Bull. Math. Soc. Sci. Math. Roumanie
Tome 65 (113), No. 3, 2022, 359–365

Some exponential Diophantine equations attached to Pythagorean triples

by

Yasutsugu Fujita[(1)], Maohua Le[(2)], Nobuhiro Terai[(3)]

Abstract

Let p be an odd prime and t a positive integer. We show that if $(u,v) \in \{(2p^t,1),(p^t,2)\}$, then the equation $x^2+(2uv)^m=(u^2+v^2)^n$ has only the positive integer solutions $(x,m,n)=(u-v,1,1),(u^2-v^2,2,2)$.

Key Words: Exponential Diophantine equations, Pellian equations.
2010 Mathematics Subject Classification: Primary 11D61; Secondary 11D09.

1 Introduction

A triple (a,b,c) of positive integers is called a *Pythagorean triple* if it satisfies $a^2+b^2=c^2$. If a, b and c are pairwise relatively prime, this triple is called *primitive*. It is well known that any primitive Pythagorean triple (a,b,c) with b even can be parameterized as

$$a=u^2-v^2, \quad b=2uv, \quad c=u^2+v^2,$$

where u,v are positive integers with $u>v$, $\gcd(u,v)=1$ and $u \not\equiv v \pmod 2$. In 1956, Jeśmanowicz [9] conjectured that for any Pythagorean triple (a,b,c), the equation $a^x+b^y=c^z$ has only the positive integer solution $(x,y,z)=(2,2,2)$. Although there are a lot of results supporting it, this conjecture has not been settled yet, even in the case where (a,b,c) is a primitive Pythagorean triple. For relevant results, see, e.g., the survey paper [13] by Le-Scott-Styer.

As an analogue of Jeśmanowicz' conjecture concerning primitive Pythagorean triples, the third author [14] proposed the following:

Conjecture 1.1. *Let u and v be positive integers satisfying*

$$u>v, \ \gcd(u,v)=1 \ \textit{and} \ u \not\equiv v \pmod 2.$$

Then the equation

$$x^2+(u^2-v^2)^m=(u^2+v^2)^n$$

has only the positive integer solution $(x,m,n)=(2uv,2,2)$.

The third author [14] proved that if p and q are primes such that (i) $q^2+1=2p$ and (ii) $d=1$ or even when $q \equiv 1 \pmod 4$, then the equation $x^2+q^m=p^n$ has only the positive integer solution $(x,m,n)=(p-1,2,2)$, where d is the order of a prime divisor of (p) in the ideal class group of $\mathbb{Q}(\sqrt{-q})$. Conjecture 1.1 has been verified to be true in many special cases. However, Conjecture 1.1 remains unsolved (cf. Le [11], Cao-Dong [5] and Yuan-Wang [18]).

Recently, the first and the third authors [15] also conjectured the following:

Conjecture 1.2. ([15, Conjecture 1.2]) *Fix u and v as above.*
(I) *If $3u^2 - 8uv + 3v^2 \neq -1$, then the equation*

$$x^2 + (2uv)^m = (u^2 + v^2)^n \tag{1.1}$$

has only the positive integer solutions $(x, m, n) = (u - v, 1, 1), (u^2 - v^2, 2, 2)$, except for the case $(u, v) = (244, 231)$, where the equation

$$x^2 + 112728^m = 112897^n$$

has exactly the three positive integer solutions $(x, m, n) = (13, 1, 1), (6175, 2, 2), (2540161, 3, 3)$.
(II) *If $3u^2 - 8uv + 3v^2 = -1$, then equation (1.1) has exactly the three positive integer solutions $(x, m, n) = (u - v, 1, 1), (u^2 - v^2, 2, 2), ((u - v)(2u^2 + 2v^2 + 1), 1, 3)$.*

It is to be noted that by the results in Bugeaud [4] and Yuan-Hu [17], the equation

$$x^2 + D^m = p^n$$

has at most two positive integer solutions (x, m, n), where $D > 2$ is an integer and p is an odd prime not dividing D with $(D, p) \neq (4, 5)$. This implies that if $u^2 + v^2$ is a prime power, then Conjecture 1.2 holds. For more general equations of the form

$$x^2 + D^m = y^n$$

in integer unknowns x, y, m, n satisfying $x \geq 1, y > 1, m \geq 1, n \geq 3$ and $\gcd(x, y) = 1$, see, e.g., a couple of papers [2], [3] by Bérczes-Pink and the survey paper [12] by Le-Soydan.

