A DIVE INTO PELL'S EQUATION

OSWADLO RAMIREZ,
FALL 2024 PROJECT

21-441, Evan O'Dorney

Contents

1 Introduction

1.1 Definition

Pell's equation take the form [4]:

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

where D is a fixed positive integer and not a perfect square. Now, we can take a solution (x_1, y_1) to the above equation and derive another solution (x_2, y_2). The process is as follows:

$$\begin{aligned}
&1 = x_1^2 - Dy_1^2 \\
\Longrightarrow\ &1 = (x_1 - \sqrt{D}y_1)(x_1 + \sqrt{D}y_1) \\
\Longrightarrow\ &1^2 = (x_1 - \sqrt{D}y_1)^2(x_1 + \sqrt{D}y_1)^2 \\
\Longrightarrow\ &1 = (x_1^2 - 2x_1y_1\sqrt{D} + y_1^2D)(x_1^2 + 2x_1y_1\sqrt{D} + y_1^2D) \\
\Longrightarrow\ &1 = ((x_1^2 + y_1^2D) - 2x_1y_1\sqrt{D})((x_1^2 + y_1^2D) + 2x_1y_1\sqrt{D}) \\
\Longrightarrow\ &1 = (x_1^2 + y_1^2D)^2 - (2x_1y_1\sqrt{D})^2.
\end{aligned}$$

Thus, $(x_2, y_2) = ((x_1^2 + y_1^2D), 2x_1y_1)$ is a new solution. We can repeat this process using different powers to generate infinitely many solutions to a Pell's equation.

1.2 Generating Pell's Equation Solutions Theorem

Theorem 1.1 (Pell's Equation)**.** *Pell's equation have positive integer solutions that are generated by*

$$x_k + y_k\sqrt{D} = (x_1 + y_1\sqrt{D})^k \qquad k = 1, 2, \ldots$$

for D a positive, non-square integer and (x_1, y_1) is a solution with x_1 being the minimal value.

2 Algorithm for Computing Continued Fraction:

2.1 Algorithm Pseudocode

We'll write down an algorithm [3] for computing the continued fraction for $\sqrt{D}$, where D is square-free.

1. Find the nearest square whole number less than D. Let's call this d^2. Then, $d^2 < D$ and $D < (d+1)^2$. Now, we know that $\sqrt{D} = d + \frac{1}{x}$ $(*)$, where x is a natural number. Furthermore, when returning back to step 1, the number d will be useful for finding the integer part of future partial quotients. For example, take $\sqrt{14}$. Then, $d = 3$ so for $\frac{\sqrt{14}+3}{5}$ we get $\frac{\sqrt{14}+3}{5} \approx \frac{3+3}{5} \approx \frac{6}{5}$ and the integer part is easy to see it's 1.

2. Solve for x in the the equation $(*)$ of Step 1. This will look like $\sqrt{D} = d + \frac{1}{x} \iff x = \frac{1}{\sqrt{D}-d}$.

3. Rationalizing the denominator to clear the radical. This is done by multiplying the top and bottom by the conjugate. This will look like $x = \frac{1}{\sqrt{D}-d} \iff x = \frac{\sqrt{D}+d}{D-d^2}$. In the next step, we will either repeat previous steps or terminate. Therefore, we'll split it into two.

4. (a) If the expression in the numerator is one we've seen before, terminate. The continued fraction are the d's that we've computed.
   (b) Start again from Step 1 using the expression derived in Step 3 (i.e., find the integer part of $x = \frac{\sqrt{D}+d}{D-d^2}$ in step 1.)

2.2 Example: Continued Fraction of $\sqrt{14}$

For the first step, we must compute m such that $m^2 < 14$ and $14 < (m+1)^2$. We can easily find m by calculating $\sqrt{14} \approx 3.742$. Then, $m = 3$ and $\sqrt{14} = 3 + \frac{1}{x_1}$. Following Steps 2 and 3, we get $x_1 = \frac{\sqrt{14}+3}{5}$. Using a calculator, we find $\frac{\sqrt{14}+3}{5} \approx 1.348$. Thus, $\frac{\sqrt{14}+3}{5} = 1 + \frac{1}{x_2}$. We repeat the Steps 2 and 3 for x_2. Then, $x_2 = \frac{\sqrt{14}+2}{2} \approx 2.871$ and $\frac{\sqrt{14}+2}{2} = 2 + \frac{1}{x_2}$. After more computations, we get $x_3 = \frac{\sqrt{14}+2}{5}$. We encountered a m that we've seen before, so we've cycled back and can terminate. The continued fraction of $\sqrt{14}$ is

$$3 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \sqrt{14}}}}}.$$

In periodic form, the continued fraction of $\sqrt{14}$ is $[3; \overline{1, 2, 1, 6}]$.

