Solving Pell's Equation using Continued Fractions

A Dissertation Submitted to the Faculty of Science at
The University of Witwatersrand

By

Vhuhwavho Matibe
606653

To Fulfill the Requirements for the Degree of:
Master of Science

School of Mathematics

Supervisor, Professor F.Luca

March 2019

Declarations

I declare that this Dissertation is my own, unaided work. It is being submitted for the Degree of Master of Science at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination at any other University.

VMatibe

(Signature of candidate)

21st day of March 20 19 in WITS University

Abstract

The aim of this dissertation is to explore the Pell equation, through studying one method of solving it that is believed to have been initially used to find good approximations to the square root of square free positive integers, namely the continued fraction [8]. We further look at its significance by considering a number of its applications.

Acknowledgements

I thank God for the opportunity to study and complete my Master of Science degree in Pure Mathematics and acknowledge the guidance from my Supervisor Professor F. Luca. I appreciate the continuous support from my father, my entire family, and all my friends.

Contents

1 Introduction

According to the authors in [7]; the study of Number Theory, Diophantine equations and Diophantine Approximations can be largely attributed to "the father of algebra", Diophantus of Alexandria. The developments thereof came about after Pierre de Fermat proved one of Diophantus' proposition which became popular as Fermat's Little Theorem [7].

The study of interest for the dissertation is based on Diophantine Equations. When working with these type of equations, it is often asked whether (see [14]);

- The equation is solvable?
- If the number of solutions is finite or infinite?
- If it is possible or not to determine all solutions?

The questions can easily be understood through comprehending the definition of a Diophantine equation.

Definition 1.1. *Diophantine Equation (see [5])*
The Diophantine Equation [5] is an equation $f(x_1, x_2, x_3, \ldots, x_n) = 0$*, such that* f *is a given function, and the unknowns* $x_1, x_2, \ldots, x_n$ *can only either be rational numbers or integers.*

We however particularly consider the Diophantine equation;

$$x^2 - dy^2 = N,$$

here x and y are positive integers, d is square free non-zero integer and we are trying to solve for x and y given d and N. Setting $N = 1$, we get

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

known as Pell's equation. We begin by investigating the continued fraction expansion of the square root of d, and also use this expansion to solve (1) in terms of (x, y). Equation (1) can be written as

$$(x + \sqrt{d}y)(x - \sqrt{d}y) = 1, \tag{2}$$

(see [10]). We express (1) in the form (2) so that the solutions of (1) yield elements of the ring $\mathbb{Z}[\sqrt{d}] = \{x + \sqrt{d}y | (x, y) \in \mathbb{Z}\}$ of norm 1. The smallest solution will be the fundamental solution of (1); that is, (x_1, y_1) and can be used to find the *nth* solution by writing;

$$x_n + \sqrt{d}y_n = (x_1 + \sqrt{d}y_1)^n.$$

Pell's equation has been known to mathematicians for over 2000 years, from the Cattle Problem defined by Archimedes to the findings of Fermat and his successors [6]. It's significance can be deduced from the large number of papers

published concerning it.

To solve the Pell equation, we use a method known as continued fractions.

Definition 1.2. *Continued Fraction*
According to [14], a finite Continued Fraction of α, where α is a non-zero real number, is expressed as,

$$\alpha = a_0 + \cfrac{b_0}{a_1 + \cfrac{b_1}{a_2 + \cfrac{b_2}{a_3 + \cfrac{b_3}{\ddots + \cfrac{b_{n-2}}{a_{n-1} + \cfrac{b_{n-1}}{a_n}}}}}} \tag{3}$$

where $a_i, b_i > 0$, $i = 0, 1, 2, \ldots$ and $a_0 \geq 0$. Here $[a_0, a_1, \ldots, a_{n-1}, a_n]$ and $[b_0, b_1, \ldots, b_{n-1}, b_n]$ are the partial quotients.

We have both continued fraction expansions of rational and irrational numbers, both with arithmetic and algebraic properties. Our interest is mainly on the irrational numbers, where we use properties of quadratic irrationals to solve the Pell equation.

The dissertation will be presented using the following order;

- We begin by understanding continued fraction expansions of both rational and irrational numbers, as well as important properties that will appear in some of the results.
- We then prove a couple of results on continued fractions that are used when solving the Pell Equation.
- Lastly, we will present problems from Number Theory which do not apparently relate to Pell's equation, but however, the Pell Equation was used to greatly assist in solving the problems.

1.1 The Continued Fraction

Real numbers, either rational or irrational can be expressed as continued fractions. According to the author in [6], if a real number $\alpha = \frac{a}{b}$, where b is non-zero and a and b are integers, then α is called a rational number. If α is not rational, then it is irrational. Continued fractions can either be finite or infinite.

Note that the exposition in this section follows [7].

1.1.1 Finite Continued Fractions

According to [7], a finite continued fraction is expressed as,

$$[a_0; a_1, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}}.$$

Here the partial quotients are given by the rational numbers $[a_0, a_1, \ldots, a_n]$, where $a_1, \ldots, a_n$ are integers with $a_n > 0$. If all $a_0, \ldots, a_n$ are nonnegative, this continued fraction is called *simple*.

We use the Euclidean algorithm to express rational numbers as continued fractions (see [14]).

Below are some results on continued fraction expansions of rational numbers;

Theorem 1.1. *There are exactly two representations of any given rational number as a continued fraction.*

Proof. Using [7], we assume that there is only one continued fraction representation of any rational number.
Let $a_0, a_1, a_2, \ldots, a_n$ be natural numbers, and $a_n > 1$. We claim that

$$\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}} = a_0' + \cfrac{1}{a_1' + \cfrac{1}{a_2' + \cfrac{1}{a_3' + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1}' + \cfrac{1}{a_n'}}}}}},$$

and $a_0', a_1', a_2', \ldots, a_{n-1}', a_n'$ are also natural with $a_n' > 1$. Then $a_0 = a_0'$, $a_1 = a_1'$, $\ldots$, $a_n = a_n'$.

The amount added to a_0 on the left is less than 1, as well as the amount added to a_0' on the left. Thus, $a_0 = a_0'$, and they are both equal to the integral part of $\frac{a}{b}$. We remove a_0 against a_0', and invert the remaining continued fraction to obtain;

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}} = a_1' + \cfrac{1}{a_2' + \cfrac{1}{a_3' + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1}' + \cfrac{1}{a_n'}}}}}$$

Thus, as before, a_1 and a_1' cancel each other based on the already stated argument. Therefore, if we continue respectively, we see that indeed there is only one continued fraction representation of any rational $\frac{a}{b}$. Note that this is only valid whenever the right hand side is less than 1.

But according to the properties of natural numbers, any natural number k, can either be expressed as k, or $k - 1 + \frac{1}{1}$. Meaning that $\frac{a}{b}$ can be represented either as

$$\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}},$$

or as

$$\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3} + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n - 1 + \frac{1}{1}}}}}},$$

two different representations. □

Definition 1.3. *According to [6] the convergents of the continued fractions is defined as,*

$$a_0, a_0 + \frac{1}{a_1}, a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}}, \cdots \tag{4}$$

obtained from truncating the fraction at an earlier term than a_n.

Note that in order to define the general continued fraction, we truncate at

a_k as follows to obtain;

$$C_k = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \cfrac{1}{a_{k-1} + \cfrac{1}{a_k}}}}}} = \frac{P_k}{Q_k} = [a_0; \ldots, a_k].$$

So that the general convergent shown above can be simply written as $C_k = \frac{P_k}{Q_k}$.

1.1.2 Infinite Continued fractions

If the chain in (3) does not stop, then we define the relation as an infinite continued fraction. It is convergent if the limit of C_k exists and is equal to some α, that is,

$$\lim_{k \to \infty} C_k = \alpha$$

An infinite continued fraction exists ad infinitum without any patterns emerging, otherwise it is periodic. In [8], a continued fraction is defined as periodic if it is non-terminating and $a_{n+r} = a_n$ for some $r \geq 1$ and all $n \geq k$. It is denoted as

$$[a_0; a_1, a_2, \ldots, \overline{a_k, a_{k+1}, \ldots, a_{k+r-1}}].$$

1.2 Solving Pell's Equation

Before we show how continued fractions are used to solve Pell's equation, it is important to define the following;

1. Continued Fractions can be expressed as sequences, where $\{C_k\}_{k \geq 0}$ is the kth convergent of the continued fractions [8].

2. The sequences $\{P_k\}_{k \geq -1}$ and $\{Q_k\}_{k \geq -1}$ defined as;

$$P_{k+1} = a_{k+1}P_k + P_{k-1},$$
$$Q_{k+1} = a_{k+1}Q_k + Q_{k-1},$$

for $0 \leq k \leq n-1$, where $P_{-1} = 1$, $Q_{-1} = 0$, $P_0 = a_0$, and $Q_0 = 1$. The sequences can be written as a fraction $\frac{P_k}{Q_k}$ equal to the convergent C_k.

The algorithm for finding Pell's equation requires one to be able to generate a continued fraction expansion on $\sqrt{d}$, and further truncating the expansion before the last partial quotient of the first periodic continued fraction, which is the convergent. Thus, the fundamental solution (x_1, y_1) of the equation will be (P_k, Q_k) for some appropriate k.

2 Using the continued fraction to solve Pell's Equation

2.1 Introduction

We use a method of solving Pell's equation that was given by Lord Brouncker in 1657, based on developing $\sqrt{d}$ into a continued fraction. He was challenged by Frenicle de Bessy who managed to tabulate the solutions to Pell's equation, for all values of d up to 150. Frenicle challenged Brouncker by asking him to solve $x^2 - 313y^2 = 1$, who managed to solve it within an hour using continued fractions. Wallis and Fermat proved that Pell's equation is always soluble using continued fractions. Fermat stated that it has infinitely many solutions, and in 1766 Lagrange showed the first proof to this. P.J. Cameron explains this history in more detail in [2].

2.2 Results

Using the theory we gathered on continued fractions, we prove a couple of results and use them to prove our main theorem.

