CONTINUED FRACTIONS AND THEIR APPLICATION TO SOLVING PELL'S EQUATION

Peter Khoury,Gerard D. Koffi
peter.a.khoury@gmail.com , gerard.koffi001@umb.edu

Abstract

This is an expository research project about continued fraction expansions of square roots of square-free integers and how they can be used to solve Pell's Equation and, for some cases, the *negative* Pell's Equation, $x^2 - dy^2 = -1$. We will provide a brief background to both Pell's Equation and Continued Fractions. We will show that the Pell's Equation $x^2 - dy^2 = 1$ is always solvable and the connection of its fundamental solution to the convergents of the continued fraction expansion of $\sqrt{d}$. We finally show how some Pell's Equations can be used to solve some problems in mathematics.

1 Introduction

The quadratic Diophantine equation of the form

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

where d is a positive square-free integer is called a Pell Equation after the English mathematician John Pell(1 March 1611- 12 December 1685). Pell did not solve equation (1). There are numerous historical accounts confirming that Pell did not have any interest in the given equation. The name Pell's equation comes from Euler who, in a letter to Goldbach, confused the name of William Brouncker, the first mathematician who gave an algorithm to solve equation (1) with that of Pell's. Because of Euler's mathematical influence the name Pell's Equation remained. Pell's Equation has been known by the Greeks. In fact, Archimedes's Cattle problem can be solved by obtaining solutions to the Pell Equation $x^2 - 4,729,494y^2 = 1$(for more information on Archimedes's Cattle problem, see [2]). It is not known whether

Archimedes was aware of Pell's Equation.
Pell's Equation has been studied intensively. Several mathematicians including Lagrange, Fermat, and Wallis have given serious attention to equation (1). In this paper, we present an algorithm using continued fractions to solve a Pell's Equation.

2 Continued fractions

Let m be a non zero real number. We define the continued fraction of m as follows

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

where the a_i's and b_i's may be non-negative reals or complex , and only a_0 may be zero. The numbers a_i are called **partial quotients** of the continued fraction. A *simple continued fraction* is one where all the a_i's are positive integers with the exception of a_0 which may be negative or zero and all the b_i's equal to one. as in

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots \cfrac{\ddots}{a_{n-2} + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}}} \tag{3}$$

If there exists such a_n at which the expansion terminates then it is called a *finite simple continued fraction* or terminating continued fraction. Otherwise, the continued fraction is said to be infinite.

Example 2.1 Take the rational number $\frac{9}{7}$, we can write it as a finite simple continued fraction as follows:

$$\frac{9}{7} = 1 + \frac{2}{7} = 1 + \frac{1}{\frac{7}{2}} = 1 + \frac{1}{3 + \frac{1}{2}} \tag{4}$$

Example 2.2 Take an irrational number such as π, when written as a simple continued fraction it turns out to be non-terminating, or infinite

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{\ddots}}}}}}}}} \tag{5}$$

where the $\ddots$ indicate repeating the process accordingly *ad infinitum* but with no emerging pattern of the partial quotients.

We will use the notation $[a_0; a_1, a_2, a_3, \ldots, a_n]$ to indicate the simple continued fraction of a non zero real number m if it is finite and $[a_0; a_1, a_2, a_3, \ldots]$ if it is infinite. For example the continued fraction of π above is given by

$$\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, 2, 2, 2, ...]. \tag{6}$$

whereas $\frac{9}{7}$ above is given by

$$\frac{9}{7} = [1; 3, 2] \tag{7}$$

Definition 2.3 A continued fraction is said to be periodic if it is non-terminating and for some given integers k and r the terms $a_k, \ldots, a_{k+r-1}$ repeat infinitely in the expansion and the continued fraction is said to have period r. As in $[a_0; a_1, \ldots, a_{k-1}, a_k, a_{k+1}, \ldots, a_{k+r-1}, a_k, a_{k+1}, \ldots]$. We will use the notation $[a_0; a_1, \ldots, \overline{a_k, \ldots, a_{k+r-1}}]$

