# Some Aspects of Quadratic Diophantine Equations 

Bal Bahadur Tamang ${ }^{1 *}$, Ajay Singh ${ }^{2}$<br>${ }^{1}$ M.Phil. Scholar, Central Department of Mathematics, Institute of Science and Technology, Tribhuvan University, Kathmandu, Nepal<br>${ }^{2}$ Central Department of Mathematics, Institute of Science and Technology, Tribhuvan University, Kathmandu, Nepal

*Corresponding Author: Bal Bahadur Tamang, M.Phil. Scholar, Central Department of Mathematics, Institute of Science and Technology, Tribhuvan University, Kathmandu, Nepal


#### Abstract

In this paper, we consider the positive integer solutions of quadratic Diophantine equation ax ${ }^{2}+$ $b x y+c y^{2}=N, a>0, b^{2}-4 a c>0$, not perfect square and can be transformed into Pell's equation $x^{2}-$ $d y^{2}=N$ by using linear transformations with integral coefficients. We also investigate if $\alpha \delta-\beta \gamma=1$. Then the unimodular transformation $x=\alpha X+\beta Y, y=\delta X+\gamma Y$ converts the form $a x^{2}+b x y+c y^{2}=N$ to $a_{0} X^{2}+b_{0} X Y+c_{0} Y^{2}=N_{0}$.


Keywords: Diophantine equation, integer solution, linear transformation, Pell's equation, solvability.

## 1. INTRODUCTION

An equation in one or more unknowns which is to be solved in integers is known as Diophantine Equation, named after the Greek Mathematician Diophantus. The word Diophantine refers to the Hellenistic mathematician of the $3^{\text {rd }}$ century, Diophantus of Alexandria, who made a study of such equations and was one of the first mathematicians to introduce symbolism into algebra.

In general, Diophantine equation
$x^{2}+b x y+c y^{2}+d x+e y+f=0$
where $a, b, c, d, e, f$ are integral coefficients. There has been interest in determining all integer solutions to Diophantine equations among mathematician [8], [10], [19]. When studying a given Diophantine equation is whether a solution exists and in the case they exists, how many solutions, there are and whether there is a general form for the solution [14], [12]. So Diophantine equation represents a conic in the Cartesian plane and solution to equation (1) in integer solutions. It means finding all lattice points situated on this conic.

Let $\Delta=\mathrm{b}^{2}-4 \mathrm{ac}$ be the discriminant of the equation (1) [17].
When $\Delta<0$, the conic given by equation (1) is an ellipse and has only a finite number of solutions.
When $\Delta=0$, then the conic given by equation (1) is a parabola.
For this, if $2 \mathrm{ae}-\mathrm{bd}=0$, then the equation (1) becomes
$(2 a x+b y+d)^{2}=d^{2}-4 a f$
If $2 a \mathrm{e}-\mathrm{bd} \neq 0$, then substitutions
$X=2 a x+b y+d, Y=(4 a e-2 b d) y+4 a f-d^{2}$
So, the equation (1) reduces to $\mathrm{X}^{2}+\mathrm{Y}=0$.
When $\Delta>0$, the conic given by equation (1) is an hyperbola. So, the equation (1) reduces to a general Pell-type equation
$x^{2}-d y^{2}=N$
with $\mathrm{x}, \mathrm{y}$ are integers, N is nonzero integer and $d>0$, not perfect square [4], [10] which is special case of equation (1) known as Generalized Pell's Equation which is named after an English Mathematician John Pell who searched for integer solutions to equation of this type in (1611-1685). A nature of the equation (2) is that if it has an integer solution ( $x, y$ ) with $x y \neq 0$, then it must have infinitely many integer solutions. Assume that $(x, y)=\left(u_{0}, v_{0}\right)$ is an integer solution of equation (2). Then one may check that $(x, y)=\left(u_{0}, v_{0}\right)$ also solves the equation (2) and when $n \in N$
$u_{n}=\frac{1}{2}\left[\left(u_{0}+v_{0} \sqrt{d}\right)\left(x_{0}+y_{0} \sqrt{d}\right)^{n-1}+\left(u_{0}-v_{0} \sqrt{d}\right)\left(x_{0}-y_{0} \sqrt{d}\right)^{n-1}\right] \in Z$
$v_{n}=\frac{1}{2 \sqrt{d}}\left[\left(u_{0}+v_{0} \sqrt{d}\right)\left(x_{0}+y_{0} \sqrt{d}\right)^{n-1}-\left(u_{0}-v_{0} \sqrt{d}\right)\left(x_{0}-y_{0} \sqrt{d}\right)^{n-1}\right] \in Z$
These solutions can be obtained from the Binomial theorem and establishing the recurrence relations. It is also known that even if equation (2) is solvable in integers x and y finding its fundamental solution may not be an easy matter.

