# On a Diophantine equation involving Mersenne number

**William S. Gayo, Jr.**
*Don Mariano Marcos Memorial State University*
*La Union, Philippines*
*wgayo@dmmmsu.edu.ph*

**Abstract.** This research work focused on studying an exponential Diophantine equation involving Mersenne numbers. Specifically, it sought to find the nonnegative integer solutions $(M_n, x, y, z)$ of the Diophantine equation $M_n^x + (M_n + 1)^y = z^2$. To obtain the solutions, a combination of modular arithmetic method and factoring method, together with some other results like Mihailescu's theorem, was utilized. Results of the Diophantine analysis revealed that aside from $(3, 2, 2, 5)$ and $(7, 0, 1, 3)$, the equation has infinitely many solutions of the form $(2^{2k} - 1, 1, 0, 2^k)$ where $k$ is a positive integer.

**Keywords:** exponential Diophantine equation, integer solution, Mersenne number, number theory.

**MSC 2020:** 11D61, 11D72

## 1. Introduction

Number theory is regarded as one of the purest areas of mathematics studied because of the intellectual fascination with properties of integers. Recently, it has been an area that also has significant applications to subjects such as cryptography [6].

Number theory researchers are very interested in the search for integer solutions to equations. These equations are termed Diophantine equations. Diophantine equations have a wide range of applications in coordinate geometry, cryptography, trigonometry, and applied algebra. It is also extremely useful in determining the solutions to many puzzle problems [1].

One of the most explored Diophantine equations is the equation of the form

$$a^x + b^y = z^2. \tag{1}$$

Equation (1) has been studied in connection with Mersenne primes by numerous researchers. Some of them focused on the case in which one of $a$ and $b$ in equation (1) is a Mersenne prime. Particularly, some considered the first three Mersenne prime numbers $3, 7$, and $31$. For instance, Asthana and Singh [2] showed that $3^x + 13^y = z^2$ has four nonnegative integer solutions which are $(1, 0, 2), (1, 1, 4), (3, 2, 14)$ and $(5, 1, 6)$. Also, Rabago [8] proved that the triples $(4, 1, 10)$ and $(1, 0, 2)$ are the only two nonnegative integer solutions to the Diophantine equation $3^x + 19^y = z^2$, and that the triples $(2, 1, 10)$ and $(1, 0, 2)$ are the only nonnegative integer solutions to $3^x + 91^y = z^2$. Furthermore, Sroysang

[10] showed that $(x, y, z) = (0, 1, 3)$ is the unique solution of $7^x + 8^y = z^2$. However, in another work of Sroysang [9], he showed that the equation $31^x + 32^y = z^2$ has no nonnegative integer solution.

In recent years, Gayo and Bacani worked on Diophantine equations that involve Mersenne primes. In 2021, they solved the nonnegative integer solutions $(M_p, M_q, x, y, z)$ of the Diophantine equation $M_p^x + (M_q + 1)^y = z^2$, where $M_p$ and $M_q$ are Mersenne primes using elementary methods in number theory [3]. In 2022, they also showed that the quadruples $(3, 1, 0, 2), (3, 0, 3, 3)$ and $(3, 2, 4, 5)$ are the only nonnegative integer solutions $(M, x, y, z)$ of the exponential Diophantine equation $M^x + (M - 1)^y = z^2$, where $M$ is a Mersenne prime [4]. In 2023, the same authors determined the nonnegative integer solutions $(p_M, a, b, c)$ of the Diophantine equation $(p_M)^a - (p_M + 1)^b = z^2$ and its more generalized form $(p_M)^a - (p_M + 1)^b = c^{2n}$, where $p_M$ is a Mersenne prime number [5]. A variation of the studies of the two aforementioned authors was made for this research study. Instead of Mersenne prime, a larger set of numbers to which Mersenne primes belong is being considered; that is the set of Mersenne numbers. Hence, the present study focused on the Diophantine equation $M_n^x + (M_n + 1)^y = z^2$ where $M_n$ is a Mersenne number.

