On the Diophantine equation $3^x + p^y = z^2$ where $p \equiv 2 \pmod 3$

WIPAWEE TANGJAI, CHUSAK CHUBTHAISONG

Department of Mathematics,
Faculty of Science Mahasarakham University Mahasarakham, 44150, THAILAND

Abstract: Let p be a prime number where $p \equiv 2 \pmod 3$. In this work, we give a non-negative integer solution for the Diophantine equation $3^x + p^y = z^2$. If $y = 0$, then $(p, x, y, z) = (p, 1, 0, 2)$ is the only solution of the equation for each prime number p. If y is not divisible by 4, then the equation has a unique solution $(p, x, y, z) = (2, 0, 3, 3)$. In case that y is a positive integer that is not divisible by 4, we give a necessary condition for an existence of a solution and give a computational result for $p < 10^{17}$. We also give a necessary condition for an existence of a solution for $q^x + p^y = z^2$ when p and q are distinct prime numbers.

Key-Words: - Diophanetine eqauation, prime number, congruence

Received: March 1, 2021. Revised: May 13, 2021. Accepted: May 28, 2021. Published: June 17, 2021.

1 Introduction

The Diophantine equation in the form

$$a^x + b^y = z^c \tag{1}$$

has been studied in [1, 2]. Cao [3] showed that if $\max\{a, b, z\} > 13$, then (1) has at most one positive solution with $c > 1$ and computed the complete solution in some cases [4]. An important result that is a basis in establishing a solution for (1) is the Catalan's conjecture proved by Mihailescue in 2004.

Theorem 1. *[5] (Catalan's conjecture) The unique solution for Diophantine equation $a^x - b^y = 1$ where $\min\{a, b, x, y\} > 1$ is $(a, b, x, y) = (3, 2, 2, 3)$.*

A solution in some cases when $c = 2$ can be found in [6, 7, 8, 9, 10]. In 2017, Burshtein [11, 12] showed that

$$a^x + b^y = z^2 \tag{2}$$

has infinite number of solutions.

Theorem 2. *[11] Let p be a prime number that is greater than 3 and a be an odd number. The Diophantine equation $a^x + p = z^2$ has infinitely many solutions*

$$(a, p, x, z) = (a, 2 \cdot a^n + 1, 2n, a^n + 1) .$$

where n is a positive integer.

Theorem 3. *[12] The Diophantine equation $2^x + b = z^2$ has infinitely many solutions*

$$(b, x, z) = (2 \cdot 2^n + 1, 2n, 2^n + 1)$$

where n is a positive integer.

Theorem 4. *[12] The Diophantine equation $3^x + b = z^2$ has infinitely many solutions*

$$(b, x, z) = (2 \cdot 3^n + 1, 2n, 3^n + 1)$$

where n is a positive integer.

Theorem 5. *[12] The Diophantine equation $3^x + b^2 = z^2$ has infinitely many solutions*

$$(b, x, z) = \left(\frac{3^{2n+1} - 1}{2}, 2n + 1, \frac{3^{2n+1} + 1}{2} \right).$$

where n is a positive integer.

The above results from Burshtein were given for (2) in cases $y = 1, 2$.

In this work, we consider $a = 3$. Sroysang [13, 14] showed that $(x, y, z) = (1, 0, 2)$ is the unique solution for (2) when $a = 3$ and $b = 5, 7$. Lu [15] gave a generalization of the Sroysang's results stated that the only solution for $3^x + p^y = z^2$, when $p \equiv 5 \pmod{12}$, is $(x, y, z) = (1, 0, 2)$. Later, Asthana and Singh [16] showed that the complete solutions for $3^x + 13^y = z^2$ are (x, y, z) is $(1, 0, 2), (1, 1, 4), (3, 2, 14)$ or $(5, 1, 16)$. We note that the result of Asthana's is not covered by that of Lu's. The result appearing in this work is a generalization of Sroysang's results but not those of Asthana's. Our result is not contained in Lu's because Lu's condition does not cover case $p \equiv 3 \pmod 4$.

