PRIME NUMBERS: HISTORY, THEORIES AND APPLICATIONS

Georgeana GLOBA[*], Dorin OTGON

Software Engineering and Applications Dept., FAF-211, Faculty of Computers, Informatics and Microelectronics,
Technical University of Moldova, Chişinău, Moldova

*Correspondent author: Globa Georgeana, georgeana.globa@isa.utm.md

Abstract. *As many properties of the primes started being discovered, so did the interest in them grow as time went on. The very existence and purpose of prime numbers has been justified by their increased usage in various scientific fields. Although many questions about them (primes) are still unanswered, their usefulness is undoubted as they are one of the founding pillars of Modern Security. Patterns involving primes have also found use in physics, engineering, and have even been part of an evolved trait in nature.*

Key words: *primes, number theory, application, algorithms*

Introduction

Prime numbers - one of the many wonders of mathematics, are a category of numbers that have the property that they cannot be divided by anything other than 1 and themselves (i.e. they are not a product of two smaller natural numbers). They have been a topic for discussion in a lot of mathematical conferences and countless people have tried solving the mystery of their uniqueness, and thus numerous conjectures and open questions have been formed – one of them being the famous Goldbach Conjecture. Fortunately, their mystery is what keeps a lot of modern Security afloat – prime factorization is one of the main components of it.

Although many may be restricted to think that they have uses only in the field they originated from – mathematics – that is not necessarily true. They have a vast variety of applications in Biology, Cryptography, Engineering, and even Arts because of their distinctive features.

A Prime Look in the Past

One of the earliest studies of prime numbers has been discovered in ancient Greece. Euclid's Elements (a mathematical treatise) demonstrated the fact that there are infinitely many prime numbers (infinitude of primes) and it formed a stable basis for the fundamental theorem of arithmetic. Another important discovery of the Greeks was the Sieve of Eratosthenes - an algorithm that finds all prime numbers up to any given limit [1].

Around the year 1640, Pierre de Fermat - a renowned French mathematician - published one of his theorems called "Fermat's little theorem"(1) which stated that if p s a prime number, then for any integer a, the number a^p is an integer multiple of p.

$$a^p \equiv a(mod\, p) \tag{1}$$

A distinctive group of numbers that has been questioned for their primality (i.e. whether they are prime or not) were the Fermat numbers - they are of the form:

$$F_n = 2^{2^{\mathrm{n}}} + 1 \tag{2}$$

out of which only the first 4 have been determined to be prime - the rest, up to n = 32, were proven to be composites. There are still some open questions which are yet to be answered, such as: "Is F_n composite for all n > 4?"; "Are there infinitely many Fermat primes?" "Are there infinitely many composite Fermat numbers?" or even "Does a Fermat number exist that is not square-free?".

Another interesting group of primes that were discovered in the 17th century by the polymath Marin Mersenne were the Mersenne primes (or the Mersenne numbers without the primality requirement). The primes are of the following form:

$$M_n = 2^n - 1 \tag{3}$$

where n is any prime. The reason why n is prime is because a composite n will provide a composite result. Even so, there has been found a smallest counterexample to that theorem:

$$M_{11} = 2^{11} - 1 = 2047 = 23 \times 89 \tag{4}$$

The largest known prime number is also a part of this set: $2^{82,589,933} - 1$ which is a Mersenne prime. Up to date, it has not been proven whether there are finitely or infinitely many Mersenne primes.

In number theory, Euler's totient function counts the positive integers up to a given integer n that are *relatively prime* to n (i.e. the only positive integer that is a divisor of both of them is 1). He introduced the given function in 1763, which he later denoted by $\varphi(n)$. This is one way of computing $\varphi(n)$:

$$\varphi(n) = n \prod_{p|n} (1 - \tfrac{1}{p}) \tag{5}$$

where the product is over the distinct prime numbers that divide n.

Nowadays, primes remain relevant within discussions regarding mathematics as there are still plenty of problems and conjectures that are yet to be solved or proven otherwise. Many uses and applications have been proposed as their properties continue to be found, ensuring improvements of our society's quality of life.

Primes: Modern Applications

The most prominent contemporary use for primes comes in the domain of cybersecurity. They are used in the generation of public and private keys (used for file encryption and decryption), and play an essential role in the RSA encryption algorithm, named after the scientists that have described it: Ron Rivest, Adi Shamir and Leonard Adleman [2]. This algorithm is commonly used almost anywhere on the Internet: sending emails, forming secure connections with websites or VPNs, online chat rooms, even digital signatures.

