Journal of Institute of Science and Technology, 29(2), 143-149 (2024)
ISSN: 2467-9062 (print), e-ISSN: 2467-9240
https://doi.org/10.3126/jist.v29i2.67929

Research Article

DETERMINING THE SOLVABILITY AND UNSOLVABILITY OF QUADRATIC DIOPHANTINE EQUATIONS USING QUADRATIC RESIDUES AND CONTINUED FRACTIONS

Bal Bahadur Tamang*, Ajaya Singh
Central Department of Mathematics, Institute of Science and Technology, Tribhuvan University, Kathmandu, Nepal
Correspondence: bb.ilam2020@gmail.com

(Received:** July 18, 2023; **Final Revision:** December 19, 2024**; Accepted:** December 28, 2024**)

ABSTRACT

This paper determines the solvability and unsolvability of quadratic Diophantine equations using quadratic residues and continued fractions. Quadratic residues provide a framework for analyzing the conditions under which these equations have integer solutions, utilizing tools like the quadratic reciprocity law and the Legendre symbol. Continued fractions, particularly the periodic expansion of $\sqrt{D}$, provide a systematic approach to solving quadratic Diophantine equations like Pell's equation $x^2 - Dy^2 = N$, where D is a positive, non-square integer and N is a non-zero integer. By combining these methods, we identify the solvability conditions and find integer solutions for quadratic Diophantine equations. The study also incorporates numerical approaches, supported by theorems, and demonstrates the results through illustrative examples.

Keywords: Continued fraction, determine, Diophantine equation, quadratic residues, solvability,

INTRODUCTION

A Diophantine equation (Mordell, 1969) is a polynomial equation with an integer solution. The objective of a Diophantine equation is to find the integer solutions. These equations are named after Diophantus, an ancient Greek mathematician (Austin, 1981) who investigated such issues. They are important in number theory and have applications in cryptography, coding theory, and other mathematical disciplines. Diophantine equations can range from simple linear equations to complex nonlinear forms. Depending on the equation, finding solutions may involve techniques from algebra, geometry, or advanced number theory.

A quadratic Diophantine equation (Andreescu & Andrica, 2015) is a polynomial equation of degree two in two or more variables 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 $a \equiv b(mod\ n)$.

Mathematicians such as Lagrange, Legendre, and Gauss (Dudley, 2012) explored and developed methods for classifying and solving quadratic Diophantine equations, frequently using the quadratic reciprocity law. However, due to their variety and complexity, the quadratic reciprocity law and related methods are insufficient to explain the basic principles of these problems.

Quadratic reciprocity law, continued fractions, and the Legendre symbols are powerful tools in number theory for studying quadratic equations. They are beneficial for determining the solvability of quadratic congruences and finding numerical approximations for the solutions, each contributing uniquely while complementing one another.

The quadratic reciprocity law, formulated by Euler and later proved by Gauss, is a cornerstone of number theory (Andreescu & Andrica, 2015). It provides a method to determine whether a quadratic congruence is solvable for integers. Specifically, it relates the solvability of the congruence modulo two primes, p and q. Euler and Legendre first proposed this law, but Gauss provided the first complete proof (Riesel, 2015). Gauss created eight different proofs, and later, Eisenstein added five more proofs (Lemmermeyer, 2013). The quadratic reciprocity law helps study quadratic equations of the form

$$x^2 + bx + c = 0,$$

where a, b, c are integers and x is a variable. It helps determine if a congruence like $x^2 \equiv a(mod\ p)$ has a solution, even though it does not provide the exact solution.

The quadratic reciprocity law and quadratic Diophantine equations are connected through their role in determining the solvability of quadratic congruences, which often arise in these equations. The quadratic reciprocity law (Baumgart, 2015) helps in determining the solvability of quadratic Diophantine equations like $x^2 - Dy^2 = N$, where N is a non-zero integer. This insight helps analyze the solvability of quadratic Diophantine equations by reducing them to modular conditions. For example, understanding whether certain numbers are quadratic residues modulo a prime can determine if specific quadratic Diophantine equations have integer solutions. Thus, the quadratic reciprocity law is a foundational tool in addressing the modular aspects of these equations.