## 2. Preliminaries

This part presents the concepts, definitions, lemmas, and theorems necessary to solve the Diophantine equation $M_n^x + (M_n + 1)^y = z^2$.

### 2.1 Mersenne numbers

**Definition 2.1.** *Mersenne numbers are numbers of the form $2^n - 1$, where $n$ is a positive integer.*

Two properties needed to solve the Diophantine equation under consideration are given by the next two lemmas.

**Lemma 2.1.** *The only Mersenne number congruent to $1 \pmod 4$ is $M_1 = 1$. All others are congruent to $3 \pmod 4$. In symbols,*

$$M_n \equiv \begin{cases} 1 \pmod 4, & \textit{if } n = 1, \\ 3 \pmod 4, & \textit{if } n > 1 \end{cases}.$$

**Proof.** Note that $M_n = 2^n - 1$ for positive integer n. If $n = 1$, then $M_n = 1$. This is obviously congruent to 1 modulo 4. If $n > 1$, then $2^n \equiv 0 \pmod 4$. This means that $2^n - 1 \equiv -1 \pmod 4$. Thus, $M_n \equiv -1 \pmod 4$, or equivalently $M_n \equiv 3 \pmod 4$. □

**Lemma 2.2.** *Positive even and odd powers of Mersenne numbers greater than 1 are congruent to 1 and 3 modulo 4, respectively.*

**Proof.** From Lemma 2.1, a Mersenne number greater than 1 is congruent 3 (mod 4). Raising it to a positive integer $x$ leads to

$$M_n^x \equiv 3^x \pmod 4.$$

If $x$ is even, let $x = 2k, k \in \mathbb{N}$. Then, $M_n^x \equiv 3^{2k} \pmod 4$ which is equivalent to $M_n^x \equiv 9^k \pmod 4$. This is also the same as $M_n^x \equiv 1^k \pmod 4$, or equivalently $M_n^x \equiv 1 \pmod 4$.

If $x$ is odd, let $x = 2k+1, k \in \mathbb{N}_0$. Then, $M_n^x \equiv 3^{2k+1} \pmod 4$ which is equivalent to $M_n^x \equiv 3 \cdot 9^k \pmod 4$. This is also the same as $M_n^x \equiv 3 \cdot 1^k \pmod 4$, or equivalently $M_n^x \equiv 3 \pmod 4$. □

### 2.2 Square of an integer

The right-hand side of the equation $M_n^x + (M_n + 1)^y = z^2$ is a perfect square. Since we will be utilizing modular arithmetic method as one of the methods, it is just right to find modular properties of the square of an integer.

**Lemma 2.3.** *The square of an integer is either congruent to* 0 *or* 1 *modulo* 4*. Specifically, the squares of an even integer and odd integer are congruent to* 0 *modulo* 4 *and* 1 *modulo* 4*, respectively.*

**Proof.** Let $z$ be an integer. Then, by Division Algorithm, $z$ can be written in the form $2n$ or $2n+1$. If $z$ is even or of the form $2n$, then $z^2 = 4n^2$, which is obviously congruent to $0 \pmod 4$. On the other hand, if $z$ is odd or of the form $2n+1$, then $z^2 = 4n^2 + 4n + 1$, which is congruent to $1 \pmod 4$. □

### 2.3 The Mihailescu's theorem

In 1844, Charles Catalan conjectured that if $\min\{a, b, x, y\} > 1$, then the only solution to the Diophantine equation $a^x - b^y = 1$ is the quadruple $(a, b, x, y) = (3, 2, 2, 3)$, which was famously known as the Catalan conjecture. Since then, a number of mathematicians have attempted to prove the conjecture, but it was only in 2002 that the conjecture was finally proven by Mihailescu [7]. Hence, the conjecture was renamed Mihailescu's Theorem. This theorem led to the solvability of many Diophantine equations and will also be used to prove our results. Mihailescu's Theorem is stated below.

