International Journal of Mathematics and
Computer Science, **18**(2023), no. 3, 487–495

On the Solutions of Some Mersenne Prime-Involved Diophantine Equations

William S. Gayo, Jr.[1], **Jerico B. Bacani**[2]

[1]General Education Department
College of Arts and Sciences
Don Mariano Marcos Memorial State University- North La Union Campus
Sapilang, Bacnotan 2515, La Union, Philippines

[2]Department of Mathematics and Computer Science
College of Science
University of the Philippines Baguio
Gov. Pack Road., Baguio City 2600, Philippines

email: wgayo@dmmmsu.edu.ph, jbbacani@up.edu.ph

(Received November 11, 2022, Revised December 16, 2022,
Accepted February 13, 2023, Published March 31, 2023)

Abstract

This work studies Diophantine equations of the form $A^X - B^Y = Z^2$. Specifically, we determine the nonnegative integer solutions (p_M, a, b, c) of the exponential Diophantine equation $(p_M)^a - (p_M+1)^b = c^2$ and its more generalized form $(p_M)^a - (p_M+1)^b = c^{2n}$, where p_M is a Mersenne prime number. Moreover, we also deal with the Diophantine equation $(p_M)^a - (q_M+1)^b = c^2$, where p_M and q_M are both Mersenne primes. We solve these equations with the aid of elementary methods in number theory like the factoring technique and the modular arithmetic method. We also utilize Mihailescu's Theorem, the concepts of quadratic residue and Legendre symbol, and some properties of Mersenne primes for our Diophantine analysis. Results show that both $(p_M)^a - (p_M+1)^b = c^2$ and $(p_M)^a - (p_M+1)^b = c^{2n}$ have trivial solutions which only exist when $a = 0$ and $b = 0$, while $(p_M)^a - (q_M+1)^b = c^2$ has two positive integer solutions.

Key words and phrases: Exponential Diophantine equation, Mersenne prime, Mihailescu's theorem.
AMS (MOS) Subject Classifications: 11A41, 11D61, 11D72.
The corresponding author is Jerico B. Bacani.
ISSN 1814-0432, 2023, http://ijmcs.future-in-tech.net

1 Introduction

Number theory, the study of integers and their properties, is a vast field of mathematics that showcases interesting topics. One interesting part of number theory is Diophantine analysis — the search for integer solutions of an equation. Equalities that require only integer solutions are often referred to as Diophantine equations. An integer solution of an n-variable Diophantine equation $f(x_1, x_2, \ldots, x_n) = 0$ is the ordered n-tuple $(x_1, x_2, \ldots, x_n)$ that satisfies the given equation. If $x_1, x_2, \ldots, x_n$ are all natural numbers, then the Diophantine equation is said to have a solution in natural numbers (and we say that the solution is positive); if $x_1, x_2, \ldots, x_n$ are all whole numbers, then the Diophantine equation is said to have a solution in whole numbers (and we say that the solution is nonnegative). A Diophantine equation may or may not have a solution. If it has a solution in the domain of interest, then we say that the Diophantine equation is solvable in that domain. Otherwise, it is unsolvable. Diophantine analysis seeks to answer whether a certain Diophantine equation is unsolvable, or solvable with unique solution, finitely many solutions or infinitely many solutions.

Diophantine equations come in different forms, and one particular type is the class of exponential Diophantine equations wherein at least one unknown is the exponent. The exponential Diophantine equation $A^X + B^Y = Z^2$ has been widely explored, and can be seen, for instance, in the works of Acu [1], Aggarwal [2], Alabbood [3], Bacani, Gayo, and Mina [4, 5, 6], Burshtein [7], Dockan and Pakapongpun [8], Kumar [15] Neres [9], Rabago [10, 14], Sroysang [11], and many more. Some of these researchers have studied this class of Diophantine equations in relation to prime numbers named after Mersenne (that is, Mersenne primes). They studied cases wherein the base A or B is any of the following Mersenne primes: $p_{M_2} = 3$, $p_{M_3} = 7$ or $p_{M_5} = 31$. As shown in the studies, solutions of such exponential Diophantine equations are unpredictable. As seen in various papers, working on these prime numbers, Sroysang [11] proved that $(0, 1, 2), (3, 0, 3)$, and $(4, 2, 5)$ are the nonnegative integer solutions of the Diophantine equation $2^x + 3^y = z^2$. On one hand, he proved the non-existence of the solution of the equations $5^x + 7^y = z^2$ and $31^x + 32^y = z^2$. However, he also showed the uniqueness of the solution of the Diophantine equations $3^x + 5^y = z^2$, $3^x + 85^y = z^2$, and $7^x + 8^y = z^2$. Rabago [10] showed that the only two solutions of the equation $2^x + 31^y = z^2$ are $(0, 3, 3)$ and $(7, 2, 33)$. Non-existence of solutions was proven by Aggarwal and Kumar [15] for $7^{2m} + (6^{r+1} + 1)^n = w^2$. When A is a Mersenne prime, one can learn from the results of Chotchaisthit [16], and

Gayo and Bacani [6].