In [15], the authors verified that Conjecture 1.2 holds in several cases. In particular, they showed the following:

Theorem 1.3. (cf. [15, Theorem 1.3 (i) and Corollary 1.4]) *Let p be an odd prime and t a positive integer. If either $(u, v) = (2p^t, 1)$ with $p \not\equiv 5 \pmod 8$ or $(u, v) = (p^t, 2)$ with $t \in \{1, 2\}$, then equation (1.1) has only the positive integer solutions $(x, m, n) = (u - v, 1, 1), (u^2 - v^2, 2, 2)$.*

Since it is obvious that $3u^2 - 8uv + 3v^2 = -1$ does not hold for $uv = 2p^t$, equation (1.1) has only the positive integer solutions $(x, m, n) = (u - v, 1, 1), (u^2 - v^2, 2, 2)$ under the assumptions in Theorem 1.3.

In this paper, we generalize Theorem 1.3 to prove the following:

Theorem 1.4. *Let p be an odd prime and t a positive integer. If $(u, v) \in \{(2p^t, 1), (p^t, 2)\}$, then equation (1.1) has only the positive integer solutions $(x, m, n) = (u - v, 1, 1), (u^2 - v^2, 2, 2)$.*

Theorem 1.4 implies that Conjecture 1.2 is true for $(u, v) \in \{(2p^t, 1), (p^t, 2)\}$.

2 Key lemmas

Lemma 2.1. *If $q = p^t$ for a prime p with $p \equiv 1 \pmod 4$ and a positive integer t, then the equation*

$$X^2 + q^m = (4q^2 + 1)^N \tag{2.1}$$

has no positive integer solution (X, m, N) with $m \equiv N \equiv 1 \pmod 2$.

Proof. Since N is odd, putting $Y = (4q^2+1)^{(N-1)/2}$ one can transform (2.1) into the Pellian equation

$$X^2 - (4q^2+1)Y^2 = -q^m. \tag{2.2}$$

If $m = 1$, then, since $4q^2 + 1 > q^2$, (2.2) has no solution by, e.g., [7, Lemma 2.3]. Since m is odd, we have $m \geq 3$. Hence,

$$(X, Y, m) = \left(\frac{2q^2 - q + 1}{2}, \frac{q-1}{2}, 3\right)$$

is the least solution of a class of solutions to (2.2) (which is defined as the solution (x', y', m') satisfying $x' > 0$, $y' > 0$, $m' > 0$ with m' minimal among the solutions in the class). Noting that $q = p^t$, we see from [10, Theorem 1] that (2.2) has only one class of solutions, and any primitive solution to (2.2) can be expressed as $m = 3m_0$ and

$$X + Y\sqrt{4q^2+1} = \left(\frac{2q^2 - q + 1}{2} \pm \frac{q-1}{2}\sqrt{4q^2+1}\right)^{m_0} \left(8q^2 + 1 + 4q\sqrt{4q^2+1}\right)^k \tag{2.3}$$

for a positive integer m_0 and a non-negative integer k, where

$$8q^2 + 1 + 4q\sqrt{4q^2+1} = \left(2q + \sqrt{4q^2+1}\right)^2$$

is the fundamental solution to the Pell equation

$$U^2 - (4q^2+1)V^2 = 1.$$

However, since $q = p^t \equiv 1 \pmod 4$ by assumption, we have $(q-1)/2 \equiv 0 \pmod 2$. It follows from (2.3) that Y must be even, which contradicts $Y = (4q^2+1)^{(N-1)/2}$. □

Lemma 2.2. *If $u = p^t$ for an odd prime p and a positive integer t, then the equation*

$$x^2 + 4u = (u^2+4)^n \tag{2.4}$$

has only the positive integer solution $(x, n) = (u-2, 1)$.

Proof. Considering (2.4) modulo 8, one easily sees that n is odd. Putting $Y = (u^2 + 4)^{(n-1)/2}$, we obtain the Pellian equation

$$x^2 - (u^2+4)Y^2 = -4u. \tag{2.5}$$

Since any solution to (2.4) corresponds to a solution (x, Y) with $\gcd(x, Y) = 1$ (i.e., a primitive solution (x, Y)) to (2.5), we may apply the argument described in [8, Section 11.5] to solve (2.4).

