Annals of Pure and Applied Mathematics
Vol. 16, No. 2, 2018, 471-477
ISSN: 2279-087X (P), 2279-0888(online)
Published on 29 March 2018
www.researchmathsci.org
DOI: http://dx.doi.org/10.22457/apam.v16n2a25

Annals of Pure and Applied Mathematics

Solutions of the Diophantine Equation $2^x + p^y = z^2$ When p is Prime

Nechemia Burshtein

117 Arlozorov Street, Tel Aviv 6209814, Israel
Email: anb17@netvision.net.il

Received 16 March 2018; accepted 29 March 2018

Abstract. In this article, we consider the Diophantine equation $2^x + p^y = z^2$ when $p = 4N + 3$ and $p = 4N + 1$ are primes. The values x, y, z are positive integers. For each prime, all the possibilities for solutions are investigated. All cases of no-solutions, as well as cases of infinitely many solutions are determined. Whenever the number of solutions for $p = 4N + 3$ / $p = 4N + 1$ is finite, we establish the respective connection between this number to all Mersenne Primes / Fermat Primes known as of 2018. Numerical solutions of various cases are also exhibited.

Keywords: Diophantine equations, Catalan's Conjecture, Mersenne, Fermat Primes

AMS Mathematics Subject Classification (2010): 11D61

1. Introduction

The field of Diophantine equations is ancient, vast, and no general method exists to decide whether a given Diophantine equation has any solutions, or how many solutions. In most cases, we are reduced to study individual equations, rather than classes of equations.

The literature contains a very large number of articles on non-linear such individual equations involving primes and powers of all kinds. Among them are for example [1, 5, 9, 10].

The famous general equation

$$p^x + q^y = z^2$$

has many forms, in particular when $p = 2$ [2, 3, 9, 11].

In this article we consider the equation

$$2^x + p^y = z^2, \tag{1}$$

and in our discussion, we utilize Catalan's Conjecture, Mersenne Primes and Fermat Primes.

In 1844 E. C. Catalan conjectured: The only solution in integers $r > 0$, $s > 0$, $a > 1$, $b > 1$ of the equation

$$r^a - s^b = 1$$

is $r = b = 3$ and $s = a = 2$.

The conjecture was proven by P. Mihăilescu [6] in 2002.

The interest in numbers $2^n - 1$ being primes dates to antiquity. When n is composite, $2^n - 1$ is not a prime. In 1644, Mersenne published a list of 11 primes for which he claimed that $2^n - 1$ is a prime. The first Mersenne Primes [4] are 3, 7, 31, 127. The condition that n be a prime is a necessary but not a sufficient condition for the primality of $2^n - 1$ ($2^{11} - 1 = 2047 = 23 \cdot 89$). The search for primes n for which $2^n - 1$ is a prime continued over the years. On January 3, 2018 the largest 50th known Mersenne Prime $2^{77,232,917} - 1$ was discovered by GIMPS [4]. It has 23,249,425 digits and is the largest prime known to mankind [4].

A Fermat Prime is a prime of the form $2^n + 1$ where n is a power of 2. As of 2018 [12], only five Fermat Primes are known. For $n = 1, 2, 4, 8, 16$, these primes are $\{3, 5, 17, 257, 65537\}$.

In Section 2 we find all the solutions of $2^x + p^y = z^2$ when $p = 4N + 3$ is prime. In Section 3 we find solutions of the above equation when $p = 4N + 1$ is prime.

2. All the solutions of $2^x + p^y = z^2$ when $p = 4N + 3$ is prime

In this section, we discuss all the cases of equation (1) when $p = 4N + 3$ is prime. In each case, we determine all the solutions. This is done in Theorems 2.1 and Theorem 2.2 which are self-contained. We also demonstrate some numerical solutions.

Theorem 2.1. Suppose that $p = 4N + 3$ $(N \geq 0)$ is prime. If $y = 2n + 1$ is odd in $2^x + p^y = z^2$, then:

(a) For $x = 1$ and $y = 1$ $(n = 0)$, equation (1) has infinitely many solutions.

(b) For $x = 1$ and $y > 1$, equation (1) has no solutions.

(c) For $x > 1$ and $y \geq 1$, equation (1) has no solutions.

Proof: In $2^x + p^y = z^2$ the integer z^2 is odd, hence z is odd. Denote $z = 2U + 1$. Then $z^2 = (2U + 1)^2 = 4U(U + 1) + 1$.

