The Nepali Mathematical Sciences Report
Regd No.: 53/033-034, ISSN: 2392–411X
http://www.journal.cdmathtu.edu.np

Year: 2024, Volume: 41, No. 2
Pages: 157–177
https://doi.org/10.3126/nmsr.v41i2.73233

Research Article

Integer Solutions to Quadratic Diophantine Equations using Efficient Algorithms with Elementary and Quadratic Ring Methods

Bal Bahadur Tamang*[1] and Ajaya Singh[2]

*[1] Mahendra Ratna Multiple Campus, Ilam, Tribhuvan University, Nepal
bal.tamang@mrmc.tu.edu.np
[2]Central Department of Mathematics, Tribhuvan University, Nepal
singh.ajaya1@email.com

Received: 18 July 2024, Accepted: 7 October 2024, Published Online: 31 December 2024

Abstract

In this paper, we study the solvability of quadratic Diophantine equations $x^2-Dy^2=N$, where x and y are unknown integers, and D is a positive integer that is a square free and N is a nonzero integer. We use elementary and quadratic ring methods to find integer solutions of these equations. These methods involve concepts like units, fundamental units, norms, and conjugates in quadratic rings. We propose efficient algorithms to solve the equations for cases where $|N|>\sqrt{D}$ and $|N|<\sqrt{D}$. The algorithms include the continued fraction algorithm, periodic quadratic algorithm, Lagrange-Matthew-Mollin algorithm, and brute-force search. These algorithms can be implemented in programming languages. Finally, we compare the algorithms and analyze their time complexity.

Keywords: Algorithms, Solvability, Quadratic Diophantine equation, Integer, Minimal solution.

AMS(MOS) Subject Classification: 11A07, 11D45, 11A55, 11D75.

1 Introduction

Diophantine equations are polynomial equations with integer variables, in which only integer solutions are studied. Diophantine equation is named after the ancient Greek mathematician Diophantus, who thoroughly studied them. Quadratic Diophantine equations are a specific

*Corresponding author

type of the Diophantine equation in which the polynomial equation is quadratic. A quadratic Diophantine equation [14] has a general form:

$$ax^2 + bxy + cy^2 + dx + ey + f = 0, \tag{1.1}$$

where a, b, c, d, e, f are integer coefficients, x and y are unknown integers. Various mathematicians [14, 15] have investigated these equations, which only have integer solutions. They were particularly interested in identifying infinitely many integer solutions. Let $\Delta = b^2 - 4ac$ represent the discriminant of equation (1.1). This discriminant represents a conic section in the Cartesian plane [7] and plays a key role in identifying the solvability of equation (1.1). If $\Delta = 0$, the conic described equation (1.1) is a parabola. When $\Delta < 0$, the conic is an ellipse, and has only a finite number of solutions. When $\Delta > 0$, the equation (1.1) represents a hyperbola. Thus, the equation (1.1) converts to a general Pell-type equation, which is expressed as follows:

$$x^2 - Dy^2 = N, \tag{1.2}$$

with $x, y \in \mathbb{Z}$ and N is a nonzero integer, and $D > 1$ and is square free. The equation (1.2) known as the generalized Pell's equation, was named after Pell, who studied the set of all nonzero positive integer solutions of equation (1.2) in his work [13].

When $N = 1$, then equation (1.2) becomes

$$x^2 - Dy^2 = 1, \tag{1.3}$$

which is Pell's equation and was discovered by Brahmagupta and Bhaskara [13]. Euler made a mistake [2], and Pell was later wrongly credited with the equation. Lagrange [8] proved that the equation (1.3) has infinitely many integer solutions, with the trivial solution always being $(x, y) = (1, 0)$. He was the first to establish the existence of such solutions. The method of finding integer solutions to the equation (1.2) is referred to as Lagrange reduction. Li [11] demonstrated that the expression for $\sqrt{D}$ as a simple continued fraction provides the minimal solution to equation (1.3). If $(x, y) = (h_1, k_1)$ is the minimal solution to equation (1.3), then the general solutions are given by $(x, y) = (h_n, k_n)$ for all $n \geq 2$, where

$$h_n = \frac{1}{2}\left[(h_1 + k_1\sqrt{D})^n + (h_1 - k_1\sqrt{D})^n\right] \in \mathbb{Z},$$
$$k_n = \frac{1}{2\sqrt{D}}\left[(h_1 + k_1\sqrt{D})^n - (h_1 - k_1\sqrt{D})^n\right] \in \mathbb{Z}.$$

Using the minimal solution $(x, y) = (h_1, k_1)$ of equation (1.3), we can apply the Binomial Theorem to derive the general solution for equation (1.2). This general solution is expressed as $(x, y) = (x_n, y_n), n \geq 2$, where

$$x_n = \frac{1}{2}\left[(s_1 + t_1\sqrt{D})(x_1 + y_1\sqrt{D})^{n-1} + (s_1 - t_1\sqrt{D})(x_1 - y_1\sqrt{D})^{n-1}\right] \in \mathbb{Z},$$
$$y_n = \frac{1}{2\sqrt{D}}\left[(s_1 + t_1\sqrt{D})(x_1 + y_1\sqrt{D})^{n-1} - (s_1 - t_1\sqrt{D})(x_1 - y_1\sqrt{D})^{n-1}\right] \in \mathbb{Z},$$

where (x_1, y_1) is a solution of equation (1.2).

A continuing fraction [12] is used to express the square root of a positive integer D, which is not a perfect square as an infinite fraction. This representation is expressed as the following:

$$\sqrt{D} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \ddots}}}} = [a_0; \overline{a_1, a_2, a_3, \cdots}],$$

where $a_0 \in \mathbb{Z}$ and $a_1, a_2, \cdots, \in \mathbb{Z}^+$ representing the terms of the simple infinite continued fraction.