Continued fractions are believed to have been initially used to find a good approximation to the square root of square-free positive integers. In this section, we provide useful facts about continued fractions that we will use to solve certain Pell's Equations. Before starting, we define a few terms.
It is often necessary to write continued fractions as sequence when used solve math problems. Let the real number M have continued fractions as in equation (2). We define a sequence of term $\{C_k\}_{k\geq 0}$ as follows:

$$C_0 = a_0,$$

$$C_1 = a_0 + \frac{1}{a_1},$$

$$C_2 = a_0 + \cfrac{1}{a_1 + \frac{1}{a_2}},$$

$$\vdots$$

$$C_k = a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\cdots + \frac{1}{a_k}}}},$$

and so on. The terms C_j are called **convergents** of the continued fraction. And C_k is called the kth convergent of M. Now we define two new sequences $\{A_k\}_{k\geq -1}$ and $\{B_k\}_{k\geq -1}$ as follows:

$$A_{-1} = 1, A_0 = a_0 \quad \text{and} \quad B_{-1} = 0, B_0 = 1$$
$$\begin{cases} A_{k+1} = a_{k+1}A_k + A_{k-1} \\ \\ B_{k+1} = a_{k+1}B_k + B_{k-1} \end{cases} \quad \text{for } 0 \leq k \leq n-1. \tag{8}$$

The following Lemma shows how the convergents are related to the sequences $\{A_k\}_{k\geq -1}$ and $\{B_k\}_{k\geq -1}$.

Lemma 2.4 The fraction A_k/B_k is the convergent C_k.

Proof: We have that $A_0/B_0 = a_0 = C_0$ and $A_1/B_1 = (a_1a_0 + 1)/a_1 = C_1$. By induction, it follows immediately that $A_k/B_k = C_k$. This completes the proof.

the sequences $\{A_k\}_{k\geq -1}$ and $\{B_k\}_{k\geq -1}$ also satisfy the following property.

Lemma 2.5 $A_kB_{k-1} - A_{k-1}B_k = (-1)^k$ for $k \geq 0$.

Proof: The proof is done by induction.

The property in Lemma 2.4 can be rewritten as

$$\frac{A_k}{B_k} - \frac{A_{k-1}}{B_{k-1}} = \frac{(-1)^{k-1}}{B_kB_{k-1}}. \tag{9}$$

Since the a_i's are positive integers, we have that the sequence $\{B_k\}_{k\geq 0}$ is increasing for $k > 0$. Thus by the alternating test, the series

$$\frac{A_0}{B_0} + \sum_{k=1}^{\infty}\left(\frac{A_k}{B_k} - \frac{A_{k-1}}{B_{k-1}}\right) = \frac{A_0}{B_0} + \sum_{k=1}^{\infty}\frac{(-1)^{k-1}}{B_kB_{k-1}} \tag{10}$$

is convergent. From the above series, we have the following Lemma.

Lemma 2.6 The sequence $\{A_k/B_k\}_{k\geq 0}$ is convergent; that is there exists t such that

$$t = \lim_{k\to\infty} \frac{A_k}{B_k}. \tag{11}$$

Proof: Since the series in (10) is convergent, we have that

$$\lim_{k\to\infty} \left(\frac{A_k}{B_k} - \frac{A_{k-1}}{B_{k-1}} \right) = 0.$$

Hence, the sequence $\{A_k/B_k\}_{k\geq 0}$ converges. This completes the proof.

If the continued fraction of t in Lemma 2.5 is finite, we have that $t = A_n/B_n$ is a rational number. Otherwise, it is an irrational number; since we can not stop the process of "chopping off" fractions rendering the number rational, the result is a number that *cannot* be expressed as $\frac{n}{d}$ where n and d are integers and $d \neq 0$. It can be shown that for $k \geq 0$

$$\left| t - \frac{A_k}{B_k} \right| < \frac{1}{2^{2\lfloor \frac{k}{2} \rfloor}}$$

where $\lfloor a \rfloor$ is the greatest integer less than a(for a proof, see [1]). Thus, the convergents $C_k = A_k/B_k$ approximates t.

