Thai Journal of **Math**ematics
Volume 22 Number 4 (2024)
Pages 579–593

http://thaijmath.in.cmu.ac.th

ISSN 1686-0209

Investigating Integer Solutions to Quadratic Diophantine Equations Using Quadratic Residues

Bal Bahadur Tamang* **and Ajaya Singh**

Central Department of Mathematics, Institute of Science and Technology, Tribhuvan University, Nepal
e-mail : bal.tamang@mrmc.tu.edu.np (B.B. Tamang); singh.ajaya1@gmail.com (A. Singh)

Abstract In this paper, we study integer solutions to quadratic Diophantine equations of the form $x^2 - Dy^2 = N$, where D is a composite number that is not a perfect square, such as $D = 14, 15, 18$, and N is an odd integer. We discuss the quadratic residues and use some strategies to determine whether these equations are solvable or not. Additionally, we apply strategies, such as the Euclidean algorithm, Bézout's identity, Thue's theorem, the Legendre symbol, the quadratic reciprocity law, and the Chinese remainder theorem to analyze the solvability and unsolvability of modified quadratic Diophantine equations. We identify research gaps in solving quadratic Diophantine equations, particularly when D is a large composite number and N is a large integer, and develop computational methods to enhance their solvability.

MSC: 11A15; 11D09; 11D79; 11F50
Keywords: integer solutions; quadratic Diophantine equation; solvability; quadratic residues

Submission date: 16.01.2024 / Acceptance date: 16.08.2024

1. Introduction

A Diophantine equation is a polynomial equation with integer coefficients that seeks solutions from the integers. Diophantine equation aims to find the integer solutions. A quadratic Diophantine equation is a polynomial equation of degree two in two variables, x and y, to find all integer solutions. These equations are essential to number theory and are frequently solved using modular arithmetic, continued fractions, and algebraic manipulation. In modular arithmetic, two integers a and b are said to be congruent modulo n, where n is modulo if their difference $a - b$ is divisible by n. It is denoted by $a \equiv b (\mathrm{mod}\, n)$. This paper aims to study integer solutions of quadratic Diophantine equations of the form $x^2 - Dy^2 = N$, where D is a composite number that is not a perfect square, such as $D = 14, 15, 18$, and N is an odd integer. We describe the concept of quadratic residues and apply some strategies like the Legendre symbol, Jacobi symbol, the quadratic reciprocity law, the Chinese remainder theorem, Thue's theorem, Bézout's identity, and the Euclidean algorithm. These strategies are used to determine

*Corresponding author

Published by The Mathematical Association of Thailand.

the solvability of quadratic Diophantine equations for given values of D and N. We also address a research gap by investigating solutions to the equation $x^2 - Dy^2 = N$, when D is a composite, not a perfect square and N is an odd integer. Mathematicians such as Lagrange, Legendre, and Gauss [1] explored and developed methods for classifying and solving quadratic Diophantine equations, frequently using the quadratic residue. It is an important concept in the study of Diophantine equations and congruences. The idea of quadratic residues is closely related to the quadratic reciprocity law [2], which is a significant and fascinating result concerning the integer solutions of quadratic Diophantine equations. Let a be an integer and p an odd prime number such that $(a, p) = 1$. A quadratic residue modulo p is the value a for which the congruence $x^2 \equiv a(\mathrm{mod}\, p)$ has a solution. Conversely, a is called a quadratic non-residue modulo p if the congruence $x^2 \equiv a(\mathrm{mod}\, p)$ has no solution. The Legendre symbol $\left(\frac{a}{p}\right)$, as defined in [3], represents the following:

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p, \\ 0 & \text{if } a \equiv 0(\mathrm{mod}\, p). \end{cases}$$

The Jacobi symbol [4] is generalization of the Legendre symbol to any positive odd integer. For example, given the prime factorization of Q as $Q = q_1^{\alpha_1} \cdots q_k^{\alpha_k}$, where each q_i is an odd prime, the Jacobi symbol can be expressed as:

$$\left(\frac{p}{Q}\right) = \Pi_{i=1}^{k} \left(\frac{p}{q_i}\right)^{\alpha_k} = \left(\frac{p}{q_1}\right)^{\alpha_1} \cdots \left(\frac{p}{q_k}\right)^{\alpha_k}.$$

Lagrange [5] extended the concept of continued fractions by incorporating non-trivial integer solutions to quadratic Diophantine equations. Serret [6] and Hermite [7] introduced the idea of solving $p = x^2 + y^2$ using Euclid's algorithm, which was later generalized to $p = x^2 + ny^2$, where $n = 2, 3, 5$. The ability of the Serret-Hermite approach to identify explicit solutions for the equation $x^2 - dy^2 = N$, when $d > 1$ is a small integer, is a significant achievement. Uspensky and Heaslet [8] addressed the cases $d = 2, 3, 5$ using a different version of Thue's theorem. Meanwhile, Nagell [9] explored the cases $d = 2, 3$ with a non-constructive variation of Thue's theorem [10]. Cornacchia [11] developed the theory for the equation $N = x^2 + ny^2$ for $n \geq 1$ and investigated conditions when $n < 0$. Matthews [12] constructed representations for equations of the form $x^2 - Dy^2$ with $D = 2, 3, 5, 6, 7$. Thomas [13] examined the representation of integers using the quadratic form $x^2 - Dy^2$ for $D = 10, 11$. Tamang and Singh [14] built upon the work of Matthews by investigating integer solutions of the equation $x^2 - Dy^2 = N$, focusing on cases where D is a prime number and N is an odd integer.

The work of Matthews [12] on quadratic Diophantine equations for specific values of D highlights a research gap in analyzing certain cases of D and N in the equation $x^2 - Dy^2 = N$. While the solutions for $D = 2$ and $D = 3$ are well understood, there is still a lack of detailed analysis for composite numbers of D and an odd integer N. The most challenging problems arise when N is a large odd integer and D is a large composite number. The prime factorization of D plays a critical role in finding solutions to the equation. When D is a large composite number, factorizing it into primes and determining the corresponding integer solutions becomes significantly more complex. Evaluating

the impact of factorizing large composite numbers of D on the solution is particularly demanding and requires further investigation.

2. Preliminaries

In this section, we discuss some algorithms and theorems for determining integer solutions and addressing the research gap in quadratic Diophantine equations. The division algorithm states that if $a, b \in \mathbb{Z}$ with $a > 0$, then there exist integers q and r such that $b = qa + r$, where $0 \leq r < a$. Problems can be solved by simply working with the remainder r. The study of the properties of remainders forms the basis of modular arithmetic. In general, if $b = qa + r$, then $b \equiv r \bmod a$ since $a \mid (b - r)$. The Euclidean algorithm [15, 16] provides techniques for determining the existence of integer solutions to quadratic Diophantine equations. Using the division algorithm, we outline the Euclidean algorithm as follows:

$$
\begin{aligned}
&a = bq_1 + r_1,\ 0 < r_1 < b,\\
&b = r_1q_2 + r_2,\ 0 < r_2 < r_1,\\
&r_1 = r_2q_3 + r_3,\ 0 < r_3 < r_2,\\
&\vdots \qquad\qquad \vdots\\
&r_{k-2} = r_{k-1}q_k + r_k,\ 0 < r_k < r_{k-1},\\
&r_{k-1} = r_kq_{k+1}.
\end{aligned}
$$

The algorithm terminates when $r_{k+1} = 0$. The final non-zero remainder r_k, represents the greatest common divisor of a and b. Furthermore, r_k can be expressed as a linear combination of a and b.

Theorem 2.1 (Bézout's identity [17]). *For each non-zero $a, b \in \mathbb{Z}$, there exist $s, t \in \mathbb{Z}$ such that $as + bt = \gcd(a, b)$, where $\gcd(a, b)$ refers to the greatest common divisor of a and b.*

Therefore, Bézout's identity (Theorem 2.1) asserts that the greatest common divisor of two integers can be expressed as a linear combination of those integers, with integer coefficients s and t. In the Euclidean algorithm, we set $a = r_0$ and $b = r_1$, where r_1 is the remainder after the first division. For each step k, we obtain $r_{k-1} = r_kq_k + r_{k+1}$, where q_k is the quotient obtained by dividing r_{k-1} by r_k, and r_{k+1} is the remainder. This process continues until we reach a remainder of 0, which means that $r_{k+1} = 0$ for some k.

We define s_k and t_k as the coefficients of a and b in the expression $r_k = s_ka + t_kb$. The signs alternate, so we have $s_k = (-1)^k|s_k|$ and $t_k = (-1)^{k+1}|t_k|$. This implies that the linear combination $as + bt$ also has alternating signs. The initial values are $s_0 = 1$, $s_1 = 0$, $t_0 = 0$, and $t_1 = 1$. The recurrence relations are $t_{k+1} = -q_kt_k + t_{k-1}$ and $s_{k+1} = -q_ks_k + s_{k-1}$. Additionally, a can be expressed as a linear combination of r_{k-1} and r_k with coefficients $|t_k|$ and $|t_{k-1}|$ such that $a = |t_k|r_{k-1} + |t_{k-1}|r_k$ for $1 \leq k \leq n+1$.

