The Primitive-Solutions of Diophantine Equation
$x^2 + pqy^2 = z^2$, for primes $p, q$

Solusi Primitif Persamaan Diophantine $x^2 + pqy^2 = z^2$ untuk bilangan-bilangan prima $p$ dan $q$

Aswad Harirri Mangalaeng*

Abstract

In this paper, we determine the primitive-solutions of diophantine equations $x^2 + pqy^2 = z^2$, for positive integers $x, y, z$ and primes $p, q$. Our work is based on the development of the previous results, namely using the solutions of the Diophantine equation $x^2 + y^2 = z^2$, and looking characteristics of the solutions of the Diophantine equation $x^2 + 3y^2 = z^2$ and $x^2 + 9y^2 = z^2$.

Keywords: composite number, diophantine equation, prime number, primitive solution.

1. INTRODUCTION

A Diophantine equation is an equation of the form
\[ f(x_1, x_2, \ldots, x_n) = 0, \]
where $f$ is an $n$-variable function with $n \geq 2$. The solution of Equation (1.1) is an $n$-uple $x_1, x_2, \ldots, x_n$ satisfying the equation [3]. For example, $14,223$ is one solution of Diophantine equation $17x + 8y = 2021$, and $3,4,5$ is the solution of Diophantine equation $x^2 + y^2 = z^2$.

Nowadays, there have been many studies about Diophantine equations. Most of their research is about finding the solutions of a given equation, one of which is the work on the equation $x^2 + 3a41^b = y^n$ by Alan and Zengin [2] where $a, b$ are non-negative integers and $x, y$ are relatively prime. There are many forms of Diophantine equations with various variables defined. Rahmawati et al [7] figured out the solutions from the equation $(7^k - 1)^x + (7^k)^y = z^2$ where $x, y, z$ are non-negative integers and $k$ is the positive even integer, Burshtein [4] stated the solutions of Diophantine equation $p^x + p^y = z^2$ when $p \geq 2$ are primes and $x, y, z$ are positive integers, and Chakraborty and Hogue [5] investigated the solvability of the Diophantine equation
\[ dx^2 + p^{2a}q^{2b} = 4y^p, \]
where $d > 1$ is a square-free integer, $p, q$ are distinct odd primes and $x, y, a, b$ are positive integers with $gcd(x, y) = 1$.

Another interesting Diophantine equation is $x^2 + cy^2 = z^2$, where all the variables are integers. Some cases of this problem have been solved, such as for case of $c = 1$ (see in [8]).

*Email address: aswadh2905@gmail.com
Next, there are Abdealim and Dyani [1] who had given the solutions for case of \( c = 3 \) by using the arithmetic technical. Following this, Rahman and Hidayat [6] presented the primitive-solutions for case of \( c = 9 \) using characteristics of the primitive solutions which are a development of the previous cases.

On this paper, we extend the results of [1], [6] and [8] to determine the primitive-solutions of Diophantine equation \( x^2 + pqy^2 = z^2 \) where \( x, y \) and \( z \) are positive integers, and \( p \) and \( q \) are primes. We establish results that the equation for case \( y \) is odd has no primitive-solution and case \( y \) is even have two primitive-solutions.

2. MAIN RESULTS

Before showing our results, firstly, we fix some notation. If not previously defined, then we use Diophantine equation \( x^2 + pqy^2 = z^2 \) with \( x, y, z \) are positive integers, and \( p, q \) are primes. Also, if integers \( m \) and \( n \) are relatively primes, we write \((m, n) = 1\). Sometimes, we just write \( x, y \) for indicate \( x \) and \( y \).

**Definition 2.1.** Any triple Phytagor as \( (x, y, z) \) is called a triple primitive Phytagoras if \((x, y, z) = 1\) [3].

Next, We note one result from [3],

**Theorem 2.2.** The positive integers \( x, y, z \) is a primitive-solution of Diophantine equation \( x^2 + y^2 = z^2 \) with \( y \) is even, if and only if there are positive integers \( m \) and \( n \) such that \( x = m^2 - n^2, y = 2mn, \) and \( z = m^2 + n^2 \) with \((m, n) = 1, m > n, \) and \( m, n \) have different parity.