Example 2.7 Take $m = \frac{9}{7} = [1; 3, 2]$. The $1st$ convergent to m is just 1. The second convergent would be

$$C_1 = 1 + \frac{1}{3} = \frac{4}{3}$$

the third convergent $C_2 = m$ is

$$m = 1\frac{1}{3 + \frac{1}{2}} = \frac{9}{7}$$

Example 2.8 In the expansion of $\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, 2, 2, 2, ...]$, the $1st$ convergent C_0 is given by

$$C_1 = 3 + \frac{1}{7} = \frac{22}{7}$$

whereas the $6th$ convergent C_5 is given by

$$C_5 = 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1 + \frac{1}{292 + \frac{1}{1}}}}} = \frac{104,370}{33,222}$$

Note that $\frac{22}{7}$ is a commonly used rational approximation to π, and that $\frac{104{,}370}{33{,}222}$ would even be a better one! Observe that $\frac{22}{7} = 3.1428571...$ and $\frac{104{,}370}{33{,}222} = 3.1415929203.....$

In general, the nth convergent is

$$C_{n-1} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots \cfrac{\ddots}{a_{n-2} + \cfrac{1}{a_{n-2} + \cfrac{1}{a_{n-1}}}}}}}}$$

The following is an algorithm to compute the simple continued fraction of a real number x.
Start by writing

$$x = \lfloor x \rfloor + \frac{1}{x_0}$$

If x_0 is an integer we are done, and x is rational and equal to $\lfloor x \rfloor + \frac{1}{x_0}$, otherwise, if x_0 is not an integer repeat the process again. Now, solve for x_0 and write

$$x_0 = \lfloor x_0 \rfloor + \frac{1}{x_1}$$

If x_1 is an integer, we are done, otherwise repeat the process.

If we repeat the process and find that for some n, $x_n = x_{n-r}$ for some integer r then the continued fraction is periodic (as we will define in the next section), then $x = [x_0; a_1, a_2, \ldots, \overline{a_{n-r}, a_{n-r+1}, \ldots, a_n}]$.

To show how one can use continued fractions to solve a Pell's Equation, we provide an exposition of the theory of periodic continued fractions. The proofs of all the theorems in the following section will not be given here; they can be found in [1].

3 Periodic Continued Fractions

Definition 3.1 A continued fraction is said to be **purely periodic** with period m if the initial block of partial quotients $a_0, a_1, \ldots, a_{m-1}$ repeats infinitely and no block of length less than m is repeated. We denote a purely periodic continued fraction as $[\overline{a_0; a_1, \ldots, a_{m-1}}]$. A continued fraction is called **periodic** with period m if it consists of an initial block of length n follow by a repeating block of length m.

To solve the Pell's equation (1) using the method of continued fractions, we need to know the continued fraction expansion of $\sqrt{d}$. The following theorem gives such expansion.

Theorem 3.2 Let $d > 1$ be a rational number that is not the square of another rational number. Then

$$\sqrt{d} = [a_0; \overline{a_1, a_2, \ldots, a_2, a_1, 2a_0}]. \tag{12}$$

The above Theorem says that the continued fraction expansion of $\sqrt{d}$ is periodic. For example, $\sqrt{\frac{11}{7}} = [1; \overline{3, 1, 16, 1, 3, 2}]$ is periodic and has period of length 6.

Remark 3.3 The converse of theorem (3.2) is also true; that is, every periodic rational fraction corresponds to an irrational number.

Now we are ready to use the theory of continued fractions to solve Pell's equation (1).

4 Pell's Equation

Recall that a Pell's Equation is a quadratic Diophantine equation of the form $x^2 - dy^2 = 1$, where d is a square free positive integer. One may ask why the restriction on d? The following theorem provides an answer.

Theorem 4.1 Equation (1) has finitely many solutions when $d < 0$ and when d is a perfect square.

