THE ENIGMA OF PRIME NUMBERS

Dmitri TRUBCA[1],
Antonela MALÎI[1],
Ana ȘARAPOVA[1*]

[1]Technical University of Moldova, Faculty of Computers, Informatics and Microelectronics, Department of Software Engineering and Automatics, FAF-192, Chișinău, Republic of Moldova

*Șarapova Ana, sarapova.ana@isa.utm.md

Abstract. *Prime numbers, regarded as the atoms of arithmetic, play an essential role in number theory. Being the keys that protect our electronic secrets on the Internet, they manifest a very mysterious behaviour. At the same time, the interest among students of Moldova in any form of mathematics is gradually decreasing and prime numbers are no longer considered as a domain of interest for the young generation. This article represents a detailed survey on prime numbers and aims to spark the interest in this area, by presenting numerous motivating factors that emphasize the necessity to further study these enigmatic numbers. Throughout this survey, the history, distribution and analysis of the patterns they form, as well as some real world applications of primes are considered.*

Keywords: *Mersenne primes, Gauss, Ulam Spirals, Cryptography, Primality testing, Cicadas*

Introduction

Prime numbers attracted human attention from the early days of civilization. They are like cousins, members of the same family, resembling one another, but not quite alike. On a smaller scale, their appearance seems random, but in reality the pattern in the distribution of primes is still not a fully understood subject that remains open to mathematician's world. Prime numbers are positive integers greater than 1 that are divisible only by one and themselves - e.g., 2, 3, 5, 7, 11, 13, 17, 19, 23, … . There are infinitely many primes. No matter how far you move up the number line there'll always be another prime number ahead.

Brief History

Since the time of the oldest civilisations, numbers have had their specific mystery and meaning. Primes have been recognized since ancient times, when they were studied thoroughly by Greek mathematicians. They are the building blocks of whole numbers - every positive integer greater than 1 can be expressed as a product of primes. This statement represents The Fundamental Theorem of Arithmetic.

From this idea we can start the understanding of Euclid's Theorem of prime numbers. About 300 B.C. the ancient Greek mathematician proved that there are infinitely many prime numbers and has put the beginning of studying these numbers.

Later, in 200 B.C., Eratosthenes created an algorithm designed to find prime numbers in a reasonable amount of time. His method, the Sieve of Eratosthenes, can be considered as one of the earliest most efficient algorithms ever written. It consists of listing all positive numbers until the given limit and marking the multiples of all numbers until the square root of the largest element in the list traversed. The only numbers that remain and are not crossed out are primes. This method enables someone to come up with large quantities of prime numbers.

Until the 18th century, Nicomachus of Gerasa, Pierre de Fermat and Leonhard Euler produced and proved several theorems concerning prime numbers. Later, during the work on expanding logarithm tables, Gauss discovered the logarithmic dependency in the distribution of prime numbers, that afford him to discover the law governing the distribution of prime numbers, now known as the Prime Number Theorem (see [3]). The below formula (fig. 1) can be used in determining the approximation of primes in a given interval [a,b] of numbers [1].

$$\int_a^b \frac{dn}{log(n)} \quad (1)$$

In his letter to a student, he presented a short story about his discovery that showed one of his tables summarizing information about distribution of primes between 1,9 and 2 million with a small deviation. In 1859, Riemann found a key to determining this deviation, proposing an elegant approximation to the number of primes less than a given number *N* [2]. His hypothesis remains one of the most important problems in mathematics and solving it can help us understand the true nature of prime numbers.

Types of Prime Numbers

According to some features that they have, primes have been divided into different groups. Each of them have their specific properties and applications. Some of the most important types of prime numbers are described below.

Mersenne primes are prime numbers of the form $p = 2^n - 1$. Due to their structure, it's easy to compute an integer modulo some Mersenne prime. Instead of performing the division literally (which is CPU time consuming), it's possible to compute the remainder by performing a series of additions [4]. Therefore, Mersenne primes are often used whenever someone needs to perform many operations of the form *x mod p*, and *p* needs to be a prime number. Some of the application areas of Mersenne primes are hashtables and pseudo random numbers generators.