More precisely, first find an integer l with $0 \leq l \leq 2u$ satisfying

$$l^2 \equiv u^2 + 4 \pmod{4u}.$$

Since $u = p^t$, it is not difficult to see that $l \in \{u-2, u+2\}$. Then, put

$$\eta = \frac{l^2 - (u^2+4)}{-4u},$$

and consider the Pell equation

$$x_1^2 - (u^2+4)y_1^2 = \eta, \tag{2.6}$$

where $\eta = 1$ if $l = u-2$ and $\eta = -1$ if $l = u+2$. Since the continued fraction expansion of $\sqrt{u^2+4}$ is

$$\sqrt{u^2+4} = \left[u, \overline{(u-1)/2, 1, 1, (u-1)/2, 2u}\,\right]$$

and $u = p^t$ is odd, the fundamental solutions to (2.6) are

$$\left(\frac{u+\sqrt{u^2+4}}{2}\right)^6 \quad \text{if} \;\; \eta = 1 \quad \text{and} \quad \left(\frac{u+\sqrt{u^2+4}}{2}\right)^3 \quad \text{if} \;\; \eta = -1.$$

Therefore, any positive integer solution (x, Y) to (2.5) can be expressed as either

$$x + Y\sqrt{u^2+4} = \left\{\pm(u-2) + \sqrt{u^2+4}\right\}\left(\frac{u+\sqrt{u^2+4}}{2}\right)^{6k_1}$$

for a non-negative integer k_1 or

$$x + Y\sqrt{u^2+4} = \left\{(u+2) \pm \sqrt{u^2+4}\right\}\left(\frac{u+\sqrt{u^2+4}}{2}\right)^{3k_2}$$

for a positive odd integer k_2. Noting that

$$\begin{aligned}
\left\{(u+2) - \sqrt{u^2+4}\right\}\frac{u+\sqrt{u^2+4}}{2} &= u - 2 + \sqrt{u^2+4}, \\
\left\{(u+2) + \sqrt{u^2+4}\right\}\frac{u+\sqrt{u^2+4}}{2} &= u^2 + u + 2 + (u+1)\sqrt{u^2+4} \\
&= \left\{-(u-2) + \sqrt{u^2+4}\right\}\left(\frac{u+\sqrt{u^2+4}}{2}\right)^2,
\end{aligned}$$

we may express any solution to (2.5) as

$$x + Y\sqrt{u^2+4} = \left\{\pm(u-2) + \sqrt{u^2+4}\right\}\left(\frac{u+\sqrt{u^2+4}}{2}\right)^{2k} \tag{2.7}$$

for a non-negative integer k.

The rest of the proof will proceed along the same lines as the proof of [15, Proposition 3.2]. Indeed, from (2.7) we easily see that

$$x \equiv \pm(u-2) \pmod{(u^2+4)}. \tag{2.8}$$

Now, let $(x, n) = (x_1, n_1)$ be a solution to (2.4). Then, the Diophantine equation

$$x^2 + 4uy^2 = (u^2 + 4)^n \tag{2.9}$$

has the solution $(x, y, n) = (x_1, 1, n_1)$. By [10, Lemmas 2 and 6], there exists a unique integer l such that

$$x_1 \equiv \pm l \pmod{(u^2+4)}, \quad l^2 \equiv -4u \pmod{(u^2+4)}, \quad 0 < l < \frac{u^2+4}{2}. \tag{2.10}$$

It follows from (2.8) and (2.10) that $l = u-2$. Note that $(u-2)^2+4u = u^2+4$ and that the solution class S of (2.9) to which $(x_1, 1, n_1)$ belongs has a solution $(x, y, n) = (u-2, 1, 1)$, which is clearly the least solution of S. Thus, [10, Theorem 2] implies that $(x, n) = (x_1, n_1)$ is a solution to the equation

$$x + 2\sqrt{-u} = \lambda_1 \left(u - 2 + 2\lambda_2\sqrt{-u}\,\right)^n \tag{2.11}$$

with $\lambda_1, \lambda_2 \in \{\pm 1\}$. Let $\alpha = u - 2 + 2\sqrt{-u}$ and $\beta = u - 2 - 2\sqrt{-u}$. Then, it is obvious that $\alpha + \beta = 2(u-2)$ and $\alpha\beta = u^2 + 4$ are coprime, and that

$$\frac{\alpha}{\beta} = \frac{u^2 - 8u + 4 + 4(u-2)\sqrt{-u}}{u^2+4}$$

is not a root of unity in $\mathbb{Q}(\sqrt{-u}\,)$. Hence, (α, β) is a Lucas pair. Moreover, if we define $U_n(\alpha, \beta) = (\alpha^n - \beta^n)/(\alpha - \beta)$, then we have $U_{n_1}(\alpha, \beta) = \pm 1$, which implies that $U_{n_1}(\alpha, \beta)$ has no primitive divisor. Since n_1 is odd (see the beginning of the proof), we conclude from [1, Theorem 1.4] and [16, Theorem 1] that $n_1 \in \{1, 3\}$. If $n_1 = 1$, then $x_1 = u - 2$, which corresponds to the solution given in the assertion. If $n_1 = 3$, then we see from (2.11) that $3u^2 - 16u + 12 = \pm 1$ and hence $u = 1$, which contradicts $u = p^t$ with $t > 0$. This completes the proof of Lemma 2.2. □

Remark 2.3. In the proof of Lemma 2.2, since α and β are complex (not real), we applied the results in [1] and [16]. In case α and β are real, one can appeal to Carmichael's theorem [6, Theorem XXIII].