A few mathematicians were also interested if a difference of two powers can be also a power. Catalan conjectured that 8 and 9 are the only consecutive powers. This was known as the Catalan's conjecture, which was renamed as Mihailescu's Theorem when Miahilescu proved it in 2002 [17]. This theorem has opened doors in solving some exponential Diophantine equations. Using this theorem, the Diophantine equation $x^2 - 4p^m = \pm y^n$ has been explored by Abu Muriefah and AL-Rashed [18], and equation $x^2 - p^m = \pm y^n$ has been scrutinized by Bugeaud [19]. Both have shown that these equations have only a finite number of solutions under some conditions that are not so restrictive.

In the present work, we consider the exponential Diophantine equation that is of the form $A^X - B^Y = Z^2$, where the base A is a Mersenne prime, and the value of the base B is one more than that Mersenne prime, or one more than another Mersenne prime. Specifically, we solve the equations $(p_M)^a - (p_M + 1)^b = c^2$, its more generalized form $(p_M)^a - (p_M + 1)^b = c^{2n}$, and $(p_M)^a - (q_M + 1)^b = c^2$ over the set of whole numbers. In these equations, p_M and q_M are Mersenne primes. Proofs of our results mainly depend on elementary methods in number theory like the Modular Arithmetic Method and Factoring Method. Modular Arithmetic Method is an approach in solving a Diophantine equation that employs simple modular arithmetic in showing that a certain Diophantine equation has no solution or in narrowing down the range of their possible solutions [20]. On the other hand, Factoring Method is a very useful technique where factorizations of a particular Diophantine equation yield to a system of equations that will generate the complete set of solutions to that Diophantine equation [20].

2 Preliminaries

The following definitions, lemmas, and theorem are needed for the discussion of results and finding regarding the solutions of the Diophantine equations under consideration.

Definition 2.1. *Let p be a prime number. A prime number p_M is called a Mersenne prime if it can be written as $p_M = 2^p - 1$.*

A useful property of Mersenne primes for this study is given below.

Lemma 2.2. *For all Mersenne primes p_M, the conguence $p_M \equiv 3 \pmod 4$ holds.*

Proof. Let p be a prime number. Since $p_M = 2^p - 1$ is a Mersenne prime, it follows that $p \geq 2$. Hence, $2^p \equiv 0 \pmod{4}$, which yields to $p_M = 2^p - 1 \equiv -1 \pmod{4}$, or equivalently $p_M \equiv 3 \pmod{4}$. □

Definition 2.3. *Let p be an odd prime number that is relatively prime with the given natural number r. The integer r is a quadratic residue of p if there is a solution to the quadratic congruence $z^2 \equiv r \pmod{p}$; otherwise, r is a quadratic non-residue of p.*

Definition 2.4. *Let p be an odd prime and relatively prime with an integer r. The Legendre symbol $\left(\dfrac{r}{p}\right)$ has the following values:*

$$\left(\frac{r}{p}\right) = \begin{cases} 1 & \textit{if } r \textit{ is a quadratic residue of } p, \\ -1 & \textit{if } r \textit{ is a quadratic non-residue of } p. \end{cases}$$

Lemma 2.5. *If p is an odd prime, then*

$$\left(\frac{-1}{p}\right) = \begin{cases} -1 & \textit{if } p \equiv 3 \pmod{4} \\ 1 & \textit{if } p \equiv 1 \pmod{4}. \end{cases}$$

Theorem 2.6 (Mihailescu's Theorem [17]). *Let a, b, x and y be integers with $min\{a, b, x, y\} > 1$. Then, the Diophantine equation $a^x - b^y = 1$ has no solution except for $(a, x, b, y) = (3, 2, 2, 3)$.*

3 Main results

3.1 The Equation $(p_M)^a - (p_M + 1)^b = c^2$

The following two lemmas are needed to determine the solutions of the Diophantine equation $(p_M)^a - (p_M + 1)^b = c^2$.