The relationship between continued fractions and quadratic Diophantine equations lies in their ability to provide systematic solutions. A continued fraction is an effective tool for approximating irrational numbers and solving equations like Pell's equation $x^2 - Dy^2 = \pm 1$, where D is a positive and not a perfect square (Arya, 1991). The square root of a non-square integer D has a periodic continued fraction representation. Rational approximations (Niven *et al.*, 2013) generated from continued fractions, known as convergents, are useful in solving quadratic Diophantine equations with integer solutions. Continued fractions provide a systematic approach to determining the fundamental solution (x_1, y_1) of Pell's equation. Once the minimal solution has been found, all subsequent solutions can be constructed by applying recurrence relations.

Fermat, Euler, Lagrange, Legendre, and Gauss (Lemmermeyer, 2013) contributed significantly to studying quadratic residues. Euler formalized the notion of quadratic residues and laid the groundwork for developing the quadratic reciprocity law. Quadratic reciprocity law directly deals with quadratic forms in modular arithmetic (Malik & Saffar, 2020), helping determine whether certain congruences of the form $x^2 \equiv a(mod\ p)$ are solvable, where p is a prime. The quadratic reciprocity law not only provides conditions under which such congruences have solutions but also connects the residues modulo different primes surprisingly.

To solve the congruence problem $x^2 \equiv a(mod\ p)$, one must determine whether a is a quadratic residue modulo p. This means checking if there exists an integer x such that $x^2 \equiv a(mod\ p)$. The law of quadratic reciprocity simplifies this verification, offering a theoretical framework that saves time and effort in computations.

The congruence $x^2 \equiv a(mod\ p)$ has a solution and $(a, p) = 1$, in which case a is a quadratic residue modulo p; otherwise, it is a quadratic non-residue modulo p (Andreescu & Andrica, 2015). Euler's criterion (Aigner & Ziegler, 2014) can be used to verify an integer to determine whether it contains a quadratic residue modulo a prime. To understand quadratic residues, we first establish some fundamental understanding, including a simple test for reciprocity. Euler's criterion provides a technique for effectively calculating the Legendre symbol. The existence of a primitive root modulo p is a handy tool for understanding the Legendre symbol. Legendre (1830) introduced an interesting concept called the Legendre symbol in his attempts to prove the quadratic reciprocity law. The Legendre symbol $\left(\frac{a}{p}\right)$ simplifies the process of determining whether a is a quadratic residue modulo p. If p represents an odd prime, $a \in \mathbb{Z}$, and $gcd(a, p) = 1$, and $a \not\equiv 0\ (mod\ p)$, then the value of Legendre symbol are 1 if $x^2 \equiv a(mod\ p)$ has solution and -1 if $x^2 \equiv a(mod\ p)$ has no solution.

The Legendre symbol can be calculated using the quadratic reciprocity law, but this method involves factoring, which becomes difficult with large numbers. To make the process easier, the Legendre symbol was modified to work with any odd integer in the denominator, not just odd primes. This generalization, introduced by Jacobi (1837), is called the Jacobi symbol. While the Legendre symbol is specific to odd primes, the Jacobi symbol extends the idea to all odd integers and can be expressed in terms of the Legendre symbol.

The Legendre symbol $\left(\frac{a}{p}\right)$ can be extended to $\left(\frac{a}{q}\right)$ and defined as the product of the Legendre symbol, corresponding to the prime factors q and

$\left(\frac{a}{q}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right)$. When $q = p$, an odd prime, the Jacobi and Legendre symbols are identical.

A fundamental characteristic of the Jacobi symbol is that it maintains the applicability of the quadratic reciprocity law and its supplements within this extended framework. It is completely multiplicative and periodic with period q. Assuming that $gcd(a, q) = 1$, where a is an integer and q is an odd integer, the Jacobi symbol $\left(\frac{a}{q}\right)$ is the solution to the congruence $x^2 \equiv a(mod\ q)$ and exists in x (Niven *et al.*, 2013).

We explain how the Legendre symbol, Euler's criterion, and Gauss's lemma are connected. These tools simplify the calculation of the Legendre symbol by linking it to solving a quadratic Diophantine equation. Using Fermat's little theorem, it becomes clear that $a^{(p-1)/2} \equiv 1(mod\ p)$ holds if and only if a is a quadratic residue in the finite field $\mathbb{F}_p$, where p is a prime number. Assume p is prime, a is an integer, and a and p are relatively prime. If $a^{(p-1)/2} \equiv 1(mod\ p)$, then a is a quadratic residue modulo p. Similarly, if $a^{(p-1)/2} \equiv -1(mod\ p)$, then a is a quadratic non-residue modulo p (Aigner & Ziegler, 2014). This means that there are exactly $\frac{(p-1)}{2}$ quadratic residues and $\frac{(p-1)}{2}$ quadratic non-residues modulo p. The even powers of a primitive root of an odd prime p are equal to the quadratic residues modulo p, while the odd powers are equal to the quadratic non-residues modulo p. This relationship, along with the Legendre symbol, Euler's criterion, and Gauss's lemma, helps us better understand how quadratic residues and non-residues are distributed in modular arithmetic.

