Annals of Pure and Applied Mathematics
Vol. 13, No. 1, 2017, 143-149
ISSN: 2279-087X (P), 2279-0888(online)
Published on 22 March 2017
www.researchmathsci.org
DOI: http://dx.doi.org/10.22457/apam.v13n1a14

Annals of **Pure and Applied Mathematics**

On Solutions of the Diophantine Equation $p^x + q^y = z^2$

Nechemia Burshtein

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

Received 28 February 2017; accepted 14 March 2017

Abstract. Two odd primes $p < q$ differ by an even value k. The values $k = 2, 4, 6, 8,$ and some particular values of $k > 8$ are investigated for solutions and no-solution cases of the title equation. All of these are established and exhibited.

Keywords: Diophantine equations, Twin primes, Sophie Germain primes

AMS Mathematics Subject Classification (2010): 11D61

1. Introduction

The history of Diophantine Equations dates back to antiquity. There are endless varieties of Diophantine Equations, and there is no general method of solution. It is often asked how big are the gaps between two consecutive primes. These gaps get larger and larger since the density of primes approaches zero in accordance with the prime number theorem. Many articles have been written on this subject, and a very small fraction of them in [4, 5] is given here.

In this article, we wish to solve the equation

$$p^x + q^y = z^2 \qquad (1)$$

in positive integers, and in particular when p, q are odd primes. The literature contains a very large number of articles with various equations involving primes and powers of all kinds. Among them are for example [7, 8, 9] which relate to (1).

Let k denote the gap between p and q in (1), i.e., $p + k = q$. Many examples correspond to (1) in which $k > 2$ and $x \ge 1$, such as:

$$3^1 + 13^1 = 4^2, \quad 3^2 + 7^1 = 4^2, \quad 3^3 + 73^1 = 10^2, \quad 3^4 + 19^1 = 10^2, \quad 3^5 + 13^1 = 16^2.$$

Therefore, in Section 2 we shall restrict ourselves to equation (1) when $x = y = 1$. The values $k = 2, 4, 6, 8,$ and some values $k > 8$ are investigated. Solutions, and also cases where (1) has no solutions are demonstrated. In Section 3, when $k > 8$ and $x > 1$, a certain type of solutions to (1) is introduced.

2. The values $k = 2, 4, 6, 8$, and some general cases of k

We consider the value $k = 2$ in Lemma 2.1, the values $k = 4, 8$ in Lemma 2.2, and the value $k = 6$ in Lemma 2.3. When $k > 8$, some general cases are established in Lemma 2.2 and Corollary 2.1.

In (1) suppose that: $p < q$ are odd primes, $k = 2$, and $x = y = 1$.

All odd integers are of the form $6N + 1, 6N + 3, 6N + 5$ where $N \ge 0$. When $N = 0$, we have in (1): $p = 3$, $q = 5$, but $8 \ne z^2$. Therefore $N > 0$. For all values of $N > 0$, the pairs with $k = 2$ such as $(6N + 1, 6N + 3)$ and $(6N + 3, 6N + 5)$ are impossible since $6N + 3$ is not prime. The only possible pairs of primes with $k = 2$ are then of the form $(6N + 5, 6(N + 1) + 1)$, or simply $(6N + 5, 6N + 7)$.

In Lemma 2.1, we establish the values of N, $6N + 5$, $6N + 7$, z, which may satisfy (1) when p, q are primes.

Lemma 2.1. Suppose that $x = y = 1$ in (1), and N, R are positive integers. If

$$(6N + 5) + (6N + 7) = z^2, \qquad (2)$$

then

(i) $N = 3R^2 – 1$,

(ii) $6N + 5 = 18R^2 - 1, \quad 6N + 7 = 18R^2 + 1$,

(iii) $z = 6R$.

Proof: From (2) it follows that

$$(6N + 5) + (6N + 7) = 12(N + 1) = z^2$$

implying that z^2 is even, thus z is even, and also a multiple of 3. Hence, $z = 6R$ which proves (iii). Then, $12(N + 1) = 36R^2$ or $N + 1 = 3R^2$, and $N = 3R^2 - 1$ yields (i). Substituting $N = 3R^2 - 1$ into $6N + 5$ and $6N + 7$ results in

$$6N + 5 = 18R^2 – 1, \qquad 6N + 7 = 18R^2 + 1$$

as in (ii).