Lemma 3.1. *The Diophantine equation $1 - (p_M + 1)^b = c^2$, where p_M is a Mersenne prime, has no solution (p_M, b, c) in whole numbers aside from the trivial solution $(p_M, 0, 0)$.*

Proof. The proof is divided into two cases of b. If $b = 0$, then $c^2 = 0$ which gives $c = 0$. If $b > 1$, then $1 - (p_M + 1)^b < 0$. This is not possible because $c^2 \geq 0$. Hence, $(p_M, 0, 0)$ is the only solution. □

Lemma 3.2. *The Diophantine equation $(p_M)^a - 1 = c^2$, where p_M is a Mersenne prime, has no solution (p_M, a, c) in whole numbers except for the trivial solution $(p_M, 0, 0)$.*

Proof. For the values of a, the cases, $a = 0$, $a = 1$ and $a > 1$, are considered. If $a = 0$, then $c^2 = 0$ and thus $c = 0$. If $a = 1$, then $c^2 = p_M - 1$. Since p_M is a Mersenne prime, then $p_M = 2^p - 1$. Note that $p_M \equiv -1 \pmod 4$ so that $c^2 \equiv 2 \pmod 4$. This is not possible. If $a > 1$, then by Mihailescu's Theorem, it is not possible. □

The result on the solutions of the Diophantine equation $(p_M)^x - (p_M + 1)^y = c^2$ in natural numbers is stated as follows.

Theorem 3.3. *The Diophantine equation $(p_M)^a - (p_M + 1)^b = c^2$, where p_M is a Mersenne prime, has no positive integer solutions.*

Proof. Note that for any positive integer a, $(p_M)^a \equiv 0 \pmod{p_M}$, and for any positive integer b, $(M + 1)^b \equiv 1 \pmod{p_M}$. So,

$$(p_M)^a - (p_M + 1)^b \equiv -1 \pmod{p_M}.$$

Thus, $c^2 \equiv -1 \pmod{p_M}$. Since $p_M \equiv 3 \pmod 4$, it follows that the Legendre symbol

$$\left(\frac{-1}{p_M}\right) = -1,$$

which means that -1 is not a quadratic residue of p_M. This further means the congruence $c^2 \equiv -1 \pmod{p_M}$ has no solution, and so does the Diophantine equation $(p_M)^a - (p_M + 1)^b = c^2$. □

Now, we state the main result on the solutions of the Diophantine equation $(p_M)^a - (p_M + 1)^b = c^2$ in whole numbers.

Theorem 3.4. *The trivial solution $(p_M, 0, 0, 0)$ is the only solution (p_M, x, y, z) of the Diophantine equation $(p_M)^a - (p_M + 1)^b = c^2$ in whole numbers, where p_M is a Mersenne prime.*

Proof. First, let us consider the case when $\min\{a, b\} = 0$. If $a = 0$, then we have the equation $1 - (p_M + 1)^b = c^2$. By Lemma 3.1, $(p_M, b, c) = (p_M, 0, 0)$. Hence, we get $(p_M, a, b, c) = (p_M, 0, 0, 0)$ as a solution. If $b = 0$, then we have the equation $(p_M)^a - 1 = c^2$. By Lemma 3.2, $(p_M, a, c) = (p_M, 0, 0)$. Hence, we get the same solution. For $\min\{a, b\} \geq 1$, there is no solution by Theorem 3.3. □

Using Theorem 3.4, we study the more general case, which is the Diophantine equation $(p_M)^a - (p_M+1)^b = c^{2n}$; and hence we get the following corollary.

Corollary 3.5. *The trivial solution* $(p_M, 0, 0, 0, t)$, $t \in \mathbb{N}$, *is the only nonnegative integer solution* (p_M, a, b, c, n) *of the Diophantine equation* $(p_M)^a - (p_M+1)^b = c^{2n}$, *where* p_M *is a Mersenne prime and* $n \in \mathbb{N}$.

Proof. Here, we are considering the Diophantine equation $(p_M)^a-(p_M+1)^b = (c^n)^2$, where n is a positive integer. By Theorem 3.4, this has trivial solutions in $\mathbb{N}_0$, and these solutions occur when $c^n = 0$. This is possible for $c = 0$ and any positive integer t. Thus, we have the solution $(p_M, a, b, c, n) = (p_M, 0, 0, 0, t)$, $t \in \mathbb{N}$. □

3.2 The Equation $(p_M)^a - (q_M + 1)^b = c^2$

The next main result is on the solutions of the Diophantine equation $(p_M)^a - (q_M+1)^b = c^2$, where p_M and q_M are Mersenne primes, and a, b and c are positive integers.

