Article

Cracking Factorization- Cryptography Challenges

Asset Durmagambetov * and Aslan Durmagambetov

Posted Date: 5 April 2024

doi: 10.20944/preprints202404.0125.v3

Keywords: Decryption; factorization problem; gradient descent algorithm; new method for solving; transition from algebraic methods to approaches based on functional analysis

 doi:10.20944/preprints202404.0125.v3

Article

Cracking Factorization - Cryptography Challenges

Asset Durmagambetov * and Aslan Durmagambetov

L.N. Gumilyov Eurasian National University aset.durmagambet@gmail.com
* Correspondence: aset.durmagambet@gmail.com; Tel.: +77787286399

Abstract: This article introduces a novel methodology for addressing the factorization problem, pivoting from traditional algebraic techniques to differential analysis through the application of the gradient descent algorithm. By integrating concepts of differential analysis, this method marks a significant leap in efficiency and methodological approach compared to previously established methods. The core of this transition lies in the utilization of gradient descent—a cornerstone of differential analysis—which optimizes the factorization process by iteratively moving towards the minimum of a function that represents the problem at hand. The adoption of differential analysis not only enhances the problem-solving efficiency but also broadens the horizon for applying advanced computational algorithms. This approach enables the exploration of intricate differential properties of the factorization process, facilitating a deeper understanding and more refined solutions. Furthermore, the application of differential analysis paves the way for leveraging the rich toolkit of calculus and numerical methods, offering robust frameworks for analyzing and solving complex factorization problems. By emphasizing the gradient descent algorithm, this methodology underscores the potential of differential analysis in transforming the computational strategies used in factorization. It opens new avenues for research, inviting further exploration of differential techniques and their applications in optimization and beyond. This innovative approach not only contributes to the advancement of mathematical theory but also has practical implications for fields where factorization plays a critical role, offering more efficient and sophisticated solutions to longstanding challenges.

Keywords: decryption; factorization problem; gradient descent algorithm; new method for solving; transition from algebraic methods to approaches based on functional analysis

---

1. Introduction

The factorization problem, involving finding the prime factors of a composite number, is one of the fundamental challenges in the field of cryptography and number theory. This problem has gained widespread attention due to its application in the RSA encryption algorithm, proposed by Rivest, Shamir, and Adleman [1]. The complexity of the factorization task underlies the security of many cryptographic systems.

In recent years, several methods have been proposed to solve the factorization problem. For instance, the quadratic sieve algorithm and the number field sieve method [2] demonstrate high efficiency when dealing with numbers of a specific size. However, despite their success, they face significant computational limitations as the size of the input data increases.

With the development of quantum technologies, new interest has arisen in factorization algorithms specifically designed for quantum computers. Shor's algorithm [3], proposed in 1994, is one such example, demonstrating the theoretical possibility of solving the factorization task in polynomial time on a quantum computer.

In this work, we propose an innovative approach to the factorization problem, utilizing the gradient descent method, which, we hope, will open new horizons in the research of this area [4,5].

2. Problem Formulation

Our research results show that applying gradient descent—a method widely used in functional analysis—to the factorization problem is not only feasible but also leads to significant improvements in efficiency compared to traditional algebraic approaches. This discovery underscores the importance of transitioning to functional methods in studying and solving the factorization problem. The task

 doi:10.20944/preprints202404.0125.v3

of factorization involves finding the prime factors of a given composite number. This task remains computationally challenging, especially for large numbers, making it one of the main problems in contemporary cryptography. Traditionally, the problem of number factorization was considered purely an algebraic task. In this work, we propose a new formulation for it using the following function:

$$f(x) = \frac{M}{x} - \left\lfloor \frac{M}{x} \right\rfloor$$

where M is a composite number, and then the task of finding factors turns into a task of searching for the minima of this function.