Theorem 2.2 (Thue's theorem [10]). *Let $a, b \in \mathbb{Z}$, with a and b being relatively prime. Then the congruence $bx \equiv y (\bmod a)$ has a solution in non-zero integers x and y such that $|x| < \sqrt{a}$ and $|y| < \sqrt{a}$.*

Theorem 2.2 asserts that in the Euclidean algorithm, the remainders $r_0, \cdots, r_n$ strictly decrease to 1, and there exists a least index k such that $r_{k-1} > \sqrt{a} > r_k$. From $a = |t_k|r_{k-1} + |t_{k-1}|r_k$, we deduce that $a > |t_k|r_{k-1} > |t_k|\sqrt{a}$. Hence, $|t_k| < \sqrt{a}$. Since $r_k = s_k a + t_k b$ for $1 \leq k \leq n+1$, it follows that $r_k \equiv bt_k \pmod{a}$. Consequently, $x = r_k$ and $y = t_k$ are integer solutions to the congruence.

Theorem 2.3 (Chinese remainder theorem [18]). *For any integers $p_1, p_2, \cdots, p_r$, and $q_1, q_2, \cdots, q_r$ are relatively prime in pairs, then simultaneous congruences*

$$x \equiv p_1 (\mathrm{mod}\, q_1), x \equiv p_2 (\mathrm{mod}\, q_2), x \equiv \cdots, x \equiv p_r (\mathrm{mod}\, q_r). \tag{2.1}$$

has a solution, and this solution is unique modulo q, where $q = q_1 q_2 \cdots q_r$. If x_0 is a solution, then an integer x satisfies the congruence (2.1) if and only if x is of the form $x = x_0 + kq$, for some integer k.

Quadratic Diophantine equations often have solutions that must be considered modulo some number. Theorem 2.3 helps in finding the solutions by breaking the problem into simpler congruences modulo pairwise co-prime numbers, and then reconstructing the original solution. The process of solving congruences modulo large numbers can be computationally expensive. However, the overall computational effort is reduced by breaking the problem down using Theorem 2.3.

By adapting these algorithms and theorems to the specific properties of different values of D and N, we can bridge the research gap and enhance the efficiency of solving quadratic Diophantine equations.

3. Main Results

We investigate the main result concerning the integer solutions to the quadratic Diophantine equation of the form $x^2 - Dy^2 = N$. We extend the work of Matthew in this study to include an odd integer N and a composite number D that is not a perfect square, such as $D = 14, 15, 18$. When N is a non-zero integer and $D > 1$ is not a perfect square, a necessary condition for the solvability of the equation $x^2 - Dy^2 = N$ with $\gcd(x, y) = 1$ is that the congruence $u^2 \equiv D (\mathrm{mod}\, N)$ is solvable, where $u = xy^{-1}$. Using the modulo operation with N and $\gcd(D, N) = 1$, along with the condition that $1 < u < N$, the Jacobi symbol $\left(\frac{D}{N}\right) = 1$, which means that the congruence $u^2 \equiv D (\mathrm{mod}\, N)$ is solvable.

When we substitute a with N and b with u in the Euclidean algorithm, the values of the expression $r_k^2 - Dt_k^2$ consistently decrease for every $k = 0, \cdots, n$ from N^2 to $1 - Dt_k^2$, and multiple of N, where (r_k, t_k) are integer solutions to the quadratic Diophantine equation $x^2 - Dy^2 = N$. For this, we have $r_k^2 - Dt_k^2 \equiv (s_k N + t_k u)^2 = t_k^2(u^2 - D) \equiv 0 (\mathrm{mod}\, N)$. If r_k and t_k have the same remainder when divided by N, then r_k must monotonically decrease to 0. Thue's Theorem 2.2 shows that the congruence has a solution such that $|r_k| < \sqrt{N}$ and $|t_k| < \sqrt{N}$. It gives

$$r_k^2 - Dt_k^2 < N, \tag{3.1}$$

and we have $t_k^2 < N$, which implies that

$$-DN < r_k^2 - Dt_k^2. \tag{3.2}$$

Combining equations (3.1) and (3.2), we obtain $-DN < r_k^2 - Dt_k^2 < N$. Hence, the equation $r_k^2 - Dt_k^2 = -lN$, where $-1 < l < D$. In fact, $1 \leq l < D$ and this equation can

be expressed as;

$$-DN < r_k^2 - Dt_k^2 \leq -N.$$

This inequality represents the modified quadratic Diophantine equations. There exists a least index $1 \leq k \leq n$ such that $r_k < \sqrt{N}$, and $r_k < \sqrt{N} < r_{k-1}$. From the Euclidean algorithm, we deduce $N = r_{k-1}|t_k| + r_k|t_{k-1}| > r_{k-1}|t_k|$. This leads to $\frac{N}{r_{k-1}} > |t_k| > \sqrt{\frac{lN}{D}}$, and we find $r_{k-1} < \sqrt{\frac{DN}{l}}$. Additionally, it is crucial to note that $r_k^2 - Dt_k^2 = -lN$, which implies that $|t_k| > \sqrt{\frac{lN}{D}}$. Similar to the Euclidean algorithm, we can write

$$(r_k r_{k-1} - Dt_k t_{k-1})^2 - D(r_k t_{k-1} - r_{k-1} t_k)^2 = (r_k^2 - Dt_k^2)(r_{k-1}^2 - Dt_{k-1}^2). \quad (3.3)$$

Since $t_k t_{k-1} < 0$, and denoting $|t_k| = T_k$ and $|t_{k-1}| = T_{k-1}$, equation (3.3) can be expressed as follows:

$$(r_k r_{k-1} + DT_k T_{k-1})^2 = DN^2 + (r_k^2 - Dt_k^2)(r_{k-1}^2 - Dt_{k-1}^2), \quad (3.4)$$

$$r_{k-1} T_k + r_k T_{k-1} = N. \quad (3.5)$$

Solving equations (3.4) and (3.5), we obtain the non-trivial integer solutions of the modified quadratic Diophantine equations. Since $1 \leq l_k l_{k-1} < D^2$, we have

$$r_k r_{k-1} + Dt_k t_{k-1} = \sqrt{l_k l_{k-1} + DN^2}, \quad (3.6)$$

where $l_k = (r_k^2 - Dt_k^2)$ and $l_{k-1} = (r_{k-1}^2 - Dt_{k-1}^2)$. The left-hand side of equation (3.6) is an integer, so the right-hand side must also be an integer. Therefore, equation (3.6) provides the integer solutions and identify the conditions for the solvability and unsolvability of the modified quadratic Diophantine equations.

Theorem 3.1. *Let $D = 14$ be a composite number and N be an odd integer in the quadratic Diophantine equation $x^2 - Dy^2 = N$. Assume that $x^2 \equiv 14 (\mathrm{mod}\ N)$ is solvable and $\gcd(14, N) = 1$. Then $\left(\frac{14}{N}\right) = 1$ when*

$$N \equiv \pm 1, \pm 3, \pm 5, \pm 9, \pm 11, \pm 13, \pm 15, \pm 17, \pm 19, \pm 23, \pm 25, \pm 27 (\mathrm{mod}\ 56).$$

The equation $x^2 - 14y^2 = N$ is solvable when $\left(\frac{14}{N}\right) = 1$. Moreover, assume that (r_k, t_k) is the integer solution to the equation $x^2 - 14y^2 = N$. Then

$$r_k^2 - 14t_k^2 = -13N, -12N, -11N, -10N, -9N, -8N, -7N, -6N - 5N, -4N, -3N, -2N, -N.$$

Proof. Given the quadratic Diophantine equation $x^2 - 14y^2 = N$ can be expressed in the congruence form $x^2 \equiv 14 (\mathrm{mod}\ N)$, which is solvable and $\gcd(14, N) = 1$. Using the quadratic reciprocity law, the Jacobi symbol can be expressed as $\left(\frac{14}{N}\right) = \left(\frac{2}{N}\right)\left(\frac{7}{N}\right)$, where

$$\left(\frac{2}{N}\right) = \begin{cases} +1 & \text{if } N \equiv 1, 7 (\mathrm{mod}\ 8) \\ -1 & \text{if } N \equiv 3, 5 (\mathrm{mod}\ 8), \end{cases}$$

and $\left(\frac{7}{N}\right) = 1$ if $N \equiv 1, 3, 9, 19, 25, 27 (\mathrm{mod}\ 28)$. Using the Chinese remainder theorem, we reduce the expression to $\left(\frac{7}{N}\right) = 1$ when $N \equiv 1, 3, 9, 19, 25, 27 (\mathrm{mod}\ 7)$. Combining $N \equiv 1, 7 (\mathrm{mod}\ 8)$ and $N \equiv 1, 3, 9, 19, 25, 27 (\mathrm{mod}\ 7)$ using Chinese remainder theorem, we obtain $N \equiv \pm 1, \pm 9, \pm 15, \pm 17, \pm 23, \pm 25 (\mathrm{mod}\ 56)$ and we combine $N \equiv 3, 5 (\mathrm{mod}\ 8)$ and $N \equiv 1, 3, 9, 19, 25, 27 (\mathrm{mod}\ 7)$, we find $N \equiv \pm 3, \pm 5, \pm 11, \pm 13, \pm 19, \pm 27 (\mathrm{mod}\ 56)$. Thus, $\left(\frac{2}{N}\right)\left(\frac{7}{N}\right) = 1$ if $N \equiv \pm 1, \pm 3, \pm 5, \pm 9, \pm 11, \pm 13, \pm 15, \pm 17, \pm 19, \pm 23, \pm 25, \pm 27 (\mathrm{mod}\ 56)$.