For $N=1$, equation (2) reduces Pell's equation
$x^{2}-d y^{2}=1$
is known as the classical Pell's equation [3], [15] and was first studied by Brahmagupta (598-670) and Bhaskara (1114-1185) [1]. Its complete theory was worked out by Lagrange (1736-1813), not Pell. Lagrange was first to prove that Pell's equation has infinitely many solutions if d is a positive, not perfect square [15]. It is often said that Euler (1707-1783) mistakenly attributed Brounckers (1620-1684) work on this equation to Pell. So equation (3) has infinitely many integer solutions $\left(x_{n}, y_{n}\right)$ for $n>1$. The first non trivial positive integer solution $\left(x_{1}, y_{1}\right)$ of equation (3) is called the fundamental solution.

In fact $\left(x_{1}, y_{1}\right)$ is fundamental solution of equation (3). Then $n^{\text {th }}$ positive solution $\left(x_{n}, y_{n}\right)$ is defined by
$\mathrm{x}_{\mathrm{n}}+\mathrm{y}_{\mathrm{n}} \sqrt{\mathrm{d}}=\left(\mathrm{x}_{1}+\mathrm{y}_{1} \sqrt{\mathrm{~d}}\right)^{\mathrm{n}}$
for integer $n>1$ [15].
In 1768 Lagrange proved that equation (3) has non-trivial integer solutions for all not perfect square $d>1$ and its all integer solutions can be generated by its fundamental solution $(\mathrm{x}, \mathrm{y})=\left(\mathrm{x}_{1}, \mathrm{y}_{1}\right)$. But the most efficient method for finding the fundamental solution is based on the simple finite continued fraction expansion of $\sqrt{d}$ [2], [13].

## Fundamental Solution

The positive solution $\left(x_{0}, y_{0}\right)$ to the Pell's equation $x^{2}-d y^{2}=1$ is called Fundamental solution if $\mathrm{x}<u, y<v$ for every other positive solution $(\mathrm{u}, \mathrm{v})$. To find the positive solution of the Pell's equation $x^{2}-d y^{2}=1$ using Continued fraction expansion of $\sqrt{d}$. Similarly fundamental solution $(u, v)$ of a class of solutions $K$ of equation $a x^{2}+b x y+c y^{2}=N$ is one where $v$ has least nonnegative value when $(u, v)$ belongs to $K$. Let $u^{\prime}=-\frac{(a u+b v)}{a}$ be the conjugate solution to $u$. If $u^{\prime}$ is not integral or if $\left(u^{\prime}, v\right)$ is not equivalent to $(u, v)$, this determines $(u, v)$. If $u^{\prime}$ is integral and $\left(u^{\prime}, v\right)$ is equivalent to $(u, v)$, where $u \neq u^{\prime}$. We choose $u>u^{\prime}$. There are finitely many equivalence classes, each indexed by a fundamental solution.

Let $\left[a_{0}, a_{1}, \ldots, a_{k}, 2 a_{0}\right]$ be the simple continued fraction expansion of $\sqrt{\mathrm{d}}$.
Let
$\mathrm{p}_{-1}=1, \mathrm{p}_{-2}=0, \mathrm{q}_{-1}=0, \mathrm{q}_{-2}=1$
$\mathrm{p}_{\mathrm{k}}=\mathrm{a}_{\mathrm{k}} \mathrm{p}_{\mathrm{k}-1}+\mathrm{p}_{\mathrm{k}-2}, \quad \mathrm{q}_{\mathrm{k}}=\mathrm{a}_{\mathrm{k}} \mathrm{q}_{\mathrm{k}-1}+\mathrm{q}_{\mathrm{k}-2}$
where $\mathrm{k}=0,1,2, \ldots, \mathrm{n}$, which is recurrence relation [16]. If k is odd, then the fundamental solution is $\left(x_{1}, y_{1}\right)=\left(p_{k}, q_{k}\right)$ where $p_{k}$ and $q_{k}$ is the $k^{\text {th }}$ convergent of $\sqrt{d}$ and if $k$ is even, then the fundamental solution is $\left(\mathrm{x}_{1}, \mathrm{y}_{1}\right)=\left(\mathrm{p}_{2 \mathrm{k}+1}, \mathrm{q}_{2 \mathrm{k}+1}\right)$ [15].