We also share the fundamental theorem of arithmetic without any comment,

**Theorem 2.3.** Every positive integer can be written uniquely as a product of primes, with the prime factors in the product written in order of non-decreasing size [3].

Now, we begin our work.

**Definition 2.4.** The positive integers \( x, y, z \) is called a primitive-solution of Diophantine equation

\[
x^2 + pqy^2 = z^2
\]

if \((x, y, z) = 1\).

**Example 2.5.** 21,45 is a primitive-solution of Diophantine equation \( x^2 + 2021y^2 = z^2 \), because of \( z^2 + 2021(1)^2 = 2025 = 45^2 \) and \((2,1,45) = 1\).

**Theorem 2.6.** If \( x, y, z \) is a solution of Diophantine equation \( x^2 + pqy^2 = z^2 \) with \((x, y, z) = d\) such that \( x = dx_1, y = dy_1, \) and \( z = dz_1 \) for integers \( x_1, y_1, z_1 \), then \( x_1, y_1, z_1 \) is a solution of Diophantine equation \( x^2 + pqy^2 = z^2 \) with \((x_1, y_1, z_1) = 1\).

**Proof.** Let integers \( x, y, z \) is a solution of Diophantine equation \( x^2 + pqy^2 = z^2 \), so

\[
(x^2 + pqy^2 = z^2)
\]

\[
(dx_1)^2 + pq(dy_1)^2 = (dz_1)^2
\]

\[
d^2(x_1^2 + pqy_1^2) = d^2z_1^2
\]

\[
x_1^2 + pqy_1^2 = z_1^2
\]

From Equation (2.1), we can conclude that \( x_1, y_1, z_1 \) is a solution of Diophantine equation \( x^2 + pqy^2 = z^2 \). Also, from \((x, y, z) = d\), we have \((x, y, z) = 1\). This is equal to \((x_1, y_1, z_1) = 1\) which completes the proof of Theorem 2.3.
Example 2.7. 4, 2, 90 is a solution of Diophantine equation \( x^2 + 2021y^2 = z^2 \). We have \((4,2,90) = 2\). Hence, we get \(x_1 = 2, y_1 = 1\) and \(z_1 = 45\). From Example 2.5, we have 2,1,45 is also the solution of the equation with \((2,1,45) = 1\).

Lemma 2.8. If the integers \(x, y, z\) is a primitive-solution of Diophantine equation \(x^2 + p q y^2 = z^2\), then \((x, y) = (y, z) = (x, z) = 1\).

Proof. Suppose \((x, y) \neq 1\), then there a prime \(p_1\) with \(p_1 = (x, y)\) so that \(p|x\) and \(p|y\). Therefore, \(p_1 | (x^2 + p q y^2 = z^2)\). Hence, \(p_1 | z^2\) and then \(p_1 | z\). Because \(p_1 | x, p_1 | y\) and \(p_1 | z\), we can conclude that \((x, y, z) = p_1\). This contradicts the fact that \(x, y, z\) is a primitive-solution of Diophantine equation \(x^2 + p q y^2 = z^2\). Consequently, it must be \((x, y) = 1\). Using similar techniques, we prove for \((y, z) = 1\) and \((x, z) = 1\).

Theorem 2.9. If the positive integers \(x, y, z\) is a primitive-solution of Diophantine equation \(x^2 + p q y^2 = z^2\) and \(y\) is even, then \(x\) dan \(z\) are odd.

Proof. Let \(y\) is even and \(x, y, z\) is a primitive-solution of Diophantine equation \(x^2 + p q y^2 = z^2\). Using Lemma 2.8, we have \((x, y) = 1\) and \((y, z) = 1\). These equations mean that \(x\) and \(z\) are odd.

Example 2.10. 95, 92, 4137 is the primitive-solution of Diophantine equation \(x^2 + 2021y^2 = z^2\) where \(y = 92\) is even, and \(x = 95\) and \(z = 4137\) are odd.

