Annals of Pure and Applied Mathematics
Vol. 18, No. 1, 2018, 51-57
ISSN: 2279-087X (P), 2279-0888(online)
Published on 31 July 2018
www.researchmathsci.org
DOI: http://dx.doi.org/10.22457/apam.v18n1a7

Annals of **Pure and Applied Mathematics**

On Solutions of the Diophantine Equations $p^3 + q^3 = z^2$ and $p^3 - q^3 = z^2$ when p, q are Primes

Nechemia Burshtein

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

Dedicated to Ali Burshtein

Received 9 June 2018; accepted 30 July 2018

Abstract. In this paper, we consider the two equations $p^3 + q^3 = z^2$ and $p^3 - q^3 = z^2$ when p, q are primes. Among the various results attained, it is shown that both equations have no solutions when $q = 2$, and z^2 is a multiple of 9 in each and every solution. In particular, when $3 \le q < p \le 101$, all the possibilities for solutions of each equation are examined for all primes p, q. It is established that each equation has exactly one solution which is exhibited. For primes larger than 101, it is presumed that both equations may have additional solutions by using a computer.

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 primes and powers of all kinds. Among them are for example [1, 4, 5, 6].

In this paper, we consider the two equations

$$p^3 + q^3 = z^2,$$
$$p^3 - q^3 = z^2$$

where p, q are primes, and z is a positive integer.

When the conditions on p, q are relaxed, i.e., at least one of p, q is composite, the two equations have solutions. Bruin [1] demonstrated seven such solutions which are as follows.

$$(p,\ q,\ z) = (8,\ 4,\ 24)$$

for the first equation, whereas

(p, q, z) € {(8, 7, 13), (32, 28, 104), (33, 6, 189), (72, 63, 351), (132, 24, 1512), (288, 252, 2808)} relate to the second equation.

In the two self-contained Sections 2 and 3, the two equations are respectively investigated for solutions. Among the results attained, we establish that each equation has exactly one solution when $3 \leq q < p \leq 101$ where for all primes p and q, all the possibilities have been examined.

2. On the solutions of $p^3 + q^3 = z^2$ when p, q are primes

In our discussion, all the integers are positive, and we distinguish two cases, namely: $q = 2$ and $q > 2$.

The case $q = 2$.

The equation $p^3 + 2^3 = z^2$ yields

$$p^3 + 2^3 = (p + 2)(p^2 - 2p + 4) = z^2. \tag{1}$$

Theorem 2.1. If p is prime, then the equation $p^3 + 2^3 = z^2$ has no solutions.

Proof: Let A, B and $R > 1$ be odd integers. If (1) has a solution, then the solution satisfies at least one of the following two possibilities:

(i) $p + 2 = A^2$ and $p^2 - 2p + 4 = B^2$,

(ii) $p + 2 = A^2R$ and $p^2 - 2p + 4 = B^2R$.

In (i) and in (ii) both conditions must exist simultaneously.

We will now show that (i) and (ii) are impossible.

Suppose (i), i.e., $p + 2 = A^2$ and $p^2 - 2p + 4 = B^2$. To prove our assertion, it suffices to show for every prime p, that $p^2 - 2p + 4$ is not a square. We shall assume that there exists a prime p for which $p^2 - 2p + 4 = B^2$, and reach a contradiction.

By our assumption, let $p^2 - 2p + 4 = B^2$. Then $p(p - 2) = B^2 - 4 = (B - 2)(B + 2)$. Hence, p divides at least one of the values $(B - 2)$, $(B + 2)$.

If $p|(B - 2)$, then $Cp = B - 2$ where C is an odd integer, and $Cp + 4 = B + 2$. Thus $p(p - 2) = (Cp)(Cp + 4)$ or $p - 2 = C(Cp + 4)$ which is impossible.

If $p|(B + 2)$, then $Dp = B + 2$ where D is an odd integer, and $Dp - 4 = B - 2$. We have $p(p - 2) = (Dp - 4)(Dp)$ or $p - 2 = D^2p - 4D$ implying $p(D^2 - 1) = 4D - 2$ and $p = \frac{4D-2}{D^2-1}$. The value $D = 1$ is impossible, and for all integers $D > 1$, it follows that $p = \frac{4D-2}{D^2-1}$ is not an integer.

Our assumption that $p^2 - 2p + 4 = B^2$ is therefore false, and the assertion follows. Case (i) does not exist.

Suppose (ii), i.e., $p + 2 = A^2R$ and $p^2 - 2p + 4 = B^2R$ where $R > 1$. Then $p + 2 = A^2R$ yields $p = A^2R - 2$, and $p^2 - 2p + 4 = A^4R^2 - 6A^2R + 12 = B^2R$. Hence $R \mid 12$. Since $R > 1$ is odd, therefore $R = 3$.

