Solvability of Certain Exponential Lebesgue-Nagell Equations

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

Patcharee Wongsason[1], Panuwat Luangchaisri[2] and Sawian Jaidee[3*]

[1]Department of Mathematics Statistics and Computer, Faculty of Science, Ubon Ratchathani University, Ubon Ratchathani 34190, Thailand

[2,3]Department of Mathematics, Faculty of Science, Khon Kaen University,

Khon Kaen 40002, Thailand

*** Corresponding author, Email address: jsawia@kku.ac.th**

Abstract

In this article, we first investigate the exponential Lebesgue-Nagell equation of the shape in the title. Eventually, we can establish a necessary and sufficient criterion for having an integer solution of such an equation under the conditions that $p \equiv 3 \pmod 4$ and $n \equiv 1 \pmod 4$. The unique factorization in the ring of Gaussian integers, the existence of primitive divisors of the Lehmer sequences and also MAGMA program are crucially applied in this work.

Keywords: Exponential Lebesgue-Nagell equations, Gaussian integers, unique factorization, Lehmer sequences, primitive divisors

Introduction

Let C be a nonzero integer and n be an integer greater than 2. The Diophantine equation

$$x^2 + C = y^n \tag{1}$$

is the so-called *generalized Ramanujan-Nagell equation*. There is a very broad literature on studying of such an equation which always has a finitely many positive integer solutions

(Landua & Ostrowski, 1920). The exploration about finding an integer solution of this equation can be studied more in (Bureaud, Mignotte & Siksek, 2006; Cohn, 1993), and these contain early results taken into account when C is a fixed integer. Many authors have been interested over the year in case $C = p^m$ when p is a fixed prime number (Arif & Muriefah, 1997; Arif & Muriefah, 1998; Arif & Muriefah, 1999; Arif & Muriefah, 2006) or even a general prime number (Arif & Muriefah, 2002; B$\acute{e}$rczes & Pink, 2008; Le, 2003; Lin Zhu, 2011; Xiaowei, 2013). More generally, the case C consisting of a product of prime powers p^m, where p belongs to some fixed finite set of primes has recently been investigated by several mathematicians (Luca, 2002; Luca & Togbc$\acute{e}$, 2008; Luca & Togb$\acute{e}$, 2009; Pink, 2007; Pink & R$\acute{a}$bai, 2011; Soydan & Tzanakis, 2016; Lin Zhu, Le & Soydan, 2015).

Our interest in this paper goes to the equation (1) in the case $C = p^m$ when p is a prime number and m is a natural number. This certain equation is known as *the exponential Lebesgue-Nagell equation*. Now, we will divide our discussion about some results concerning our considered equation into 2 cases as m being odd or even:

Case A: Let $m = 2k + 1$, where k is a positive integer, p be odd such that $p \not\equiv 7 \pmod 8$, and $n > 3$ be an odd integer with $\gcd(n, h) = 1$, where h is the class number of the number field $\mathbb{Q}(\sqrt{-p})$. Arif and Abu Muriefah illustrated in (Arif & Muriefah, 1998) that the equation $x^2 + 3^m = y^n$ has the unique positive integral solution given by $n = 3,\ m = 5 + 6N,\ x = 10 \times 3^{3N},\ y = 7 \times 3^{2N}$ when N is the one-third of the highest power of 3 which divides x. In 2002, they also proved that the equation $x^2 + p^{2k+1} = y^n$, where $\gcd(p, x) = 1$ and $n \geq 5$ is not a multiple of 3 has exactly two families of solutions given by

$$p = 19, n = 5, k = 5M, x = 22434 \times 19^{5M}, y = 55 \times 19^{2M} \text{ and}$$

$$p = 341, n = 5, k = 5M, x = 2759646 \times 341^{5M}, y = 377 \times 19^{2M}$$

when M is the one - fifth of the highest power of p which divides x. This work can be found in (Arif & Muriefah, 2002). In addition, all integer solutions to the equation $x^2 + q^m = y^3$ can be exactly one solution $(q, k, x, y) = (11, 1, 9324, 443)$ due to (Lin Zhu, 2011).

