^n + 2)/2}{(p^n + 1)/2}, \\ &\frac{P_3}{Q_3} = \frac{p^{2n} + 2}{p^n}, \quad \frac{P_4}{Q_4} = \frac{(p^{2n} + 3)p^n/2}{(p^{2n} + 1)/2}. \end{aligned} \tag{3.4}$$

$$k_0 = 4, k_1 = p^n, k_2 = p^n, k_3 = 4, k_4 = 1. \tag{3.5}$$

We are now ready to give the proof of Proposition 3.1.

PROOF OF PROPOSITION 3.1. Let $p, q \in \mathbb{P}$, $3 \nmid pq$. Assume $2^x + p^y = q^z$ has two solutions (x, y, z). Let Z_1 be the least positive integer such that there exist rational integers X and Y with $\gcd(X, qY) = 1$ satisfying $X^2 - qY^2 = \pm p^{Z_1}$ (such Z_1 exists by Theorem 1.2). Let θ be any integer of the field $\mathbb{Q}(\sqrt{q})$ with norm $-p^{Z_1}$ such that $p \nmid \theta$ and $\theta \in \mathbb{Z}[\sqrt{q}]$ (such θ exist by [21, Theorem 107] and Theorem 1.3). By Lemma 3.1 of [25], $Z_1 \mid Z$ in any solution of $X^2 - qY^2 = \pm p^Z$ with X and Y rational integers, $\gcd(X, qY) = 1$. Applying Theorem 1.2 and using (1.3), let $\beta = 2^{x_2/2} + q^{(z_2-1)/2}\sqrt{q}$. By (1.3), β has norm $-p^{y_2}$, so $Z_1 \mid y_2$. Let $\alpha = \theta^t$ where $t = \frac{y_2}{Z_1}$, where y_2 is as in (1.3). Since y_2 is odd, t is odd, so that α has norm $-p^{y_2}$. Now we have $\beta\overline{\beta} = \alpha\overline{\alpha}$. Noting $\left(\frac{q}{p}\right) = 1$ where $\left(\frac{q}{p}\right)$ is the Legendre symbol, let $\mathfrak{p}\overline{\mathfrak{p}}$ be the unique ideal factorization of p in $\mathbb{Q}(\sqrt{q})$. Now we have the equation in ideals

$$[\beta][\overline{\beta}] = [\alpha][\overline{\alpha}] = \mathfrak{p}^{y_2}\overline{\mathfrak{p}}^{y_2},$$

where $p \nmid \alpha$ and $p \nmid \beta$, so that $[\beta] = \mathfrak{p}^{y_2}$ or $[\beta] = \overline{\mathfrak{p}}^{y_2}$, and $[\alpha] = \mathfrak{p}^{y_2}$ or $[\alpha] = \overline{\mathfrak{p}}^{y_2}$. Thus, $[\beta] = [\alpha]$ or $[\beta] = [\overline{\alpha}]$ so there exists a unit δ such that

$$\beta = \delta\alpha, \text{ or } \beta = \delta\overline{\alpha}.$$

Since the norms of α and β are odd, we must have $\delta \in \mathbb{Z}[\sqrt{q}]$. Let $\xi = \theta$ or $\overline{\theta}$ according as $\beta = \delta\alpha$ or $\delta\overline{\alpha}$. Thus we have

$$2^{x_2/2} + q^{(z_2-1)/2}\sqrt{q} = \xi^t\delta, \tag{3.6}$$

where δ has norm 1 since ξ^t has norm $-p^{y_2}$. Let

$$\theta = X_1 + Y_1\sqrt{q}, \delta = U + V\sqrt{q}, \tag{3.7}$$

where V is a rational integer, and X_1, Y_1, and U are nonzero rational integers.

Now we assume $q \equiv 5 \bmod 8$ and apply Lemma 3.5 with $D = q$, $n = y_1/2$, and p as in (1.2), noting that, since $q \equiv 5 \bmod 8$ and $2 \mid y_1$, we must have $x_1 = 2$ in (1.2). By (3.1), (3.4), and (3.5) we see that

$$P_2^2 - qQ_2^2 = -p^{y_1/2}. \tag{3.8}$$

Suppose $X^2 - qY^2 = \pm p^{n_0}$ for some integers X, Y and $n_0 > 0$ such that $\gcd(X, Y) = 1$ and $n_0 < y_1/2$. Then by Lemma 3.4 we must have $p^{n_0} = k_m$ for some $m \leq 4$, contradicting (3.5). So we have

$$Z_1 = y_1/2. \tag{3.9}$$

Since θ is any integer of the field in $\mathbb{Z}[\sqrt{q}]$ having norm $-p^{Z_1}$ and satisfying $p \nmid \theta$, by (3.8) and (3.4) we can take $\theta = X_1 + Y_1\sqrt{q}$ in (3.7) where

$$(X_1, Y_1, Z_1) = \left(\frac{1}{2}(p^{y_1} + p^{y_1/2} + 2), \frac{1}{2}(p^{y_1/2} + 1), y_1/2\right). \tag{3.10}$$

