Deterministic and Probabilistic Prime Numbers: A Theoretical Approach

Poonam Kumari, Research Scholar, Department of Mathematics, Singhania University, Pacheri Bari, Jhunjhunu (Raj.), India
Dr. Vijesh Kumar, Research Supervisor, Department of Mathematics, Singhania University, Pacheri Bari, Jhunjhunu (Raj.), India

Abstract

The primality test and prime numbers are the foundation of this survey work. The fundamental units of number theory are prime numbers. Number theory relies heavily on prime numbers, which are mostly used in encryption. When a number is extremely large, it can be exceedingly challenging to determine whether it is prime or not. There are several algorithms to solve this issue. This paper discusses prime numbers and associated testing techniques, including the Lucas test, the Chinese primality test, the AKS algorithm, and Fermat's primality test.

Keywords: Prime Numbers, Lucas test, AKS algorithm, Number theory

1. Introduction:

Prime numbers are very essential in current computer science, especially in the realm of cryptography, even though they are not just numbers. Many cryptographic methods, such as the well-known public-key systems RSA, Diffie-Hellman, and Elliptic Curve Cryptography, rely largely on the availability of big prime integers to stay safe. These systems use the fact that it is hard to factor the product of two huge primes or similar difficulties. This is what makes secure digital communication, online banking, e-commerce, and private data exchange possible. So, in today's environment, it's important to be able to quickly and reliably produce huge prime numbers in order to keep digital information safe and secure. The problem in generating prime numbers is finding the right balance between speed and accuracy. Early approaches like trial division and the Sieve of Eratosthenes are easy to understand and work well for tiny integers, but they don't work well for cryptographic applications since they need to work with very big numbers. As a result, a number of more advanced algorithms have been created. These include probabilistic primality tests like the Miller-Rabin and Fermat tests, which can quickly find likely primes with a very low error margin, and deterministic tests like the AKS primality test, which guarantee correctness but often cost more to run. As the need for secure systems and more powerful computers grows, it is also important to look into and improve techniques for generating prime numbers. This means not only knowing the math behind it, but also taking advantage of new developments in algorithm design, computational complexity, and hardware capabilities. Researchers look at parallel processing, probabilistic methods, and machine learning to make prime generation faster and more accurate.

It is necessary to understand about prime numbers since they are a fascinating topic in mathematics, especially in number theory. What is the largest prime number that you can guess? Would 963333333333331 work? Primality is the quality of a number being a prime number. There are only two kinds of numbers in this nature: prime and composite (apart from 1). Composite numbers are defined as natural numbers with factors greater than two but greater than one. For instance, 6, 8, 9, 12, etc. Speaking of prime numbers, those that have only two components—the first being 1 and the second being itself—are referred to as such. For instance, 3,5, 7, 11, 13, and so forth. Alternatively, prime numbers are defined as natural numbers (>1) that are divisible by both 1 and themselves. Here are a few prime numbers: 2, 3, 5, 7, 11, 13, 17. Prime numbers can also be defined as follows: if m is divided by any integer $2 \leq \sqrt{m}$ m, then m is a composite number; if not, it is a prime number. Euclid came up with the concept of prime numbers many centuries ago. According to him, the number of prime numbers is unlimited. Since the amount of digits in a prime number is inversely proportionate to the likelihood that the number is a prime, there is no formula that can be used to connect prime and composite numbers. The number "2" is notable since it is the only even prime number and is regarded as the first in the list. The trial version is a slow method that allows us to verify the primality of an integer n. This approach determines if n is a multiple of any positive integer

between 2 and √n. There are still several unanswered questions regarding prime numbers. It include Goldbach Conjecture, all even integers which are greater than 2 can be written as addition of two primes, other is Twin Prime Conjecture it states there are infinitely many pair number of primes having one even number with between them. When we write a number as a product of prime it is called prime factorization of the number.

