Journal of Computer and Mathematical Sciences, *Vol.12(6),8-21 June 2021* *ISSN 0976-5727 (Print)*
(An International Research Journal), *www.compmath-journal.org* *ISSN 2319-8133 (Online)*

Solving Pell's Equation via Lattice Reduction

P. Anuradha Kameswari* and S B T Sundari Katakam

Department of Mathematics,
Andhra University,
Visakhapatnam - 530003, Andhra Pradesh, INDIA.
email:panuradhakameswari@yahoo.in, sribalakatakam@gmail.com.

(Received on: May 28, 2021)

ABSTRACT

In this paper, we adapted rational approximation of $\alpha = \sqrt{N}$ for N a non square positive integer via lattice reduction of a quadratic form $q(y,x) = M(\bar{\alpha}y - x)^2 + \frac{1}{M}y^2$ for $\overline{\alpha} = \overline{\sqrt{N}}$, decimal approximation of $\sqrt{N}$ to the precision $\frac{1}{M}$, we obtained the convergent of $\sqrt{N}$ that is a solution of Pell's equation $x^2 - Ny^2 = 1$ as a short vector of the above quadratic form for an appropriate M.

Keywords: Pell's equation, convergent, Lattice reduction, LLL algorithm, quadratic form.

1. INTRODUCTION

Equation of the form $x^2 - Ny^2 = 1$, for N a positive integer is called Pell's equation. Pell's equation always has a solution (x, y) in integers. If N is a perfect square then Pell's equation has only the trivial solution (1,0). If N is not a perfect square, there are various ways to obtain the solutions of Pell's equations. Mathematicians like Brahmagupta, Bhaskara, Wallis, Fermat, Lagrange, Euler, etc., have all contributed to the study of solutions of the Pell's equations and existence of infinitely many solutions. Lord Brouncker gave a method for solving Pell's equation by developing $\sqrt{N}$ into a continued fraction, as any solution (x, y) of a Pell's equation corresponds to the convergent $\frac{x}{y}$ of $\sqrt{N}$. A positive solution (x_0, y_0) of Pell's equation minimizing x is called a minimal solution and if (x_0, y_0) is a minimal solution, then for all $n \geq 0$, (x_n, y_n) given as $x_n + \sqrt{N}y_n = (x_0 + \sqrt{N}y_0)^n$ are all convergents of $\sqrt{N}$ and are positive solutions of Pell's equation. Thus, with a minimal solution we can generate infinitely many solutions of Pell's equation and hence the study of obtaining the minimal solution plays a vital role in the study of solutions of Pell's equation. In this paper we obtained the minimal solution of Pell's equation with Rational approximation via Lattice reduction. The solution that is a convergent of $\sqrt{N}$ is obtained as a short vector of the quadratic form $q(y,x) = M(\bar{\alpha}y - x)^2 + \frac{1}{M}y^2$ for $\alpha = \sqrt{N}$, for some appropriate M.

In the following, in section 2 we first describe the process of obtaining solutions of Pell's equation by continued fraction and then in section 3 we describe the process of obtaining the minimal solution as a short vector by Lattice Reduction and an algorithm for computing the solution as a short vector is given, also a graphical review on the advantage of obtaining the solution as a short vector is given.

2. SOLUTIONS OF PELL EQUATION BY CONTINUED FRACTIONS

Definition 1 An infinite continued fraction denoted as $[a_0; a_1, \cdots, a_m, \cdots, a_{m+r}, \cdots]$ is called periodic if it contains a block of partial denominators $b_1, b_2, \cdots, b_n$ which repeats indefinitely. Then a periodic continued fraction is given as

$$[a_0; a_1, \cdots, a_m, b_1, \cdots, b_n, b_1 \cdots, b_n, \cdots]$$

and can be written in the form

$$[a_0; a_1, \cdots, a_m, \overline{b_1, \cdots, b_n}]$$

where the bar over $b_1, \cdots, b_n$ indicates that this block of integers repeats over and over. We say that $b_1, \cdots, b_n$ is the period of the expansion and n is the length of the period.

Example 1 $\sqrt{2} = 1 + \frac{1}{2+\frac{1}{2+\frac{1}{2+\ddots}}}$

$$= [1; 2,2,2, \cdots]$$
$$= [1; \overline{2}]$$

Definition 2 An infinite continued fraction is said to be purely periodic if it is periodic from the beginning itself.

Example 2 $\sqrt{6} + 2 = 4 + \frac{1}{2+\frac{1}{4+\frac{1}{2+\ddots}}}$

$$= [4; 2,4,2, \cdots]$$
$$= [\overline{4; 2}]$$

Definition 3 A quadratic irrational number α is an irrational root of some quadratic equation $ax^2 + bx + c = 0$ where, a, b, c are integers and

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \frac{P \pm \sqrt{D}}{Q},$$

where P, Q are integers, D is a positive integer which is not perfect square. Thus, $\alpha = \frac{P+\sqrt{D}}{Q}$, and the conjugate α' of α being the other root of the quadraic equation is given by $\frac{P-\sqrt{D}}{Q}$.

Theorem 1 (Lagrange's theorem): Any quadratic irrational number has a continued fraction which is periodic after a certain stage.

Definition 4 A quadratic irrational number α is reduced if $\alpha > 1$ and if the conjugate of α, denoted by α' satisfies $-1 < \alpha' < 0$.