## Theorem

If $d$ is a positive integer, not perfect square, then the equation $u^{2}-d v^{2}=1$ han infinitely many solutions in positive integers and the general solution is $\left(u_{n}, v_{n}\right)_{n \geq 0}$
$u_{n+1}=u_{1} u_{n}+d v_{1} v_{n}, v_{n+1}=v_{1} u_{n}+u_{1} v_{n}$
where $\left(u_{1}, v_{1}\right)$ is fundamental solution.
Assume that equation (2) is solvable and let ( $x, y$ ) be one of its solutions. Then

$$
\begin{aligned}
& \left(u_{n}+v_{n} \sqrt{d}\right)(x+y \sqrt{d})=u_{n} x+u_{n} y \sqrt{d}+x v_{n} \sqrt{d}+v_{n} y d \\
& =\left(u_{n} x+v_{n} y d\right)+\left(u_{n} y+v_{n} x\right) \sqrt{d}
\end{aligned}
$$

And
$\left(u_{n} x+v_{n} y d\right)^{2}-d\left(u_{n} y+v_{n} x\right)^{2}=u_{n}{ }^{2} x^{2}+2 x y d u_{n} v_{n}+v_{n}{ }^{2} y^{2} d^{2}-d u_{n}{ }^{2} y^{2}-2 d x y u_{n} v_{n}-d v_{n}{ }^{2} x^{2}$
$=\left(x^{2}-d y^{2}\right)\left(u_{n}{ }^{2}-d v_{n}{ }^{2}\right)$
$=\mathrm{N} .1=\mathrm{N}$
It follows that $\left(x_{n}, y_{n}\right)_{n \geq 0}$, where
$x_{n}=u_{n} x+v_{n} y d, \quad y_{n}=u_{n} y+v_{n} x$
satisfies the general Pell's equation. Hence every initial solution of the equation (2) generates its own family of infinitely many solutions. We say that the solution $\left(x_{n}, y_{n}\right)_{n \geq 0}$ is associated with the solution $\left(u_{n}, v_{n}\right)_{n \geq 0}$. The set of all solutions associated with each other forms a class of solutions to equation (2).

## 2. Materials and Methods

We considered some aspects of quadratic Diophantine equations. In this paper, we consider the integer solutions of quadratic Diophantine equation and is to be determine the solvability for quadratic Diophantine equation $\mathrm{ax}^{2}+\mathrm{bxy}+\mathrm{cy}^{2}=\mathrm{N}$. The main result of the quadratic Diophantine equation was made on the basis of different published documents.

## 3. RESULTS

## Quadratic Diophantine Equation

In 1885, Serret [21] studied the quadratic Diophantine equation
$\mathrm{ax}^{2}+\mathrm{bxy}+\mathrm{cy}^{2}=\mathrm{N}, \mathrm{a}>0, \operatorname{gcd}(\mathrm{a}, \mathrm{b}, \mathrm{c})=1 \mathrm{~b}^{2}-4 \mathrm{ac}>0$ is positive, not perfect square and $0<$ $|\mathrm{N}|<\frac{\sqrt{d}}{2}$. Serret showed that if $\mathrm{N}>0$, then any relatively prime solution ( $\mathrm{x}, \mathrm{y}$ ) with $\mathrm{y}>o$ is a convergent to $\rho=\frac{(-\mathrm{b}+\mathrm{pd})}{2 \mathrm{a}}$ or $\sigma=\frac{(-\mathrm{b}-\mathrm{pd})}{2 \mathrm{a}}$. However he was unable to deal conclusively with the case $\mathrm{N}<0$. This was done by M . Pavone [18] in the special case when $|\mathrm{N}|<\mu$ is the least of the absolute values of integers represented by $\mu$ for integers $x$ and y not both zero. We remark that Lagrange [4] proved $\mu<\frac{\sqrt{d}}{2}$. We modify M. Pavone proof when $-\frac{\sqrt{d}}{2}<\mu<0$ to show that either $\frac{x}{y}$ is a convergent to $\rho$ or $\sigma$ or has the form
$p_{m}-p_{m-1}, q_{m}-q_{m-1}$ or $p_{r}-p_{r-1}, q_{r}-q_{r-1}$
where
$\rho=\left[\mathrm{a}_{0}, \ldots, \mathrm{a}_{\mathrm{m}}, \overline{\mathrm{b}_{1}, \ldots, \mathrm{~b}_{\mathrm{n}}}\right]$ and
$\sigma=\left[\mathrm{c}_{0}, \ldots, \mathrm{c}_{\mathrm{r}}, \overline{\mathrm{d}_{1}}, \ldots, \mathrm{~d}_{\mathrm{n}}\right]$
where $a_{m} \neq b_{n}, c_{r} \neq d_{n}, \frac{p_{k}}{q_{k}}$ and $\frac{P_{k}}{Q_{k}}$ denote convergence of $\rho$ and $\sigma$ respectively.
Finally, we remark that there is a continued fraction algorithm [10] for solving equation $a x^{2}+b x y+c y^{2}=N$ irrespective of the size of $N$.

