BINARY TREES AND SUM OF TWO SQUARES

Hongshen Chua
Puchong, Selangor, Malaysia
hschua0622@hotmail.com

Received: 8/14/25, Accepted: 5/23/26, Published: 6/8/26

Abstract

In this paper, we introduce a matrix-based binary tree that forms the foundation of both the Stern–Brocot and Calkin–Wilf trees. We then explore its connection to continued fractions. Building on this relationship, we provide a path-based representation of Brillhart's proof of the sum of two squares.

1. Introduction

When it comes to binary trees of rational numbers, there are two that stand out in particular, namely the Stern–Brocot tree (Figure 1) and the Calkin–Wilf tree (Figure 2).

Both trees start with the number 1 at the 0-th level. The $(i+1)$-th level of the Stern-Brocot tree is generated from two adjacent terms, a_1/b_1 and a_2/b_2, on the i-th level by computing their mediant, $(a_1+a_2)/(b_1+b_2)$. In contrast, to construct the Calkin–Wilf tree, we take a vertex a/b at the i-th level, then set its left child as $a/(a+b)$ and its right child as $(a+b)/b$.

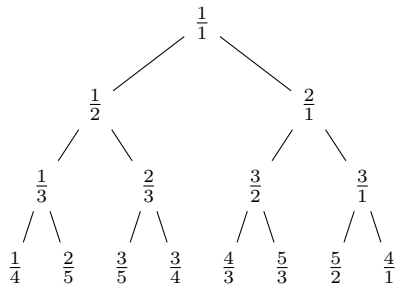

Figure 1: Stern–Brocot tree

DOI: 10.5281/zenodo.20597662

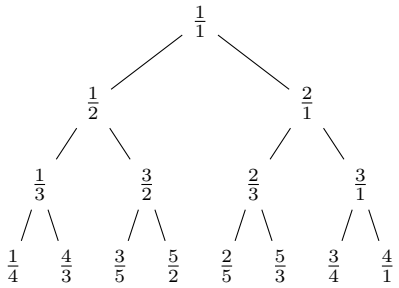

Figure 2: Calkin–Wilf tree

Both trees appear quite similar, so it is perhaps unsurprising that they are closely related. In fact, Backhouse and Ferreira [1] described a remarkable matrix-based binary tree that naturally generates both the Stern–Brocot and Calkin–Wilf trees. We will explore this construction in more detail in Section 2.

The matrix binary tree also integrates seamlessly with the theory of continued fractions. The convergents of a continued fraction can be derived from a matrix similar to the one we use to generate our tree. Consequently, these convergents can be represented as paths through the matrix binary tree. This will be the focus of Section 3.

Finally, Brillhart wrote a brief note [2] presenting a proof of Fermat's famous theorem on the sum of two squares. The main idea of his method relies on continued fractions. Our path-based approach offers a new interpretation of his proof, which we will present in Section 4.

2. Binary Trees

First, we construct a matrix binary tree that underlies both the Stern–Brocot and Calkin–Wilf trees. Starting with the 2×2 identity matrix, a right (R) and a left (L) move correspond to post-multiplication by the matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, respectively. Alternatively, an R-move can be thought of as adding the left column to the *right* column, while an L-move involves adding the right column to the *left* column. By repeatedly applying these moves, we can construct the matrix binary tree shown in Figure 3.

From the matrix binary tree, we can easily recover the Stern–Brocot and Calkin–Wilf trees. By post-multiplying each matrix by $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$, which is equivalent to adding the columns together, we obtain the Stern–Brocot tree (Figure 1). On the other hand, if we pre-multiply each matrix by $\begin{pmatrix} 1 & 1 \end{pmatrix}$, which corresponds to adding the

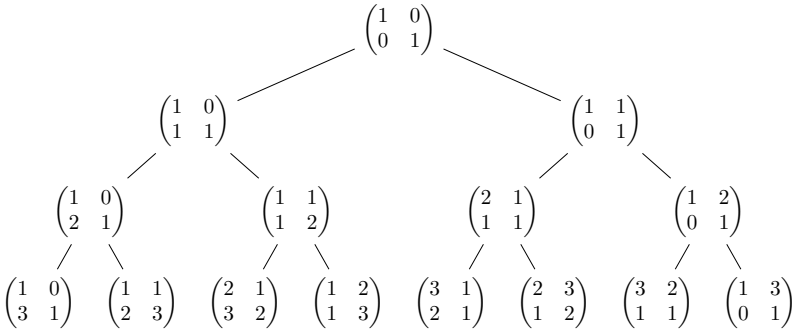

Figure 3: Matrix binary tree

rows together, we get the Calkin–Wilf tree (Figure 2).