Another common use of primes is within mathematical theories and statements. They lie at the base of the Fundamental Theorem of Arithmetic, which states that any positive integer can be represented in a unique product of primes. Other principles related to prime numbers include the aptly named "Prime number theorem" and Dirichlet's theorem on arithmetic progressions. Prime numbers are also related to a number of conjectures - theories that are yet to be proven or disproven. The Riemann hypothesis is directly related to primes, as the zeroes of its associated function can help describe their distribution [3]:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1-p^{-s}} \tag{6}$$

Problems of similar nature include the following: the Goldbach conjecture, Fortune's conjecture and Polignac's conjecture.

Prime numbers have managed to find their use in physics as well, as gears within machinery usually have co-prime numbers of teeth, resulting in even wear throughout the gear. Another application, which is just as important, is for avoiding resonance within systems with multiple oscillators, whether it be the number of spokes on a car wheel (which are most commonly 5) or the number of blades on a rotor or a turbine. This way, one can avoid the generation of vibrations or excessive noise within a system. A more intriguing use for primes is within quantum mechanics, where the series of prime numbers can represent the energy eigenvalues of a potential [4-5]. The sequence of prime numbers, due to their aperiodic order, can help form quasicrystals - crystals with no translational symmetry at an atomic level, which tend to possess unusual properties [6].

Scientists concerned with looking out for extraterrestrial life were debating for a way to communicate with possible intelligent life through some method which did not rely on language. Frank Drake came up with a system to send messages similar to Morse code, where the dots would represent parts of an image instead of a letter. The number of signals to be sent would be a product of 2 prime numbers, as one could arrange the signals in only 2 possible rectangular layouts. Such a sequence was sent from the Arecibo Observatory in Puerto Rico to the star cluster M13 back in 1974, the code now known as the "Arecibo message" [7] (Fig. 1).

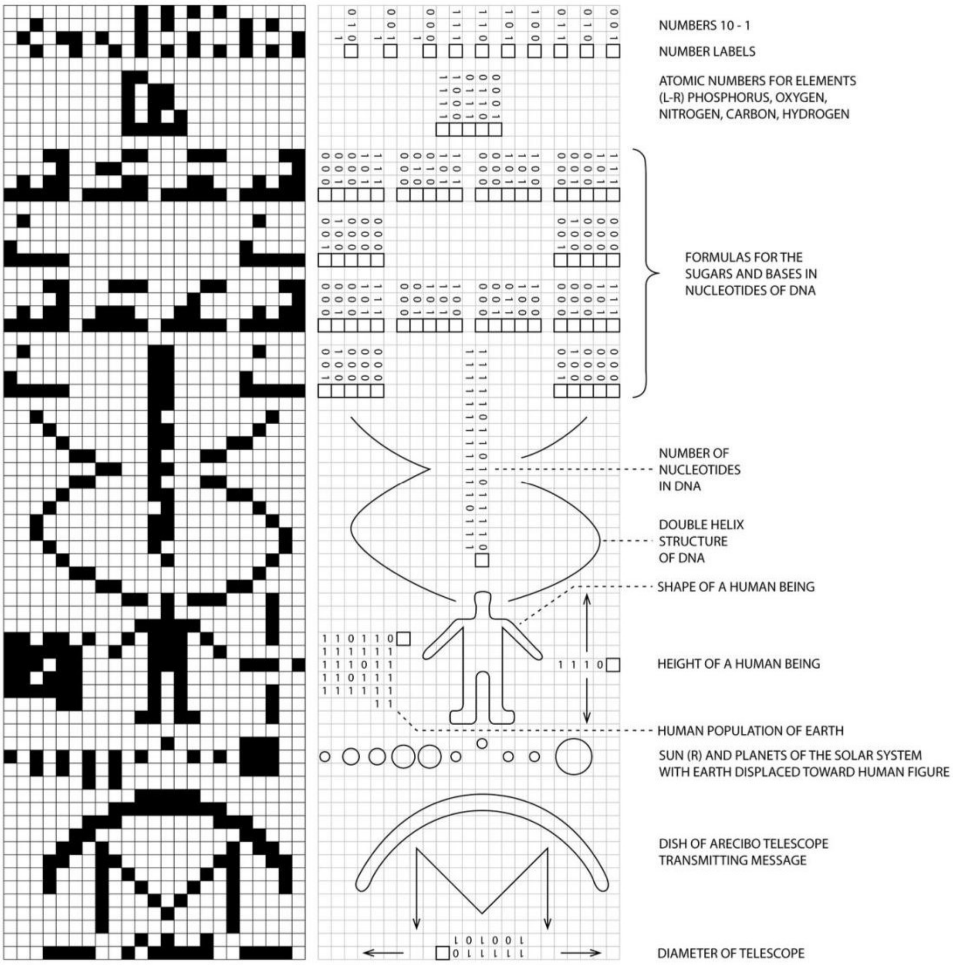
NUMBERS 10 - 1
NUMBER LABELS
ATOMIC NUMBERS FOR ELEMENTS (L-R) PHOSPHORUS, OXYGEN, NITROGEN, CARBON, HYDROGEN
FORMULAS FOR THE SUGARS AND BASES IN NUCLEOTIDES OF DNA
NUMBER OF NUCLEOTIDES IN DNA
DOUBLE HELIX STRUCTURE OF DNA
SHAPE OF A HUMAN BEING
HEIGHT OF A HUMAN BEING
HUMAN POPULATION OF EARTH
SUN (R) AND PLANETS OF THE SOLAR SYSTEM WITH EARTH DISPLACED TOWARD HUMAN FIGURE
DISH OF ARECIBO TELESCOPE TRANSMITTING MESSAGE
DIAMETER OF TELESCOPE