Fermat primes are prime numbers of the form $p = 2^{2^n} + 1$. There are known 5 Fermat primes, the largest one being *65 537*. They find their applications in PRNG and are also related to geometry [6]. Gauss' Theorem states that "A regular n-gon is constructible with compass and straightedge if and only if n a product of distinct Fermat primes, multiplied by a power of two".

Twin primes are pairs of prime numbers that differ in value by two. This definition can be extended to categorize all prime pairs of the form *(p, p + 2*k)*. The Polignac's conjecture states that there are infinitely many such pairs. In 2013, Yitang Zhang proved that for some integer *N* that's less than 70 million, there are infinitely many pairs of primes that differ by *N* [8].

Primes in nature

Long before humans realised the significance of primes, the astounding properties of these numbers had been used by many other creatures of our Universe. The Cicadas - small insects that live in North America have their lifecycle connected directly to prime numbers.

For 7, 13 or 17 years the cicadas hide underground and then emerge all together into the forest. After a 6-week period - the forest goes quiet again. Clearly, a prime year lifecycle cannot be just a coincidence. As it turns out - this particular property helps them avoid other periodic predators. For instance, a predator that appears every 6 years will intersect with the cicadas with a 7 year lifecycle only each 42 years (LCM (Least Common Multiple) of the two numbers). If the cicadas would have a composite number lifecycle (for example 8 or 9 years), they would meet much more frequently. Therefore, the survival of these amazing species depends directly on prime numbers.

Analysis of different patterns

Prime numbers have a very strange behaviour. They manifest properties both of randomness and regularities. In order to understand this bizarre behaviour we need to look for patterns. If you start with number one in the middle, and continue writing down all successive integers as you spiral out counter-clockwise (fig. 1 a)), remove all composite numbers and replace the value of primes with a mark you will notice that prime numbers seem to be lining up on diagonal lines or in other words, some diagonal.

Figure 1 a). Ulam Spiral Setup lines seem to have much more primes than average. To be sure that it's not any kind of illusion, we can compare the resulting image (fig. 1 b)) with randomly distributed dots on a square (fig. 1 c)).

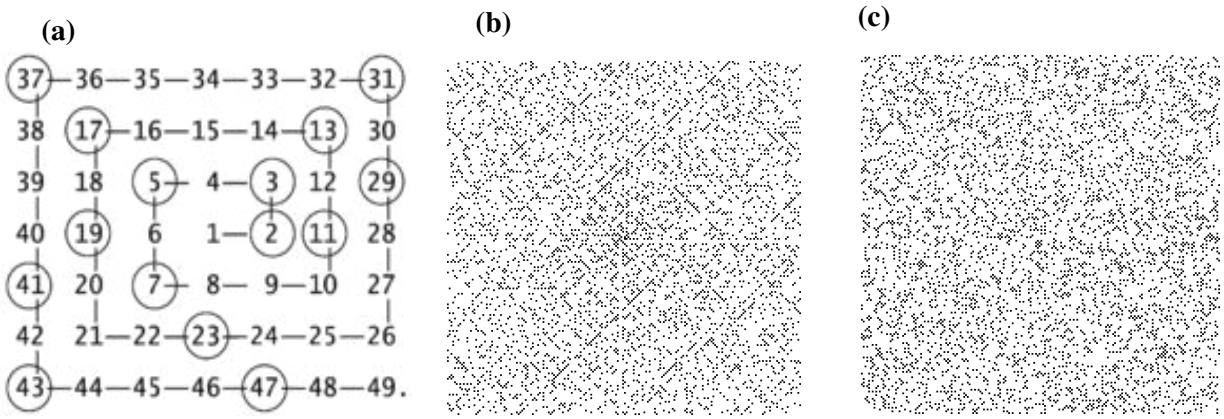

Figure 1 a). Ulam Spiral Setup b). Ulam Spiral c).Random Spiral

The persisting pattern in prime numbers distribution can be explained. If we analyze the Ulam spirals more carefully, it turns out that all diagonal lines have different quadratic equations. What the pattern is really revealing is that some quadratic equations have more primes on them than others - and that's a conjecture that hasn't been proven yet [5], though there are already known some high prime density polynomials, such as $x^2 - x + 41$, which produces 40 consecutive primes in a row (for $0 \leq n \leq 39$). As it turns out, primes are not as random as you might think of, there are equations to help us find prime numbers.

