A Novel Factorization Method Using Continued Fractions

Malshi Vinodya
Department of Mathematics
Faculty of Science
University of Peradeniya
Kandy, Sri Lanka
s18545@sci.pdn.ac.lk

Rajitha Ranasinghe
Department of Mathematics
Faculty of Science
University of Peradeniya
Kandy, Sri Lanka
rajithamath@sci.pdn.ac.lk

***Abstract*— The study of continued fractions is a significant area of mathematics with diverse applications, particularly in the field of factorization. Continued fractions can be used to approximate irrational numbers and are integral to algorithms for factoring integers. In this study, we present a novel method for factoring large integers that utilize generalized continued fractions to improve efficient factorization. Additionally, we introduce several theoretical statements about generalized continued fractions and demonstrate their application within the proposed factorization algorithm. Using this algorithm, we successfully factor a large integer into two prime numbers, whose product constitutes the original large number. Our findings suggest that this method is a highly effective tool in number theory, cryptography, and computational mathematics.**

Keywords—continued fractions, generalized continued fractions, integer factorization, prime numbers

I. Introduction

Integer factorization is the decomposition of a positive integer into a product of integers. The study of integer factorization has a very long history and the studies have a wide range of applications. Although there are many different integer factorization algorithms to choose from, we will focus on integer factorization method by using continued fractions called as CFRAC algorithm. First, CFRAC algorithm was founded by D. H. Lehmer and R. E. Powers in 1931, and developed as a computer algorithm by Michael A. Morrison and John Brillhart in 1975. The CFRAC algorithm has the ability to factor integers that are fifty digits or less. In the present study, we will describe a method of factoring large integers by using generalized continued fractions, it is a generalization of regular continued fractions in canonical form. Before we start looking at this algorithm, we will explore the theoretical foundations of generalized continued fractions.

Definition 1.1.
A generalized continued fraction is an expression of the form,

$$x = b_0 + \cfrac{a_1}{b_1 + \cfrac{a_2}{b_2 + \cfrac{a_3}{b_3 + \cfrac{a_4}{b_4 + \ddots}}}} \qquad (1)$$

where $a_k (k > 0)$are the partial numerators, b_k $(k > 0)$ are the partial denominators, and the leading term b_0 is called the integer part of the continued fraction.

Generalized continued fractions may also be written in the forms

$$x = b_0 + \frac{a_1}{b_1 +} \frac{a_2}{b_2 +} \cdots \qquad (2)$$

or

$$x = b_0 + \sum_{k=1}^{\infty} \frac{a_k}{b_k} \qquad (3)$$

For any k, a natural number, k th convergent of (1) is given by,

$$C_k = \frac{A_k}{B_k} = b_0 + \frac{a_1}{b_1 +} \frac{a_2}{b_2 +} \cdots \frac{a_k}{+b_k} \qquad (4)$$

Definition 1.2.
The partial denominators of the fractions' successive convergents are related by the fundamental recurrence formulas:

$$A_k = b_k A_{k-1} + a_k A_{k-2} \qquad (5)$$

$$B_k = b_k B_{k-1} + a_k B_{k-2} \qquad (6)$$

for $k \geq 1$ with initial values,

$A_{-1} = 1$ $\qquad$ $A_0 = b_0$

$B_{-1} = 0$ $\qquad$ $B_0 = 1$

Theorem 1.1.
Suppose N is a positive integer which is not a perfect square with convergent $\frac{A_k}{B_k}$ .Then,

$$A_k^2 > 2\sqrt{N} \ (\text{mod } N) \qquad (7)$$

This theorem is one of the reasons why this algorithm works.[6]

Theorem 1.2.
If N is a composite integer, $X, Y \in \mathbb{Z}$ and $X^2 \equiv Y^2 (\text{mod } N)$, but $X \not\equiv \pm Y (\text{mod } N)$, then $\gcd(X - Y, N)$ and $\gcd(X + Y, N)$ are proper factors of N. [2]

The n^{th} root of any positive number z^m can be expressed by restating $z = x^n + y$, resulting in,

$$\sqrt[n]{z^m} = \sqrt[n]{(x^n + y)^m}$$

$$= x^m + \cfrac{my}{nx^{n-m} + \cfrac{(n-m)y}{2x^m + \cfrac{(n+m)y}{3nx^{n-m} + \cfrac{(2n-m)y}{2x^m + \ddots}}}} \quad (8)$$