Let us consider an infinite form $\mathrm{f}(\mathrm{x}, \mathrm{y})=\mathrm{ax}^{2}+\mathrm{bxy}+\mathrm{cy}^{2}=\mathrm{N}$ is Hermite reduced [5] if the roots $\theta_{1}$ and $\theta_{2}$ of $\mathrm{f}(\mathrm{x}, 1)=0$ satisfy $\theta_{1}>1$ and $-1<\theta_{2}<0$. Equivalently
$\theta_{1}=\left[b_{1}, \ldots, b_{n}\right]$ and $\theta_{2}=-\left[0, b_{n}, \ldots, b_{1}\right]$, where $b_{i}$ are positive integers. Let us consider
$\theta_{1}=\left[a_{0}, a_{1}, \ldots\right]$ and $\theta_{2}=-\left[a_{1}, a_{2}, \ldots\right]$ be Hermite reduced and infinite sequences $\left(S_{k}\right),\left(T_{k}\right)[18]$ be defined as
$\mathrm{S}_{0}=\mathrm{T}_{-1}, \mathrm{~S}_{-1}=\mathrm{T}_{0}=0$
$\mathrm{S}_{\mathrm{k}+1}=\mathrm{a}_{\mathrm{k}} \mathrm{S}_{-\mathrm{k}}+\mathrm{S}_{\mathrm{k}-1}, \mathrm{~T}_{\mathrm{k}+1}=\mathrm{a}_{\mathrm{k}} \mathrm{T}_{\mathrm{k}}+\mathrm{T}_{\mathrm{k}-1}, \mathrm{k} \geq 0$
$\mathrm{S}_{-\mathrm{k}-1}=-\mathrm{a}_{-\mathrm{k}} \mathrm{S}_{-\mathrm{k}}+\mathrm{S}_{-\mathrm{k}+1}, \mathrm{~T}_{-\mathrm{k}-1}=-\mathrm{a}_{\mathrm{k}} \mathrm{T}_{-\mathrm{k}}+\mathrm{T}_{-\mathrm{k}+1} \mathrm{~T}_{-1}, \mathrm{k} \geq 0$
For $\mathrm{k} \geq 1$, the convergents to $\theta_{1}$ are
$\frac{\mathrm{S}_{\mathrm{k}}}{\mathrm{T}_{\mathrm{k}}}=\frac{\mathrm{A}_{\mathrm{k}-1}}{\mathrm{~B}_{\mathrm{k}-1}}=\left[\mathrm{a}_{0}, \ldots, \mathrm{a}_{\mathrm{k}-1}\right]$
To determine the convergent to $\theta_{2}$ are
$\frac{\mathrm{S}_{-\mathrm{k}-1}}{\mathrm{~T}_{-\mathrm{k}-1}}=\left[0, \mathrm{a}_{-1}, \ldots, \mathrm{a}_{\mathrm{k}}\right]$
and use the following result [6]
$\theta_{2}=\left\{\begin{array}{l}{\left[-1,1, a_{-1}+1, a_{-2}, \ldots\right] \text { if } a_{-1}>1} \\ {\left[-1, \quad a_{-2}+1, a_{3, \ldots}\right] \text { if } a_{-1}=1}\end{array}\right.$
For $\mathrm{k} \geq 0$, the convergent to $\theta_{2}$ are
$\left(\mathrm{A}_{0}, \mathrm{~B}_{0}\right)=(-1,1)$
$\left(A_{k}, B_{k}\right)=\left\{\begin{array}{c}(-1)^{k+1}\left(S_{k}, T_{K}\right), \quad k \geq 1, \quad \text { if } a_{-1}>1 \\ (-1)^{k+1}\left(S_{-k-2}, T_{-K-2}\right), \quad k \geq 0, \quad \text { if } a_{-1}=1\end{array}\right.$
For $\mathrm{k} \geq 1, \mathrm{~S}_{-\mathrm{k}-1}$ is positive when k is odd and $\mathrm{T}_{-\mathrm{k}-1}$ is negative when k is odd.

## Theorem [11]

Suppose that $0<N<\frac{\sqrt{d}}{2}$. Let $(\mathrm{p}, \mathrm{q})$ be a relatively prime solution of $\mathrm{ax}^{2}+\mathrm{bxy}+\mathrm{cy}^{2}=\mathrm{N}, \mathrm{a}>0$
with $\mathrm{q}>0$. Then $\frac{\mathrm{p}}{\mathrm{q}}$ is a convergent to $\rho=\frac{(-\mathrm{b}+\sqrt{\mathrm{d}})}{2 \mathrm{a}}$ or $\sigma=\frac{(-\mathrm{b}-\sqrt{\mathrm{d}})}{2 \mathrm{a}}$
Proof
We have
$a\left(\frac{p}{q}-\rho\right)\left(\frac{p}{q}-\sigma\right)=\frac{N}{q^{2}}$
Assume that $\frac{\mathrm{p}}{\mathrm{q}}>\sigma$, then

$$
\begin{aligned}
& \frac{p}{q}-\rho=\frac{N}{a\left(\frac{p}{q}-\sigma\right) q^{2}} \\
& =\frac{N}{a\left(\frac{p}{q}-\rho+\rho-\sigma\right) q^{2}} \\
& \frac{\sqrt{d}}{2 a(\rho-\sigma) q^{2}} \\
& \quad=\frac{\sqrt{d}}{2 q^{2}}
\end{aligned}
$$