Counterexample of the simple infinite continued fraction expansion for $\sqrt{92}$ are

$$\sqrt{92} = 9 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{4 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{18 + \cfrac{1}{\ddots}}}}}}}}} = [9; \overline{1, 1, 2, 4, 2, 1, 1, 18}]$$

where the bar over $1, 1, 2, 4, 2, 1, 1, 18$ indicates that these numbers are repeated over and over. A finite simple continued fraction is rational, and the reverse is also true. Similarly, an infinite simple continued fraction is irrational [10]. Furthermore, a periodic simple continued fraction is equivalent to a quadratic irrational number [14]. Any quadratic irrational number ξ_0 can be written as an infinite simple continued fraction:

$$\xi_0 = \frac{p_0 + \sqrt{D}}{q_0} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}},$$

where D, p_0, $q_0 \in \mathbb{Z}$, and $q_0 \neq 0$ and $D > 1$, is square-free, and a_n is partial quotients of quadratic irrational ξ_0. Defined

$$a_0 = \lfloor\sqrt{D}\rfloor, \quad q_0 = 1, p_0 = 0, \quad a_n = \left\lfloor \frac{p_n + \sqrt{D}}{q_n} \right\rfloor,$$

$$p_{n+1} = a_n q_n - p_n, \quad q_{n+1} = \frac{D - p_{n+1}^2}{q_n}.$$

Theorem 1.1. *Suppose that $D > 1$ is square free. Then [14] for all $n \geq -1$*

$$h_n^2 - Dk_n^2 = (-1)^{n-1} q_{n+1}.$$

Theorem (1.1) gives the integer solutions (h_n, k_n) to equation $x^2 - Dy^2 = N$ for a certain value of N. The continued fraction algorithm stops if $h_n^2 - Dk_n^2 = 1$, where $(-1)^{n-1}q_{n+1} = 1$. The $h_1 + k_1\sqrt{D}$ is the minimal positive integer solution to equation $x^2 - Dy^2 = 1$. Theorem (1.1) is useful in the study of quadratic Diophantine equations because it provides a systematic way to generate integer solutions to equations of the form $h_n^2 - Dk_n^2 = (-1)^{n-1}q_{n+1}$, which are closely related to Pell's equation.

Theorem 1.2. *Suppose that r is the length of the period of the expansion of $\sqrt{D}$. Then [14] for all $n \geq 0$*

$$h_{nr-1}^2 - Dk_{nr-1}^2 = (-1)^{nr}.$$

Theorem (1.2) provides infinitely many integer solutions (h_{nr-1}, k_{nr-1}) to the equation $x^2 - Dy^2 = 1$ using even values of nr. If r is even, all values of nr are even. Conversely, if r is odd, Theorem (1.2) yields infinitely many solutions to $x^2 - Dy^2 = -1$ using odd integers $n \geq 1$.

Theorem 1.3. *Suppose that $D > 1$ is square free. Let $\frac{h_n}{k_n}$ denote the n^{th} convergents of the continued fraction expansion of $\sqrt{D}$. Assume there exists a nonzero integer N such that $|N| < \sqrt{D}$. Then [14] for any positive solution $(x, y) = (s, t)$ of the equation $x^2 - Dy^2 = N$ with $\gcd(s, t) = 1$, it follows that $(s, t) = (h_n, k_n)$ for some positive integer n.*

Theorem (1.3) shows that every integer solutions (h_n, k_n) to equation $x^2 - Dy^2 = N$ when $|N| < \sqrt{D}$ can be obtained from n^{th} convergent of the continued fraction expansion of $\sqrt{D}$.

2 Using Elementary and Quadratic Ring Methods

In this section, we study the solvability of the quadratic Diophantine equations using elementary and quadratic ring approaches. We use an elementary method [7] to find integer solutions to these equations. If $(-1)^{n-1}q_{n+1} = 1$ in Theorem (1.1), then we have

$h_n^2 - Dk_n^2 = 1$. Therefore, (h_n, k_n) is the general solution to equation (1.3). Assume that (1.2) is solvable. If (x, y) is a solution of equation (1.2). Then we obtain

$$(h_n + k_n\sqrt{D})(x + y\sqrt{D}) = (h_nx + k_nyD) + (h_ny + k_nx)\sqrt{D}$$

Therefore, the general solution of the equation (1.2) is (x_n, y_n) for all $n > 0$, where

$$x_n = h_nx + k_nyD,\ y_n = h_ny + k_nx.$$

When $|N| < \sqrt{D}$, Theorem (1.3) is applied to determine the minimal solution, which leads to infinitely many positive integer solutions. If $N \neq (-1)^{n-1}q_{n+1}$, for all $n \geq -1$ in Theorem (1.1), then equation (1.2) has no solution. However, if $N = (-1)^{n-1}q_{n+1}$ for some n, then (x_n, y_n) is the general solution to equation (1.2) and we have

$$x + y\sqrt{D} = (x_n + y_n\sqrt{D})(h_1 + k_1\sqrt{D})^n, n \geq 1,$$

where $(h_1 + k_1\sqrt{D})^n$ denote the minimal solution to equation (1.3).

Conversely, when $|N| > \sqrt{D}$, then N can be expressed as δN_0, where δ is either $+1$ or -1 and $N_0 > 0$. Given that $\gcd(x, y) = 1$ Bezout's identity ensures the existence of integers x_1 and y_1 such that

$$xy_1 - yx_1 = \delta. \tag{2.1}$$

Now, we can express it in the following form:

$$(xx_1 - Dyy_1)^2 - D = (xx_1 - Dyy_1)^2 - D(xy_1 - yx_1)^2 = N(x_1^2 - Dy_1^2).$$

It gives

$$x_1^2 - Dy_1^2 = \frac{\beta^2 - D}{\delta N_0} = \eta h, \eta = \pm 1, h > 0, N = \delta N_0, \tag{2.2}$$

where

$$\beta = xx_1 - Dyy_1. \tag{2.3}$$

Assuming that (x_0, y_0) is a solution to equation (2.1) with the parameter $t \in \mathbb{Z}$, the general solution to equation (2.1) can be expressed as $x_1 = x_0 + tx$, $y_1 = y_0 + ty$. Thus, it can be written as:

$$|xx_1 - Dyy_1| = |xx_0 - Dyy_0 + t\delta N_0|.$$

We select a parameter t such that $|xx_1 - Dyy_1| \leq \frac{N_0}{2}$. Consequently, we obtain

$$|t\delta N_0| \leq \frac{N_0}{2} - |xx_0 - Dyy_0|. \tag{2.4}$$

If $\delta = 1$, then inequality (2.4) becomes $|tN_0| \leq \frac{N_0}{2} - |xx_0 - Dyy_0|$. On the other hand, if $\delta = -1$, the inequality (2.4) becomes $| - tN_0| \leq \frac{N_0}{2} - |xx_0 - Dyy_0|$. Combining these two inequalities, we obtain

$$|t| \leq \frac{1}{2} - \frac{|xx_0 - Dyy_0|}{N_0}.$$

Therefore, to find integer solutions to (1.3), the value of t must satisfy this condition to create valid solutions. From (2.3), we obtain $\beta < \frac{N_0}{2}$, and we have $\sqrt{D} < N_0$. From (2.2), it follows that

$$h \leq \frac{\max\{D, \beta^2\}}{N_0} < \frac{\max\{N_o^2, \frac{N_0^2}{4}\}}{N_0} = \frac{N_0^2}{N_0} = N_0.$$