In 2019, Bushtein [17] established some non-negative solutions for Diophantine equation

$$3^x + p^y = z^2, \tag{3}$$

where p is an odd prime number and $x+y \leq 8$. The result's of Bushtein [11, 12, 17] restricted values of x and y in small numbers while in this work, our investigation does not have such restriction.

In this work, we are interested in a non-negative integer solution for the Diophantine equation (3), where p is a prime number that $p \equiv 2 \pmod 3$. Our result generalizes the results of Sroysang [13, 14]. We give the complete solution in case of $y=0$ or y is not divisible by 4. In case that y is a positive number that is divisible by 4, we give a necessary condition for an existence of a solution in a more general term. We give a necessary condition for an existence of a solution for $q^x+p^y=z^2$ when p,q are distinct prime numbers. Finally, we compute that for a positive integer y that is divisible by 4 and $p<10^{17}$, a solution for (3) exists only if $p=2$ or $p=11$ The solutions for such case are $(p,x,y,z)=(2,2,4,5)$ and $(p,x,y,z)=(11,5,4,122)$, respectively. Most of the application of a Diophantine equation are in cryptography [18, 19]. Application in other fields can be found in [20, 21].

2 Main results

The following lemmas are direct results from Theorem 1.

Lemma 6. *The only non-negative integer solution for* $3^x+1=z^2$ *is* $(x,z)=(1,2)$.

Lemma 7. *Let p be a prime number. The only non-negative integer solution for* $1+p^y=z^2$ *is* $(p,y,z)=(2,3,3)$.

Theorem 8. *Let p be a prime number. If $y=0$, then* $3^x+p^y=z^2$ *has a unique solution* $(p,x,y,z)=(p,1,0,2)$ *for each prime p.*

Proof. If $y=0$, then $z^2=3^x+p^0=3^x+1$; hence, we have $(p,x,y,z)=(p,1,0,2)$ by Lemma 6. □

Theorem 9. *Let p be a prime number where* $p \equiv 2 \pmod 3$. *If y is not divisible by 4, then* $3^x+p^y=z^2$ *has a unique solution* $(p,x,y,z)=(2,0,3,3)$.

Proof. Let p be a prime number where $p \equiv 2 \pmod 3$ and x,y and z be non-negative integers such that $3^x+p^y=z^2$. If $x=0$, then $1+p^y=3^0+p^y=z^2$. The only solution for this case is $(p,x,y,z)=(2,0,3,3)$ by Lemma 7. Now, we suppose $x \geq 1$ and consider the cases of y.

Case 9.1. *y is an odd number.*

Since y is an odd number, it follows that $y=2k+1$ for some $k \in \mathbb{N}\cup\{0\}$. So $3^x+p^{2k+1}=z^2$. Since $p \equiv 2 \pmod 3$, it follows that $p^{2k+1} \equiv (-1)^{2k+1} \equiv -1 \pmod 3$. We note that $z^2 \equiv 0,1 \pmod 3$ for all $z \in \mathbb{Z}$. Hence $z^2 \equiv 3^x+p^{2k+1} \equiv 0+(-1) \equiv 2 \pmod 3$ is not possible. Thus, if y is an odd number then the equation has no solution.