From (3.10) we see that

$$X_1^2 \equiv Y_1^2 q \equiv 1 \bmod p, \tag{3.11}$$

where the last congruence holds since $q \equiv 2^{x_1} = 4 \bmod p$, noting $x_1 = 2$ in (1.2).

By (3.4) and (3.5), we see that $P_4 + Q_4\sqrt{q}$ is the fundamental solution of $x^2 - qy^2 = -1$ (since P_m and Q_m increase with m). Since $p \mid P_4$, by Lemma 3.2 we must have $p \mid V$ in (3.7). Also $U^2 = V^2q + 1 \equiv 1 \bmod p$. So, in (3.7), we have

$$V \equiv 0 \bmod p, U \equiv \pm 1 \bmod p. \tag{3.12}$$

By (3.6) we have

$$2^{x_2/2} + q^{(z_2-1)/2}\sqrt{q} = (X_1 \pm Y_1\sqrt{q})^t(U + V\sqrt{q}). \tag{3.13}$$

Using (3.11) and considering the binomial expansion of $(X_1 \pm Y_1\sqrt{q})^t = X_t + Y_t\sqrt{q}$ with t odd we find

$$\pm Y_t \equiv 2^{t-1}Y_1 = 2^{t-2}(2Y_1) \equiv 2^{t-2} \bmod p, \tag{3.14}$$

where the last congruence follows from (3.10). Since $q \equiv 4 \bmod p$, (3.13) and (3.12) give

$$2^{z_2-1} \equiv q^{(z_2-1)/2} \equiv X_tV + Y_tU \equiv \pm Y_t \bmod p. \tag{3.15}$$

(3.14) and (3.15) give

$$2^{z_2-1} \equiv \pm 2^{t-2} \bmod p. \tag{3.16}$$

Since z_2 and t are both odd, and $p \equiv 1 \bmod 4$ by Theorem 1.3, (3.16) requires $\left(\frac{2}{p}\right) = 1$, $p \not\equiv 5 \bmod 8$, completing the proof of Proposition 3.1. □

4. $(p, q) \not\equiv (13, 17) \bmod 24$

The purpose of this section is to prove the following proposition.

Proposition 4.1. *If* $p \equiv 5 \bmod 8$ *and* $q \equiv 1 \bmod 8$*, then the equation*

$$2^x + p^y = q^z, p, q \in \mathbb{P}$$

has at most one solution in positive integers (x, y, z)*.*

We first prove a general lemma. We use the following notation: let d be a primitive root of a prime p; if an integer $n \equiv d^i \bmod p$ with $0 < i \leq p-1$, we call i the index of n for that primitive root d and write

$$i = i_p(n).$$

We also use the notation $v_2(n)$ to indicate the greatest integer t such that $2^t \mid n$. Notice that $v_2(\gcd(i_p(n), p-1))$ is independent of the choice of primitive root d. For brevity, we use the following notation:

$$w_p(n) = \min(v_2(i_p(n)), v_2(p-1)),$$

so that $0 \leq w_p(n) \leq v_2(p-1)$.

We use three simple observations.

Observation 4.2. *If* $a \equiv b \bmod p$*, then* $w_p(a) = w_p(b)$*.*

Observation 4.3. *We have*

(i) $w_p(-a) = w_p(a)$ *when* $w_p(a) < v_2((p-1)/2)$*,*
(ii) $w_p(-a) = v_2(p-1)$ *when* $w_p(a) = v_2((p-1)/2)$*,*
(iii) $w_p(-a) = v_2((p-1)/2)$ *when* $w_p(a) = v_2(p-1)$*.*

PROOF. If $w_p(a) \neq w_p(b)$, then $w_p(ab) = \min(w_p(a), w_p(b))$. If $w_p(a) = w_p(b)$ then $w_p(ab) > w_p(a)$. Since $w_p(-1) = v_2((p-1)/2)$, the observation holds. □

