CONTINUED FRACTIONS

Anay Garodia
Euler Circle
Kolkata WB 700106, IND
agarodia98@gmail.com

August 18, 2024

ABSTRACT

In this expository paper, we discuss continued fractions and their significant applications in cryptography, focusing particularly on the Continued Fraction Factorization Algorithm (CFRAC). The CFRAC algorithm leverages the properties of continued fractions to factor integers of up to 50 digits, posing a potential threat to cryptographic systems like RSA, which depend on the difficulty of factoring large numbers. We explore the mathematical underpinnings of continued fractions, providing rigorous proofs and examples, and demonstrate how the CFRAC algorithm utilizes these properties to achieve efficient factorization.

1 Introduction

The CFRAC algorithm is a powerful tool for integer factorization, crucial for understanding the security of cryptographic systems. The RSA encryption system, among others, relies heavily on the difficulty of factoring large composite numbers into primes. By exploiting properties of continued fractions, the CFRAC algorithm provides an efficient method for factorizing numbers, particularly those with up to 50 digits. In this paper, we delve into the mathematical concepts underlying continued fractions and their application in the CFRAC algorithm, offering formal proofs and illustrative examples.

2 Fundamental Concepts

Definition 2.1. (Continued Fraction) A continued fraction is an expression of the form:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}$$

where $a_0 \in \mathbb{Z}$ and $a_i \in \mathbb{Z}^+$ for $i \geq 1$. The terms $a_0, a_1, \ldots, a_n$ are called the partial denominators of the continued fraction.

Theorem 2.2. *(Representation of Rational Numbers) Any rational number can be represented as a finite continued fraction.*

Proof. Let $x \in \mathbb{Q}$ be a rational number such that $x = \frac{p}{q}$, where $p, q \in \mathbb{Z}$ and $q > 0$. We can express x in the form $x = a_0 + \frac{1}{x_1}$ where $a_0 = \lfloor x \rfloor$ and $x_1 = \frac{1}{x - a_0}$. The process can be iterated to express x_1 as a continued fraction, and so on, until the remainder is zero. Since the remainder eventually becomes zero (because x is rational), this process terminates after a finite number of steps, resulting in a finite continued fraction representation. ■

Consider the rational number $\frac{487}{165}$. We can find its continued fraction representation by performing the Euclidean algorithm:

$$487 = 2 \times 165 + 157$$

$$165 = 1 \times 157 + 8$$

$$157 = 19 \times 8 + 5$$

$$8 = 1 \times 5 + 3$$

$$5 = 1 \times 3 + 2$$

$$3 = 1 \times 2 + 1$$

$$2 = 2 \times 1 + 0$$

Thus, the continued fraction representation is $[2; 1, 19, 1, 1, 1, 2]$.

Theorem 2.3. *(Uniqueness of Continued Fractions) The continued fraction representation of a rational number is unique.*

Proof. Suppose a rational number $x = \frac{p}{q}$ has two different continued fraction representations. Consider the representations $x = [a_0; a_1, a_2, \ldots, a_n]$ and $x = [b_0; b_1, b_2, \ldots, b_m]$, where a_i, b_i are integers. We assume without loss of generality that $a_0 = b_0$ and $n < m$. Then we have:

$$[a_1, a_2, \ldots, a_n] = [b_1, b_2, \ldots, b_m].$$

By expanding the continued fractions, this would imply:

$$\frac{p}{q} = \frac{p'}{q'}$$

where $p, p' \in \mathbb{Z}$ and $q, q' \in \mathbb{Z}^+$, leading to a contradiction unless $p = p'$ and $q = q'$. Hence, the continued fraction representation is unique. ■

Theorem 2.4. *(The Approximation Property of Continued Fractions) The continued fraction representation of a real number α provides the best rational approximations to α among all rational numbers with denominators not exceeding the denominator of the convergent.*

Proof. Let $\alpha = [a_0; a_1, a_2, \ldots]$ be the continued fraction expansion of α. The convergents $C_n = \frac{p_n}{q_n}$ are defined by the recurrence relations:

$$p_n = a_n p_{n-1} + p_{n-2}, \quad q_n = a_n q_{n-1} + q_{n-2},$$

with initial conditions $p_{-1} = 1$, $p_0 = a_0$, $q_{-1} = 0$, $q_0 = 1$.