3. Results

Here, we consider the gradient descent method, which allows for effectively finding the prime factors of a number. Consider the function:

$$f(x) = \frac{M}{x} - \left\lfloor \frac{M}{x} \right\rfloor \tag{1}$$

Theorem 1. *Let M be a composite integer,*
then the zeros of $f(x)$ determine the factors of the number M
$f(x)$ is infinitely differentiable in the intervals between local minima.

Proof. The proof follows from the fact that when $f(x)$ is nullified, the number

$$\frac{M}{x} = \left\lfloor \frac{M}{x} \right\rfloor$$

from which it follows that

$$y = \frac{M}{x}$$

is an integer. And since

$$y \cdot x = M$$

we obtain the integer factors of the number M. Infinite differentiability follows from the infinite differentiability of the function $\{x\}$. □

4. Data Analysis and Visualization

In this section, we present the main numerical methods used for analyzing the factorization task, as well as the visualization of the obtained results. An important part of the research is the application of the gradient descent method to find local minima of the function $f(x) = \frac{M}{x} - \left\lfloor \frac{M}{x} \right\rfloor$, which allows us to visually demonstrate the effectiveness of the proposed approach to factorization.

Theorem 2. *If M is a composite number, then for the derivative within the smoothness intervals, it is valid that:*

$$\frac{df(x)}{dx} = -\frac{M}{x^2} \tag{2}$$

$$\frac{{x_0}^2}{M} < (x_1 - x_0) < \frac{{x_1}^2}{M} \tag{3}$$

$$(x_1 - x_0) = \frac{{x_0}^2}{M} + O\left(\frac{{x_0}^3}{M}\right) \tag{4}$$

 doi:10.20944/preprints202404.0125.v3

Proof. The proof follows direct verification within the smoothness interval. The graphs show that the distance between adjacent zeros changes slightly at small x. Let's estimate more precisely, calculate the difference in function values at the point of local maximum x_0 and at the point of local minimum x_1, and use Lagrange's Theorem, which asserts that there exists a point $x_0 < \theta < x_1$ such that:

$$1 - 0 = f(x_0) - f(x_1) = \frac{df(x)}{dx}\Big|_\theta (x_1 - x_0) = -\frac{M}{\theta^2}(x_1 - x_0)$$

$$\frac{\theta^2}{M} = (x_1 - x_0)$$

$$\frac{{x_0}^2}{M} < (x_1 - x_0) < \frac{{x_1}^2}{M}$$

The second equation follows upon examining the decomposition into higher order components. □

Theorem 3. *If M is a composite number, then the number of intervals is estimated by:*

$$N < M^{5/8} + \sqrt{M} \tag{5}$$

Proof. Consider the segments

$$[\sqrt{M}, M^{5/8}], [M^{5/8}, M^{3/4}], [M^{3/4}, M]$$

Count the number of intervals between local extrema for each separate segment,

within the first segment, we can take the actual number of points on this segment, which significantly exceeds the number of intervals. On the second segment, consider that according to Theorem 4.3, the length of an interval is determined by the formula

$$\frac{{x_0}^2}{M} < (x_1 - x_0) < \frac{{x_1}^2}{M} \tag{6}$$

therefore, the number of intervals is estimated by the formula $M^{3/4-2/8}$ since the distance between adjacent extrema is greater than $M^{2/8}$ and correspondingly, on the last segment, the distance between extrema is greater than $\sqrt{M}$, therefore the number of intervals between adjacent extrema is less than $\frac{M}{\sqrt{M}} = \sqrt{M}$

$$N < M^{5/8} - \sqrt{M} + M^{3/4-2/8} + M^{1-1/2}$$

$$N < M^{5/8} - \sqrt{M} + M^{1/2} + M^{1-1/2} < M^{5/8} + \sqrt{M}$$

from which we derive the theorem's statement. □

The obtained result shows that such an approach is feasible, but at this stage, it only demonstrates the idea. Let's move on to more substantial applications of this idea.

