Annals of Pure and Applied Mathematics
Vol.19, No.2, 2019, 121-125
ISSN: 2279-087X (P), 2279-0888(online)
Published on 10 June 2019
www.researchmathsci.org
DOI: http://dx.doi.org/10.22457/apam.620v19n2a02

Annals of
Pure and Applied Mathematics

On Solutions of the Diophantine Equation $A^2 - B^2 = Z^4$ when A, B, Z are Positive Integers

Nechemia Burshtein

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

Received 4 June 2019; accepted 8 June 2019

Abstract. In this article, we consider the equation $A^2 - B^2 = Z^4$ with positive integers A, B, Z. We establish: (i) For all primes A, B, the equation has a unique solution. (ii) When $B = 4N + 3$ $(N > 0)$ is prime, the equation has no solutions. (iii) For $B = 4N + 1$ prime, the necessary and sufficient conditions for a solution are determined. (iv) For the composite $B = 4N + 3$ $(N = 3a)$, the necessary and sufficient conditions for a solution are provided. Several solutions are also exhibited.

Keywords: Diophantine equations

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.

The famous general equation

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

has many forms. The literature contains a very large number of articles on non-linear such individual equations involving particular primes and powers of all kinds. Among them are for example [1, 2, 5].

In this paper, we consider the equation $A^2 - B^2 = Z^4$ when A, B, Z are positive integers. All other values introduced are also positive integers. We investigate the equation when A, B are both primes, and also when at least one of A, B is composite.

2. Solutions of $A^2 - B^2 = Z^4$ when A, B are primes

When A, B are odd primes, the unique solution of the equation $A^2 - B^2 = Z^4$ is determined in Theorem 2.1.

Theorem 2.1. Suppose that p, q are odd primes where $A = p$ and $B = q$. Then the equation

$$p^2 - q^2 = Z^4 \tag{1}$$

has a unique solution.

Proof: The equation $p^2 - q^2 = Z^4$ implies $q^2 = p^2 - Z^4 = (p - Z^2)(p + Z^2)$. Three possibilities then exist, namely: $p - Z^2 = 1, q, q^2$, where the last two of which are a priori impossible. Thus, $p - Z^2 = 1$ or $p = Z^2 + 1$, and $p + Z^2 = q^2$ or $p = q^2 - Z^2$. Hence $p = (q - Z)(q + Z)$ where $q - Z = 1$ or $q = Z + 1$, and $p = q + Z$ or $p = 2Z + 1$. Since $p = Z^2 + 1 = 2Z + 1$, it follows that $Z^2 + 1 - (2Z + 1) = 0$ or $Z(Z - 2) = 0$ and $Z = 2$. Therefore $p = 2Z + 1 = 5$, and $q = Z + 1 = 3$.

Hence, with odd primes p, q, $p^2 - q^2 = Z^4$ has the unique solution

Solution 1. $(p, q, Z) = (5, 3, 2)$.

The proof of Theorem 2.1 is complete. □

Remark 2.1. As a consequence of Theorem 2.1 we have: The case $p = 2$ and q an odd prime is a priori impossible in (1). When $q = 2$, it follows from Theorem 2.1 that $p - Z^2 = 1$ and $p + Z^2 = 4$ or $2p = 5$ which is impossible. Hence in (1) none of the primes p, q is equal to 2.

3. Solutions of $A^2 - B^2 = Z^4$ when at least one of A, B is composite

In Section 2, it has been shown that when A, B are both primes, then $A^2 - B^2 = Z^4$ has the unique solution $(A, B, Z) = (5, 3, 2)$. Therefore, more solutions of the equation may be obtained only when exactly one of A, B is prime, or when both A, B are odd composites. In Theorem 3.1 we consider the case when $B = 4N + 3$ $(N > 0)$ is prime. It is shown that the equation has no solutions. In Theorem 3.2, when $B = 4N + 1$ is prime, it is shown that the equation turns into an identity having solutions provided two conditions hold simultaneously. Finally, in Theorem 3.3 when B is composite, the equation is an identity, and has solutions provided two conditions are satisfied simultaneously. For each of Theorems 3.2 and 3.3, two solutions are demonstrated.

Theorem 3.1. If $B = 4N + 3$ is prime where $N > 0$, then $A^2 - B^2 = Z^4$ has no solutions.

Proof: We shall assume that there exists a prime $B = 4N + 3$ $(N > 0)$, for which $A^2 - B^2 = Z^4$ has a solution and reach a contradiction.