This implies that the equation $x^2 - 14y^2 = N$ is solvable when $\left(\frac{14}{N}\right) = 1$. Conversely, if $\left(\frac{14}{N}\right) = -1$, the equation $x^2 - 14y^2 = N$ is unsolvable.

As a counterexample, we consider the Jacobi symbol $\left(\frac{14}{27}\right) = -1$. This indicates that the congruence $x^2 \equiv 14 (\mathrm{mod}\, 27)$ has no solution. Therefore, 14 is a quadratic non-residue modulo 27. Hence, $x^2 - 14y^2 = 27$ is unsolvable.

Suppose (η_0, ζ_0) is a nonzero solution to the general Pell's equation $x^2 - Dy^2 = \pm N$, where η_0 and ζ_0 are integers, a positive integer D is not perfect square and N ia a non zero integer. Let (x_n, y_n) be other solution in the same equivalence class as (η_0, ζ_0) and (r_1, t_1) be the smallest positive solution of the Pell's equation $x^2 - Dy^2 = 1$. Then the general solutions (x_n, y_n) for $x^2 - Dy^2 = \pm N$ can be expressed as:

$$(x_n + y_n\sqrt{D}) = (\eta_0 + \zeta_0\sqrt{D})(r_1 + t_1\sqrt{D})^n,\ n \in \mathbb{Z}^+.$$

Thus, if we take $D = 14$ and a non zero integer N in the equation $x^2 - 14y^2 = \pm N$, we can find the smallest solution $(r_1, t_1) = (15, 4)$ to equation $x^2 - 14y^2 = 1$ using the continued fraction expansion of $\sqrt{14}$ and its convergents. Let (η_0, ζ_0) be any particular solution to the equation $x^2 - Dy^2 = \pm N$. Then the general solutions (x_n, y_n) for the equation $x^2 - 14y^2 = \pm N$ can be derived from:

$$(x_n + y_n\sqrt{14}) = (\eta_0 + \zeta_0\sqrt{14})(15 + 4\sqrt{14})^n,\ n \in \mathbb{Z}^+.$$

A similar approach can be applied for $D = 15$ and 18, where a non zero integer N is considered in the equation $x^2 - Dy^2 = \pm N$, under the condition $|N| < \sqrt{D}$.

Assuming that (r_k, t_k) represents the integer solutions to the equation $x^2 - 14y^2 = N$, we have $r_k^2 - 14t_k^2 = -lN$, for all $1 \leq l < 14$, implying that $-14N < r_k^2 - 14t_k^2 \leq -N$. Thus, the modified equations become $r_k^2 - 14t_k^2 = -13N, -12N, -11N, -10N, -9N, -8N, -7N, -6N, -5N, -4N, -3N, -2N, -N$. The solvability of these modified equations depends on the value of N modulo 56 and whether N is a quadratic residue or non-residue modulo 56. If N is a quadratic non-residue modulo 56, the equations have no integer solutions. In particular, the modified equations $r_k^2 - 14t_k^2 = -12N, -9N, -8N, -6N, -4N, -3N$ are unsolvable because they represent quadratic non-residues modulo 56.

The equation $r_k^2 - 14t_k^2 = -13N$ is solvable and the solutions are $r_k \equiv \pm 1 (\mathrm{mod}\, 7)$ when $N \equiv 1, -13, 15, -27 (\mathrm{mod}\, 56)$, $r_k \equiv \pm 2 (\mathrm{mod}\, 7)$ when $N \equiv -3, 11, -17, 25 (\mathrm{mod}\, 56)$ and $r_k \equiv \pm 3 (\mathrm{mod}\, 7)$ when $N \equiv -5, 9, -19, 23 (\mathrm{mod}\, 56)$ respectively. Taking modulo 13 in equation $r_k^2 - 14t_k^2 = -13N$, we have $r_k^2 - 14t_k^2 \equiv 0 (\mathrm{mod}\, 13)$ implies $r_k \equiv \pm t_k (\mathrm{mod}\, 13)$. Since $r_{k-1}^2 < \frac{14N}{13}$, then $-13N = r_k^2 - 14t_k^2 < r_{k-1}^2 - 14t_{k-1}^2 < r_{k-1}^2 < \frac{14N}{13}$. This implies that $r_{k-1}^2 - 14t_{k-1}^2 = -12N, -11N, -10N, -9N, -8N, -7N, -6N, -5N, -4N, -3N, -2N, -N, N$. Only two equations $r_{k-1}^2 - 14t_{k-1}^2 = -10N, N$ are solvable and we have

$$14T_k = 12r_k + 13r_{k-1}, r_k = 12T_k - 13T_{k-1},$$
$$14T_k = r_k + 13r_{k-1}, r_k = T_k - 13T_{k-1}.$$

From these relations, we obtain the solutions are $r_k \equiv \pm T_k (\mathrm{mod}\, 13)$. Other equations $r_{k-1}^2 - 14t_{k-1}^2 = -12N, -11N, -9N, -8N, -7N, -6N, -5N, -4N, -3N, -2N, -N$ are unsolvable because these equations are not satisfied equation (3.6).

The equations $r_k^2 - 14t_k^2 = -11N$ is solvable and the solutions are $r_k \equiv \pm 1 (\mathrm{mod}\, 7)$ when $N \equiv 5, -9, 19, -23 (\mathrm{mod}\, 56)$, $r_k \equiv \pm 2 (\mathrm{mod}\, 7)$ when $N \equiv -1, 13, -15, 27 (\mathrm{mod}\, 56)$ and $r_k \equiv \pm 3 (\mathrm{mod}\, 7)$ when $N \equiv 3, -11, 17, -25 (\mathrm{mod}\, 56)$ respectively. Taking modulo 11 in equation $r_k^2 - 14t_k^2 = -11N$, then $r_k^2 - 14t_k^2 \equiv 0 (\mathrm{mod}\, 11)$, we have $r_k \equiv \pm 5t_k (\mathrm{mod}\, 11)$.

Since $r_{k-1} < \frac{14N}{11}$, then $-11N = r_k^2 - 14t_k^2 < r_{k-1}^2 - 14t_{k-1}^2 < r_{k-1}^2 < \frac{14N}{11}$ implies $r_{k-1}^2 - 14t_{k-1}^2 = -10N, -9N, -8N, -7N, -6N, -5N, -4N, -3N, -2N, -N, N$. The equations $r_{k-1}^2 - 14t_{k-1}^2 = -2N, -N$ are solvable and

$$14T_k = 6r_k + 11r_{k-1}, r_k = 6T_k - 11T_{k-1},$$
$$14T_k = 5r_k + 11r_{k-1}, r_k = 5T_k - 11T_{k-1}.$$

Combining these relations, we obtain the solutions are $r_k \equiv \pm 5T_k (\mathrm{mod}\, 11)$. Equations $r_{k-1}^2 - 14t_{k-1}^2 = -10N, -9N, -8N, -7N, -6N, -5N, -4N, -3N, N$ are unsolvable.