OBSERVATION 4.4. *For a given prime p and a given integer a, if $w_p(a^t) < v_2(p-1)$, then $v_2(t)$ is determined by $w_p(a^t)$.*

PROOF. Since the prime p and the integer a are known, $w_p(a)$ is known. Since $w_p(a^t) = w_p(a) + v_2(t)$, we see that $v_2(t)$ is known when $w_p(a^t)$ is known. □

LEMMA 4.5. *If (1.2) and (1.3) hold with $v_2(x_1) = v_2(x_2)$, then*

$$w_q(2^{x_1}) = v_2((q-1)/2). \tag{4.1}$$

PROOF. We consider (1.2) and (1.3) modulo q.

If $w_q(2^{x_1}) < v_2((q-1)/2)$, then, by Observation 4.3, $w_q(p^{y_1}) = w_q(-2^{x_1}) = w_q(2^{x_1})$. But then also, since $v_2(x_2) = v_2(x_1)$, we have $w_q(2^{x_2}) = w_q(2^{x_1}) = w_q(p^{y_1})$ and, by Observation 4.3, $w_q(2^{x_2}) = w_q(p^{y_2})$ so that $w_q(p^{y_1}) = w_q(p^{y_2})$. But this is impossible by Observation 4.4 since $2 \nmid y_1 - y_2$ and $w_q(2^{x_1}) = w_q(p^{y_1}) = w_q(p^{y_2}) < v_2((q-1)/2)$.

Similarly, if $w_q(2^{x_1}) = v_2(q-1)$, then, by Observation 4.3, $w_q(p^{y_1}) = v_2((q-1)/2)$, and, since $w_q(2^{x_1}) = w_q(2^{x_2})$, also $w_q(p^{y_2}) = w_q(-2^{x_2}) = v_2((q-1)/2)$, which is impossible by Observation 4.4 since $2 \nmid y_1 - y_2$.

So we must have (4.1). □

PROOF OF PROPOSITION 4.1. Assume (1.1) has more than one solution with $p \equiv 5 \bmod 8$, $q \equiv 1 \bmod 8$. By Theorem 1.3, we can assume that $5 \nmid pq$. We have (1.2) and (1.3). Considering congruences modulo 8, we find $2^{x_2} = 4$. Since 2 is a quadratic nonresidue of p, we have $w_p(2) = 0$, so that, by Observation 4.2, we have $1 = w_p(4) = w_p(2^{x_2}) = w_p(q^{z_2}) = w_p(q) = w_p(2^{x_1})$, so that, by Observation 4.4,

$$v_2(x_1) = v_2(x_2) = 1, \tag{4.2}$$

noting that $w_p(q^{z_2}) = w_p(q)$ since z_2 is odd. So we can apply Lemma 4.5 to obtain (4.1).

From (4.2) we have $v_2(x_1) = 1$, so that $2^{x_1} \equiv 4 \bmod 5$. Since $5 \nmid pq$ and $2 \mid y_1$ in (1.2), we must have $p^{y_1} \equiv 4 \bmod 5$. So $2 \parallel y_1$, giving

$$p^{y_1} \equiv 9 \bmod 16. \tag{4.3}$$

Since $q \equiv 1 \bmod 8$, we have $2^{x_1} > 4$ by (1.2), which, along with (4.2), gives

$$2 \parallel x_1 \geq 6. \tag{4.4}$$

Considering congruences modulo 16 and using (1.2), (4.3), and (4.4), we see that $2^3 \parallel q-1$, so that $v_2((q-1)/2) = 2$, and (4.1) becomes

$$w_q(2^{x_1}) = v_2((q-1)/2) = 2. \tag{4.5}$$

From (4.4) we see that $q = p^{y_1} + 2^{x_1}$ is of the form $a^2 + 64b^2 = (p^{y_1/2})^2 + 64(2^{(x_1-6)/2})^2$, so, by Lemma 2.3, 2 is a quartic residue modulo q, so that $4 \mid i_q(2)$ for any choice of primitive root d. Thus $8 \mid i_q(2^{x_1})$ so that

$$w_q(2^{x_1}) = \min(v_2(i_q(2^{x_1})), v_2(q-1)) = 3,$$

contradicting (4.5), proving Proposition 4.1. □

5. Proofs of Theorem 1.4 and Theorem 1.5

Proof of Theorem 1.4. From Theorem 1.3, Proposition 3.1, and Proposition 4.1, we have

$$p \equiv 1 \bmod 24, q \equiv 17 \bmod 24. \tag{5.1}$$

We prove (i), (ii), and (iii) separately.