Case 9.2. *y is an even number.*

We have $y=2k$ for some $k \in \mathbb{N}$. So

$$\begin{aligned} 3^x+p^{2k} &= z^2 \\ 3^x &= z^2-p^{2k} \\ &= (z-p^k)(z+p^k). \end{aligned}$$

Hence $3^u=z-p^k$ and $3^{x-u}=z+p^k$ for some non-negative integer u. Since

$$3^{x-u}=z+p^k>z-p^k=3^u,$$

we have $x-u>u$ that is $x>2u$. Thus

$$\begin{aligned} (z+p^k)-(z-p^k) &= 3^{x-u}-3^u \\ 2\cdot p^k &= 3^u(3^{x-2u}-1). \end{aligned}$$

Since $x>2u$, it follows that $3^{x-2u}-1$ is an integer. Thus $3^u \mid 2\cdot p^k$. Since $(3,p)=1$, it follows that $3^u \mid 2$. Then $3^u=3^0$ that is $u=0$. So

$$2\cdot p^k=3^x-1. \tag{4}$$

Since $p \equiv 2 \pmod 3$, we have $p^k \equiv (-1)^k \pmod 3$. By the assumption $4 \nmid y$, we have that k is an odd number, so $p^k \equiv -1 \pmod 3$ contradiction. Therefore $3^x+p^y=z^2$ has exactly one non-negative integer solution which is $(p,x,y,z)=(2,0,3,3)$ when y is not divisible by 4. □

Theorem 10. *Let p and q be odd prime numbers, where $p \neq q$. The solution for $q^x+p^y=z^2$ exists only if one of the following is true:*

- $q \equiv 1 \pmod 4$, $p \equiv 3 \pmod 4$ *and y is an odd number,*
- $q \equiv 3 \pmod 4$, $p \equiv 1 \pmod 4$ *and x is an odd number,*
- $q \equiv 3 \pmod 4$, $p \equiv 3 \pmod 4$ *and the parity of x,y is different.*

Proof. Since p and q are odd numbers, it follows that z is even. Hence $z^2 \equiv 0 \pmod 4$. If $q \equiv 1 \pmod 4$, then $q^x \equiv 1 \pmod 4$ for all non-negative integer x. Hence $p^y \equiv 3 \pmod 4$ which implies that $p \equiv 3 \pmod 4$ and y is an odd number.

Consider $q \equiv 3 \pmod 4$ and x is odd. We have $q^x \equiv 3 \pmod 4$. Hence $p^y \equiv 1 \pmod 4$ which implies that either $p \equiv 3 \pmod 4$ and y is an even number or $p \equiv 1 \pmod 4$.

Consider $q \equiv 3 \pmod 4$ and x is even. We have $q^x \equiv 1 \pmod 4$. Hence $p^y \equiv 3 \pmod 4$ which implies that $p \equiv 3 \pmod 4$ and y is an odd number. This completes the proof. □

Therefore, a solution for $3^x + p^y = z^2$ exists only if one of the following is true:

- $p \equiv 1 \pmod 4$ and x is odd
- $p \equiv 3 \pmod 4$ and x, y have different parity.

Theorem 11. *Let p, q be prime numbers, where q is odd and $p \neq q$, and y be an even positive number. If a non-negative integer solution of $q^x + p^y = z^2$ exists, then the solution is in the form*

$$(q, p, x, y, z) = \left(q, \left(\frac{q^x - 1}{2}\right)^{\frac{2}{y}}, x, y, \frac{q^x + 1}{2}\right).$$

Proof. Suppose that $q^x + p^y = z^2$ has a non-negative integer solution (q, p, x, y, z). Since y is an even positive number, we have $y = 2k$ for some $k \in \mathbb{N}$. So

$$\begin{aligned} q^x + p^{2k} &= z^2 \\ q^x &= z^2 - p^{2k} \\ &= (z - p^k)(z + p^k). \end{aligned}$$

Thus $q^u = z - p^k$ and $q^{x-u} = z + p^k$ for some non-negative integer u. Since $q^{x-u} = z + p^k > z - p^k = q^u$. We obtain $x - u > u$ that is $x > 2u$. Thus

$$\begin{aligned} (z + p^k) - (z - p^k) &= q^{x-u} - q^u \\ 2 \cdot p^k &= q^u(q^{x-2u} - 1). \end{aligned}$$