Numerical approaches involve using computational methods to explore, solve, or verify mathematical problems. These methods are essential for providing practical solutions or testing theoretical predictions in specific cases. Numerical approaches compute results for specific equations, analyze patterns, and verify

general theories. They often involve iterative algorithms, simulations, or straightforward computations.

However, numerical approaches do not exist in independence; they are led and justified by theorems that establish the problem's underlying principles.

Illustrative examples are used to clarify and demonstrate the concepts, methods, and results in an accessible way. Examples walk through specific cases step-by-step to show how a numerical method works or how a theorem applies. They bridge the gap between abstract theory and practical application.

MATERIALS AND METHODS

This study uses a combination of theoretical and computational approaches to determine the solvability of quadratic Diophantine equations. A theoretical framework is developed by deriving and applying the quadratic reciprocity law to analyze the solvability of congruences. Key theorems related to quadratic residues and continued fractions are proved and verified. Computational techniques are employed to calculate Legendre symbols and test the residue conditions. Continued fraction expansions of $\sqrt{D}$ are generated to identify fundamental solutions. Illustrative examples are provided to demonstrate the practical application of these methods. For instance, Pell's equations

$$x^2 - Dy^2 = \pm 1,$$

where D is a positive, and square free (Arya, 1991) are solved to highlight the connection between quadratic residues and continued fractions. Results are analyzed and validated by cross-referencing solutions derived from continued fractions with those obtained using quadratic residue conditions.

Theorem 2.1 [Fermat's Little Theorem] Let p be a prime and a be an integer such that $(a,p) = 1$. If $p \nmid a$, then $a^{(p-1)/2} \equiv 1(mod\ p)$. If $p \mid a$, then $a^p \equiv a(mod\ p)$ (Aigner & Ziegler, 2014).

Theorem 2.2 [Euler's Criterion Theorem] Assume that p is an odd prime, and a is an integer, and $p \nmid a$, then $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2}(mod\ \ p)$ (Aigner & Ziegler, 2014).

Theorem 2.3 [Gauss's Lemma] Consider the integers $r, 2r, 3r, \cdots, \frac{p-1}{2}$ with their least positive residues module p and $p \nmid r$. Assume that p is an odd prime and positive integer s is used to calculate the number of these residues are exceed $\left(\frac{p}{2}\right)$, then $\left(\frac{r}{p}\right) = (-1)^s$ (Niven *et al.*, 2013).

RESULTS AND DISCUSSION

We discuss the results on whether quadratic Diophantine equations are solvable or not. These results are supported by theorems and examples that involve the quadratic reciprocity law, continued fractions, and Legendre symbols. Euler's criterion offers a quick method to calculate the Legendre symbol $\left(\frac{a}{p}\right)$, and the quadratic reciprocity law makes this process easier.

Theorem 3.1 [The Quadratic Reciprocity Law] Let p and q be distinct odd primes of the form $4k+1$. One of the congruence $x^2 \equiv p(mod\ q)$ or $x^2 \equiv q(mod\ p)$ is solvable, while the other is not. However, if at least one of the primes is of the form $4k+1$, then both congruences are either solvable or unsolvable (Weintraub, 2011).

Proof.

If p and q are both of the form $4k+1$, right hand the exponent of -1 is even. Assuming $p > q$ and $p \equiv q(mod\ 4)$, then we can write $p - q = 4a$, where $a \in \mathbb{Z}$. We have

$\left(\frac{p}{q}\right) = \left(\frac{4a+q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right)$ and

$\left(\frac{q}{p}\right) = \left(\frac{p-4a}{p}\right) = \left(\frac{-4a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right)$. Therefore, $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ are the same because p and q give the same remainder when divided by $4a$.

