Continued Fraction Factorisation Method

Mircea Măierean

January 12, 2025

Abstract

This paper presents the required steps for finding a factor of a number using the Continued Fraction Method (CFRAC). Initially, the theoretical aspects of the method are presented, followed by an exemplification on a natural number.

Contents

1 Definitions

In this section, we will define some of the terms that will be used across this paper, as well as their corresponding notations

Definition 1.1. A continued fraction is of the form

$$x = \frac{q_0}{q_1 + \frac{1}{q_2 + \frac{1}{q_3 \cdots}}} \tag{1}$$

We can also identify continued fractions in sequence form as

$$x = [q_0; q_1, q_2, \ldots], q_i \in \mathbb{Z}, i \in \mathbb{N}$$

The above is as an example of an *infinite continued fraction*; a *finite continued fraction in sequence form is*

$$x = [q_0; q_1, q_2, \ldots, q_n], n \in \mathbb{N}, q_i \in \mathbb{Z}, i = \overline{1, n}$$

Definition 1.2. The k-th convergent of a finite continued fraction is $[q_0; q_1, q_2 \ldots q_k], k \in \mathbb{N}$

Definition 1.3. A *periodic infinite continued fraction* corresponds to an irrational number x, where $x = [q_0; q_1, q_2 \ldots q_j, \overline{q_{j+1}, q_{j+2}, \ldots q_{j+p}}$. Here, p denotes the periodicity of the terms repeated.

Definition 1.4. Let N be a positive integer that is not a square. The n-th complete quotient of x_n, where x_n is the n-th convergent of $\sqrt{N}$ is defined as

$$x_n = \begin{cases} \sqrt{N}, & \text{if } n = 0, \\ \frac{1}{x_{i-1} - q_{i-1}}, & \text{if } n \geq 1. \end{cases} \tag{2}$$

With respect to x_n, $q_n = \lfloor x_n \rfloor$

Definition 1.5. Let P and Q be 2 sequences defined by the following recurrences:

$$P_n = \begin{cases} 0, & \text{if } n = 0, \\ q_0, & \text{if } n = 1, \\ q_{n-1}Q_{n-1} - P_{n-1}, & \text{if } n \geq 2. \end{cases} \tag{3}$$

$$Q_n = \begin{cases} 1, & \text{if } n = 0, \\ N - q_0^2, & \text{if } n = 1, \\ Q_{n-2} + (P_{n-1} - P_n)q_{n-1}, & \text{if } n \geq 2. \end{cases} \tag{4}$$

Definition 1.6. Let $(-1)^n Q_n = Q_n^*$. Two Q_n^*'s are equivalent if their product is a square, that is, Q_i^* is equivalent to Q_j^* if $x^2 Q_i^* = y^2 Q_j^*$, for $x, y \in \mathbb{Z}$

2 Theorems

In this section, the theorems that are used will be listed below, with their proper citations.

Theorem 2.1. *For a positive non-square integer N, the period starts after the first term in the continued fraction for $\sqrt{N}$, i.e $\sqrt{N} = [q_0; \overline{q_1, q_2, \ldots, q_{p-1}, 2q_0}]$. Moreover, the sequence $q_1, q_2, \ldots, q_{p-1}$ has the property that $q_{p-i} = q_i, i = \overline{1, p-1}$ [1]*

3 Propositions

Proposition 3.1. For any positive integer N that is not a square, the statement:

$$A(n) : N = P_n^2 + Q_n Q_{n-1}, \forall n \in \mathbb{N}^* \tag{5}$$

is always true

Proof. This statement will be proven using mathematical induction.
Base case: Let $n = 1$.
We check that the statement holds for $n = 1$:

$$A(1) : N = P_1^2 + Q_1 Q_0 = q_0^2 + N - q_0^2 = N.$$

Thus, the base case holds.

Inductive Step:
Assume that the statement holds for some arbitrary k, i.e.,

$$A(k) : N = P_k^2 + Q_k Q_{k-1}.$$

We need to show that $A(k+1)$ also holds:

$$A(k+1) : N = P_{k+1}^2 + Q_{k+1}Q_k.$$

Based on the statements, we have:

$$P_k^2 + Q_kQ_{k-1} = P_{k+1}^2 + Q_{k+1}Q_k \iff$$

$$P_k^2 - P_{k+1}^2 = Q_{k+1}Q_k - Q_kQ_{k-1} \iff$$
$$(P_k - P_{k+1})(P_k + P_{k+1}) = Q_k(Q_{k+1} - Q_{k-1}) \iff$$
$$(P_k - P_{k+1})q_kQ_k = Q_k(Q_{k+1} - Q_{k-1}) \iff$$
$$(P_k - P_{k+1})q_k = Q_{k+1} - Q_{k-1} \iff$$
$$(P_k - P_{k+1})q_k = Q_{k-1} + (P_k - P_{k+1})q_k - Q_{k-1} \iff$$
$$(P_k - P_{k+1})q_k = (P_k - P_{k+1})q_k.$$

Since this holds for any $k \in \mathbb{N}$, the inductive step is proven.

