Number theory applications in our daily life

Ahmed Mohamed Shalaby Mohamed

Abstract- This is the central question of number theory, a vast, ancient, complex, and, most importantly, beautiful branch of mathematics. Number theory was historically known as the Queen of Mathematics, and it was very much a branch of pure mathematics, studied for its own sake rather than to understand real-world applications.

***Index Terms*-** Number theory – Modern Number Theory – Elementary Number Theory – Algebraic Number Theory – Analytic Number Theory – Geometric Number Theory – Probabilistic Number Theory

I. INTRODUCTION

The Number theory is a branch of mathematics that studies the properties of positive integers (1, 2, 3,...). It is one of the oldest and most natural mathematical pursuits, sometimes referred to as "higher arithmetic."

Number theory has always captivated both amateur and professional mathematicians. Unlike other branches of mathematics, many of the problems and theorems of number theory are understandable to laypeople, though solutions to the problems and proofs of the theorems frequently require a sophisticated mathematical background.

Number theory was thought to be the purest branch of mathematics until the mid-twentieth century, with no direct applications to the real world. With the advent of digital computers and communications, it became clear that number theory could provide unexpected solutions to real-world problems. Simultaneously, advances in computer technology

II. IDENTIFY, RESEARCH AND COLLECT IDEA

Number Theory as a branch can be traced back to the B. Cs, specifically to the lifetime of one Euclid. Euclid of Alexandria, also known as the "Father of Geometry," was a brilliant mathematician who devised one of the first "algorithms" (a set of sequential operations).

The main goal of number theory is to discover and prove interesting and unexpected relationships between different types of numbers.

Modern number theory is a broad subject with subcategories such as elementary number theory, algebraic number theory, analytic number theory, geometric number theory, and probabilistic number theory. These categories reflect the approaches taken to solve integer-related problems.

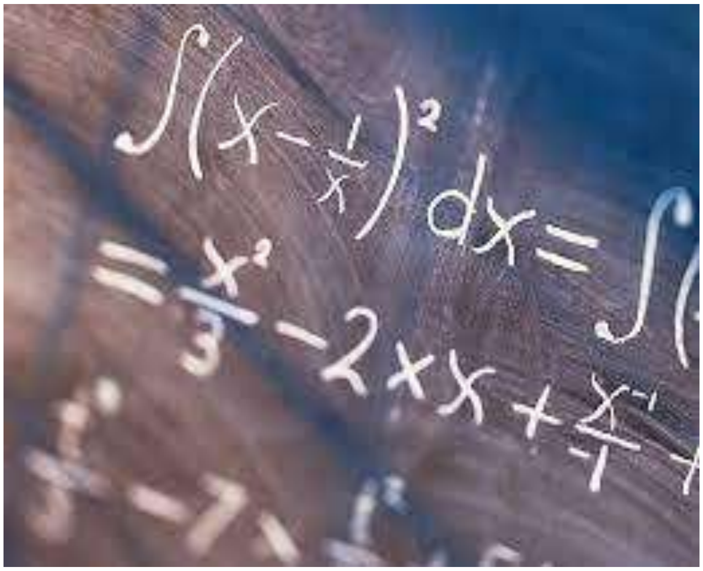

Figure 1 The number theory

Elementary number theory refers to those problems whose solution does not require methods from calculus. While this is still an important area in number theory, various other branches have developed in modern times. One such branch, known as the geometry of numbers, arose from a theorem by Hermann Minkowski.

Algebraic number theory is a branch of number theory that studies integers, rational numbers, and their generalizations using abstract algebra techniques.

Analytic number theory is a branch of number theory that solves integer-related problems using techniques from analysis. It is well known for its prime number results (for example, the celebrated Prime Number Theorem states that the number of prime numbers less than N is approximately N/logN) and additive number theory (the recently proven Goldbach's weak conjecture states that every odd number greater than 7 can be expressed as the sum of three odd primes).

Geometry number Theory is a branch of number theory that studies algebraic numbers using geometry. A ring of algebraic integers is typically viewed as a lattice in R^n, and the study of these lattices provides fundamental information on algebraic numbers. Hermann Minkowski pioneered the study of number geometry.

Probabilistic number theory is a branch of number theory that uses probability to answer questions about integers and integer-valued functions. One fundamental idea underlying it is that different prime numbers are, in some ways, similar to independent random variables.

III. WRITE DOWN YOUR STUDIES AND FINDINGS

Gauss dubbed number theory the "Queen of Mathematics." For many years, it was assumed that it had little practical uses. With the introduction of computers in the twentieth century, this position altered dramatically.

Prime and composite numbers are crucial in current encryption and coding systems. Every day, massive quantities of personal information (such as credit card details and bank account numbers) and money are sent electronically throughout the world, all of which must be kept hidden. Keeping secrets is an essential use of number theory.