Hence $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right) = \begin{cases} 1, if\ p \equiv 1(mod\ 4) \\ -1, if\ p \equiv 3(mod\ 4). \end{cases}$

On the other hand, since $p \not\equiv q(mod\ 4)$, then we can write $p \equiv -q(mod\ 4)$. We have

$\left(\frac{p}{q}\right) = \left(\frac{4a-q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right)$ and

$\left(\frac{q}{p}\right) = \left(\frac{-p+4a}{p}\right) = \left(\frac{4a}{p}\right) = \left(\frac{a}{p}\right)$. Therefore, $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ are the same because p and q give the opposite remainder when divided by $4a$. Hence $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$.

Theorem 3.2 Assume that p and q are odd primes. Then (Burton, 1980)

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), if\ p \equiv 1(mod\ 4),\ \ q \equiv 1(mod\ 4) \\ -\left(\frac{q}{p}\right), if\ p \equiv q \equiv 3(mod\ 4). \end{cases}$$

In conclusion, the quadratic reciprocity law provides that $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ if p and q are different odd primes and except $p \equiv q \equiv 3(mod\ 4)$, in which case $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

We know that the Legendre symbol is multiplicative. Thus, for any $a, b \in \mathbb{Z}$ and an odd prime p, we have

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right)(mod\ p).$$

Since $p \equiv 1(mod\ 4)$ is exclusively true if and only if $\frac{p-1}{2}$ is even, using Euler's criteria, we can determine that

$$\frac{-1}{p} = (-1)^{(p-1)/2} = \begin{cases} 1, if\ p \equiv 1(mod\ 4) \\ -1, if\ p \equiv 3(mod\ 4). \end{cases}$$

It gives $x^2 \equiv -1(mod\ p)$ as a solution for odd prime p if and only if p is of the form $4k+1$. Using Theorem 3.1 and 3.2, gives the solution of quadratic Diophantine equation. So, we consider the equation $x^2 - 17y^2 = 12$ in integer solutions.

We take a modulo 17, and $x^2 \equiv 12(mod\ 17)$.

Now, $\left(\frac{12}{17}\right) = \left(\frac{3}{17}\right)\left(\frac{4}{17}\right) = \left(\frac{3}{17}\right)$. We have $3 \equiv 3(mod\ 4)$ and $17 \equiv 1(mod\ 4)$. Using quadratic reciprocity law, $\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right)$. Therefore, we have reduced the solvability of $x^2 \equiv 12(mod\ 17)$ to the solvability of $x^2 \equiv 2(mod\ 3)$. Since 2 is a quadratic non-residue modulo 3. Then $\left(\frac{2}{17}\right) = -1$. Therefore, $\left(\frac{12}{17}\right) = -1$. Hence, $x^2 - 17y^2 = 12$ is not solvable.

Theorem 3.3 Let p be an odd prime. Then 2 is a quadratic residue modulo p if and only if

$p \equiv 1(mod\ 8)$ (Malik & Saffar, 2020).

Theorem 3.3 gives for a prime p to be of the form

$4k+3$. Then $x^2 - py^2 = \pm 2$ is solvale.

For any odd prime p, we know

$$\left(\frac{2}{p}\right) = \left(\frac{2-p}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p-2}{p}\right).$$

Taking for any odd prime k,

$$\left(\frac{k-2}{k}\right) = \left(\frac{k}{k-2}\right) = \left(\frac{2-(2-k)}{k-2}\right) = \left(\frac{-1}{k-2}\right)\left(\frac{k-2}{k}\right)$$

Now,

$$\left(\frac{2}{p}\right) = \left(\frac{2-p}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p-2}{p}\right) = \left(\frac{-1}{p-2}\right)\left(\frac{p-2}{p}\right)\left(\frac{p-4}{p-2}\right) = \cdots = \left(\frac{-1}{p-2}\right)\left(\frac{p-2}{p}\right)\cdots\left(\frac{-1}{3}\right)\left(\frac{1}{3}\right) = (-1)^{\frac{p-1}{2}\frac{p-2}{2}\cdots\frac{3-1}{2}} = (-1)^{1+2+\cdots+\frac{p-1}{2}} = (-1)^{\frac{p^2-1}{8}}.$$

It follows that

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, if\ p \equiv \pm 1(mod\ 8) \\ -1, if\ p \equiv \pm 3(mod\ 8). \end{cases}$$

