JOURNAL OF EUROPEAN ACADEMY OPEN UNIVERSITY OPEN UNIVERSITY

Vol. 2, No. 7, 2026 16
Research Article

A Finite Verification of Jeśmanowicz' Conjecture under 2 // mn for n ≤ 200

Haoyuan Wu[1,*]

[1] School of Science, University of Science and Technology Liaoning, Anshan 114051, China
** Correspondence: luvzhuoer@163.com*

Abstract

Jeśmanowicz' conjecture is a long-standing problem on exponential Diophantine equations associated with primitive Pythagorean triples. Let $m > n$ be coprime positive integers of opposite parity. The conjecture asserts that $(m^2 - n^2)^x + (2mn)^y = (m^2 + n^2)^z$ has only the positive integer solution $(x, y, z) = (2, 2, 2)$. In this article, we prove the conjecture in the case $2 \nmid mn$ for $n \leq 200$. The proof combines four known results with an exact finite modular argument. The known results reduce the problem to 170 admissible parameter pairs, and every exceptional solution for a remaining pair must satisfy $y = 1$. All residual cases are then excluded by comparing finite power-residue sets modulo a fixed collection of 13 moduli. The verification uses only exact integer and modular arithmetic and is reproducible from the script provided in the appendix.

Keywords

Jeśmanowicz' conjecture; exponential Diophantine equation; primitive Pythagorean triple; modular arithmetic; power residues

MSC 2020: 11D61; 11D41

1. Introduction

Exponential Diophantine equations occupy a central place in number theory because simple additive relations between integer powers can lead to difficult questions about divisibility, parity, and the arithmetic structure of the bases. One important family is the ternary purely exponential equation $a^x + b^y = c^z$. Jeśmanowicz' conjecture concerns the special situation in which the three bases form a primitive Pythagorean triple, so that the underlying quadratic identity already supplies the solution $(x, y, z) = (2, 2, 2)$. The conjecture asks whether any other positive exponent triple can occur.

Let (a, b, c) be a primitive Pythagorean triple. After interchanging the two legs if necessary, it can be parameterized as

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2. \quad (1.1)$$

where $m > n$ are positive integers, $\gcd(m, n) = 1$, and m and n have opposite parity. In 1956, Jeśmanowicz [1] conjectured that

$$(m^2 - n^2)^x + (2mn)^y = (m^2 + n^2)^z \quad (1.2)$$

has only the positive integer solution

$$(x, y, z) = (2, 2, 2). \quad (1.3)$$

The conjecture remains open in general. Research over the past several decades has proceeded through special families of Pythagorean triples, congruence restrictions, parity arguments, and effective estimates for exponential Diophantine equations. Miyazaki [2] developed generalizations of classical results for primitive triples, while Fujita and Miyazaki [3] obtained criteria based on congruence relations. Ma and Chen [4] established a strong restriction when 4 does not divide mn and $y \geq 2$, and Han and Yuan [5] introduced a prime-divisor criterion in the case $2 \nmid mn$. The broader development of the ternary equation $a^x + b^y = c^z$ and its connection with Jeśmanowicz' conjecture is reviewed by Le, Scott and Styer [6].

Other arithmetic criteria for primitive triples were obtained by Deng and Huang [9] and Deng and Guo [10]. A result especially relevant to bounded values of the Euclidean parameter was proved by Miyazaki and Terai [11]: under

$n \equiv 2 \pmod 4$, they obtained several sufficient conditions, and as a corollary established the conjecture without any restriction on m when n/2 is odd and $n < 100$. The finite range considered here is different in scope because it treats

both parity placements allowed by $2 \mathbin{/\!/} mn$ and extends the bounded parameter region to $n \leq 200$ by combining later effective results with exact modular certificates.

More recent results provide effective restrictions on the remaining parameter space. Yang and Fu [7], combining Baker's method with elementary arguments, proved the conjecture when $mn \equiv 2 \pmod 4$ and $m > 17.8n$. Styer [8] subsequently proved the primitive case whenever one of the two legs of the Pythagorean triple is at most 10^6. These results do not subsume one another: each eliminates a different region of the parameter space or a different type of exceptional solution.

The present article studies how these complementary results interact in the arithmetic case

$$2 \mathbin{/\!/} mn. \quad (1.4)$$

Our aim is not to derive a new global bound for the conjecture. Instead, we combine the available structural and effective criteria to reduce a finite parameter region to a small exact residual set, and then eliminate that residual set by modular power-residue certificates. This approach yields the following theorem.