Therefore, we obtain $h < N_0$. However, Theorem (1.1), there exists x_1 and y_1 such that $x_1^2 - Dy_1^2 = \eta h$. Solving equations (2.1) and (2.3), we find

$$x = \frac{-\delta D y_1 \pm \beta x_1}{\eta h}, \quad y = \frac{-\delta x_1 \pm \beta y_1}{\eta h}.$$

Combining these two terms gives:

$$(x + y\sqrt{D}) = \frac{(x_1 + y_1\sqrt{D})(\beta - \delta\sqrt{D})}{\eta h}. \tag{2.5}$$

Its conjugate is

$$(x - y\sqrt{D}) = \frac{(x_1 - y_1\sqrt{D})(\beta + \delta\sqrt{D})}{\eta h}. \tag{2.6}$$

Combining (2.5) and (2.6), we obtain the following:

$$(x^2 - Dy^2) = \frac{1}{\eta^2 h^2}(x_1^2 - Dy_1^2)(\beta^2 - D)) = \frac{1}{\eta^2 h^2}\eta h.\eta h.\delta N_0 = \delta N_0 = N.$$

Therefore, $(x, y) = \left(\frac{-\delta D y_1 + \beta x_1}{\eta h}, \frac{-\delta x_1 + \beta y_1}{\eta h}\right)$ is the integer solutions to the equation (1.2).

Alternatively, we use the quadratic ring approach [4] to solve quadratic Diophantine equations, applying the structure and characteristics of quadratic rings. We define the quadratic ring $R = \{\xi = a + b\sqrt{D} : a, b \in \mathbb{Z}\}$, which provides integral solutions to equation (1.2), where the norm $N(\xi) = N$. The fundamental unit is uniquely significant within the ring of integers in the quadratic field, and the norm $N(\xi) = a^2 - Db^2 = \xi \cdot \overline{\xi} = 1$ plays a key role in the unique factorization of integers in this field. If ω_0 is the fundamental unit of the ring R, then if $N(\omega_0) = 1$, we have $\omega = \omega_0$ and if $N(\omega_0) = -1$, we have $\omega = \omega_0^2$. This relationship between the norm and fundamental units provides insight into the properties of integers in quadratic fields. The vectors $(1, 1)$ and $l(\omega)$ form a basis in the linear space $\mathbb{R}^2$. If $\eta(1, 1) + \zeta l(\omega) = 0$, where η and ζ are real numbers, then $\eta + \zeta \log(\omega) = 0$ and $\eta + \zeta \log(\overline{\omega}) = 0$. This implies $\log(\omega) = \log(\overline{\omega})$, leading to $\eta = \zeta = 0$.

Given $\xi = a + b\sqrt{D} \in R$ with $N(\xi) = N$, and since $N \neq 0$ it follows that $\xi \neq 0$. Therefore, for $\eta, \zeta \in \mathbb{R}$, there exists

$$l(\xi) = \eta(1, 1) + \zeta l|\omega|. \tag{2.7}$$

Thus, we obtain $\log \xi = \eta + \zeta \log |\omega|$ and $\log \overline{\xi} = \eta + \zeta \log |\overline{\omega}|$.

Now,

$$\log |N| = \log |N(\xi)| = \log |\xi| + \log |\overline{\xi}| = 2\eta + \zeta \log |N(\omega)| = 2\eta.$$

Therefore, we have $\eta = \frac{\log|N|}{2}$ and equation (2.7) simplifies to

$$l(\xi) = \frac{\log|N|}{2}(1,1) + \zeta l(\omega). \tag{2.8}$$

Assume that t is the nearest integer to ζ. We establish $\zeta_1 = \zeta - t$ under the condition that $\zeta_1 \leq \frac{1}{2}$. Introducing $\xi_0 = \omega^{-\eta}\xi$, we obtain that ξ is equivalent to ξ_0 with $N(\xi_0) = N(\xi) = N$, where $\xi_0 \in R$. With these considerations, we reduce equation (2.8) to

$$l(\xi_0) = \frac{\log|N|}{2}(1,1) + \zeta_1 l(\omega),$$

which gives

$$\log|\xi_0| = \frac{\log|N|}{2} + \zeta_1 \log\omega, \tag{2.9}$$

$$\log|\overline{\xi_0}| = \frac{\log|N|}{2} + \zeta_1 \log\overline{\omega} = \frac{\log|N|}{2} - \zeta_1 \log\omega. \tag{2.10}$$

From equation (2.9), we can write it as follows:

$$\left|\log|\xi_0| - \frac{\log|N|}{2}\right| \leq \frac{1}{2}\log\omega.$$

This leads to the inequality $\sqrt{\frac{|N|}{\omega}} \leq |\xi_0| \leq \sqrt{\omega|N|}$. Similarly, equation (2.10) can be expressed as follows:

$$\left|\log|\overline{\xi_0}| - \frac{\log|N|}{2}\right| \leq \frac{1}{2}\log\omega.$$

This yields the inequality $\sqrt{\frac{|N|}{\omega}} \leq |\overline{\xi_0}| \leq \sqrt{\omega|N|}$. Therefore, $|\xi_0|$ and $|\overline{\xi_0}|$ can be represented as $r + t\sqrt{D}$, where $r, t \in \mathbb{Z}^+$, and we have

$$t\sqrt{D} \leq \max\{|\xi_0|, |\overline{\xi_0}|\} \leq \sqrt{|N|\omega}. \tag{2.11}$$

From inequality (2.11), we have $t \leq \sqrt{\frac{|N|\omega}{D}}$. Additionally, the maximum value of r in the expression $r + t\sqrt{D}$ is constrained by $|\xi_0|$ and $|\overline{\xi_0}|$, both of which are bounded by $\sqrt{|N|\omega}$. Therefore, we also have $r \leq \sqrt{|N|\omega}$.