So, Gauss' lemma allows us to derive some remarkable results. It gives a technique for identifying primes with 2 as a quadratic residue and, consequently, the property that $\left(\frac{-2}{a}\right) = 1$ if and only if $a \equiv 1 \text{ or } 3(mod\ 8)$. Similarly, by quadratic reciprocity law, to compute

$$\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right).$$

The following inferences are made because of the fact that the reduction $p(mod\ 3)$ completely determines $\left(\frac{3}{p}\right)$ and that the reduction of $p(mod\ 4)$ completely determines $(-1)^{p-1}$. Therefore,

$$\left(\frac{3}{p}\right) = \begin{cases} 1, if\ p \equiv \pm 1(mod\ 12) \\ -1, if\ p \equiv \pm 5(mod\ 12) \end{cases}$$

The Gauss lemma is an essential requirement for the quadratic reciprocity law. Suppose that the positive integers a, b, c are square-free and relatively primes. Then non-zero solutions (Weintraub, 2011) for the equation $ax^2 + by^2 = cz^2$ exist for the numbers x, y, z if and only if the Legendre symbol

$\left(\frac{-ab}{c}\right) = \left(\frac{bc}{a}\right) = \left(\frac{ca}{b}\right) = 1$ are holds.

Theorem 3.4 Assume that p is an odd prime and q is an integer. If $d \equiv 3(mod\ 4)$ and $\left(\frac{q}{d}\right) = 1$, then the quadratic Diophantine equation $x^2 - dy^2 = -q$ is unsolvable.

Proof.

If possible, assume that $x^2 - dy^2 = -q$ is solvable, then for some integers r and s such that $r^2 - dys^2 = -q$ is also solvable. It follows that $r^2 \equiv -q(mod\ d)$. It gives $\left(\frac{-q}{d}\right) = 1$. The properties of the Legendre symbol are

$1 = \left(\frac{-q}{d}\right) = \left(\frac{-1}{d}\right)\left(\frac{q}{d}\right)$ and
$\left(\frac{-1}{d}\right) = \left(\frac{-1}{d}\right).1 = \left(\frac{-1}{d}\right)\left(\frac{q}{d}\right) = 1.$

By quadratic reciprocity law, $d \equiv 1(mod\ 4)$, which is a contradiction of our assumption. Hence, the quadratic Diophantine equation $x^2 - dy^2 = -q$ is unsolvable. Theorem 3.4 connects the Legendre symbol, the quadratic reciprocity law, and quadratic Diophantine equations, using this relationship to determine their solvability. It shows how the quadratic reciprocity law can be used to solve quadratic Diophantine equations. Let us consider the equation is $x^2 - 5y^2 = 1$. We write the equation in congruence as the form $x^2 \equiv 1(mod\ 5y^2)$. This implies that finding the integer solution (x, y) such that $x^2 - 1$ is divisible by $5y^2$. We consider modular arithmetic focus on prime numbers to apply the quadratic reciprocity law in the congruence $x^2 \equiv 1(mod\ 5)$. The solutions to this congruence are $x \equiv \pm 1(mod\ 5)$. We claim that -5 is a quadratic residue modulo a prime p.

Consider a prime $p = 13$, then

$\left(\frac{-5}{13}\right) = \left(\frac{-1}{13}\right)\left(\frac{5}{13}\right)$. Using the supplementary law; $\left(\frac{-1}{13}\right) = (-1)^{(13-1)/2} = 1$ and $\left(\frac{5}{13}\right)\left(\frac{13}{5}\right) = (-1)^{(5-1)(13-1)/4} = 1$.

Since $13 \equiv 3(mod\ 5)$, then $\left(\frac{13}{5}\right) = \left(\frac{3}{5}\right)$.

Now, $\left(\frac{3}{5}\right) = -\left(\frac{5}{3}\right) = -\left(\frac{2}{3}\right) = -(-1)^{\frac{3^2-1}{8}} = 1$. So, $\left(\frac{-5}{13}\right) = 1$. It means that -5 is quadratic residue modulo 13. Therefore, the equation $x^2 - 5y^2 = 1$ has solutions for some integers x and y and solution $(x, y) = (9,4)$. Similarly, consider the equation

$x^2 - Dy^2 = N$.

Let D be an odd prime and N a positive integer with $\left(\frac{N}{D}\right) = 1$. Then equation $x^2 - Dy^2 = N$ is not solvable if D is a prime of the form $4k + 3$ or $8k + 7, k \in \mathbb{Z}$. For the equations $x^2 - Dy^2 = 2$and $x^2 - Dy^2 = -2$, exactly one is solvable. If D is a prime of the form $4k + 3, k \in \mathbb{Z}$, then the system of equations $(D-1)x^2 + y^2 = u^2$ and $x^2 + (D-1)y^2 = v^2$ has no solutions in non-zero integers u and v.