This completes our proof.

Remark 2.1. It is noted, that clearly Lemma 2.1 can not guarantee that $6N + 5$, $6N + 7$ are both primes. However, it does guarantee that for each value of R when $R = 1, 2, \ldots$, the right-hand side of (2) is indeed always a square. This is shown in Table 1.

For each fixed value N, the two integers $6N + 5$, $6N + 7$ may assume one of four possibilities, namely: the possibility of two primes, two composites, and composite/prime being interchanged. This is demonstrated in the following Table 1 when $R = 2, 3, 4, 5$.

Table 1.

R	$18R^2 - 1 = 6N + 5$		$18R^2 + 1 = 6N + 7$		z^2	$6R = z$
1	17	prime	19	prime	36	6
2	71	prime	73	prime	144	12
3	$161 = 7·23$	composite	163	prime	324	18
4	$287 = 7·41$	composite	$289 = 17^2$	composite	576	24
5	449	prime	$451 = 11·41$	composite	900	30

We now conclude the case $k = 2$ in the following Remark 2.2.

Remark 2.2. If in (1) $x = y = 1$, and p, q are substituted respectively by $6N + 5$ and $6N + 7$, then by Lemma 2.1 it follows that for each value $R \ge 1$, (1) has one and only one solution in positive integers namely:

$$(p, q, x, y, z) = (18R^2 – 1, 18R^2 + 1, 1, 1, 6R).$$

In particular, this is true when $p = 18R^2 – 1$, $q = 18R^2 + 1$, p, q are primes and $q = p + 2$ (twin primes). Clearly, if the twin primes conjecture is true, i.e., there exist infinitely many primes p and $p + 2$, then for each such prime $p = 18R^2 - 1$, (1) has a unique solution.

Lemma 2.2. Suppose that $x = y = 1$ in (1), and $p < q$ are odd primes. If $q = p + 2^n$ when $n \geq 2$ is an integer, then for each such value n, equation (1) has no solutions.

Proof: By (1) and our supposition, we have

$$p + q = p + (p + 2^n) = 2(p + 2^{n-1}) = z^2 \qquad (3)$$

implying that z is even, and z^2 is a multiple of 4. But, in (3) $2(p + 2^{n-1})$ is a multiple of 2, whereas z^2 is a multiple of 4. Therefore, when $k = 2^n$ and $n \geq 2$, (3) is impossible, and hence equation (1) has no solutions.

An extension of Lemma 2.2 for values of $k > 8$ is provided in the following Corollary 2.1.

Corollary 2.1. Suppose that $x = y = 1$ in (1), and $p < q$ are odd primes. Let $n \geq 2$, $M \geq 1$ be integers, and gcd $(p, 2M + 1) = 1$. If $k = (2M + 1)\cdot 2^n$, then equation (1) has no solutions.

Proof: By (1) and our supposition, we get

$$p + q = p + (p + (2M + 1)2^n) = 2(p + (2M + 1)2^{n-1}) = z^2 \qquad (4)$$

and therefore z is even, and z^2 is a multiple of 4. In (4), $2(p + (2M + 1)2^{n-1})$ is a multiple of 2, whereas z^2 is a multiple of 4. It then follows that (4) is impossible.

Thus, equation (1) has no solutions.

Remark 2.3. From Lemma 2.2 it follows that when $k = 4$ $(n = 2)$, $k = 8$ $(n = 3)$, and also larger values of k such as $k \geq 16$ $(n \geq 4)$, equation (1) has no solutions. Moreover, from Corollary 2.1 it follows that when $k = (2M + 1)\cdot 2^n \geq 12$, more no-solutions cases of equation (1) exist.

It is noted that every odd integer belongs exactly to one member of the set

$$\{10A + 1,\quad 10A + 3,\quad 10A + 5,\quad 10A + 7,\quad 10A + 9\}.$$

We shall apply this set in the following Lemma 2.3, in which we consider the case $k = 6$.

Lemma 2.3. Suppose that $x = y = 1$ in (1), and $p < q$ are odd primes such that $q = p + 6$.

(a) If p is of the form $10A + 1$, $10A + 3$, $10A + 9$, then (1) has no solutions.