Case B: Let $m = 2k$, where k is a positive integer. Bérczes and Pink showed in (Bérczes & Pink, 2008) that all integer solutions to the equation $x^2 + p^{2k} = y^n$ are

$$(x, y, p, n, k) = (11,5,2,3,1), (46,13,3,3,2), (524,65,7,3,1), (2,5,11,3,1),$$

$$(278, 5, 29, 7, 1), (38, 5, 41, 5, 1), (52, 17, 47, 3, 1), (1405096, 12545, 97, 3, 1),$$

where i) x, y, n, k are unknown integers satisfying $x \geq 5\ y > 1$, $n \geq 3$ is a prime and $k \geq 0$ with $\gcd(x, y) = 1$, and ii) $2 < p < 100$. Observe that the equation $x^2 + p^2 = y^n$ has no integer solution (x, y, p, n) when n is a prime with $p \equiv 3 \pmod 4$ and $n \equiv 1 \pmod 4$ such that $2 < p < 100$.

Being motivated by the works of Bérczes and Pink as mentioned above in the particular case $k = 1$ leads us to assert that the equation $x^2 + p^2 = y^n$ would have no any integer solution when $p \equiv 3 \pmod 4$ and $n \equiv 1 \pmod 4$. Eventually, it turns out that we are able to obtain the following main result.

Theorem 1 Let p and n be a prime number and a natural number greater than 1 satisfying $p \equiv 3 \pmod 4$ and $n \equiv 1 \pmod 4$, respectively. Then the Diophantine equation $x^2 + p^2 = y^n$ has an integer solution (x, y) if and only if

$$-p = \sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k} (-1)^{n-k-1} b^{2k} \qquad (2)$$

for some even positive integer b such that $b^2 < \left[\frac{\binom{n}{n-3}}{\binom{n}{n-1}}\right]$.

The important tools used to prove this main result are the unique factorization in the ring of Gaussian integers, the existence of primitive divisors of the Lehmer sequences and

MAGMA program at some points. Indeed, we have explicitly illustrated in (Jaidee & Saosoong, 2022) that the equation $x^2 + p^2 = y^5$ has no integer solution for any prime p with $p \equiv 3 \pmod 4$ without applying the second tool.

Preliminaries

In order to complete our main result, let us first give the necessary and sufficient condition for having an integer solution of the Fermat-type equation with signatures $(2,2,n)$ as follows:

Theorem 2 Let n be an integer greater than 1. Then the equation $x^2 + p^2 = y^n$ with $\gcd(x, y) = 1$ has an integer solution if and only if the equation

$$x + yi = u(a + bi)^n \tag{3}$$

has an integer solution (x, y, a, b) for some $u \in \{\pm i, \pm 1\}$.

To prove Theorem 2, we need Lemma 1 and Lemma 2 below. The first lemma is easily proven by applying the unique factorization in the ring of Gaussian integers. In fact, this lemma is true for any unique factorization domain and also for its advanced analogue in the unique prime ideal factorization appearing in the book written by (Alaca & Kenneth, 2004).

Lemma 1 Let n be any natural number and α, β and γ be nonzero and nonunit Gaussian integers such that β and γ are coprime. If $\alpha^n = \beta\,\gamma$, then there exist $\beta_1,$ γ_1 and unit elements u, v in Gaussian integers for which $\beta = u\beta_1$ and $\gamma = v\gamma_1$ where β_1 and γ_1 are coprime.

Lemma 2 Let n be a natural number greater than 2. If the equation $x^2 + p^2 = y^n$ has an integer solution (x, y) with $\gcd(x, y) = 1$, then $x + yi$ and $x - yi$ are coprime.