Suppose there exists a rational number $\frac{p}{q}$ with $0 < q \leq q_n$ such that:

$$\left| \alpha - \frac{p}{q} \right| < \left| \alpha - \frac{p_n}{q_n} \right|.$$

This would imply that $|q_n \alpha - p_n|$ is not minimized by $\frac{p_n}{q_n}$, contradicting the fact that the continued fraction convergents minimize the expression:

$$|q\alpha - p|$$

for any rational approximation $\frac{p}{q}$ with $0 < q \leq q_n$. Therefore, the convergents provide the best approximations. ■

3 Convergents as Best Rational Approximations

Convergents of continued fractions in CFRAC provide good approximations to $\sqrt{N}$. They're used to efficiently generate congruences of the form $x^2 \equiv y^2 \pmod{N}$, which can lead to factor pairs $(x+y, x-y)$ of N when combined.

Definition 3.1. (Convergent) Given a continued fraction $\alpha = [a_0; a_1, a_2, \ldots]$, the nth convergent is defined as:

$$\frac{p_n}{q_n} = [a_0; a_1, \ldots, a_n]$$

where p_n and q_n are determined by the recursive relations:

$$p_n = a_n p_{n-1} + p_{n-2}, \quad q_n = a_n q_{n-1} + q_{n-2}$$

with initial conditions $p_{-1} = 1$, $p_0 = a_0$, $q_{-1} = 0$, and $q_0 = 1$.

Consider the continued fraction representation of $\pi = [3; 7, 15, 1, 292, \ldots]$. The first few convergents are:

$$\frac{22}{7}, \quad \frac{333}{106}, \quad \frac{355}{113}$$

The convergent $\frac{355}{113}$ provides an accurate approximation of π, as $\pi \approx 3.141592653\ldots$ and $\frac{355}{113} \approx 3.141592920\ldots$.

Theorem 3.2. *(Convergents as Best Approximations) Let $[a_0; a_1, a_2, \ldots]$ be the continued fraction expansion of a real number α. Then the convergents $\frac{p_n}{q_n}$ are the best rational approximations of α, meaning that for any $\frac{p}{q} \neq \frac{p_n}{q_n}$ with $0 < q \leq q_n$, we have:*

$$\left|\alpha - \frac{p_n}{q_n}\right| < \left|\alpha - \frac{p}{q}\right|.$$

Proof. Consider the continued fraction expansion of α, and let the nth convergent be given by $C_n = \frac{p_n}{q_n}$. By properties of continued fractions, we have the recursive relations:

$$p_n = a_n p_{n-1} + p_{n-2}, \quad q_n = a_n q_{n-1} + q_{n-2}.$$

The difference between α and its convergent is:

$$\left|\alpha - \frac{p_n}{q_n}\right| = \left|\frac{(\alpha q_n - p_n)}{q_n}\right|$$

By the recurrence relation and properties of continued fractions, we know:

$$|\alpha q_n - p_n| = \frac{1}{q_{n+1}}$$

Thus,

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n q_{n+1}}$$

Suppose there exists another rational approximation $\frac{p}{q}$ with $0 < q < q_n$ such that:

$$\left|\alpha - \frac{p}{q}\right| < \left|\alpha - \frac{p_n}{q_n}\right|$$

Then, we have:

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q_n q_{n+1}}$$

implying:

$$|q\alpha - p| < \frac{q}{q_n q_{n+1}}$$

which contradicts the minimality of $|\alpha q_n - p_n| = \frac{1}{q_{n+1}}$. Hence, the convergents are indeed the best approximations. ■

4 Periodic Continued Fractions and Quadratic Irrationals

Periodic continued fractions and quadratic irrationals play a crucial role in the CFRAC algorithm. In CFRAC, we work with the continued fraction expansion of $\sqrt{N}$, where N is the number to be factored. $\sqrt{N}$ is a quadratic irrational when N is not a perfect square. Importantly, the continued fraction expansion of $\sqrt{N}$ is always periodic when N is not a perfect square. This periodicity is crucial for the efficiency of CFRAC, as it allows for efficient computation of convergents. These convergents provide good rational approximations to $\sqrt{N}$, which are used to generate congruences of squares modulo N. The periodicity ensures a steady supply of these congruences, which are key to finding factors of N.