Theorem 2.1. *Given the sequences $p_0, p_1, \ldots, p_n$ and $q_0, q_1, \ldots, q_n$ for the continued fraction $[a_0, a_1, \ldots, a_n]$, and $k \geq 2$, the author in [4] begins by recursively defining the sequences below as;*

$$\begin{aligned} p_0 &= a_0, \qquad q_0 = 1 \\ p_1 &= a_0 a_1 + 1, \qquad q_1 = a_1 \\ p_k &= a_k p_{k-1} + p_{k-2}, \qquad q_k = a_k q_{k-1} + q_{k-2}. \end{aligned}$$

Then,

1. *The convergent C_k is given by p_k/q_k.*
2. *When $k \geq 1$,*
$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}.$$
3. *The identities,*
$$C_k - C_{k-1} = \frac{(-1)^{k-1}}{q_k q_{k-1}},$$
for $1 \leq k \leq n$, and
$$C_k - C_{k-2} = \frac{a_k (-1)^k}{q_k q_{k-1}},$$
for $2 \leq k \leq n$ hold.
4. *Lastly,*
$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \ldots < \alpha < \ldots < \frac{p_5}{q_5} < \frac{p_3}{q_3} < \frac{p_1}{q_1}$$

Proof. 1. We prove using induction on k;
Begin at $k = 0$, so that we have,

$$C_0 = [a_0] = \frac{a_0}{1} = \frac{p_0}{q_0};$$

For $k = 1$, we have

$$\begin{aligned} C_1 = [a_0, a_1] &= a_0 + \frac{1}{a_1} \\ &= \frac{a_0 a_1 + 1}{a_1} = \frac{p_1}{q_1}. \end{aligned}$$

Now assume that this holds for k, that is,

$$C_k = \frac{a_k p_{k-1} + p_{k-2}}{a_k q_{k-1} + q_{k-2}} = \frac{p_k}{q_k}.$$

Then,

$$\begin{aligned} C_{k+1} &= [a_0, a_1, \ldots, a_{k-1}, a_k + \frac{1}{a_{k+1}}] \\ &= \frac{(a_k + \frac{1}{a_{k+1}})p_{k-1} + p_{k-2}}{(a_k + \frac{1}{a_{k+1}})q_{k-1} + q_{k-2}} \\ &= \frac{a_{k+1}(a_k p_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_k q_{k-1} + q_{k-2}) + q_{k-1}} \\ &= \frac{a_{k+1}p_k + p_{k-1}}{a_{k+1}q_k + q_{k-1}} = \frac{p_{k+1}}{q_{k+1}}. \end{aligned}$$

2. Once again we prove by induction on k.
For $k = 1$,

$$p_1 q_0 - p_0 q_1 = (a_0 a_1 + 1)(1) - (a_0)(a_1) = a_0 a_1 + 1 - a_0 a_1 = 1.$$

Therefore, whenever k is postive and greater than 1;

$$\begin{aligned} p_{k+1}q_k - p_k q_{k+1} &= (a_{k+1}p_k + p_{k-1})q_k - p_k(a_{k+1}q_k + q_{k-1}) \\ &= a_{k+1}p_k q_k + p_{k-1}q_k - a_{k+1}p_k q_k - p_k q_{k-1} \\ &= p_{k-1}q_k - p_k q_{k-1} \\ &= -(-1)^{k-1} = (-1)^{k-1+1} = (-1)^k. \end{aligned}$$

3. To prove the first part, we use the results from 2 above,

$$p_k q_{k-1} - q_{k-1}p_{k-1} = (-1)^{k-1},$$

divide by $q_k q_{k-1}$ on either sides to get;

$$\begin{aligned} \frac{p_k q_{k-1}}{q_k q_{k-1}} - \frac{q_k p_{k-1}}{q_k q_{k-1}} &= \frac{(-1)^{k-1}}{q_k q_{k-1}} \\ \frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} &= \frac{(-1)^{k-1}}{q_k q_{k-1}}. \end{aligned}$$

Thus,

$$C_k - C_{k-1} = \frac{(-1)^{k-1}}{q_k q_{k-1}}.$$

Now for $C_k - C_{k-2}$, we can write this as;

$$\begin{aligned} C_k - C_{k-2} &= \frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} \\ &= \frac{p_k q_{k-2} - q_k p_{k-2}}{q_k q_{k-2}}. \end{aligned}$$

We take the numerator and write it as,

$$\begin{aligned} p_k q_{k-2} - q_k p_{k-2} &= (a_k p_{k-1} + p_{k-2}) q_{k-2} - q_k (a_k q_{k-1} + q_{k-2}) p_{k-2} \\ &= a_k p_{k-1} q_{k-2} + p_{k-2} q_{k-2} - a_k q_{k-1} p_{k-2} - q_{k-2} p_{k-2} \\ &= a_k (p_{k-1} q_{k-2} - q_{k-1} p_{k-2}) = a_k (-1)^{k-2}. \end{aligned}$$

Thus, we can write $C_k - C_{k-2}$ as,

$$C_k - C_{k-2} = \frac{a_k (-1)^{k-2}}{q_k q_{k-2}}.$$

4. We need to first show that for k odd,

$$C_1 > C_3 > C_5 > \dots$$

also for k even,

$$C_0 < C_2 < C_4 > \dots$$

According to the results in 3,

$$C_k - C_{k-2} = \frac{a_k (-1)^k}{q_k q_{k-2}}. \tag{5}$$

Thus, if k is even, we will have that $C_k - C_{k-2} > 0$, therefore,

$$C_k > C_{k-2}.$$

Also, when k is odd, $C_k - C_{k-2} < 0$, thus,

$$C_k < C_{k-2}.$$

Lastly, we need to show that for every convergent,

$$C_{g+1} > C_{2k},$$

where C_{g+1}, $g \geq 0$ are odd numbered and C_{2k}, $k \geq 0$ are even numbered. Here the author in [4] uses equation (5) for an even and odd numbered convergent as follows;

$$C_{2t} - C_{2t-1} = \frac{p_{2t}}{q_{2t}} - \frac{p_{2t-1}}{q_{2t-1}} = \frac{(-1)^{2t-1}}{q_{2t} q_{2t-1}}.$$

Since $2t - 1$ is odd,

$$C_{2t} - C_{2t-1} < 0$$

Thus $C_{2t} < C_{2t-1}$. And we can therefore write that,

$$C_{2k} < C_{2(g+k+1)} < C_{2(g+k)+1} < C_{2g+1}$$

□

Theorem 2.2. *(See [4])*

1. *Let α be irrational with convergents $C_j = p_j/q_j$ for $j \geq 0$ to its continued fraction. Assume (u, v) are integers with v positive and that for some $k \geq 0$, the inequality*
$$|v\alpha - u| < |q_k\alpha - p_k|,$$
holds. Then $v \geq q_{k+1}$.

2. *If u/v is a rational number in reduced form, with $v > 0$ such that*
$$\left|\alpha - \frac{u}{v}\right| < \frac{1}{2v^2}$$
then $u/v = p_k/q_k$ for some $k \geq 0$.

Proof. 1. In order to prove the first part, we assume that $1 \leq v < q_{k+1}$ and write the following system of linear equations,

$$p_k x + p_{k+1} y = u, \tag{6}$$

$$q_k x + q_{k+1} y = v. \tag{7}$$

In order to solve for (x,y) in (6) and (7) we can either use Cramer's rule or Gaussian Elimination. To use Gaussian Elimination, we represent (6) and (7) as a matrix in the following way,

$$\left[\begin{array}{cc|c} p_k & p_{k+1} & u \\ q_k & q_{k+1} & v \end{array}\right].$$

Thus after Gaussian Elimination we end up with the following matrix,

$$\left[\begin{array}{cc|c} 1 & 0 & \frac{uq_{k+1} - vp_{k+1}}{p_k q_{k+1} - q_k p_{k+1}} \\ 0 & 1 & \frac{vp_k - uq_k}{p_k q_{k+1} - q_k p_{k+1}} \end{array}\right].$$

We can therefore deduce that,

$$x = \frac{uq_{k+1} - vp_{k+1}}{p_k q_{k+1} - q_k p_{k+1}}, \tag{8}$$

and,

$$y = \frac{vp_k - uq_k}{p_k q_{k+1} - q_k p_{k+1}}, \tag{9}$$

which can also be written as follows;

$$(p_k q_{k+1} - q_k p_{k+1})x = uq_{k+1} - vp_{k+1}, \tag{10}$$

and,

$$(p_k q_{k+1} - q_k p_{k+1})y = vp_k - uq_k. \tag{11}$$

We can express $p_k q_{k+1} - p_{k+1} q_k$ in (10) and (11) as,

$$p_k q_{k+1} - p_{k+1} q_k = -(p_{k+1} q_k - p_k q_{k+1}) = -(-1)^k = (-1)^{k+1},$$

by simply using Cramer's rule or the results from Theorem 2.1.2. Thus,

$$(-1)^k y = uq_k - vp_k,$$

or,

$$y = (-1)^k(uq_k - vp_k),$$

and,

$$(-1)^k x = uq_{k+1} - vp_{k+1},$$

or,

$$x = (-1)^k(uq_{k+1} - vp_{k+1}).$$

Lastly we need to show that x and y are non-zero, non-negative and have opposite signs. To prove they are non-zero, we use contradiction as follows; Let $x = 0$. Then,

$$uq_{k+1} - vp_{k+1} = 0,$$

so,

$$\begin{aligned} uq_{k+1} &= vp_{k+1} \\ \frac{u}{v} &= \frac{p_{k+1}}{q_{k+1}}, \end{aligned}$$

therefore,

$$u = \frac{p_{k+1}v}{q_{k+1}}. \tag{12}$$

Since $gcd(p_{k+1}, q_{k+1}) = 1$, q_{k+1} divides v which implies that $q_{k+1} \leq v$, a contradiction to our assumption.
If on the other hand, we let $y = 0$, then $p_k x = u$ and $q_k x = v$. Thus,

$$|v\alpha - u| = |q_k x\alpha - p_k x| = |x||q_k\alpha - p_k| \geq |q_k\alpha - p_k|,$$

a contradiction.

Now assume that $y < 0$. Then in $q_k x = v - q_{k+1}y$, $v - q_{k+1} > 0$ and so $x > 0$. However, if $y > 0$, then for $q_k x = v - q_{k+1}y$, $q_{k+1}y \geq q_{k+1} > v$ and so $v - q_{k+1}y < 0$, thus $q_k x = vq_{k+1}y < 0$, so $x < 0$. It thus becomes straightforward that x and y have opposite signs.