2. Literature Review

Ezz-Eldien et al. (2024) found a number of performance problems with standard generation methods and suggested algorithmic fixes that would make the process faster and more reliable. Their results showed how important prime number theory is to modern information security systems and how important it is to keep coming up with new ways to do cryptographic calculations. Knežević (2021) looked into using evolutionary algorithms to find prime numbers and came up with a new heuristic-based way to evolve possible prime candidates over time. The study showed that genetic algorithms could be useful for generating huge numbers of prime numbers, especially in limited or specialized settings, even if they might not always be as fast as sieve-based approaches. Abdulqader et al. (2024) suggested that the strange distribution of primes is similar to some dynamic systems seen in nature and society. This makes them suitable for showing nonlinear thinking in school settings. This work showed that prime number theory could be useful for teaching in many subjects, especially for helping students think about systems and use arithmetic to solve problems. Loconsole and Regolin (2022) looked examined whether prime numbers have biological or cognitive "special" features that set them apart from other numbers. Their results showed that primes might be cognitively important because they can't be divided and are spread out in an irregular way. This study looked at prime numbers from a different standpoint, proposing that their perceived uniqueness might go beyond math and into biology and psychology. Carbó-Dorca (2023) looked at both how quickly primes can be generated and how they are paired in a way that makes sense, with the goal of making related computing tasks easier and faster. This study helped improve mathematical software and encryption systems that need to quickly analyze huge prime values by improving the methods used to find prime pairs. Curtis and Tularam (2011) showed that even after hundreds of years of research, there are still many things about the distribution of prime numbers that are hard to understand. The writers said that further research should be done on the basic nature of primes. They suggested that this research should combine real-world examination with abstract theoretical exploration. Kwame, Owa, and Tawfik (2024) talked about the real-world problem of producing prime numbers for cryptography, especially for RSA encryption. The results showed that their method made processing time and energy use much better, making it good for real-time cryptography applications, especially in places with limited resources. Gunasekara et al. (2015) talked about how these ideas could be used in real life, in areas like blockchain technologies and signal processing. The authors put together decades of study to give a full picture that not only put current research in context but also pointed to interesting areas for future research. Lee and Kim (2024) revealed that data-driven methods could speed up the process of finding prime numbers, which could lead to hybrid models that use both mathematical rules and statistical learning.

3. Objectives of the Study

- **To review and compare existing algorithms for prime number generation**, including both deterministic and probabilistic methods.
- **To analyze the computational efficiency and scalability** of prime generation techniques, especially for large integers.

4. Need of the study

- Large prime numbers are fundamental to cryptographic algorithms such as RSA and Diffie-Hellman, which protect data and ensure secure communication online. This study aims to ensure the robustness of these systems in the face of evolving threats.

- The research seeks to identify the most efficient and scalable prime generation algorithms, including both deterministic (like Sieve of Eratosthenes) and probabilistic (like Miller-Rabin) methods. This comparison will guide the selection of optimal algorithms for various applications.
- The study's results will provide practical guidance for developers and researchers on choosing appropriate algorithms based on accuracy, computational cost, and scalability requirements for specific use cases.
- The research contributes to the broader field of computational number theory by providing insights into the performance of different prime number generation techniques.

5. Why this Study is Relevant

In essence, this study addresses a critical need for efficient and secure prime number generation, driven by the evolving landscape of digital security and computing power. It bridges the gap between theoretical algorithmic understanding and practical, real-world applications in cryptography and other fields.

6. Data Analysis and Results

Trial Division-

After considering a number n, we determine if any number m between 2 and √n n divides. n is a composite number if it is divisible by any m; otherwise, it is prime. For instance, let's say N=100.

m = 2,3,4,5,6,7,8,9,10

$N\%2 = 0$ so 100 is not a prime number, it is a composite number.

