Decryption of Factorization - Cryptography Challenges

Asset Durmagambetov * and Aslan Durmagambetov

Posted Date: 2 April 2024

doi: 10.20944/preprints202404.0125.v1

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

Article

Decryption of Factorization - Cryptography Challenges

Asset Durmagambetov [1,*] and Aslan Durmagambetov [2]

[1] L.N. Gumilyov Eurasian National University
[2] Ministry of Energy of the Republic of Kazakhstan; TristesUrsi@gmail.com
* Correspondence: aset.durmagambet@gmail.com

Abstract: This article presents a description of a new method for solving the factorization problem, based on the gradient descent algorithm. This approach demonstrates significant improvements in efficiency compared to traditional methods proposed in previous research. This article describes a new method for solving the factorization problem, based on the gradient descent algorithm, and demonstrates the transition from algebraic methods to approaches based on functional analysis. The proposed approach not only improves the efficiency of solving the problem but also allows the application of computational algorithms of functional analysis, opening new possibilities for research and optimization.

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

---

1. Introduction

The problem of factorization, which involves finding the prime factors of a composite number, is one of the foundational 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. 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 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 specially developed for quantum computers. Shor's algorithm, proposed in 1994, is one such example, showing 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.

2. Problem Formulation

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

The factorization task consists of finding the prime factors of a given composite number. This task remains computationally complex, 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:

$$f(x) = M/x - [M/x]$$

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

 doi:10.20944/preprints202404.0125.v1

3. Results

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

$$f(x) = M/x - [M/x] \tag{1}$$

Theorem 1. *Let M be an integer composite number,*
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

$$M/x = [M/x]$$

from which it follows that

$$y = M/x$$

is an integer. And since

$$y * x = M$$

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 the analysis of 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 for finding local minima of the function $f(x) = \frac{M}{x} - \lfloor \frac{M}{x} \rfloor$, 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 intervals of smoothness, the following is valid:*

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

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

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

Proof. The proof follows directly from inspection within the interval of smoothness. The graphs show that the distance between adjacent zeros changes slightly at small x, we estimate more precisely, we calculate the difference in the values of the function at the point of local maximum x_0 and at the point of the local minimum x_1 and use Lagrange's Theorem, that there exists a point $x_0 < \theta < x_1$ it holds that

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

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

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

 doi:10.20944/preprints202404.0125.v1

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

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

$$N < cM^{1/4} \tag{5}$$

Proof. According to Theorem 2,
we can consider

$$(x_{i+1} - x_i) = \frac{{x_i}^2}{M} + O\left(\frac{{x_0}^3}{M}\right) \tag{6}$$

as a numerical approximation of the equation

$$\frac{dx}{dt} = \frac{x^2}{M} \tag{7}$$

with the initial condition

$$x\Big|_{t=0} = x_0,\ x_0 > 0 \tag{8}$$

assuming the solution reaches the level $M^{1/2}$ and solving approximately, we get

$$N < cM^{1/4}$$

□

Our assumption that $L < M^{1/2}$, where L is the length of the search area, is based on the fact that all solutions lie in this area, which is obvious, as violating this condition immediately yields a factor smaller than $M^{1/2}$. Thus, the factorization task is reduced to analyzing less than $N < cM^{1/4}$, which is significantly better than the sieve method and other algebraic methods. Below are graphs that demonstrate the analyzed function and the distribution of distances between its local maxima and minima. These graphs are crucial for visualizing the behavior of the function and confirming the effectiveness of the proposed method. According to Theorems 2 and 3, we have the ability to control intervals and construct fast algorithms for computing local minima.

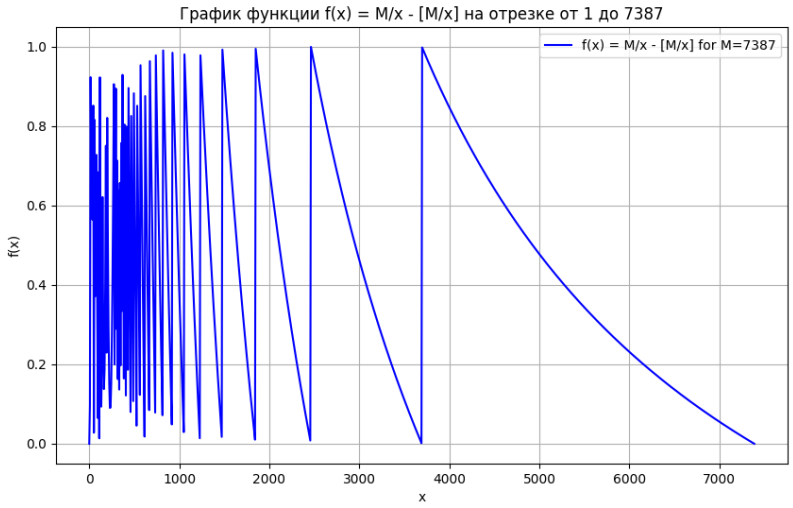

Figure 1. Graph of the function $f(x)$ highlighting local maxima and minima.

 doi:10.20944/preprints202404.0125.v1

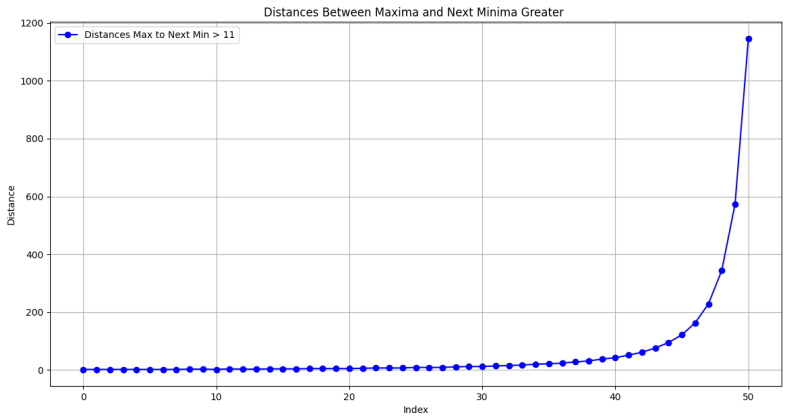

Figure 2. Distances between maxima and the following minima, greater than a given threshold.

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.

5. Conclusions

The study confirmed the significance and effectiveness of transitioning from algebraic methods of solving the factorization problem to approaches based on functional analysis. Applying gradient descent to factorization opens new perspectives for researching this important problem, offering a powerful tool for future scientific work in the field of cryptography and beyond. We hope that our approach stimulates further study of functional methods in factorization tasks and will contribute to the development of new, more efficient algorithms.

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.

Reimagining the factorization task as a problem of functional analysis and transitioning from algebraic to functional approaches have allowed us to engage computational algorithms that offer new possibilities for research and optimization. This not only deepens our understanding of the nature of the factorization task but also provides valuable tools for developing more effective solving methods, which can find wide application in cryptography and beyond.

Thus, the study not only revealed potential advantages of using the gradient descent method for factorization but also made a significant step towards rethinking the very task of factorization. This transition to functional methods opens new perspectives for engaging a variety of computational algorithms and technologies, facilitating a deeper understanding and more effective solution of one of the most fundamental tasks in mathematics and cryptography.

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.

References

1. Lenstra, A. K., Lenstra, H. W., Manasse, M. S., & Pollard, J. M. (1990). The number field sieve. *Proceedings of the twenty-second annual ACM symposium on Theory of computing*, 564-572.

 doi:10.20944/preprints202404.0125.v1

2. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings 35th annual symposium on foundations of computer science*, 124-134.
3. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120-126.