(i) From (1.2) and (1.3) we have

$$2^{x_1} + (p^{y_1} - 1) = (q-1), 2 \mid x_1, 2 \mid y_1,$$

and

$$2^{x_2} + (p^{y_2} - 1) = (q^{z_2} - 1), 2 \mid x_2, 2 \nmid y_2, 2 \nmid z_2.$$

If $v_2(p-1) > v_2(q-1)$, then we see that $x_1 = v_2(q-1) = v_2(q^{z_2}-1) = x_2$, contradicting Lemma 2.1, so that

$$v_2(p-1) \le v_2(q-1). \tag{5.2}$$

So now we have either

$$v_2(p-1) = v_2(q-1) = x_1 \tag{5.3}$$

or

$$v_2(q-1) > v_2(p-1) = x_2. \tag{5.4}$$

Since $2 \mid x_1$ and $2 \mid x_2$, from (5.3) and (5.4) we have

$$2 \mid v_2(p-1). \tag{5.5}$$

From (5.1) and (5.5) we have

$$v_2(p-1) \ge 4, \tag{5.6}$$

which, in combination with (5.1) and (5.2), gives

$$p \equiv 1 \bmod 48, q \equiv 17 \bmod 48. \tag{5.7}$$

(5.7), (5.5), and (5.2) give (i) of Theorem 1.4.

(ii) We use the notation of Sections 1 and 4. Using Observation 4.2 and noting that z_2 is odd, we find

$$w_p(2^{x_1}) = w_p(q) = w_p(q^{z_2}) = w_p(2^{x_2}).$$

If $u_p(q)$ is even, then $w_p(q) < v_2(p-1)$, so that $w_p(2^{x_1}) = w_p(2^{x_2}) \le v_2(\frac{p-1}{2})$, so that, by Observation 4.4,

$$v_2(x_1) = v_2(x_2). \tag{5.8}$$

So we can apply Lemma 4.5 to find

$$w_q(2^{x_1}) = v_2\left(\frac{q-1}{2}\right).$$

So also, by (5.8), $w_q(2^{x_2}) = v_2(\frac{q-1}{2})$, so that by (ii) of Observation 4.3, $w_q(p) = w_q(p^{y_2}) = w_q(-2^{x_2}) = v_2(q-1)$, so that $u_q(p)$ is odd, giving (ii) of Theorem 1.4.

(iii) Assume that we do not have $v_2(p-1) = v_2(q-1) = 4$. We can also assume we do not have $v_2(p-1) = v_2(q-1) = 6$ since then (1.2) becomes $2^6 + p^{y_1} = q$ so that, by Lemma 2.3 and Lemma 2.4, $w_q(2) = 2$ and $w_q(2^{x_1}) = w_q(2) + v_2(6) = 3$; applying Observation 4.3 (i) to equations (1.2) and (1.3) and noting that $v_2(y_1) > v_2(y_2)$, we find $3 = w_q(p^{y_1}) > w_q(p^{y_2}) = w_q(2^{x_2})$, requiring $2 \nmid x_2$, contradicting (1.3).

So now, if $v_2(p-1) = v_2(q-1)$, then $x_1 \geq 8$ (by (5.5)). And if $v_2(p-1) < v_2(q-1)$, then $x_2 = v_2(p-1)$ and $x_1 > v_2(p-1)$, so that, by (5.5) and (5.6), $x_1 \geq 8$, unless $x_2 = 4$ and $x_1 = 6$ which is an impossible case by Lemma 2.2 and Lemma 2.5. So $x_1 \geq 8$, so that q is of the form $a^2 + 256b^2$. By (5.7), $q \equiv 1 \bmod 16$. So (iii) of Theorem 1.4 follows from Lemma 2.4. □

Proof of Theorem 1.5. By [16, Corollary 1.6], $z_2 > 1$ in (1.3). So, using Lemma 2.5, we have

$$2^{27} < \frac{10^9}{4} < \frac{q^{1/2}}{4}, 2^{87} < \frac{10^{27}}{4} < \frac{q^{3/2}}{4} \leq \frac{q^{z_2/2}}{4},$$

so that Lemma 2.2 applies to give (i) of Theorem 1.5. So (5.3) and (5.4) give (ii) of Theorem 1.5. □