Definition 4.1. (Quadratic Irrational) A quadratic irrational is a number of the form $\alpha = \frac{P+\sqrt{D}}{Q}$, where P, Q, D are integers, D is not a perfect square, and the gcd of P, Q is 1.

Theorem 4.2. *(Periodic Continued Fraction) The continued fraction expansion of a quadratic irrational is periodic.*

Proof. Let $\alpha = \frac{P+\sqrt{D}}{Q}$ be a quadratic irrational. Consider the continued fraction expansion of α:

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

We express α as:

$$\alpha = a_0 + \frac{1}{\alpha_1}$$

where $a_0 = \lfloor \alpha \rfloor$ and $\alpha_1 = \frac{1}{\alpha - a_0}$. Substituting, we have:

$$\alpha_1 = \frac{Q}{\sqrt{D} - (P - a_0 Q)}$$

This form:

$$\alpha_1 = \frac{P_1 + \sqrt{D}}{Q_1}$$

is another quadratic irrational, similar to α. The sequence of quadratic irrationals generated by this process is finite due to a limited number of possible values for P, Q. Therefore, the continued fraction eventually repeats, leading to periodicity. ■

Consider $\sqrt{3}$. Its continued fraction is:

$$\sqrt{3} = 1 + (\sqrt{3} - 1) \Rightarrow a_0 = 1$$

Calculate:

$$\frac{1}{\sqrt{3} - 1} = \frac{\sqrt{3} + 1}{2} = 1 + \frac{\sqrt{3} - 1}{2}$$

Thus, the continued fraction expansion of $\sqrt{3}$ is:

$$\sqrt{3} = [1; \overline{1, 2}]$$

The periodicity after the first term confirms the repeating pattern.

5 The Continued Fraction Factorization Algorithm (CFRAC)

CFRAC uses continued fractions to find numbers a and b such that $a^2 \equiv b^2 \pmod{N}$, aiding integer factorization.

Definition 5.1. (Quadratic Residue) A number a is a quadratic residue modulo N if there exists an integer x such that:

$$x^2 \equiv a \pmod{N}$$

If no such x exists, a is a quadratic non-residue modulo N.

For $N = 15$, quadratic residues are $0, 1, 4, 9, 10$ from squares $0, 1, 2, 3, 4$ modulo 15.

Continued Fraction Factorization Algorithm (CFRAC)

Input: A composite number N.

Output: A non-trivial factor of N.

Steps: 1. Compute the continued fraction expansion of $\sqrt{N}$. 2. Use convergents $\frac{p_k}{q_k}$ to find integers x_k and y_k such that:

$$x_k^2 \equiv y_k \pmod{N}$$

where $x_k = p_k$ and $y_k = p_k^2 - q_k^2 N$. 3. For each k, check if y_k is a perfect square. If so, set $b_k = \sqrt{y_k}$. 4. Attempt to factor N using:

$$\gcd(x_k - b_k, N)$$

If unsuccessful, continue with the next convergent.

Theorem 5.2. *(CFRAC Success) CFRAC factors a composite number N using continued fractions and quadratic residues.*

Proof. CFRAC finds $x^2 \equiv y^2 \pmod{N}$. This implies:

$$(x - y)(x + y) \equiv 0 \pmod{N}$$

Thus, $N \mid (x - y)(x + y)$, and $\gcd(x - y, N)$ or $\gcd(x + y, N)$ reveals a non-trivial factor if $x - y$ or $x + y$ is not a multiple of N.