The equation $A^2 - B^2 = Z^4$ yields

$$A^2 - Z^4 = (A - Z^2)(A + Z^2) = B^2 = (4N + 3)^2. \quad (2)$$

Since B is prime, it follows that $A - Z^2 = 1, B, B^2$, where from (2) the last two possibilities are a priori impossible. Hence,

$$A - Z^2 = 1 \quad \text{and} \quad A + Z^2 = B^2. \quad (3)$$

From (3) we obtain that $2Z^2 = B^2 - 1$ or $2Z^2 = (4N + 3)^2 - 1$, and after simplifications

$$Z^2 = 8N^2 + 12N + 4 = 4(2N^2 + 3N + 1) = 4(N + 1)(2N + 1). \quad (4)$$

Since gcd$(N + 1, 2N + 1) = 1$ and Z is an integer, it follows from (4) that $N + 1$ and $2N + 1$ are two squares. Denote $N + 1 = G^2$ and $2N + 1 = K^2$. Thus $Z^2 = 4G^2K^2 = (2GK)^2$.

We now have

$$B = 4N + 3 = 4(N + 1) - 1 = 4G^2 - 1 = (2G - 1)(2G + 1). \quad (5)$$

Since B is prime, it follows from (5) that $2G - 1 = 1$ and $2G + 1 = B$. But, $2G - 1 = 1$ implies that $G = 1$ which yields $N = 0$ contrary to our supposition that $N > 0$.

Our assumption that for some prime $B = 4N + 3$ $(N > 0)$, the equation $A^2 - B^2 = Z^4$ has a solution is therefore false, and the assertion follows.

This concludes the proof of Theorem 3.1. □

Remark 3.1. In Theorem 3.1, we have obtained that $G = 1$ implies $N = 0$ and also $B = 3$. In (3), the value $B = 3$ yields the values $A = 5$ and $Z = 2$ which were already demonstrated as **Solution 1** in Section 2.

Corollary 3.1. For any prime $B = 4N + 3$ $(N > 0)$, it has been shown in Theorem 3.1 that $A^2 - B^2 = Z^4$ has no solutions. Therefore, if the equation has a solution when B is prime, then $B = 4N + 1$.

Theorem 3.2. Suppose that $B = 4N + 1$ is prime. If N satisfies simultaneously the conditions

(i) $N = L^2$,

(ii) $2N + 1 = M^2$,

then $A^2 - B^2 = Z^4$ has the solution

$$(A, B, Z) = (4L^2M^2 + 1,\ 4L^2 + 1,\ 2LM), \quad (6)$$

where L, M are integers.

Proof: The equation $A^2 - B^2 = Z^4$ yields

$$A^2 - Z^4 = (A - Z^2)(A + Z^2) = B^2 = (4N + 1)^2. \quad (7)$$

Since B is prime, it follows that $A - Z^2 = 1, B, B^2$, where from (7), the last two possibilities are a priori impossible. Thus,

$$A - Z^2 = 1 \quad \text{and} \quad A + Z^2 = B^2. \quad (8)$$

From (8) we obtain that $2Z^2 = B^2 - 1 = (4N + 1)^2 - 1$, and after simplifications

$$Z^2 = 8N^2 + 4N = 4N(2N + 1). \quad (9)$$

Since gcd $(N, 2N + 1) = 1$ and Z is an integer, it then follows from (9) that N and $2N + 1$ are two squares. Denote $N = L^2$ and $2N + 1 = M^2$. Then $Z^2 = 4L^2M^2 = (2LM)^2$, and $Z = 2LM$ is an integer. From (8) we have $A = Z^2 + 1$, and therefore $A = 4L^2M^2 + 1$.

We have shown that when $B = 4N + 1$ is prime, and N satisfies conditions (i) and (ii) simultaneously, then $A^2 - B^2 = Z^4$ has solution (6). The equalities $N = L^2$ and $2N + 1 = M^2$ in this case are necessary and sufficient conditions for a solution.

The proof of Theorem 3.2 is complete. □

The following two solutions of $A^2 - B^2 = Z^4$ in which $B = 4N + 1$ is prime, and A is composite, are the smallest possible ones in accordance with (6).

Solution 2. $145^2 - 17^2 = 12^4$.

Solution 3. $166465^2 - 577^2 = 408^4$.

We now investigate the odd value B, a composite of the form $4N + 3$. In order to show that $A^2 - B^2 = Z^4$ has solutions, it suffices to consider the simplest form of composites $4N + 3$ when $N = 3a$. This is done in Theorem 3.3.