3. Continued Fraction

Let $[q_0; q_1, q_2, \ldots]$ represent the continued fraction

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots}}.$$

The *n-th convergent* A_n/B_n of a continued fraction is the fraction obtained by truncating the continued fraction at q_n, i.e., $A_n/B_n = [q_0; q_1, q_2, \ldots, q_n]$. These convergents are related by the following linear recurrences:

$$A_n = q_n A_{n-1} + A_{n-2} \quad \text{and} \quad B_n = q_n B_{n-1} + B_{n-2},$$

with the initial values $A_{-1} = 1$, $A_0 = q_0$, $B_{-1} = 0$, and $B_0 = 1$.

The matrix binary tree provides a powerful representation of the convergents. Given a continued fraction $[q_0; q_1, q_2, \ldots]$, we define a path W through the tree by starting with q_0 R-moves, followed by q_1 L-moves, and so on, alternating the direction after each term. By an abuse of notation, we write $R = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $L = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, and the matrix corresponding to the path W as $R^{q_0} L^{q_1} \ldots$. This path produces the convergents, as demonstrated in the next theorem.

Theorem 1. *Let A_n/B_n be the n-th convergent of a continued fraction $[q_0; q_1, q_2, \ldots]$.*

If a path $W_n = R^{q_0}L^{q_1}\ldots$ ends with an R-move, then

$$W_n = \begin{pmatrix} A_{n-1} & A_n \\ B_{n-1} & B_n \end{pmatrix}.$$

Otherwise, if W_n ends with an L-move, then

$$W_n = \begin{pmatrix} A_n & A_{n-1} \\ B_n & B_{n-1} \end{pmatrix}.$$

Proof. A quick calculation shows that consecutive R or L moves have a simple matrix representation of

$$R^q = \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad L^q = \begin{pmatrix} 1 & 0 \\ q & 1 \end{pmatrix}.$$

We proceed by induction. For the base case of $n = 0$, we have

$$W_0 = R^{q_0} = \begin{pmatrix} 1 & q_0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} A_{-1} & A_0 \\ B_{-1} & B_0 \end{pmatrix}.$$

Next, it is simple to verify that

$$A_1 = q_1A_0 + A_{-1} = q_0q_1 + 1 \quad \text{and} \quad B_1 = q_1B_0 + B_{-1} = 1.$$

Hence, for the case $n = 1$, we compute

$$R^{q_0}L^{q_1} = \begin{pmatrix} 1 & q_0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ q_1 & 1 \end{pmatrix} = \begin{pmatrix} q_0q_1 + 1 & q_0 \\ q_1 & 1 \end{pmatrix} = \begin{pmatrix} A_1 & A_0 \\ B_1 & B_0 \end{pmatrix}.$$

This completes the base cases for $n = 0$ and $n = 1$.

Now, suppose the result holds for all $n \le N$ for some $N \ge 1$. We prove it for $n = N + 1$. If W_{N+1} ends with an R-move, then W_N must have ended with an L-move. By the inductive hypothesis, we get

$$W_{N+1} = \begin{pmatrix} A_N & A_{N-1} \\ B_N & B_{N-1} \end{pmatrix}\begin{pmatrix} 1 & q_{N+1} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} A_N & q_{N+1}A_N + A_{N-1} \\ B_N & q_{N+1}B_N + B_{N-1} \end{pmatrix}.$$

Using the recurrence relation for convergents, the last matrix simplifies to

$$W_{N+1} = \begin{pmatrix} A_N & A_{N+1} \\ B_N & B_{N+1} \end{pmatrix}.$$

On the other hand, if W_{N+1} ends with an L-move, then W_N must have ended with an R-move, so

$$W_{N+1} = \begin{pmatrix} A_{N-1} & A_N \\ B_{N-1} & B_N \end{pmatrix}\begin{pmatrix} 1 & 0 \\ q_{N+1} & 1 \end{pmatrix} = \begin{pmatrix} q_{N+1}A_N + A_{N-1} & A_N \\ q_{N+1}B_N + B_{N-1} & B_N \end{pmatrix}.$$

Again, the recurrence relation for convergents yields

$$W_{N+1} = \begin{pmatrix} A_{N+1} & A_N \\ B_{N+1} & B_N \end{pmatrix}.$$

This completes the induction step, and hence the proof. □

4. Sum of Two Squares

In a letter to Mersenne, Fermat stated that any prime p of the form $4k+1$ can be written as a sum of two squares [4]. However, like many of his conjectures, Fermat did not provide a proof for this result. The first complete proof was given by Euler, using the method of infinite descent, a technique, rather fittingly, invented by Fermat.