Hence $\frac{\mathrm{p}}{\mathrm{q}}$ is a convergent $\frac{\mathrm{p}_{\mathrm{k}}}{\mathrm{q}_{\mathrm{k}}}, \mathrm{k} \geq 0$, to $\rho$ by Lagrange [7]. There is a similar argument if $\frac{\mathrm{p}}{\mathrm{q}}<\sigma$

## Theorem [11]

Let $f(x, y)=\mathrm{ax}^{2}+\mathrm{bxy}+\mathrm{cy}^{2}=\mathrm{N}, \mathrm{a}>0, \mathrm{~b}^{2}-4 \mathrm{ac}>0$, not perfect square. Let p and $\mathrm{q}>0$ be relatively primes integers such that $f(p, q)=\mu$. Let the roots of $f(x, 1)=0$ be
$\rho=\left[\mathrm{a}_{0}, \ldots, \mathrm{a}_{\mathrm{m}}, \overline{\mathrm{b}_{1}, \ldots, \mathrm{~b}_{\mathrm{n}}}\right]$
$\sigma=\left[\mathrm{c}_{0}, \ldots, \mathrm{c}_{\mathrm{r}}, \overline{\mathrm{d}_{1}}, \ldots, \mathrm{~d}_{\mathrm{n}}\right]$
where $a_{m} \neq b_{n}, c_{r} \neq d_{n}$. Let the convergents of $\rho$ and $\sigma$ be denoted by $\frac{p_{k}}{q_{k}}$ and $\frac{P_{k}}{Q_{k}}$ respectively.

1. If $0<\mu<\frac{\sqrt{d}}{2}$, then $\frac{p}{q}$ is a convergent to $\rho$ or $\sigma$.
2. If $-\frac{\sqrt{d}}{2}<\mu<0$, then $\frac{p}{q}$ is a convergent to $\rho$ or $\sigma$ or has the form
$p_{m}-p_{m-1}, q_{m}-q_{m-1}$ or $P_{r}-P_{r-1}, Q_{r}-Q_{r-1}$
Proof
Assume that $\mathrm{f}(\mathrm{p}, \mathrm{q})=\mathrm{ap}^{2}+\mathrm{bpq}+\mathrm{cq}^{2}=\mu$, where $0<|\mu|<\frac{\sqrt{\mathrm{d}}}{2}$ and
$\operatorname{gcd}(p, q)=1$. By Pavone's argument and define $g(x, y)$ by
$g(x, y)=f\left(p_{m} x+p_{m-1} y, q_{m} x-q_{m-1} y\right)$
Then $g$ is Hermite reduced with roots
$\theta_{1}=\left[b_{1}, \ldots, b_{n}\right]$
$\theta_{2}=\left[0, b_{n}, \ldots, b_{1}\right]$
and with sequences $\left(S_{k}\right),\left(T_{k}\right)$ for $\theta_{1}$ and $\theta_{2}$
$\left(\begin{array}{ll}\mathrm{p}_{\mathrm{m}} & \mathrm{p}_{\mathrm{m}-1} \\ \mathrm{q}_{\mathrm{m}} & \mathrm{q}_{\mathrm{m}-1}\end{array}\right)\binom{\mathrm{S}_{\mathrm{k}}}{\mathrm{T}_{\mathrm{k}}}= \pm\binom{\mathrm{P}_{\mathrm{m}+\mathrm{k}}}{\mathrm{Q}_{\mathrm{m}+\mathrm{k}}}$
Moreover, there exists $\mathrm{i}, 1 \leq \mathrm{i} \leq 3$ such that
$\sigma=\left[c_{0}, \ldots, c_{r}, \overline{b_{n-1}}, \ldots, b_{1}, b_{n}, b_{n-1}, \ldots, b_{n-1+1}\right]$
$\left(\begin{array}{ll}\mathrm{p}_{\mathrm{m}} & \mathrm{p}_{\mathrm{m}-1} \\ \mathrm{q}_{\mathrm{m}} & \mathrm{q}_{\mathrm{m}-1}\end{array}\right)\binom{\mathrm{S}_{-\mathrm{k}}}{\mathrm{T}_{-\mathrm{k}}}= \pm\binom{\mathrm{P}_{\mathrm{r}+\mathrm{k}-(\mathrm{i}+1)}}{\mathrm{Q}_{\mathrm{r}+\mathrm{k}-(\mathrm{i}+1)}}, \mathrm{k} \geq \mathrm{i}$
Also $\mathrm{i}=3 \Rightarrow \mathrm{~b}_{\mathrm{n}-1}=1$ while $\mathrm{b}_{\mathrm{n}}=\mathrm{b}_{\mathrm{n}-1}=1 \Rightarrow \mathrm{i}=3$
Define integers $\alpha$ and $\beta$ by
$\mathrm{p}_{\mathrm{m}} \alpha+\mathrm{p}_{\mathrm{m}-1} \beta=\mathrm{p}, \mathrm{q}_{\mathrm{m}} \alpha+\mathrm{q}_{\mathrm{m}-1} \beta=\mathrm{q}$
Then $g(\alpha, \beta)=\mu$ and there exists an integer $k$ such that $(\alpha, \beta)= \pm\left(S_{k}, T_{k}\right)$. Hence
$\binom{\mathrm{p}}{\mathrm{q}}=\left(\begin{array}{ll}\mathrm{p}_{\mathrm{m}} & \mathrm{p}_{\mathrm{m}-1} \\ \mathrm{q}_{\mathrm{m}} & \mathrm{q}_{\mathrm{m}-1}\end{array}\right)\binom{\mathrm{S}_{\mathrm{k}}}{\mathrm{T}_{\mathrm{k}}}, \mathrm{k} \geq-1$
Let $i$ be the integer satisfying equation (5) and (6). If $i=1$ or 2 , then by equation (4) and (6)
$\binom{p}{q}= \pm\binom{ p_{h}}{q_{h}}$ or $\binom{P_{h}}{Q_{h}}$
for some $h$ and $\frac{q}{q}$ is a convergent to $\rho$ or $\sigma$. If $i=3$, then $\binom{S_{k}}{T_{k}}$ occurs in equation (4) or (6) for all $\mathrm{k} \neq-2$. Hence either p or q is a convergent to $\rho$ or $\sigma$ or