6. Unlikelihood of equation (1.3)

In this section we consider the equation (1.3) in the context of the *abc* conjecture. Let a, b, and c be positive integers such that $a + b = c$; define $Q = Q(a,b,c)$ as

$$Q = \frac{\log(c)}{\log(\text{rad}(abc))}$$

where $\text{rad}(m)$ is the product of all distinct primes dividing m. Then for (1.3) we have

$$\begin{aligned} Q = \frac{z_2 \log(q)}{\log(2) + \log(p) + \log(q)} &\geq \frac{3\log(q)}{(3/2)\log(q) + \log(2)} \\ &= 2 - \frac{2\log(2)}{(3/2)\log(q) + \log(2)} > 1.97 \end{aligned}$$

by Lemma 2.5.

The highest value for Q found in recent researches on the *abc* conjecture is $Q = 1.62991$ for $(a,b,c) = (2, 3^{10} \cdot 109, 23^5)$. If $z_2 > 3$, then we have

$Q > 3.29$: if a conjecture of Tenenbaum (quoted in [9, Section B19]) is true, then $Q = 3.29$ is impossible, so that $z_2 = 3$.

If $y_2 > 1$, then $\min(x_2, y_2, z_2) > 2$, so that (1.3) contradicts the familiar Beal conjecture (see [9, Section B19]). If we assume the Beal conjecture is true, then we can eliminate the case $v_2(p-1) < v_2(q-1)$ from consideration, since this case requires $y_2 > y_1 \geq 2$ (if $v_2(p-1) < v_2(q-1)$, then $x_2 = v_2(p^{y_2} - 1) < \min(v_2(p^{y_1} - 1), v_2(q-1)) \leq x_1$, so that, since $q^{z_2} > q^{z_1} = q$, we must have $y_2 > y_1 \geq 2$).

If $y_2 = 1$, we can assume $v_2(p-1) = v_2(q-1)$. Writing (1.3) as

$$2^{x_2} - q^{z_2} = (2^{x_2/2})^2 - (q^{(z_2-1)/2})^2 q = -p, |-p| < \sqrt{q},$$

we see that $\frac{2^{x_2/2}}{q^{(z_2-1)/2}}$ must be a convergent of the continued fraction expansion of $\sqrt{q}$. If it can be shown that $y_2 = 1$ is impossible, then the Conjecture 1.1 at the beginning of this paper would follow from the Beal conjecture.

Acknowledgements

The authors thank the anonymous referees for very helpful suggestions and corrections.

References

[1] L. J. Alex, *Diophantine equations related to finite groups*, Comm. Algebra **4** (1976), 77–100.

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

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

[4] M. A. Bennett, *Differences between perfect powers*, Canad. Math. Bull. **51** (2008), 337–347.

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

[6] J. L. Brenner and L. L. Foster, *Exponential Diophantine equations*, Pacific J. Math. **101** (1982), 263–301.

[7] G. Lejeune Dirichlet, *Ueber den biquadratischen Character der Zahl "Zwei"*, J. Reine Angew. Math. **57** (1860), 187–188.

[8] A. Gelfond, *Sur la divisibilité de la différence des puissances de deux nombres entiers par une puissance d'un idéal premier*, Rec. Math. [Mat. Sbornik] N.S. **7(49)** (1940), 7–25.

[9] R. K. Guy, Unsolved problems in number theory, Springer-Verlag, New York, 2004.

[10] T. Hadano, *On the Diophantine equation* $a^x = b^y + c^z$, Math. J. Okayama Univ. **19** (1976/77), 25–29.

[11] A. Herschfeld, *The equation* $2^x - 3^y = d$, Bull. Amer. Math. Soc. **42** (1936), 231–234.

[12] Y. Hu and M. Le, *An upper bound for the number of solutions of ternary purely exponential diophantine equations*, J. Number Theory **183** (2018), 62–73.

[13] Y. Hu and M. Le, *An upper bound for the number of solutions of ternary purely exponential Diophantine equations II*, Publ. Math. Debrecen **95** (2019), 335–354.

[14] 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).

[15] M. Le, *A conjecture concerning the exponential Diophantine equation* $a^x + b^y = c^z$, Acta Arith. **106** (2003), 345–353.

[16] M. Le and R. Styer, *On a conjecture concerning the number of solutions to* $a^x + b^y = c^z$, Bull. Aust. Math. Soc. **108** (2023), 40–49.