From Theorem 2.1 item 4, we established that when k is even,

$$\frac{p_k}{q_k} < \alpha < \frac{p_{k+1}}{q_{k+1}}$$

and,

$$\frac{p_{k+1}}{q_{k+1}} < \alpha < \frac{p_k}{q_k},$$

when k is odd. Thus the sign for $q_k\alpha - p_k$ and $q_{k+1}\alpha - p_k$ will be opposite and so the signs for $x(q_k\alpha - p_k)$ and $y(q_{k+1}\alpha - p_k)$ will be the same. Thus,

$$\begin{aligned}|v\alpha - u| &= |(q_k x - q_{k+1}y)\alpha - (p_k x - p_{k+1}y)| \\ &= |x(q_k\alpha - p_k) + y(q_{k+1}\alpha - p_{k+1})| = |x||q_k\alpha - p_k| + |y||q_{k+1}\alpha - p_{k+1}| \\ &\geq |x||q_k\alpha - p_k| \geq |q_k\alpha - p_k|,\end{aligned}$$

is not a convergent, another contradiction.

2. We begin by assuming the contrary, that u/v is not a convergent to the continued fraction of α, this implies that for all n, $u/v \neq p_n/q_n$. Also note that the sequence q_k where k is the largest integer such that $v \geq q_k$ is strictly increasing, that is, since $v \geq q_0$ and q_k tends to infinity as k tends to infinity. Thus, $q_k \leq v < q_{k+1}$.
Recall in 1 above that

$$|v\alpha - u| \geq |q_k\alpha - p_k|,$$

thus,

$$|q_k\alpha - p_k| \leq |v\alpha - u| = v|\alpha - u/v| < \frac{1}{2v^2} < \frac{1}{2v},$$

and so,

$$|\alpha - \frac{p_k}{q_k}| < \frac{1}{2vq_k}.$$

Because we have assumed that $\frac{u}{v} \neq \frac{p_k}{q_k}$, then $1 \leq |vp_k - uq_k|$. If we divide both sides by vq_k, we get

$$\frac{1}{vq_k} \leq |\frac{p_k}{q_k} - \frac{u}{v}|.$$

Then,

$$\begin{aligned}\frac{1}{vq_k} &= \left|\frac{p_k}{q_k} - \frac{u}{v} + \alpha - \alpha\right| \leq \left|\alpha - \frac{p_k}{q_k}\right| + \left|\alpha - \frac{u}{v}\right| \\ &< \frac{1}{2vq_k} + \frac{1}{2v^2}.\end{aligned}$$

Thus,

$$\frac{1}{vq_k} < \frac{1}{2vq_k} + \frac{1}{2v^2},$$

so,

$$\frac{1}{vq_k} < \frac{1}{2v^2}.$$

Therefore $q_k > v$, a contradiction. The results therefore imply that $\frac{u}{v} = \frac{p_k}{q_k}$ and thus u/v is a convergent to α.

□

Theorem 2.3. *(see [14])*
Let an integer d be positive and square free, and suppose that $x^2 - dy^2 = \pm 1$ for $x, y \in \mathbb{Z}^+$. Then x/y is a convergent of $\sqrt{d}$.

Proof. Let (x, y) be a solution.

Case 1 Using [10] we suppose,

$$0 < x^2 - dy^2 < \sqrt{d}.$$

Subsequently,

$$(x + y\sqrt{d})(x - y\sqrt{d}) > 0$$

which implies that

$$x > y\sqrt{d}$$

Now observe that;

$$\begin{aligned}\left|\sqrt{d} - \frac{x}{y}\right| &= \left|\frac{y\sqrt{d} - x}{y}\right| = \left|\frac{(y\sqrt{d} - x)(y\sqrt{d} + x)}{y(y\sqrt{d} + x)}\right| = \left|\frac{y^2 d - x^2}{y^2(\sqrt{d} + \frac{x}{y})}\right| \\ &= \left|\frac{1}{y^2(\sqrt{d} + \frac{x}{y})}\right| < \frac{1}{2y^2}\end{aligned}$$

The last inequality is true because $d > 1$ and $x > y$. Now, we use Theorem 2.2.2 to conclude.

Case 2 We suppose that,

$$-\sqrt{d} < x^2 - dy^2 < 0.$$

Then,

$$0 < dy^2 - x^2 = d(y^2 - \frac{1}{d}x^2) = 1 < \sqrt{d}.$$

We divide by d to obtain,

$$\begin{aligned}0 < y^2 - \frac{1}{d}x^2 &< \frac{1}{\sqrt{d}}, \\ 0 < \left(y - \frac{1}{\sqrt{d}}x\right)\left(y + \frac{1}{\sqrt{d}}x\right) &< \frac{1}{\sqrt{d}},\end{aligned}$$

we further divide by $x\left(y + \frac{1}{\sqrt{d}}x\right)$ so that,

$$o < \frac{y}{x} - \frac{1}{\sqrt{d}} < \frac{1}{\sqrt{d}\left(y + \frac{1}{\sqrt{d}}x\right)x} < \frac{1}{2x^2},$$

thus,

$$y > \frac{x}{\sqrt{d}},$$

and so,

$$y + \frac{x}{\sqrt{d}} > \frac{2x}{\sqrt{d}},$$

therefore,

$$\sqrt{d}\left(y + \frac{x}{\sqrt{d}}\right) > 2x.$$

□

Theorem 2.4. (*see[4]*)
For $k = 0, 1, 2, \ldots$ define the following recursively;

$$\alpha_k = \frac{P_k + \sqrt{d}}{Q_k}, \tag{13}$$

$$a_k = \lfloor \alpha_k \rfloor, \tag{14}$$

$$P_{k+1} = a_k Q_k - P_k, \tag{15}$$

$$Q_{k+1} = \frac{d - P_{k+1}^2}{Qk}, \tag{16}$$

for k=0,1,2,... It follows that,
(a)There exists d and P_0, Q_0 integers, where

$$\alpha = \frac{P_0 + \sqrt{d}}{Q_0},$$

given that $Q_0 | (d - P_0^2)$.
(b)The expansion of α as a simple continued fraction is $[a_0, a_1, \ldots]$.

Proof. Using [4] we prove (a) by introducing integers a, b, e, f, such that e is square free, where both e and f are greater than zero in such a way that;

$$\alpha = \frac{a + b\sqrt{e}}{f} = \frac{af + \sqrt{eb^2 f^2}}{f^2}.$$

As seen above, if we multiply by f we get that $f^2 | (a^2 f^2 - eb^2 f^2)$. Thus, if we set $P_0 = af$, $Q_0 = f^2$, $d = eb^2 f^2$, then

$$\alpha = \frac{P_0 + \sqrt{d}}{Q_0},$$

and $Q_0 | d - P_0^2$.

(b) To show that α is expressed by $[a_0, a_1, a_2, \ldots]$ as a simple continued fraction, we only prove;

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k}.$$

for all k positive.
However,

$$\begin{aligned}
\alpha_k - a_k &= \frac{P_k + \sqrt{d}}{Q_k} - a_k \\
&= \frac{P_k + \sqrt{d} - a_k Q_K}{Q_k} = \frac{\sqrt{d} - (a_k Q_k - P_k)}{Q_k} \\
&= \frac{\sqrt{d} - P_{k+1}}{Q_k} = \frac{d - P_{k+1}^2}{Q_k(\sqrt{d} + P_{k+1})} \\
&= \frac{Q_k Q_{k+1}}{Q_k(\sqrt{d} + P_{k+1})} = \frac{1}{\alpha_{k+1}},
\end{aligned}$$

which is what we wanted. □

Theorem 2.5. *The simple continued fraction of a quadratic irrational α is periodic (see [4]).*

Proof. We use equation (13), (14), (15) and (16) from Theorem 2.4. We write

$$\alpha = \frac{P_0 + \sqrt{d}}{Q_0},$$

where $Q_0 | (d - P_0^2)$.

Let $\alpha = \alpha_0 = [\alpha_0, \alpha_1] = \ldots = [a_0, a_1, \ldots, a_{k-1}, \alpha_k]$.
Then

$$\alpha = \frac{p_{k-1}\alpha_k + p_{k-2}}{q_{k-1}\alpha_k + q_{k-2}}. \tag{17}$$

Let α' be the rational conjugate of α. Then,

$$\alpha' = \frac{\alpha'_k p_{k-1} + p_{k-2}}{\alpha'_k q_{k-1} + q_{k-2}}.$$

We can solve for α'_k as follows;

$$\begin{aligned}
\alpha'\alpha'_k q_{k-1} + \alpha' q_{k-2} &= \alpha'_k p_{k-1} + p_{k-1}, \\
\alpha'\alpha'_{k-1} q_{k-1} - \alpha'_k p_{k-1} &= p_{k-2} - \alpha' q_{k-2}, \\
\alpha'_k(\alpha' q_{k-1} - p_{k-1} &= p_{k-2} - \alpha' q_{k-2}, \\
\alpha'_k &= \frac{p_{k-2} - \alpha' q_{k-2}}{\alpha' q_{k-1} - p_{k-1}} = \frac{-(\alpha' q_{k-2} - p_{k-2})}{\alpha' q_{k-1} - p_{k-1}}.
\end{aligned}$$

If we factor out q_{k-2} from the numerator and q_{k-1} from the denominator we get

$$\alpha'_k = -\frac{q_{k-2}(\alpha' - \frac{p_{k-2}}{q_{k-2}})}{q_{k-1}(\alpha' - \frac{p_{k-1}}{q_{k-1}})}. \tag{18}$$

But we already know from the theory we studied on convergents of continued fractions that $C_k = \frac{p_k}{q_k}$, so equation (18) becomes

$$\alpha'_k = -\frac{q_{k-2}}{q_{k-1}}\left(\frac{\alpha' - C_{k-2}}{\alpha' - C_{k-1}}\right). \tag{19}$$

In equation (19), we know that as $k \to \infty$, C_{k-1} and C_{k-2} will tend to α. Thus, we have that,

$$\frac{\alpha' - C_{k-2}}{\alpha' - C_{k-1}} \to \frac{\alpha' - \alpha}{\alpha' - \alpha} \to 1.$$