$$
\binom{\mathrm{p}}{\mathrm{q}}= \pm\left(\begin{array}{ll}
\mathrm{p}_{\mathrm{m}} & \mathrm{p}_{\mathrm{m}-1} \\
\mathrm{q}_{\mathrm{m}} & \mathrm{q}_{\mathrm{m}-1}
\end{array}\right)\binom{\mathrm{S}_{-2}}{\mathrm{~T}_{-2}}
$$

$$
\begin{aligned}
& \binom{p}{q}= \pm\left(\begin{array}{ll}
p_{m} & p_{m-1} \\
q_{m} & q_{m-1}
\end{array}\right)\binom{1}{-b_{n}} \\
& (p, q)= \pm\left(p_{m}-b_{n} p_{m-1}, q_{m}-b_{m} q_{m-1}\right)
\end{aligned}
$$

However we can interchange $\rho$ and $\sigma$ and deduce
$(\mathrm{p}, \mathrm{q})=\left(\mathrm{p}_{\mathrm{r}}-\mathrm{b}_{\mathrm{n}}-2 \mathrm{p}_{\mathrm{r}-1}, \mathrm{Q}_{\mathrm{r}}-\mathrm{b}_{\mathrm{n}}-2 \mathrm{Q}_{\mathrm{r}-1}\right)$
If $b_{n}=2$, we have $q_{m}-b_{n} q_{m-1}=q_{m}-q_{m-1}>0$
$(p, q)=\left(p_{m}-p_{m-1}, q_{m}-q_{m-1}\right)$. If $b_{n}>1$, then $b_{n-1}=1$ and $g\left(S_{-2}, T_{-2}\right)=\mu$, it follows $b_{n-2}=1$.
Hence $\mathrm{Q}_{\mathrm{r}}-\mathrm{b}_{\mathrm{n}}-2 \mathrm{Q}_{\mathrm{r}-1}=\mathrm{Q}_{\mathrm{r}}-\mathrm{Q}_{\mathrm{r}-1}>0$ and $(\mathrm{p}, \mathrm{q})=\left(\mathrm{P}_{\mathrm{r}}-\mathrm{P}_{\mathrm{r}-1}, \mathrm{Q}_{\mathrm{r}}-\mathrm{Q}_{\mathrm{r}-1}\right)$.