The proof of Lemma 2 may be found in (Andreescu, Andrica & Cucurezeanu, 2010). Instead of being arbitrary integer y in the necessary condition stated in Theorem 2, we can choose y

as a fixed prime p such that $p \equiv 3 \pmod 4$ in order to apply Theorem 2 specifically as illustrated in the following lemma. Its proof may be seen in (Jaidee & Wannalookkhee, 2020).

Lemma 3 Let n be a natural number greater than 2, and p be a prime number such that $p \equiv 3 \pmod 4$. If the equation $x^2 + p^2 = y^n$ has an integer solution (x, y), then $\gcd(x, p) = 1$.

Let α and β be algebraic integers for which $(\alpha+\beta)^2$ and $\alpha\beta$ are nonzero coprime rational integers, and $\frac{\alpha}{\beta}$ is not a root of unity. For each natural number n, we call

$$\tilde{u}_n = \tilde{u}_n(\alpha, \beta) = \begin{cases} \dfrac{(\alpha^n - \beta^n)}{\alpha - \beta} & \text{if } n \text{ is odd,} \\ \dfrac{(\alpha^n - \beta^n)}{\alpha^2 - \beta^2} & \text{if } n \text{ is even} \end{cases}$$

the Lehmer sequences. A rational prime p is a primitive divisor of $\tilde{u}_n$ if p divides $\tilde{u}_n$ but does not divide $(\alpha^n - \beta^n)^2 \tilde{u}_1 \cdots \tilde{u}_{n-1}$. For instance, if $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$, then the term $\tilde{u}_n$ is the Fibonacci number F_n for any natural number n. These numbers are formed to be the Fibonacci sequence listed as A00045 in the On-Line Encyclopedia of Integer Sequences (OEIS) (Sloane, 2022) begins with

$$F_0 = 0, F_1 = 1, F_2 = 1, F_3 = 2,\ F_4 = 3, F_5 = 5, F_6 = 8, F_7 = 13, F_8 = 21, F_9 = 34, \ldots.$$

Clearly, F_1, F_2, F_5 and F_6 have no primitive divisors, but F_3, F_4, F_7, F_8 and F_9 have a primitive divisor. The following two theorems taken from (Bureaud, Mignotte, & Siksek, 2006) will play an important key in the next section.

Theorem 3 For every integer $n > 30$, $\tilde{u}_n(\alpha, \beta)$ has a primitive divisor.

Theorem 4 Let n satisfy $6 < n \leq 30$ and $n \neq 8, 10, 12$. Then all $\tilde{u}_n(\alpha, \beta)$ having no primitive divisors are of the form

$$(\alpha, \beta) = \left(\frac{\sqrt{a} - \sqrt{b}}{2}, \frac{\sqrt{a} + \sqrt{b}}{2}\right),$$

where (a, b, n) are given as follows:

$(7,1,-7), (7,1,-19), (7,3,-5), (7,5,-7), (7,13,-3), (7,14,-22), (9,5,-3), (9,7,-1), (9,7,-5),$

$(13,1,-7), (14,3,-13), (14,5,-3), (14,7,-1), (14,7,-5), (14,19,-1), (14,22,-14), (15,7,-1),$

$(15,10,-2), (18,1,-7), (18,3,-5), (18,5,-7), (24,3,-5), (24,5,-3), (26,7,-1), (30,1,-7),$

$(30,2,10)$.

The proof of Theorem 1

Before showing the proof of Theorem 1, the following facts will be needed.

Theorem 5 There have no natural numbers $a > 1$ and b such that $a \not\equiv b \pmod{2}$ and $\gcd(a, b) = 1$ satisfying the equation

$$1 = \sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k} (a)^{n-2k-1} (-b^2)^k \tag{4}$$

for any natural number $n > 1$ with $n \equiv 1 \pmod{4}$.