The equation $r_k^2 - 14t_k^2 = -10N$ is solvable and solutions are $r_k \equiv \pm 1 (\mathrm{mod}\, 7)$ when $N \equiv -5, 9, -19, 23 (\mathrm{mod}\, 56)$, $r_k \equiv \pm 2 (\mathrm{mod}\, 7)$ when $N \equiv 1, -13, 15, -27 (\mathrm{mod}\, 56)$ and $r_k \equiv \pm 3 (\mathrm{mod}\, 7)$ when $N \equiv -3, 11, -17, 25 (\mathrm{mod}\, 56)$ respectively. Taking modulo 10 in equation $r_k^2 - 14t_k^2 = -10N$, we get $r_k^2 - 14t_k^2 \equiv 0 (\mathrm{mod}\, 10)$ implies $r_k \equiv \pm 2t_k (\mathrm{mod}\, 10)$. Since $r_{k-1} < \frac{14N}{10}$, then $-10N = r_k^2 - 14t_k^2 < r_{k-1}^2 - 14t_{k-1}^2 < r_{k-1}^2 < \frac{14N}{10}$. This implies that $r_{k-1}^2 - 14t_{k-1}^2 = -9N, -8N, -7N, -6N, -5N, -4N, -3N, -2N, -N, N$. Two equations $r_{k-1}^2 - 14t_{k-1}^2 = -5N, N$ are solvable and we get

$$7T_k = 4r_k + 5r_{k-1}, r_k = 8T_k - 10T_{k-1},$$
$$7T_k = r_k + 5r_{k-1}, r_k = 2T_k - 10T_{k-1}.$$

From these relations, we obtain the solutions are $r_k \equiv \pm 2T_k (\mathrm{mod}\, 10)$. Other equations $r_{k-1}^2 - 14t_{k-1}^2 = -9N, -8N, -7N, -6N, -4N, -3N, -2N, -N$ are unsolvable from equation (3.6) gives $\sqrt{104}, \sqrt{94}, \sqrt{84}, \sqrt{74}, \sqrt{54}, \sqrt{44}, \sqrt{34}, \sqrt{24}$. These values are not given integer solutions.

The equations $r_k^2 - 14t_k^2 = -7N$ is solvable and solutions are $r_k^2 \equiv 0 (\mathrm{mod}\, 7)$ when $N \equiv \pm 1, \pm 3, \pm 5, \pm 9, \pm 11, \pm 13, \pm 15, \pm 17, \pm 19, \pm 23, \pm 25, \pm 27 (\mathrm{mod}\, 56)$. Taking modulo 7 in equation $r_k^2 - 14t_k^2 = -7N$, we get $r_k^2 - 14t_k^2 \equiv 0 (\mathrm{mod}\, 7)$. Then $r_k^2 \equiv 0 (\mathrm{mod}\, 7)$. Since $r_{k-1} < \frac{14N}{7}$, we get $-7N = r_k^2 - 14t_k^2 < r_{k-1}^2 - 14t_{k-1}^2 < r_{k-1}^2 < \frac{14N}{7}$. This implies that $r_{k-1}^2 - 14t_{k-1}^2 = -6N, -5N, -4N, -3N, -2N, -N, N$. Only one equation $r_{k-1}^2 - 14t_{k-1}^2 = -5N$ is solvable and we get $2T_k = r_k + r_{k-1}, r_k = 7T_k - 7T_{k-1}$, and solution is $r_k \equiv 0 (\mathrm{mod}\, 7)$. Other equations $r_{k-1}^2 - 14t_{k-1}^2 = -6N, -4N, -3N, -2N, -N, N$ are unsolvable.

The equations $r_k^2 - 14t_k^2 = -5N$ is solvable and solutions are $r_k \equiv \pm 1 (\mathrm{mod}\, 7)$ when $N \equiv -3, 11, -17, 25 (\mathrm{mod}\, 56)$, $r_k \equiv \pm 2 (\mathrm{mod}\, 7)$ when $N \equiv -5, 9, -19, 23 (\mathrm{mod}\, 56)$ and $r_k \equiv \pm 3 (\mathrm{mod}\, 7)$ when $N \equiv 1, -13, 15, -27 (\mathrm{mod}\, 56)$ respectively. Taking modulo 5 in equation $r_k^2 - 14t_k^2 = -5N$, we have $r_k^2 - 14t_k^2 \equiv 0 (\mathrm{mod}\ 5)$ implies that $r_k \equiv \pm 2t_k (\mathrm{mod}\ 5)$. Since $r_{k-1}^2 < \frac{14N}{5}$, then $-5N = r_k^2 - 14t_k^2 < r_{k-1}^2 - 14t_{k-1}^2 < r_{k-1}^2 < \frac{14N}{5}$ implies $r_{k-1}^2 - 14t_{k-1}^2 = -4N, -3N, -2N, -N, N, 2N$. Only two equations $r_{k-1}^2 - 14t_{k-1}^2 = N, 2N$ are solvable and we have $14T_k = 3r_k + 5r_{k-1}, r_k = 3T_k - 5T_{k-1}$and gives the solution is $r_k \equiv -2T_k (\mathrm{mod}\ 5)$ and $14T_k = 2r_k + 5r_{k-1}, r_k = 2T_k - 5T_{k-1}$ and gives the solution is $r_k \equiv 2T_k (\mathrm{mod}\ 5)$. Equations $r_{k-1}^2 - 14t_{k-1}^2 = -4N, -3N, -2N, -N$ are unsolvable.

The equations $r_k^2 - 14t_k^2 = -2N$ is solvable and solutions are $r_k \equiv \pm 1 (\mathrm{mod}\, 7)$ when $N \equiv 3, -11, 17, -25 (\mathrm{mod}\, 56)$, $r_k \equiv \pm 2 (\mathrm{mod}\, 7)$ when $N \equiv 5, -9, 19, -23 (\mathrm{mod}\, 56)$ and $r_k \equiv \pm 3 (\mathrm{mod}\, 7)$ when $N \equiv -1, 13, -15, 27 (\mathrm{mod}\, 56)$ respectively. Taking modulo 2 in equation $r_k^2 - 14t_k^2 = -2N$, then $r_k^2 - 14t_k^2 \equiv 0 (\mathrm{mod}\, 2)$ implies that $r_k \equiv 0 (\mathrm{mod}\, 2)$. Since $r_{k-1}^2 < \frac{14N}{2}$ then $-2N = r_k^2 - 14t_k^2 < r_{k-1}^2 - 14t_{k-1}^2 < r_{k-1}^2 < \frac{14N}{2}$ implies $r_{k-1}^2 - 14t_{k-1}^2 = -N, N, 2N, 3N, 4N, 5N, 6N$. The equations $r_{k-1}^2 - 14t_{k-1}^2 = -N, 5N$ are

solvable and we have

$$14T_k = 4r_k + 2r_{k-1}, 2T_{k-1} = 4T_k - r_k,$$
$$7T_k = r_k + r_{k-1}, 2T_{k-1} = 2T_k - r_k.$$

Combining this relation, we have the solution is $r_k \equiv 0(\mathrm{mod}\, 2)$. Similarly, other equations $r_{k-1}^2 - 14t_{k-1}^2 = N, 2N, 3N, 4N, 6N$, are unsolvable.

The equations $r_k^2 - 14t_k^2 = -N$ is solvable and solutions are $r_k \equiv \pm 1(\mathrm{mod}\, 7)$ when $N \equiv -1, 13, -15, 27(\mathrm{mod}\, 56)$, $r_k \equiv \pm 2(\mathrm{mod}\, 7)$ when $N \equiv 3, -11, 17, -25(\mathrm{mod}\, 56)$ and $r_k \equiv \pm 3(\mathrm{mod}\, 7)$ when $N \equiv 5, -9, 19, 23(\mathrm{mod}\, 56)$ respectively. Taking modulo 2 in equation $r_k^2 - 14t_k^2 = -N$, then $r_k^2 - 15t_k^2 \equiv 1(\mathrm{mod}\, 2)$, we get $r_k \equiv t_k \pm 1(\mathrm{mod}\, 2)$. Since $r_{k-1}^2 < \frac{14N}{1}$ then $-N = r_k^2 - 14t_k^2 < r_{k-1}^2 - 14t_{k-1}^2 < r_{k-1}^2 < \frac{14N}{1}$ implies $r_{k-1}^2 - 14t_{k-1}^2 = N, 2N, 3N, 4N, 5N, 6N, 7N, 8N, 9N, 10N, 11N, 12N, 13N$. The equations $r_{k-1}^2 - 14t_{k-1}^2 = 5N, 10N, 13N$ are solvable and we have

$$14T_k = 3r_k + r_{k-1}, T_{k-1} = 3T_k - r_k,$$
$$14T_k = 2r_k + r_{k-1}, T_{k-1} = 2T_k - r_k,$$
$$14T_k = r_k + r_{k-1}, T_{k-1} = T_k - r_k.$$

From these relations, then the solutions are $5r_k \equiv r_{k-1}(\mathrm{mod}\, 14), 5r_k \equiv r_{k-1}(\mathrm{mod}\, 7)$, $13r_k \equiv r_{k-1}(\mathrm{mod}\, 14)$ respectively. Other equations $r_{k-1}^2 - 14t_{k-1}^2 = N, 2N, 3N, 4N, 6N$, $7N, 8N, 9N, 11N, 12N$ are unsolvable because these equations are not satisfied equation (3.6). ∎