Proof: When $d < 0$, we have that the left hand side of equation (1) is positive; that is $x^2 - dy^2 > 0$. Hence, the only solutions are $(\pm 1, 0)$. When d is a perfect square, say, $d = a^2$, equation (1) can be factored as $(x - ay)(x + ay) = 1$. And it follows that there can be only finitely many solutions, namely two: $(x, y) = (\pm 1, 0)$. This completes the proof.

Theorem 4.1 says that we can find the solutions of equation (1) by using simple algebraic method. Before we move on to solving equation (1) we study briefly the general Pell's Equation of the form

$$x^2 - dy^2 = N, \tag{13}$$

where N is an integer. The following theorem that we do not prove(see proof in [1]) states for which N equation (13) is solvable; that is it has integer solutions.

Theorem 4.2 If $|N| < \sqrt{d}$, then the solutions of equation (13) are $x = A_k$ and B_k, where A_k/B_k is a convergent of $\sqrt{d}$.

Example 4.3 Observe the Pell Equation

$$x^2 - 7y^2 = 2$$

Since $2 < |\sqrt{7}|$ we know that the solution (A_k, B_k) is a convergent $\frac{A_k}{B_k}$ of the continued fraction expansion of $\sqrt{7}$. Now, $7 = [2; \overline{1, 1, 1, 4}]$. Let us compute the first few convergents.

$$C_0 = 2,\ C_1 = 2 + \frac{1}{1} = 3,\ C_2 = 2 + \frac{1}{1 + \frac{1}{1}} = \frac{5}{2},$$

$$C_3 = 2 + \frac{1}{1 + \frac{1}{1+\frac{1}{1}}} = \frac{8}{3},\ C_4 = 2 + \frac{1}{1 + \frac{1}{1+\frac{1}{1+\frac{1}{4}}}} = \frac{37}{14}$$

And indeed, the fundamental solution of the above equation is $(x, y) = (9, 7)$ which is (A_k, B_k) where $\frac{A_k}{B_k} = C_1 = \frac{A_1}{B_1} = \frac{3}{1}$.

Now we are ready to state our main theorem. A proof of the following theorem can be found in [1] and [2].

Theorem 4.4 If $N = 1$, then equation (13) is always solvable and the solution are (A_k, B_k) where A_k/B_k is a convergent of $\sqrt{d}$. If $N = -1$, then (13) is solvable if and only if the length of the period of the continued expansion of $\sqrt{d}$ is odd.

Theorem 4.3 says that equation (1) has solution and that solution can be found by using the continued fraction expansion of $\sqrt{d}$. In general, we are interested in the minimal positive solution of equation (1). This solution is also called **the fundamental solution**. The fundamental solution is a solution of (1) from which other solutions can be obtained. In fact, the following Lemma shows that if (x_1, y_1) is the fundamental solution to equation (1) then there are infinitely many solutions and all can be obtained from (x_1, y_1).

Lemma 4.5 Let (x_1, y_1) with $x_1 > 1, y_1 \geq 1$ be the fundamental solution to equation (1), then (x_n, y_n) where $(x_n + y_n\sqrt{d}) = (x_1 + y_1\sqrt{d})^n$ are solutions to equation (1) , and $x_{n+1} > x_n$ and $y_{n+1} > y_n$.

Proof: Since (x_1, y_1) is a solution to equation (1), we have that $x_1^2 - dy_1^2 = 1$. Now we write $x_1^2 - dy_1^2 = 1$ as $(x_1 - \sqrt{d}y_1)(x_1 + \sqrt{d}y_1)$. Taking the square and gathering terms so that the equation is in the form of (1), it follows that the resulting (x_2, y_2) is a solution. This process can continue indefinitely. Hence, we found infinitely many more positive solutions to equation (1). From $(x_n + y_n\sqrt{d}) = (x_1 + y_1\sqrt{d})^n$, it follows immediately using the binomial expansion that $x_{n+1} > x_n$ and $y_{n+1} > y_n$. This completes the proof.