(a) Suppose that $x = 1$ and $y = 1$. We have from equation (1)

$$2 + p = z^2. \qquad (2)$$

From equation (2) we then obtain

$$2 + (4N + 3) = 4U(U + 1) + 1 = z^2.$$

Thus, $p = 4N + 3 = 4U(U + 1) - 1$. Evidently, equation (2) is now

$$2 + (4U(U + 1) - 1) = (2U + 1)^2$$

an identity valid for infinitely many values $U \geq 1$. Hence, equation (2) has infinitely many solutions as asserted.

For the first five values $U = 1, 2, 3, 4, 6$, and the convenience of the readers, we exhibit the five solutions of equation (2) as follows:

Solution 1. $2^1 + 7^1 = 3^2$.
Solution 2. $2^1 + 23^1 = 5^2$.
Solution 3. $2^1 + 47^1 = 7^2$.
Solution 4. $2^1 + 79^1 = 9^2$.
Solution 5. $2^1 + 167^1 = 13^2$.

We note that Solution 1 has already been obtained in [3].

(b) Suppose that $x = 1$ and $y > 1$ is odd. The equation $2^x + p^y = z^2$ is

$$2 + p^y = z^2. \qquad (3)$$

From (3) it follows that $p^y + 1 = z^2 - 1 = 4U(U + 1)$ or

$$p^{2n+1} + 1 = 4U(U + 1), \qquad n \geq 1. \qquad (4)$$

Equality (4) yields

$$p^{2n+1} + 1^{2n+1} = (p + 1)(p^{2n} - p^{2n-1} \cdot 1^1 + \cdots + 1^{2n}) = 4U(U + 1). \qquad (5)$$

In (5), the factor $(p^{2n} - p^{2n-1} \cdot 1^1 + \cdots + 1^{2n})$ is odd for all values p. Therefore $4 \mid (p + 1)$, and hence from (5)

$$(N + 1)((4N + 3)^{2n} - (4N + 3)^{2n-1} \cdot 1^1 + \cdots + 1^{2n}) = U(U + 1). \qquad (6)$$

The even term $U(U + 1)$ in (6) is the product of two consecutive integers, and hence N is odd. It is seen that equality (6) does not hold.

Therefore, equation (3) has no solutions when $y > 1$ is odd.

(c) Suppose that $x > 1$ and $y \geq 1$ is odd. Then $2^x + p^y = z^2$ is

$$2^x + p^{2n+1} = z^2, \qquad n \geq 0. \qquad (7)$$

For all integers $x > 1$, $2^x = 4 \cdot 2^{x-2}$. The integer z^2 has the form $4T + 1$. It is easily verified for every value $n \geq 0$, that p^{2n+1} is of the form $4M + 3$.

In (7), the left-hand side has the form

$$2^x + p^{2n+1} = 4 \cdot 2^{x-2} + (4M + 3) = 4(2^{x-2} + M) + 3,$$

whereas the right-hand side of (7) is of the form

$$z^2 = 4T + 1.$$

The two sides of equation (7) contradict each other. Therefore, for each prime p, there do not exist integers x, y and z which satisfy equation (1).

This concludes the proof of Theorem 2.1. □

Theorem 2.2. Suppose that $p = 4N + 3$ $(N \geq 0)$ is prime. If in $2^x + p^y = z^2$ $y = 2n$ is even, then:

(a) For $n = 1$, equation (1) has 50 solutions.

(b) For $n > 1$, equation (1) has no solutions.

Proof: Equation (1) is now

$$2^x + p^{2n} = z^2, \qquad n \geq 1. \qquad (8)$$

From (8) we obtain

$$2^x = z^2 - p^{2n} = z^2 - (p^n)^2 = (z - p^n)(z + p^n).$$

Denote

$$z - p^n = 2^\alpha, \qquad z + p^n = 2^\beta, \qquad \alpha < \beta, \qquad \alpha + \beta = x. \qquad (9)$$

Hence from (9)

$$2 p^n = 2^\beta - 2^\alpha = 2^\alpha (2^{\beta-\alpha} - 1). \qquad (10)$$

It clearly follows from (10) that $\alpha = 1$, and therefore

$$2^{\beta-1} - 1 = p^n. \qquad (11)$$

(a) Suppose that $n = 1$. Then (11) yields $2^{\beta-1} - 1 = p$ which may be a Mersenne Prime. Every Mersenne Prime is of the form $4N + 3$ as required by our supposition, and therefore is a solution of equation (1). It is known [4], that there are 50 Mersenne Primes, of which by January 2018 the largest is equal to $p = 2^{77,232,917} - 1$ being the

50th prime. Hence, equation (1) has 50 solutions up to $2^{77,232,917} – 1$ inclusive, as asserted. Each such solution is of the form $2^{1+\beta} + (2^{\beta-1} – 1)^2 = z^2$.