3 Connecting Continued Fractions to Pell's Equation:

3.1 Notation

First, we should introduce some notation, definitions, and Euler's rule. Albeit interesting notation, we'll adopt

$$q_0 + \frac{1}{q_1 +}\frac{1}{q_2 +}\cdots\frac{1}{q_n} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}$$

The bracket notation is $[q_0] = q_0, [q_0, q_1] = q_0 q_1 + 1$ following the recurrence relation: $[q_0, q_1, \ldots, q_n] = q_0[q_1, q_2, \ldots, q_n] + [q_2, q_3, \ldots, q_n]$. The notation helps to express continued fractions:

$$q_0 + \frac{1}{q_1 +}\cdots\frac{1}{q_n} = \frac{[q_0, \ldots, q_n]}{[q_1, \ldots, q_n]}.$$

We'll define the n^{th} convergent of a rational/irrational to be $\frac{A_n}{B_n}$, where $A_n = [q_0, \ldots, q_n]$ and $B_n = [q_1, \ldots, q_n]$. These are given by the recurrence relations

$$A_n = q_n A_{n-1} + A_{n-2}$$
$$B_n = q_n B_{n-1} + B_{n-2}$$

3.2 Euler's rule

Euler's rule states

The numerator A_n is unchanged if the terms are written in reverse order:
$$[q_0, q_1, \ldots, q_n] = [q_n, q_{n-1}, \ldots, q_0]$$

Before proving the rule, let's seen an example. Let's go back to the example of $\sqrt{14}$. As we saw earlier, the continued fraction for $\sqrt{14}$ is $[3;\overline{1,2,1,6}]$. We'll go through a few convergents and see if reversing the order preserves the value of the numerator.

n = 0: This case is uninteresting as there is only value in our continued fraction so it's evident that A_0 is the same forwards and backwards.

n = 1: Now, we have the continued fraction [3; 1]. We want to see if the numerator of [3;1] is the same as the numerator of [1;3]. Let's see.

$$[3; 1] = 3 + \frac{1}{1} = \frac{4}{1}$$

$$[1;3] = 1 + \frac{1}{3} = \frac{4}{3}$$

Both fractions have 4 as the numerator. Nice!

n = 2: Now, we have the continued fraction [3;1,2]. We want to see if the numerator of [3;1,2] is the same as the numerator of [2;1,3]. Let's see.

$$[3;1,2] = 3 + \frac{1}{1+\frac{1}{2}} = 3 + \frac{1}{\frac{3}{2}} = 3 + \frac{2}{3} = \frac{11}{3}$$

$$[2;1,3] = 2 + \frac{1}{1+\frac{1}{3}} = 2 + \frac{1}{\frac{4}{3}} = 2 + \frac{3}{4} = \frac{11}{4}$$

Both fractions have 11 as the numerator. Let's now prove it using **Lemma 1.9** from Donaldson's Continued Fractions.

3.3 Lemma 1.9: Expressing Continued Fractions as Matrix Multiplication

Let $c_1, c_2, \ldots, c_n$ be integers such that the continued fraction $[c_1;c_2,\ldots,c_n]$ exists. Then,

$$\begin{pmatrix} c_1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} c_2 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} c_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \implies [c_1;c_2,\ldots,c_n] = \frac{A}{C}[2].$$

Now, we transpose both sides of the above equation to get

$$\begin{aligned}
&\left(\begin{pmatrix} c_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} c_2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} c_n & 1 \\ 1 & 0 \end{pmatrix}\right)^{\mathsf{T}} = \begin{pmatrix} A & B \\ C & D \end{pmatrix}^{\mathsf{T}} \\
\implies &\begin{pmatrix} c_n & 1 \\ 1 & 0 \end{pmatrix}^{\mathsf{T}} \cdots \begin{pmatrix} c_{n-1} & 1 \\ 1 & 0 \end{pmatrix}^{\mathsf{T}} \begin{pmatrix} c_1 & 1 \\ 1 & 0 \end{pmatrix}^{\mathsf{T}} = \begin{pmatrix} A & B \\ C & D \end{pmatrix}^{\mathsf{T}} \\
\implies &\begin{pmatrix} c_n & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} c_{n-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} c_1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} A & C \\ B & D \end{pmatrix} \\
\implies &[c_n;c_{n-1},\ldots,c_1] = \frac{A}{B}
\end{aligned}$$

Therefore, the numerator A_n remains unchanged if the terms are written in reverse order.