Proof. Suppose that there exist natural numbers $a > 1$, b and n such that $a \not\equiv b \pmod{2}$ with $\gcd(a, b) = 1$, and $n \equiv 1 \pmod{4}$ satisfying the equation (4). Let $\alpha = a + bi$ and $\beta = a - bi$. Following the binomial theorem and the equation (4), we eventually obtain that

$$\alpha^n + \beta^n = 2a = \alpha + \beta.$$

Then we may write

$$\alpha^n + \beta^n = (\alpha + \beta) \left(\frac{\alpha^{2n} - \beta^{2n}}{\alpha^2 - \beta^2} \right) \left(\frac{\alpha - \beta}{\alpha^n - \beta^n} \right).$$

Consequently,

$$\left(\frac{\alpha^{2n} - \beta^{2n}}{\alpha^2 - \beta^2} \right) = \left(\frac{\alpha^n - \beta^n}{\alpha - \beta} \right) \tag{5}$$

Since α and β are roots of the polynomial equation $X^2 - 2aX + (a^2 + b^2) = 0$, we have α and β are algebraic integers. Obviously, $(\alpha + \beta)^2$and $\alpha\beta$ are coprime. We claim that $\frac{\alpha}{\beta}$ is not a root of unity. Suppose that it is a root of unity, that is, $(\frac{\alpha}{\beta})^m = 1$ for some natural number m. Then, it is a root of the polynomial equation $X^m - 1 = 0$. Since we know that

$$X^m - 1 = \prod_{d|m} \varphi_d(X),$$

there exists a natural number d_0 such that $\varphi_{d_0}(\alpha/\beta) = 0$. Note that $\varphi_d(X)$ is the d^{th} cyclotomic polynomial. One can check that $\frac{\alpha}{\beta}$ is a zero of the polynomial

$$p(X) = X^2 - \frac{2(a^2-b^2)}{\alpha\beta}X + 1.$$

This implies that the polynomial $\varphi_{d_0}(X)$ must divide $p(X)$ as $\varphi_{d_0}(X)$ is always monic and irreducible. Indeed, $p(X)$ can not be divided by all possibilities of $\varphi_{d_0}(X)$, a contradiction. Hence $\frac{\alpha}{\beta}$ is not a root of unity. Now, we are able to define $\tilde{u}_n(\alpha, \beta)$ as the Lehmer sequence. From (5), we deduce that the Lehmer sequence $\tilde{u}_{2n}(\alpha, \beta)$ has no primitive divisors for any natural number n. Applying Theorem 3 and Theorem 4 together with the condition $n \equiv 1 \pmod 4$, we eventually yield that $\tilde{u}_{2n}(\alpha, \beta)$ has a primitive divisor for all natural number n excluding $n = 5$. This leads to a contradiction. It remains to focus on the case $n = 5$ only. By (4), we have $a^4 - 10a^2b^2 + 5b^4 = 1$. By applying the ThueSolve function in **MAGMA** (Bosma, Cannon, & Playoust, 1997), we know that $(x, y) = (\pm 1, 0)$ are only integer solutions of the Thue equation $x^4 - 10x^2y^2 + 5y^4 = 1$. Again, we have a contradiction. Hence we complete the proof of the theorem.

Lemma 4 Let n be a natural number greater than 1 with $n \equiv 1 \pmod 4$. Then

$$\sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k} (-1)^{n-k-1} b^{2k} \geq 0 \qquad (6)$$

for any even positive integer b such that $b^2 \geq \left\lceil \frac{\binom{n}{n-3}}{\binom{n}{n-1}} \right\rceil$.

Proof. Let b be an even positive integer such that $b^2 \geq \left\lceil \frac{\binom{n}{n-3}}{\binom{n}{n-1}} \right\rceil$. Rearranging the summation in (6), we obtain that

$$1 + \binom{n}{4} b^4 + \binom{n}{8} b^8 + \cdots + nb^{n-1} - \left[\binom{n}{2} b^2 + \binom{n}{6} b^6 + \cdots + \binom{n}{n-3} b^{n-3} \right]$$

$$> \binom{n}{4} b^2 \left(b^2 - \left\lceil \frac{\binom{n}{2}}{\binom{n}{4}} \right\rceil \right) + \binom{n}{8} b^6 \left(b^2 - \left\lceil \frac{\binom{n}{6}}{\binom{n}{8}} \right\rceil \right) + \cdots + nb^{n-3} \left(b^2 - \left\lceil \frac{\binom{n}{n-3}}{\binom{n}{n-1}} \right\rceil \right) \geq 0$$

Now, we are ready to prove Theorem 1.