We then have

$$p + 2 = 3A^2 \quad \text{and} \quad p^2 - 2p + 4 = 3B^2 \tag{2}$$

which must exist simultaneously. Both equalities in (2) do not exist simultaneously. A formal proof which is lengthy and includes many technical details is not given here.

Nevertheless, the validity of the above statement can be verified by the reader. Case (ii) does not exist, and hence the equation $p^3 + 2^3 = z^2$ has no solutions.

The proof of Theorem 2.1 is complete. □

The case $q > 2$.
The equation $p^3 + q^3 = z^2$ yields

$$p^3 + q^3 = (p + q)(p^2 - pq + q^2) = z^2. \qquad (3)$$

Let A be an even integer, and B, $R > 1$ odd integers. Any solution of (3) must now satisfy at least one of the following two cases:
(i) $p + q = A^2$ and $p^2 - pq + q^2 = B^2$,
(ii) $p + q = A^2R$ and $p^2 - pq + q^2 = B^2R$.
In each case, both conditions must exist simultaneously.

In Theorem 2.2, we show that case (i) does not exist.

Theorem 2.2. If p, q are primes, then $p^2 - pq + q^2 \neq B^2$.

Proof: Without loss of generality let $p > q$. To prove our assertion, we shall assume that there exist primes p, q satisfying $p^2 - pq + q^2 = B^2$, and reach a contradiction.

By our assumption, we have $p^2 - pq + q^2 = B^2$ or

$$p(p - q) = B^2 - q^2 = (B - q)(B + q)$$

implying that p divides at least one of the values $(B - q),(B + q)$.

If $p|(B - q)$, then $pa = B - q$ where a is an even integer, and $pa + 2q = B + q$. Thus, $p(p - q) = (pa)(pa + 2q)$ or $p - q = a(pa + 2q)$ which is impossible for all values a.

If $p|(B + q)$, then $pb = B + q$ where b is an even integer, and $pb - 2q = B - q$. Hence, $p(p - q) = (pb - 2q)(pb)$ or $p - q = b(pb - 2q)$ implying that $p(b^2 - 1) = q(2b - 1)$ and $p = \frac{(2b-1)q}{b^2-1}$. When $b = 2$, then $p = q$ which is impossible, and therefore $b \neq 2$. Since $p > q$, it follows that $1 < \frac{p}{q} = \frac{2b-1}{b^2-1}$. But, for all integers $b > 2$, we have that $\frac{2b-1}{b^2-1} < 1$, a contradiction.

Our assumption that there exist primes p, q for which $p^2 - pq + q^2 = B^2$ is therefore false, and the assertion follows.

This concludes the proof of Theorem 2.2. □

Remark 2.1. The first condition in (i) is satisfied for infinitely many primes p, q. For example: $13 + 3 = 4^2$, $19 + 17 = 6^2$, $41 + 23 = 8^2$, and so on. By Theorem 2.2, the second condition in (i) does not exist. The two conditions in (i) are not satisfied simultaneously. Therefore, in this case the equation $p^3 + q^3 = z^2$ has no solutions.

In the following Proposition 2.1, case (ii) is considered, and the value $R > 1$ is determined.

Proposition 2.1. Suppose that p, q are primes. If $p + q = A^2R$ and $p^2 - pq + q^2 = B^2R$ are satisfied simultaneously, then $R = 3$.

Proof: The integer $p + q = A^2R$ implies $p = A^2R - q$. Substituting p in $p^2 - pq + q^2 = B^2R$ yields $A^4R^2 - 3A^2R\,q + 3q^2 = B^2R$. Hence $R \mid 3q^2$. Since $R > 1$, the only possible value R is $R = 3$. □

Any solution of $p^3 + q^3 = z^2$ now satisfies the conditions:

$$p + q = 3A^2, \qquad p^2 - pq + q^2 = 3B^2, \qquad z^2 = 9A^2B^2.$$

Remark 2.2. For all primes p, q satisfying $3 \leq q < p \leq 101$, all the possibilities have been examined for solutions of $p^3 + q^3 = z^2$. It is established that the equation has exactly one solution when $p = 37$, $q = 11$ and $z = 228$, namely:

Solution 2.1. $$37^3 + 11^3 = 228^2.$$

In accordance with Proposition 2.1, this solution satisfies:

$$p + q = A^2R = 3\cdot 4^2,$$
$$p^2 - pq + q^2 = B^2R = 3\cdot 19^2,$$
$$z^2 = 9A^2B^2 = 9\cdot 4^2\cdot 19^2.$$

3. On the solutions of $p^3 - q^3 = z^2$ when p, q are primes

Although the two equations are distinct, we follow here the procedure outlined in Section 2. Since both sections are each self-contained, we shall apply here the same style and notation as in Section 2.

We shall consider the two cases $q = 2$ and $q > 2$.