Theorem 3.3. When $N = 3a$ ($a > 0$), the value $4N + 3$ is composite. If the two conditions
(i) $N + 1 = 3a + 1 = Q^2$,
(ii) $2N + 1 = 6a + 1 = R^2$
are satisfied simultaneously, then $A^2 - B^2 = Z^4$ has the solution

$$(A, B, Z) = \left(4(3a + 1)(6a + 1) + 1,\ \ 3(4a + 1),\ \ \sqrt{4(3a+1)(6a+1)}\right), \quad (10)$$

where $\sqrt{(3a+1)(6a+1)}$ is an integer.

Proof: We have

$$B = 4N + 3 = 4 \cdot 3a + 3 = 3(4a + 1). \quad (11)$$

The equation $A^2 - B^2 = Z^4$ and (11) yield

$$A^2 - Z^4 = (A - Z^2)(A + Z^2) = B^2 = (4N + 3)^2. \quad (12)$$

To prove our assertion, it will suffice to consider from (12) the only case

$$A - Z^2 = 1 \text{ and } A + Z^2 = B^2. \quad (13)$$

From (13) and (12) we obtain $2Z^2 = B^2 - 1 = (4N + 3)^2 - 1$, and after simplifications

$$Z^2 = 8N^2 + 12N + 4 = 4(2N^2 + 3N + 1) = 4(N + 1)(2N + 1). \quad (14)$$

Since gcd $(N + 1, 2N + 1) = 1$, and Z is an integer, it follows from (14) that $N + 1$ and $2N + 1$ are two squares. Denote $N + 1 = Q^2$ and $2N + 1 = R^2$. Then $Z^2 = 4Q^2R^2 = (2QR)^2$, and $Z = 2QR$ is an integer. From (13) we have $A = Z^2 + 1$, and $A = 4Q^2R^2 + 1 = 4(N + 1)(2N + 1) + 1$.

Since $N = 3a$, the integers

$$A = 4(N + 1)(2N + 1) + 1 = 4(3a + 1)(6a + 1) + 1,$$

$$B = 4N + 3 = 4 \cdot 3a + 3 = 3(4a + 1),$$

$$Z = \sqrt{4(N+1)(2N+1)} = \sqrt{4(3a+1)(6a+1)}$$

as in (10) form a solution of the equation $A^2 - B^2 = Z^4$.

This concludes the proof of Theorem 3.3. □

Two solutions of $A^2 - B^2 = Z^4$ with composites A, and $B = 4N + 3 = 3(4a + 1)$ in accordance with (10) are as follows:

Solution 4. $4901^2 - 99^2 = 70^4$.

Solution 5. $5654885^2 - 3363^2 = 2378^4$.

4. Conclusion

We sum up the results achieved in this paper. When A, B are primes, the equation has only **solution1** (Theorem 2.1). When B is prime of the form $4N + 3$ ($N > 0$), the equation has no solutions (Theorem 3.1). When $B = 4N + 1$ is prime, the necessary and sufficient conditions for a solution of the equation are obtained (Theorem 3.2), and accordingly **Solutions 2** and **3** where A is composite are demonstrated. When $B = 4N + 3$ ($N = 3a$) is composite, the necessary and sufficient conditions for a solution are achieved (Theorem 3.3). In accordance, **Solutions 4** and **5** where A is a composite are exhibited.

The following question may now be raised.

Question 1. With A prime and B composite, does $A^2 - B^2 = Z^4$ have a solution ?

The numbers A, B, Z are quite large. This may be seen for instance in **Solution 5** where we have:

$5654885^2 - 3363^2 = 2378^4$ or $31977724363225 - 11309769 = 31977713053456$

consisting of 14 digits. Therefore, in order to find more solutions, and also prove or disprove **Question 1**, can be done only with the aid of a computer.

REFERENCES

1. N. Burshtein, On solutions of the diophantine equations $p^4 + q^4 = z^2$ and $p^4 - q^4 = z^2$ when p and q are primes, *Annals of Pure and Applied Mathematics*, 19 (1) (2019) 1 – 5.
2. N. Burshtein, On solutions to the diophantine equation $p^2 + q^2 = z^4$, *Annals of Pure and Applied Mathematics*, 18 (2) (2018) 135 – 138.
3. N. Burshtein, All the solutions of the diophantine equation $p^4 + q^2 = z^2$ when p is prime, *Annals of Pure and Applied Mathematics*, 14 (3) (2017) 457 – 459.
4. S. Chotchaisthit, On the diophantine equation $4^x + p^y = z^2$ where p is a prime number, *Amer. J. Math. Sci*., 1 (1) (2012) 191 – 193.
5. B. Poonen, Some diophantine equations of the form $x^n + y^n = z^m$, *Acta Arith*., 86 (1998) 193-205.