**Theorem 2.1** ([7], Mihailescu's Theorem)**.** *The triple* $(3, 2, 2, 3)$ *is the unique solution* $(a, b, x, y)$ *for the Diophantine equation* $a^x - b^y = 1$*, where* $a, b, x$ *and* $y$ *are integers with* $\min\{a, b, x, y\} > 1$*.*

## 3. Main results

This section presents the solutions of the Diophantine equation $M_n + (M_n + 1)^y = z^2$. The cases when $x = 0$ or $y = 0$ will be solved first.

### 3.1 The equation $1 + (M_n + 1)^y = z^2$

The case when $x = 0$ is solved here. This is when the equation is $1+(M_n+1)^y = z^2$. The solution of this equation is given in the following lemma.

**Lemma 3.1.** *The triple* $(7, 1, 3)$ *is the unique solution* $(M_n, y, z)$ *for the Diophantine equation* $1 + (M_n + 1)^y = z^2$*, where* $M_n > 1$ *is a Mersenne number and* $y, z$ *are a nonnegative integer.*

**Proof.** Let $M_n > 1$ be a Mersenne number, and $y, z$ be nonnegative integers such that $1 + (M_n + 1)^y = z^2$. Then, there exists a positive integer $n$ such that $M_n = 2^n - 1, n > 1$. This results to

$$1 + 2^{ny} = z^2.$$

Three cases for the value of $y$ are considered.

If $y = 0$, then $z^2 = 2$, which has no integer solution.

If $y = 1$, then $1 + 2^n = z^2$, which can be expressed as $z^2 - 1 = 2^n$. This can be factored as $(z-1)(z+1) = 2^n$. There exist nonnegative integers $u$ and $v$ such that $u + v = n$ and $u > v$. So, the equation now becomes $(z - 1)(z + 1) = 2^{u+v}$. Since $(z - 1) < (z + 1)$ and $u > v$, it follows that

$$\begin{cases} z + 1 = 2^u, \\ z - 1 = 2^v \end{cases}.$$

Combining the two equations in the system gives $2 = 2^u - 2^v$. Because the greatest common factor of $2^u$ and $2^v$ is $2^v$, this can be factored out, yielding to $2 = 2^v(2^{u-v} - 1)$. Note that $2^v$ and $2^{u-v} - 1$ are relatively prime. Equating powers of 2 and non-powers of 2 results to

$$\begin{cases} 2^v = 2, \\ 2^{u-v} - 1 = 1 \end{cases}.$$

The first equation in the system gives the value $v = 1$. So, the value of $z$ is $z = 2^v + 1 = 2^1 + 1 = 3$. Moreover, the second equation in the same system becomes $2^{u-1} = 2$, which has the solution $u = 2$. Computing for the value of $n$ based from $u = 2$ and $v = 1$ results to $n = 3$. This further results to $M_n = 2^3 - 1 = 7$. Thus, $(M_n, x, z) = (7, 1, 3)$ is a solution.

If $y > 1$, then by Mihailescu's Theorem, the Diophantine equation $1 + 2^{ny} = z^2$ can have a solution if $ny = 3$ and $z = 3$. Since $y > 1$, it follows that $y = 3$ and $n = 1$. This implies that $M_n = 1$, which contradicts the assumption that $M_n > 1$. □

### 3.2 The equation $M_n^x + 1 = z^2$

The case when $y = 0$ is solved here. This is when the equation is $M_n^x + 1 = z^2$. The solution of this equation is given in the following lemma.

**Lemma 3.2.** *The solutions $(M_n, x, z)$ of the Diophantine equation $M_n^x + 1 = z^2$, where $M_n > 1$ is a Mersenne number and $x, z$ are nonnegative integers are of the form $(2^{2k} - 1, 1, 2^k)$ where $k$ is a positive integer.*

**Proof.** Let $M_n > 1$ be a Mersenne number, and $x, z$ be nonnegative integers such that $M_n^x + 1^y = z^2$. Then, there exists a positive integer $n$ such that $M_n = 2^n - 1, n > 1$. This results to

$$(2^n - 1)^x + 1 = z^2.$$

Three cases for the value of $x$ are considered. These are $x = 0, x = 1$, and $x > 1$.

When $x = 0$, the equation becomes $z^2 = 2$. This quadratic equation has no integer solution.