Theorem 1.1. Let $m > n$ be positive integers satisfying $\gcd(m, n) = 1$, $m \not\equiv n \pmod 2$, and $2 \mathbin{/\!/} mn$. If $n \leq 200$, then Equation (1.2) has only the positive integer solution $(x, y, z) = (2, 2, 2)$.

The proof has two components. First, the cited analytic and arithmetic criteria reduce the range $n \leq 200$ to exactly 170 residual pairs (m, n). Second, Ma and Chen's theorem forces $y = 1$ for any exceptional solution in this case. For each residual pair, we then find a modulus q for which the possible residues of $A^x + B$ and C^z are disjoint, where $A = m^2 - n^2$, $B = 2mn$, and $C = m^2 + n^2$. A fixed collection of 13 moduli covers all 170 pairs.

The modular stage is finite but not a bounded search over the exponents. Because powers modulo q are eventually periodic, the full sets of positive power residues can be computed exactly. Thus a single disjointness certificate excludes all positive values of x and z simultaneously. The exact verification script is given in Appendix B.

The remainder of the article is organized as follows. Section 2 recalls the known results used in the reduction. Section 3 performs the finite parameter reduction. Section 4 develops the modular certificate argument, and Section 5 proves the main theorem. Concluding remarks and complete verification data are given in Section 6 and the appendices.

2. Preliminary results

Throughout the article, put

$$A = m^2 - n^2, \quad B = 2mn, \quad C = m^2 + n^2. \quad (2.1)$$

We recall four results that will be used in the proof. The first one is due to Ma and Chen [4].

Lemma 2.1. *Suppose that 4 does not divide mn. If $A^x + B^y = C^z$ and $y \geq 2$, then $(x, y, z) = (2, 2, 2)$.*

Under $2 \mathbin{/\!/} mn$, Lemma 2.1 gives an immediate reduction.

Corollary 2.2. *Assume $2 \mathbin{/\!/} mn$. Every exceptional solution of Equation (1.2) satisfies $y = 1$.*

The second criterion is due to Han and Yuan [5].

Lemma 2.3. *Assume $2 \mathbin{/\!/} mn$. If $m + n$ has a prime divisor p with p not congruent to 1 modulo 16, then Equation (1.2) has only the solution (2, 2, 2).*

The following effective ratio estimate was proved by Yang and Fu [7].

Lemma 2.4. *Suppose $mn \equiv 2 \pmod 4$. If $m > 17.8n$, then Jeśmanowicz' conjecture holds for the primitive Pythagorean triple generated by m and n.*

Finally, we use a finite-base theorem of Styer [8].

Lemma 2.5. *For a primitive Pythagorean triple (A, B, C), Jeśmanowicz' conjecture holds if $A \leq 10^6$ or $B \leq 10^6$.*

The proof below depends on the successive application of Lemmas 2.1, 2.3, 2.4, and 2.5. Each result removes a different part of the parameter space.

3. Reduction of the parameter space

We begin with a direct consequence of the ratio bound and the finite-base theorem.

Proposition 3.1. *Under the assumptions of Theorem 1.1, Jeśmanowicz' conjecture holds whenever $n \le 167$.*

Proof. If $m > 17.8n$, the conclusion follows from Lemma 2.4. It therefore remains to consider $m \le 17.8n$.

In this range, $B = 2mn \le 35.6n^2$. For $n \le 167$, we have $35.6 \times 167^2 = 992848.4 < 10^6$. Hence $B < 10^6$, and Lemma 2.5 applies. □

The value $n = 168$ is impossible under $2 \mathbin{/\!/} mn$, because 8 divides 168. Hence only

$$169 \le n \le 200 \tag{3.1}$$

requires further consideration.

For each n in (3.1), we enumerate integers m satisfying $n < m \le 89n/5$ and retain only those pairs for which

$$\gcd(m,n)=1, \quad m \text{ not congruent to } n \pmod 2, \quad mn \text{ congruent to } 2 \pmod 4, \tag{3.2}$$

$$A > 10^6, \quad B > 10^6, \tag{3.3}$$

and every prime divisor p of $m + n$ satisfies

$$p \text{ congruent to } 1 \pmod{16}. \tag{3.4}$$

The use of $89n/5$ instead of $17.8n$ avoids floating-point arithmetic. Any pair outside this interval is covered by Lemma 2.4. A pair violating (3.3) is covered by Lemma 2.5, and a pair violating (3.4) is covered by Lemma 2.3.