Since $x > 2u$, it follows that $q^{x-2u} - 1$ is an integer. Thus $q^u \mid 2 \cdot p^k$. Since $(q, p) = 1$ and q is odd, it follows that $q^u \mid 2$. Then $q^u = q^0$ that is $u = 0$. Hence, $2 \cdot p^k = q^x - 1$ implying that $p^k = \frac{q^x-1}{2}$. By substituting $p^k = \frac{q^x-1}{2}$ in $q^x + p^y = z^2$, we have $z = \frac{q^x+1}{2}$. This completes the proof. □

Corollary 12. *Let p be a prime number and $y = 4k$ for some positive integer k. If a non-negative integer solution of (3) exists, then x is an odd number and the solution is in the form*

$$(p, x, y, z) = \left(\left(\frac{3^x - 1}{2}\right)^{\frac{1}{2k}}, x, 4k, \frac{3^x + 1}{2}\right).$$

Proof. This is a direct result from Theorems 10 and 11. □

Corollary 13. *Let p be an odd prime number and y be a positive integer that is divisible by 4. If a non-negative integer solution of (3) exists, then $\sqrt{\frac{3^x-1}{2}}$ is a power of the prime number p.*

x	n
1	1
2	2
5	11
65	2269476972881366
66	3930849423638141
67	6808430918644098

Table 1: List of $x, n \in \mathbb{N}$ such that $3^x + n^y = z^2$ where $n < 10^{17}$ for some $z \in \mathbb{N}$

By Corollary 13, we compute the value of $x, n \in \mathbb{N}$ and determine whether the corresponding z is an integer. The values of $x, n \in \mathbb{N}$ satisfying $3^x + n^y = z^2$, where $n < 10^{17}$ and z is an integer, are listed in Table 1. We compute such values up to $x = 68$ and find that $x = 67$ is the largest value that $\sqrt{\frac{3^x-1}{2}} < 10^{17}$. Next, we determine whether n is a power of a prime number. We find that 2269476972881366, 3930849423638141 and 6808430918644098 are not power of a prime number. Thus, we can conclude that for a prime number $p < 10^k$ where $p \equiv 2 \pmod 3$ and y is a positive integer that is divisible by 4, the equation (3) has a solution only when $p = 2$ or $p = 11$.

3 Conclusion

By computing the result in Corollary 13 up to $x = 68$, we have that $(p, x, y, z) = (2, 2, 4, 5)$ and $(p, x, y, z) = (11, 5, 4, 122)$ are the only solutions within the range of $p < 10^{17}$ in case that y is a positive integer that is divisible by 4. If $y = 0$ or y is not divisible by 4, the solution for (3) is either $(p, x, y, z) = (p, 1, 0, 2)$ or $(p, x, y, z) = (2, 0, 3, 3)$. Therefore, for each prime number $p < 10^{17}$ that $p \equiv 2 \pmod 3$ the solution for $3^x + p^y = z^2$ is $(p, x, y, z) \in \{(p, 1, 0, 2), (2, 0, 3, 3), (2, 2, 4, 5), (11, 5, 4, 122)\}$. This is a generalization of [13, 14]. However, the solution given in case is that y is a positive integer that is divisible by y might not be a complete solution. In this paper, we have a restriction on the prime number p that $p \equiv 2 \pmod 3$; hence, it is not covered the result of Asthana and Singh [16].

References:

[1] T. Hadano, On the Diophantine equation $a^x = b^y + c^z$, *Math. J. Okayama Univ.*, Vol.19, 1976, pp. 1-53.

[2] A. Suvarnamani, Solutions of the Diophantine equations $2^x + p^y = z^2$, *International Journal of Mathematical Sciences and Applications*, Vol.1, No.3, 2011, pp. 1415-1419.

[3] Z. Cao, On the diophantine equation $a^x + b^y = c^z$, *Acta Arithmetica*, Vol.91, No.2, 1999, pp. 85-93.

[4] Z. Cao, On the diophantine equation $a^x + b^y = c^z$, *Chinese Sci. Bull*, Vol.32, 1987, pp. 1519-1521.