For $x = 1$, the equation becomes $z^2 = 2^n$. Let $z = 2^k$, where $k \in \mathbb{N}$. Then, $2^{2k} = 2^n$, and thus, $n = 2k$. It follows that $M_n = 2^{2k} - 1$. Hence, $(2^{2k} - 1, 1, 2^{2k})$ are solutions of the Diophantine equation.

If $x > 1$, then by Mihailescu's Theorem, $z = 3, x = 3$, and $2^n - 1 = 2$. However, the last equation does not have an integer solution. □

### 3.3 The Diophantine equation $M_n^x + (M_n + 1)^y = z^2$

In this part, the Diophantine equation $M_n^x + (M_n + 1)^y = z^2$ is solved. Its solutions are given in the following theorem.

**Theorem 3.1.** *The solutions $(M_n, x, y, z)$ of the Diophantine equation $M_n^x + (M_n + 1)^y = z^2$ with nonnegative integers $x, y, z$ and Mersenne number $M_n > 1$ are $(7, 0, 1, 3), (3, 2, 2, 5)$ and $(2^{2k} - 1, 1, 0, 2^k)$, where $k$ is a positive integer.*

**Proof.** Let $M_n > 1$ be a Mersenne number, and $x, y, z$ be nonnegative integers such that $M_n^x + (M_n + 1)^y = z^2$. If $x = 0$, then $1 + (M_n + 1)^y = z^2$. By Lemma 3.1, this equation has the only solution $(7, 1, 3)$. Thus, $(M_n, x, y, z) = (7, 0, 1, 3)$ is a solution to $M_n^x + (M_n + 1)^y = z^2$. On the other hand, if $y = 0$, then $M_n^x + 1 = z^2$. By virtue of Lemma 3.2, this equation has solutions of the form $(2^{2k} - 1, 1, 2^k)$ where $k$ is a positive integer. Hence, $(M_n, x, y, z) \in \{(2^k - 1, 1, 0, 2^k)\}$ is a solution set of $M_n^x + (M_n + 1)^y = z^2$.

Now, suppose $x, y \geq 0$. Since $M_n = 2^n - 1 > 1$, it is clear that $n > 1$. From this, it is easy to observe that $M_n \equiv -1 \pmod 4$. So, $M_n + 1 \equiv 0 \pmod 4$. It follows then by Lemma 2.2 that for every positive integer $x$,

$$M_n^x \equiv \begin{cases} 1 \pmod 4, & \text{if } x \text{ is even,} \\ 3 \pmod 4, & \text{if } x \text{ is odd} \end{cases}.$$

Also, it is easy to see that for every positive integer $y$, $(M_n+1)^y \equiv 0 \pmod 4$. This means that

$$M_n^x + (M_n+1)^y \equiv \begin{cases} 1 \pmod 4, & \text{if } x \text{ is even,} \\ 3 \pmod 4, & \text{if } x \text{ is odd} \end{cases}.$$

Because $z^2 \equiv 1 \pmod 4$, it must be true that $x$ is even. There exists a positive integer $k$ such that $x = 2k$. So, the equation now becomes $M_n^{2k} + (M_n+1)^y = z^2$. This can be expressed as $z^2 - M_n^{2k} = (M_n+1)^y$. Since the left-hand side of the equation is a difference of two squares, it can be factored into $(z - M_n^k)(z + M_n^k) = (M_n+1)^y$. For the reason that $M_n = 2^n - 1$, the equation can be written as $(z - M_n^k)(z + M_n^k) = 2^{ny}$. There exist nonnegative integers $u$ and $v$ such that $u + v = ny$ and $u > v$. So, the equation now becomes $(z - M_n^k)(z + M_n^k) = 2^{u+v}$. Since $(z - M_n^k) < (z + M_n^k)$ and $u > v$, it follows that

$$\begin{cases} z + M_n^k = 2^u, \\ z - M_n^k = 2^v \end{cases}.$$

Subtracting the two equations in the system results to $2M_n^k = 2^u - 2^v$. Note that the greatest common factor of $2^u$ and $2^v$ is $2^v$. This can be factored out, resulting to $2M_n^k = 2^v(2^{u-v} - 1)$. Note that $2^v$ and $2^{u-v} - 1$ are relatively prime. Equating powers of 2 and non-powers of 2 results to

$$\begin{cases} 2 = 2^v, \\ M_n^k = 2^{u-v} - 1 \end{cases}.$$

The first equation implies that $v = 1$, which implies that $u > 1$ , $u + 1 = ny$ and $z = M_n^k + 2$. Because $v = 1$ and $M_n = 2^n - 1$, the second equation becomes