CFRAC relies on the property that continued fraction convergents of $\sqrt{N}$ satisfy:

$$p_k^2 \equiv y_k \pmod{N}$$

This exploits periodicity in quadratic irrationals to efficiently identify k where y_k is a perfect square, leading to successful factorization. ■

Example: Factor $N = 899$ using CFRAC.

1. Compute $\sqrt{899} \approx 29.9833$, yielding continued fraction: $[29; 1, 1, 5, \ldots]$.

2. Convergents: $\frac{p_0}{q_0} = \frac{29}{1}$, $\frac{p_1}{q_1} = \frac{30}{1}$, $\frac{p_2}{q_2} = \frac{59}{2}$

3. For $\frac{p_2}{q_2} = \frac{59}{2}$: $x_2 = 59$, $y_2 = 59^2 - 2^2 \times 899 = 3481 - 3596 = -115$

Since y_2 is not a perfect square, we continue to the next convergent.

4. For $\frac{p_3}{q_3} = \frac{89}{3}$: $x_3 = 89$, $y_3 = 89^2 - 3^2 \times 899 = 7921 - 8091 = -170$

Again, y_3 is not a perfect square.

5. For $\frac{p_4}{q_4} = \frac{504}{17}$: $x_4 = 504$, $y_4 = 504^2 - 17^2 \times 899 = 254016 - 259911 = -5895 = 3^2 \times 5 \times 131$

Here, y_4 is not a perfect square, but it's divisible by a perfect square (3^2). We can use this.

6. Set $x = 504$ and $y = 3 \times \sqrt{5 \times 131} = 3 \times 26 = 78$.

7. Now we have $x^2 \equiv y^2 \pmod{N}$, or $504^2 \equiv 78^2 \pmod{899}$.

8. Calculate: $\gcd(x - y, N) = \gcd(504 - 78, 899) = \gcd(426, 899) = 29$ $\gcd(x + y, N) = \gcd(504 + 78, 899) = \gcd(582, 899) = 31$

9. We have found the factors of N: $899 = 29 \times 31$.

6 Conclusion

This paper explores the mathematical foundation of continued fractions and their application in cryptography, focusing on the CFRAC algorithm. Continued fractions provide powerful tools for rational approximation and integer factorization, relevant to cryptographic security. CFRAC's ability to factor large numbers highlights potential risks to systems relying on the difficulty of factorization, emphasizing the importance of research in this area.

Through rigorous proofs and examples, we demonstrate CFRAC's effectiveness and dependence on continued fraction properties. The paper underscores understanding and advancing mathematical techniques to protect cryptographic systems from computational threats. Future work involves exploring efficient algorithms and strengthening protocols to mitigate vulnerabilities exposed by factorization methods like CFRAC.

References

[1] L. Euler, *Introductio in Analysin Infinitorum*, vol. I, 1748.

[2] D. H. Lehmer and R. E. Powers, "On Factoring Large Numbers," *Bull. Amer. Math. Soc.*, vol. 37, no. 10, pp. 770–776, 1931, doi: 10.1090/S0002-9904-1931-05271-X.

[3] M. A. Morrison and J. Brillhart, "A Method of Factoring and the Factorization of F7," *Math. Comput.*, vol. 29, no. 129, pp. 183–205, Jan. 1975, American Mathematical Society, doi: 10.2307/2005475.

[4] W. B. Jones and W. J. Thron, *Continued Fractions: Analytic Theory and Applications*, vol. 11, Encyclopedia of Mathematics and its Applications, Reading, MA: Addison-Wesley, 1980, ISBN: 0-201-13510-8.

[5] M. S. Frey, "Factoring Large Numbers with Continued Fractions," Undergraduate honors thesis, University of Redlands, 2009. [Online]. Available: `https://core.ac.uk/download/pdf/217142258.pdf`.

[6] A. Ya. Khinchin, *Continued Fractions*, University of Chicago Press, 1964 [Originally published in Russian, 1935], ISBN: 0-486-69630-8.

[7] E. W. Weisstein, "Periodic Continued Fraction," *MathWorld*, 2022. [Online]. Available: `https://mathworld.wolfram.com/PeriodicContinuedFraction.html`. [Accessed: Apr. 26, 2022].