[5] P. Mihailescu, Primary cyclotomic units and a proof of Catalan's conjecture, *Journal fur die reine und angewandte Mathematik*, Vol.572, 2004, pp. 167-195.

[6] N. Burshtein, On the Diophantine Equation $p^x + p^y = z^2$, *Annals Pure and Applied Mathematics*, Vol.19, No.2, 2019, pp. 111-119.

[7] N. Burshtein, On the Diophantine Equation $p^4 + q^3 = z^2$ and $p^4 - q^3 = z^2$ when p, q are distinct odd primes, *Annals Pure and Applied Mathematics*, Vol.21, No.1, 2020, pp. 15-17.

[8] A. Elshahed and H. Kamarulhaili, On the Diophantine Equation $(4^n)^x - p^y = z^2$, *WSEAS Transactions on Mathematics*, Vol.19, 2020, pp. 349-352.

[9] W. Orosram and C. Chomemuang, On the Diophantine Equation $8^x + n^y = z^2$, *WSEAS Transactions on Mathematics*, Vol.19, 2020, pp. 520-522.

[10] B. Sroysang, On the diophantine equation $7^x + 8^y = z^2$, *International Journal of Pure and Applied Mathematics*, Vol.84, No.1, 2013, pp. 111-114.

[11] N. Burshtein, On the Diophantine Equation $p^x + q^y = z^2$, *Annals Pure and Applied Mathematics*, Vol.13, No.2, 2017, pp. 229-233.

[12] N. Burshtein, On the Diophantine Equation $p^x + q^y = z^2$ when $p = 2$ and $p = 3$, *Annals of Pure and Applied Mathematics*, Vol.13, No.2, 2017, pp. 207-210.

[13] B. Sroysang, On the Diophantine equation $3^x + 5^y = z^2$, *International Journal of Pure and Applied Mathematics*, Vol.81, No.4, 2012, pp. 605-608.

[14] B. Sroysang, On the Diophantine Equation $3^x + 17^y = z^2$, *International Journal of Pure and Applied Mathematics*, Vol.89, No.1, 2013, pp. 111-114.

[15] L. Lu, A Note on the Diophantine Equation qx + py = z2, *Journal of Physics: Conference Series*, Vol.1039, 2018, pp. 012007.

[16] S. Asthana and Madan Mohan Singh, On the Diophantine Equation $3^x + 13^y = z^2$, *International Journal of Pure and Applied Mathematics*, Vol.114, No.2, 2017, pp. 301-304.

[17] N. Burshtein, On the Diophantine Equation $3^x + q^y = z^2$, *Annals Pure and Applied Mathematics*, Vol.19, No.2, 2019, pp. 169-173.

[18] J. Ding, M. Kudo, S. Okumura, T. Takagi and C. Tao, Cryptanalysis of a public key cryptosystem based on Diophantine equations via weighted LLL reduction, *Japan Journal of Industrial and Applied Mathematics volume*, Vol.35, 2018, 1123-1152.

[19] S. Okumura, A Public Key Cryptosystem Based on Diophantine Equations of Degree Increasing Type, *Pac. J. Math. Ind.*, Vol.7, No.2, 2015.

[20] G. Feretzakis, D. Kalles and V.S. Verykios, On Using Linear Diophantine Equations for in-Parallel Hiding of Decision Tree Rules, *Entropy*, Vol.21, No.1, 2019.

[21] R. Radha and G.Janaki, Applications of Diophantine Equations in Chemical Reactions and Cryptography, *Turkish Journal of Computer and Mathematics Education*, Vol.12, No.7, 2021, 3175-3178.

Contribution of individual authors to the creation of a scientific article (ghostwriting policy)

Wipawee Tangjai gives the idea of proof of Theorem 9, proves the rest of of the results in the paper and computes the computational results.
Chusak Chubthaisong gives a detail of proof in Theorem 9.