Real world application

Prime numbers play a very important role in our daily life. Every time we visit a website, purchase something online or perform some other type of online transaction, prime numbers are used to protect our data. They stand at the basis of modern cryptography which relies on one simple property - it's much easier to multiply numbers together, than to factor them. Since the factorisation of a really large product of primes would take an eternity, these numbers, used to encrypt our data, can be publicly known. The only way to decrypt the information would be find its factors - which represents a challenge even for modern supercomputers.

Primes are used not only in mathematical sciences. In the last century, a correlation between primes and quantum mechanics has been found. Particularly, the statistical distribution of the non-trivial zeros of the Riemann zeta function happens to be closely related to the quantum chaos theory [7]. This discovery encouraged mathematicians and physicists to work together in order to unveil the laws governing our Universe, with the help of prime numbers.

Primality testing

Since primes play an important role in cryptography, specific algorithms have been developed in order to identify if a particular number is prime.

a) Fermat Primality Test

It is a test based on *Fermat Little Theorem* and modular ex onentiation, that states that for every prime *p* and an integer *a* comprime to it: $a^{p-1} \equiv 1 \, mod \, p$. Hence, if the equality does not hold, then we can be sure that the number is not prime. Testing the equality for several values of *a* will give us an estimation whether *p* might pe prime.

c) AKS Primality Test

It's a deterministic primality testing algorithm that can be used to verify the primality of any general number given and runs in a polynomial amount of time. The AKS Primality Test is based upon the following theorem: *An integer* $n>2$ *is prime if and only if the below polynomial congruence relation holds for some a coprime to n. (x is just a formal symbol).*

$$(x+a)^n \equiv (x^n+a)(mod\ n) \qquad (2)$$

Conclusion

Prime numbers manifest a very bizarre behaviour. On a smaller scale they seem to obey the law of chance, but on a larger one, primes happen to exhibit a stunning regularity. The properties of these numbers are widely used in nature, as well as by humans in our daily life. They stand at the foundation of modern cryptography and represent the key to our electronic secrets. There are special methods for generating prime numbers, as well as for identifying whether certain numbers are prime. The correlation between primes and geometry, informational technology, nature and quantum physics, as well as our current lack of understanding of these numbers, shows the great necessity for continuation of studies in the area of prime numbers. As a result, it's essential to stimulate the interest and continue the investigation of prime numbers, which may potentially reveal the laws governing our Universe.

References

1. TSCHINKEL,Y., *About the cover: on the distribution of primes - Gauss' tables*, Bulletin of the American Mathematical Society, 2005
2. MAZUR, B., STEIN, W. A., *Prime Numbers and the Riemann Hypothesis*, Cambridge University Press, 2016
   1.1. ANDREWS, G. E., *Number Theory,* Dover Publications, INC. New York
3. BOS, J. W., KLEINJUNG, T., LENSTRA, A. K., MONTGOMERY, P. L., *Efficient SIMD arithmetic modulo a Mersenne number*, 20th Symposium on Computer Arithmetic, 2011
4. NAJERA, J., *Unexpected Beauty in Primes*, Cantor's Paradise, 2019
5. KUH, D., *Constructible Regular n-gons*, Senior Project, Whitman College, 2013
6. DEVINE THOMAS, K., *From Prime Numbers to Nuclear Physics and Beyond*, The Institute Letter Spring 2013
7. Klarreich, E., *Unheralded Mathematician Bridges the Prime Gap,* Quanta Magazine of Illuminating Science,2013