Using section 2 and Theorem 4.3, we can find the fundamental solution of (1). We provide and application to section 2 and Theorem 4.3. Consider the Pell's equation $x^2 - 14y^2 = 1$. The continued fraction of $\sqrt{14}$ is $[3; \overline{1, 2, 1, 6}]$. Now truncate the continued fraction right before the end of the first period, we have that

$$\frac{15}{4} = [3; 1, 2, 1]$$

$x = 15, y = 4$ is the fundamental solution.

Example 4.6 Solve the following Pell's Equation using the method of Continued Fractions and convergents:

$$x^2 - 41y^2 = 1$$

Solution : We begin by computing the continued fraction expansion of $\sqrt{41}$ as follows:

$$\sqrt{41} = \lfloor\sqrt{41}\rfloor + \frac{1}{x_1}$$

where $\lfloor\sqrt{41}\rfloor = 6$ and $\frac{1}{x_1} = \sqrt{41} - 6$

solving for x_1 we have :

$\frac{1}{x_1} = \sqrt{41} - 6 \implies x_1 = \frac{\sqrt{41}+6}{5}$

now, we will compute the continued fraction for x_1 the same way by doing the following :

$x_1 = \frac{\sqrt{41}+6}{5} = \lfloor x_1 \rfloor + \frac{1}{x_2}$

$\frac{1}{x_2} = \frac{\sqrt{41}+6}{5} - \lfloor x_1 \rfloor = \frac{\sqrt{41}+6}{5} - 2$

$\frac{1}{x_2} = \frac{\sqrt{41}-4}{5} \cdot \frac{\sqrt{41}+4}{\sqrt{41}+4} = \frac{25}{5(\sqrt{41}+4)} \implies x_2 = \frac{\sqrt{41}+4}{5}$

again, let us repeat the same process for x_2 by writing :

$x_2 = \lfloor x_2 \rfloor + \frac{1}{x_3} = 2 + \frac{1}{x_3}$

$\frac{1}{x_3} = \frac{\sqrt{41}+4}{5} - 2 = \frac{\sqrt{41}-6}{5} \cdot \frac{\sqrt{41}+6}{\sqrt{41}+6} = \frac{5}{5(\sqrt{41}+6)} = \frac{1}{\sqrt{41}+6}$

so, no we have :

$x_3 = \sqrt{41} + 6 = \lfloor \sqrt{41} + 6 \rfloor + \frac{1}{x_4} = 12 + \frac{1}{x_4}$

$\frac{1}{x_4} = \sqrt{41} + 6 - 12 = \sqrt{41} - 6 \implies x_4 = \frac{1}{\sqrt{41}-6}$

but $x_4 = \frac{1}{\sqrt{41}-6} \cdot \frac{\sqrt{41}+6}{\sqrt{41}+6} = \frac{\sqrt{41}+6}{5} = x_1$

since $x_4 = x_1$, it is now evident that

$\sqrt{41} = 6 + \frac{1}{x_1} = 6 + \frac{1}{2+\frac{1}{x_2}} = 6 + \frac{1}{2+\frac{1}{2+\frac{1}{x_3}}} = 6 + \frac{1}{2+\frac{1}{2+\frac{1}{12+\frac{1}{x_1}}}}$

so $\sqrt{41} = [6; \overline{2, 2, 12}]$. It has period of length 3. Let us now compute the $3rd$ convergent, C_2.

$$C_2 = 6 + \frac{1}{2+\frac{1}{2}} = 6 + \frac{1}{\frac{5}{2}} = 6 + \frac{2}{5} = \frac{32}{5}$$