Theorem 2.11. If the positive integers \(x, y, z\) is a primitive-solution of Diophantine equation \(x^2 + p q y^2 = z^2\) and \(y\) is odd, then \(x\) dan \(z\) are even.

Proof. Let \(y\) is odd and \(x, y, z\) is a primitive-solution of Diophantine equation \(x^2 + p q y^2 = z^2\). Using Lemma 2.8, we have \((x, y) = 1\) and \((y, z) = 1\). These equations mean that \(x\) and \(z\) are even.

Theorem 2.12. If \(r, s, t\) are positive integers with \((r, s) = 1\) and \(rs = p q t^2\) where \(p, q\) are primes, then there are integers \(m\) and \(n\) such that

i. \(r = p q m^2\) and \(s = n^2\),

ii. \(r = m^2\) and \(s = p q n^2\), or

iii. \(r = p m^2\) and \(s = q n^2\).

Proof. Based on Theorem 2.3, we can write each positive integers \(r, s\), and \(t\) as a single product of their primes. Write \(r = \prod_{i=1}^{a_1} p_i^{a_1} \cdots p_u^{a_u}, \ s = p_u^{a_{u+1}} p_{u+2}^{a_{u+2}} \cdots p_v^{a_v}\), and \(t = q_1^{\beta_1} q_2^{\beta_2} \cdots q_k^{\beta_k}\). So, we get \(p q t^2 = p q_1^{2\beta_1} q_2^{2\beta_2} \cdots q_k^{2\beta_k}\). Since \((r, s) = 1\), It means that prime factors of \(r\) and \(s\) are different. Because \(rs = p q t^2\), we get

\[
(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_u^{\alpha_u})(p_u^{\alpha_{u+1}} p_{u+2}^{\alpha_{u+2}} \cdots p_v^{\alpha_v}) = p q_1^{2\beta_1} q_2^{2\beta_2} \cdots q_k^{2\beta_k} . \tag{2.2}
\]

Case 1. \(p = q\)

If \(p = q\), we can write \(p q = q^{2\beta_k+1}\) where \(\beta_{k+1} = 1\). Hence, we can write Equation (2.2) as the following

\[
(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_u^{\alpha_u})(p_u^{\alpha_{u+1}} p_{u+2}^{\alpha_{u+2}} \cdots p_v^{\alpha_v}) = q_1^{2\beta_1} q_2^{2\beta_2} \cdots q_k^{2\beta_k} q_{k+1} q_{k+1} . \tag{2.3}
\]
If we look at the details on Equations (2.3), two sides of the equation must be equal. Therefore, every \( p_i \) has to be equal with \( q_j \), so that \( \alpha_i = 2\beta_j \). Hence, every exponent \( \alpha_i \) is even. Consequently, \( \beta_j = \frac{\alpha_i}{2} \) is an integer.

Let \( m \) and \( n \) are integers with \( m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_u^{\alpha_u} \) and \( n = p_{u+1}^{\alpha_{u+1}} p_{u+2}^{\alpha_{u+2}} \cdots p_v^{\alpha_v} \). So,

\[
pq q_1^{2\beta_1} q_2^{2\beta_2} \cdots q_k^{2\beta_k} = pq \left( \frac{\alpha_1}{p_1^2} \frac{\alpha_2}{p_2^2} \cdots \frac{\alpha_u}{p_u^2} \right)^2 \left( \frac{\alpha_{u+1}}{p_{u+1}^2} \frac{\alpha_{u+2}}{p_{u+2}^2} \cdots \frac{\alpha_v}{p_v^2} \right)^2
\]

\[
pqt^2 = pqm^2n^2
\]

\[
pqt^2 = pqm^2n^2
\]

\[
pqt^2 = (pqm^2)(n^2)
\]

\[
pqt^2 = (pm^2)(qn^2)
\]

Case 2. \( p \neq q \)