Theorem 2 The continued fraction for a reduced quadratic rational α is purely periodic.

Remark 1 If N is a non-square positive integer and q_0 is the integral part of $\sqrt{N}$, then the continued fraction of $\sqrt{N} + q_0$ is purely periodic and the continued fractions of $\sqrt{N} + q_0$ and $\sqrt{N}$ are given as in (1) and (2) in the following:

$$\sqrt{N} + q_0 = 2q_0 + \cfrac{1}{q_1 + \cfrac{1}{\ddots + \cfrac{1}{q_n + \cfrac{1}{2q_0 + \cfrac{1}{\ddots}}}}} \tag{1}$$

$$\sqrt{N} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\ddots + \cfrac{1}{q_n + \cfrac{1}{2q_0 + \cfrac{1}{q_1 + \cfrac{1}{\ddots}}}}}} \tag{2}$$

Thus, $\sqrt{N} = [q_0; \overline{q_1, \cdots, q_n, 2q_0}]$, with $q_n = q_1, q_{n-1} = q_2, \dots ..$ note, the period begins immediately after the first term q_0, and consists of a symmetrical part $q_1, q_2, \dots, q_2, q_1$, followed by the number $2q_0$.

Definition 5 The positive solution (x_0, y_0) of Pell's equation $x^2 - Ny^2 = 1$ minimizing x is called the minimal solution, smallest solution or fundamental solution.

Theorem 3 Any solution (x, y) of Pell's equation $x^2 - Ny^2 = 1$ corresponds to the convergent $\frac{x}{y}$ of $\sqrt{N}$ and $|\sqrt{N} - \frac{x}{y}| < \frac{1}{2y^2}$. [17].

Theorem 4 [17] Let l be the length of period of the continued fraction of $\sqrt{N}$ and $\frac{A_i}{B_i}$ be any $i^{t□}$ convergent of $\sqrt{N}$ then the minimal solution to Pell's equation is :

$$(x_0, y_0) = \begin{cases} (A_{l-1}, B_{l-1}) & \text{if } l \text{ is even} \\ (A_{2l-1}, B_{2l-1}) & \text{if } l \text{ is odd.} \end{cases}$$

Remark 2 If (x_0, y_0) is the minimal solution of $x^2 - Ny^2 = 1$, then the general solution (x, y) is given by $x + y\sqrt{N} = \pm(x_0 + y_0\sqrt{N})^{\pm r}$, where $r = 0,1,2,3 \cdots$.

As any general solution (x, y) of the Pell's equation can be obtained from the minimal solution by direct calculation without developing further continued fractions, the study of the search of convergent $\frac{A_n}{B_n}$ leading to the minimal solution plays a vital role in the study of solution of Pell equation. In section 3, in the following we show that this convergent $\frac{A_n}{B_n}$ can be obtained as a short vector (B_n, A_n), i.e., the search now confined to list of short vectors.

3. SOLUTION OF PELL EQUATION WITH LATTICE REDUCTION AS A SHORT VECTOR

Definition 6 A Lattice L is a discrete additive subgroup of $\mathbf{R}^m$, that is L is the Z −span of a linearly independent subset of $\mathbf{R}^m$:

$$L = \mathrm{Z}b_1 + Zb_2 + \cdots + Zb_n$$

with the quadratic form $q(x) =< x, x >$, for $x \in L$. The vectors $b_1, b_2, \dots, b_n$ are a basis for L, and $A = [< b_i, b_j >]_{1 \le i,\mathrm{j} \le n}$ is the corresponding Gram matrix also note $q(x) = x^T Ax$.

Definition 7 The short vector in a lattice L is a nonzero vector $v \in L$ that minimizes the Euclidean norm $||v||$. The problem of finding the vector $v \in L$ that minimizes $||v||$ is called the short vector problem denoted as SVP.

Definition 8 Let $B =< b_1, b_2, \dots, b_n >$ be a basis for a lattice L and let $\mathbf{B}^* =< b_1^*, b_2^*, \dots, b_n^* >$ be the associated Gram - Schmidt orthogonal basis. The basis B is said to be LLL reduced if it satisfies the following two conditions:

1. $|\mu_{i,\mathrm{j}}| = \frac{|b_i \cdot b_j^*|}{||b_j^*||^2} \le \frac{1}{2}$ for all $1 \le i < \mathrm{j} \le n$.
2. $||b_i^*||^2 \ge (\frac{3}{4} - \mu_{i,i-1}^2)||b_{i-1}^*||^2$ for all $1 < i \le n$.

Theorem 5 Let L be a lattice of dimension n. Any LLL reduced basis $< b_1^{'}, b_2^{'}, \dots, b_n^{'} >$ for L has the following two properties:

1. $\prod_{i=1}^{n} ||\mathrm{b}_\mathrm{i}'|| \le 2^{\frac{n(n-1)}{4}} \det \mathrm{L}$.
2. $||\mathrm{b}_\mathrm{j}'|| \le 2^{(\mathrm{i}-1)/2}||b_i^*||$ for all $1 \le j \le i \le n$.

Remark 3 An algorithm that returns an LLL reduced basis called LLL algorithm comes close to solve SVP in small dimensions, as the initial vector in an LLL reduced basis satisfies $||\mathrm{b}_1'|| \le 2^{n(n-1)/4}|\mathrm{det}L|^{1/n}$.