A computer can swiftly determine whether a number—even a big number—is prime using Fermat's theorem. However, after a computer determines that a number is not prime, it takes a considerable time to determine its components, particularly if the number is a huge composite (say 120 digits long). Finding the prime factors of huge composite numbers can take years on a supercomputer.

Cryptographers benefit from the time lag between determining if a number is prime and factoring the primes in a composite number. They construct numerical codes for the letters and characters of a communication to build a security mechanism. The message is then converted into a long integer using an encoding method (a sequence of procedures to solve a problem). If the message is longer than a specific length, say 100 characters, the cryptography programme divides it into 100-character blocks. The software multiplies the number of an encoded message by a particular prime (which may be a 100-digit integer) and by a composite number once the message has been translated into a number.

The composite number is the product of two prime integers chosen at random and required by both the sender's encoding process and the receiver's decoding procedure. The prime numbers that comprise the composite number are extremely lengthy (100 digits and longer). Some of the numbers in the message are made public when it is sent from the sender to the receiver, but the primes that make up the composite number are kept private. Only the authorized individual who receives the message's decoding algorithm is aware of them. Many of the numbers will be visible to anybody listening in on the transmission, but without the prime numbers from the encoding and decoding systems, it is impossible to decode the message in any acceptable period.

Number theory has many applications, including computer cryptography systems. Other number theory formulae allow computer systems to predict what days of the week will fall on what dates of the month many years in advance, allowing people to know what day of the week Christmas or the Fourth of July will fall on. Many computers come with internal programs that inform users when they last edited a file to the second, minute, hour, day of the week, and month. These programs' function owing to number theorists' formulae.

Computational Number Theory

Computational number theory is the field of number theory concerned with the development and use of efficient computer methods for the solution of complicated number problems.

For the most part, computational number theory is concerned with whole numbers as well as rational and algebraic numbers. Number theory is unique among current mathematical sciences in that it offers a large variety of issues that are easy for non-specialists to comprehend. This software is widely used to test big numbers for prime factorization and primality. The procedure of determining whether a number is prime or not using a matrix to decompose it into its constituent prime factors. Accelerating the Primality Test is one of the most critical academic concerns at the moment. Larger numbers can be prime factorised in computational number theory. The most common generic factorial algorithm at the moment is General Number Field Sieve. Combinatorial Number Theory is simply an algorithmic version of integers with a few combinatorial characteristics. It is related to other branches of number theory in that it concentrates on the features of organised sets of integers rather than algebraic expressions or non-discrete integers.

THE APPLICATIONS OF NUMBER THEORY IN CRYPTOGRAPHY:

Overview

Cryptography is a branch of applied mathematics concerned with developing schemes and formulas to improve communication privacy through the use of codes. Cryptography enables its users, whether governments, military, businesses, or individuals, to keep their communications private and confidential. Every cryptographic scheme strives to be "crack proof" (I.e., only able to be decoded and understood by authorized recipients). Cryptography can also be used to protect data from tampering and ensure its integrity. Modern cryptographic systems rely on functions associated with advanced mathematics, including number theory, a specialized branch of mathematics that investigates the properties of numbers and their relationships.

Figure 2 Cryptography and the number theory

Background

Attempts to keep communications private are an age-old quest. The modern science of cryptography evolved from the use of hidden text, disappearing inks, and code pads. The term cryptography is derived from the Greek word kryptos (to hide). In essence, cryptography is the study of procedures that allow messages or information to be encoded (obscured) in such a way that reading or understanding the information without a specific key is extremely difficult (i.e., procedures to decode).

Encryption systems can be as simple as replacing letters with numbers, or as complex as using highly secure "one-time pads" (also known as Vernam ciphers). Because one-time pads are based on codes and keys that can only be used once, they provide the only "crack proof" method of cryptography currently available. However, due to the large number of codes and keys required, one-time pads are impractical for general use.

Many wars and diplomatic negotiations have hinged on one combatant's or country's ability to read the ostensibly secret messages of its adversaries. During World War II, for example, the Allied Forces gained significant strategic and tactical advantages by intercepting and reading Nazi Germany's secret messages encoded with the Enigma cypher machine. Furthermore, the development of operation MAGIC, which cracked the codes used by Japan to protect its communications, gave the US a decisive advantage over Japanese forces.

During the latter half of the twentieth century, the importance of cryptography increased in tandem with the advancement of computing technologies and the decline of paper and pen record keeping. As data volumes increased, permanent storage became limited to computer memory. Although the technological revolution and the rise of the Internet presented unique security challenges, there were also challenges to the fundamental security of increasing amounts of information stored and transmitted only in electronic form. Because of the increased reliance on electronic communication and data storage, there is a greater need for advances in cryptologic science. Cryptography's use has expanded beyond its original diplomatic and military applications to include companies and individuals seeking privacy in their communications. Governments, businesses, and individuals all needed more secure—and To secure their databases and email, governments, businesses, and individuals required more secure—and easier to use—cryptologic systems.