3 Using Different Efficient Algorithms and Time Complexity

In this section, we present efficient algorithms for finding integer solutions to the equation $x^2 - Dy^2 = N$, including counterexamples. We describe how to build these algorithms using programming languages. The process involves expressing square roots as continued fractions and using specific algorithms to find the integer solutions. Programming languages can efficiently manage these algorithms, which allows practical computation solutions, especially with large values of D and N. These algorithms are designed to compute the minimal and general solutions for cases where $|N| > \sqrt{D}$ and $|N| < \sqrt{D}$. We determine the time complexity of these algorithms in solving quadratic Diophantine equations. Time complexity is a computational idea that describes how long an algorithm takes to complete based on the size of its input. When dealing with algorithms that identify integer solutions to equations, time complexity determines how long it takes for the algorithm to run as the problem parameters, such as D and N increases.

3.1 Continued fraction algorithm

The continued fraction plays a crucial role in solving the equation $x^2 - Dy^2 = N$. For a positive integer D that is not perfect square, the continued fraction expansion of $\sqrt{D}$ is $\sqrt{D} = [a_0; \overline{a_1, a_2, \cdots, a_{r-1}, 2a_0}]$, where $a_0 = \lfloor \sqrt{D} \rfloor$. Here, r represents the period length, and the terms a_j are determined by a recursive formula [10];

$$\begin{aligned}&\xi_0 = \sqrt{D},\ a_k = \lfloor \xi_k \rfloor, \xi_k = \frac{1}{\xi_k - a_k},\ k = 0, 1, 2, \cdots,\\ &a_r = 2a_0,\ a_{r+k} = a_k,\ k \geq 1.\end{aligned}$$

The numerators h_n and denominators k_n of the n^{th} convergents of the continued fraction are given by

$$\frac{h_n}{k_n} = [a_0; a_1, a_2, \cdots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n.}}}}}}$$

These satisfy the following recursively relations for all $n = 3, 4, 5, \cdots$,

$$h_n = a_n h_{n-1} + h_{n-2},\ k_n = a_n k_{n-1} + k_{n-2},$$

with the initial conditions:

$$h_0 = a_0,\ k_0 = 1,\ h_1 = a_1,\ k_1 = 1,\ h_2 = a_2 a_1 + 1,\ k_2 = a_2.$$

It follows that $h_n k_{n-1} - k_n h_{n-1} = (-1)^{n-1}$. Therefore, using Theorem (1.2), we obtain $h_n^2 - Dk_n^2 = (-1)^n$.

We begin by choosing $D > 1$ and is a square-free and use a simple continued fraction to expand $\sqrt{D}$ as described in Algorithm (1). Next, we compute the convergents following the steps in Algorithm (2). Finally, using Algorithm (3), we find the integer solutions to the equation $x^2 - Dy^2 = 1$.

Algorithm 1 An algorithm for simple continued fraction expansion of $\sqrt{D}$

```
Input: $D$ is a positive square-free integer.
Input: Initialize variables.
    1. Compute the integer part $a_0 = \lfloor \sqrt{D} \rfloor$ of $\sqrt{D}$.
    2. Initialize variables $h_0 = 0, k_0 = 1, h_1 = 1, k_1 = \sqrt{D} - a_0$.
    3. Initialize an empty list to store the terms of the continued fraction expansion, starting with $a_0$.
Input: Compute the continued fraction.
    1. Repeat the steps until the sequence of pairs $(h_n, k_n)$ begins to repeat.
    2. For each $n$, compute:
        (a) $a_n = \left\lfloor \frac{h_n+\sqrt{D}}{k_n} \right\rfloor$.
        (b) Update $h_{n+1} = a_n k_n - h_n$.
        (c) Update $k_{n+1} = \frac{D-h_{n+1}^2}{k_n}$.
        (d) Add $a_n$ to the list of terms.
Output: The list now contains the simple continued fraction expansion of $\sqrt{D}$.
```

Example 3.1. Using Algorithm (1) for simple continued fraction expansion of

$$\sqrt{92} = [9; \overline{1, 1, 2, 4, 2, 1, 18}].$$

After expanding $\sqrt{D}$, the convergents of the continued fraction can be represented as $\frac{h_n}{k_n}$, providing an approximation of $\sqrt{D}$ in Algorithm (2).

Algorithm 2 An algorithm to compute the convergent of the continued fraction expansion of $\sqrt{D}$

```
Input: $D$ is a positive square-free integer, and $n$ is the number of convergents to compute.
Input: Initialize variables.
    1. Set $a_0$ to be the integer part of $\sqrt{D}$, i.e., $a_0 = \lfloor \sqrt{D} \rfloor$.
    2. Initialize: $h_{-2} = 0$, $h_{-1} = 1$, $k_{-2} = 1$, $k_{-1} = 0$.
Input: Compute convergents for $n$ from 0 to $n-1$.
    1. If $n = 0$, set $h_0 = a_0$ and $k_0 = 1$.
    2. For each subsequent $n \geq 1$, compute the continued fraction terms $a_n$ as follows:
        (a) Set $h_n = a_{n-1}k_{n-1} - h_{n-1}$.
        (b) Set $k_n = \frac{D-h_n^2}{k_{n-1}}$.
        (c) Compute $a_n = \left\lfloor \frac{h_n+\sqrt{D}}{k_n} \right\rfloor$.
    3. Compute $h_n$ and $k_n$ using the recursive relations:
           $$h_n = a_n h_{n-1} + h_{n-2}, k_n = a_n k_{n-1} + k_{n-2}.$$
Output: The fraction $\frac{h_n}{k_n}$ is the $n^{th}$ convergent, and the sequence of convergents approximates $\sqrt{D}$.
```

Example 3.2. Using Algorithm (2) to compute the convergent of the continued fraction expansion of $\sqrt{92}$ are

$$\frac{9}{1}, \frac{10}{1}, \frac{19}{2}, \frac{48}{5}, \frac{211}{22}, \frac{470}{49}, \frac{681}{71}, \frac{1151}{120}.$$

Algorithm (3) describes how to find the minimal solution and how to use the minimal solution to the equation (1.3) to obtain other solutions. This algorithm is based on the properties of the theory of continued fractions.