Also, note for any short vector $(x_1, x_2, \ldots, x_n)$ we have $q(x_1, \ldots, x_n) \leq 2^{\frac{n-1}{2}}$ det$q^{\frac{1}{n}}$ [13].
Now to solve Pell equation via Lattice reduction we first show in the following theorem that any short vector (y, x) of a quadratic form
$q(\mathrm{y}, x) = M(\bar{\alpha}y - x)^2 + \frac{1}{M}y^2$ for $M = 10^s$, is such that $\frac{x}{y}$ is a rational approximation of α.

Theorem 6 If α is a real number then for $M = 10^s$, for some $s > 0$, integer with $\bar{\alpha}$ a decimal approximation of α to precision $\frac{1}{M}$, any short vector (y, x) of the quadratic form $q(y, x) = M(\bar{\alpha}y - x)^2 + \frac{1}{M}y^2$ is such that $\frac{x}{y}$ is a rational approximation of α.
Proof. For a given α choose M with $\bar{\alpha}$, a decimal approximation to $\frac{1}{M}$ and the quadratic form $q(y, x) = M(\bar{\alpha}y - x)^2 + \frac{1}{M}y^2$. Now, we obtain the short vector (y, x) by reducing the lattice Z^2 equipped with quadratic form,

$$q(y, x) = M(\bar{\alpha}y - x)^2 + \frac{1}{M}y^2$$

The 2-dimensional Gram-matrix associated with the quadratic form is given by a symmetric positive definite matrix,

$$A = \begin{bmatrix} \bar{\alpha}^2 M + \frac{1}{M} & -\bar{\alpha}M \\ -\bar{\alpha}M & M \end{bmatrix}$$

whose determinant is 1, and hence it corresponds to a lattice of determinant 1 .
The underlying lattice in the Euclidean space R^2 is given by the matrix B,

$$B = \begin{bmatrix} \frac{1}{\sqrt{M}} & 0 \\ \bar{\alpha}\sqrt{M} & -\sqrt{M} \end{bmatrix}$$

whose columns forms a basis for the lattice. Let $b_{i'}'s$ be the rows of B^T. Applying LLL algorithm to B^T, the resultant of LLL is then a reduced basis B' of the same lattice. As B and B'^T are the matrices whose columns represent basis of the same lattice, B and B' are related by integer unimodular transformation matrix, U as $BU = B'^T$. Therefore, the matrix U, is obtained by $U = B^{-1}B'^T$,

$$U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

the vector(a, c) short vector (y, x). This short vector (y, x) is such that $\frac{x}{y}$ is a rational approximation of α.

By LLL for any short vector $(x_1, x_2, \ldots, x_n)$ we have $q(x_1, \ldots, x_n) \leq 2^{\frac{n-1}{2}}\ \det q^{\frac{1}{n}}$, Thus, we have for the 2-dimensional lattice L above $q(y, x) \leq \sqrt{2}$.

Therefore, we have

$$q(y,x) = M(\bar{\alpha}y - x)^2 + \frac{1}{M}y^2 \leq \sqrt{2}$$
$$\Longrightarrow\ M(\bar{\alpha}y - x)^2 \leq \sqrt{2}\ \text{ and }\ \frac{1}{M}y^2 \leq \sqrt{2}$$
$$\Longrightarrow (\bar{\alpha}y - x)^2 \leq \frac{\sqrt{2}}{M}\ \text{ and }\ y^2 \leq \sqrt{2}M$$
$$\Longrightarrow |\bar{\alpha}y - x|^2 \leq \frac{\sqrt{2}}{M}\ \text{ and }\ |y|^2 \leq \sqrt{2}M$$

Now, as $\bar{\alpha}$ is a decimal approximation of α to precision $\frac{1}{M}$, we have $|\alpha - \bar{\alpha}| \leq \frac{1}{M}$ and using the inequalities above, we get:

$$\begin{aligned} |\alpha y - x| &= |\alpha y - \bar{\alpha}y + \bar{\alpha}y - x| \\ &\leq |\alpha y - \bar{\alpha}y| + |\bar{\alpha}y - x| \\ &= |\ y(\alpha - \bar{\alpha})| + |\bar{\alpha}y - x| \\ &= |\ y||(\alpha - \bar{\alpha})| + |\bar{\alpha}y - x| \end{aligned}$$
$$\leq 2^{\frac{1}{4}}\sqrt{M}\,\frac{1}{M} + \frac{2^{\frac{1}{4}}}{\sqrt{M}}$$
$$= 2 \cdot 2^{\frac{1}{4}} \cdot \frac{1}{\sqrt{M}}$$
$$= 2 \cdot 2^{\frac{1}{4}} \cdot \frac{1}{\sqrt{M}}$$
$$= 2^{\frac{5}{4}} \cdot \frac{1}{\sqrt{M}}$$

which implies, $|\alpha - \frac{x}{y}| = |\frac{\alpha y - x}{y}| \leq \frac{2^{\frac{5}{4}}}{\sqrt{M}y} \leq \frac{2^{\frac{3}{2}}}{y^2} = \frac{1}{ky^2}$, for $k = \frac{1}{2^{\frac{3}{2}}}\cdot$ Therefore, as for all $k < \sqrt{5}$ by [7] we have $\frac{x}{y}$ is a rational approximation of α.