By the principle of mathematical induction, the statement $A(n)$ holds for all $n \geq 1$. □

Proposition 3.2. For any positive integer N that is not a square, the statement:

$$B(n) : x_n = \frac{\sqrt{N} + P_n}{Q_n}, \forall n \in \mathbb{N} \tag{6}$$

is always true

Proof. This statement will be proven using mathematical induction.

Base case: Let $n = 0$.
We check that the statement holds for $n = 0$:

$$B(0) : x_0 = \frac{\sqrt{N} + P_0}{Q_0} = \frac{\sqrt{N} + 0}{1} = \sqrt{N}$$

Thus, the base case holds.

Inductive Step:
Assume that the statement holds for some arbitrary k, i.e.,

$$B(k) : x_k = \frac{\sqrt{N} + P_k}{Q_k}.$$

We need to show that $B(k+1)$ also holds:

$$B(k+1) : x_{k+1} = \frac{\sqrt{N} + P_{k+1}}{Q_{k+1}}.$$

From the definition of x, we have:

$$x_{k+1} = \frac{1}{x_k - q_k} \iff$$

$$x_{k+1} = \frac{1}{\frac{\sqrt{N}+P_k}{Q_k} - q_k} \iff$$

$$x_{k+1} = \frac{1}{\frac{\sqrt{N}+P_k-q_kQ_k}{Q_k}} \iff$$

$$x_{k+1} = \frac{Q_k}{\sqrt{N}-(q_kQ_k-P_k)} \iff$$

$$x_{k+1} = \frac{Q_k}{\sqrt{N}-P_{k+1}} \iff$$

$$x_{k+1} = \frac{Q_k(\sqrt{N}+P_{k+1})}{N-P_{k+1}^2}$$

Based on **Proposition 3.1**, $N - P_{k+1}^2 = Q_k * Q_{k+1}$, thus resulting in

$$x_{k+1} = \frac{Q_k(\sqrt{N}+P_{k+1})}{Q_k * Q_{k+1}} \iff$$

$$x_{k+1} = \frac{\sqrt{N}+P_{k+1}}{Q_{k+1}}$$

Since this holds for any $k \in \mathbb{N}$, the inductive step is proven.

By the principle of mathematical induction, the statement $B(n)$ holds for all $n \geq 0$. □

Proposition 3.3. The P Method

For any positive integer N that is not a square, the statement:

$$C(n) : (-1)^n Q_n(P_{n-1}P_{n-3}P_{n-5}\dots P_r)^2 \equiv (P_nP_{n-2}P_{n-4}\dots P_s)^2 \pmod{N}, \tag{7}$$

where $r = 1$ and $s = 2$ if n is even and reversed otherwise, is always true, $\forall n \in \mathbb{N}^*$

Proof. This statement will be proven using mathematical induction.

From **(5)**, we have

$$-Q_nQ_{n-1} \equiv P_n^2 \pmod{N}$$

Base case: Let $n = 1$.
We check that the statement holds for $n = 1$:

$$C(1) : -Q_1 \equiv P_1^2 \pmod{N} \iff -Q_1Q_0 \equiv P_1^2 \pmod{N} \iff q_0^2 - N \equiv q_0^2 \pmod{N}$$

Thus, the base case holds.

Inductive Step:
Assume that the statement holds for some arbitrary k, i.e.,

$$C(k) : (-1)^k Q_k(P_{k-1}P_{k-3}P_{k-5}\dots P_r)^2 \equiv (P_kP_{k-2}P_{k-4}\dots P_s)^2 \pmod{N},$$

We need to show that $C(k+1)$ also holds:

$$C(k+1) : (-1)^{k+1} Q_{k+1}(P_kP_{k-2}P_{k-4}\dots P_s)^2 \equiv (P_{k+1}P_{k-1}P_{k-3}\dots P_r) \pmod{N},$$

$$(-1)^k Q_k(P_{k-1}P_{k-3}P_{k-5}\dots P_r)^2 \equiv (P_kP_{k-2}P_{k-4}\dots P_s) \pmod{N} \iff$$

$$(-1)^{k+1} Q_{k+1}Q_k(P_{k-1}P_{k-3}P_{k-5}\dots P_r)^2 \equiv -Q_{k+1}(P_kP_{k-2}P_{k-4}\dots P_s)^2 \pmod{N} \iff$$

$$-Q_{k+1}(P_kP_{k-2}P_{k-4}\dots P_s)^2 \equiv (-1)^k(-Q_{k+1}Q_k)(P_{k-1}P_{k-3}P_{k-5}\dots P_r)^2 \pmod{N} \iff$$

$$-Q_{k+1}(P_kP_{k-2}P_{k-4}\dots P_s)^2 \equiv (-1)^k(P_{k+1}P_{k-1}P_{k-3}P_{k-5}\dots P_r)^2 \pmod{N} \iff$$

$$(-1)^{k+1} Q_{k+1}(P_kP_{k-2}P_{k-4}\dots P_s)^2 \equiv (P_{k+1}P_{k-1}P_{k-3}P_{k-5}\dots P_r)^2 \pmod{N}$$

Since this holds for any $k \in \mathbb{N}^*$, the inductive step is proven.