Theorem 4. *If $M = pq > 1000$ and $p > q + 1000$, where p and q are prime numbers, then there exists an optimal algorithm that reroutes in 1000 steps.*

Proof. Let

$$x_i = \left\{ \frac{M}{i} \right\} \tag{7}$$

Consider intervals $i << \sqrt{M}/4$; this is possible because $p > \sqrt{M}$ and we choose

$$i < \frac{\sqrt{M}}{2}$$

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 April 2024 doi:10.20944/preprints202404.0125.v3

$$x_i = \left\{ \frac{pq}{p+i-p} \right\} = \left\{ \frac{pq}{p(i/p-1)} \right\} = \left\{ \frac{q}{(i/p-1)} \right\}$$

$$x_i = \left\{ \frac{pq}{p+i-p} \right\} = \left\{ \frac{q}{(i/p-1)} \right\} = -\left\{ q(i/p+1) + O((i/p)^2) \right\}$$

$$x_i = -\left\{ \frac{iq}{p} + O((i/p)^2) \right\} = \left\{ i\frac{q}{p} + O((i/p)^2) \right\} = 1 - \frac{q}{p} + O((i/p)^2)$$

from which we have a monotonically linearly decreasing sequence. By calculating the slope $\frac{q}{p}$, we obtain a value, as a result, we get a system of equations

$$pq = M, \quad \frac{p}{q} = C \tag{8}$$

from which we derive the statement of the theorem. □

This is significantly better than the sieve method and other algebraic methods. Below are graphs 1 and 2 demonstrating the analyzed function and the distribution of distances between its local maxima and minima. These graphs are important for visualizing the behavior of the function and confirming the efficiency of the proposed method. According to Theorem 4.2 and Theorem 4.3, we have the ability to control intervals and construct fast algorithms for computing local minima.

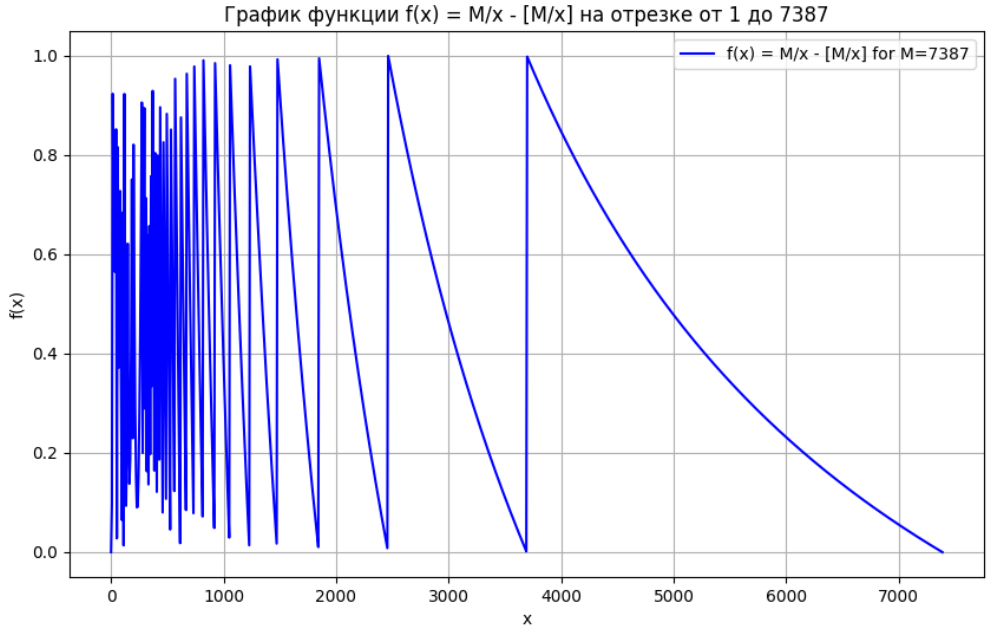

Figure 1. Graph of the function $f(x)$ highlighting local maxima and minima.