Now to solve Pell equation $x^2 - Ny^2 = 1$ we search the convergents $\frac{A_n}{B_n}$ in the class of convergents of $\sqrt{N}$ that satisfies the equation $x^2 - Ny^2 = 1$. In the following theorem, we prove that the convergents $\frac{A_n}{B_n}$ as above may be obtained via lattice reduction as a short vector (B_n, A_n) of quadratic form $q(y, x) = M(\bar{\alpha}y - x)^2 + \frac{1}{M}y^2$ for $\alpha = \sqrt{N}$.

Theorem 7 Any solution (x, y) of Pell's equation can be obtained as short vector (y, x) of a lattice $\mathbf{Z}^2$ equipped with a quadratic form $q(y, x) = M\left(\sqrt{N}y - x\right)^2 + \frac{1}{M}y^2$ for an appropriate M.

Proof. First note for each choice of $M = 10^l$ for some l, and $\overline{\sqrt{N}}$ decimal approximation of $\sqrt{N}$ to the precision $\frac{1}{M}$, we reduce the lattice $\mathbf{Z}^2$ with a quadratic form $q(y, x)$ in the variables y, x given as

$$q(y,x) = M\left(\sqrt{N}y - x\right)^2 + \frac{1}{M}y^2$$

and the 2-dimensional Gram-matrix for the above is given as

$$A = \begin{bmatrix} \sqrt{\mathrm{N}}^2 M + \frac{1}{M} & -\sqrt{N}M \\ & \\ -\sqrt{N}M & M \\ & \end{bmatrix}.$$

and note the corresponding lattice in R^2 is given by the basis as columns of matrix B given as

$$B = \begin{bmatrix} \frac{1}{\sqrt{M}} & 0 \\ & \\ \sqrt{N}\sqrt{M} & -\sqrt{M} \\ & \end{bmatrix}$$

which may be deduced by the results in *Lattices and Quadratic Forms* of [5]. Now applying LLL algorithm to B^T, we get reduced basis matrix B' of the same lattice. As B and B'^T are the matrices whose columns represent basis of the same lattice, B and B'^T are related by integer unimodular transformation matrix, U as $BU = B'^T$. Therefore, the matrix U, is obtained by $U = B^{-1}B'^T$,

$$U = \begin{bmatrix} \mathrm{a} & \mathrm{b} \\ \mathrm{c} & \mathrm{d} \end{bmatrix}$$

with (a, c) as short vector obtained for the choice of $M = 10^l$. Also, note as any short vector (y, x) of quadratic form is an approximation of $\sqrt{N}$ [Theorem 6], now, we find the necessary condition for an approximation of $\sqrt{N}$ to be a short vector for any (v, u) such that $\frac{u}{v}$ is an approximation of $\sqrt{N}$, we have

$$\begin{aligned} q(v,u) &= M(\sqrt{\mathrm{N}}v - u)^2 + \frac{1}{M}v^2 \\ &= Mv^2(\sqrt{\mathrm{N}} - \frac{u}{v})^2 + \frac{1}{M}v^2 \\ &= O(\frac{M}{v^2}) + O(\frac{v^2}{M}) + O(1) \end{aligned}$$

Therefore, (v, u) is a short vector only for $q(v, u) = O(1)$ and the above holds for an $M \ni M \approx v^2$, and note of all approximations (v, u) with $M \approx v^2$, note short vector is the vector (v, u) with minimal $q(v, u)$. Now for $q(v, u) = M(\sqrt{\mathrm{N}}v - u)^2 + \frac{1}{M}v^2$ note any solution (x, y) of the Pell's equation $x^2 - Ny^2 = 1$ is $\ni \frac{x}{y}$ is a convergent of $\sqrt{N}$ with $|\sqrt{N} - \frac{x}{y}| \leq \frac{1}{2y^2}$ and therefore for $M \approx y^2$, we have

$$q(y,x) = \min_{(v,u)}\{q(v,u): \frac{u}{v}\ \text{convergentof}\sqrt{N}\ \text{with}\ v^2 \approx y^2 \approx M,\}$$

$$\Rightarrow (y,x)\text{is the short vector of}\ q(y,x)\text{for}\ M \approx y^2.$$

Note 1 The search of the convergent $\frac{A_n}{B_n}$ leading to solution of the Pell equation may be obtained form the class of short vectors (B_n, A_n) for $q(y,x) = M\left(\sqrt{N}y - x\right)^2 + \frac{1}{M}y^2$ for an appropriate choice of M. In the following theorem it is proved that such M is possible.

Theorem 8 Let (x, y) be a minimal solution of the Pell's equation $x^2 - Ny^2 = 1$ then (y, x) is a short vector of the quadratic form,

$$q(y,x) = M\left(\sqrt{N}y - x\right)^2 + \frac{1}{M}y^2,$$

for M such that $M = 10^s$ for some s with $1 \leq s < 2[N^{\frac{1}{2}}(\log(4N) + 2)]$.