The exact enumeration leaves no pair for $n = 169$ and exactly 170 pairs for $170 \le n \le 200$. Their distribution by n is shown in Table 1.

Table 1. Number of residual pairs after the analytic and arithmetic filters

n	Number	n	Number
170	3	186	12
171	3	187	11
174	5	190	13
175	7	191	13
178	9	194	15
179	10	195	15
182	10	198	17
183	10	199	17

Lemma 3.2. The finite set defined by conditions (3.1)–(3.4) contains exactly 170 pairs. Its distribution with respect to n is the one shown in Table 1.

Proof. This follows from exact integer enumeration. The bounds, coprimality and parity tests, exact prime factorization of $m + n$, and the two base inequalities are implemented in Appendix B. The script also verifies the counts in Table 1. □

By Corollary 2.2, every exceptional solution attached to one of these 170 pairs must satisfy $y = 1$. Thus, it remains to eliminate

$$A^x + B = C^z. \tag{3.5}$$

4. Modular power-residue certificates

For an integer t and a modulus $q \ge 2$, define the positive power-residue set

$$R_q(t) = \{ t^k \bmod q : k \ge 1 \}. \tag{4.1}$$

Because the sequence of powers of t modulo q takes values in a finite set, $R_q(t)$ is finite and can be obtained by iteration until the first repeated residue.

For a residue set $R_q(A)$, we write $R_q(A) + B := \{ (r + B) \bmod q : r \in R_q(A) \}$.

Lemma 4.1. *Let A, B, and C be positive integers and $q \geq 2$. If $(R_q(A) + B) \cap R_q(C)$ is empty, then $A^x + B = C^z$ has no solution in positive integers x and z.*

Proof. Suppose that $A^x + B = C^z$ for some positive integers x and z. Reducing modulo q gives $A^x + B \equiv C^z \pmod q$. By definition, $A^x \bmod q$ belongs to $R_q(A)$ and $C^z \bmod q$ belongs to $R_q(C)$. Hence $C^z \bmod q$ belongs to $(R_q(A) + B) \cap R_q(C)$, contradicting the assumed disjointness. □

The important point is that Lemma 4.1 excludes all positive x and z at once. No upper bound for either exponent is required.

For the 170 residual pairs of Section 3, the following set of 13 moduli is sufficient:

$$Q = \{27, 88, 91, 109, 133, 136, 259, 275, 292, 315, 341, 451, 481\}. \tag{4.2}$$

Proposition 4.2. For every residual pair (m, n) of Lemma 3.2, there exists $q \in Q$ such that condition (4.3) holds.

$$(R_q(A) + B) \cap R_q(C) = \varnothing \ . \tag{4.3}$$

Proof. Appendix A records, for each of the 170 pairs, the first modulus in the ordered set Q that satisfies (4.3). Appendix B reproduces the residual set, verifies its distribution, and checks the disjointness condition using exact modular arithmetic. □

We give three elementary examples. For (m, n) = (2951, 170), reduction modulo 25 gives $A \equiv 1$, $B \equiv 15$, and $C \equiv 1$. Hence $A^x + B \equiv 16 \pmod{25}$, whereas $C^z \equiv 1 \pmod{25}$. For (m, n) = (2967, 170), reduction modulo 9 gives $A \equiv -1$, $B \equiv 6$, and $C \equiv 1$. Therefore $A^x + B$ is congruent to 5 or 7 modulo 9, while $C^z \equiv 1$. Finally, for (m, n) = (2999, 170), modulo 25 one has $A \equiv 1$, $B \equiv 10$, and $C \equiv 1$, so $A^x + B \equiv 11$ and $C^z \equiv 1$. These examples illustrate the same finite-residue mechanism used for the complete residual set.

5. Proof of the main theorem

We now combine the reductions above.

Proof. Let m and n satisfy the hypotheses of Theorem 1.1. If $n \leq 167$, the conclusion follows from Proposition 3.1. The value n = 168 is incompatible with $2 \mathbin{/\!/} mn$. We may therefore assume $169 \leq n \leq 200$.

If $m > 17.8n$, Lemma 2.4 applies. Hence we may assume $m \leq 17.8n$. If $A \leq 10^6$ or $B \leq 10^6$, Lemma 2.5 applies. Thus we may further assume $A > 10^6$ and $B > 10^6$.