By the principle of mathematical induction, the statement $C(n)$ holds for all $n \geq 1$. □

4 Finding the factors

The assigned number is $N = 7861$. For this number, we will compute the corresponding values for q_n, P_n and $Q_n^* \pmod N$, using equations (2), (3), (4). Initially, we need to compute $q_0 = \lfloor\sqrt{n}\rfloor = \lfloor\sqrt{7861}\rfloor = 88$. The values obtained are:

n	P_n	Q_n^*	q_n
0	0	1	88
1	88	-117	1
2	29	60	1
3	31	-115	1
4	84	7	24
5	84	- 115	1
6	31	60	1
7	29	-117	1
8	88	1	176
9	88	-117	1
10	29	60	1
11	31	-115	1
12	84	7	24
13	84	-115	1
14	31	60	1
15	29	-117	1
16	88	1	176
17	88	-117	1
18	29	60	1
19	31	-115	1
20	84	7	24
21	84	-115	1
22	31	60	1
23	29	-117	1
24	88	1	176
25	88	-117	1
26	29	60	1
27	31	-115	1

Table 1: Table of values for P_n, Q_n^*, q_n, and corresponding results.

Since 7861 is a positive integer that is not a square, based on **(2.1)**, we can represent it as a ***periodic infinite continued fraction***:

$$7861 = [88; \overline{1, 1, 1, 24, 1, 1, 1, 176}]$$

Moreover, we observe that, after the $8th$ iteration, 176 appears, which is exactly $2 * 88$. We can stop iterating after this value appears, as everything will be repeated, but for the purpose of visualizing data we have iterated a few more steps.

The goal now is to obtain 2 squares that have the same congruence mod N, which can lead to a possible solution. **(7)** provides in its corresponding equation already a square on both sides as a factor. Unfortunately, none of the values for Q^* are squares, so we will try to find 2 equations, i, j such that $Q_i^* Q_j^*$ will also form a square.

Looking at Table 1, Q_3^* and Q_5^*, besides having the same parity for their indexes, they have the same sign, so we obtain:

$$Q_3^* P_2^2 \equiv (P_3 P_1)^2 \pmod N$$

and

$$Q_5^* (P_4 P_2)^2 \equiv (P_5 P_3 P_1)^2 \pmod N$$

Multiplying these 2 equations, a new congruence is obtained:

$$(115 P_4 P_2^2)^2 \equiv (P_5 P_3^2 P_1^2)^2 \pmod N$$

Let $t_1 = 115 P_4 P_2^2$ and $t_2 = P_5 P_3^2 P_1^2$.

$$t_1 = 8124060 \longrightarrow t_1^2 = 66000350883600 \longrightarrow t_1^2 \equiv 7658 \pmod{7861}$$

$$t_2 = 625126656 \longrightarrow t_2^2 = 390783336041742336 \longrightarrow t_2^2 \equiv 7658 \pmod{7861}$$

The previous relation can be written as well as $(t_1 + t_2) * (t_2 - t_1) \equiv 0 \pmod N$. One of the $\gcd(t_1 + t_2, N)$ and $\gcd(t_2 - t_1, N)$ might be a proper factor of N. We will compute them accordingly.

$$\gcd(t_1 + t_2, N) = \gcd(8124060 + 625126656, 7861) = \gcd(633250716, 7861) = 7861$$

which is not a proper factor, since it is equal to N.

$$\gcd(t_2 - t_1, N) = \gcd(617002596, 7861) = 7$$

which corresponds to a proper factor.

Moreover, we can find the other factor as well, $\frac{7861}{7} = 1123$, which is also a prime number.

Concluding, $7861 = 7 * 1123$

If we would have obtained both values of the gcd's invalid, then we would have needed to retry the whole process, by selecting different equations for Q_i^* and Q_j^*.

5 Conclusion

In this paper, we have applied the theoretical aspects of **The P Method** for finding the factors of 7861. We have found that $7 * 1123 = 7861$.

References

[1] H. E. Rose, *A Course in Number Theory*, Oxford Science Publications, 2nd Edition, pg. 130, 1994.