Observe that since the solution to the negative Pell Equation $x^2 - 41y^2 = -1$ exists (the length of the period of $\sqrt{41}$ is odd) it is yielded by the $3rd$ convergent

$$(32)^2 - 41(5^2) = 1024 - 1025 = -1$$

To obtain a solution to our initial equation we need to compute the $6th$ convergent, C_5, that is:

$$C_5 = 6 + \cfrac{1}{2 + \cfrac{1}{\cfrac{1}{2+\cfrac{1}{12+\cfrac{1}{2+\frac{1}{2}}}}}} = \frac{2049}{320}$$

to verify that this is indeed a solution

$$(2049)^2 - 41(320^2) = 4,198,401 - 41(102,400) = 4,198,401 - 4,198,400 = 1$$

We can obtain infinitely more solution by taking powers of $(2049+320\sqrt{41})$. The result will be of the form $a + b\sqrt{41}$, in which case $(x, y) = (a, b)$ will be a solution. To try one "small" example we take

$$(2049+320\sqrt{41})^2 = 4,198,401+1,311,360\sqrt{41}+4,198,400 = 8,396,801+1,311,360\sqrt{41}$$

And so

$$(8,396,801)^2 - 41(1,311,360)^2 = 70,506,267,033,601 - 70,506,267,033,600 = 1$$

If we had computed the $12th$ convergent, we notice that it would have been $\frac{8,396,801}{1,311,360}$. In general, to obtain solutions we calculate the $6k\,th$ convergent $\frac{A_{6k}}{B_{6k}}$ and $(x, y) = (A_{6k}, B_{6k})$.

In the next section, we give some problems that can be solved using Pell's equation.

5 Application of Pell's Equation

Pell's equations can be used to solve numerous problems in Number Theory. We give two examples the solutions of which require the use of Pell's equation. The reader is encouraged to solve the two problems as an exercise.

Problem 1: The numbers $1, 3, 6, 10, 15, 21, 28, 36, 45, \ldots, t_n = \frac{1}{2}n(n + 1)$ are called triangular numbers, since the nth number counts the number of dots in an equilateral triangular array with n dots to the side. It happens that some triangular numbers are square. We want to find them or at least generate them.

Solution: The condition that the nth triangular number t_n is equal to the mth square is that $\frac{1}{2}n(n+1) = m^2$. Rewriting that expression, we can put it in the form $(2n+1)^2 - 8m^2 = 1$. Now setting $x = 2n+1$ and $y = m$, we are down to solving the equation $x^2 - 8y^2 = 1$.

Problem 2: The root-mean-square of a set of $\{a_1, \ldots, a_n\}$ of positive integers is equal to

$$\sqrt{\frac{a_1^2 + a_2^2 + \cdots + a_k^2}{k}}.$$

Is the root-mean-square of the first n positive integers ever an integer?.

Solution: The condition on n is that $(n+1)(2n+1) = 6m^2$ for some integer m. We can rewrite that as $(4n+3)^2 - 3(4m)^2 = 1$. Thus, we want to find solutions of $x^2 - 3y^2 = 1$ for which $x+1$ is a multiple of 4. Using the continued fraction expansion of $\sqrt{3}$, we find that (7,4) and (1351,780) as solutions and these solutions lead to $n = 1$ and $n = 337$, respectively. In fact, there are infinitely many such integers n, we can generate them by taking powers of $(7+4\sqrt{3})$ and the resulting $a+b\sqrt{3}$ generates another such n with $(x, y) = (a, b)$.

Many more problems have solutions that can be found by solving a Pell's Equation. Refer to [2] for more problems.

Conclusion

Solving a Pell's Equation using the above method provides not only a powerful tool but a mechanical one. In this way one can instruct a machine to do the computation and would save a lot of computation power compared to trial and error or exhausting a large set of pairs $(x, y) \in \mathbb{Z}^+ \times \mathbb{Z}^+$. We provided a complete worked example as one would do it with a pencil and paper in Example 4.5.

References

[1] Andrew M. Rockett, Peter Szüsz, *Continued fractions*, World Scientific, 1992.

[2] Bardeau, Edward, *Pell's equation*, Springer, 1938.

[3] Gregor Dick, *Pell's Equation and Continued Fractions*.

[4] H. W. Lenstra Jr., *Solving the Pell Equation*, Notices of the AMS, Volume 49, Number 2, 182-192, 2002.

[5] Olds, C.D., *Continued Fractions*, from the *New Mathematical Library*, Random House, 1963