Proof. Let p and n be a prime number and a natural number greater than 1 satisfying $p \equiv 3 \pmod 4$ and $n \equiv 1 \pmod 4$, respectively. For the necessary condition, let us assume that the equation $x^2 + p^2 = y^n$ has an integral solution (x, y), and suppose that the equation (2) is not true for all even positive integers b such that $b^2 < \left\lceil \frac{\binom{n}{n-3}}{\binom{n}{n-1}} \right\rceil$. Applying Lemma 3 and Theorem 2 together with the fact that $u = u^n$ for any $u \in \{\pm i, \pm 1\}$, we eventually obtain that $p + xi = (a + bi)^n$ for some $a, b \in \mathbb{Z}$. Observe that $p - xi = (a - bi)^n$ and recall that $\gcd(x, p) = 1$ and y is odd. Then we have

$$y^n = x^2 + p^2 = (p + xi)(p - xi) = (a^2 + b^2)^n,$$

which implies that $y = a^2 + b^2$. If $a \equiv b \pmod 2$, then we have that y is even, which is a contradiction. So, a and b have an opposite parity. Now, we consider

$$p + xi = \left(\sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k} (-1)^k a^{n-2k} b^{2k} \right) + \left(\sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k+1} (-1)^k a^{n-1-2k} b^{2k+1} \right) i.$$

Then, we have

$$p = a\sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k} (-1)^k a^{n-2k-1} b^{2k},$$

which implies that $a = \pm 1$ or $a = \pm p$. If $a = 1$, then b must be even. Since $n \equiv 1 \pmod 4$, it follows that

$$p = 1 - \binom{n}{2} b^2 + \binom{n}{4} b^4 - \cdots + nb^{n-1} \equiv 1 (\mathrm{mod}\ 4),$$

which is a contradiction. If $a = -1$, then we have that

$$-p = \sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k} (-1)^{n-k-1} b^{2k},$$

which is impossible by referring Lemma 4 together with the assumption. If $a = -p$, then b must be even. As $n \equiv 1 \pmod 4$ and $\gcd(4, p) = 1$, we eventually obtain that

$$-1 = p^{n-1} - \binom{n}{2} p^{n-3} b^2 + \binom{n}{4} p^{n-5} b^4 - \cdots + nb^{n-1} \equiv 1 (\mathrm{mod}\ 4),$$

which is a contradiction. Applying Theorem 5 to the other case leads us to get a contradiction as well. For the sufficient condition, suppose that there exists an even positive integer b_0 for which $b_0{}^2 < \left|\left[\frac{\binom{n}{n-3}}{\binom{n}{n-1}}\right]\right|$ and

$$p = -\sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k} (-1)^{n-k-1} a^{n-2k} b_0{}^{2k}.\blacksquare$$

Then we choose

$$x_0 = -\sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k+1} (-1)^{n-k-1} b_0{}^{2k+1}.\blacksquare$$

It is not hard to see that $(p, x_0, -1, b_0)$ satisfies the equation (3) in Theorem 2 for some $u \in \{\pm i, \ \pm 1\}$. Hence we complete the proof.