Wilson's Theorem:

According to this deterministic primality test, a number must follow if it is prime.

$$(n-1)! \equiv -1 \mathrm{mod} n$$

Algorithm: Wilson's Theorem

Step1. Input the number;
Step2. Calculate its factorial of $n-1$;
Step3. Add one store it (say l);
Step4. If n is divided by l then it's not prime else print prime.

SEIVE METHOD:

We should make a list up to the number and then mark the numbers that are divisible by some other numbers (apart from 1 and itself) since it is also a deterministic primality test.

Algorithm: Seive Method

Step1. Create a list of numbers from 2 to n;
Step2. From number 2 start marking the number which are divisible;
Step3. Increase the number by 1, repeat step 2
Step4. Some numbers are not marked these are primes up to n;

Algorithm: Miller Rabin Test

Step1. Miller Rabin (n, s)
Step2. For j = 1 to s
a = random $(1, n-1)$
Step3. If witness (a, n)
Return composite
Else Return Prime

Fermat Primality Test

It is moreover a probabilistic primality test, it is not anything but a sweeping form of Chinese Primality test. The only disparity is that 2 was old in the Chinese primality experiment except here in Fermat's we resolve use a all-purpose base so precisely it is: $A\hat{}K \equiv A \mathrm{mod} K$, where A is several positive number and K be prime. Is p prime?

$a^p - a \leftarrow$ if p is prime then this number is multiple of p

$$\{1 <= a < p\}$$

Example $p = 5$

$$1^5 - 1 = 0$$
$$2^5 - 2 = 30$$
$$3^5 - 3 = 240$$
$$4^5 - 4 = 1020$$

in view of the fact that every number is multiple of p, the integer p is thought prime.

Rimality Test Complexity

Table 1: Analyzing and contrasting various primality tests

Wilsons Theorem	o(n)	No	Yes
Trial Division	0(n1/2)	No	Yes
Seive Method	O(nlog(log n))	No	Yes
Miller Rabin	O (log n)	Yes	No
Fermats Primality Test	O (m log n)	Yes	No
Lucas Test	$O(n^2 \log n \log(\log n))$	Yes	No
Aks Algorithm	O (log 5n)	No	Yes

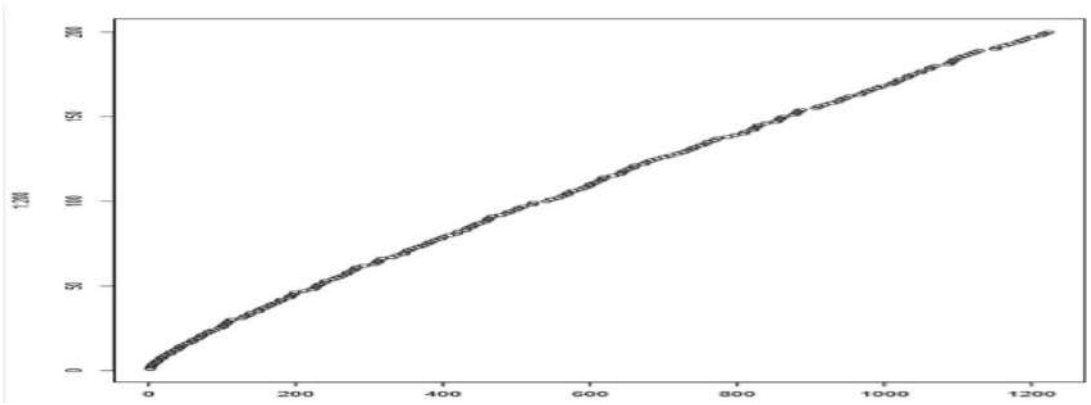

Figure 1: Prime numbers' distribution over whole numbers

The vertical axis in the graph above (Figure 1) displays whole numbers, while the horizontal axis displays prime numbers. Typically, this indicates that there are roughly 200 prime numbers for every 1200 whole numbers. The prime numbers from 2 to... (200 in number) are shown on the graph, bringing the total numbers up to 1200. Moving on to the following segment, which is from 100 to 150, the graph is a little more discontinuous than the previous segment, and the discontinuity indicates a jump in the full number. This change is very significant, and it also does not receive any N. The whole number jump indicates that there is a lower chance of discovering a prime number than there was for the preceding one. Speaking of the third and final section, we can observe that there are abrupt jumps and a more irregular graph. Compared to the previous two segments, the likelihood of obtaining a prime number in the final segment is rather low. According to the aforementioned observation, the likelihood of discovering a prime number decreases significantly as one moves up the whole number scale.