Algorithm 3 An algorithm for solving quadratic Diophantine equation $x^2 - Dy^2 = 1$

```
Input: Expansion of $\sqrt{D} = [a_0; \overline{a_1, \cdots, a_r}]$ using a continued fraction.
Input: Initialize variables:
  1. Set $h_0 = a_0$, $k_0 = 1$, $h_1 = a_1 a_0 + 1$, $k_1 = a_1$.
  2. Compute the continued fraction expansion of $\sqrt{D}$ and iterate for each $n = 2$ to $r$,
     where $r$ is the length of the period in the continued fraction expansion.
  3. For each iteration $n$:
     (a) Compute $h_n$ and $k_n$ using the recursive relations:
             $h_n = a_n h_{n-1} + h_{n-2}, k_n = a_n k_{n-1} + k_{n-2}.$
     (b) Check if $h_n^2 - Dk_n^2 = 1$. If true, $(h_n, k_n)$ is a solution to the Pell's equation
         $h_n^2 - Dk_n^2 = 1$. Stop the iteration.
Output: $(h_{r-1}, k_{r-1})$ is the minimal solution to the equation $h_n^2 - Dk_n^2 = 1$. The general
  solutions are given by $(x_n + y_n\sqrt{D}) = (h_{r-1} + k_{r-1}\sqrt{D})^n$ for $n > 0$.
```

Example 3.3. In the Algorithm (3), the length of periodic of expansion $\sqrt{92}$ is $r = 8$ and we find the minimal solution of equation $x^2 - 92y^2 = 1$ is

$$(x_1, y_1) = (h_{r-1}, k_{r-1}) = (h_7, k_7) = (1151, 120).$$

Using this minimal solution, we obtain other integer solutions.

The continued fraction algorithm is commonly used to solve quadratic Diophantine equations by finding the integer solutions through the continued fraction expansion of $\sqrt{D}$. The complexity is typically polynomial in the input size, with a runtime around $\mathbf{O}(\sqrt{D})$ in [1, 3]. However, computing the continued fraction expansion of $\sqrt{D}$ generally has a time complexity of $\mathbf{O}(\log D)$ in [1, 6] often using techniques that exploit the periodicity of the continued fraction expansion of $\sqrt{D}$. The main iteration step iterates r times, where r is the length of period of the continued fraction expansion with time complexity $\mathbf{O}(r)$ for each iteration. Therefore, the overall time complexity of the algorithm can be expressed as $\mathbf{O}(\log D + r)$.

Using Theorem (1.3), we apply Algorithm (4), which provides the integer solution to the equation $x^2 - Dy^2 = N$ when $|N| < \sqrt{D}$.

Algorithm 4 An algorithm of equation $x^2 - Dy^2 = N$ in case $|N| < \sqrt{D}$

Input: If $|N| < \sqrt{D}$, apply the following steps:

1. Use Theorem (1.1), which states that $h_n^2 - Dk_n^2 = (-1)^{n-1}q_{n+1}$, where q_{n+1} is an integer sequence dependent on n.
2. Ensure that $D > 1$ and D is square-free.
3. Verify that Theorem (1.1) is applicable for all integers $n \geq -1$.
4. Recognize that the terms h_n and k_n represent positive integers as described in Theorem (1.3).
5. Note that $(-1)^{n-1}$ alternates sign, being positive for odd n and negative for even n.

Output: Calculate the values for h_n and k_n that satisfy Theorem (1.3).

Algorithms (4) is designed to search for all integer solutions to equation $x^2 - Dy^2 = N$ when $|N| < \sqrt{D}$.

On the other hand, using elementary approach and Theorem (1.3), we apply Algorithm (5), which provides the integer solution to the equation $x^2 - Dy^2 = N$ when $|N| > \sqrt{D}$.

Algorithm 5 An algorithm of equation $x^2 - Dy^2 = N$ in case $|N| > \sqrt{D}$

Input: Fix n and apply the following steps:

1. **Case 1: When** $h_n < \sqrt{D}$
   - (a) If $h_n < \sqrt{D}$, proceed to the next steps. Otherwise, there will be no solution to $x_n^2 - Dy_n^2 = \eta_n h_n$.
   - (b) Given that $D > 1$ and is square-free, apply Theorem (1.1) to find integer solutions to $x_n^2 - Dy_n^2 = \eta_n h_n$.
   - (c) The solutions (x, y) can be determined using the following expressions:

     $$x = \frac{-\delta D y_n \pm p_n x_n}{\eta_n h_n}, y = \frac{-\delta D x_n \pm p_n y_n}{\eta_n h_n},$$

     where $\delta, p_n, x_n, y_n, \eta_n, h_n$ are values determined based on the equations and parameters. These solutions (x, y) apply to the specific case considered.
2. **Case 2: When** $h_n > \sqrt{D}$
   - (a) If $h_n > \sqrt{D}$, reapply Algorithm (4) with modifications:
     - Replace δ with η_n.
     - Replace N with h_n.

     Modify the expressions for input into Algorithm (4) as follows:

     $$x = \frac{-\eta_n D y_n + p_n x_n}{h_n}, y = \frac{-x_n + p_n y_n}{h_n}.$$

     By making these replacements, continue the process to find all solutions to the equation $x_n^2 - Dy_n^2 = \eta_n h_n$. Given the condition $0 < h_n < N$, after a finite number of operations, all solutions will eventually be found.

Output: Considering the equation $x_n^2 - Dy_n^2 = \eta_n h_n$, find the values of x_n and y_n that satisfy the given conditions and the range of h_n.