3 Proof of Theorem 1.4

Proof of Theorem 1.4. Consider first the case where $(u, v) = (2p^t, 1)$. In view of Corollary 1.4, Propositions 3.1, 4.2 and the proof of Theorem 1.3 (i) in [15], it only remains to prove that the equation $2^{2m-2} + q^m = (4q^2+1)^N$ has no positive integer solution (m, N) with $m \equiv N \equiv 1 \pmod 2$ in the case where $p \equiv 5 \pmod 8$, which is confirmed by Lemma 2.1.

Consider second the case where $(u, v) = (p^t, 2)$. By Proposition 4.1 and the proof of Theorem 1.3 (ii) in [15], it suffices to show that equation (2.4) has only the positive integer solution $(x, n) = (u-2, 1)$ in case $u = p^t$, which is exactly what Lemma 2.2 asserts. This completes the proof of Theorem 1.4. □

Acknowledgement *The authors thank the referee for reading the draft carefully and reminding us of Carmichael's paper [6]. The third author is supported by JSPS Grant No. 22K03271.*

References

[1] Y. Bilu, G. Hanrot, P. M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, with an appendix by M. Mignotte, *J. Reine Angew. Math.*, **539**, 75–122 (2001).

[2] A. Bérczes, I. Pink, On the Diophantine equation $x^2+p^{2k}=y^n$, *Arch. Math.*, **91**, 505–517 (2008).

[3] A. Bérczes, I. Pink, On the Diophantine equation $x^2+d^{2l+1}=y^n$, *Glasg. Math. J.*, **54**, 415–428 (2012).

[4] Y. Bugeaud, On some exponential diophantine equations, *Monatsh. Math.*, **132**, 93–97 (2001).

[5] Z.-F. Cao, X.-L. Dong, On Terai's conjecture, *Proc. Japan Acad.*, **74A**, 127–129 (1998).

[6] R. D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, *Ann. of Math. (2)*, **15**, 30–70 (1913).

[7] Y. Fujita, The non-extensibility of $D(4k)$-triples $\{1, 4k(k-1), 4k^2+1\}$ with $|k|$ prime, *Glas. Mat. Ser. III*, **41**, 205–216 (2006).

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

[9] L. Jeśmanowicz, Several remarks on Pythagorean numbers, *Wiadom. Math.*, **1**, 196–202 (1955/1956) (in Polish).

[10] M.-H. Le, Some exponential Diophantine equations I: the equation $D_1x^2-D_2y^2=\lambda k^z$, *J. Number Theory*, **55**, 209–221 (1995).

[11] M.-H. Le, On Terai's conjecture concerning Pythagorean numbers, *Acta Arith.*, **100**, 41–45 (2001).

[12] M.-H. Le, G. Soydan, A brief survey on the generalized Lebesgue-Ramanujan-Nagell equation, *Survey in Mathematics and its Applications*, **15**, 473–523 (2020).

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

[14] N. Terai, The Diophantine equation $x^2+q^m=p^n$, *Acta Arith.*, **63**, 351–358 (1993).

[15] N. Terai, Y. Fujita, On exponential Diophantine equations concerning Pythagorean triples, *Publ. Math. Debrecen*, **101**, 147–168 (2022).

[16] P. M. Voutier, Primitive divisors of Lucas and Lehmer sequences, *Math. Comp.*, **64**, 869–888 (1995).

[17] P.-Z. Yuan, Y.-Z. Hu, On the Diophantine equation $x^2 + D^m = p^n$, *J. Number Theory*, **111**, 144–153 (2005).

[18] P.-Z. Yuan, J.-B. Wang, On the Diophantine equation $x^2 + b^y = c^z$, *Acta Arith.*, **84**, 145–147 (1998).

Received: 01.11.2021
Revised: 12.01.2022
Accepted: 18.01.2022

(1) Department of Mathematics, College of Industrial Technology,
Nihon University, 2-11-1 Shin-ei, Narashino, Chiba, Japan
E-mail: `fujita.yasutsugu@nihon-u.ac.jp`

(2) Institute of Mathematics, Lingnan Normal College,
Zhanjiang, Guangdong, 524048 China
E-mail: `lemaohua2008@163.com`

(3) Division of Mathematical Sciences, Department of Integrated Science and Technology,
Faculty of Science and Technology, Oita University, 700 Dannoharu, Oita 870–1192, Japan
E-mail: `terai-nobuhiro@oita-u.ac.jp`