Therefore, we see that from equation (18), $\alpha'_k < 0$ whenever k is sufficiently large. Also recall that $\alpha_k > 0$. Thus,

$$\alpha_k - \alpha'_k = \frac{P_k + \sqrt{d}}{Q_k} - \frac{P_k - \sqrt{d}}{Q_k} = \frac{2\sqrt{d}}{Q_k} > 0,$$

for k sufficiently large. This implies that $Q_k > 0$. Together with equation (17) we have that $Q_k Q_{k+1} = d - P_{k+1}^2 > 0$ and so,

$$Q_k \leq Q_k Q_{k+1} = d - P_{k+1}^2 \leq d. \tag{20}$$

From this, we can see that there can only be a finite number of possible values P_k and Q_k, this can be seen from narrowing down equation (20) to,

$$P_{k+1}^2 \leq d - Q_k \leq d.$$

Therefore there exists integers i and j, such that $i < j$ and $P_i = P_j$ further $Q_i = Q_j$. Thus we can write;

$$\alpha = [a_0, a_1, \ldots, a_{i-1}, \overline{a_i, \ldots, a_{j-1}}],$$

where a_i=a_j.
Hence, α is therefore periodic. □

Theorem 2.6. *(See [4]) If a positive integer d is square free and $\alpha = \alpha_0 = \sqrt{d}$, then*

$$p_{k-1}^2 - dq_{k-1}^2 = (-1)^k Q_k. \tag{21}$$

Proof. We begin the proof by an inspection when $k = 1$ on $p_{k-1}^2 - dq_{k-1}^2$, to give

$$p_0^2 - dq_0^2 = \left\lfloor \sqrt{d} \right\rfloor^2 - d(1) = \left\lfloor \sqrt{d} \right\rfloor^2 - d = -Q_1. \tag{22}$$

Equation (22) holds because of our definition of Q_{k+1} from Theorem 2.4. Now we suppose that $k \geq 2$. From the theorem, we are given that $\alpha = \alpha_0 = \sqrt{d}$ and so,

$$\sqrt{d} = \alpha_0 = [a_0, a_1, \ldots, a_{k-1}, \alpha_k],$$

which can be written as;

$$\sqrt{d} = \frac{\alpha_k p_{k-1} + p_{k-2}}{\alpha_k q_{k-1} + q_{k-2}}.$$

Using equation (13), we substitute α_k above with $\frac{P_k+\sqrt{d}}{Q_k}$, so that

$$\sqrt{d} = \frac{(\frac{P_k+\sqrt{d}}{Q_k})p_{k-1} + p_{k-2}}{(\frac{P_k+\sqrt{d}}{Q_k})q_{k-1} + q_{k-2}}. \tag{23}$$

We multiply across on both the numerator and denominator of equation (23) by Q_k to obtain,

$$\sqrt{d} = \frac{(P_k +\sqrt{d})p_{k-1} + Q_k p_{k-2}}{(P_k +\sqrt{d})q_{k-1} + Q_k q_{k-2}},$$

and so,

$$\sqrt{d} = \frac{P_k p_{k-1} +\sqrt{d}p_{k-1} + Q_k p_{k-2}}{P_k q_{k-1} +\sqrt{d}q_{k-1} + Q_k q_{k-2}}. \tag{24}$$

We cross multiply equation to get;

$$\begin{aligned}\sqrt{d}P_k q_{k-1} + dq_{k-1} +\sqrt{d}Q_k q_{k-2} &= P_k p_{k-1} +\sqrt{d}p_{k-1} + Q_k p_{k-2},\\ dq_{k-1} + (P_k q_{k-1} + Q_k q_{k-2})\sqrt{d} &= P_k p_{k-1} +\sqrt{d}p_{k-1} + Q_k p_{k-2}.\end{aligned}$$

Equating coefficients, we obtain,

$$dq_{k-1} = P_k p_{k-1} + Q_k p_{k-2}, \tag{25}$$

and,

$$(P_k q_{k-1} + Q_k q_{k-2}) = p_{k-1},$$

or

$$p_{k-1} = P_k q_{k-1} + Q_k q_{k-2}. \tag{26}$$

Multiplying equation (25) by q_{k-1} and equation (26) by p_{k-1} and subtracting equation (25) from (26) we get,

$$\begin{aligned}p_{k-1}^2 - dq_{k-1}^2 &= (P_k q_{k-1} p_{k-1} + Q_k q_{k-1} p_{k-2}) - (P_k p_{k-1} q_{k-1} + Q_k p_{k-1} q_{k-2})\\ &= Q_k q_{k-1} p_{k-2} - Q_k p_{k-1} q_{k-2},\end{aligned}$$

which we can write as

$$p_{k-1}^2 - dq_{k-1}^2 = (p_{k-1}q_{k-2} - p_{k-2}q_{k-1})Q_k. \tag{27}$$

The factor multiplying Q_k in equation (27) becomes $(-1)^k$ as already proven in Theorem 2.1.2, so that,

$$p_{k-1}^2 - dq_{k-1}^2 = (-1)^k Q_k.$$

□

Remark 2.7. *See [4]. If we let the period of the continued fraction of* $\sqrt{d}$ *be* n*. Then, according to the characteristics of purely periodic continued fractions it can be shown,* n *is the least positive integer resulting in* $Q_n = 1$*, and* $Q_j \neq -1$*, for all* j*, and therefore* $(-1)^k Q_k = \pm 1$ *if and only if* n *divides* k*.*

We now look at our final result for the chapter.

Theorem 2.8. *(see [4]) Begin by letting the period of the continued fraction expansion of* $\sqrt{d}$ *to be given by* n*.)*
(a) All the integer outcomes of Pell's equation, where $\frac{p_{n-1}}{q_{n-1}}$ *exist as the* $(n-1)$*th convergent, and* l *is an integer are represented by the equation,*

$$x + y\sqrt{d} = \pm(p_{n-1} + q_{n-1}\sqrt{d})^l,$$

(b) The equation,

$$x^2 - dy^2 = -1,$$

can only yield an integer solution when n *is odd.*
(c) Whenever there is a prime divisor $p \equiv 3 \pmod 4$ *of* d*,*

$$x^2 - dy^2 = -1,$$

yields no integer solution.

Proof. We use other methods than the continued fraction to determine the fundamental solution as well as the consecutive solutions of Pell's equation when proving (a).

(a) H Davenport in [3] defines

$$(x + \sqrt{d}y)^{-1} = \pm(x - \sqrt{d}y),$$

as true for any solutions (x, y) of the Pell equation. Therefore there are four possible different pairs of solutions $\pm(a, \pm b)$, where all pairs are solutions to $x^2 - dy^2 = \pm 1$. Now note that since

$$(\pm x)^2 - d(\pm y)^2 = \pm 1,$$

will always yield a positive answer, we will use a positive solution pair to prove the solutions are identified as

$$x + y\sqrt{d} = (p_{n-1} + q_{n-1}\sqrt{d})^l,$$

where $l > 0$. Recall that Theorem 2.3, showing the convergents of (x, y) gives that $x = p_{k-1}$ and $y = q_{k-1}$. Now note that remark 2.7 showed that equation (27) can be written as

$$p_{k-1}^2 - dq_{k-1}^2 = \pm 1,$$

and that $n|k$. The least positive integer outcome to Pell's equation is thus given by $x = p_{n-1}$ and $y = q_{n-1}$ and this is because,

$$p_{n-1} < p_{2n-1} < \dots$$

and

$$q_{n-1} < q_{2n-1} < \dots$$

Thus, the first part of the proof of (a) has been shown. That is, we have determined the fundamental solution. Therefore, it suffices to show the consecutive pairs of solutions to the Pell equation, that is, all the solutions to our equation.

Now this is done by using the fundamental solution (x_1, y_1) and particularly showing that all the positive solutions (x_l, y_l) are given by the equation,

$$x_l + y_l\sqrt{d} = (x_1 + y_1\sqrt{d})^l, l > 0. \tag{28}$$

Thus, (x_l, y_l) will indeed be the positive solutions because if we take the $\mathbb{Q}$-conjugates of equation (28), we have that,

$$x_l - y_l\sqrt{d} = (x_1 - y_1\sqrt{d})^l,$$

and so,

$$(x_l + y_l\sqrt{d})(x_l - y_l\sqrt{d}) = ((x_1 + y_1\sqrt{d}))^l(x_1 - y_1\sqrt{d})^l = (x_1^2 - dy_1^2)^l \tag{29}$$

$$= (\pm 1)^l = \pm 1. \tag{30}$$

Furthermore, $x_1 < x_l$ and so is $y_1 < y_l$.
Now assume that some (x, y) is a positive solution to the equation as well. Then we can say that there exists an integer k that is positive or zero, where;

$$(x_1 + y_1\sqrt{d})^k < x + \sqrt{d}y < (x_1 + y_1\sqrt{d})^{k+1}. \tag{31}$$

We divide equation (31) by $(x_1 + y_1\sqrt{d})^k$.

$$1 < (x_1 + y_1\sqrt{d})^{-k})(x + \sqrt{d}y) < (x_1 + y_1\sqrt{d})^{k+1}(x_1 + y_1\sqrt{d})^{-k},$$

to obtain,

$$1 < (x_1 + y_1\sqrt{d})^{-k}(x + \sqrt{d}y) < x_1 + y_1\sqrt{d}. \tag{32}$$

We continue to define integers, s and t where,

$$s + t\sqrt{d} = (x_1 + y_1\sqrt{d})^{-k}(x + y\sqrt{d}) \tag{33}$$

$$= \pm(x_1 - y_1\sqrt{d})^k(x + y\sqrt{d}). \tag{34}$$

This is true since we know that $x_1^2 - dy_1^2 = \pm 1$ implies that

$$(x_1 + y_1\sqrt{d})^{-k} = [(x_1 + y_1\sqrt{d})^{-1}]^k = [\pm(x_1 - y_1\sqrt{d})]^k,$$

which is true by equation (30). Therefore,

$$s^2 - dt^2 = (s + t\sqrt{d})(s - t\sqrt{d}) = [\pm(x_1 - y_1\sqrt{d})^k(x + y\sqrt{d})][\pm(x_1 + y_1\sqrt{d})^k(x - y\sqrt{d})]$$
$$= (x_l + y_l\sqrt{d})(x_l - y_l\sqrt{d}) = x_l^2 - dy_l^2 = \pm 1.$$

This means that (s, t) is also a solution, such that

$$1 < s + t\sqrt{d} < x_1 + y_1\sqrt{d},$$

by equation (32) and (34) above.