Concluding discussion

According to the Table 1 and Table 2 below together with applying Theorem 1, we conclude that for any prime p with $p \equiv 3 \pmod 4$ and a natural number $1 < n \leq 49$ with $n \equiv 1 \pmod 4$, the Diophantine equation $x^2 + p^2 = y^n$ has no integer solution (x, y). For each fixed natural number $1 < n \leq 49$ with $n \equiv 1 \pmod 4$, this result generalizes the works of Bérczes and Pink mentioned in the case B for only the particular case $k = 1$ and $p \equiv 3 \pmod 4$. There are infinitely many primes of the form $4k + 3$, listed as A002145 in the On-Line Encyclopedia of Integer Sequences (OEIS) (Sloane, 2022). We, moreover, conjecture that our considered equation has no integer solution for any natural number $n > 1$ with $n \equiv 1 \pmod 4$ and for any prime p with $p \equiv 3 \pmod 4$.

Acknowledgements

The authors specially thank the anonymous referees for her/his careful reading and valuable suggestions. This research was supported by Department of Mathematics, Faculty of Science, Khon Kaen University, fiscal year 2022.

References

Alaca, S., & Williams, S. K. (2004). *Introductory Algebraic Number Theory*. Cambridge, England: Cambridge University Press.

Andreecu, T., Andrica, D., & Cucurezeanu, I. (2010). *An Introduction to Diophantine Equations (A Problem-Based Approach)*. London, England: Springer.

Arif, S. A., & Muriefah, F. S. (1997). On the Diophantine equation $x^2 + 2^k = y^n$. *International Journal of Mathematics and Mathematical Science*, *38*, 299-304.

Arif, S. A., & Muriefah, F. S. (1998). On the Diophantine equation $x^2 + 3^k = y^n$. *International Journal of Mathematics and Mathematical Science*, *38*, 619-620.

Arif, S. A., & Muriefah, F. S. (1999). On the Diophantine equation $x^2 + 5^{2k+1} = y^n$. *Indian Journal of Pure and Applied Mathematics*, *30*, 229-231.

Arif, S. A., & Muriefah, F. S. (2002). On the Diophantine equation $x^2 + q^{2k+1} = y^n$. *Journal of Number Theory*, *95*, 95-100.

Arif, S. A., & Muriefah, F. S. (2006). On the Diophantine equation $x^2 + 5^k = y^n$. *Demonstratio Mathematica*, *30*, 285-289.

Bérczes, A., & Pink, I. (2008). On the Diophantine equation $x^2 + p^{2k} = y^n$. *Archiv der Mathematik, 91*, 505-517.

Bilu, Y., Hanrot, G., & Voutier, P. M. (2001). Existence of primitive divisor of Lucas number and Lehmer number, with an appendix by M. Mignotte. *Journal für die Reine und Angewandte Mathematik*, *539,* 75-122.

Bosma, W., Cannon, J., & Playoust, C. (1997). The Magma algebra system. I. The user Language. *Journal of Symbolic Computation*, *24*(3-4), 235-265.

Bureaud, Y., Mignotte, M., & Siksek, S. (2006). Classical and modular approaches to exponential Diophantine equation II. The Lebesgue-Nagell equation, *Compositio Mathematica*, *19*, 31-62.

Cohn, J. H. E. (1993). On the Diophantine equation $x^2 + C = y^n$. *Acta Arithmetica,* 64, 367-381.

Jaidee, S., & Wannalookkhee, F. (2020). Solvability of the Diophantine Equation $x^2 + p^2 = y^n$ when p is a Prime. KKU Science Journal, 48(2), 175-182.

Jaidee, S., & Soasoong, K. (2022). The Fermat-type equation with signature (2, 2, n) and

Bunyakovsky conjecture, *Songklanakarin Journal of Science and Technology*.(accepted)

Jones, G. A., & Mary Jones, J. (1998). *Elementary Number Theory*. London: England, Springer.

Landua E., & Ostrowski, A. (1920). On the Diophantine equation $ay^2 + b^y + c = dx^n$. *Proceedings of the London Mathematical Society*, *19*, 76-280.

Le M. (2003). On the Diophantine equation $x^2 + p^2 = y^n$. *Publicationes Mathematicae Debrecen*, *63*, 2003, 67-78.

Lin Zhu, H. (2011). A note on the Diophantine equation $x^2 + q^m = y^3$. *Acta Arithmetica*, *146*, 195-202.