For the convenience of the readers, we demonstrate the first three solutions of equation (8) when $n = 1$.

Solution 6. ($\beta – 1 = 2$, $p = 3$) $2^4 + 3^2 = 5^2$.
Solution 7. ($\beta – 1 = 3$, $p = 7$) $2^5 + 7^2 = 9^2$.
Solution 8. ($\beta – 1 = 5$, $p = 31$) $2^7 + 31^2 = 33^2$.

We remark that Solution 7 has already been obtained in [2].

(b) Suppose that $n > 1$. It clearly follows from (11) that $\beta – 1 > 1$. Therefore, by Catalan's Conjecture the equation $2^{\beta-1} – p^n = 1$ has no solutions. Thus, for all values $n > 1$ equation (1) has no solutions as asserted.

This concludes the proof of Theorem 2.2. □

Concluding remark. It is now known that there exist 50 Mersenne Primes. In Theorem 2.2 part **(a)**, when $y = 2$ and p is a Mersenne Prime, it has been established that $2^x + p^2 = z^2$ has exactly 50 known solutions. Almost all of these solutions are achieved by a computer. Additional solutions of the above equation solely depend on finding more Mersenne Primes.

3. Solutions of $2^x + p^y = z^2$ when $p = 4N + 1$ is prime

In this section, $p = 4N + 1$ is prime, and all cases of equation (1) are considered. This is done in the following Theorems 3.1 – 3.3 each of which is self-contained. Numerical solutions are also exhibited.

Theorem 3.1. Suppose that $p = 4N + 1$ is prime. If $y = 2n$ is even in $2^x + p^y = z^2$, then for all values x, the equation

$$2^x + p^{2n} = z^2, \qquad n \geq 1 \tag{12}$$

has no solutions.

Proof: In $2^x + p^y = z^2$ the integer z^2 is odd, hence z is odd. Denote $z = 2U + 1$. Then $z^2 = (2U + 1)^2 = 4U(U + 1) + 1$.

From (12) we have

$$2^x = z^2 - p^{2n} = z^2 - (p^n)^2 = (z - p^n)(z + p^n).$$

Denote

$$z – p^n = 2^\alpha, \qquad z + p^n = 2^\beta, \qquad \alpha < \beta, \qquad \alpha + \beta = x. \tag{13}$$

From (13) it follows that

$$2 \cdot p^n = 2^\beta - 2^\alpha = 2^\alpha (2^{\beta-\alpha} – 1). \tag{14}$$

Equality (14) implies that $\alpha = 1$. Thus (14) yields

$$p^n = 2^{\beta-1} – 1. \tag{15}$$

By (13) $\beta > \alpha = 1$, and from (15) $\beta = 2$ is impossible. Thus $\beta > 2$. Since

$p = 4N + 1$, therefore for each and every $n \geq 1$, p^n is of the form $4M + 1$. For all values $\beta > 2$, the right-hand side of (15) is of the form $4V + 3$. The two sides of (15) contradict each other, and therefore (15) is impossible.

Hence, equation (12) has no solutions as asserted. □

Theorem 3.2. Suppose that $p = 4N + 1$ is prime. If in $2^x + p^y = z^2$ $x = 2t$ is even and $y = 2n + 1$ is odd, then the equation

$$2^{2t} + p^{2n+1} = z^2, \qquad t \geq 1, \qquad n \geq 0 \tag{16}$$

has:

(a) No solutions for all values $n \geq 1$.

(b) 4 solutions when $n = 0$.

Proof: **(a)** Suppose that $n \geq 1$. From (16) we obtain

$$p^{2n+1} = z^2 - 2^{2t} = z^2 - (2^t)^2 = (z - 2^t)(z + 2^t).$$

Denote

$$z - 2^t = p^\alpha, \qquad z + 2^t = p^\beta, \qquad \alpha < \beta, \qquad \alpha + \beta = 2n + 1. \tag{17}$$

From (17) it follows that

$$2 \cdot 2^t = p^\beta - p^\alpha = p^\alpha (p^{\beta-\alpha} - 1). \tag{18}$$

Equality (18) implies that $\alpha = 0$, and hence (18) yields

$$2^{t+1} = p^\beta - 1. \tag{19}$$

From (19) and Catalan's Conjecture, $p^\beta - 2^{t+1} = 1$ has the only solution $p = 3$ ($\beta = 2$, $t = 2$). But $p = 3$ is not of the form $4N + 1$. Therefore, for all values t, $n \geq 1$ and $p = 4N + 1$, the equation $2^{2t} + p^{2n+1} = z^2$ has no solutions.