But this implies that (s, t) is smaller than (x_1, y_1) and given that (x_1, y_1) is the smallest solution to the equation, we have a contradiction.

(b) Once again, recall that Theorem 2.3 shows that $x^2 - dy^2 = -1$ implies that

$x = p_{n-1}$ and $y = q_{n-1}$. Recall also that Remark 2.7 says that $p_{k-1}^2 - dq_{k-1}^2 = (-1)^k Q^k = -1$, implies that k is odd, which can only mean that n is also odd.

(c) Say there is a such an x such that $x^2 \equiv -1 \pmod{p}$, then this implies that,

$$x^4 \equiv (-1)^2 \equiv 1 \pmod{p}.$$

Now note, the order of $x \pmod{p}$ gives the minimal k such that $x^k \equiv 1 \pmod{p}$. So the order of x is 4. But,

$$\begin{aligned} p &\equiv 4k+3, \quad so \\ p-1 &\equiv 4k+2 \end{aligned}$$

and $4k+2$ is not a multiple of 4, a contradiction. □

3 Applications

In this section, we look at different problems, were either Pell's equation or solving Pell's equation using continued fraction expansions were used directly or indirectly to solve these problems.

3.1 Two divisors of $\frac{(n^2+1)}{2}$ summing up to $n+1$

.

Theorem 3.1. *(This is from [1]) Two divisors $w_1, w_2 \geq 0$ of $\frac{(n^2+1)}{2}$ and an odd integer $n > 1$ do not exist such that $w_1 + w_2 = n + 1$.*

Note:It is of great importance that the condition $n > 1$ remains since if $n = 1$ we can let $w_1 = w_2 = 1$ that is;

$$\Big(\frac{(1)^2+1}{2} = 1, w_1 + w_2 = 1 + 1 = 2 = 1 + 1 = n + 1\Big).$$

Proof. We let $n > 1$ be an odd integer such that w_1 and w_2 are two positive divisors of $\frac{(n^2+1)}{2}$ where $w_1 + w_2 = n+1$. Since we assume that n is odd, $n^2 \equiv 1 \pmod 8$. And so, we have that $\frac{n^2+1}{2}$ is also odd. Now we need to prove w_1 and w_2 are coprime.

We assume that an odd prime q exists such that $q|\gcd(w_1, w_2)$. Hence, $q|w_1+w_2$, meaning that

$$n \equiv -1 \pmod q.$$

This is true since it is implied by $q|w_1 + w_2 = n + 1 = (n - (-1))$. We also get that,

$$n^2 \equiv -1 \pmod q, \tag{35}$$

since we have that $q|w_1|n^2 + 1$. Thus, equation (35) implies that $(-1)^2 \equiv -1 \pmod q$ and this means that $q|2$, that is,

$$q|((-1)^2 - (-1)) = 2.$$

This is impossible, because q is an odd prime. Therefore w_1 and w_2 are coprime.

If we have two coprime integers dividing a number, then their product also divides that number. Now since w_1 and w_2 are coprime and they divide $\frac{n^2+1}{2}$, then $w_1w_2|(\frac{n^2+1}{2})$. Now

$$w_1w_2\Big|\frac{n^2+1}{2}$$

implies that,

$$\begin{aligned}\frac{(\frac{n^2+1}{2})}{w_1w_2} &= w,\\ \frac{(\frac{n^2+1}{2})}{w} &= w_1w_2,\\ \frac{(n^2+1)}{2w} &= w_1w_2.\end{aligned}$$

Thus we write that $w_1w_2 = \frac{(n^2+1)}{2w}$. Then,

$$\begin{aligned}(w_1-w_2)^2 &= w_1^2 - 2w_1w_2 + w_2^2\\ &= (w_1+w_2)^2 - 4w_1w_2 = (n+1)^2 - 2\left(\frac{n^2+1}{w}\right).\end{aligned}$$

We multiply by $(\frac{w-2}{w-2})$ to get

$$(w_1-w_2)^2 = \frac{((w-2)n+w)^2 + 4 - 4w}{w(w-2)}. \tag{36}$$

If we have a prime divisor $p|n^2+1$ then $n^2 \equiv -1 \pmod{p}$ and this implies that $p \equiv 1 \pmod 4$. Thus, $n^2+1 \equiv 1 \pmod 4$ for all the divisors of n^2+1, which applies particularly to w_1, w_2 and w. Hence, we also have that

$$n = w_1 + w_2 - 1 \equiv 1(\mod 4).$$

We continue by dividing equation (36) by 4^2 to get

$$\begin{aligned}\frac{(w_1-w_2)^2}{4^2} &= \frac{((w-2)n+w)^2+4-4w}{4^2w(w-2)}\\ w(w-2)\left(\frac{w_1-w_2}{4}\right)^2 &= \left(\frac{(w-2)n+w}{w}\right)^2 - \frac{(w-1)}{4}.\end{aligned}$$

So that,

$$U = \left|\frac{(w-2)n+w}{w}\right|, \quad V = \left|\frac{w_1-w_2}{4}\right|, \quad s = \frac{w-1}{4},$$

are non-negative integers that satisfy

$$U^2 - DV^2 = s, \tag{37}$$

with

$$D = w(w-2) = (4s+1)(w-1-1) = (4s-1)(4s-1) = (4s)^2 - 1.$$

We begin by looking at the case when $s = 0$, then

$$U^2 - [(0)^2 - 1]V^2 = 0,$$

and so,

$$U^2 - (-V^2) = 0,$$

thus,

$$\Rightarrow U^2 + V^2 = 0.$$

This implies that $y = 0$ and thus $0 = \left|\frac{w_1 - w_2}{w}\right| \Rightarrow w_1 = w_2$. Since $w_1 = w_2$ and we have already mentioned that w_1 and w_2 are coprime, then this can only imply that w_1 and w_2 are both equal to 1. Now recall from the statement of theorem that $n + 1 = w_1 + w_2$, implies that $n = 1$, since $w_1 + w_2 = 1 + 1 = 2 = n + 1$. But this contradicts the fact $n > 1$. And so we assume instead that $s \geq 1$. The Diophantine equation (37) above gives,

$$(U + V\sqrt{D})(U - V\sqrt{D}) = s$$

$$(U - V\sqrt{D}) = \frac{s}{(U + V\sqrt{D})} \tag{38}$$

$$\left(\frac{U}{V} - \sqrt{D}\right) = \frac{s}{V(U + V\sqrt{D})}$$
$$\left|\frac{U}{V} - \sqrt{D}\right| = \frac{s}{V(U + V\sqrt{D})}$$

From equation (38), we note that $U > V\sqrt{D}$ and thus $U + V\sqrt{D} > 2U\sqrt{D} > 2sV$, since $\sqrt{D} = \sqrt{(4s)^2 - 1} > s$. Therefore,

$$\left|\frac{U}{V} - \sqrt{D}\right| < \frac{s}{V(2sV)} = \frac{1}{2V^2}.$$

By Theorem 2.2.2, we conclude that for arbitrarily large Y, $\frac{U}{V}$ must be a convergent of $\sqrt{D}$. We let $\psi = 4s$, and so that $D = (\psi)^2 - 1$ and we can express $\sqrt{D} = \sqrt{\psi^2 - 1}$ as a continued fraction expansion as follows,

$$\begin{aligned}
\sqrt{\psi^2 - 1} &= \psi - 1 + (\sqrt{\psi^2 - 1} - (\psi - 1)) = \psi - 1 + \frac{1}{\frac{1}{\sqrt{\psi^2-1}-(\psi-1)}} \\
&= \psi - 1 + \frac{1}{\frac{\sqrt{\psi^2-1}+\psi-1}{(\psi^2-1)-(\psi-1)^2}} = \psi - 1 + \frac{1}{\frac{\psi^2-1+\psi-1}{2\psi-2}} \\
&= \psi - 1 + \frac{1}{1 + \frac{\sqrt{\psi^2-1}-(\psi-1)}{2\psi-2}} = \psi - 1 + \frac{1}{1 + \frac{1}{\frac{2(\psi-1)}{\psi^2-1-(\psi-1)^2}}} \\
&= \psi - 1 + \frac{1}{1 + \frac{1}{\sqrt{\psi^2-1}+(\psi-1)}}.
\end{aligned}$$

This implies that,

$$\psi - 1 < \sqrt{\psi^2 - 1} < \psi,$$

and so,

$$2(\psi - 1) < \sqrt{\psi^2 - 1} + \psi - 1$$

thus,

$$\sqrt{\psi^2 - 1} = [\psi - 1, 1, \overline{2(\psi - 1), 1}].$$

Using Theorem 2.3 it suffices that if $\frac{p_m}{q_m}$ denotes the mth convergent of$\sqrt{D}$, then

$$p_m^2 - Dq_m^2 = -2\psi + 2 \quad or \quad 1,$$

depending on whether m is odd or even. This means equation (37) will be in the range $-2\psi + 2, 1$, but $\psi = 4s$, so;

$$U^2 - VY^2 \in \{-8s + 2, 1\}. \tag{39}$$

When comparing equation (39) with equation (37), we get that $s = 1$. So, $s = \frac{w-1}{4}$ implies $w = 5$ and $D = 5(5 - 2) = 15$, thus (U, V) is a solution to the equation,

$$U^2 - 15V^2 = 1. \tag{40}$$

The Pell equation in (40) will have $(U_1, V_1) = (4, 1)$ as the smallest solution. Therefore the tth solution (U_t, V_t) of equation (40) for all t will be,

$$U_t + \sqrt{15}V_t = (4 + \sqrt{15})^t.$$

For all positive integers t, it is easy to see that $U_t \equiv 1 \pmod 3$. Thus if

$$U_t = s(n + 1) - \frac{n - 1}{4},$$

for positive n where $s = 1$, we would then get that,

$$\begin{aligned} (n + 1) - \frac{(n - 1)}{4} &= U_t \\ \frac{4(n + 1) - n + 1}{4} &= U_t, \\ n &= \frac{4U_t - 5}{3}. \end{aligned}$$

but then since $4U_t - 5 \equiv -1 \pmod 3$, $\frac{(4U_t - 5)}{3}$ is never be an integer for any positive integer t. Therefore there isn't any solution and we are done. □

3.2 Estimating $|\alpha - p/q|$

From the knowledge we have gathered so far, one can conclude that the fundamentals of solving the Pell Equation using the continued fraction is based on an estimate of the distance of the ratio the ratio of the two integers x, y to the square root of a square-free integer d. In order to understand this estimate, it is critical to understand the relation between x, y and $\sqrt{d}$.