Theorem 3.2. *Let $D = 15$ be a composite number and N be an odd integer in the quadratic Diophantine equation $x^2 - Dy^2 = N$. Assume that $x^2 \equiv 15(\mathrm{mod}\ N)$ is solvable and $\gcd(15, N) = 1$. Then $\left(\frac{15}{N}\right) = 1$ when $N \equiv 1, 7, 11, 17, 43, 49, 53, 59(\mathrm{mod}\, 60)$. The equation $x^2 - 15y^2 = N$ is solvable when $\left(\frac{15}{N}\right) = 1$. Moreover, assume that (r_k, t_k) is the integer solutions to the equation $x^2 - 15y^2 = N$. Then*

$$r_k^2 - 15t_k^2 = -14N - 13N, -12N, -11N, -10N, -9N, -8N, -7N, -6N - 5N, \\ -4N, -3N, -2N, -N.$$

Proof. Given the congruence $x^2 \equiv 15(\mathrm{mod}\ N)$ is solvable and $\gcd(15, N) = 1$ along with the condition $1 < x < N$. The Jacobi symbol is $\left(\frac{15}{N}\right) = \left(\frac{3}{N}\right)\left(\frac{5}{N}\right)$, using quadratic reciprocity law;

$$\left(\frac{3}{N}\right) = \begin{cases} +1 & \text{if } N \equiv 1, 11(\mathrm{mod}\, 12), \\ -1 & \text{if } N \equiv 5, 7(\mathrm{mod}\, 12), \end{cases}$$
$$\left(\frac{5}{N}\right) = \begin{cases} +1 & \text{if } N \equiv 1, 4(\mathrm{mod}\, 5), \\ -1 & \text{if } N \equiv 2, 3(\mathrm{mod}\, 5). \end{cases}$$

Combining $N \equiv 1, 11(\mathrm{mod}\, 12)$ and $N \equiv 1, 4(\mathrm{mod}\, 5)$, using Chinese remainder theorem, we find $N \equiv 1, 11, 49, 59(\mathrm{mod}\, 60)$. Solving $N \equiv 5, 7(\mathrm{mod}\, 12)$ and $N \equiv 2, 3(\mathrm{mod}\, 5)$, gives $N \equiv 7, 17, 43, 53(\mathrm{mod}\, 60)$. Thus, $\left(\frac{3}{N}\right)\left(\frac{5}{N}\right) = 1$ if $N \equiv 1, 7, 11, 17, 43, 49, 53, 59(\mathrm{mod}\, 60)$. Therefore, the equation $x^2 - 15y^2 = N$ is solvable when $\left(\frac{15}{N}\right) = 1$. If $\left(\frac{15}{N}\right) = -1$, then the equation $x^2 - 15y^2 = N$ is unsolvable.

Suppose that (r_k, t_k) is the integer solution to the equation $x^2 - 15y^2 = N$, then we obtain $r_k^2 - 15t_k^2 = -lN$ for all $1 \leq l < 15$. Consequently, we have $-15N < r_k^2 - 15t_k^2 \leq -N$, and

we can write $r_k^2-15t_k^2=-14N,-13N,-12N,-11N,-10N,-9N,-8N,-7N,-6N,-5N,$ $-4N,-3N,-2N,-N$. Equations $r_k^2-15t_k^2=-14N,-11N,-6N,-N$ are solvable, with integer solutions $r_k\equiv\pm1,\pm2(\mathrm{mod}\,5)$ when $N\equiv1,11,49,59(\mathrm{mod}\,60)$. Taking modulo 14 in equation $r_k^2-15t_k^2=-14N$, we find $r_k^2-15t_k^2\equiv0(\mathrm{mod}\ 14)$ gives $r_k\equiv\pm t_k(\mathrm{mod}\ 14)$. Since $r_{k-1}^2<\frac{15N}{14}$, then $-14N<r_k^2-15t_k^2<r_{k-1}^2-15t_{k-1}^2<r_{k-1}^2<\frac{15N}{14}$. This gives $r_{k-1}^2-15t_{k-1}^2=-13N,-12N,-11N,-10N,-9N,-8N,-7N,-6N,-5N,-4N,-3N,$ $-2N,-N,N$. The equations $r_{k-1}^2-15t_{k-1}^2=-11N,N$ are solvable, leading to the following relations;

$$15T_k=14r_k+14r_{k-1},r_k=13T_k-14T_{k-1},$$
$$15T_k=r_k+14r_{k-1},r_k=T_k-14t_{k-1}.$$

From these relations, we find the solutions are $r_k\equiv-T_k(\mathrm{mod},14)$ and $r_k\equiv T_k(\mathrm{mod}\,14)$ respectively. Other equations $r_{k-1}^2-15t_{k-1}^2=-13N,-12N,-10N,-9N,-8N,-7N,$ $-6N,-5N,-4N,-3N,-2N,-N$ do not satisfied equation (3.6). Thus, these equations are unsolvable. Similarly, by taking modulo 11 in equation $r_k^2-15t_k^2=-11N$, we find $r_k^2-15t_k^2\equiv0(\mathrm{mod}\,11)$, implying that $r_k\equiv\pm2t_k(\mathrm{mod}\,11)$. Since $r_{k-1}^2<\frac{15N}{11}$, then we have $-11N<r_k^2-15t_k^2<r_{k-1}^2-15t_{k-1}^2<r_{k-1}^2<\frac{15N}{11}$. Therefore, we can write the equations $r_{k-1}^2-15t_{k-1}^2=-10N,-9N,-8N,-7N,-6N,-5N,-4N,-3N,-2N,-N,N$. Among these, some equations $r_{k-1}^2-15t_{k-1}^2=-6N,N$ are solvable, for which we have:

$$15T_k=9r_k+11r_{k-1},r_k=9t_k-11T_k,$$
$$15T_k=2r_k+11r_{k-1},r_k=2T_k-11T_{k-1}.$$

Combining these, we find the solutions are $r_k\equiv-2T_k(\mathrm{mod}\,11)$ and $r_k\equiv2T_k(\mathrm{mod}\,11)$. The other equations $r_{k-1}^2-15t_{k-1}^2=-10N,-9N,-8N,-7N,-5N,-4N,-3N,-2N,-N$ are unsolvable, as they do not yield integer solutions. Taking modulo 6 in equation $r_k^2-15t_k^2=-6N$, we find $r_k^2-15t_k^2\equiv0(\mathrm{mod}\,6)$, implying that $r_k\equiv\pm3t_k(\mathrm{mod}\,6)$. Since $r_{k-1}^2<\frac{15N}{6}$, then $-6N<r_k^2-15t_k^2<r_{k-1}^2-15t_{k-1}^2<r_{k-1}^2<\frac{15N}{6}$. This means that $r_{k-1}^2-15t_{k-1}^2=-5N,-4N,-3N,-2N,-N,N,2N$. The equation $r_{k-1}^2-15t_{k-1}^2=N$ is solvable, yielding $15T_k=3r_k+6r_{k-1}$ and $r_k=3T_k-6T_{k-1}$, with the integer solution is $r_k\equiv3T_k(\mathrm{mod}\,6)$. The other equations $r_{k-1}^2-15t_{k-1}^2=-5N,-4N,-3N,-2N,-N,2N$ are unsolvable. Similarly, by taking modulo 2 in equation $r_k^2-15t_k^2=-N$, then we have $r_k^2-15t_k^2\equiv1(\mathrm{mod}\,2)$, implying that $r_k\equiv t_k\pm1(\mathrm{mod}\,2)$. Since $r_{k-1}^2<\frac{15N}{1}$, then we have $-N<r_k^2-15t_k^2<r_{k-1}^2-15t_{k-1}^2<r_{k-1}^2<\frac{15N}{1}$. Therefore, we can find the equations $r_{k-1}^2-15t_{k-1}^2=N,2N,3N,4N,5N,6N,7N,8N,9N,10N,11N,12N,13N,14N$. The equations $r_{k-1}^2-15t_{k-1}^2=6N,11N,14N$ are solvable, and

$$15T_k=3r_k+r_{k-1},T_{k-1}=3T_k-r_k,$$
$$15T_k=2r_k+r_{k-1},T_{k-1}=2T_k-r_k,$$
$$15T_k=r_k+r_{k-1},T_{k-1}=T_k-r_k.$$

Combining these relations, we obtain $2r_k\equiv r_{k-1}(\mathrm{mod}\,5),11r_k\equiv2r_{k-1}(\mathrm{mod}\,15)$, $14r_k\equiv r_{k-1}(\mathrm{mod}\,15)$ are integer solutions. Other equations $r_{k-1}^2-15t_{k-1}^2=N,2N,3N,$ $4N,5N,7N,8N,9N,10N,12N,13N$ are unsolvable since these equations are not satisfied equation (3.5). Similarly, equations $r_k^2-15t_k^2=-10N,-5N$ are solvable and whose intger solutions are $r_k^2\equiv0(\mathrm{mod}\,5)$ when $N\equiv1,7,11,17,43,49,53,59(\mathrm{mod}\,60)$. Taking modulo 10 in equation $r_k^2-15t_k^2=-10N$, then we get $r_k^2-15t_k^2\equiv0(\mathrm{mod}\,10)$ and gives $r_k\equiv5t_k(\mathrm{mod}\ 10)$. If $r_{k-1}<\frac{15N}{10}$, then $-10N=r_k^2-15t_k^2<r_{k-1}^2-15t_{k-1}^2<r_{k-1}^2<\frac{15N}{10}$,

it gives $r_{k-1}^2 - 15t_{k-1}^2 = -9N, -8N, -7N, -6N, -5N, -4N, -3N, -2N, -N, N$. But equation $r_{k-1}^2 - 15t_{k-1}^2 = -N$ is solvable and gives $3T_k = r_k + 2r_{k-1}, r_k = 5T_k - 15T_{k-1}$. Combining these two, we obtain the integer solution is $r_k \equiv 5T_k (\mathrm{mod}\, 15)$. Other equations $r_{k-1}^2 - 15t_{k-1}^2 = -9N, -8N, -7N, -6N, -5N, -4N, -3N, -2N, N$ are unsolvable.