This completes the proof of part **(a)**.

(b) Suppose that $n = 0$. When $\alpha = 0$ in (17) then $\beta = 1$. Therefore (19) yields

$$2^{t+1} + 1 = p. \tag{20}$$

In (20), the prime p is known as Fermat Prime, where $(t + 1)$ must be a power of 2. To the present day [12], only five Fermat Primes are known. These are

$$\{3, 5, 17, 257, 65537\}.$$

The prime $p = 3$ cannot be used in (16), since it is not of the form $p = 4N + 1$. Note that for all $t \geq 1$, the prime p in (20) is of the form $4N + 1$. Thus, any Fermat Prime > 3 is a solution of (16). Therefore, when $t \geq 1$, $n = 0$ and $p = 4N + 1$, the equation $2^{2t} + p^{2n+1} = z^2$ has only 4 solutions.

The 4 solutions are presented as follows.

Solution 9.	2^2	+	5^1	=	3^2.
Solution 10.	2^6	+	17^1	=	9^2.
Solution 11.	2^{14}	+	257^1	=	129^2.
Solution 12.	2^{30}	+	65537^1	=	32769^2.

This concludes the proof of Theorem 3.2. □

Theorem 3.3. Suppose that $p = 4N + 1$ is prime. If in $2^x + p^y = z^2$ $x = 2t + 1$ is odd and $y = 2n + 1$ is odd, then the equation

$$2^{2t+1} + p^{2n+1} = z^2, \qquad t \geq 0, \qquad n \geq 0 \qquad (21)$$

has:

(a) No solutions when $t = 0$ and $n = 0$.

(b) Infinitely many solutions when $t \geq 1$ and $n = 0$.

(c) No solutions when $t = 0$ and $n \geq 1$.

(d) At least one solution when $t \geq 1$ and $n \geq 1$.

Proof: **(a)** Suppose that $t = 0$ and $n = 0$. From (21) we obtain

$$2^1 + p^1 = 2 + (4N + 1) = 4N + 3 = z^2$$

which is impossible since z^2 is odd and has the form $z^2 = 4T + 1$. In case **(a)**, equation (21) has no solutions as asserted.

(b) Suppose that $t \geq 1$ and $n = 0$. It is then easily seen that infinitely many solutions of (21) exist. Some of these are demonstrated here.

Solution 13. $2^3 + 17^1 = 5^2$.

Solution 14. $2^5 + 89^1 = 11^2$.

Solution 15. $2^7 + 41^1 = 13^2$.

Solution 16. $2^9 + 113^1 = 25^2$.

Solution 17. $2^{11} + 353^1 = 49^2$.

It is noted that more than one solution may exist for a value t. For instance: $2^3 + 41^1 = 7^2$, $2^7 + 97^1 = 15^2$, and so on. Case **(b)** is complete.

(c) Suppose that $t = 0$ and $n \geq 1$. We have from (21)

$$2^1 + p^{2n+1} = z^2. \qquad (22)$$

The form of z^2 is equal to $4T + 1$, and for all $n \geq 1$, p^{2n+1} has the form $4M + 1$. Then, the left-hand side of (22) is of the form $4M + 3$, whereas the right-hand side has the form $4T + 1$. This contradicts the existence of (22). Hence, the equation $2 + p^{2n+1} = z^2$ has no solutions as asserted.

(d) Suppose that $t \geq 1$ and $n \geq 1$. We obtain

$$2^{2t+1} + p^{2n+1} = z^2, \qquad t \geq 1, \qquad n \geq 1. \qquad (23)$$

Then $2^{2t+1} = 4 \cdot 2^{2t-1}$, $p^{2n+1} = (4N + 1)^{2n+1}$, and z^2 equals to $4U(U + 1) + 1$. By the Binomial Theorem, the expansion of $(4N + 1)^{2n+1}$ has $(2n + 2)$ terms. The first $(2n + 1)$ terms are each a multiple of $(4N)$, the $(2n + 2)^{\text{th}}$ term is equal to 1. Denote the sum of the $(2n + 1)$ terms by $(4N)M$ where M is odd. Then, from (23) we have