3.2 Periodic quadratic algorithm

The periodic quadratic algorithm, often known as the PQa algorithm [5, 9], is a method used to solve equation (1.3). This algorithm uses continued fractions to identify a fundamental solution to equation (1.3) by analyzing the periodic sequences resulting from the recurrence structure of $\sqrt{D}$. The initial conditions and recursive relations are defined as follows, for all $n \geq 0$

$$\begin{aligned} &G_{-2} = -P_0, \quad G_{-1} = Q_0, \quad B_{-2} = 1, \quad B_{-1} = 0, \\ &G_n = a_n G_{n-1} + G_{n-2}, \quad B_n = a_n B_{n-1} + B_{n-2}. \end{aligned}$$

Sometimes, A_n is also computed as follows, for all $n \geq 0$

$$A_{-2} = 0, \quad A_{-1} = 1, \quad A_i = a_n A_{n-1} + A_{n-2}.$$

Then, we have $G_n = Q_0 A_n - P_0 B_n$. We compute the continued fraction expansion of the quadratic irrational, where $Q_0 \neq 0, P_0, Q_0 \in \mathbb{Z}$,

$$\frac{P_0 + \sqrt{D}}{Q_0} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}},$$

where $a_0 = \left\lfloor \frac{P_0+\sqrt{D}}{Q_0} \right\rfloor$ and $a_n = \left\lfloor \frac{P_n+\sqrt{D}}{Q_n} \right\rfloor$ for all $n \geq 1$. Consequently, we have the relation $G_n^2 - DB_n^2 = (-1)^{n+1} Q_{n+1} Q_0$. If we setting $Q_0 = |N|$, then $(-1)^{n+1} Q_{n+1} = \frac{N}{|N|}$. Therefore, we have the equation $G_n^2 - DB_n^2 = N$. Hence, (G_n, B_n) can be used as a solution to the equation under consideration. The sequence a_n represents the simple continued fraction expansion of quadratic irrational $\frac{P_0+\sqrt{D}}{Q_0}$ and the fraction $\frac{P_n}{Q_n}$ is the convergents to this continued fraction. The sequences $\{P_n\}, \{Q_n\}$ and $\{a_n\}$ are periodic and denote the length of period by r. The mathematical approach detailed in the algorithms provides a clear and systematic framework for solving quadratic Diophantine equations, providing that each stage is completed precisely and quickly.

```
**Algorithm 6** Using PQa algorithm to solve the equation $x^2 - Dy^2 = N$
**Input:** Initialization of variables:
    1. $D$: Positive integer, not a perfect square.
    2. $P_0$: Integer.
    3. $Q_0$: Positive integer.
    4. $N$: Non-zero integer.
**Input:** Initial setup:
    1. Set $P_{-2} = -P_0$, $P_{-1} = Q_0$, $B_{-2} = 1$, $B_{-1} = 0$, $A_{-2} = 0$, $A_{-1} = 1$.
    2. Compute initial values: $G_{-2} = -P_0$, $G_{-1} = Q_0$.
**Input:** Compute continued fraction expansion:
    1. For each $n$ from 0 to the desired number of iterations:
        (a) Calculate $a_n = \left\lfloor \frac{P_n+\sqrt{D}}{Q_n} \right\rfloor$.
        (b) Update the numerators and denominators:
                $P_n = a_n P_{n-1} - P_{n-2},\ Q_n = \dfrac{D - P_n^2}{Q_{n-1}}.$
**Input:** Compute the convergents:
    1. For each $n$ from 0 to the desired number of iterations:
        (a) Calculate:
                $G_n = a_n G_{n-1} + G_{n-2},\ B_n = a_n B_{n-1} + B_{n-2}.$
**Input:** Compute $A_n$:
    1. For each $n$ from 0 to the desired number of iterations:
        (a) Calculate:
                $A_n = a_n A_{n-1} + A_{n-2},\ G_n = a_n Q_0 - P_0 B_n.$
**Input:** Verify the quadratic Diophantine equation:
    1. For each $n$ from 0 to the desired number of iterations:
        (a) Check if $G_n^2 - DB_n^2 = (-1)^{n+1} Q_{n+1} Q_0$.
        (b) If $G_n^2 - DB_n^2 = 1$, output $(G_n, B_n)$ as a solution to the quadratic Diophantine
            equation.
**Output:** The algorithm outputs a solution to the quadratic Diophantine equation, representing the pair $(x, y)$.
```

The complexity of the PQa algorithm is determined by the size of D and the level of accuracy required for continued fraction expansion. The PQa algorithm is recognized for its efficiency, and its time complexity has been proposed as a polynomial to the input size. The length of the period of the continued fraction expansion for $\sqrt{D}$ is $\mathbf{O}(\log D)$ in most cases, but in the worst case, it can be as large as $\mathbf{O}(\sqrt{D})$. Therefore, the overall worst-case time complexity of the PQa algorithm is $\mathbf{O}(\sqrt{D} \log D)$. The complexity of using the PQa algorithm to solve equation (1.3) is primarily determined by the size of the input and the specific implementation.

3.3 Lagrange-Matthew-Mollin algorithm

Euler used the continued fraction expansion of $\sqrt{D}$ to create a more accessible method for solving quadratic Diophantine equations. Building on this concept, the Lagrange-Matthew-Mollin (LMM) algorithm [5, 9] was designed to identify the fundamental solution to equation (1.2) using continued fractions. The LMM algorithm aims to find primitive solutions for each equivalence class associated with equation (1.2).

We create a list of positive integers h such that h^2 divides N. For each h in this list, we set $t = \frac{N}{h^2}$ and find all integers z, satisfying $-\frac{|t|}{2} < z \leq \frac{|t|}{2}$ and $z^2 \equiv D(\mathrm{mod}|t|)$. For each such z, we apply the PQa algorithm with $P_0 = z, \quad Q_0 = |t|, D = D$. The process continues until either an index $n \geq 1$ is reached where $Q_n = \pm 1$ or the end of the first period in the sequence a_n is completed without finding n where $Q_n = \pm 1$. If the first period completes without finding n where $Q_n = \pm 1$. Then no such n exists. However, if n is reached with $Q_n = \pm 1$, we set $r = G_{n-1}, s = B_{n-1}$. If the equation $r^2 - ds^2 = t$, then we add $x = hr, y = hs$ to the list of solutions. If the equation $r^2 - ds^2 = -t$, then we add $x = h(ru + svD), y = h(rv + su)$ to the list of solution, where (u, v) is the minimal solution to $r^2 - Ds^2 = -1$.