Continued fractions have a deep and elegant connection to solving quadratic Diophantine equations. The periodic continued fraction expansion of $\sqrt{D}$ provides a clear method to find fundamental solutions by using the properties of convergents. This approach is especially useful for solving Pell's equation $x^2 - Dy^2 = 1$, based on the properties of continued fractions for non-square roots.

An infinite simple continued fraction for a number α is an expression of the form as;

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}}$$

where $a_0 \in \mathbb{Z}$ and $a_1, a_2, a_3, \cdots \in \mathbb{N}$. The continued fraction expansion of $\sqrt{D}$ is written as $\sqrt{D} = [a_0; a_1, a_2, \cdots, a_{2r}]$, where a_0 is an integer part of $\sqrt{D}$ and the sequence $a_1, a_2, \cdots, a_{2r}$ are positive integers and repeats periodically. The convergents of this continued fraction are rational approximations of $\sqrt{D}$ in the form $\frac{p_k}{q_k}$, where p_k and q_k are integers. These convergents approximate $\sqrt{D}$ and satisfy the equation $p_k^2 - Dq_k^2 = \pm 1$. The minimal solution to equation $x^2 - Dy^2 = 1$ can be found among the convergents of the continued fraction expansion of $\sqrt{D}$. Specifically, it corresponds to the convergent at the end of the first period of the expansion. Periodic continued fractions, especially for quadratic irrationals like $\sqrt{D}$, play a crucial role in solving equations of the form $x^2 - Dy^2 = 1$. The periodic expansion of $\sqrt{D}$ provides a systematic way to find the minimal solution to this equation. The minimal solution is (x_1, y_1) and it generates all other solutions through $x_{k+1} + \sqrt{D}y_{k+1} = \left(x_1 + \sqrt{D}y_1\right)^k,\ k > 0$. Continued fractions are also useful for solving generalized forms like $x^2 - Dy^2 = N$. The periodicity of $\sqrt{D}$ helps identify integer solutions or prove their absence by analyzing the congruence conditions and approximation properties of the convergents.

We assume that $d = pq$ is prime factorization, where p, q are primes such that $p \equiv 3(mod\ 4)$ and $q \equiv 5(mod\ 8)$. The simple continued fraction expansion of $\sqrt{d} = [q_0; \overline{q_1, q_2, \cdots, q_r}]$ and Legendre symbol

$\left(\frac{p}{q}\right) = (-1)^r$ (Aleksander, 1997).

Friesen (1991) provided $d = pq \equiv 1(mod\ 4)$ and $d = 2pq$. But

$q_n = \left\lfloor \frac{q_0 + b_n}{c_n} \right\rfloor, b_n + b_{n+1} = c_n q_n,$

$d = b_n^2 + c_n c_{n+1}, n \geq 0$. If $i = 2k + 1$, then minimal number k, for which $c_k = c_{k-1}$ is $k = \frac{i-1}{2}$ and if $i = 2k$, then minimal number k, for which $b_k = b_{k+1}$ is $k = \frac{i}{2}$, we found

$1 < c_n < 2\sqrt{d}$ for $0 \leq n \leq i - 1$ and equation is $P_{n-1}^2 - dQ_{n-1}^2 = (-1)^n c_n$, where $\frac{P_n}{Q_n}$ is n^{th} convergent of $\sqrt{d}$, which is the relation between Legendre symbol and the representation of $\sqrt{pq}$, as a simple continued fraction. Let p and q represent two different odd primes. Friesen (1991) established relationships between the value of the Legendre symbol $\left(\frac{p}{q}\right)$ and the length of the period of continued fraction expansion of $D = pq$. A conjecture of Chowla and Chowla (1972) was resolved by these findings, in addition to those of Schinzel (1974). As there is an integer solution to the equation

$px^2 - qy^2 = \pm 1$, we generalize those results to evaluating Jacobi symbols $\left(\frac{p}{q}\right)$ and observe the continued fraction expansion for $\sqrt{pq}$ or $\sqrt{\frac{p}{q}}$.