The square root of z is a special case with $m = 1$ and $n = 2$. So,

$$\sqrt{z} = \sqrt{x^2 + y} = x + \cfrac{y}{2x + \cfrac{y}{2x + \cfrac{3y}{6x + \cfrac{3y}{2x + \ddots}}}} \quad (9)$$

which can be simplified as,

$$\sqrt{z} = \sqrt{x^2 + y} = x + \cfrac{y}{2x + \cfrac{y}{2x + \cfrac{y}{2x + \cfrac{y}{2x + \ddots}}}} \quad (10)$$

II. METHODOLOGY

To factor a number $N(> 1)$, the first step is to determine whether N is a perfect square or a prime power. If N is a perfect square, we can find the factors by getting the square root of N. In the case of N being a prime power, it can be expressed as $N = p^k$, where p is a prime number and k is a positive integer. Then, assess whether N is odd or even. If N is even, repeatedly factor out 2 until the number is odd. Hence, we can write N as $N = 2^k q$, where k is a positive integer and q is odd. Therefore, we consider N is an odd, composite integer that is not a perfect square or prime power.

We start by expanding $\sqrt{N}$ as,

$$\sqrt{N} = \sqrt{x^2 + y} = x + \cfrac{y}{2x + \cfrac{y}{2x + \cfrac{y}{2x + \cfrac{y}{2x + \ddots}}}} \quad (11)$$

where x, y be positive integers, x be the largest integer less than $\sqrt{N}$ and y is not a multiple of x. If y is a multiple of x, say $y = kx$, then we can write

$$\sqrt{N} = \sqrt{x^2 + kx} = \sqrt{x(x + k)} \quad (12)$$

Hence, we can factor N as, $N = x(x + k)$.

Therefore, we consider y as not a multiple of x. By looking at (5), we can define A_k as the numerator of the k th convergent and that A_k is dependent upon $a_k, b_k, A_{k-1}, A_{k-2}$. These A_k terms represent the possible values for X and thus A_k^2 modulo N represents the possible values for Y^2, from which we can computer A_k term of the k th convergent $\frac{A_k}{B_k}$ of the generalized continued fraction expansion of $\sqrt{N}$.

By considering the expressions (1) and (11), we obtain $a_k = y, b_k = 2x$ for all $k = 1,2,3, \dots$ and $b_0 = x$. Next, we construct a table with $a_k,\ b_k,\ A_k(\text{mod } N)$ and $A_k^2(\text{mod } N)$ terms.

Note that,

$$A_k(\text{mod } N) \neq \sqrt{A_k^2(\text{mod } N)} \quad (13)$$

For the corresponding k value that satisfies the previous steps, let

$$X = A_k(\text{mod } N) \quad (14)$$

then we obtain

$$X^2 \equiv Y^2(\text{mod } N)$$

So,

$$Y^2 = A_k^2(\text{mod } N) \quad (15)$$

If $X \equiv Y(\text{mod } N)$, then, a new $A_k^2(\text{mod } N)$ value needs to be found. Otherwise, we can find the factors of N.

If $X \not\equiv Y(\text{mod } N)$ and $X + Y \neq N$, then we can get factors of N by calculating,

$$\gcd\,(X + Y, N)$$

and

$$\gcd\,(X - Y, N).$$

III. RESULTS AND DISCUSSION

Consider an example to find the factors of an integer.

Let $N = 10123$ and we can find the generalized continued expansion of $\sqrt{N}$ in the form,

$$\sqrt{N} = \sqrt{10123} = \sqrt{100^2 + 123}$$

$$= 100 + \cfrac{123}{200 + \cfrac{123}{200 + \cfrac{123}{200 + \cfrac{123}{200 + \ddots}}}}$$

From the given expression we can deduce that $x = 100$ and $y = 123$. Thus, we obtain $a_k = 123$, $b_k = 200$ for all $k = 1,2,3, \dots$ with $b_0 = 100$.

Hence, we can write A_k term as,

$$A_k = 200A_{k-1} + 123A_{k-2} \text{ for } k = 1,2,3 \dots$$
$$A_0 = 100$$
$$A_{-1} = 1$$

We will compute the $A_k(\text{mod } N)$ and $A_k^2(\text{mod } N)$ values until the value of $A_k^2(\text{mod } N)$ is conformed as a perfect square.

We construct a table as follows.