Theorem 3.6. *The positive integer solutions* (p_M, q_M, a, b, c) *of the Diophantine equation* $(p_M)^a - (q_M+1)^b = c^2$ *are the quintuples* $(3, 31, 4, 1, 7)$ *and* $(3, 7, 2, 1, 1)$.

Proof. First, note that every Mersenne prime is congruent to $3 \pmod 4$. Hence, $p_M \equiv 3 \pmod 4$ and $q_M + 1 \equiv 0 \pmod 4$. Thus, for every positive integer b,

$$(p_M)^a - (q_M+1)^b \equiv \begin{cases} 3 \pmod 4 & \text{if } a \text{ is odd} \\ 1 \pmod 4 & \text{if } a \text{ is even.} \end{cases}$$

Since $c^2 \equiv 1 \pmod 4$, we therefore conclude that a is even, that is, $a = 2k$, where k is a positive integer. Thus, we have the equation $(p_M)^{2k}-(q_M+1)^b = c^2$. This can written as $((p_M)^k + c)((p_M)^k - c) = 2^{qb}$, where q is a prime number. There are nonnegative integers u and v with $u > v$ such that $u + v = qy$ and

$$\begin{cases} (p_M)^k + c = 2^u \\ (p_M)^k - c = 2^v. \end{cases}$$

Adding the two equations in the system leads to $2(p_M)^k = 2^u + 2^v$. Because $u > v$, we get the factored equation $2(p_M)^k = 2^v(2^{u-v} + 1)$. This leads to the system

$$\begin{cases} 2^v = 2 \\ (p_M)^k = 2^{u-v} + 1. \end{cases}$$

The first equality gives the value $v = 1$. Hence, $u > 1$ and $c = (p_M)^k - 2$. The second equation becomes

$$(p_M)^k - 2^{u-1} = 1.$$

If $k > 1$ and $u > 2$, then by Mihailescu's Theorem, we acquire the values $p_M = 3$, $k = 2$ and $u = 4$. Hence, we get the values $c = 7$, $a = 4$ and $qb = 5$. Because q is a prime number, we obtain $q = 5$ and $b = 1$. Thus, $q_M = 31$ and we have the solution $(p_M, q_M, a, b, c) = (3, 31, 4, 1, 7)$. It remains to be studied is the case when $k = 1$ or when $u = 2$. If $k = 1$, then $a = 2$ and $p_M = 2^{u-1}+1$. If $p_M = 3$, then $c = 1$ and $u = 2$. Thus, $qb = 3$, yielding the values $q = 3$ and $b = 1$. Hence, we have the solution $(p_M, q_M, a, b, c) = (3, 7, 2, 1, 1)$. If $u = 2$, then $qb = 3$ and $(p_M)^k = 3$. This leads to the same solution $(p_M, q_M, a, b, c) = (3, 7, 2, 1, 1)$. □

Note that if we take $q_M = p_M$, then Theorem 3.3 becomes a corollary of Theorem 3.6. Furthermore, by using Theorem 3.4, it would be clear that the nonnegative integer solutions (p_M, q_M, a, b, c) of $(p_M)^a - (q_M + 1)^b = c^2$ are $(3, 31, 4, 1, 7)$, $(3, 7, 2, 1, 1)$, and $(p_M, q_M, 0, 0, 0)$, where p_M and q_M are Mersenne primes that are not necessarily distinct.

4 Conclusion

The exponential Diophantine equations $(p_M)^a - (p_M + 1)^b = c^2, (p_M)^a - (p_M + 1)^b = c^{2n}$, and $(p_M)^a - (q_M + 1)^b = c^2$ were considered and solved using elementary number theory methods. Result shows that only the trivial solution $(p_M, 0, 0, 0)$ exists as nonnegative integer solution (p_M, a, b, c) of the exponential Diophantine equation $(p_M)^a - (p_M + 1)^b = c^2$, where p_M is a Mersenne prime. Also, the trivial solution $(p_M, 0, 0, 0, t)$, $t \in \mathbb{N}$, is the only nonnegative integer solution (p_M, a, b, c, n) of the Diophantine equation $(p_M)^a - (p_M+1)^b = c^{2n}$, where p_M is a Mersenne prime and $n \in \mathbb{N}$. Moreover, the positive integer solutions (p_M, q_M, a, b, c) of the Diophantine equation $(p_M)^a - (q_M + 1)^b = c^2$ are the quintuples $(3, 31, 4, 1, 7)$ and $(3, 7, 2, 1, 1)$.