Proof. Let (x, y) be minimal solution of $x^2 - Ny^2 = 1$, then by Theorem 3, $(x, y) = (A_n, B_n)$ for some convergent $\frac{A_n}{B_n}$ of $\sqrt{N}$ and by above theorem the (B_n, A_n) is a short vector for he quadratic form,

$$q(y,x) = M\left(\sqrt{N}y - x\right)^2 + \frac{1}{M}y^2$$

for $M_l = 10^l$ for some appropriate l, such that $B_n \approx \sqrt{M_l}$. Now, note as (A_n, B_n) is a minimal solution and if $d(B_n)$ is the number of digits in B_n, as in[12] we have:

$$\log B_n = \ d(B_n) < N^{\frac{1}{2}}(\log(4N) + 2)$$

$$\Rightarrow B_n < 10^{N^{\frac{1}{2}}(\log(4N)+2)}$$

$$\Rightarrow l < 2[N^{\frac{1}{2}}(\log(4N) + 2)] \qquad \text{for } M_l \approx B_n^2$$

Now for, $r = 2[N^{\frac{1}{2}}(\log(4N) + 2)]$, varying s in the range $1 \leq s < r$ and taking $M_s = 10^s$ if we compute short vector of the quadratic form

$$q(y,x) = M\left(\sqrt{N}y - x\right)^2 + \frac{1}{M}y^2,$$

then as s reaches l, we have $M_s = M_l \approx B_l^2$ and the coresponding short vector of the quadratic form with $M = M_s$ is (B_n, A_n) the minimal solution of the Pell's equation $x^2 - Ny^2 = 1$.

3.1 Algorithm:

An algorithm for finding the smallest solution of the Pell's equation $x^2 - Ny^2 = 1$ via Lattice reduction is given in the following:

Algorithm:
Step 1: Start

Step 2: Input N.

Step 3: Compute $\sqrt{N}$ to r decimals, where

$r = 2[N^{\frac{1}{2}}(\log(4N) + 2)]$.

Step 4: Set $i = 1$.

Step 5: Set $M = 10^i$, $\overline{\sqrt{N}} = \sqrt{N}$ corrected to i decimal places.

Step 6: Set

$$B = \begin{bmatrix} \frac{1}{\sqrt{M}} & 0 \\ \overline{\sqrt{N}} & -\sqrt{M} \end{bmatrix}$$

Apply LLL algorithm to B^T and then obtain unimodular transformation matrix $B = B^{-1}(B')^T$, where B' is the resultant obtained using LLL

$$U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Set $A_i = |\mathrm{c}|$,$B_i = |a|$

Step 7: If $A_i^2 - NB_i^2 = \pm 1$ then stop, otherwise $i = \mathrm{i} + 1$ and go to step 5.

Step 8: If (A_i, B_i) is a solution of $x^2 - Ny^2 = 1$, then $(x_0, y_0) = (A_i, B_i)$ or if (A_i, B_i) is a solution of $x^2 - Ny^2 = -1$, then we have (x_0, y_0) using the relation $x_0 + y_0\sqrt{N} = (A_i + B_i\sqrt{N})^2$.

Example 3 For $N = 46$, by varying s from 1 to r, for $r = 2[N^{\frac{1}{2}}(\log(4N) + 2)]$ i.e., $r = 62$, we have obtained the smallest solution (x_0, y_0) of the equation $x^2 - 46y^2 = 1$ for s= 8 as $(x_0, y_0) = (24335{,}3588)$. The convergent deduced as a short vector for each $M = 10^s$ and the corresponding unimodular matrix obtained by LLL algorithm for Lattice Reduction of the quadratic form $q(y, x) = M(\overline{\alpha}y - x)^2 + \frac{1}{M}y^2$, $\alpha = \sqrt{N}$ for $M = 10^s$ and $\bar{\alpha} = \overline{\sqrt{N}}$ is the decimal approximation of $\sqrt{N}$ to the precision $\frac{1}{M}$, is depicted in the Table 1.

Table 1: The smallest solution (x_0, y_0) of the Pell equation $x^2 - 46y^2 = 1$ obtained as short vector for $M = 10^8$.

$1 \leq s \leq 62$, $M = 10^s$	$\sqrt{N}$	Unimodular matrix using LLL, $U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$	$\frac{A_i}{B_i} = \frac{\lvert c\rvert}{\lvert a\rvert}$	$A_i^2 - NB_i^2$	(x_0, y_0)/ Set M to iterate
$M = 10^1$	6.8	$U = \begin{bmatrix} 1 & -4 \\ 7 & -27 \end{bmatrix}$	$\frac{7}{1}$	3	Set $M = 10^2$
$M = 10^2$	6.78	$U = \begin{bmatrix} -9 & -5 \\ -61 & -34 \end{bmatrix}$	$\frac{61}{9}$	-5	Set $M = 10^3$
$M = 10^3$	6.782	$U = \begin{bmatrix} -23 & -9 \\ -156 & -61 \end{bmatrix}$	$\frac{156}{23}$	2	Set $M = 10^4$
$M = 10^4$	6.7823	$U = \begin{bmatrix} -23 & -124 \\ -156 & -841 \end{bmatrix}$	$\frac{156}{23}$	2	Set $M = 10^5$
$M = 10^5$	6.78233	$U = \begin{bmatrix} 147 & -317 \\ 997 & -2150 \end{bmatrix}$	$\frac{997}{147}$	-5	Set $M = 10^6$
$M = 10^6$	6.782330	$U = \begin{bmatrix} 781 & -464 \\ 5297 & -3147 \end{bmatrix}$	$\frac{5297}{781}$	3	Set $M = 10^7$
$M = 10^7$	6.7823300	$U = \begin{bmatrix} 781 & -3588 \\ 5297 & -24335 \end{bmatrix}$	$\frac{5297}{781}$	3	Set $M = 10^8$
$M = 10^8$	6.78232998	$U = \begin{bmatrix} -3588 & -13571 \\ -24335 & -92043 \end{bmatrix}$	$\frac{24335}{3588}$	1	$(x_0, y_0) = (24335{,}3588)$