The equation $px^2 - qy^2 = \pm 1$ has a solution in positive integers x, y where p and q are square-free positive integers with $p > q > 1$. Assume that the continued fraction expansion of

$\sqrt{pq} = [a_0; a_1, a_2, \cdots, a_i]$. Then, in that case, the central partial quotient (Van der Poorten & Walsh 1999) and the period length $r = 2i$ are both even and continued fraction expansion of

$$\sqrt{\frac{p}{q}} = \left[\frac{1}{2}a_1;\ \overline{a_{i+1}, a_{i+2}, \cdots, a_1, a_i}\right]$$

$$= \left[\frac{1}{2}a_1;\ \overline{a_{l-1}, a_{l-2}, \cdots, a_1, a_{l-1}, a_l}\right].$$

Therefore, r is the length of the continued fraction expansion of $\sqrt{pq}$. Then the following Jacobi symbol equality holds $\left(\frac{p}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{r}{2}+1}$ and $\left(\frac{q}{p}\right) = \left(\frac{-1}{q}\right)^{\frac{r}{2}}$. Consider $p \equiv q \equiv 3(mod\ 4)$ as a different prime numbers and $d = pq$. Then r is even and

$$\left(\frac{p}{q}\right) = \varepsilon(-1)^{r/2},$$

where $\varepsilon = 1$ if $p < q$ and $\varepsilon = -1$ if $p > q$. Also, $p \equiv 3(mod\ 8)$ and $q \equiv 7(mod\ 8)$ as different prime numbers and $d = pq$. Then r is even and $\left(\frac{p}{q}\right) = \varepsilon(-1)^{r/2}$, where $\varepsilon = 1$ if $2p < q$ and $\varepsilon = -1$ if $2p > q$.

The choice between using continued fractions and the quadratic reciprocity law to solve quadratic Diophantine equations depends on the specific problem. Each method has unique strengths and is suited for different scenarios. Continued fractions are best for solving equations like Pell's equation or similar forms. They provide a direct way to compute fundamental solutions by using the periodicity of $\sqrt{D}$. This method is particularly effective for equations where D is positive and non-square. However, continued fractions are less useful for equations where D is negative or not square-free. The quadratic reciprocity law is most helpful for determining whether quadratic congruences

$x^2 \equiv a(mod\ p)$ are solvable.

It works efficiently in modular arithmetic and is ideal for checking solvability, especially when dealing with primes. However, it does not provide the actual solutions to the equations. For problems requiring explicit solutions, continued fractions are better. For problems focused on solvability, especially in modular arithmetic, the quadratic reciprocity law is the better choice. In some cases, both methods can be combined. The quadratic reciprocity law can first verify whether a solution exists, and continued fractions can then be used to find the exact solutions when applicable.

For the quadratic Diophantine equation $x^2 - Dy^2 = N$, a numerical approach might involve using the continued fraction expansion of $\sqrt{D}$ and its convergent to find the fundamental solution. Numerical approaches make theoretical concepts more concrete and allow for practical problem-solving when analytical solutions are difficult or impossible. For instance, a counterexample can involve solving the quadratic Diophantine equation $x^2 - 61y^2 = 1$ using the continued fraction method to find integer solutions numerically.

Theorems provide the logical foundation and justification for why specific numerical approaches work. They also offer constraints or conditions under which solutions exist. For example, a theorem might state that the quadratic equation $x^2 - Dy^2 = N$ has integer solutions only if N satisfies certain congruences modulo D. This theoretical result helps focus the numerical search on valid cases. The theorem of fundamental units in quadratic fields could guide how solutions are derived using properties of quadratic rings. By linking numerical work with theoretical results, the study ensures mathematical rigor and provides insights into why the methods succeed.

After introducing a method for solving $x^2 - Dy^2 = N$, the study might solve $x^2 - 23y^2 = 7$ as an example, detailing every step, such as finding the continued fraction expansion of $\sqrt{23}$, calculating its convergents, and using them to derive the fundamental solution. Examples make the study accessible to readers, helping them understand the application of theoretical and numerical tools.