## 4. Discussion

## Solution of Quadratic Diophantine Equation

Quadratic Diophantine equation
$a x^{2}+b x y+c y^{2}=N$
can be transformed into Pell's equation $\mathrm{x}^{2}-\mathrm{dy}^{2}=\mathrm{N}$ by using linear transformations with integral coefficients. The problem of determining all the solutions of the equation (7) in integers $u$ and $v$, then reduces to the problem of finding all the integral solutions x and y of (7) which satisfy certain linear congruences [14]. The structure of the integer solutions of equation (7) given in Skolem [22]. The primitive solutions $x+y \sqrt{d}$ of the equation (7) fall into equivalence classes, with $x+y \sqrt{d}$ and $x_{0}+$ $y_{0} \sqrt{d}$ being equivalent if and only if
$2 a x+b y+y \sqrt{d}=\frac{(u+v \sqrt{d})}{2}\left(2 a x_{0}+b y_{0}+y_{0} \sqrt{d}\right)$
where $u^{2}-d v^{2}=4$. These in turn are equivalent to the equations
$\mathrm{x}=\frac{(\mathrm{u}-\mathrm{bv})}{2}\left(\mathrm{x}_{0}-\mathrm{cvy}_{0}\right), \quad \mathrm{y}=\mathrm{avx}_{0}+\frac{(\mathrm{u}+\mathrm{bv})}{2} \mathrm{y}_{0}$
The standard approach to solving the equation (7) is reduction of the quadratic form as in Mathews [9]. Then there exist integers $\alpha, \gamma$ such that $a \alpha^{2}+\mathrm{b} \alpha \gamma+\mathrm{c} \gamma^{2}=\mathrm{N}_{0}$ where $\operatorname{gcd}\left(\mathrm{N}_{0}, \mathrm{~N}\right)=1$. If $\alpha \delta-$ $\beta \gamma=1$. Then the uni-modular transformation $x=\alpha X+\beta Y, y=\gamma X+\delta Y$ converts the form $a x^{2}+$ bxy $+c y^{2}=N$ to $a_{0} X^{2}+b_{0} X Y+c_{0} Y^{2}=N_{0}$. The two forms represent the same integers and consequently we can assume, without loss of generality, that $\operatorname{gcd}(\mathrm{a}, \mathrm{N})=1$.
In 1770, Lagrange [20] gave an algorithm if the equation (7) is solvable in integers $x, y$ and in the case of solvability constructing solutions when $\operatorname{gcd}(a, b, c)=\operatorname{gcd}(a, N)=1$ and $d=b^{2}-4 a c>0$, is not a perfect square.
M. Pavone [18] solved the equation (7) if $\mathrm{N}=|\mu|$ where
$\mu=\min _{(x, y) \neq(0,0)}\left|a x^{2}+b x y+y^{2}=N\right|$
He had essentially solved the equation (7) in general, as Lagrange showed how to reduce the problem to the case $\mathrm{N}= \pm 1$. The continued fractions approach also has the attraction that it produces the solution ( $\mathrm{x}, \mathrm{y}$ ) with least positive y from each class, if $\operatorname{gcd}(\mathrm{a}, \mathrm{N})=1$.
Multiplying both sides of equation (7) by 4 a , then we have
$(a x+b y)^{2}-d y^{2}=4 a N$
where $d=b^{2}-4 a c$, assume that $d>0$, not perfect square, is a general Pell's equation. Let $\left(u_{n}, v_{n}\right)$ be the general solution to its Pell's resolving $u^{2}-d v^{2}=1$ and $(\alpha, \beta)$ be the fundamental solution of the class $K$ to the equation $X^{2}-d Y^{2}=4 a N$.

## Theorem

All integer solutions $\left(\mathrm{x}_{\mathrm{n}}, \mathrm{y}_{\mathrm{n}}\right)_{\mathrm{n} \geq 1}$ to equation $\mathrm{ax}^{2}+\mathrm{bxy}+\mathrm{cy}^{2}=\mathrm{N}$ are given by
$x_{n}=\frac{(a-b \beta) u_{n}-(b \alpha-d \beta) v_{n}}{2 a}, \quad y_{n}=\beta u_{n}+\alpha v_{n}$
where $\left(u_{n}, v_{n}\right)_{n \geq 1}$ is the solution to the Pell's resolving and $(\alpha, \beta)$ is the fundamental solution of the class K.