Our approach is inspired by Brillhart's excellent note [2] on this subject. First, we find a solution x_0 to the congruence $x^2 \equiv -1 \pmod{p}$, where $0 < x_0 < p/2$. Such a solution always exists as -1 is a quadratic residue modulo p. Specifically, $(-1 \mid p) = (-1)^{(p-1)/2} = 1$, where $(\cdot \mid p)$ denotes the Legendre symbol modulo p.

Once we have chosen our x_0, a result from Perron states that the continued fraction of p/x_0 has a particularly neat structure.

Lemma 1 ([6])**.** *The continued fraction of p/x_0 has an even number of terms and is palindromic, i.e.,*

$$p/x_0 = [q_0, q_1, \ldots, q_n, q_n, \ldots, q_1, q_0].$$

So far, our proof follows Brillhart's approach, but this is the point where we diverge. Rather than working with continuants, consider the path

$$W = R^{q_0} L^{q_1} \ldots S^{q_n} S^{q_n} \ldots R^{q_1} L^{q_0},$$

where S is either R or L, depending on whether n is odd or even. Since the path W ends with an L-move, Theorem 1 tells us that

$$W = \begin{pmatrix} p & * \\ x_0 & * \end{pmatrix}.$$

On the other hand, let $M = R^{q_0-1} L^{q_1} \ldots S^{q_n} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where a, b, c, and d are integers. Since $R = L^T$, we have $W = RMM^TL$. The middle term MM^T evaluates to

$$MM^T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} a^2+b^2 & ac+bd \\ ac+bd & c^2+d^2 \end{pmatrix}.$$

Therefore, we have

$$RMM^TL = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^2+b^2 & ac+bd \\ ac+bd & c^2+d^2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

which simplifies to

$$W = \begin{pmatrix} (a+c)^2+(b+d)^2 & (a+c)c+(b+d)d \\ (a+c)c+(b+d)d & c^2+d^2 \end{pmatrix}.$$

Comparing both expressions for W yields

$$p = (a+c)^2 + (b+d)^2.$$

Thus, we conclude the following theorem.

Theorem 2. *If a prime p has the form $4k+1$, then p is a sum of two squares.*

Remark 1. We also have the relation $x_0 = (a+c)c + (b+d)d$.

An advantage of this method is that we can explicitly identify the two squares that make up the sum. The numbers $(a+c)$ and $(b+d)$ correspond to the path M^T applied to the matrix $\begin{pmatrix}1\\1\end{pmatrix}$. Hence, we can state the following theorem.

Theorem 3. *If the fraction x/y corresponds to the path M^T in the Stern–Brocot tree, then $p = x^2 + y^2$.*

Remark 2. The same holds for the Calkin–Wilf tree, but with the path M instead.

Acknowledgement. We thank the anonymous referee for helpful suggestions that improved this paper.

References

[1] R. Backhouse and J. Ferreira. Recounting the rationals: Twice! *International Conference on Mathematics of Program Construction* **5133** (2008), 79–91.

[2] J. Brillhart. Note on representing a prime as sum of two squares. *Math. Comp.* **26**(120) (1972), 1011–1013.

[3] F. Clarke, N. Everitt, L. Littlejohn, and R. Vorster. H. J. S. Smith and the Fermat two squares theorems. *Amer. Math. Monthly* **106**(7) (1999), 652–665.

[4] L. Dickson. *History of the Theory of Numbers*. Chelsea, New York, 1919.

[5] J. Ferreira and A. Mendes. A calculational approach to path-based properties of the Eisenstein–Stern and Stern–Brocot trees via matrix algebra. *J. Log. Algebr. Methods Program.* **85**(5) (2015), 906–920.

[6] O. Perron. *Die Lehre von den Kettenbrüchen*. Chelsea, New York, 1950.