(b) If p is of the form $10A + 5$, then (1) has exactly one solution.

(c) If p is of the form $10A + 7$ and $p < 10^5$, then (1) has exactly six solutions.

Proof: (a) Suppose $p = 10A + 1$ when $A \geq 1$.

Then $p + 6 = 10A + 7$, and $p + (p + 6) = 2p + 6 = 20A + 8 = 4(5A + 2) = z^2$ implying that $5A + 2$ must be a square in order to satisfy (1). But, all values of $5A + 2$ end either in the digit 2 or in the digit 7. Hence, $5A + 2$ is never a square. Thus, $p = 10A + 1$ when $A \geq 1$ does not yield solutions of (1).

Suppose $p = 10A + 3$ when $A \geq 0$.

When $A = 0$, then $p = 3$, but $p + 6 = 9$ is not prime. Therefore, let $A \geq 1$. Then $p + 6 = 10A + 9$, and $p + (p + 6) = 2p + 6 = 20A + 12 = 4(5A + 3) = z^2$ implying that $5A + 3$ must be a square in order to satisfy (1). Since all values of $5A + 3$ end either in the digit 3 or in the digit 8, it follows that $5A + 3$ is never a square. Hence, equation (1) has no solutions when $p = 10A + 3$ and $A \geq 0$.

Suppose $p = 10A + 9$ when $A \geq 1$.

Since $p + 6 = (10A + 9) + 6 = 10A + 15$, hence, for all values $A \geq 1$ $p + 6$ is not prime, and (1) has no solutions.

This concludes the proof of **(a)**.

(b) Suppose $p = 10A + 5$ when $A \geq 0$.

When $A = 0$, then $p = 5$ and $p + 6 = 11$. Hence, in (1) $p + (p + 6) = 16 = z^2$ and $z = 4$. Thus

$$(p, q, x, y, z) = (5, 11, 1, 1, 4)$$

is a solution of (1).

For all values $A \geq 1$, $10A + 5$ is not prime, and (1) has no solutions.

Thus, the above solution is the only solution of (1) as asserted, and completes part **(b**

(c) Suppose $p = 10A + 7$ when $A \geq 0$.

When $A = 0$, then $p = 7$ and $p + 6 = 13$. Hence, in (1) $p + (p + 6) = 7 + 13 = 20 \neq z^2$. Therefore, $A \neq 0$ and $A \geq 1$. For all values of A, it follows from (1) that

$$p + (p + 6) = (10A + 7) + (10A + 13) = 4 \cdot 5\,(A + 1) = z^2$$

implying that (1) exists only if $A + 1 = 5K^2$ where K is a positive integer. Since $A = 5K^2 - 1$, it follows that

$$10A + 7 = 50K^2 - 3 \quad \text{and} \quad 10A + 13 = 50K^2 + 3.$$

Furthermore, since $10A + 7$ and $10A + 13$ are both primes, hence K is not a multiple of 3. Therefore, $K = 3T + 1$ or $K = 3T + 2$ where $T \geq 0$ is an integer.

We shall now investigate these two possibilities of K for all values of $10A + 7$ and $10A + 13$ up to 10^5.

Let $K = 3T + 1$. Then

$$10A + 7 = 50K^2 - 3 = 450T^2 + 300T + 47. \tag{5}$$

Formula (5) implies that there are fifteen possible values of T, $0 \leq T \leq 14$ up to 10^5. The values $T = 0, 7, 8$ yield three solutions of (1) namely:

$(p, q, x, y, z) = (47, 53, 1, 1, 10), (24197, 24203, 1, 1, 220), (31247, 31253, 1, 1, 250)$.

Let $K = 3T + 2$. Then

$$10A + 7 = 50K^2 - 3 = 450T^2 + 600T + 197. \tag{6}$$

From (6), it follows that there are fifteen possible values of T, $0 \leq T \leq 14$ up to 10^5, and we obtain for $T = 3, 10, 13$ the following three solutions of (1):

$(p, q, x, y, z) = (6047, 6053,1,1,110), (51197, 51203,1,1,320), (84047, 84053,1,1,410)$.

When $p = 10A + 7$ and $q = 10A + 13$ are both primes, the six solutions of (1) up to 10^5 are established, and part **(c)** is proved.