 doi:10.20944/preprints202404.0125.v3

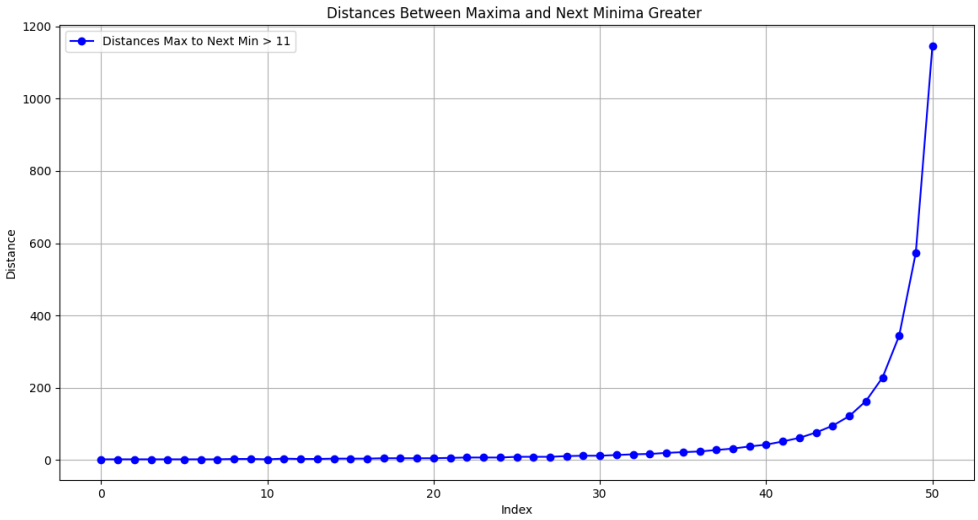

Figure 2. Distances between maxima and the following minima, greater than a given threshold.

5. Conclusion

The course of this research marked an important transition in understanding the factorization task: from a traditional algebraic approach to one based on principles of functional analysis. This paradigm shift allows us to consider the factorization task not just as a search for numerical solutions, but as an optimization problem in a multidimensional functional space. Such an approach opens doors for the use of powerful functional analysis methods and accompanying computational algorithms, which was successfully demonstrated using the gradient descent method. In conclusion, the approach to factorization through gradient descent and its interpretation within the framework of functional analysis open new horizons for research and development in the fields of mathematics, cryptography, and computational technology. We expect that our research will make a significant contribution to the scientific community and stimulate further work in this direction. Data analysis and visualization are key aspects of this research, allowing not only to confirm theoretical assumptions but also to visually demonstrate the advantages of the proposed method.

References

1. Rivest, R. L., Shamir, A., & Adleman, L. "A method for obtaining digital signatures and public-key cryptosystems." *Communications of the ACM*, vol. 21, no. 2, 1978, pp. 120-126.
2. Lenstra, A. K., Lenstra, H. W., Manasse, M. S., & Pollard, J. M. "The number field sieve." *Proceedings of the twenty-second annual ACM symposium on Theory of computing*, 1990, pp. 564-572.
3. Shor, P. W. "Algorithms for quantum computation: Discrete logarithms and factoring." *Proceedings 35th annual symposium on foundations of computer science*, 1994, pp. 124-134.
4. Overmars, Anthony and Venkatraman, Sitalakshmi. "Mathematical Attack of RSA by Extending the Sum of Squares of Primes to Factorize a Semi-Prime." *Math. Comput. Appl.*, vol. 25, no. 4, 2020, p. 63. https://doi.org/10.3390/mca25040063
5. Overmars, Anthony and Venkatraman, Sitalakshmi. "New Semi-Prime Factorization and Application in Large RSA Key Attacks." *J. Cybersecur. Priv.*, vol. 1, no. 4, 2021, pp. 660–674. https://doi.org/10.3390/jcp1040033