Next, we will characterize quadratic irrationals. For a positive integer D that isn't a square, we have the following definition:

$$\sqrt{D} = q_0, \overline{q_1, q_2, \ldots, q_2, q_1, 2q_0}, \text{ for } q_i \in \mathbb{N}$$

Proof: We shall take these facts for granted (proofs for them are in *The Higher Arithmetic* [1])

1. The continued fraction of a quadratic irrational is unique.
2. The continued fraction of a quadratic irrational becomes periodic after a certain stage.
3. The continued fraction of a quadratic irrational is purely periodic (i.e., periodic from the start) if the quadratic irrational is reduced. Reduced in this context means the quadratic irrational is strictly greater than 1 and its conjugate lies between -1 and 0.

Back to the proof. We know that the continued fraction of $\sqrt{D}$ isn't purely periodic because its conjugate doesn't lie in -1 and 0. However, consider $\sqrt{D} + q_0$, where q_0 is the positive integer part of $\sqrt{D}$. The conjugate, namely $-\sqrt{D} + q_0$ does lie between -1 and 0. Therefore, $\sqrt{D} + q_0$ is purely periodic. This will look like

$$\sqrt{D} + q_0 = 2q_0 + \frac{1}{q_1+} \cdots \frac{1}{q_n+} \frac{1}{2q_0} \cdots$$

Now, $\alpha = \sqrt{D} + q_0$ and its conjugate $\alpha' = -\sqrt{D} + q_0$. The continued fraction for α is $[2q_0, q_1, \ldots, q_n, \alpha]$. We will use this to derive the continued fraction for α'.

$$\alpha = 2q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{q_n + \cfrac{1}{\alpha}}}}}$$

$$\implies \alpha - 2q_0 = \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{q_n + \cfrac{1}{\alpha}}}}} \implies \frac{1}{\alpha - 2q_0} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{q_n + \cfrac{1}{\alpha}}}}$$

Continue solving for $\frac{1}{\alpha}$ to get

$$\frac{1}{\alpha} = -q_n + \cfrac{1}{-q_{n-1} + \cfrac{1}{\ddots + \cfrac{1}{-2q_0 + \alpha}}}.$$

Next, we'll manipulate the above equation to get α' on the left-hand side. Note, $-2q_0 + \alpha = -\alpha'$. Therefore,

$$\frac{1}{\alpha} = -q_n + \cfrac{1}{-q_{n-1} + \cfrac{1}{\ddots + \cfrac{1}{-\alpha'}}}$$

$$\implies \alpha = \cfrac{1}{-q_n + \cfrac{1}{-q_{n-1} + \cfrac{1}{\ddots + \cfrac{1}{-\alpha'}}}} \implies \quad \alpha' = 2q_0 + \cfrac{1}{q_n + \cfrac{1}{q_{n-1} + \cfrac{1}{\ddots + \cfrac{1}{\alpha'}}}}$$

Therefore, the continued fraction of α' is $[2q_0; q_n, \ldots, q_1, \alpha']$. Now, we can use continued fractions of α and its conjugate to derive continued fractions for $\sqrt{D}$ and $-\sqrt{D}$.

$$\sqrt{D} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{\alpha}}}} \text{ and } -\sqrt{D} = q_0 + \cfrac{1}{q_n + \cfrac{1}{q_{n-1} + \cfrac{1}{\ddots + \cfrac{1}{\alpha'}}}} (*)$$

Now, we know that from the continued fraction of α,

$$\alpha = [2q_0; q_1, \ldots, q_n, \alpha].$$

Then, set $x = \alpha$ and simplify the right-hand side to get

$$x = \frac{Ax + B}{Cx + D} \text{ for } A, B, C, D > 0 \text{ because the coefficients are positive.}$$

This then turns into a quadratic equation: $Cx^2 + x(D - A) - B = 0$. We know it has exactly two roots because the discriminant is positive and one of the roots is α. The other root must be the conjugate of α by the quadratic formula. Next, we can swap $-\sqrt{D}$ and $\frac{1}{\alpha'}$ from $(*)$ with $\sqrt{D}$ and $\frac{1}{\alpha}$, respectively, because they're both roots of the same equation. Finally, we use the fact that the continued fraction for quadratic irrationals is unique and conclude $q_n = q_1, q_{n-1} = q_2, \ldots$ and finally get the characterization of $\sqrt{D}$ as we wanted:

$$\sqrt{D} = q_0, \overline{q_1, q_2, \ldots, q_2, q_1, 2q_0}, \text{ for } q_i \in \mathbb{N}$$

Now, we will show the convergent of $\sqrt{D}$ can be used as a solution to a Pell's equation.