Algorithm 7 Using LMM algorithm to solve the equation $x^2 - Dy^2 = N$

```
Input: Consider the following variables:
    1. Positive integer $N$ and $h$, where $h > 0$.
    2. Calculate $t = \frac{N}{h^2}$.
Input: List generation:
    1. Generate a list of positive integers $h$ such that $h > 0$ and $h^2$ divides $N$.
Input: Solving quadratic congruence:
    1. For each $h$ in the list:
        (a) Calculate $t = \frac{N}{h^2}$.
        (b) For each $z$ in the range $\left(-\frac{|t|}{2} < z \leq \frac{|t|}{2}\right)$ and $z^2 \equiv D \pmod{|t|}$:
            i. Apply the PQa algorithm with initial values $P_0 = z, Q_0 = |t|, D = D$.
            ii. Iterate the PQa algorithm to obtain $a_n$ for $n \geq 1$.
            iii. Check if there exists $n$ such that $Q_n = \pm 1$.
            iv. If such $n$ with $Q_n = \pm 1$ is found, then set $(r, s) = (G_{n-1}, B_{n-1})$.
Input: Adding solutions:
    1. If there exists $n$ with $Q_n = \pm 1$:
        (a) Add $x = hr$, $y = hs$ to the solution set if $r^2 - Ds^2 = t$.
        (b) Add $x = h(ru + svD)$, $y = h(rv + su)$ to the solution set if $u^2 - Dv^2 = -t$,
            where $(u, v)$ is the minimal solution to $r^2 - Ds^2 = -1$.
Output: The algorithm produces the complete set of solutions $z$.
```

Example 3.4. Using Algorithm (7), to solve the equation $x^2 - 13y^2 = 108$, we first note that $h > 0$ and h^2 divides 108. The possible values of h are $1, 2, 3, 6$. Setting $h = 1$, we get $t = 108$. Next, we evaluate z within the range $-\frac{108}{2} < z \leq \frac{108}{2}$ and find that the solutions to $z^2 \equiv 13 (\mathrm{mod}\, 108)$ are ± 11 and ± 43.

Using PQa algorithm (6) with $P_0 = 11, Q_0 = |t| = 108, D = 13$, the first occurrence of $Q_n = \pm 1$ is at $Q_1 = -1$. Therefore, we add the solution $(x, y) = (G_0, B_0) = (-11, 1)$ to the list of solution for the equation $x^2 - 13y^2 = 108$. Similarly, using PQa algorithm (6) with $P_0 = 43, Q_0 = 108, D = 13$, the first occurrence of $Q_n = \pm 1$ is at $Q_3 = 1$, but $G_2^2 - 13B_2^2 = 23^2 - 13.7^2 = -108$. Since the equation $h^2 - 13k^2 = -1$ has a solution with the minimal solution $(h, k) = (18, 5)$, we add $x = 1(23.18 + 7.5.13) = 869, y = (7.18 + 23.5) = 241$ to the list of solution to equation $x^2 - 13y^2 = 108$ and so on. Similarly, by setting $h = 2, 3, 6$ with corresponding values $t = 27, 12, 3$ and applying the PQa algorithm, we find the additional solutions to the equation $x^2 - 13y^2 = 108$.

Selecting a list of positive integers h such that h^2 divides N takes runtime $\mathbf{O}(\sqrt{N})$. The PQa algorithm depends on the value of t, with a range for z given by R. We know that time complexity of the PQa algorithm is $\mathbf{O}(\sqrt{N}\log|t|)$, where $|t|$ represents the absolute value of t. Let S be a generating solution of equation and a time complexity is $\mathbf{O}(S)$. Therefore, the time complexity of the LMM algorithm becomes $\mathbf{O}(\sqrt{N}\log(|t|)R+S)$.

3.4 Brute-force algorithm

The brute-force search algorithm [5, 9] is a simple problem-solving method for solving equations by systematically studying all possible integers (x, y) until a solution satisfies the equation. The algorithm iterates through every possible y value within a certain range, computing the corresponding x values if they satisfy the given equation, and then finds a solution. Let (h, k) be the minimal solution to the equation $x^2 - Dy^2 = N$.

If $N > 0$, the search range is defined by $l_1 = 0$ to $l_2 = \sqrt{\frac{(h-1)N}{2D}}$. If $N < 0$, the range is from $l_1 = \sqrt{\frac{|N|}{2}}$ to $l_2 = \sqrt{\frac{(h+1)|N|}{2D}}$. If $l_1 \leq y \leq l_2$ and $N + Dy^2$ is square, the corresponding x value can be computed as $x = \sqrt{N + Dy^2}$. If l_2 is not excessively large, and $\sqrt{\frac{(h\pm1)|N|}{2D}}$ remains manageable, searching within the bounds l_1 and l_2 is sufficient and to find all integer solutions.

Algorithm 8 Using Brute-force algorithm to solve the equation $x^2 - Dy^2 = N$

```
Input: Initialize variables:
    1. Set $N$, $D$, $h$, $l_1$, $l_2$.
    2. Initialize an empty list for solutions: $(x, y)$.
Input: Define the search range for $y$:
    1. If $N > 0$, set $l_1 = 0$ and $l_2 = \sqrt{\frac{N(h-1)}{2D}}$.
    2. If $N < 0$, set $l_1 = \sqrt{\frac{|N|}{2}}$ and $l_2 = \sqrt{\frac{|N|(h+1)}{2D}}$.
Input: Perform a brute-force search:
    1. Iterate through values of $y$ from $l_1$ to $l_2$.
    2. For each $y$, calculate $x$ using $x = \sqrt{N + Dy^2}$ if $N + Dy^2$ is a perfect square.
    3. Check if $x$ and $y$ satisfy the equation $x^2 - Dy^2 = N$.
    4. If the equation is satisfied, add the pair $(x, y)$ to the list of solutions.
Output: The algorithm produces all integer pairs $(x, y)$ that satisfy the equation $x^2 -$
    $Dy^2 = N$ for the given $N$, $D$, $h$.
```

Example 3.5. Using Algorithm (8), we solve the equation $x^2 - 13y^2 = 108$, and obtain the minimal positive solution of equation $h^2 - 13k^2 = 1$ is $(h, k) = (649, 180)$. Given

$N = 108 > 0$, the search range for l_1 begins at 0 extends to $l_2 = \sqrt{\frac{108(649-1)}{2\times 13}} \approx 51.882$. Thus, the range for y is $0 \leq y \leq 51.882$. The values of y for which $108 + 13y^2$ is a perfect square are $y = 1, 3, 6, 11, 22, 39$. The solutions for (x, y) are $(\pm 11, 1), (\pm 15, 3), (\pm 24, 11), (\pm 80, 22)$, and $(\pm 141, 39)$.