Similarly, taking modulo 5 in equation $r_k^2 - 15t_k^2 = -5N$, we have $r_k^2 \equiv 0 (\mathrm{mod} 5)$. Since $r_{k-1} < \frac{15N}{5}$, then $-5N = r_k^2 - 15t_k^2 < r_{k-1}^2 - 15t_{k-1}^2 < r_{k-1}^2 < \frac{15N}{5}$, it gives $r_{k-1}^2 - 15t_{k-1}^2 = -4N, -3N, -2N, -N, N, 2N$. The equation $r_{k-1}^2 - 15t_{k-1}^2 = -2N$ is solvable and we have $3T_k = r_k + r_{k-1}, r_k 5T_k - 5T_{k-1}$ and gives the integer solution is $r_k \equiv 0 (\mathrm{mod} 5)$. The equations $r_k^2 - 15t_k^2 = -7N, -3N, -2N$ are solvable and its integer solutions $r_k \equiv \pm 1, \pm 2 (\mathrm{mod} 5)$ if $N \equiv 7, 17, 43, 53 (\mathrm{mod} 60)$. We take a modulo 7 in equation $r_k^2 - 15t_k^2 = -7N$, then we get $r_k^2 - 15t_k^2 \equiv 0 (\mathrm{mod} 7)$ and gives $r_k \equiv t_k (\mathrm{mod}\ 7)$. Since $r_{k-1} < \frac{15N}{7}$, then $-7N = r_k^2 - 15t_k^2 < r_{k-1}^2 - 15t_{k-1}^2 < r_{k-1}^2 < \frac{15N}{7}$, it gives $r_{k-1}^2 - 15t_{k-1}^2 = -6N, -5N, -4N, -3N, -2N, -N, N, 2N$. Therefore, the equations $r_{k-1}^2 - 15t_{k-1}^2 = -3N, 2N$ are solvable and

$$15T_k = 6r_k + 7r_{k-1}, r_k = 6T_k - 7T_{k-1},$$
$$15T_k = r_k + 7r_{k-1}, r_k = T_k - 7T_{k-1}.$$

From these relations, we have $r_k \equiv T_k (\mathrm{mod}\, 7)$ and $r_k \equiv -T_k (\mathrm{mod}\, 7)$ are integer solutions. Other equations $r_{k-1}^2 - 15t_{k-1}^2 = -6N, -5N, -4N, -2N, -N, N$ are unsolvable. Similarly, taking modulo 3 in equation $r_k^2 - 15t_k^2 = -3N$, and gives $r_k^2 \equiv 0 (\mathrm{mod} 3)$. Since $r_{k-1} < \frac{15N}{3}$, then $-3N = r_k^2 - 15t_k^2 < r_{k-1}^2 - 15t_{k-1}^2 < r_{k-1}^2 < \frac{15N}{3}$, it gives $r_{k-1}^2 - 15t_{k-1}^2 = -2N, -N, N, 2N, 3N, 4N$. Equation $r_{k-1}^2 - 15t_{k-1}^2 = 2N$ is solvable and we have $5T_k = r_k + r_{k-1}, r_k = 3T_k - 3T_{k-1}$ gives the integer solution is $r_k \equiv 0 (\mathrm{mod}\, 3)$ and other equations $r_{k-1}^2 - 15t_{k-1}^2 = -2N, -N, N, 3N, 4N$ are unsolvable. But, equations $r_k^2 - 15t_k^2 = -13N, -12N, -9N, -8N, -4N$ are quadratic non-residue modulo 60. These equations are not given the integer solutions. ∎

Theorem 3.3. *Let $D = 18$ be a composite number and N be an odd integer in the quadratic Diophantine equation $x^2 - Dy^2 = N$. Assume that $x^2 \equiv 18 (\mathrm{mod}\ N)$ is solvable and $\gcd(18, N) = 1$. Then $\left(\frac{18}{N}\right) = 1$ when $N \equiv 1, 5, 7, 11, 13, 17, 19, 23 (\mathrm{mod}\, 24)$, and the equation $x^2 - 18y^2 = N$ is solvable when $\left(\frac{18}{N}\right) = 1$. Moreover, assume that (r_k, t_k) is the integer solutions to the equation $x^2 - 18y^2 = N$. Then*

$$r_k^2 - 18t_k^2 = -17N, -16N, -15N - 14N - 13N, -12N, -11N, -10N, -9N, -8N, \\ -7N, -6N - 5N, -4N, -3N, -2N, -N.$$

Proof. The quadratic Diophantine equation $x^2 - 18y^2 = N$ can be expressed as the congruence $x^2 \equiv 18 (\mathrm{mod}\, N)$, which is solvable and $\gcd(18, N) = 1$. The Jacobi symbol can be factored as $\left(\frac{18}{N}\right) = \left(\frac{3}{N}\right)\left(\frac{6}{N}\right)$, using quadratic reciprocity law

$$\left(\frac{3}{N}\right) = \begin{cases} +1 & \text{if } N \equiv 1, 11 (\mathrm{mod}\, 12), \\ -1 & \text{if } N \equiv 5, 7 (\mathrm{mod}\, 12). \end{cases}$$

Using Chinese remainder theorem, we reduced

$$\left(\frac{3}{N}\right) = \begin{cases} +1 & \text{if } N \equiv 1, 11 (\mathrm{mod}\, 3), \\ -1 & \text{if } N \equiv 5, 7 (\mathrm{mod}\, 3), \end{cases}$$

and $\left(\frac{6}{N}\right) = 1$ if $N \equiv 1,5,7,11,13,17,19,23 \pmod{24}$. By reducing the modulus, this becomes $N \equiv 1,5,7,11,13,17,19,23 \pmod{8}$. Using the Chinese remainder theorem, we combine the conditions $N \equiv 1,11 \pmod{3}$ and $N \equiv 1,5,7,11,13,17,19,23 \pmod{8}$, yielding $N \equiv 1,5,7,11,13,17,19,23 \pmod{24}$. Similarly, combining $N \equiv 5,7 \pmod{3}$ with $N \equiv 1,5,7,11,13,17,19,23 \pmod{8}$ gives the same result; $N \equiv 1,5,7,11,13,17,19,23 \pmod{24}$. Therefore, $\left(\frac{3}{N}\right)\left(\frac{6}{N}\right) = 1$ when $N \equiv 1,5,7,11,13,17,19,23 \pmod{24}$. The equation $x^2 - 18y^2 = N$ is solvable when $\left(\frac{18}{N}\right) = 1$. Conversely, if $\left(\frac{18}{N}\right) = -1$, then the equation $x^2 - 18y^2 = N$ is unsolvable.