CONCLUSIONS

In the conclusion, the quadratic Diophantine equations, such as $x^2 - Dy^2 = N$, can be analyzed modulo a prime p as well as continued fraction. For example, solving $x^2 \equiv D(mod\ p)$ or $x^2 \equiv N(mod\ p)$ is a critical step in determining whether integer solutions to the original equation exist. Using the quadratic reciprocity law, the problem of evaluating $\left(\frac{a}{p}\right)$ can be transformed into evaluating $\left(\frac{p}{a}\right)$, simplifying the computations. If the quadratic reciprocity law shows that $x^2 \equiv D(mod\ p)$ is unsolvable for a prime p, this may imply that the equation $x^2 - Dy^2 = N$ has no integer solutions. Conversely, if $x^2 \equiv D(mod\ p)$ is solvable for relevant primes, it suggests that solutions may exist. We found the relationship between the value of the Legendre symbol $\left(\frac{p}{q}\right)$ and the length of the period of continued fraction expansion of $D = pq$. We generalized those results to evaluating Jacobi symbols $\left(\frac{p}{q}\right)$ and observe the continued fraction expansion $\sqrt{pq}$ or $\sqrt{\frac{p}{q}}$. By combining numerical methods, theorems, and examples, the researcher develops a comprehensive framework for analyzing and solving quadratic Diophantine equations. Numerical methods handle computations, theorems provide theoretical support, and examples make the topics understandable and accessible. This approach combines practical problem-solving with rigorous theory to compute and verify solutions, while using examples to clarify and demonstrate the results, making the research both robust and comprehensible.

ACKNOWLEDGMENTS

The first author is grateful to the University Grants Commission (UGC), Nepal for providing a PhD Fellowship and Research Support for PhD research (UGC Award No. PhD-78/79-S & T-10 [Faculty]).

AUTHOR CONTRIBUTIONS

This paper is part of a Ph.D. study. The first author designed the research and developed the paper, including the concept, research strategy, and results. The second author contributed to the discussion and handled text editing.

CONFLICT OF INTERESTS

The authors declare no conflict of interest.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the first author and corresponding author, upon reasonable request.

REFERENCES

Aigner, M., & Ziegler, G.M. (2014). *Proofs from the book: Fifth edition*. Springer-Verlag, Berlin.

Aleksander, G. (1997). On some connections between Legendre symbols and continued fractions. *Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae, 24*, 19-21.

Andreescu, T., & Andrica, D. (2015). *Quadratic Diophantine equations*. USA: Springer.

Arya, S.P. (1991). On the brahmagupta-bhaskara equation. *Mathematical Education,* 8(1), 23–27.

Austin, M.M. (1981). *The Hellenistic World from Alexander to the Roman Conquest: A Selection of Ancient Sources in Translation*. Cambridge University Press.

Baumgart, O. (2015). *The quadratic reciprocity law: A collection of classical proofs*. New York: Birkh Basel.

Burton, D.M. (1980). *Elementary number theory*. Allyn and Bacon, Boston.

Chowla, P., & Chowla, S. (1972). Problems with periodic simple continued fractions. *Proceedings of the National Academy of Sciences, 69*, 37-45.

Dudley, U. (2012). *Elementary number theory*. Courier Corporation.

Friesen, C. (1991). Legendre symbols and continued fractions. *Acta Arithmetica, 59*, 365-379.

Jacobi, C.G.J. (1837). *Uber die kreisteilung und ihre anwendung auf die zahlentheorie*. Bericht Ak. Wiss. Berlin.

Legendre, A.M. (1830). *Theorie des nombres, third edition*. Paris: Libraire Scientifique A. Hermann.

Lemmermeyer, F. (2013). *Reciprocity laws: from Euler to Eisenstein*. Springer Science and Business Media.

Malik, K.A., & Al Saffar, N.F.H. (2020). On the quadratic reciprocity law. *Journal of Discrete Mathematical Sciences & Cryptography, 25*(6), 1777-1790.

Mordell, L.J. (1969). *Diophantine equations*. New York: Academic Press.

Niven, I., Zuckerman, H.S., & Montgomery, H.L. (2013). *An introduction to the theory of numbers*. John Wiley and Sons.

Riesel, H. (2015). *Prime numbers and computer methods for factorization: Second Edition*. New York: Birkh Basel.

Schinzel, A. (1974). On two conjectures of P. Chowla and S. Chowla concerning continued fractions. *Annali di Matematica Pura ed Applicata, 98, 111*-117.

Van der Poorten, A.J., & Walsh, P.G. (1999). A Note on Jacobi symbols and continued fractions. *The American Mathematical Monthly, 106*(1), 52-56.

Weintraub, S.H. (2011). In Legendre's work on the law of quadratic reciprocity. *The American Mathematical Monthly*, *118*(3), 210-216.