A brute-force algorithm to solve the equation (1.2) typically has exponential time complexity. This is due to the exhaustive nature of the brute-force algorithm, which involves verifying many possibilities to identify those that satisfy the equation. As a result, the time complexity is usually $\mathbf{O}(2^n)$, where n is the size of the input data.

The differences between these algorithms have a specific purpose and technique for solving quadratic Diophantine equations, particularly Pell's equation. The continued fraction algorithm is more efficient and systematic in finding solutions, especially for a small value of D. The PQa algorithm efficiently uses the periodicity properties of integer solutions to identify periodic solutions to quadratic Diophantine equations. We can describe the LMM algorithm as expanding the PQa algorithm's results. While the PQa algorithm focuses mainly on constructing the continued fraction expansion and the related convergents, the LMM algorithm uses these convergents to solve the quadratic Diophantine equation. Specifically, the LMM algorithm uses the convergents generated by the PQa algorithm to identify the fundamental solution to generalized Pell's equation, which can then be used to solve more general cases. The brute-force algorithm is a simple but potentially computationally expensive approach.

These algorithms will be implemented in a programming language, with the code provided to compute integer solutions to quadratic Diophantine equations. The implementation will involve representing square roots as continued fractions and applying specific algorithms, each with different time complexities.

4 Conclusion

In this study, we investigated the solvability of quadratic Diophantine equations $x^2 - Dy^2 = N$, where D is a positive square-free integer, and N is a non-zero integer. We utilized both elementary and quadratic ring methods, incorporating concepts such as units, fundamental units, norms, and conjugates to establish a theoretical foundation for finding integer solutions. Efficient algorithms were developed for specific cases where $|N| < \sqrt{D}$ and $|N| > \sqrt{D}$ of equation $x^2 - Dy^2 = N$. These include the continued fraction algorithm, the periodic quadratic algorithm, the Lagrange-Matthew-Mollin algorithm, and the brute-force search. Each algorithm was implemented in programming languages.

The study demonstrated the practical application of these algorithms through numerical experiments. We analyzed and compared the algorithms regarding their time complexity, identifying their strengths and limitations for different ranges of D and N. This comprehensive framework offers a robust foundation for further research and application in solving quadratic Diophantine equations.

Conflicts of Interest

I hereby want to ensure that there is no conflict of interest among the authors.

Acknowledgments

The first author wishes to extend heartfelt gratitude to the University Grants Commission (UGC), Nepal, for providing the PhD Fellowship and Research Support for the PhD study (UGC Award No. PhD-78/79-S&T-10 [Faculty]).

Additionally, the author sincerely acknowledges the University Grants Commission for the travel grants provided in 2080/081.

Special thanks are also extended to the Nepal Mathematical Society (NMS) for sponsoring the NMS-Nick Simon PhD Fellowship in 2022 to support the PhD work.

References

[1] B.B. Tamang, and A. Singh, Efficient Approaches to Solving Quadratic Diophantine Equations and their Time Complexity, *Journal of Nepal Mathematical Society*, Vol. 6, No. 2, pp 1-6, 2024.
https://doi.org/10.3126/jnms.v6i2.63005

[2] E.J. Barbeau, *Pell's Equation, Problem Books in Mathematics*, Springer-Verlag, New York, 2003.

[3] H.W. Lenstra Jr., Solving the Pell Equation, *Notices of the AMS*, Vol. 49, No. 2, pp 182-192, 2002. http://hometown.aol.com/jpr2718/pell.pdf

[4] I. Niven, H. S. Zuckerman and H. L. Montgomery, *it An introduction to the theory of numbers*, John Wiley and Sons, New York, 2013.

[5] J. Robertson, *Solving the generalized Pell's equation* $x^2 - Dy^2 = N$, 2004.
http://hometown.aol.com/jpr2718/pell.pdf

[6] J.C. Lagarias, On the computational complexity of determining the solvability or Unsolvability of the equation $x^2 - dy^2 = 1$, *Trans. Amer. Math. Soc.*, Vol. 260, pp 485-508, 1980.

[7] J.C. (Jr) Owings, An elementary approach to diophantine equations of the second degree, *Duke Math. J.*, Vol. 37, pp 76-104, 1970.

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

[9] K. Matthews, The Diophantine equation $x^2 - Dy^2 = N, D > 0$. *Expositiones Mathematics*, Vol. 18, pp 323-331, 2000.

[10] K. Matthews, J. Robertson and J. White, Midpoint Criteria For Solving Pell's Equation Using The Nearest Square Continued Fraction, *MATHEMATICS OF COMPUTATION*, Vol. 79, No. 269, pp 485-499, 2010. S 0025-5718(09)02286-8

[11] K.Y. Li, Pell's equation, *Math. Exc.*, Vol. 6, pp 1-4, 2001.

[12] R.A. Mollin, K. Cheng and B. Goddard, The Diophantine equation $x^2 - Dy^2 = c$ Solved via continued fractions, *Acta Mathematika University Comenianae*, Vol. 71, pp 545-560, 2002.

[13] S.P. Arya, On the Brahmagupta-Bhaskara equation, *Math. Ed.*, Vol. 8, No. 1, pp 23-27, 1991.

[14] T. Andreescu and D. Andrica, *Quadratic Diophantine Equations*, Springer, New York, 2015.

[15] T. Nagell, *Introduction to Number Theory*, Chelsea Publishing Company, New York, 1981.

[16] Y.T. Cheng, *Continued Fractions*, Cornell University, USA, 2007.