In this section, we look at a paper by R.T Worley [17], which considers the relation amongst α the continued fraction of a positive real irrational, as well as a rational approximation to α, p/q. This relation explains the estimate for $q^2|\alpha - p/q|$, and extends to the standard result; "$q^2|\alpha - p/q| < \frac{1}{2}$ implies that for some n, $\frac{p}{q} = \frac{p_n}{q_n}$."

Worley defines α and p/q as,

$$\alpha = [a_0, a_1, \ldots, a_n, a_{n+1}, \ldots], \tag{41}$$

$$p/q = [a_0, a_1, \ldots, a_n, b_1, \ldots, b_r]. \tag{42}$$

Since p/q is written in reduced form, p and q are relatively prime positive integers. Also to ensure the uniqueness of p/q, $b_r \geq 2$. Furthermore we suppose that $\frac{p}{q}$ is not p_m/q_m a convergent to α, that is, $b_1 \neq a_{n+1}$ and $r \geq 1$ (there is more than one b_r).

Worley's paper [17] considers and strengthens the following; "What could be said if $q^2|\alpha - p/q| < 2$". To show this, we use the knowledge we gathered in Chapter 2, together with the two new lemmas below;

Lemma 3.2. *Let*

$$P_m/Q_m = [0, a_{m+2}, a_{m+3}, \ldots, a_{m+k}],$$

if $k = 1$ the continued fraction is explained by $0/1$. Then

$$q_{m+k} = q_m Q_m([a_{m+1}, \ldots, a_{m+k}] + q_{n-1}/q_n).$$

Thus,

$$q = q_n d([b_1, \ldots, b_r] + q_{n-1}/q_n), \tag{43}$$

and the denominator of $[b_1, \ldots, b_r]$ is d.

Note that the proof of Lemma 3.2 can be found in Worley[17].

Lemma 3.3. *If the convergent of α is not given by p/q , then*

$$q^2|\alpha - p/q| > d^2(\varphi - \varphi^2/\rho),$$

if $\varphi < \rho$, and

$$q^2|\alpha - p/q| > d^2(\varphi - \rho)(\varphi + 1)(\rho + 1),$$

if $\varphi > \rho$,
where $\varphi = [b_1, \ldots, b_r]$ and $\rho = [a_{n+1}, a_{n+2}, \ldots,]$ as seen on equation (41) and (42) above.

Proof. (As seen in [17])
We can represent $|\alpha - p/q|$ as follows,

$$|\alpha - p/q| = \left| \frac{\rho p_n + p_{n-1}}{\rho q_n + q_{n-1}} - \frac{\varphi p_n + p_{n-1}}{\varphi q_n + q_{n-1}} \right|.$$

We take the lowest common denominator, multiply through and cancel out a few terms to get,

$$\begin{aligned} |\alpha - p/q| &= \left| \frac{\rho p_n q_{n-1} - \rho q_n p_{n-1} + \varphi q_n p_{n-1} - \varphi p_n q_{n-1}}{(\rho q_n + q_{n-1})(\varphi q - n + q_{n-1})} \right|, \\ &= \left| \frac{\rho(p_n q_{n-1} - q_n p_{n-1}) - \varphi(p_n q_{n-1} - q_n p_{n-1})}{(\rho q_n + q_{n-1})(\varphi q_n + q_{n-1})} \right|. \end{aligned}$$

We have,

$$\frac{|\rho - \varphi|}{(\rho q_n + q_{n-1})(\varphi q_n + q_{n-1})}. \tag{44}$$

We multiply equation (44) by q^2 and use equation (43) to write it as,

$$q^2|\alpha - p/q| = \frac{d^2|\rho - \varphi|(\varphi + q_{n-1}/q_n)}{(\rho + q_{n-1}/q_n)}.$$

We conclude the proof based on the fact that $\frac{(\varphi+x)}{(\rho+x)}$ $(0 \leq x \leq 1)$ increases as x increases whenever $\varphi < \rho$ and decreases when $\varphi > \rho$. □

We can now use the results from the above lemmas to show the main result. Worley [17] gives the results based on two theorems, the first one, which we will not focus on is based on the unique cases $k = 1/2$ and $k = 1$ of classical results 1 and 2 shown in his paper. We however, take more interest in the following proof.

Theorem 3.4. *(As seen on [17])*
If α is irrational, $k \geq 1/2$, and p/q is a rational approximation to α [17] such that,

$$q^2|\alpha - p/q| < k,$$

then p/q converges to α or;
(i)

$$p/q = \frac{ap_n + bp_{n-1}}{aq_n + bq_{n-1}},$$

where $a \geq b$ and $ab < 2k$, or $a \leq b$ and $ab < k + a^2/a_{n+1}$,
(ii)

$$p/q = \frac{ap_n - bp_{n-1}}{aq_n - bq_{n-1}},$$

where $a \leq b$ and $ab < 2k$, or $a \geq b$ and $ab(1 - b/2a) < k$.
Also note that $a, b > 0$.

Proof. (As seen in [17]) To prove Theorem 3.4, we take note of the following based on the information given in the theorem, and the lemmas above.

We begin by making the assumption that $q^2|\alpha - p/q| < k$ and the convergent p_n/q_n to α is not given by p/q .

We also define p/q as well as α according to equations (41) and (42), that were described in the beginning on this section.

Recall as well the following bounds that were given in Lemma 3.3;

$$q^2|\alpha - p/q| > d^2(\varphi - \varphi^2/\rho),$$

if $\varphi < \rho$, and

$$q^2|\alpha - p/q| > d^2(\varphi - \rho)(\varphi + 1)(\rho + 1),$$

if $\varphi > \rho$.
We compare these bounds to k.

Also based on the bounds in Lemma 3.3, we can plot the graph $f_\rho(x) = x - x^2/\rho$, a parabola where the maximum is given by $x = 1/2\rho$ and $x = 1/2$ is the axis of symmetry.

The graph above cuts the axis at,

$$f_\rho(x) = 0 \to x - x^2/\rho = 0,$$

$x = 0$ or $x = \rho$. So if $m \leq \min(\varphi, \rho - \varphi)$, then

$$f(\varphi) = \varphi - \varphi^2/\rho \geq f(m) = m - m^2/\rho = m(1 - m/\rho),$$

$$\varphi - \varphi^2/\rho \geq m - m^2/\rho. \tag{45}$$

With the help of all the information we have listed above, we break the proof into four cases and prove accordingly as seen below.

Case 1 Set $r = 1$, $\varphi = b_1 < \rho$, then the denominator d of φ will be 1. Also setting $m = \min(b_1, a_{n+1} - b_1)$ and using equation (45) and Lemma 3.3, we get;

$$k > q^2|\alpha - p/q| > d^2(\varphi - \varphi^2/\rho);$$
$$k > q^2|\alpha - p/q| > 1(\varphi - \varphi^2/\rho) > m(1 - m/\rho).$$

As a side note,

$$m = b_1 \leq a_{n+1} - b_1,$$

if and only if,

$$a_{n+1} \geq 2b_1,$$

tends to,

$$\alpha_{n+1} > 2b_1.$$

Say $m = a_{n+1} - b_1 \leq b_1$, then

$$a_{n+1} \geq 2m,$$

which is equivalent to,

$$a_{n+1} \geq 2(a_{n+1} - b_1),$$

or,

$$2b_1 \geq a_{n+1}.$$

So we can say that

$$\rho > a_{n+1} \geq 2b_1 = 2m,$$

since

$$\frac{m}{\rho} < 1/2,$$

and so $1 - m/\rho > 1/2$ and $m > 2k$. We can write,

$$p/q = [a_0, a_1, \ldots, a_n, b_1] = \frac{mp_n + p_{n-1}}{mq_n + q_{n-1}}$$

and

$$\begin{aligned} p/q &= [a_0, a_1, \ldots, a_n, a_{n+1} - m] \\ &= \frac{(a_{n+1-m})p_n + p_{n-1}}{(a_{n+1-m})q_n + q_{n-1}} = \frac{p_{n+1} - mp_n}{q_{n+1} - mq_n}, \end{aligned}$$

for $\varphi = a_{n+1} - m$. Case 1 is complete.

Case 2 Set $r > 1$, $\varphi < \rho$. We represent φ in two ways, as $m + \tau/d$ if $\varphi \leq 1/2a_{n+1}$ or as $a_{n+1} - m - \tau/d$ if $\varphi > 1/2a_{n+1}$, and $1 < \tau \leq d - 1$, so that we can use equation (45) and Lemma 3.3 to get;

$$\begin{aligned} k > q^2|\alpha - p/q| > d^2(\varphi - \varphi^2/\rho) \geq d^2(m + \tau/d)\left(1 - \frac{m + \tau/d}{\rho}\right) \\ = d(dm + \tau)\left(1 - \frac{m + \tau/d}{\rho}\right). \end{aligned}$$

As a side note, since $\varphi = a_{n+1} - m\tau/d$ if $\varphi > 1/2a_{n+1}$ then,

$$\begin{aligned} a_{n+1} - m - \tau/d &> 1/2a_{n+1} \\ a_{n+1} &> 2(m + \tau/d). \end{aligned}$$

Thus, if $m \geq 1$ we see that $\rho > a_{n+1} > 2m + \tau/d$, meaning,

$$\begin{aligned} 1 &> \frac{2(m + \tau/d)}{\rho} \\ 1/2 &> \frac{m + \tau/d}{\rho}. \end{aligned}$$

Therefore, we can write,

$$\begin{aligned} k &> d(dm + \tau)(1 - \frac{(m + \tau/d)}{\rho}), \\ k &> d(dm + \tau)(1 - 1/2). \end{aligned}$$