If m + n has a prime divisor p not congruent to 1 modulo 16, the result follows from Lemma 2.3. After these cases are removed, Lemma 3.2 leaves exactly 170 pairs.

For every such pair, Corollary 2.2 forces y = 1 in any exceptional solution. Therefore only $Ax + B = Cz$ remains. Proposition 4.2 supplies a modulus q for which the shifted power-residue set and the power-residue set of C are disjoint. Lemma 4.1 excludes every exceptional solution. Therefore Equation (1.2) has only (x, y, z) = (2, 2, 2). □

6. Concluding remarks

We have proved Jeśmanowicz' conjecture under $2 \mathbin{/\!/} mn$ for $n \leq 200$. The proof is based on the interaction of several established results rather than on a new global bound for the exponential Diophantine equation. This is useful in a finite-parameter problem because the known criteria remove complementary regions of the parameter space.

The modular-certificate stage is stronger than a bounded search over x and z. Once y = 1 is known, a single modulus with disjoint power-residue sets excludes all positive exponents. The method is exact, elementary after the initial reductions, and straightforward to reproduce.

The same framework can be extended in two directions. First, improved ratio bounds or larger verified base ranges would immediately reduce the residual parameter set and permit larger values of n. Second, one may search for

parameter-dependent congruence families that replace individual finite certificates by infinite arithmetic subclasses. The latter direction would provide a more structural extension of the present theorem.

Appendix A. Modular assignments for the residual pairs

For each modulus q listed below, every displayed pair (m, n) satisfies condition (4.3). The notation n: {m_1, m_2, ...} is used for compactness. Each of the 170 residual pairs occurs exactly once in this appendix.

q = 27

170: {2967}; 171: {2998}; 174: {2915, 3043};
179: {2910, 2958, 3102}; 183: {2906, 3034, 3178}; 186: {2935, 2951, 3095};
190: {2643, 2931, 2979, 3027, 3123, 3171}; 195: {2638, 2926, 2942, 3086}; 198: {2699, 2971, 3131};
199: {2634, 2922, 3018, 3162, 3498}.

q = 88

171: {2950}; 174: {2963}; 178: {2911};
183: {2858}; 191: {2642, 2946, 3122, 3170}.

q = 91

178: {2959, 3039, 3135, 3151}; 179: {2862}; 183: {2954, 3130, 3146};
186: {2711, 2855, 3127}; 187: {2950, 3174}; 190: {2851, 3139};
191: {2898}; 194: {2943, 3023, 3167, 3423}; 195: {2606, 2846, 3022, 3166};
198: {2635, 2939, 3163}; 199: {2602, 2842, 2890, 2970, 3082, 3130}.

q = 109

198: {2843, 3419}.

q = 133

170: {2951, 2999}; 175: {2866, 2962, 3042, 3106}; 179: {2990, 3134};
182: {2859}; 186: {3031, 3175}; 187: {2710, 2934};
190: {2707}; 191: {2706}; 194: {2639, 2895, 3087, 3135};
195: {2894, 2974, 3134}; 198: {2603, 3083, 3115}; 199: {2554, 3114}.

q = 136

175: {2994}; 179: {3182}; 182: {2907, 2955, 3131, 3179};
187: {2854, 2902, 2982, 3030, 3126, 3142, 3270}; 190: {3091}; 191: {3026, 3138};
194: {2703, 2975}; 195: {3262}; 198: {2923};
199: {2938}.

q = 259

174: {2947, 2995}; 178: {3103}; 179: {2942};
182: {3035, 3099}; 183: {2938, 2986}; 186: {2903, 2983};
191: {2930, 2978, 3090, 3266}; 194: {2607, 2927}; 195: {3118}.

q = 275

175: {2946}; 178: {2943, 2991}; 179: {3150};
186: {3143}; 190: {2899, 3267}; 191: {2850};
194: {2847}; 198: {2555}; 199: {2698, 3258, 3418}.

q = 292

175: {2914}; 195: {2702, 3422}; 198: {3019}.

q = 315

182: {3147}; 183: {3098}; 190: {2947};

198: {3499}.

q = 341

171: {2966}; 178: {2863}; 194: {3119}.

q = 451

179: {3038}; 182: {2939, 2987}; 194: {3263};

198: {2891, 3259}.

q = 481

186: {3271}.