Assume that (r_k, t_k) is the solution to equation $x^2 - 18y^2 = N$, then $r_k^2 - 18t_k^2 = lN$, where $1 \le l < 18$ and gives $-18N < r_k^2 - 18t_k^2 \le -N$. From this relation, we obtain $r_k^2 - 15t_k^2 = -17N, -16N, -15N, -14N, -13N, -12N, -11N, -10N, -9N, -8N, -7N$ $-6N, -5N, -4N, -3N, -2N, -N$. The equations $r_k^2 - 18t_k^2 = -17N, -14N$ are solvable and the integer solutions are $r_k \equiv \pm 1 \pmod{3}$ when $N \equiv 1,7,13,19 \pmod{24}$ and the equations $r_k^2 - 18t_k^2 = -7N, -N$ are solvable and integer solutions are $r_k \equiv \pm 1 \pmod{3}$ when $N \equiv 5,11,17,23 \pmod{24}$. The equations $r_k^2 - 18t_k^2 = -9N, -6N, -3N, -2N$ are solvable and solution is $r_k^2 \equiv 0 \pmod{3}$ if $N \equiv 1,5,7,11,13,17,19,23 \pmod{24}$. Other equations $r_k^2 - 18t_k^2 = -16N, -15N, -13N, -12N, -10N, -8N, -5N, -4N$ are unsolvable since the solutions $r_k \equiv 2 \pmod{3}$ do not exists, if $N \equiv 1,5,7,11,13,17,19,23 \pmod{24}$. Taking modulo 17 in equation $r_k^2 - 18t_k^2 = -17N$, then we have $r_k \equiv \pm t_k \pmod{17}$. Since $r_{k-1}^2 < \frac{18N}{17}$, then $-17N = r_k^2 - 18t_k^2 < r_{k-1}^2 - 18t_{k-1}^2 < r_{k-1}^2 < \frac{18N}{17}$, it gives

$$\begin{aligned} r_{k-1}^2 - 18t_{k-1}^2 = &-16N, -15N, -14N, -13N, -12N, -11N, -10N, -9N, -8N, \\ &-7N, -6N, -5N, -4N, -3N, -2N, -N, N. \end{aligned}$$

The equations $r_{k-1}^2 - 18t_{k-1}^2 = -14N, N$ are solvable and we have

$$\begin{aligned} 18T_k &= 16r_k + 17r_{k-1}, r_k = 16T_k - 17T_{k-1}, \\ 18T_k &= r_k + 17r_{k-1}, r_k = T_k - 17T_{k-1}. \end{aligned}$$

From these relations, we find the integer solutions are $r_k \equiv \pm T_k \pmod{17}$. The equations $r_{k-1}^2 - 18t_{k-1}^2 = -16N, -15N, -13N, -12N, -11N, -10N, -9N, -8N, -7N, -6N, -5N,$ $-4N, -3N, -2N, -N$ are unsolvable since from equation (3.6) gives $\sqrt{290}, \sqrt{273}, \sqrt{239},$ $\sqrt{222}, \sqrt{205}, \sqrt{188}, \sqrt{171}, \sqrt{154}, \sqrt{137}, \sqrt{120}, \sqrt{103}, \sqrt{86}, \sqrt{69}, \sqrt{52}, \sqrt{35}$, which are not the integer solutions. Taking modulo 14 in equation $r_k^2 - 18t_k^2 = -14N$, then we have $r_k \equiv \pm 2t_k \pmod{14}$. If $r_{k-1}^2 < \frac{18N}{14}$, $-14N = r_k^2 - 18t_k^2 < r_{k-1}^2 - 18t_{k-1}^2 < r_{k-1}^2 < \frac{18N}{14}$, it gives $r_{k-1}^2 - 18t_{k-1}^2 = -13N, -12N, -11N, -10N, -9N, -8N, -7N, -6N, -5N, -4N,$ $-3N, -2N, -N, N$. But, the equations $r_{k-1}^2 - 15t_{k-1}^2 = -9N, N$ are solvable and we have

$$\begin{aligned} 9T_k &= 6r_k + 7r_{k-1}, r_k = 12T_k - 14T_{k-1}, \\ 9T_k &= r_k + 7r_{k-1}, r_k = 2T_k - 14T_{k-1}. \end{aligned}$$

Combining these, find the integer solutions are $r_k \equiv \pm 2T_k \pmod{14}$. Other equations $r_{k-1}^2 - 18t_{k-1}^2 = -13N, -12N, -11N, -10N, -8N, -7N, -6N, -5N, -4N, -3N, -2N,$ $-N$ are unsolvable since these equations are not satisfied equation (3.6). We take a modulo 7 in equation $r_k^2 - 18t_k^2 = -7N$, then we have $r_k \equiv \pm 5 \pmod{7}$. Since $r_{k-1}^2 < \frac{18N}{7}$, then $-7N = r_k^2 - 18t_k^2 < r_{k-1}^2 - 18t_{k-1}^2 < r_{k-1}^2 < \frac{18N}{7}$. So, it gives $r_{k-1}^2 - 18t_{k-1}^2 =$ $-6N, -5N, -4N, -3N, -2N, -N, N, 2N$. The equation $r_{k-1}^2 - 18t_{k-1}^2 = 2N$ is solvable and we have $18T_k = 2r_k + 7r_{k-1}, r_k = 2T_k - 7T_{k-1}$ and find the integral solution is $r_k \equiv 2T_k \pmod{7}$. Other equations $r_{k-1}^2 - 18t_{k-1}^2 = -6N, -5N, -4N, -3N, -2N, -N, N$

are unsolvable because $\sqrt{60}, \sqrt{53}, \sqrt{46}, \sqrt{39}, \sqrt{32}, \sqrt{11}$ are not the integer solutions. Again taking modulo 2 in equation $r_k^2 - 18t_k^2 = -N$, then $r_k^2 - 18t_k^2 \equiv 1(\text{mod } 2)$ and we have $r_k \equiv t_k \pm 1(\text{mod } 2)$. If $r_{k-1}^2 < \frac{18N}{1}$, then $-N = r_k^2 - 18t_k^2 < r_{k-1}^2 - 18t_{k-1}^2 < r_{k-1}^2 < \frac{18N}{1}$, and gives $r_{k-1}^2 - 18t_{k-1}^2 = N, 2N, 3N, 4N, 5N, 6N, 7N, 8N, 9N, 10N, 11N, 12N, 13N, 14N, 15N, 16N, 17N$. The equation $r_{k-1}^2 - 18t_{k-1}^2 = 2N, 9N, 17N$ are solvable and we have

$$\begin{aligned}
18T_k &= 4r_k + r_{k-1}, T_{k-1} = 4T_k - r_k,\\
18T_k &= 3r_k + r_{k-1}, T_{k-1} = 3T_k - r_k,\\
18T_k &= r_k + r_{k-1}, T_{k-1} = T_k - r_k.
\end{aligned}$$

Combining these, we find integer solutions are $r_k \equiv 2r_{k-1}(\text{mod } 9), 3r_k \equiv r_{k-1}(\text{mod } 6)$, $17r_k \equiv r_{k-1}(\text{mod } 18)$ respectively. But equations $r_{k-1}^2 - 18t_{k-1}^2 = N, 3N, 4N, 5N, 6N$, $7N, 8N, 10N, 11N, 12N, 13N, 14N, 15N, 16N$ are unsolvable. Similarly, taking modulo 9 in equation $r_k^2 - 18t_k^2 = -9N$, and we have $r_k^2 \equiv 0(\text{mod } 9)$. Since $r_{k-1}^2 < \frac{18N}{9}$, then we have $-9N = r_k^2 - 18t_k^2 < r_{k-1}^2 - 18t_{k-1}^2 < r_{k-1}^2 < \frac{18N}{9}$. Then we found the equations $r_{k-1}^2 - 18t_{k-1}^2 = -8N, -7N, -6N, -5N, -4N, -3N, -2N, -N, N$. So, some equations $r_{k-1}^2 - 18t_{k-1}^2 = -7N, -2N, N$ are solvable and we have

$$\begin{aligned}
2T_k &= r_k + r_{k-1}, r_k = 9T_k - 9T_{k-1},\\
6T_k &= 2r_k + 3r_{k-1}, r_k = 6T_k - 9t_{k-1},\\
6T_k &= r_k + 3r_{k-1}, r_k = 3T_k - 9T_{k-1}.
\end{aligned}$$