So, $d(dm + \tau) < 2k$. If $\varphi = m + \tau/d$, then

$$\begin{aligned} \frac{p}{q} &= [a_0, a_1, \cdots, a_n, m + \tau/d] = \frac{(m + \tau/d)p_n + p_{n-1}}{(m + \tau/d)q_n + q_{n-1}}, \\ &= \frac{d}{d}\left(\frac{(m + \tau/d)p_n + p_{n-1}}{(m + \tau/d)q_n + q_{n-1}}\right) = \frac{(dm + \tau)p_n + dp_{n-1}}{(dm + \tau)q_n + dq_{n-1}}. \end{aligned}$$

We let $a = (dm + \tau)$ and $b = d$, then

$$\frac{p}{q} = \frac{ap_n + bp_{n-1}}{aq_n + bq_{n-1}}.$$

If on the other hand $\varphi = a_{n+1} - m - \tau/d$ then

$$\begin{aligned} \frac{p}{q} &= [a_0, a_1, \cdots, a_n, a_{n+1} - m - \tau/d], \\ &= \frac{(a_{n+1} - m - \tau/d)p_n + p_{n-1}}{(a_{n+1} - m - \tau/d)q_n + q_{n-1}} = \frac{d}{d}\frac{(a_{n+1} - m - \tau/d)p_n + p_{n-1}}{(a_{n+1} - m - \tau/d)q_n + q_{n-1}}, \\ &= \frac{a_{n+1}p_n d - (dm + \tau)p_n + dp_{n-1}}{a_{n+1}q_n d - (dm + \tau)q_n + dp_{n-1}} = \frac{d(a_{n+1}p_n + p_{n-1}) - (dm + \tau)p_n}{d(a_{n+1}q_n + q_{n-1}) - (dm + \tau)q_n}, \\ &= \frac{dp_{n+1} - (dm + \tau)p_n}{dq_{n+1} - (dm + \tau)q_n}. \end{aligned}$$

It is now clear to see that if we let $a = d$ and $b = dm + \tau$ then

$$\frac{p}{q} = \frac{ap_{n+1} - bp_n}{aq_{n+1} - bq_n}.$$

This concludes the proof of Case 2.

Case 3 Set $r = 1$, $\varphi = b_1 > \rho$. Since φ only has one element, then the denominator $d = 1$ like in Case 1. Using Lemma 3.3 we will have,

$$k > q^2|\alpha - p/q| > (1)^2(\varphi - \alpha)(\varphi + 1)/(\rho + 1) > \varphi - \rho.$$

Since $\rho < a_{n+1} + \frac{1}{a_{n+2}}$, then

$$\varphi - \rho < k,$$

and so,

$$b_1 - a_{n+1} - \frac{1}{a_{n+2}} < k.$$

If we let $b_1 = a_{n+1} + b$, then $p/q = [a_0, a_1, \ldots, a_n, a_{n+1} + b]$, which will become,

$$\begin{aligned}\frac{p}{q} &= \frac{(a_{n+1}+b)p_n + p_{n-1}}{(a_{n+1}+b)q_n + q_{n-1}} = \frac{(a_{n+1}p_n + p_{n-1}) + bp_n}{(a_{n+1}q_n + q_{n-1}) + bq_n},\\ &= \frac{p_{n+1} + bp_n}{q_{n+1} + bq_n},\end{aligned}$$

where $a_{n+1} + b - a_{n+1} - \frac{1}{a_{n+1}} < k$, that is $b < k + \frac{1}{a_{n+2}}$. This completes Case 3.

Case 4 Set $r > 1$, $\varphi > \rho$. Let $\varphi = b_1 + \tau/d$, where $1 \leq \tau \leq d-1$. Then, using Lemma 3.3,

$$\begin{aligned}k &> q^2|\alpha - p/q| > d^2(\varphi - \rho)(\varphi + 1)/(\rho + 1) > d^2(\varphi - \rho)\\ &= d^2(b_1 + p/q - a_{n+1} - a_{n+1} - \frac{1}{a_{n+1}})\\ &> d(db_1 + \tau - da_{n+1} - \frac{d}{a_{n+2}}).\end{aligned}$$

We write $m = b_1 - a_{n+1}$, so that

$$\begin{aligned}k &> d(d(b_1 - a_{n+1}) + \tau - \frac{d}{a_{n+1}}),\\ &= d(dm + \tau) - \frac{d^2}{a_{n+2}},\end{aligned}$$

giving $d(m + \tau) < k + \frac{d^2}{a_{n+2}}$, since

$$\frac{p}{q} = \frac{dp_{n+1} + (dm + \tau)p_n}{dq_{n+1} + (dm + \tau)q_n}.$$

The proof is now complete. □

Recall that the aim of this particular paper was for strengthen the result when $k = 2$, Worley [17] concludes his paper with this case, through the corollary shown below.

Corollary 1. *(As seen on [17])*
When $q^2|\alpha - p/q| < 2$ then the convergent to α (p_n/q_n) is given by p/q or p/q is one of,
(i)'

$$p/q = (ap_n + p_{n-1})/(aq_n + q_{n-1})$$

$a = 1, 2, 3, a_{n+1} - 3, a_{n+1} - 2, a_{n+1} - 1$,
(ii)'

$$p/q = (ap_n + 2p_{n-1})/(aq_n + 2q_{n-1})$$

$a = 1$ *or* $2a_{n+1}$*-1.*

Proof. (As seen on [17])
To prove the corollary, we look at all the possible cases of Theorem 3.4.

Case 1 We consider the case where $a \geq b$, and $ab < 2(2) = 4$.

The possibilities of (a, b) are as follows;
(i) $a = b$, which implies that $a = b = 1$, and so $(a, b) = (1, 1)$,
(ii) $(a, b) = (2.1)$,
(iii) $(a, b) = (3, 1)$.

Case 2 $a \leq b$ and $ab < k + a^2/a_{n+1} = 2 + a^2/a_{n+1}$.

We observe that $ab < 2 + a^2/a_{n+1} < 2 + a^2$, from this we can deduce that

$$\begin{aligned} ab - a^2 &< 2, \\ a \leq a(b - a) &< 2. \end{aligned}$$

If $a = b$, we get a similar case with one, where $(a, b) = (1, 1)$ and

$$\frac{p}{q} = \frac{p_n + p_{n-1}}{q_n + q_{n-1}}.$$

Also since $a \leq b$ and $b - a \geq 1$, then if $a = 1$,

$$b(1) < 2 + a/a_{n+1},$$

So b cannot be greater than 2, and so we will have $(a, b) = (1, 2)$.

We observe that so far cases 1 and 2 have given (a, b) the following solutions; (1,1), (2,1), (3,1) and (1,2).

Case 3 $a \leq b$, $ab < 2k = 4$.

Since $a \leq b$, the $a = 1$ and $b = 1, 2, 3$. So,

$$\frac{p_n - p_{n-1}}{q_n - q_{n-1}}, \frac{p_n - 2p_{n-1}}{q_n - 2q_{n-1}}, \frac{p_n - 3p_{n-1}}{q_n - 3q_{n-1}}. \tag{46}$$

We write $p_n = a_{n+1}p_{n-1} + p_{n-2}$, so that (46) can be written as,

$$(a_{n+1} - 1)p_{n-1} + p_{n-2}, (a_{n+1} - 2)p_{n-1} + p_{n-2}, (a_{n+1} - 3)p_{n-1} + p_{n-2}.$$

This gives the combinations $(a, b) = (a_{n+1} - 1, 1), (a_{n+1} - 2, 1)$ and $(a_{n+1} - 3, 1)$.

Case 4 $a \geq b$, $ab(1 - b/2a) < k = 2$.

Rewrite $a \geq b$ as:

$$\begin{aligned} b &\leq a, \\ b/2a &\leq 1/2, \\ 1 - b/2a &< 1/2, \\ 2 > ab(1 - b/2a) &> ab/2, \end{aligned}$$

this implies that $ab < 4$. Since $b \leq a$, then $b = 1$ and $a = 1, 2$. After representing this in the form $\frac{ap_n - bp_{n-1}}{aq_n - q_{n-1}}$, we end up with $a = 1$ or $2a_{n+1} - 1$ as stated in the corollary. We are done. $\square$

3.3 The Equation $x^2 - (k^2 - 4)y^2 = 4t$

Here we discuss work from Luca et al. [13], where, the theory of the Pell equation and the continued fractions are used to solve the equation,

$$k = \frac{a^2 + b^2}{ab + 1}. \tag{47}$$

With rearrangement and substitution, equation (47)) is further written as the quadratic equation,

$$x^2 - (k^2 - 4)y^2 = 4k, \tag{48}$$

where $x = bk - 2a$, and $y = b$, and the solutions (a, b, k) are in correspondence with the solutions (x, y, k).

We begin by taking note of the definition below;

Definition 3.1. *Mediating Fraction*
Let α be given by,

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

For $1 \leq m \leq a_{n+1}$, a mediating fraction to α is defined as any rational p/q of the following form,

$$p = mp_n + p_{n-1},$$

and,

$$q = mq_n + q_{n-1}.$$

The convergent p_{n+1}/q_{n+1} is the special case of the mediating fraction, with $m = a_{n+1}$.

The results below were already proved in Worley [17]. However, the authors in [13] have reproved these results.

Theorem 3.5. *Let α denote an irrational number and let r/s be a rational number in reduced form, with $s \geq \max(2, q_1)$, such that*

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{s^2}. \tag{49}$$

Then there exist $n \geq 1$ and $1 \leq m < a_{n+1}$, such that one of the conditions below hold;
(i) $(r, s) = (p_n, q_n)$;
(ii) $(r, s) = (mp_n + p_{n-1}, mq_n + q_{n-1})$;
(iii) $(r, s) = (p_n + 2p_{n-1}, q_n + 2q_{n-1})$;
(iv) $(r, s) = (2p_n - p_{n-1}, 2q_n - q_{n-1})$.

We are particularly interested in proving the following results.

Theorem 3.6. *(See [13])*
Let $k > 1$ be an odd integer. If t is a positive integer for which $t < 2\sqrt{k^2-4}$ and the equation

$$x^2 - y^2(k^2-4) = 4t \tag{50}$$

has solutions in coprime positive integers x, y, then $t = 1$ or $t = k+2$.