Luca, F.(2002). On the Diophantine equation $x^2 + 2^a 3^b = y^n$. *International Journal of Mathematics and Mathematical Sciences*, 29, 239-244.

Luca, F., & Togb$\acute{e}$, A.(2008). On the Diophantine equation $x^2 + 2^a 5^b = y^n$. *International Journal of Number Theory*, *6* , 973-979.

Luca, F., & Togb$\acute{e}$, A.(2009). On the Diophantine equation $x^2 + 2^a 13^b = y^n$. *Colloquium Mathematicum*, *116* , 139-146.

Pink, I. (2007). On the Diophantine equations $x^2 + 2^a 3^b 5^c 7^d = y^n$. *Publicationes Mathematicae Debrecen*, *70*, 149-166.

Pink, I., & R$\acute{a}$bai, Z. (2011). On the Diophantine equations $x^2 + 5^k 17^l = y^n$. *Communications in Mathematics*, *19*, 1-9.

Sloane, N. J. A. (2022). The On-Line Encyclopedia of Integer Sequences. Available at https://oeis.org.

Soydan, G., & Tzanakis, N. (2016). Complete solution of the Diophantine equation $x^2 + 5^a 11^b = y^n$. *Bulletin of the Hellenic Mathematical Society, 60*, 125-151.

Xiaowei, P. (2013). On the Diophantine equation $x^2 + p^{2m} = y^n$. *Periodica*

Mathematica Hungarica, *67*, 231-242.

Zhu H., Le, M., & Soydan, G. (2015). On the exponential Diophantine equation $x^2 + 2^a p^b = y^n$. *Periodica Mathematica Hungarica, 70*, 233-247.

Table

n	*b*	Values of the sum in (2)	Remark
5	all even	≥40	positive
9	2	-1199	composite
13	2	-8839	prime ≡ 1 (mod 4)
	4	-4291039	composite
17	2	873121	positive
	4	-24553864319	composite
	6	7005476875681	positive
21	2	-6699319	composite
	4	-7547952442399	composite
	6	-9382001116577399	composite
25	2	-451910159	composite
	4	-379677384665279	composite
	6	-33413277960843515279	composite
	8	1500111128083892163841	composite
29	2	10513816601	positive
	4	508156418079387041	positive
	6	-54656126356697865345959	composite
	8	-86830731409525073357567359	composite
	10	28714774144970063639717469401	positive
33	2	135250416961	positive
	4	195337401466191394561	positive
	6	-55544682746808341439157439	composite
	8	-671582932652885722310459458559	composite
	10	-173156776127815926903091558852799	composite
	12	178179625643608687570320730917646081	positive
37	2	-8464641213079	composite
	4	20456911077705143997281	positive
	6	-17653223669804406176810517719	composite
	8	-3437192033013175861274046101509759	composite
	10	-6243764616905212012976446882123616599	composite
	12	631477325821592776208040048198094984801	positive
	14	135174135846655757423281431224261441223268	positive

Table 1. The values of the sum in (2)

n	***b***	**Values of the sum in (2)**	**Remark**
41	2	33973466382481	positive
	4	-9727649740836715098004799	composite
	6	65933408587323941845688405725201	positive
	8	-13536412949968925749002920977371720959	composite
	10	-99376498767324043660260758523750875381999	composite
	12	-53665717085918221112725250796920790368950079	composite
	14	23525696254572342402118496445124787158685773201	positive
	16	13932512484569015094869100053411051281882786483201	positive
45	2	4814772228819641	positive
	4	-4840884886670433593354451679	composite
	6	175633012692018657955115709876643321	positive
	8	-39165376532163420253440671987199758092159	composite
	10	-1218748280038458927839876515654580684070148999	composite
	12	-2412142537849669341564627051505411745844937390559	composite
	14	-283668767912640307359465836370366577155604220340679	composite
	16	546467594673009682304230256786294510968059831519224321	positive
49	2	-88640227692525599	composite
	4	-746301899503456335359674623359	composite
	6	2561487504687167123255029365909544286	positive
	8	-49208654712806503603755163905249327148623359	composite
	10	-1257374684957935908101711595079174190553509735759959	composite
	12	-72150053530469629308059274221073511792264518509408639	composite
	14	-565611735929982524628863778424017901863350099446791009	composite
	16	9168771727839287761217425376646039689426830969756505303041	positive
	18	14244515680539506494265991915655837682633397745431493110682081	positive