From these relations, we find the integer solutions are $r_k \equiv 0(\text{mod } 9)$, $r_k \equiv 6T_k(\text{mod } 9)$, $r_k \equiv 3T_k(\text{mod } 9)$ respectively. From equation (3.6), we have $\sqrt{200}, \sqrt{186}, \sqrt{172}, \sqrt{158}$, $\sqrt{130}, \sqrt{116}, \sqrt{102}, \sqrt{88}, \sqrt{74}, \sqrt{60}, \sqrt{46}, \sqrt{32}$ are not given the integer solutions, then the equations $r_{k-1}^2 - 18t_{k-1}^2 = -13N, -12N, -11N, -10N, -8N, -7N, -6N, -5N, -4N, -3N$ $-2N, -N$ are unsolvable. Moreover, taking modulo 6 in equation $r_k^2 - 18t_k^2 = -6N$, then $r_k^2 \equiv 0(\text{mod } 6)$. If $r_{k-1}^2 < \frac{18N}{6}$, then $-6N = r_k^2 - 18t_k^2 < r_{k-1}^2 - 18t_{k-1}^2 < r_{k-1}^2 < \frac{18N}{6}$, and gives $r_{k-1}^2 - 18t_{k-1}^2 = -5N, -4N, -3N, -2N, -N, N, 2N$. Equation $r_{k-1}^2 - 18t_{k-1}^2 = -3N$ is solvable and we have $3T_k = r_k + 4_{k-1}, r_k = 6T_k - 6T_{k-1}$ and find the integer solution is $r_k \equiv 0(\text{mod } 6)$. Other equations $r_{k-1}^2 - 18t_{k-1}^2 = -5N, -4N, -3N, -N, N, 2N$ are unsolvable since $\sqrt{48}, \sqrt{42}, \sqrt{30}, \sqrt{24}, \sqrt{12}, \sqrt{6}$ are not integer solutions. We take a modulo 3 in equation $r_k^2 - 18t_k^2 = -3N$ and gives $r_k^2 \equiv 0(\text{mod } 3)$. Since $r_{k-1}^2 < \frac{18N}{3}$, then $-3N = r_k^2 - 18t_k^2 < r_{k-1}^2 - 18t_{k-1}^2 < r_{k-1}^2 < \frac{18N}{3}$, and gives $r_{k-1}^2 - 18t_{k-1}^2 = -2N, -N, N, 2N, 3N, 4N, 5N$. Equation $r_{k-1}^2 - 18t_{k-1}^2 = 3N$ is solvable and we have $6T_k = r_k + 3r_{k-1}, r_k = 3T_k - 3T_{k-1}$ and we find the solution is $r_k \equiv 0(\text{mod } 3)$. Equations $r_{k-1}^2 - 18t_{k-1}^2 = -2N, -N, N, 2N, 4N, 5N$ are unsolvable. Taking modulo 2 in equation $r_k^2 - 18t_k^2 = -2N$, then $r_k^2 \equiv 0(\text{ mod } 2)$. Since $r_{k-1}^2 < \frac{18N}{2}$, then $-2N = r_k^2 - 18t_k^2 < r_{k-1}^2 - 18t_{k-1}^2 < r_{k-1}^2 < \frac{18N}{2}$, and gives $r_{k-1}^2 - 18t_{k-1}^2 = -N, N, 2N, 3N, 4N, 5N, 6N, 7N, 8N$. Some equations $r_{k-1}^2 - 18t_{k-1}^2 = N, 7N$ are solvable and we have

$$\begin{aligned}
9T_k &= 2r_k + 3r_{k-1}, r_k = 4T_k - 2T_{k-1},\\
9T_k &= r_k + r_{k-1}, r_k = 2T_k - 2T_{k-1}.
\end{aligned}$$

From these relations, we find the integer solutions are $r_k \equiv 0(\text{mod } 2)$ and $r_k \equiv 0(\text{mod } 2)$. But equations $r_{k-1}^2 - 18t_{k-1}^2 = -N, 2N, 3N, 4N, 5N, 6N, 8N$ are not satisfied equation (3.6). Therefore, these equations are quadratic non-residue modulo 24. ∎

To identify research gaps, we evaluate current mathematical approaches for solving the equation $x^2 - Dy^2 = N$, where D is a composite numbers that is not a perfect square, and N is an odd integer. The described approaches, such as the Euclidean algorithm, quadratic reciprocity law, Thue's theorem, and the Chinese remainder theorem, perform well in fundamental conditions but may not be successful with larger composite numbers of D. These constraints emphasize the need for creative approaches to effectively address more complex situations.

To address the research gap identified in the work of Matthew regarding composite numbers of D in the quadratic Diophantine equation $x^2 - Dy^2 = N$, it is essential to investigate how the prime factors of D influence the existence and structure of solutions. This investigation aims to understand the impact of D's factorization on the presence and arrangement of solutions, analyzing whether specific factorizations of D result in a greater or lesser number of solutions and how they affect the properties of these solutions. For example, composite numbers of D with multiple prime factors may lead to a more complex solution pattern compared to cases where D is a prime number. We propose a comprehensive strategy that focuses on both prime and composite numbers of D. Since all composite numbers can be factored into primes, we will leverage this property to deepen our understanding of the solutions. This approach systematically analyzes the solutions for various composite numbers of D to identify patterns and applicable features.

To better understand the behavior of solutions for different composite numbers of D and an odd integer N, we will develop new theorems and mathematical frameworks. We aim to create more efficient computational methods for solving these equations and to deepen the understanding of both prime and composite numbers of D in quadratic Diophantine equations. Developing new theoretical frameworks that extend solvability conditions for quadratic Diophantine equations with large D and N. These should provide insights into when integer solutions exist without relying on full factorization.

4. Conclusion

We studied the integer solutions of quadratic Diophantine equation $x^2 - Dy^2 = N$, where D is a composite number such as $D = 14, 15, 18$, and N is an odd integer. To solve the modified quadratic Diophantine equations $r_k^2 - Dt_k^2 = N$ and determine integer solutions, we applied several mathematical techniques such as the quadratic residue method, the Euclidean algorithm, Bézout's identity, Thue's theorem, and the Chinese remainder theorem. Additionally, we identified research gaps in solving quadratic Diophantine equations, especially when D is a large composite number and N is a large integer, and to develop computational methods to improve solvability and we analyzed the conditions under which these equations have integer solutions and investigated cases where they are unsolvable. Our study covered all composite values of D that are not perfect squares and examined how the size of N affects solvability. For large composite values of D and large integers N, we found that existing methods are often insufficient, highlighting the need for further research and the development of new techniques. While the properties and integer solutions for $D = 2$ and $D = 3$ are well understood, extending these results to other composite values of D remains a complex problem. The factorization of D plays a significant role in determining solvability, but its exact influence requires deeper investigation. We developed new theoretical frameworks that extend solvability

conditions for quadratic Diophantine equations with large D and N. These frameworks provide insights into when integer solutions exist without requiring full factorization. Additionally, we improved computational techniques for handling large composite D and large N, incorporating advanced algorithms. Furthermore, we extended known results on integer solutions to include cases where both D and N are large, bridging the gap between theoretical number theory and computational feasibility.

Data Availability

Data sharing does not apply to this research because no datasets were generated or searched during the current study.

Conflicts of Interest

There are no relevant conflicts of interest for the authors regarding to this work.

Authors Contribution

This paper is based on a Ph.D. study. The research was designed by the first author, who also prepared the paper and contributed to the discussion and results. The co-author developed the concept, designed the research strategy, and edited the text.

Acknowledgments

The first author sincerely thanks the University Grants Commission (UGC), Nepal, for their support through the Ph.D. Fellowship and Research Grant (UGC Award No. PhD-78/79-S&T-10 [Faculty]).

Similarly, the first author also expresses gratitude to the University Grants Commission (UGC) for providing travel grants (2080/081).

References

[1] U. Dudley, Elementary Number Theory, Courier Corporation, 2012.

[2] O. Baumgart, The Quadratic Reciprocity Law: A Collection of Classical Proofs, Birkh Basel, NY, 2015.

[3] A.M. Legendre, Theorie des Nombres, Third Edition, Libraire Scientifique A. Hermann, Paris, 1830.

[4] C.G.L. Jacobi, Uber die Kreisteilung und ihre Anwendung auf die Zahlentheorie, Bericht Ak. Wiss. Berlin, 1837.

[5] J.L. Lagrange, Euores II, Chez courcier, Paris, 1868.

[6] J.A. Serret, Sur un theoreme relatif aux nombres entieres, J. Math. Pures Appl. 13 (1848) 12–14.

[7] C. Hermite, Note au sujet de l'article precedent, J. Math. Pures Appl. 13 (1848) 1–15.

[8] J.V. Uspensky, M.A. Heaslet, Elementary Number Theory, McGraw-Hill, NY, 1939.

[9] T. Nagell, Introduction to Number Theory, Chelsea Publishing Company, NY, 1981.

[10] A. Thue, Et par antydninger til en taltheorisk methode, Selected Mathematical Papers of Axel Thue, Universitets for laget, Oslo, 1977.

[11] G. Cornacchia, Su di un metodo per la risoluzione in numeri interi dell equazione $\sum_{h=0}^{n} C_h x^{n-h} = P$, Giornale di Mathmatiche di Battaglini. 46 (1908) 33–90.

[12] K. Matthews, Thue's theorem and the Diophantine equation $x^2 - Dy^2 = \pm N$, Math. Comp. 71 (2002) 1281–1286.

[13] C. Thomas, On Representations of Integers by the Quadratic Form $x^2 - Dy^2$, Thesis, Rochester Institute of Technology, 2012.

[14] B.B. Tamang, A. Singh, For different prime numbers D and an odd integer N in the quadratic Diophantine equation $x^2 - Dy^2 = \pm N$, Indian Journal of Mathematics 66 (2) (2024) 201–228.

[15] I. Niven, H.S. Zuckerman, H.L. Montgomery, An Introduction to the Theory of Numbers, John Wiley and Sons, 2013.

[16] T. Andreescu, D. Andrica, Quadratic Diophantine Equations, Springer NY, 2015.

[17] https://brilliant.org/wiki/bezouts-identity/, Retrieved from December, 2023.

[18] G.B. Andrews, Number Theory, Courier Corporation, 1994.