TABLE I. CONTINUED FRACTION FOR $\sqrt{10123}$

$\boldsymbol{k}$	$\boldsymbol{a_k}$	$\boldsymbol{b_k}$	$\boldsymbol{A_k}(\mathbf{mod}\ \boldsymbol{N})$	$\boldsymbol{A_k^2}(\mathbf{mod}\ \boldsymbol{N})$
0	-	100	100	10000
1	123	200	10000	5006
2	123	200	7946	1765
3	123	200	5006	5611
4	123	200	4573	8334
5	123	200	1765	7464
6	123	200	4409	3121
7	123	200	5611	791
8	123	200	4335	3937
9	123	200	8334	1653
10	123	200	3314	9264
11	123	200	7464	4427
12	123	200	7421	2121
13	123	200	3121	2315
14	123	200	8410	8822
15	123	200	791	8178
16	123	200	8239	6406
17	123	200	3937	1656
18	123	200	9026	8895
19	123	200	1653	9322
20	123	200	3332	7416
21	123	200	9264	9025

Examining the values in the table, we observe that when $k = 21$, the corresponding $A_k^2(\text{mod } N)$ value yields a perfect square.

So, when $k = 21$,

$$A_k^2(\text{mod } N) = 9025 = (\pm 95)^2$$

Then, we will verify whether $A_k(\text{mod } N) \neq \sqrt{A_k^2(\text{mod } N)}$

Since, $A_k(\text{mod } N) = 9264$,

$$A_k(\text{mod } N) \neq \sqrt{A_k^2(\text{mod } N)} \quad \text{when } k = 21$$

Let

$$X = 9264 \ (\text{mod } 10123)$$

and

$$Y^2 = 9025 = (\pm 95)^2 \ (\text{mod } 10123)$$

This implies $Y = \pm 95 \ (\text{mod } 10123)$

Also, we can observe that $X \neq Y(\text{mod } 10123)$ and $X + Y \ \neq 10123$

Therefore, we can find the factors of $N = 10123$ by calculating $\gcd(X + Y, N)$ and $\gcd(X - Y, N)$.

$$\begin{aligned} \gcd(X + Y, N) &= \gcd(9264 + 95, 10123) \\ &= \gcd\ (9359, 10123) \\ &= 191 \end{aligned}$$

and

$$\begin{aligned} \gcd(X - Y, N) &= \gcd(9264 - 95, 10123) \\ &= \gcd\ (9169, 10123) \\ &= 53 \end{aligned}$$

Therefore,

$$N = 10123 = 191 \times 53.$$

Recall that we are trying to solve $X^2 \equiv Y^2(\text{mod } N)$ where $X \neq Y(\text{mod } 10123)$. In this algorithm, we utilize the numerators of the convergent to represent values for X .The numerator of the convergent squared is going to be greater than $-2\sqrt{N}$ and less than $2\sqrt{N}$ according to the theorem 1.1. This bounding is significant, because this will in turn create smaller prime. We could have to attempt to determine the prime factorization of a large number if we did not have this constraint. In general, this is an issue because factoring a large number is quite challenging. Hence, this simplification is the key to the overall effectiveness of the factorization process.

IV. CONCLUSION

In this research, we developed a factorization algorithm based on generalized continued fractions. As an application, this can be utilized to effectively decrypt messages encoded using cryptographic algorithms such as RSA encryption. This algorithm not only offers a practical and straightforward approach for small-scale cases but is also designed to be easily understood and implemented. For future enhancements, we plan to implement the algorithm in a programming language and conduct comprehensive testing across a diverse range of integers, from small to large. Furthermore, we will compare the efficiency of our algorithm with other established factorization techniques, thereby contributing valuable insights to the field of cryptography.

REFERENCES

[1] D. M. Burton, “Elementary Number Theory”, 7th Edition, McGraw-Hill, 2010.

[2] J. P. Hii, “Continued fraction factorization algorithm”, Cross-section, (XIII), ANU Student Journals, 2022.

[3] K. H. Rosen, “Elementary Number Theory”, Pearson Education, London, 2011.

[4] M. Anselm and S. H. Weintraub, “A generalization of continued fractions”, Journal of Number Theory 131(12), pp.2442-2460, 2011.

[5] M. A.. Morrison and J. Brillhart, “A method of factoring and factorization of F7,” Mathematical of computation, American Mathematical Society, 1975.

[6] M. S. Ferey, “Factoring large numbers with continued fractions” (University of Redlands), 2009.

[7] S. Farhangi, “What is the continued fraction factoring method? (Ohio State University), 2018.

[8] S. Kadyrov, F. Mashurov, “Generalized continued fraction expansions for π and e”, Journal of Discrete Mathematical Science and Cryptography, 24(6), pp.1809-1819, 2021.