On the solutions of the Diophantine equation $M^x + (M-1)^y = z^2$

William S. Gayo, Jr.[*]
General Education Department
College of Arts and Sciences
Don Mariano Marcos Memorial State
University-North La Union Campus
Bacnotan, La Union 2515
Philippines
wsgayo2@up.edu.ph

Jerico B. Bacani
Department of Mathematics and Computer Science
College of Science
University of the Philippines Baguio
Baguio City 2600, Benguet
Philippines
jbbacani@up.edu.ph

Abstract. A Mersenne prime M is a prime number of the form $2^p - 1$, where p is also a prime number. In this study, we consider the Mersenne prime-involved exponential Diophantine equation $M^x + (M-1)^y = z^2$. The main goal is to find the complete set of solutions of the given Diophantine equation in non-negative integers x, y and z. Though it is not yet known whether there are infinitely many Mersenne primes, we have proven that the equation under consideration has only finitely many solutions. The proof uses techniques on quadratic congruence, factorization and modular arithmetic.
Keywords: Mersenne primes, exponential diophantine equation, quadratic residue, non-negative integer solutions.

1. Introduction

Number theory is considered as the Queen of Mathematics and one of the precious jewels on its crown is the family of Diophantine equations. Diophantine equations are simply equations with the condition that only integer solutions are required. They come in different forms. The simplest type is the two-variable linear Diophantine equation $ax + by = c$, where x and y are the unknowns and the rest of the parameters are integer constants. There is also the class of exponential Diophantine equations, wherein the exponents are the unknowns. Recently, exponential Diophantine equations of the form $a^x + b^y = z^2$ are widely studied. Researchers study these equations in connection with several prime pairs, such as the twin primes, sexy primes and cousin primes. The literature

∗. Corresponding author

contains a large number of published articles (cf. [1], [2], [3], [4], [5], [6] and [7].) In this work, we consider the exponential Diophantine equation

$$M^x + (M-1)^y = z^2, \tag{1}$$

where M is a Mersenne prime. It is conjectured that there are infinitely many Mersenne primes but as of now, there are only 51 Mersenne primes being discovered. The search for other Mersenne primes is still an active research area. Fortunately, we have shown that no large Mersenne primes that satisfy equation (1). More precisely, we found out that there are only a finite number of solutions to (1).

2. Preliminaries

The following definitions, lemmas and a theorem are needed for the main result of this study.

Definition 2.1. *A Mersenne prime is a prime number of the form* $2^p - 1$*, where* p *is also a prime number.*

Lemma 2.1. *For all Mersenne primes* $M > 3$*, the congruence* $M \equiv 7 \pmod 8$ *always hold.*

Proof. From $M > 3$, we get $2^p - 1 > 3$. It follows that $p > 2$ and thus, $2^p \equiv 0 \pmod 8$. This yields to $M = 2^p - 1 \equiv -1 \pmod 8$ which is equivalent to $M \equiv 7 \pmod 8$. □

Definition 2.2. *Let* p *be an odd prime and* $\gcd(a,p) = 1$*. If the quadratic congruence* $z^2 \equiv a \pmod p$ *has a solution, then* a *is said to be a quadratic residue of* p*. Otherwise,* a *is called a quadratic nonresidue of* p*.*

Lemma 2.2 (Euler's criterion)**.** *Let* p *be an odd prime and* $\gcd(a,p) = 1$*. Then,* a *is a quadratic residue of* p *if and only if* $a^{(p-1)/2} \equiv 1 \pmod p$*.*

Lemma 2.3 ([8])**.** *The Diophantine equation* $3^x + 2^y = z^2$ *has exactly three nonnegative integer solutions* (x,y,z)*, namely,* $(1,0,2)$*,* $(0,3,3)$*,* $(2,4,5)$*.*

Theorem 2.1 (Mihailescu's Theorem [9])**.** *The quadruple* $(3,2,2,3)$ *is the unique solution 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

We now state the main result which is about the solutions of the Diophantine equation (1).

Theorem 3.1. *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.*

Proof. The proof is divided into two cases for the Mersenne prime M.

Case 1. If $M = 3$, then equation (1) becomes

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

By Lemma 2.3, equation (2) has exactly three solutions (x, y, z), which are $(1, 0, 2)$, $(0, 3, 3)$ and $(2, 4, 5)$. Thus, the quadruples in the set

$$\{M, x, y, z\} = \{(3, 1, 0, 2), (3, 0, 3, 3), (3, 2, 4, 5)\}$$

are solutions of equation (1).

Case 2. For $M > 3$, we consider two cases for the exponent y.

Subcase 2.1. If y is even, let $y = 2t$ for some integer $t \geq 0$. Then, equation (1) becomes

$$M^x + (M-1)^{2t} = z^2.$$

This can be expressed as $M^x = z^2 - (M-1)^{2t} = (z + (M-1)^t)(z - (M-1)^t)$. There exist nonnegative integers α and β with $\alpha + \beta = x$ and $\alpha > \beta$ such that $z + (M-1)^t = M^\alpha$ and $z - (M-1)^t = M^\beta$. Combining these two equations leads to $2(M-1)^t = M^\alpha - M^\beta$. By factoring out M^β, we get $2(M-1)^t = M^\beta(M^{\alpha-\beta} - 1)$. Since M is an odd prime and $\gcd(M, M-1) = 1$, it follows that

$$\begin{cases} M^\beta = 1, \\ M^{\alpha-\beta} - 1 = 2(M-1)^t. \end{cases} \tag{3}$$