If \( p \neq q \), then there are two \( p_i \) which are equal to each \( p \) and \( q \). Suppose both are \( p_c = p \) and \( p_c = q \). Then, Equation (2.2) can be written as the following

\[
p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_c^{\alpha_c} p_d^{\alpha_d} \cdots p_u^{\alpha_u} p_{u+1}^{\alpha_{u+1}} \cdots p_v^{\alpha_v} = pq q_1^{2\beta_1} q_2^{2\beta_2} \cdots q_k^{2\beta_k}
\]

\[
p_1^{\alpha_c} p_2^{\alpha_c} \cdots p_c^{\alpha_c} p_d^{\alpha_g} \cdots p_u^{\alpha_u} p_{u+1}^{\alpha_{u+1}} \cdots p_v^{\alpha_v} = q_1^{2\beta_1} q_2^{2\beta_2} \cdots q_k^{2\beta_k}
\]

where \( \alpha_c = \alpha_c - 1 \) and \( \alpha_g = \alpha_g - 1 \). For a note, positions of \( p_c \) and \( p_q \) in Equation (2.4) can be randomly in \( r \) or \( s \). We don’t go into detail about them because they will give the same result later. Using similar techniques in Case 1, we get every exponent \( \alpha_i \) in Equation (2.4) is even. Hence, \( \beta_j = \frac{\alpha_i}{2} \) is an integer.

Let \( m \) and \( n \) are integers with \( m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_c^{\alpha_c} p_d^{\alpha_d} \cdots p_u^{\alpha_u} \) and \( n = p_{u+1}^{\alpha_{u+1}} p_{u+2}^{\alpha_{u+2}} \cdots p_v^{\alpha_v} \). So,

\[
pq q_1^{2\beta_1} q_2^{2\beta_2} \cdots q_k^{2\beta_k} = pq \left( \frac{\alpha_1}{p_1^2} \frac{\alpha_2}{p_2^2} \cdots \frac{\alpha_u}{p_u^2} \right)^2 \left( \frac{\alpha_{u+1}}{p_{u+1}^2} \frac{\alpha_{u+2}}{p_{u+2}^2} \cdots \frac{\alpha_v}{p_v^2} \right)^2
\]

\[
pqt^2 = pqm^2n^2
\]

\[
pqt^2 = pqm^2n^2
\]

\[
pqt^2 = (pqm^2)(n^2)
\]

\[
pqt^2 = (pm^2)(qn^2)
\]

Combining Case 1 and Case 2, it has proven that \( rs = pqm^2 \) and \( s = n^2 \), \( r = m^2 \) and \( s = pqn^2 \), or \( r = pm^2 \) and \( s = qn^2 \), where \( r \) and \( s \) are integers.

**Example 2.13.** Take \( p = 3 \), \( q = 2 \) and \( t = 5 \). Hence, we get \( rs = pqt^2 = 150 \). Next, we can choose integers \( m \) and \( n \) to define \( r \) and \( s \), such as

i. \( m = 5 \) and \( n = 1 \) so that \( r = pqm^2 = 150 \) and \( s = n^2 = 1 \),

ii. \( m = 1 \) and \( n = 5 \) so that \( r = m^2 = 1 \) and \( s = pqn^2 = 150 \), or

iii. \( m = 25 \) and \( n = 1 \) so that \( r = pm^2 = 75 \) and \( s = qn^2 = 2 \).

It is clear that \( rs = 150 \) when \( r = 15 \) and \( s = 2 \), \( r = 1 \) and \( s = 150 \), or \( r = 75 \) and \( s = 2 \).