3.4 Continued Fractions as a Solution to Pell's Equation

We know that

$$\sqrt{D} = \frac{\alpha_{n+1}A_n + A_{n-1}}{\alpha_{n+1}B_n + B_{n-1}}, \text{ where } \alpha_k \text{ is the } k^{th} \text{ complete quotient in the CF}$$

The equation can be derived from our formulation of CF using the bracket notation and the recurrence relation for the A_n and B_n

Now, since α_{n+1} is the n^{th} complete quotient in the CF, it'll look like this:

$$\alpha_{n+1} = 2q_0 + \frac{1}{q_1+} \cdots = \sqrt{D} + q_0$$

Plugging this equation into the one above, we get

$$\begin{aligned}
&\sqrt{D} = \frac{(\sqrt{D} + q_0)A_n + A_{n-1}}{(\sqrt{D} + q_0)B_n + B_{n-1}} \\
\implies &\sqrt{D}((\sqrt{D} + q_0)B_n + B_{n-1}) = (\sqrt{D} + q_0)A_n + A_{n-1} \\
\implies &DB_n + \sqrt{D}B_n q_0 + \sqrt{D}B_{n-1} = (\sqrt{D} + q_0)A_n + A_{n-1}
\end{aligned}$$

Since $\sqrt{D}$ is irrational, we can derive two equations from the equation above:

$$\begin{aligned}
DB_n = q_0 A_n + A_{n-1} &\implies A_{n-1} = DB_n - q_0 A_n \\
B_n q_0 + B_{n-1} = A_n &\implies B_{n-1} = A_n - B_n q_0
\end{aligned}$$

Using the recurrence relation and using the difference between consecutive convergents, we can derive $A_n B_{n-1} - B_n A_{n-1} = (-1)^{n-1}$. Then, plug in the two equations from above to arrive at

$$\begin{aligned}
&A_n(A_n - B_n q_0) - B_n(DB_n - q_0 A_n) = (-1)^{n-1} \\
\implies &A_n^2 - DB_n^2 = (-1)^{n-1}
\end{aligned}$$

We can note that this in the form of a Pell's equation, and if n is odd, we have a solution. Otherwise, we can square both sides of the equation to derive a solution to the Pell's equation equal to 1.

$$(A_n^2 - DB_n^2)^2 = ((-1)^{n-1})^2 \implies \quad (A_n^2 + B_n^2 D)^2 + D(2A_n B_n)^2 = 1$$

The solution is $(A_n^2 + B_n^2 D, 2A_n B_n)$. This is similar to how we derived other solutions to the Pell's equation in the beginning of the paper.

4 All the Solutions to Pell's Equation come from Continued Fractions

4.1 Convergents to $\sqrt{D}$ are Solutions to Pell's Equation

Assume $A^2 - DB^2 = 1$. Then,

$$
\begin{aligned}
|\frac{A}{B} - \sqrt{D}| &= |\frac{A - B\sqrt{D}}{B}| \\
&= |\frac{(A - B\sqrt{D})(A + B\sqrt{D})}{B(A + B\sqrt{D})}| \\
&= |\frac{A^2 - DB^2}{B(A + B\sqrt{D})}| \\
&= |\frac{1}{B(A + B\sqrt{D})}| \\
&= \frac{1}{B^2(\sqrt{D} + \frac{A}{B})}[6].
\end{aligned}
$$

Since $D > 1$ and $A > B$ ($\frac{A}{B} > 1$), the $\frac{1}{B^2(\sqrt{D}+\frac{A}{B})} < \frac{1}{2B^2}$. By a theorem in Donaldson's Continued Fractions [2], we see that $\frac{A}{B}$ is a convergent to $\sqrt{D}$. Thus, solutions of Pell's equation consist of those convergent to $\sqrt{D}$. Furthermore, we can catch more of those solutions using the formula for generating solutions to Pell's equation.

References

[1] H. Davenport and J.H. Davenport. *The Higher Arithmetic: An Introduction to the Theory of Numbers*. IT Pro. Cambridge University Press, 2008.

[2] Neil Donaldson. Introduction to continued fractions, 2021. Accessed: 2024-12-02.

[3] Ron Knott. The contactron. `https://r-knott.surrey.ac.uk/contactron.html`, 2024. Accessed: 2024-11-18.

[4] L. J. (Louis Joel) Mordell. *Diophantine equations [by] L. J. Mordell.* Pure and applied mathematics (Academic Press) ; 30. Academic P., London, 1969.

[5] J.H. Silverman. *A Friendly Introduction to Number Theory: Pearson New International Edition*. Pearson Education, 2013.

[6] SEUNG HYUN YANG. Continued fractions and pell's equation, 2008. Accessed: 2024-12-03.