Using the algorithm above, the unimodular matrix obtaining LLL algorithm by Lattice Reduction fo the quadratic form $q(y, x) = M(\overline{\alpha}y - x)^2 + \frac{1}{M}y^2$, $\alpha = \sqrt{N}$ for the appropriate M giving the smallest solution (x_0, y_0) of the equation $x^2 - Ny^2 = \pm 1$ for $N = 2$ to 30 are depicted in the following Table 2:

Table 2: The list of Unimodular matrices and appropriate $M's$ leading to the smallest solution (x_0, y_0) of the equations $x^2 - Ny^2 = \pm 1$, for $N = 2$ to 30.

N	M	$\sqrt{N}$	Unimodular matrix using LLL, U	$\frac{x}{y} = \frac{\lvert c\rvert}{\lvert a\rvert}$	$x^2 - Ny^2$	(x_0, y_0)
2	$M = 10^1$	1.4	$U = \begin{bmatrix} -2 & 3 \\ -3 & 4 \end{bmatrix}$	$\frac{3}{2}$	1	(3,2)
3	$M = 10^1$	1.7	$U = \begin{bmatrix} -1 & 3 \\ -2 & 5 \end{bmatrix}$	$\frac{2}{1}$	1	(2,1)
5	$M = 10^1$	2.2	$U = \begin{bmatrix} 1 & 4 \\ 2 & 9 \end{bmatrix}$	$\frac{2}{1}$	-1	(2,1)
6	$M = 10^1$	2.4	$U = \begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix}$	$\frac{5}{2}$	1	(5,2)
7	$M = 10^2$	2.65	$U = \begin{bmatrix} -3 & -14 \\ -8 & -37 \end{bmatrix}$	$\frac{8}{3}$	1	(8,3)
8	$M = 10^1$	2.8	$U = \begin{bmatrix} 1 & -4 \\ 3 & -11 \end{bmatrix}$	$\frac{3}{1}$	1	(3,1)
10	$M = 10^1$	3.1	$U = \begin{bmatrix} 1 & 5 \\ 3 & 16 \end{bmatrix}$	$\frac{3}{1}$	-1	(3,1)
11	$M = 10^2$	3.32	$U = \begin{bmatrix} 3 & 16 \\ 10 & 53 \end{bmatrix}$	$\frac{10}{3}$	1	(10,3)

12	$M = 10^2$	3.5	$U = \begin{bmatrix} -2 & 1 \\ -7 & 4 \end{bmatrix}$	$\frac{7}{2}$	1	(7,2)
13	$M = 10^2$	3.61	$U = \begin{bmatrix} -5 & -8 \\ -18 & -29 \end{bmatrix}$	$\frac{18}{5}$	-1	(18,5)
14	$M = 10^2$	3.74	$U = \begin{bmatrix} -4 & -11 \\ -15 & -41 \end{bmatrix}$	$\frac{15}{4}$	1	(15,4)
15	$M = 10^1$	3.9	$U = \begin{bmatrix} 1 & -5 \\ 4 & -19 \end{bmatrix}$	$\frac{4}{1}$	1	(4,1)
17	$M = 10^1$	3.32	$U = \begin{bmatrix} 1 & 5 \\ 4 & 21 \end{bmatrix}$	$\frac{4}{1}$	-1	(4,1)
18	$M = 10^1$	3.32	$U = \begin{bmatrix} 4 & 13 \\ 17 & 55 \end{bmatrix}$	$\frac{17}{4}$	1	(17,4)
19	$M = 10^4$	4.3589	$U = \begin{bmatrix} -39 & -131 \\ -170 & -571 \end{bmatrix}$	$\frac{170}{39}$	1	(170,39)
20	$M = 10^2$	4.47	$U = \begin{bmatrix} 2 & 15 \\ 9 & 67 \end{bmatrix}$	$\frac{9}{2}$	1	(9,2)
21	$M = 10^3$	4.582	$U = \begin{bmatrix} 12 & 43 \\ 55 & 197 \end{bmatrix}$	$\frac{55}{12}$	1	(55,12)
22	$M = 10^4$	4.6904	$U = \begin{bmatrix} -42 & -113 \\ -197 & -530 \end{bmatrix}$	$\frac{197}{42}$	1	(197,42)
23	$M = 10^2$	4.80	$U = \begin{bmatrix} -5 & 1 \\ -24 & 5 \end{bmatrix}$	$\frac{24}{5}$	1	(24,5)
24	$M = 10^1$	4.9	$U = \begin{bmatrix} 1 & -5 \\ 5 & -24 \end{bmatrix}$	$\frac{5}{1}$	1	(5,1)
26	$M = 10^1$	5.1	$U = \begin{bmatrix} 1 & 5 \\ 5 & 26 \end{bmatrix}$	$\frac{5}{1}$	-1	(5,1)
27	$M = 10^2$	5.20	$U = \begin{bmatrix} 5 & 1 \\ 26 & 5 \end{bmatrix}$	$\frac{26}{5}$	1	(26,5)
28	$M = 10^3$	5.292	$U = \begin{bmatrix} 24 & -17 \\ 127 & -90 \end{bmatrix}$	$\frac{127}{24}$	1	(127,24)
29	$M = 10^2$	5.385	$U = \begin{bmatrix} 13 & -31 \\ 70 & -167 \end{bmatrix}$	$\frac{70}{13}$	-1	(70,13)
30	$M = 10^1$	5.5	$U = \begin{bmatrix} -2 & 1 \\ 11 & 6 \end{bmatrix}$	$\frac{2}{11}$	1	(2,11)