Table 2 The values of the sum in (2)

Dear the reviewer 2

The corrected statements are shown below:

Suggestions or comments	Corrected statements
Line 42 The authors should state clearly what the 'N' is.	I have stated already.
Line 45 The authors should state clearly what the 'M' is.	I have stated already.
Line 54 'integer unknowns' should be 'unknown integers'.	I have changed already
Line 58 'Motivated' should be 'Being motivated'.	I have added it more already
Line 60 'we enable' should be 'we are able'.	I have changed already
Line 66 'can happen for some ...' should be 'for some...'.	I have changed already
Line 83 'advance' should be 'advanced'.	I have added it more already
Line 127 The authors write 'Observe that $\alpha^n + \beta^n = 2a = \alpha + \beta$'. I think it needs more explanation (or proof) why it follows from the existence of a > 1, b, and n	*I have put more explanation without proving* because the proof is directly and this fact can be true for every positive integers a,b,n. Note that the conditions of a,b,n will be used in the other part later.
Line 132 Since α = a + bi and β = a − bi with a, b ∈ Z, α and β are algebraic integers. The authors might not need to use the fact that there are roots of the mentioned monic polynomial.	I do agree with you that α = a + bi and β = a – bi are clearly algebraic integers as a and b are integers if we employ the fact that the ring of integers in Q(i) is Z(i)=Z+Zi. However, in order to clarify it, *I would like to keep the current explanation.*
Line 133 The authors prove that α /β is not a root of unity. Note that α, β, α /β ∈ Q[i] and the set of roots of unity in Q[i] is {1, −1, i, −i}. It should be easier to consider directly the equation α β = j, where j ∈ {1, −1, i, −i}. Since a > 1, a ≢ b (mod 2), and gcd(a, b) = 1, we have α β ≠ j, for each such j. We can use the fact that a ≠ 0 ≠ b if need be	I cannot prove that the set of roots of unity in Q[i] is {1, −1, i, −i} right now and also I haven't found its relevant reference yet. So, *I would like to keep the current proof.* Note that if we apply that the suggested fact above, the conditions of natural numbers $a > 1,\ b$ such that $a \not\equiv b \pmod{2}$ with $\gcd(a, b) = 1$ will be used. Indeed, these conditions have been applied to show that $(\alpha + \beta)^2$ and $\alpha\beta$ are coprime appearing in the Line132
Line 141 'Hence α /β is a root of unity.' should be 'Hence α β is not a root of unity.'	I have added more already
Line 146 'we get...' should be 'we obtain...' or 'we have...'.	I have changed already
Line 148 Should it be x 4 − 10x 2y 2 + 5y 4 = 1?	I have added more already
Line 148 'we get a contradiction.' should be 'we have a contradiction.'.	I have changed already
Line 161 'for all even positive integer b' should be 'for all even positive integers b'.	I have added more already
Line 166 'we get y is even' should be 'we have that y is even'.	I have changed already
Line 174 'we get that' should be 'we have that'.	I have changed already
Lines 182 and 183 There should be periods '.' after the equations.	I have added more already
Line194 'There are infinitely many primes in the form' should be 'There are infinitely many primes of the form	I have changed already
Line195 'We moreover...' should be 'We, moreover,...'	I have added more already

In case such corrected statements are not completed yet, please feel free to let me know.

Note that the words or sentences made as the green highlight are rewritten by the author.

Best wishes,

Sawian Jaidee

The corresponding author