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

Three cases for the value of $k$ and $u$ are considered.

If $u > 2$ and $k > 1$, by Mihailescu's Theorem, the equation has no integer solution.

If $u = 2$, then $(2^n - 1)^k = 1$, which implies that $k = 0$. This is a contradiction to $k$ being positive.

If $k = 1$, then $x = 2, z = M_n + 2$ and $2^{u-1} - 1 = 2^n - 1$. The latter equation is equivalent to $2^{u-1} = 2^n$, which implies that $u - 1 = n$. It is known that $u + 1 = ny$. The equations $u - 1 = n$ and $u + 1 = ny$, when combined, becomes $2 = ny - n = n(y - 1)$. Since $n > 1$, it can be concluded that $n = 2$ and $y = 2$. It follows that $M_n = 3$. This further implies that $z = 5$. Hence, $(M_n, x, y, z) = (3, 2, 2, 5)$. □

## 4. Concluding remarks

In this research study, we solve the exponential Diophantine equation $M_n^x + (M_n + 1)^y = z^2$ in the set of nonnegative integers. Results show that when $y = 0$, the equation has infinitely many solutions of the form $(2^{2k} - 1, 1, 0, 2^k)$ where $k$ is a positive integer. Also, when $x = 0$, it has only one solution which is $(7, 0, 1, 3)$. Moreover, when $x$ and $y$ are positive integers, the unique solution is the quadruple $(3, 2, 2, 5)$.

## Acknowledgment

The researcher would like to thank Don Mariano Marcos Memorial State University for funding this research. Sincere gratitude is also given to the reviewer for the comments and suggestions that led to the improvement of the paper.

## References

[1] S. Aggarwal, S. Kumar, *On the exponential Diophantine equation* $(19)^{2m} + (12\gamma + 1)^n = \rho^2$, Int. J. Res. Innovation Appl. Sci., 6 (2021), 14-16.

[2] S. Asthana, M. M. Singh, *On the Diophantine equation* $3^x + 13^y = z^2$, Int. J. Pure Appl. Math., 114 (2017), 301-304.

[3] W. S. Gayo, J. B. Bacani, *On the Diophantine equation* $M_p^x + (M_q + 1)^y = z^2$, Eur. J. Pure Appl. Math., 14 (2021), 396–403.

[4] W. S. Gayo, J. B. Bacani, *On the solutions of the Diophantine equation* $M^x + (M - 1)^y = z^2$, Ital. J. Pure Appl. Math., 47 (2022), 1113–1117.

[5] W. S. Gayo, J. B. Bacani, *On the solutions of some Mersenne prime-involved Diophantine equations*, Int. J. Math. Comput. Sci., 18 (2023), 487–495.

[6] J. S. Kraft, L. C. Washington, *An introduction to number theory with cryptography*, Chapman and Hall/CRC, 2013.

[7] P. Mihailescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math., 27 (2004), 167-195.

[8] J. F. T. Rabago, *On two Diophantine equations* $3^x + 19^y = z^2$ *and* $3^x + 91^y = z^2$, Int. J. Math. Sci. Comp., 3 (2013), 301-304.

[9] B. Sroysang, *On the Diophantine equation* $31^x + 32^y = z^2$, Int. J. Pure Appl. Math., 81 (2012), 609-612.

[10] B. Sroysang, *On the Diophantine equation* $7^x + 8^y = z^2$, Int. J. Pure Appl. Math., 84 (2013), 111-114.

Accepted: May 17, 2024