3.2 A graphical review on solutions via Lattice reduction:

An infinite list of the solutions of a given Pell equation may be obtained from the minimal solution and the minimal solution is obtained from the list of convergents of $\sqrt{N}$. Now this search for minimal solution in the list of convergents may now be confined to the list of short vectors of the quadratic form $q(y,x) = M(\overline{\alpha}y - x)^2 + \frac{1}{M}y^2,\ \alpha = \sqrt{N}$, by varying M in the range 10^1 to 10^s, for $s \leq r = 2[N^{\frac{1}{2}}(\log(4\text{N}) + 2)]$. Note the required solution always arrives as a short vector for an appropriate M, and the class of short vectors leading to solution of $x^2 - Ny^2 = 1$ is the subclass of continued fraction of $\sqrt{N}$ as for a given N the set of all short vectors (y,x) of quadratic form $q(y,x) = M(\overline{\alpha}y - x)^2 + \frac{1}{M}y^2$, $\alpha = \sqrt{N}$ for some M is a subset of set of all (y,x) such that $\frac{x}{y}$ is a convergent of $\sqrt{N}$. This is depicted in the following graphs with respect to logarithmic scale taken on both the axes to show the distribution of the points clearly for $N = 46$, by plotting the convergent $\frac{A_n}{B_n}$ as a point (B_n, A_n) in a given range in a plane. Note all points (B_n, A_n) lie close to the line $y = \sqrt{46}x$ as $\frac{A_n}{B_n}$ are approximations to $\sqrt{46}$, and note if the points (B_n, A_n) that are short vectors of the quadratic form $q(y,x) = M(\overline{\alpha}y - x)^2 + \frac{1}{M}y^2$, $\alpha = \sqrt{N}$ for some M are represented by "∘" and the points (B_n, A_n) for which $\frac{A_n}{B_n}$ are only convergents and not short vectors for M of the form $M = 10^l$ are represented by "∘", figure 1 represents the convergents that are short vectors reaching to minimal solution for $M = 10^8$. Figure 2 represents the list of 11 convergents of which only 6 convergents are short vectors leading to minimal solution. In this search of minimal solution of Pell equation for N= 46 from the list of 11 convergents only the 6 convergents represented by "∘" may be considered and the convergents corresponding the points represented by "∘" will be avoided in the search of solutions of $x^2 - Ny^2 = 1$ via lattice reduction. Thus, the search of list of convergents is reduced in approximation via Lattice reduction and hence adapting rational approximation via Lattice reduction is preferable.

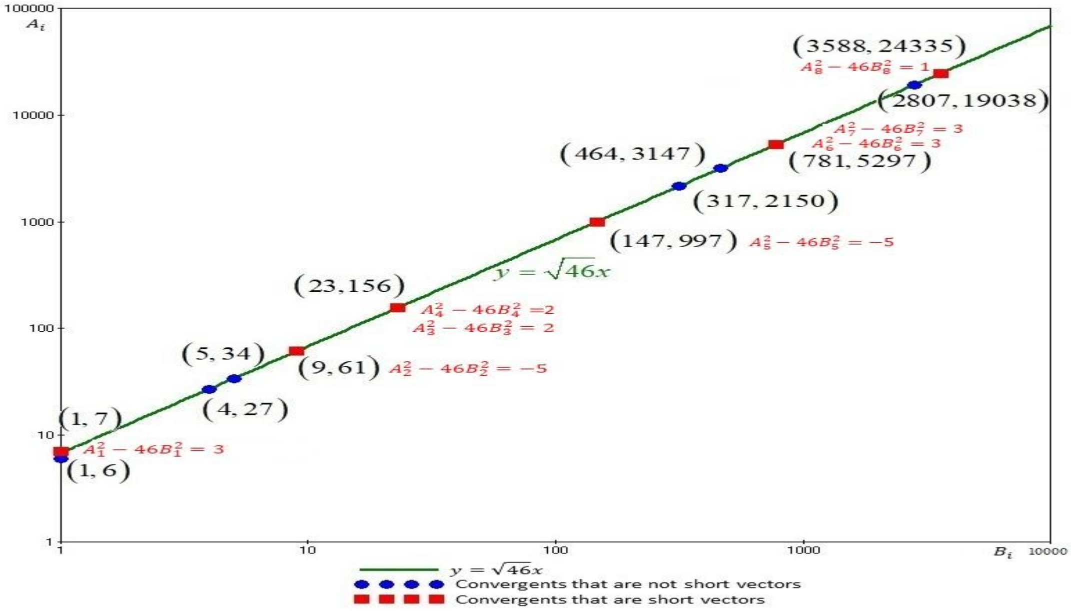

Figure 1: Represents the minimal solution $(3588, 24335)$ from the set of convergents of $\sqrt{46}$ obtained as short vector for $M = 10^8$.