[17] K. Mahler, *Zur Approximation algebraischer Zahlen. I*, Math. Ann. **107** (1933), 691–730.

[18] T. Miyazaki and I. Pink, *Number of solutions to a special type of unit equations in two variables*, Amer. J. Math. **146** (2024), 295–369.

[19] T. Miyazaki and I. Pink, *Number of solutions to a special type of unit equations in two variables II*, Res. Number Theory **10** (2024), Paper No. 36.

[20] D. Z. Mo and R. Tijdeman, *Exponential Diophantine equations with four terms*, Indag. Math. (N.S.) **3** (1992), 47–57.

[21] T. Nagell, Introduction to Number Theory, John Wiley & Sons, Inc., New York; Almqvist & Wiksell, Stockholm, 1951.

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

[23] O. Perron, Die Lehre von den Kettenbrüchen, Chelsea Publishing Co., New York, 1950.

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

[25] R. Scott, *Elementary treatment of* $p^a \pm p^b + 1 = x^2$, (2006), arxiv:math.0608796.

[26] 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.

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

[28] R. Scott and R. Styer, *Number of solutions to* $a^x + b^y = c^z$, Publ. Math. Debrecen **88** (2016), 131–138.

[29] C. G. Reuschle, *Mathematische Abhandlung, enthaltend neue Zahlentheoretische Tabellen, Programm zum Schlusse des Schuljahrs 1855–56 am Königlichen Gymnasium zu Stuttgart*, (1856), 61 pp.

[30] S. Uchiyama, *On the Diophantine equation* $2^x = 3^y + 13^z$, Math. J. Okayama Univ. **19** (1976/77), 31–38.

[31] B. M. M. de Weger, *Solving exponential Diophantine equations using lattice basis reduction algorithms*, J. Number Theory **26** (1987), 325–367.

[32] A. E. Western, *Some criteria for the residues of eighth and other powers*, Proc. London Math. Soc. (2) **9** (1911), 244–272.

[33] A. L. Whiteman, *The sixteenth power residue character of* 2, Canad. J. Math. **6** (1954), 364–373.

M. H. Le
Institute of Mathematics
Lingnan Normal College
Zhanjiang 524048, Guangdong
China
E-mail : lemaohua2008@163.com

R. Scott
Somerville, MA
USA

R. Styer
Department of Mathematics
Villanova University
Villanova, PA
USA
E-mail : robert.styer@villanova.edu

Received: 7.7.2023.
Revised: 10.1.2024.

O HIPOTEZI O BROJU RJEŠENJA JEDNADŽBE $a^x + b^y = c^z$, II. DIO

Sažetak. Neka su a, b, c različiti prosti brojevi uz $a < b$. Neka je $N(a, b, c)$ broj prirodnih rješenja (x, y, z) jednadžbe $a^x + b^y = c^z$. U prošlom članku [16] pokazano je da ako je (a, b, c) trojka različitih prostih brojeva za koju je $N(a, b, c) > 1$ i (a, b, c) nije jedna od šest poznatih takvih trojki, onda su samo tri mogućnosti za (a, b, c). U ovom radu eliminiramo dvije od ove tri mogućnosti (koristeći specijalna svojstva određenih verižnih razlomaka u jednom od ovih slučajeva i koristeći Dirichletov rezultat o ostatcima četvrtih potencija za drugi slučaj). Zatim pokazujemo da jedini preostali slučaj zahtijeva stroga ograničenja, uključujući: $a = 2$, $b \equiv 1 \bmod 48$, $c \equiv 17 \mod 48$, $b > 10^9$, $c > 10^{18}$; barem jedan od multiplikativnih redova $u_c(b)$ ili $u_b(c)$ mora biti neparan (gdje je $u_p(n)$ najmanji cijeli prirodan broj t takav da je $n^t \equiv 1 \bmod p$); 2 mora biti ostatak osme potencije za c osim u jednom posebnom slučaju; $2 \mid v_2(b-1) \leq v_2(c-1)$ (gdje $v_2(n)$ zadovoljava $2^{v_2(n)} \parallel n$); postoje točno dva rješenja (x_1, y_1, z_1) i (x_2, y_2, z_2) uz $1 = z_1 < z_2$ te vrijedi ili $x_1 \geq 28$ ili $x_2 \geq 88$. Ovi rezultati podržavaju hipotezu iznesenu u [28] i poboljšavaju rezultate iz [16].