Proof. Let $\alpha = \frac{1+\sqrt{k^2-4}}{2}$ and rewrite equation (50) as follows;

$$\begin{aligned}
(x - y\sqrt{k^2-4})(x + y\sqrt{k^2-4}) &= 4t \\
[x + y - (1+\sqrt{k^2-4})y][x + y - (1-\sqrt{k^2-4})y] &= 4t \\
\left[\frac{x+y}{2} - \left(\frac{1+\sqrt{k^2-4}}{2}\right)y\right]\left[\frac{x+y}{2} - \left(\frac{1-\sqrt{k^2-4}}{2}\right)y\right] &= t \\
\left(\frac{(x+2)/2}{y} - \left(\frac{1+\sqrt{k^2-4}}{2}\right)\right)\left(\frac{(x+y)/2}{y} - \left(\frac{1-\sqrt{k^2-4}}{2}\right)\right) &= \frac{t}{y^2}.
\end{aligned}$$

Since t is positive, if $\frac{(x+2)/2}{y} < \frac{(1+\sqrt{k^2-4})}{2}$, then the product will be negative, a contradiction. Therefore $\frac{(x+y)/2}{y} > \frac{(1+\sqrt{k^2-4})}{2}$. Dividing both sides by $\left(\frac{(x+y)/2}{y} - \left(\frac{1-\sqrt{k^2-4}}{2}\right)\right)$ we have,

$$\begin{aligned}
\left(\frac{(x+y)/2}{y} - \left(\frac{1+\sqrt{k^2-4}}{2}\right)\right) &= \frac{t}{y^2(((x+y)/2)y - (1-\sqrt{k^2-4})/2)} \\
&< \frac{t}{y^2\sqrt{k^2-4}}
\end{aligned}$$

Therefore,

$$\left(\frac{(x+y)/2}{y} - \left(\frac{1+\sqrt{k^2-4}}{2}\right)\right) < \frac{2}{y^2}.$$

Based on equation (49), Theorem 3.5 above tells us that $((x+y)/2)/y$ is either a convergent, a mediating fraction to α, or there are two consecutive convergents p_{n-1}/q_{n-1}, p_{n-2}/q_{n-2} to α where;

$$\frac{(x+y)/2}{y} = \frac{p_{n-1} + 2p_{n-2}}{q_{n-1+2q_{n-2}}},$$

or

$$\frac{(x+y)/2}{y} = \frac{2p_{n-1} - p_{n-2}}{2q_{n-1} - q_{n-2}}.$$

To obtain the partial quotients to α, we express α as a continued fraction as

follows;

$$\begin{aligned}
\alpha &= \frac{1+\sqrt{k^2-4}}{2} = \frac{k-1}{2} + \left(\frac{1+\sqrt{k^2-4}}{2} - \frac{k-1}{2}\right) \\
&= \frac{k-1}{2} + \left(\frac{\sqrt{k^2-4}-(k-2)}{2}\right) = \frac{k-1}{2} + \frac{1}{\frac{2}{(\sqrt{k^2-4}-(k-2))}} \\
&= \frac{k-1}{2} + \frac{1}{\frac{2(\sqrt{k^2-4}+(k-2))}{k^2-4-(k-2)^2}} = \frac{k-1}{2} + \frac{1}{\frac{(\sqrt{k^2-4})+(k-2)}{2(k-2)}} \\
&= \frac{k-1}{2} + \frac{1}{1+\left(\frac{(\sqrt{k^2-4})+(k-2)}{2(k-2)} - 1\right)} = \frac{k-1}{2} + \frac{1}{1+\frac{\sqrt{k^2-4-(k-2)}}{2(k-2)}} \\
&= \frac{k-1}{2} + \frac{1}{1+\frac{1}{\frac{1+\sqrt{k^2-4}}{2} - \frac{(k-3)}{2}}} = \left[\frac{k-1}{2}, 1, \alpha + \frac{k-3}{2}\right]
\end{aligned}$$

Thus, the partial quotients are given by,

$$[\frac{k-1}{2}, 1, k-2, 1, k-2, 1, \ldots] = [\frac{k-1}{2}, \overline{k-2}],$$

and so the first few convergents $p_0/q_0, p_1/q_1, \ldots$ are,

$$((k-1)/2)/1, ((k+1)/2)/1, ((k^2-3)/2)/(k-1), \ldots.$$

Using an inductive argument, it can be shown that x and y where $(x, y) = (2p_i, q_i)$, satisfy;

$$x^2 - y^2(k^2-4) = 4,$$

for $i \geq 0$ and odd as follows;

$$\begin{aligned}
x^2 - y^2(k^2-4) &= (2p_i - q_i)^2 - (k^2-4)q_i^2 = (2p_1 - q_1)^2 - (k^2-4)q_i^2 \\
&= \left(2\left(\frac{k+1}{2}\right) - 1\right)^2 - (k^2-4)(1) = 4,
\end{aligned}$$

However for $i \geq 0$ and even, we get,

$$x^2 - y^2(k^2-4) = -4(k-2),$$

as follows;

$$\begin{aligned}
x^2 - y^2(k^2-4) &= (2p_i - q_i)^2 - (k^2-4)q_i^2 = \left(2\left(\frac{k-1}{2}\right) - 1\right)^2 - (k^2-4)(1) \\
&= -4k + 8 = -4(k-2),
\end{aligned}$$

which does not satisfy the assumptions on t.

For the case where $((x+y)/2)/y$ is a mediating fraction, the mediating fractions will always lead to (x, y) where $x^2 - y^2(k^2-4)$ is negative. If we use

the first iteration for example, where the mediating fractions are $i/1$, such that $1 \leq i \leq (k-1)/2$ and putting $(2i-1, 1)$, we will have;

$$\begin{aligned} x^2 - y^2(k^2-4) &= (2i-1)^2 - (1)^2(k^2-4) = (2(1)-1)^2 - 1(k^2-4) \\ &= -k^2 + 3, \end{aligned}$$

which is negative. This applies for all $i's$.

Now consider the final case where there are convergents $p_{n-1}/q_{n-1}, p_{n-2}/q_{n-2}$ to α where,

$$\frac{(x+y)/2}{y} = \frac{p_{n-1} + 2p_{n-2}}{q_{n-1} + 2q_{n-2}}, \tag{51}$$

or

$$\frac{(x+y)/2}{y} = \frac{(2p_{n-1} - p_{n-2})}{(2q_{n-1} - q_{n-2})}. \tag{52}$$

We begin by showing the first case in equation (51). It follows that n must be odd since $a_n = 1$. In this we can only use $n \geq 3$ (because p_{-1}/q_{-1} does not exist). Thus, for $n = 3$, we have;

$$\frac{(x+y)/2}{y} = \frac{p_2 + 2p_1}{q_2 + 2q_1} = \frac{(k^2-3)/2 + 2(k+1)/2}{(k-1) + 2(1)},$$

and so $x = k^2 + k - 2$ and $y = k + 1$. Thus,

$$\begin{aligned} x^2 - y^2(k^2-4) &= (k^2+k-2)^2 - (k+1)^2(k^2-4) \\ &= k^4 2k^3 - 3k^2 - 4k + 4 - (k^2+2k+1)(k^2-4) \\ &= 4k + 8 = 4(k+2). \end{aligned}$$

Using a similar analysis for the case in equation (52), we also get that,

$$x^2 - y^2(k^2-4) = 4(k+2)$$

or,

$$x^2 - y^2(k^2-4) = -6k + 13.$$

The proof is now complete. □

References

[1] M. Ayad, F.Luca, *Two divisors of* $\frac{(n^2+1)}{2}$ *summing up to* $n+1$, Journal de Théorie des Nombres de Bordeaux, Vol. 19(3) (2007), pp. 561-566.

[2] P. J. Cameron, *A Course in Number Theory*, online [http://www.maths.qmul.ac.uk/∼pjc/notes/nt.pdf], pp. 17-60.

[3] H. Davenport, *The Higher Arithmetic, An Introduction to the Theory of Numbers*, Cambridge University Press 2008, pp. 68-74, pp. 78, pp. 83-99.

[4] J. Esmonde, M. R. Murty, *Problems in Algebraic Number Theory*, Springer 2005, pp. 108-114.

[5] G. Everest, T. Ward, *An Introduction to Number Theory*, Springer 2005.

[6] M. J. Jacobson, H. C. Williams, *Solving the Pell Equation*, Springer 2009, pp. 1-3.

[7] G. M. Katz, D. Schaps, S.Shnider, *Almost Equal: The method of Adequality from Diophantus to Fermat and Beyond*, Perspectives on Science, Vol. 21(3) (2013), pp. 283-324.

[8] G. D. Koffi, P. Khourg, *Continued Fractions and their Application to Solving Pell's Equation*, University of Massachusetts, Boston 2009, pp. 7-12.

[9] D. H. Lehmer, *On a problem of Störmer*, Illinois J. Math 8 (1964), pp. 57-59.

[10] H. W. Lenstra, *Solving the Pell Equation*, Notices of the AMS, Vol 49(2) (2002), pp. 1-6.

[11] F. Luca, *Primitive Divisors of Lucas Sequences and Prime Factors of* x^2+1 *and* x^4+1, Acta Acad. Paedagog. Agriensis Sect. Mat. (N.S.) Vol. 31 (2004), pp. 1-10.

[12] F. Luca, F. Najman, *On the largest prime factor of* x^2-1, Mathematics of Computation, Vol. 80(273) (2011), pp. 429-435.

[13] F. Luca, C. F. Osgood, P. G. Walsh, *Diophantine Approximations and A Problem From The 1988 IMO*, Rocky Mountain Journal of Mathematics, Vol. 36(2) (2006), pp. 642-648.

[14] K. H. Rosen, *Elementary Number Theory and its Applications*, Addison-Wesley Publishing Company 1984, pp. 336-375.

[15] R. T. Worley, *Denominator Sequences of Continued Fractions I*, J. Austral. Math. Soc. Vol. 15 (1973), pp. 112-113.

[16] R. T. Worley, *Restricted Diophantine Approximation*, J. Austral. Math. Soc. (Series A) Vol. 24 (1977), pp. 425-439.

[17] R. T. Worley, *Estimating* $|\alpha - p/q|$, J. Austral. Math. Soc. (Series A) Vol. 31 (1981), pp. 202-206.

[18] S. H Yang, *Continued Fractions and Pell's Equation*, University of Chicago (2008), pp. 11.