$$4 \cdot 2^{2t-1} + (4N)M + 1 = 4U(U + 1) + 1$$

which after simplifications yields

$$2^{2t-1} + NM = U(U + 1). \qquad (24)$$

The value $U(U + 1)$ is a product of two consecutive integers and is even. Therefore, N is even and denote $N = 2R$, $U(U + 1) = 2W$. From (24) we then obtain

$$2^{2t-2} + RM = W. \qquad (25)$$

In (25), if $t > 1$ then R and W are of the same parity, whereas when $t = 1$, R and W are of a different parity. The process of finding solutions from here on presents great difficulties, and we shall not pursue this matter any further.

However, the following values $t = 3$, $p = 17$, $n = 1$, $z = 71$ when substituted in (23) yield the solution:

Solution 18. $2^7 + 17^3 = 71^2$.

Equivalently, we then have in (25)

$$2^{2t-2} = 2^4, \quad R = 2, \quad M = 307, \quad W = 630.$$

The proof of Theorem 3.3 is now complete. □

Concluding remark. It is noted that $p = 17$ is the third known Fermat Prime. The first Fermat Prime 3 is not of the form $4N + 1$. For the second Fermat Prime 5, all powers of 5 have a last digit equal to 5. When added an odd power of 2 whose last digit is either 2 or 8, it follows that in $2^{2t+1} + 5^{2n+1} = z^2$, z^2 has a last digit which is respectively either 7 or 3. Since a square never has a last digit which is either 7 or 3, it follows that the above equation has no solutions.

A solution of $2^{2t+1} + p^{2n+1} = z^2$ if such exists with either Fermat Prime 257 or 65537 requires the aid of a computer. Moreover, from [12], finding more Fermat Primes has a very low expectation.

Conjecture. Except for $p = 5, 17$, for all other primes p either Fermat Primes or not, we conjecture that no solutions exist for $2^{2t+1} + p^{2n+1} = z^2$ when $t \geq 1$, $n \geq 1$.

If indeed the answer is affirmative, then the above equation has exactly one solution when $p = 17$, namely Solution 18. Moreover, it then follows in Section 3 that all the solutions of $2^x + p^y = z^2$ when $p = 4N + 1$ have been established.

REFERENCES

1. N. Burshtein, On the diophantine equation $p^x + q^y = z^2$, *Annals of Pure and Applied Mathematics*, 13 (2) (2017) 229 – 233.
2. N.Burshtein, On the diophantine equation $2^{2x+1} + 7^y = z^2$, *Annals of Pure and Applied Mathematics*, 16 (1) (2018) 177 – 179.
3. N.Burshtein, All the solutions to an open problem of S. Chotchaisthit on the diophantine equation $2^x + p^y = z^2$ when p are particular primes and $y = 1$, *Annals of Pure and Applied Mathematics*, 16 (1) (2018) 31 – 35.
4. GIMPS Great Internet Mersenne Prime Search, GIMPS Finding World Record Primes.
5. Md.A.A.Khan, A.Rashid and Md. S.Uddin, Non-negative integer solutions of two diophantine equations $2^x + 9^y = z^2$ and $5^x + 9^y = z^2$, *Journal of Applied Mathematics and Physics*, 4 (2016) 762 – 765.
6. P.Mihăilescu, Primary cyclotomic units and a proof of Catalan's conjecture, *J. Reine Angew. Math*. 572 (2004) 167 – 195.
7. B.Poonen, Some diophantine equations of the form $x^n + y^n = z^m$, *Acta Arith*., 86 (1998) 193–205.
8. B.Sroysang, On the diophantine equation $5^x + 7^y = z^2$, *Int. J. Pure Appl. Math*., 89 (2013) 115–118.
9. B.Sroysang, More on the diophantine equation $8^x + 19^y = z^2$, *Int. J. Pure Appl. Math*., 81 (4) (2012) 601 – 604.
10. A.Suvarnamani, On the diophantine equation $p^x + (p+1)^y = z^2$, *Int. J. Pure Appl. Math*., 94 (5) (2014) 689 – 692.
11. A.Suvarnamani, A.Singta and S.Chotchaisthit, On two diophantine equations $4^x + 7^y = z^2$ and $4^x + 11^y = z^2$, *Sci. Techno. RMUTT J*., 1 (1) (2011) 25–28.
12. Wolfram MathWorld, Fermat Prime.