The proof of the lemma is complete.

Remark 2.4. In Lemma 2.3, the solutions of (1) have been restricted to all values of p where $p < S = 10^5$. Evidently, formulae (5) and (6) are valid for all values of T, and enable us to find all the solutions of (1) up to any value of S where S is as large as we wish.

3. On $p^x + q^y = z^2$ and Sophie Germain primes

The problem concerning the infinitude of pairs of primes having the form $(P, 2P + 1)$ has been of great interest to the author [1, 2] and to a vast number of other authors.

In this section, we establish the connection between equation (1) and the Sophie Germain primes.

Sophie Germain (1776 – 1831) was a French lady mathematician, physicist and philosopher. Among other fields, she was also known in Number Theory for her work on Fermat's Last Theorem, and for the Sophie Germain prime numbers.

A Sophie Germain prime is a prime number $\boldsymbol{P}$ such that $\mathbf{2}\boldsymbol{P}\mathbf{+1}$ is also prime. The prime $\boldsymbol{P}$ is also called a "Sophie Germain number", whereas $\mathbf{2}\boldsymbol{P}\mathbf{+1}$ is called a "safe prime". The first few Sophie Germain primes are $\boldsymbol{P} = 2, 3, 5, 11, 23, 29, \ldots$.

Numerous articles have been written on the Sophie Germain primes, as well as on the Twin primes. It is conjectured that there are an infinite number of: Twin prime pairs $(p, p + 2)$, and also of Sophie Germain pairs $(\boldsymbol{P}, \mathbf{2}\boldsymbol{P} \mathbf{+ 1})$. These two conjectures are related, and it is extremely difficult to prove them.

From [3] we cite the conjecture on Sophie Germain primes.

Conjecture. The number of Sophie Germain primes $\boldsymbol{P}$ with $\boldsymbol{P} \le N$ is approximately

$$2C_2 \int_2^N \frac{dx}{\log x \log 2x} \sim \frac{2C_2 N}{(\log N)^2}$$

where $C_2 = 0.66016 \ldots$ is the twin prime constant.

From [6] we also cite: As of 29.2.2016, the largest known proven Sophie Germain prime $\boldsymbol{P}$ denoted here by $\boldsymbol{P_L}$ is

$$\boldsymbol{P_L} = 2618163402417 \cdot 2^{1290000} - 1$$

having 388342 decimal digits.

If indeed, the Sophie Germain conjecture is true, i.e., there exist infinitely many pairs $(\boldsymbol{P}, \mathbf{2}\boldsymbol{P} \mathbf{+ 1})$, then there exist infinitely many solutions of equation (1). Under this assumption, the infinite solutions of (1) are established in Lemma 3.1.

Lemma 3.1. Let (p, q) be any Sophie Germain pair $(\boldsymbol{P}, \mathbf{2}\boldsymbol{P} \mathbf{+ 1})$. If there exist infinitely many Sophie Germain pairs, then equation (1) has infinitely many solutions each of which is unique.

Proof: In $p^x + q^y = z^2$, set

$$p = \boldsymbol{P}, \quad x = 2, \quad q = \mathbf{2}\boldsymbol{P} \mathbf{+ 1}, \quad y = 1.$$

We then obtain

$$z^2 = p^x + q^y = \boldsymbol{P}^2 + (\mathbf{2}\boldsymbol{P} \mathbf{+ 1})^1 = (\boldsymbol{P} + 1)^2$$

where $z = \boldsymbol{P} + 1$.

The infinite solutions of (1) of the form

$$(p, q, x, y, z) = (\boldsymbol{P}, \mathbf{2}\boldsymbol{P} \mathbf{+ 1}, 2, 1, \boldsymbol{P} + 1)$$

correspond to each Sophie Germain prime $\boldsymbol{P}$ (even $\boldsymbol{P} = 2$), and each such solution is clearly unique.

This completes our proof.

Remark 3.1. If $\boldsymbol{P_L}$ is still the largest Sophie Germain prime, then accordingly the solution of (1)

$$(p, q, x, y, z) = (\boldsymbol{P_L}, \mathbf{2}\boldsymbol{P_L} \mathbf{+ 1}, 2, 1, \boldsymbol{P_L} + 1)$$

contains the largest values of p, q, and z.