**Theorem 2.14.** The Diophantine equation \( x^2 + py^2 = z^2 \) with \( y \) is odd, and \( p,q \) are primes have no primitive-solution.
Proof. Using Theorem 2.11, If \( y \) is odd then \( x \) and \( z \) are even. Hence, \( z - x \) and \( z + x \) are even. Write \( z - x = t_1 \) and \( z + x = t_2 \), for integers \( t_1, t_2 \). From the Diophantine equation \( x^2 + pqy^2 = z^2 \), we get \( pqy^2 = (z - x)(z + x) = 4t_1t_2 \). Because \( y \) is odd, \( pq \) must divide by 4. The only possible values are \( p = 2 \) and \( q = 2 \). So, we have \( 4y^2 = (z - x)(z + x) \). If \( z - x = 4y^2 \) and \( z + x = 1 \), then \( z = \frac{4y^2 - 1}{2} \) is not an integer. So, this is impossible. Next, if \( z - x = 1 \) and \( z + x = 4y^2 \), then \( z = \frac{1-4y^2}{2} \) is not integer. So, this is also impossible. Then, If \( z - x = 2y \) and \( z + x = 2y \) then we get \( x = 0 \) but this is also not possible since \( (x, y, z) = 1 \). So, we can conclude that the Diophantine equation \( x^2 + pqy^2 = z^2 \) with \( y \) is odd don’t have primitive-solutions.

After we have proved Theorem 2.14, we will share our results on the case \( y \) is even.

In the following theorem, we determine the primitive-solutions of Diophantine equation \( x^2 + pqy^2 = z^2 \) for case of \( p = q \).

**Theorem 2.15.** The positive integers \( x, y, z \) is a primitive-solution of Diophantine equation \( x^2 + p^2y^2 = z^2 \) with \( y \) is even, and \( p \) is prime, if and only if \( x = m^2 - n^2, \ y = \frac{2}{p}mn, \) and \( z = m^2 + n^2 \), where \( (m, n) = 1, m \) and \( n \) have different parity, \( m > n, \) and \( m = pa \) or \( n = pb \) for any integers \( a, b \).

**Proof.** \((\Rightarrow)\) Let \( t = py \). Because \( y \) is even, \( t \) is also even. Based on Theorem 2.2, the primitive-solution of Diophantine equation \( x^2 + t^2 = z^2 \) such as \( x = m^2 - n^2, t = 2mn, \) and \( z = m^2 + n^2 \), with \( (m, n) = 1, m > n, \) and \( m, n \) has different parity. Because \( t = py \) and \( t = 2mn \), we get \( y = \frac{2}{p}mn \). Since \( y \) is a positive integer and \( p \) is prime, \( mn \) must be divisible by \( p \). Consequently, \( m = pa \) or \( n = pb \) for any integers \( a, b \).

\((\Leftarrow)\) We will show that \( x, y, z \) satisfies the Diophantine equation \( x^2 + p^2y^2 = z^2 \).

Case 1. \( m = pa \)

\[
x^2 + p^2y^2 = (m^2 - n^2) + p^2 \left( \frac{2}{p}mn \right)^2
= (p^2a^2 - n^2)^2 + (2pan)^2
= (p^2a^2 + n^2)^2
= (m^2 + n^2)^2
= z^2.
\]

Case 2. \( n = pb \)

\[
x^2 + p^2y^2 = (m^2 - n^2) + p^2 \left( \frac{2}{p}mn \right)^2
= (m - p^2b^2)^2 + (2mpb)^2
= (m^2 + p^2b^2)^2
= (m^2 + n^2)^2
= z^2.
\]

So, \( x, y, z \) is the solution of Diophantine equation \( x^2 + p^2y^2 = z^2 \). Next, integers \( x, y, z \) is called primitive if \( (x, y, z) = 1 \). Suppose \( (x, y, z) \neq 1 \). This means that there is a prime \( p \) such that \( p = (x, y, z) \). Hence, \( p|x \) and \( p|z \). Furthermore, \( p|(x + z) = 2m^2 \) and \( p|(x - z) = n^2 \). Because \( m \) and \( n \) have different parity, we get \( p \neq 2 \) so that \( p|m^2 \) and \( p|m \). Also, it is clear that \( p|n^2 \) and \( p|n \). Because \( p|m \) and \( p|n \), we can conclude that \( p = (m, n) \). It contradicts to \( (m, n) = 1 \). However, it must be \( (x, y, z) = 1 \). So, \( x, y, z \) is a primitive-solution of Diophantine equation \( x^2 + p^2y^2 = z^2 \).
Example 2.16. Take $m = 3$ and $n = 2$. Hence, we get $x = m^2 - n^2 = 5$, $y = \frac{2}{p} mn = 4$ for $p = 3$, and $z = m^2 + n^2 = 13$. It is clear that 5,4,13 is a primitive-solution of Diophantine equation $x^2 + 9y^2 = z^2$.