From the first equation of the system (3), it can be implied that $\beta = 0$. Hence, $\alpha = x > 0$ and $z = (M-1)^t + 1$. The second equation of the system (3) becomes

$$M^x - 1 = 2(M-1)^t.$$

Note that $M^x - 1 \equiv -1 \pmod{M}$, and $2(M-1)^t \equiv 2(-1)^t \pmod{M}$. These two congruences imply that $M^x - 1 = -1 + nM$ and $2(M-1)^t = 2(-1)^t + mM$ for some integers m and n. Thus,

$$-1 + nM = 2(-1)^t + mM. \tag{4}$$

If t is odd, then equation (4) becomes $-1+nM = -2+mM$ which can be written as $M(n-m) = -1$. But this impossible because $M > 3$. On the other hand, if t is even, then equation (4) becomes $-1 + nM = 2 + mM$ which is equivalent to $M(m - n) = 3$. This means that $M = 3$, which contradicts the assumption that $M > 3$. Thus, equation (1) has no solution for even y and $M > 3$.

Subcase 2.2. If y is odd, then $M^x + (M-1)^y \equiv -1 \pmod{M}$ for positive integer x; hence $z^2 \equiv -1 \pmod{M}$. Since $M > 3$, it follows that $M \equiv 7 \pmod{8}$ by Lemma 2.1. So, there exists an integer m such that $M = 8m + 7$. Using Euler's criterion, $(-1)^{(M-1)/2} = (-1)^{(8m+6)/2} = (-1)^{4m+3} = -1$. Hence, -1 is a quadratic nonresidue of M. This means that quadratic congruence

$z^2 \equiv -1 \pmod{M}$ has no solution and so does the equation (1) for positive integer x, odd integer y and $M > 3$. For the case when $x = 0$, the equation (1) becomes $1 + (M-1)^y = z^2$. By Mihailescu's Theorem, $M = 3, y = 3$ and $z = 3$. This is a contradiction to $M > 3$. Hence, equation (1) has no solution for odd integer y and $M > 3$.

To sum up all the cases, the Diophantine equation (1) has exactly three nonnegative solutions (M, x, y, z) which are $(3, 1, 0, 2), (3, 0, 3, 3)$ and $(3, 2, 4, 5)$. □

Corollary 3.1. *The quintuples* $(3, 1, 0, 2, 1), (3, 0, 3, 3, 1)$ *and* $(3, 2, 4, 5, 1)$ *are the only nonnegative integer solutions* (M, x, y, z, n) *of the exponential Diophantine equation* $M^x + (M-1)^y = z^{2n}$, *where* M *is a Mersenne prime and* n *is a natural number.*

Proof. Let x, y and z be nonnegative integers, n be natural number, and M be a Mersenne prime such that $M^x + (M-1)^y = (z^n)^2$. By Theorem 3.1, we can see that $(M, x, y, z^n) = (3, 1, 0, 2), (3, 0, 3, 3)$ and $(3, 2, 4, 5)$. By the primality of $2, 3$ and 5, we get $n = 1$. Thus, the have the solutions $(3, 1, 0, 2, 1), (3, 0, 3, 3, 1)$ and $(3, 2, 4, 5, 1)$. □

4. Concluding remarks

In this study, we have proven that there are exactly three nonnegative integer solutions of the Diophantine equation (1), and these solutions exist only for the Mersenne prime $M = 3$. For other Mersenne primes larger than 3, the equation (1) will have no solution. A list of some exponential Diophantine equations with no solutions in the set of nonnegative integers is given in Table 1.

Table 1: List of Some Exponential Diophantine Equations of the Form $M^x + (M-1)^y = z^2$ with No Solution

1.) $7^x + 6^y = z^2$	6.) $(2^{19} - 1)^x + (2^{19} - 2)^y = z^2$
2.) $31^x + 30^y = z^2$	7.) $(2^{31} - 1)^x + (2^{31} - 2)^y = z^2$
3.) $127^x + 126^y = z^2$	8.) $(2^{61} - 1)^x + (2^{61} - 2)^y = z^2$
4.) $8191^x + 8190^y = z^2$	9.) $(2^{89} - 1)^x + (2^{89} - 2)^y = z^2$
5.) $131071^x + 131070^y = z^2$	10.) $(2^{107} - 1)^x + (2^{107} - 2)^y = z^2$

Acknowledgment

The authors would like to thank the University of the Philippines Baguio for the support, and the referees for their valuable comments.

References

[1] B. Sroysang, *On the Diophantine equation* $3^x + 5^y = z^2$, Int. J. Pure Appl. Math., 81 (2012), 605-608.

[2] B. Sroysang, *On the Diophantine equation* $5^x + 7^y = z^2$, Int. J. Pure Appl. Math., 89 (2013), 115-118.

[3] J.F.T. Rabago, *A note on two Diophantine equations* $17^x + 19^y = z^2$ *and* $71^x + 73^y = z^2$, Math. J. Interdisciplinary Sci., 2 (2013), 19-24.

[4] 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, Int. J. Pure Appl. Math., 104 (2013), 517-521.

[5] 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 (2018), 241-244.

[6] S. Kumar, S. Gutpa, H. Kishan, *On the non-linear Diophantine equations* $61^x + 67^y = z^2$ *and* $67^x + 73^y = z^2$, Annals of Pure and Applied Mathematics, 16 (2018), 91-94.

[7] N. Burshtein, *On solutions to the Diophantine equations* $5^x + 103^y = z^2$ *and* $5^x + 11^y = z^2$ *with positive integers* x, y, z, Annals of Pure and Applied Mathematics, 19 (2019), 75-77.

[8] B. Sroysang, *More on the Diophantine equation* $2^x + 3^y = z^2$, Int. J. Pure Appl. Math., 84 (2013), 133-137.

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

Accepted: January 13, 2021