Figure 1. The Arecibo message on the left, with an interpretation of each corresponding part [8]

Prime numbers also influence the living creatures around us, as some species of animals have developed survival strategies based on the property that prime numbers do not have any factors other than 1 and itself. Seven species of cicadas in North America have developed a 13 or even 17 year long life cycle, where they emerge from their nymphs within their last year of their life. Scientists speculate that this particularity was evolved to avoid the development cycles of the predators of the cicadas, as to minimize the number of years when both are active [9].

Conclusions

People have been interested in the peculiar set of prime numbers ever since Antiquity, this curiosity being propagated throughout the ages by various great minds to the present day. Lying at the foundations of algebra, primes have great influence over different domains of science and even have an impact in our day-to-day life, being at the core of cryptography, finding applications within engineering, and posing questions of great interest within the fields of mathematics, even being witnessed among nature. By understanding the properties of the sequence of prime numbers, we can further our knowledge within various scientific fields.

Acknowledgements

We would like to thank Cojuhari Elena, Associate Professor at the Department of Mathematics, Technical University of Moldova, for a thorough scientifical check and for her suggestions with reference to the topic, and Gogoi Elena, univ. lect., Department of Software Engineering and Automatics, Technical University of Moldova, for providing extensive feedback on the paper.

References

1. O'CONNOR, ROBERTSON, E., F.: *Prime Numbers*, 2018, [online]. [accessed 22.02.2022]. Available: https://mathshistory.st-andrews.ac.uk/HistTopics/Prime_numbers/
2. MICHAEL, C. *The RSA Cryptosystem: History, Algorithm, Primes*, 2007, [online]. [accessed 22.02.2022]. Available: http://www.math.uchicago.edu/~may/VIGRE/VIGRE2007/REUPapers/FINALAPP/Calderbank.pdf
3. ENRICO, B. *Problems of the Millennium: the Riemann Hypothesis.*, 2000, [online]. [accessed 23.02.2022]. Available: https://www.claymath.org/sites/default/files/official_problem_description.pdf
4. BARRY, C. A Prime Case of Chaos. In: *What's Happening in the Mathematical Sciences, Volume 4*, 1999, pp. 2-17
5. MUSSARDO, G. *The quantum mechanical potential for the prime numbers.*, 1997, [online]. [accessed 24.02.2022]. Available: arXiv:cond-mat/9712010v1
6. NATALIE, W. *A Chemist Shines Light on a Surprising Prime Number Pattern.*, 2018, [online]. [accessed 24.02.2022]. Available: https://www.quantamagazine.org/a-chemist-shines-light-on-a-surprising-prime-number-pattern-20180514
7. CARL, P. *Prime Numbers and the Search for Extraterrestrial Intelligence*, 2004, [online]. [accessed 24.02.2022]. Available: https://math.dartmouth.edu/~carlp/PDF/extraterrestrial.pdf
8. *Areibo message and decoded key*, Science Photo Library, United States, [online]. [accessed 24.02.2022]. Available: https://www.sciencephoto.com/media/520525/view/arecibo-message-and-decoded-key
9. PAUL, L. *Prime Numbers*, 2008, [online]. [accessed 22.02.2022]. Available: https://arachnoid.com/prime_numbers/index.html