The case $q = 2$.

The equation $p^3 - 2^3 = z^2$ yields

$$p^3 - 2^3 = (p - 2)(p^2 + 2p + 4) = z^2. \tag{4}$$

Theorem 3.1. If p is prime, then the equation $p^3 - 2^3 = z^2$ has no solutions.

Proof: Let A, B and $R > 1$ be odd integers. Any solution of (4) must satisfy at least one of the following two possibilities:

(i) $p - 2 = A^2$ and $p^2 + 2p + 4 = B^2$,

(ii) $p - 2 = A^2R$ and $p^2 + 2p + 4 = B^2R$.

In each case, both conditions must exist simultaneously.

We will show that (i) and (ii) are impossible.

Suppose (i), i.e., $p - 2 = A^2$ and $p^2 + 2p + 4 = B^2$. To prove our assertion, it suffices to show for all primes p that $p^2 + 2p + 4$ is not a square. We shall assume that there exists a prime p for which $p^2 + 2p + 4 = B^2$, and reach a contradiction.

By our assumption, let $p^2 + 2p + 4 = B^2$. Then $p(p + 2) = B^2 - 4 = (B - 2)(B + 2)$. Thus, p divides at least one of the values $(B - 2)$, $(B + 2)$.

If $p|(B - 2)$, then $Cp = B - 2$ where C is an odd integer, and $Cp + 4 = B + 2$. Hence, $p(p + 2) = (Cp)(Cp + 4)$ or $p + 2 = C(Cp + 4)$ which is impossible.

If $p|(B + 2)$, then $Dp = B + 2$ where D is an odd integer, and $Dp - 4 = B - 2$. We obtain $p(p + 2) = (Dp - 4)(Dp)$ or $p + 2 = D^2p - 4D$ implying that $p(D^2 - 1) = 4D$

+2 and $p = \frac{4D+2}{D^2-1}$. The value $D = 1$ is impossible, and for all integers $D > 1$, it follows that $p = \frac{4D+2}{D^2-1}$ is not an integer.

Our assumption that $p^2 + 2p + 4 = B^2$ is therefore false, and the assertion follows. Case (i) does not exist.

Suppose (ii), i.e., $p - 2 = A^2R$ and $p^2 + 2p + 4 = B^2R$ where $R > 1$. The integer $p - 2 = A^2R$ yields $p = A^2R + 2$ implying that $p^2 + 2p + 4 = A^4R^2 + 6A^2R + 12 = B^2R$. Thus $R \mid 12$. Since $R > 1$ is odd, therefore $R = 3$.

We then have

$$p - 2 = 3A^2 \quad \text{and} \quad p^2 + 2p + 4 = 3B^2 \qquad (5)$$

which must exist simultaneously. Both equalities in (5) do not exist simultaneously. The proof which is rather long, very detailed and tedious will not be given here. The validity of the above statement may be verified by the reader. Case (ii) does not exist, and hence the equation $p^3 - 2^3 = z^2$ has no solutions as asserted.

This concludes the proof of Theorem 3.1. □

The case $q > 2$.

The equation $p^3 - q^3 = z^2$ yields

$$p^3 - q^3 = (p - q)(p^2 + pq + q^2) = z^2. \qquad (6)$$

Let A be an even integer, and B, $R > 1$ odd integers. Any solution of (6) must now satisfy at least one of the following two cases:

(i) $p - q = A^2$ and $p^2 + pq + q^2 = B^2$,
(ii) $p - q = A^2R$ and $p^2 + pq + q^2 = B^2R$.
In each case, both conditions must exist simultaneously.

In Theorem 3.2, we show that case (i) does not exist.

Theorem 3.2. If p, q are primes, then $p - q = A^2$ and $p^2 + pq + q^2 = B^2$ do not exist simultaneously.
The equation $p^3 - q^3 = z^2$ has no solutions.

Proof: We shall assume in (i) that there exist primes p, q which satisfy both conditions simultaneously, and reach a contradiction.

By our assumption, we have $p^2 + pq + q^2 = B^2$ or

$$p(p + q) = B^2 - q^2 = (B - q)(B + q)$$

implying that p divides at least one of the values $(B - q)$,$(B + q)$.

If $p|(B - q)$, then $pa = B - q$ where a is an even integer, and $pa + 2q = B + q$. Thus, $p(p + q) = (pa)(pa + 2q)$ or $p + q = a(pa + 2q)$ which is impossible for all values a.