Apendix B. Exact verification script

The following pure-Python script reproduces the finite reduction, verifies the distribution in Table 1, and checks that the 13 moduli in (4.2) cover all 170 residual pairs. For each pair it stores the first valid modulus in the ordered list Q, matching the convention used in Appendix A. It uses no floating-point arithmetic. The script was tested with Python 3.13.5; the expected terminal output is 'verified residual pairs: 170'.

```
from math import gcd
from collections import Counter

Q = [27, 88, 91, 109, 133, 136, 259,
     275, 292, 315, 341, 451, 481]

EXPECTED = {170: 3, 171: 3, 174: 5, 175: 7,
            178: 9, 179: 10, 182: 10, 183: 10,
            186: 12, 187: 11, 190: 13, 191: 13,
            194: 15, 195: 15, 198: 17, 199: 17}

def primefactors(n):
    F = []
    d = 2
    while d*d <= n:
        if n % d == 0:
            F.append(d)
            while n % d == 0:
                n //= d
        d = 3 if d == 2 else d + 2
    if n > 1:
        F.append(n)
    return F

def powerresidues(a, q):
    seen = set()
    r = a % q
    while r not in seen:
        seen.add(r)
        r = (r*a) % q
    return seen

S = []
for n in range(169, 201):
    for m in range(n + 1, (89*n)//5 + 1):
        if gcd(m, n) != 1 or (m - n) % 2 == 0:
            continue
        if (m*n) % 4 != 2:
            continue
        A = m*m - n*n
        B = 2*m*n
        if A <= 10**6 or B <= 10**6:
```

```
            continue
        if any(p % 16 != 1 for p in primefactors(m + n)):
            continue
        S.append((m, n))

assert len(S) == 170
assert Counter(n for m, n in S) == Counter(EXPECTED)

certificate = {}
for m, n in S:
    A = m*m - n*n
    B = 2*m*n
    C = m*m + n*n
    for q in Q:
        RA = powerresidues(A, q)
        RC = powerresidues(C, q)
        shifted = {(r + B) % q for r in RA}
        if shifted.isdisjoint(RC):
            certificate[(m, n)] = q
            break
    assert (m, n) in certificate

assert len(certificate) == 170
print('verified residual pairs:', len(S))
```

Refrences

[1] L. Jeśmanowicz, Several remarks on Pythagorean numbers, Wiadom. Mat. 1 (1955/56), 196-202.

[2] T. Miyazaki, Generalizations of classical results on Jeśmanowicz' conjecture concerning Pythagorean triples, J. Number Theory 133 (2013), 583-595. https://doi.org/10.1016/j.jnt.2012.08.018.

[3] Y. Fujita and T. Miyazaki, Jeśmanowicz' conjecture with congruence relations, Colloq. Math. 128 (2012), 211-222. https://doi.org/10.4064/cm128-2-6.

[4] M.-M. Ma and Y.-G. Chen, Jeśmanowicz' conjecture on Pythagorean triples, Bull. Aust. Math. Soc. 96 (2017), 30-35. https://doi.org/10.1017/S0004972717000107.

[5] Q. Han and P. Yuan, A note on Jeśmanowicz' conjecture, Acta Math. Hungar. 156 (2018), 220-225. https://doi.org/10.1007/s10474-018-0837-4.

[6] M.-H. Le, R. Scott and R. Styer, A survey on the ternary purely exponential Diophantine equation $a^x + b^y = c^z$, Surv. Math. Appl. 14 (2019), 109-140.

[7] H. Yang and R. Fu, A further note on Jeśmanowicz' conjecture concerning primitive Pythagorean triples, Mediterr. J. Math. 19 (2022), Article 57. https://doi.org/10.1007/s00009-022-01990-y.

[8] R. Styer, At most one solution to $a^x + b^y = c^z$ for some ranges of a, b, c, Glas. Mat. Ser. III 59(79) (2024), 277–298. https://doi.org/10.3336/gm.59.2.02.

[9] M.-J. Deng and D.-M. Huang, A note on Jeśmanowicz' conjecture concerning primitive Pythagorean triples, Bull. Aust. Math. Soc. 95 (2017), 5-13. https://doi.org/10.1017/S0004972716000605.

[10] M.-J. Deng and J. Guo, A note on Jeśmanowicz' conjecture concerning primitive Pythagorean triples II, Acta Math. Hungar. 153 (2017), 436-448. https://doi.org/10.1007/s10474-017-0751-1.

[11] T. Miyazaki and N. Terai, On Jeśmanowicz' conjecture concerning primitive Pythagorean triples. II, Acta Math. Hungar. 147 (2015), 286–293. https://doi.org/10.1007/s10474-015-0552-3.