Remark 3.2. Throughout this paper, our main objective has been finding solutions of (1) in the case of odd primes $p < q$. The proof of Lemma 3.1 nevertheless suggests the following generalized solution of (1) when the restriction p, q are primes is omitted. In Lemma 3.1, replace (p, q) by $(B, 2B + 1)$ where B is an integer. Then, clearly equation (1) has a solution of the form $(B, 2B+1, 2, 1, B + 1)$ for each value of B where $B \geq 1$.

The following question may now be raised: How many solutions of the form

$$(p, q, x, y, z) = (\boldsymbol{P}, \mathbf{2}\boldsymbol{P} + \mathbf{1}, 1, 1, z)$$

satisfy (1) ? The answer is given in Lemma 3.2.

Lemma 3.2. Suppose *(p, q)* is a Sophie Germain pair $(\boldsymbol{P}, \mathbf{2}\boldsymbol{P} + \mathbf{1})$. If $x = y = 1$, then (1) has exactly one solution.

Proof: Any solution of (1) of the form

$$(p, q, 1, 1, z) = (\boldsymbol{P}, \mathbf{2}\boldsymbol{P} + \mathbf{1}, 1, 1, z)$$

implies that $3\boldsymbol{P} + 1 = z^2$, and $\boldsymbol{P} = \frac{z^2 - 1}{3} = \frac{(z-1)(z+1)}{3}$. If $3|(z + 1)$, then $z = 2$ and hence $\boldsymbol{P} = 1$ which is impossible. But $3|(z - 1)$ yields $z = 4$ which implies $\boldsymbol{P} = z + 1 = 5$ and $\mathbf{2}\boldsymbol{P} + \mathbf{1} = 11$. Thus, the only solution of (1) is

$$(p, q, 1, 1, z) = (5, 11, 1, 1, 4).$$

This concludes our proof.

We note that the above solution has already been obtained in Lemma 2.3 for $k = 6$ in the case $p = 10A + 5$ when $A = 0$.

4. Conclusion

Equation (1) folds in itself some interesting questions, two of which are brought here. In Section 1, we have presented five solutions of (1) with $y = 1$ and $x = 1, 2, 3, 4, 5$. The following Question 1 is now raised:

Question 1. Does (1) have a solution of the form

$$(p, q, x, y, z) = (p, q, x, 1, z) \qquad \text{for every value } x = 6, 7, 8, \ldots?$$

We believe that the answer is affirmative.

Since $3^2 + 7^1 = 2^4$, $5^1 + 59^1 = 2^6$, $3^5 + 13^1 = 2^8$, $5^1 + 1019^1 = 2^{10}$, $3^5 + 3853^1 = 2^{12}$, we may ask:

Question 2. If a solution of (1) is of the form

$$(p, q, x, y, z) = (p, q, x, 1, \sqrt{2^t}\,) \qquad t \text{ an even positive integer,}$$

what conditions must p, q, x satisfy ?
how many solutions exist for any given value t ?

We presume that some more interesting questions concerning (1) may be raised.

REFERENCES

1. N.Burshtein, Some results on the infinitude of the pairs $(p, 2p + 1)$, Written communication to P. Erdös, 1959, unpublished.
2. N.Burshtein, On Sophie Germain primes, *Journal for Algebra and Number Theory Academia*, 6 (1) (2016) 37 – 41.

3. Chris K. Caldwell, An amazing prime heuristic, 2000.//www.utm.edu./caldweii//
4. P.Erdös, On the difference of consecutive primes, *Quart. J. Math. Oxford*, 6 (1935) 124 – 128.
5. A.Hildebrand and H.Maier, Gaps between prime numbers, *Proceedings of the American Mathematical Society*, 104 (1988) 1 – 9.
6. Primegrid, www.primegrid.com/
7. 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.
8. B.Sroysang, On the Diophantine Equation $5^x + 7^y = z^2$, *Int. J. Pure Appl. Math.*, 89 (2013) 115 – 118.
9. A.Suvarnamani, Solution of the diophantine equation $p^x + q^y = z^2$, *Int. J. Pure Appl. Math.*, 94 (2014) 457 – 460.