If $p|(B + q)$, then $pb = B + q$ where b is an even integer, and $pb - 2q = B - q$. Hence, $p(p + q) = (pb - 2q)(pb)$ or $p + q = b(pb - 2q)$ implying that $p(b^2 - 1) = q(2b + 1)$ and $p = \frac{(2b+1)q}{b^2-1}$. When $b = 2$, then $3p = 5q$. Thus $q = 3$, $p = 5$ and $B^2 = 49$ are the unique values of this equality. But $5 - 3 \neq A^2$, hence (i) is not satisfied simultaneously. Therefore $b \neq 2$. Since $p > q$, we have $1 < \frac{p}{q} = \frac{2b+1}{b^2-1}$. For all integers $b > 2$, then $\frac{2b+1}{b^2-1} < 1$, a contradiction.

Our assumption in (i) that there exist primes p, q which satisfy both conditions simultaneously is false, and the assertion follows. Case (i) does not exist, and the equation has no solutions.

This completes the proof of Theorem 3.2. □

In the following Proposition 3.1 we consider case (ii), and determine the value R.

Proposition 3.1. Suppose that p, q are primes. If $p - q = A^2R$ and $p^2 + pq + q^2 = B^2R$ are satisfied simultaneously, then $R = 3$.

Proof: The integer $p - q = A^2R$ implies that $p = A^2R + q$. Substituting p into $p^2 + pq + q^2 = B^2R$ results in $A^4R^2 + 3A^2Rq + 3q^2 = B^2R$. Thus, $R \mid 3q^2$. Since $R > 1$, $R = 3$ is the only possible value. □

Any solution of $p^3 - q^3 = z^2$ now satisfies the conditions:

$$p - q = 3A^2, \qquad p^2 + pq + q^2 = 3B^2, \qquad z^2 = 9A^2B^2.$$

Remark 3.1. For all primes p, q satisfying $3 \le q < p \le 101$, all the possibilities have been examined for solutions of $p^3 - q^3 = z^2$. It is established that the equation has exactly one solution when $p = 71$, $q = 23$ and $z = 588$, namely:

Solution 3.1. $71^3 - 23^3 = 588^2$.

Proposition 3.1 is satisfied by the solution as follows:

$$p - q = A^2R = 3\cdot 4^2,$$
$$p^2 + pq + q^2 = B^2R = 3\cdot 49^2,$$
$$z^2 = 9A^2B^2 = 9\cdot 4^2\cdot 49^2.$$

4. Conclusion

Besides the demonstrated two solutions, we can sum up the other results achieved in this paper as follows.

(a) For all primes p, the equations $p^3 + 2^3 = z^2$ and $p^3 - 2^3 = z^2$ have no solutions.

(b) For $z^2 = p^3 + q^3 = (p + q)(p^2 - pq + q^2)$ where $2 \le q < p$, each of the values $p^2 - 2p + 4$ and $p^2 - pq + q^2$ is not a square. Hence, both factors are not squares simultaneously.

(c) For $z^2 = p^3 - q^3 = (p - q)(p^2 + pq + q^2)$ where $2 \le q < p$, the value $p^2 + 2p + 4$ is not a square, whereas $p^2 + pq + q^2$ is a square only when $p = 5$ and $q = 3$, but $5 - 3$ is not a square. Thus, both factors are not squares simultaneously.

(d) In any possible solution of $p^3 + q^3 = z^2$ and of $p^3 - q^3 = z^2$, the value z^2 is a multiple of 9. Indeed, z^2 is a multiple of 9 in Solutions 2.1 and 3.1.

For primes $p > 101$ onward, both cubes of each equation are getting larger and larger. Therefore, only with the aid of a computer one may obtain additional solutions if such exist. We presume that such solutions exist.

REFERENCES

1. N.Bruin, The primitive solutions to $x^3 + y^9 = z^2$, *Journal of Number Theory*, 111 (2005) 179 – 189.
2. N.Bruin, The diophantine equations $x^2 \pm y^4 = \pm z^6$ and $x^2 + y^8 = z^3$, *Compositio Mathematica* 118 (1999) 305 – 321.
3. N.Burshtein, All the solutions of the diophantine equation $p^3 + q^2 = z^3$, *Annals of Pure and Applied Mathematics*, 14 (2) (2017) 207 – 211.
4. N.Burshtein, All the solutions of the diophantine equation $p^3 + q^2 = z^2$, *Annals of Pure and Applied Mathematics*, 14 (1) (2017) 115 – 117.
5. S.Chowla, J.Cowles and M.Cowles, On $x^3 + y^3 = D$, *Journal of Number Theory*, 14 (1982) 369 – 373.
6. B.Poonen, Some diophantine equations of the form $x^n + y^n = z^m$, *Acta Arith*., 86 (1998) 193 – 205.
7. B.Sroysang, More on the diophantine equation $8^x + 19^y = z^2$, *Int. J. Pure Appl. Math*., 81 (4) (2012) 601 – 604.
8. A.Suvarnamani, Solution of the diophantine equation $p^x + q^y = z^2$, *Int. J. Pure Appl. Math*., 94 (4) (2014) 457 – 460.