Theorem 2.17. The positive integers $x, y, z$ with $y$ is even is a primitive-solution of Diophantine equation $x^2 + pqy^2 = z^2$ if and only if

i. $x = pqm^2 - n^2$, $y = 2mn$, and $z = pqm^2 + n^2$.

ii. $x = m^2 - pqn^2$, $y = 2mn$, and $z = m^2 + pqn^2$, or

iii. $x = pm^2 - pn^2$, $y = 2mn$, and $z = pm^2 + qn^2$.

where $(m, n) = 1$, $m > n$, and $m, n$ has different parity.

Proof. $(\Rightarrow)$ Based on Theorem 2.9, If $y$ is even, then $x$ and $z$ are odd. Hence, $z + x$ dan $z - x$ are even so that there are two integers $r = \frac{x + z}{2}$ and $s = \frac{z - x}{2}$. Write $y = 2t$, for any integer $t$. So, we get $x^2 + pq(2t)^2 = z^2$ or $pq t^2 = rs$. Furthermore, using Theorem 2.12, we have

i. $r = pqm^2$ and $s = n^2$.

ii. $r = m^2$ and $s = pqn^2$, or

iii. $r = pm^2$ and $s = qn^2$.

Substituting values of $r$ and $s$ above to the equations $r = \frac{x + z}{2}$, $s = \frac{z - x}{2}$ and $y = 2t$. We get respectively

i. $x = pqm^2 - n^2$, $y = 2mn$, and $z = pqm^2 + n^2$.

ii. $x = m^2 - pqn^2$, $y = 2mn$, and $z = m^2 + pqn^2$, and

iii. $x = pm^2 - pn^2$, $y = 2mn$, and $z = pm^2 + qn^2$.

$(\Leftarrow)$ We substitute values of $x, y$ and $z$ to the Diophantine equation $x^2 + pqy^2 = z^2$.

i. $x^2 + pqy^2 = (pqm^2 - n^2)^2 + pq(2mn)^2$

$= p^2 q^2 m^4 + 2pqm^2 n^2 + n^4$

$= (pqm^2 + n^2)^2$

$= z^2$.

ii. $x^2 + pqy^2 = (m^2 - pqn^2)^2 + pq(2mn)^2$

$= m^4 + 2pq m^2 n^2 + p^2 q^2 n^4$

$= (m^2 + pqn^2)^2$

$= z^2$.

iii. $x^2 + pqy^2 = (pm^2 - qn^2)^2 + pq(2mn)^2$

$= p^2 m^4 + 2pqm^2 n^2 + q^2 n^4$

$= (pm^2 + pn^2)^2$

$= z^2$.

Because $(m, n) = 1$, $m > n$, and $m, n$ has different parity, we can conclude that integers $x, y, z$ is a primitive-solution of Diophantine equation $x^2 + pqy^2 = z^2$. Also, from $y = 2mn$, we get $y$ which is even.

Example 2.18. Take $p = 47$, $q = 43$, $m = 2$ and $n = 1$. It is clear that
i. \( x = pqm^2 - n^2 = 8083, y = 2mn = 4 \) and \( z = pqm^2 + n^2 = 8085 \), and 

ii. \( x = pm^2 - pn^2 = 145, y = 2mn = 4 \) and \( z = pm^2 + qn^2 = 231 \) are two primitive-solutions of Diophantine equation \( x^2 + 2021y^2 = z^2 \).

**Example 2.19.** Take \( p = 47, q = 43, m = 46 \) and \( n = 1 \). Hence, we get \( x = m^2 - pqn^2 = 95, y = 2mn = 92, \) and \( z = m^2 + pqn^2 = 4137 \). From Example 2.10, we get 95,92,4137 is the primitive-solution of Diophantine equation \( x^2 + 2021y^2 = z^2 \).

**REFERENCES**