Acknowledgment. The authors would like to DMMMSU-NLU Campus and UP Baguio for their support in the conduct of this research. Furthermore, they would like to extend their gratitude to UP Baguio for allowing these results to be disseminated through the MathTech 2022 and be published eventually. Last but not least, many thanks go to the anonymous encouraging referees whose comments and suggestions are truly helpful in obtaining a publishable paper for this journal.

References

[1] D. Acu, On a Diophantine equation $2^x + 5^y = z^2$, Gen. Math., **15,** no. 4, (2007), 145–148.

[2] S. Aggarwal, On the existence of solution of Diophantine equation $193^x + 211^y = z^2$, Journal of Advanced Research in Applied Mathematics and Statistics, **5,** nos. 3–4, (2020), 1–2.

[3] M. A. Alabbood, On some exponential Diophantine equations, International Journal of Mathematics and Computer Science, **17**, no. 1, (2022), 431–438.

[4] R. J. S. Mina and J. B. Bacani, Non-existence of solutions of Diophantine equations of the form $p^x + q^y = z^{2n}$, Mathematics and Statistics, **7,** no. 3, (2019), 78–81.

[5] R. J. S. Mina, J. B. Bacani, On the solutions of the Diophantine equation $p^x + (p + 4k)^y = z^{2n}$ for prime pairs p and $p + 4k$, European Journal of Pure and Applied Mathematics, **14,** no. 2, (2021), 471–479.

[6] W. S. Gayo, Jr., J. B. Bacani, On the Diophantine equation $M_p^x + (M_q + 1)^y = z^2$, European Journal of Pure and Applied Mathematics, **14,** no. 2, (2021), 396–403.

[7] N. Burshtein, All the solutions of the Diophantine equation $p^x + (p + 4)^y = z^2$ when $p, (p + 4)$ are primes and $x + y = 2, 3, 4$, Annals of Pure and Applied Mathematics, **16**, no. 1, (2018), 241–244.

[8] R. Dockan, A. Pakapongpun, On the Diophantine equation $p^x + (p + 20)^y = z^2$, where p and $p + 20$ are primes, International Journal of Mathematics and Computer Science, **16,** no. 1, (2021), 179–183.

[9] F. Neres, On the solvability of the Diophantine equation $p^x + (p+8)^y = z^2$ when $p > 3$ and $p + 8$ are primes, Annals of Pure and Applied Mathematics, **18,** no. 1, (2018), 179–183.

[10] J. F. T. Rabago, A note on an open problem by B. Sroysang, Science and Technology RMUTT Journal, **3**, no. 1, (2013), 41–43.

[11] B. Sroysang, On the Diophantine equation $3^x + 5^y = z^2$, Int. J. Pure Appl. Math., **81,** no. 4, (2012), 605–608.

[12] A. Hoque, H. Kalita, On the Diophantine equation $(p^q - 1)^x + p^{qy} = z^2$, Journal of Analysis & Number Theory, **3**, no. 2, (2015), 117–119.

[13] S. Cenberci, B. Peker, On the Diophantine equation $(2^n)^x + p^y = z^2$, Amer. J. Math. Sci., **1**, (2012), 195–199.

[14] J. B. Bacani, J. F. T. Rabago, The complete set of solutions of the Diophantine equation $p^x + q^y = z^2$ for twin primes p and q, International Journal of Pure and Applied Mathematics, **104,** no. 4, (2015), 517–521.

[15] S. Aggarwal, S. Kumar, On the exponential Diophantine equation $7^{2m} + ((6^{r+1} + 1)^n = w^2$, International Journal of Research and Scientific Innovation, **8,** no. 4, (2021), 58–60.

[16] S. Chotchaisthit, On the Diophantine equation $p^x + (p+1)^y = z^2$, where p is a Mersenne prime, Int. J. Pure Appl. Math., **88,** no. 2, (2013), 169–172.

[17] P. Mihailescu, Primary cyclotomic units and a proof of Catalan's conjecture, J. Reine Angew Math., **572,** (2004), 167–195.

[18] F. S. Abu Muriefah, A. AL-Rashed, On the Diophantine equation $x^2 - 4p^m = \pm y^n$, Arab Journal of Mathematical Sciences, **18,** (2012), 97–103.

[19] Y. Bugeaud, On the Diophantine equation $x^2 - p^m = \pm y^n$, Acta Arith., **80,** no. 3, (1997), 213–223.

[20] T. Andreescu, D. Andrica, I. Cucurezeanu, An Introduction to Diophantine Equations, Springer Science+Business Media, USA, 2010.