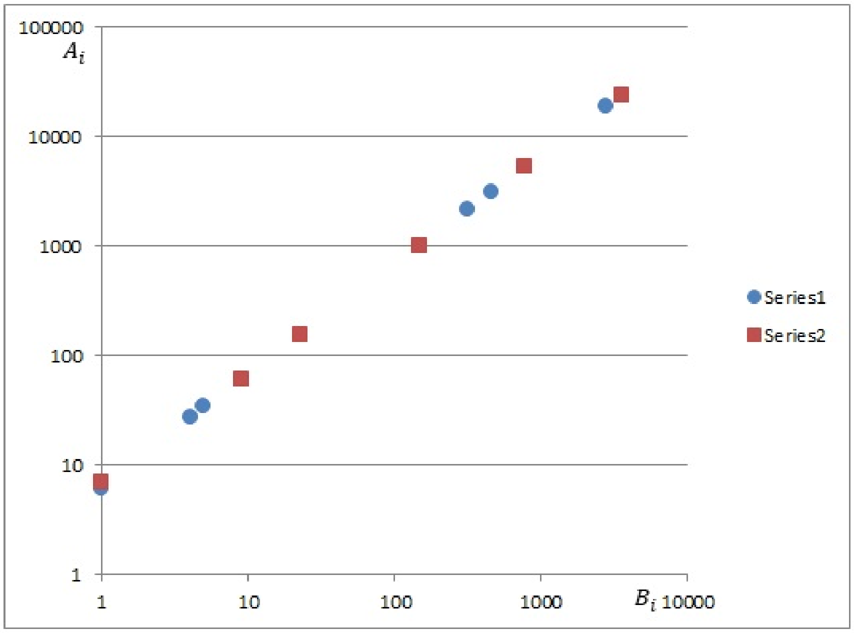

Figure 2: Represents the list of 11 convergents and the list of 6 short vectors leading to minimal solution $(\mathbf{3588}, \mathbf{24335})$.

CONCLUSION

For any general solution (x, y) of the Pell's equation $x^2 - Ny^2 = 1$ for N a non-square positive integer, as $x + \sqrt{N}y = (x_0 + \sqrt{N}y_0)^r$ for $r = 0, \pm1, \pm2, \cdots$, for (x_0, y_0) the minimal solution of $x^2 - Ny^2 = 1$, it is enough to evaluate (x_0, y_0) to find the solutions of the given Pell's equation. As $\frac{x_0}{y_0}$ is a convergent, it is obtained by searching in the class of convergents of $\sqrt{N}$. In this paper, this search of (x_0, y_0)in the class of continued fractions of $\sqrt{N}$ is adapted via lattice reduction in the class of short vectors of the quadratic form $q(\mathrm{y}, \mathrm{x}) = M\left(\sqrt{N}y - x\right)^2 + \frac{1}{M}\mathrm{y}^2$ for an appropriate choice of M. The existence of appropriate M and the process that leads to (y_0, x_0) as a short vector are depicted and supported by numerical examples. An algorithm to compute (y_0, x_0) as short vector is given and is used in all the computations by using LLL algorithm.

REFERENCES

1. Tom M. Apostol, Introduction to Analytical Number Theory, Springer International student edition, Narosa Publishing House.

2. Stefano Barbero, Umberto Cerruti, and Nadir Murru, Solving the Pell equation via Redei rational functions, *The Fibonacci Quarterly*, Volume 48, Number 4, November (2010).
3. J. Buchmann, Introduction to cryptography, Springer-Verlag (2001).
4. David M. Burton, Elementary Number Theory, Second Edition, Universal Book Stall, New Delhi.
5. H.Cohen, A course in Computational Algebraic Number Theory, *Graduate Texts in Math.*138. Springer (1996).
6. S.C. Coutinho, The Mathematics of Ciphers, University Press.
7. H. Davenport, The Higher Arithmetic, Cambridge University Press, Eighth edition, (2008).
8. Jeffery Hoftstein, Jill Pipher, Joseph H. Silverman, *An Introduction to Mathematical Cryptography*, Springer.
9. P. Anuradha Kameswari, S B T Sundari Katakam, Implementing Wiener Attack with Lattice Reduction, *Journal of Global Research in Mathematical Archives*, Vol 6,No.1, ISSN: 2320-5822, 7-14. January (2019).
10. Neal Koblitz, A course in Number Theory and cryptography, *Graduate Texts in Mathematics*, second edition, Springer.
11. A.K.Lenstra, H.W. Lenstra and L. Lovasz, Factoring Polynomials with Rational coefficients, *Math.Ann.*261, Springer – Verlag, 515-534 (1982).
12. Hendrik Lenstra, Peter Stevenhagen, Book Review: Solving the Pell equation, *Bulletin of the American Mathematical Society*, 52(2):345-351 April (2014).
13. Phong Q. Nguyen, Brigitte VallÃ©ee (Eds.), The LLL Algorithm, *Survey and Applications*, Springer, (2010).
14. Jean-Louis Sikorav, Best rational approximations of an irrational number, Preprint July 17 (2018).
15. Nigel P.Smart, The Algorithmic Resolution of Diophantine Equations, London Mathematical Society, Student Texts 41, (1998).
16. Michael J.Wiener, Cryptanalysis of short RSA secret exponent, IEEE. *Transaction on Information Theory*, Vol.36, No.3, 553-558 May (1990).
17. Seung Hyun Yang, Continued fractions and Pell's equation, University of Chicago REU Papers. (2008).