7. Conclusion:

Problems involving prime numbers are fascinating and useful for research. In this field, a lot of effort needs to be done. According to GIMPS, the largest prime number is $2^{74,207,281} - 1$; nevertheless, since infinite exists, we can assume that there will be a prime number larger than $2^{74,207,281} - 1$. Prime numbers contain a wide range of fascinating topics, which makes them suitable for research projects as well. There are a lot of undiscovered things in this sector.

Speaking of this, there is a thorough investigation into primes, their varieties, and the various primality tests that are currently available. Additionally, the practical uses of primes are examined. Since the AKS algorithm is the newest of all of them and is also the least complicated and easiest to comprehend and compute, it is truly desirable in our situation to use an algorithm that requires less time or has less complexity.

8. Limitations

- Sieve-based methods are efficient for finding all primes up to a given limit but are not ideal for generating primes within a specific range or for generating single large primes. Their memory usage can also become a bottleneck for very large limits.
- Probabilistic tests are vital for generating large prime numbers needed in cryptography because they offer a pragmatic and efficient solution that avoids the extreme computational cost of deterministic algorithms for such large values.
- Generating very large primes requires a different strategy. A common method involves picking a random number of the desired bit-size and then applying a probabilistic primality test. The limitations of these methods are their inherent unreliability (probabilistic) and the fact that sieve-based algorithms become computationally infeasible at scale.

9. REFERENCES

1. Abdulqader, S. A., Al_Barazanchi, I. I., Jaaz, Z. A., Sekhar, R., Shah, P., &Malge, S. (2024). Exploring Anomalous Relaxation Models in Prime Number Distribution and Their Relevance to Sustainable Development Education. Mathematical Modelling of Engineering Problems, 11(5).
2. Carbó-Dorca, R. (2023). On prime numbers generation and pairing. International Journal of Innovative Research in Sciences and Engineering Studies, 3, 12-17.
3. Curtis, M., & Tularam, G. A. (2011). The importance of numbers and the need to study primes: The prime questions. Journal of Mathematics and Statistics, 7(4), 262-269.
4. Ezz-Eldien, A., Ezz, M., Alsirhani, A., Mostafa, A. M., Alomari, A., Alserhani, F., & Alshahrani, M. M. (2024). Computational challenges and solutions: Prime number generation for enhanced data security. PloS one, 19(11), e0311782.
5. Knežević, K. (2021, September). Generating Prime Numbers Using Genetic Algorithms. In 2021 44th International Convention on Information, Communication and Electronic Technology (MIPRO) (pp. 1224-1229). IEEE.
6. Machado, J. T., & Lopes, A. M. (2020). Multidimensional scaling and visualization of patterns in prime numbers. Communications in Nonlinear Science and Numerical Simulation, 83, 105128.
7. Kwame, A. A., Owa, K., & Tawfik, A. H. (2024, July). An Efficient Generation of Prime Numbers for RSA Encryption Scheme. In World Congress in Computer Science, Computer Engineering & Applied Computing (pp. 409-420). Cham: Springer Nature Switzerland.
8. Lee, S., & Kim, S. (2024). Exploring Prime Number Classification: Achieving High Recall Rate and Rapid Convergence with Sparse Encoding. arXiv preprint arXiv:2402.03363.
9. Loconsole, M., & Regolin, L. (2022). Are prime numbers special? Insights from the life sciences. Biology Direct, 17(1), 11.