Proof
We have $(a x+b y)^{2}-d^{2}=4 a N$ where $d=b^{2}-4 a c$, assume that $d>0$, not perfect square. Put $X=2 a x+b y, Y=y, N_{1}=4 a N$,
we have general solution to
$\mathrm{X}^{2}-\mathrm{dY} \mathrm{Y}^{2}=\mathrm{N}_{1} \quad$ are
$\mathrm{X}_{\mathrm{n}}=\alpha \mathrm{u}_{\mathrm{n}}+\mathrm{d} \beta \mathrm{v}_{\mathrm{n}}, \quad \mathrm{y}_{\mathrm{n}}=\beta \mathrm{u}_{\mathrm{n}}+\alpha \mathrm{v}_{\mathrm{n}}$
So
$2 a x_{n}+b y_{n}=\alpha u_{n}+d \beta v_{n}$
$\Rightarrow \mathrm{x}_{\mathrm{n}}=\frac{(\mathrm{a}-\mathrm{b} \beta) \mathrm{u}_{\mathrm{n}}-(\mathrm{b} \alpha-\mathrm{d} \beta) \mathrm{v}_{\mathrm{n}}}{2 \mathrm{a}}, \quad \mathrm{y}_{\mathrm{n}}=\beta \mathrm{u}_{\mathrm{n}}+\alpha \mathrm{v}_{\mathrm{n}}$
Which is general solution to equation $(a x+b y)^{2}-d y^{2}=4 a N$.
Next, we want to show that $x_{n}$ is an integer. For this, it is enough to show that $2 a \mid(\alpha-b \beta)$ and
$2 a \mid(\alpha b-\beta d)$.
Indeed, we have
$(\alpha-\mathrm{b} \beta)=2 \mathrm{ax}$ and $\quad(\alpha b-\beta d)=\alpha \mathrm{b}-\beta\left(\mathrm{b}^{2}-4 \mathrm{ac}\right)$
$=(\alpha-b \beta) b+4 a c \beta$
$=2 \mathrm{axb}+4 \mathrm{ac} \beta$
$=2 \mathrm{a}(\mathrm{xb}+2 \mathrm{c} \beta)$

## 5. Conclusion

Diophantine equations are rich in variety. There is no universal method for finding all possible integer solutions for quadratic Diophantine equations. In this paper, we investigate positive integral solutions of the quadratic Diophantine equation $a x^{2}+b x y+c y^{2}=N$ which is transformed into Pell's equation by different methods and we try to find all positive integer solutions.

## References

[1] Arya, S.P. (1991). On the Brahmagupta-Bhaskara equation, Math.Ed. 8(1).
[2] Baltus, C. (1994). Continued fractions and the Pell equations, The work of Eulerand Lagrange, Comm. Anal. Theory Continued Fractions 3.
[3] Barbeau, E. J. (2003). Pells Equation, Springer, New York.
[4] Dickson, L. E. (1957). Introduction to the Theory of Numbers, Dover.
[5] Gbur, M. E. (1977). The Markov spectrum and minima of indefinite binary quadratic forms, Proc. Amer. Math. Soc. 63.
[6] HalterKoch, F. (2014). Principal ideals in quadratic orders, continued fractions and Diophantine equations, J. Comb. Number Theory 6.
[7] Hardy, G. H. and Wright, E. M. (1962). An Introduction to Theory of Numbers, Oxford University Press.
[8] Keskin, R. (2010). Solutions of some Quadratic Diophantine Equations, Computers and Mathematics with Applications, 60(8).
[9] Mathews, G. B. (1961). Theory of numbers, 2nd edition, Chelsea Publishing Co., NewYork.
[10] Matthews, K. R. (2002). The Diophantine equation $a x^{2}+b x y+c y^{2}=N, d=b^{2}-4 a c>0$,
J. Theor. Nombres Bordeaux 14.
[11] Matthews, K. R. and Robertson, J. P. (2017). Extending Theorems of Serret and Pavone, Journal of Integer Sequences, Vol. 20.
[12] Mordell, L. J. (1969). Diophantine Equations, Academic Press, London and New York.
[13] Mollin, R. A. (2001). Simple continued fraction solutions for Diophantine equations, Expo. Math. 19(1).
[14] Nagell, T. (1981). Introduction to Number Theory, Chelsea Publishing Company, New York.
[15] Niven, I., Zuckerman, H.S., Montgomery, H.L. (1991). An introduction to the Number Theory, John Wiley and Sons, Inc., fifth edition, New York.
[16] Olds, C.D. (1963). Continued Fractions, New York: Random House Inc.
[17] Owings, Jr., J.C. (1970). An elementary approach to Diophantine equations of the second degree, Duke Math. J. 37.
[18] Pavone, M. (1986). A Remark on a Theorem of Serret, J. Number Theory 23.
[19] Robertson, J. P. Matthews' Method for Solving $a x^{2}+b x y+c y^{2}=N$,
http://www.jpr2718.org/mathin.pdf.
[20] Serret, J. A. (1877). Oeuvres de Lagrange, I-XIV, Gauthiers-Villars, Paris.
[21] Serret, J. A. (1885). Cours d'Algebre superieurw, Tome 1, Gauthier-Villars.
[22] Skolem, T. (1950). Diophantische Gleichungen, Chelsea, NY.

Citation: Bal Bahadur Tamang \& Ajay Singh, Some Aspects of Quadratic Diophantine Equations, International Journal of Scientific and Innovative Mathematical Research (IJSIMR), vol. 8, no. 5, pp. 1-8, 2020. Available : DOI: https://doi.org/10.20431/2347-3142.0805001

Copyright: © 2020 Authors. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