In addition to improvements to cryptologic systems based on information made public from classified government research programs, international scientific research organizations devoted solely to the advancement of cryptography (for example, the International Association for Cryptologic Research, or IACR) began to apply mathematical number theory to improve data privacy, confidentiality, and security. Number theory applications were used to create increasingly complex algorithms (step-by-step procedures for solving a mathematical problem). Furthermore, as commercial, and personal Internet use increased, it became increasingly important not only to keep information private, but also to be able to confirm the identity of the message sender. The use of cryptographic algorithms known as "keys" allows information to be restricted to a specific and limited audience whose individual identities can be verified.

Encryption is achieved in some cryptologic systems by selecting prime numbers and then using products of those prime numbers as the basis for further mathematical operations. In addition to developing such mathematical keys, the data is divided into blocks of specific and limited length, limiting the amount of information that can be obtained even from the message's form. Decryption is typically accomplished through an intricate reconstruction process that involves unique mathematical operations. In other cases, decryption is achieved by performing the inverse mathematical operations that were used during encryption.

Although it may have been developed earlier by government intelligence agencies, Ronald Rivest, Adi Shamir, and Leonard Adleman published an algorithm that would become a major breakthrough in cryptology in August 1977. The difficulty in factoring very large composite numbers lends security to the system's underlying RSA algorithm. By the end of the twentieth century, the RSA algorithm had become the world's most widely used encryption and authentication algorithm. The RSA algorithm was used in the creation of Internet web browsers, spreadsheets, data analysis software, email, and word processing software.

Rivest, Shamir, and Adleman did more than just publish a mathematical algorithm; they created the first public key cryptologic system that was widely available to commercial and private users. "Public key" systems are the most important modern cryptographic systems based on the RSA algorithm (and its modifications and derivations). These systems are widely regarded as among the most secure cryptographic techniques. Encoding and decoding are accomplished through the use of two keys—mathematical procedures for locking (coding) and unlocking (decoding) messages. Those who want to use the public key system distribute the "public" key to those who will be able to encode messages in such "two-key" cryptologic systems. The sender encodes the message using the recipient's public key, but the message can only be decoded by the recipient’s private key. This ensures that an encoded message can only be decoded by the holder of the private key. Starting in 1991, the public key method was used to improve Internet security via a freely distributed package known as Pretty Good Privacy (PGP).

Impact

Number theory applications enable the development of mathematical algorithms that can render information (data) incomprehensible to all but the intended users. Furthermore, mathematical algorithms can provide physical data security by allowing only authorized users to delete or update data. Finding ways to factor very large numbers is one of the challenges in developing tools to crack encryption codes. Advances in number theory applications, as well as significant improvements in computer power, have made factoring large numbers less intimidating.

In general, the larger the key size used in PGP-based RSA public-key cryptology systems, the longer computers will take to factor the composite numbers in the keys. As a result, the reliability of RSA cryptology systems is derived from the fact that there are an infinite number of prime numbers—as well as the difficulties encountered in factoring large composite numbers composed of prime numbers.

Number theory derivations with specialized mathematical derivations, such as theory and equations dealing with elliptical curves, are also having an increasing impact on cryptology. Although larger keys provide greater security in general, applications of number theory and elliptical curves to cryptological algorithms allow the use of smaller keys with no loss of security.

Another consequence of number theory applications is the emergence of "untrustworthy" transactions. Non-trustworthy means that parties cannot later deny involvement in authorizing specific transactions (e.g., entering into a contract or agreement). Many cryptologists and communication experts believe that the development of verifiable and non-reputable transactions with the legal weight of paper contracts is essential for the development of a global electronic economy. Cases involving electronic communications are increasingly being heard in legal courts around the world.

However, advances in number theory have also been applied in an attempt to crack important cryptologic systems. There are public keys and private keys in RSA composite number-based, two-key cryptologic systems. Attempting to crack the codes (the encryption procedures) necessitates the use of advanced number theories, which allow an unauthorized user, for example, to determine the product of the prime numbers used to begin the encryption process. To determine the underlying prime numbers, factoring this product is a difficult and time-consuming procedure. An uncomplicated approach would be to simply try all prime numbers. The time required to complete this task, on the other hand, can defeat all but the most determined unauthorized users. Other more exotic attempts include quadratic sieves algorithms, a method of factoring integers developed by Carl

Pomerance that is used to attack smaller numbers, and field sieves algorithms, which are used to determine larger integers.

Within the last two decades of the twentieth century, advances in number theory enabled the factoring of large numbers that would have taken billions of years by hand to procedures that could be completed in a matter of months using advanced computing. Further advances in number theory could lead to the development of a polynomial time factoring algorithm that can do in hours what currently takes months or years of computer time.

Advances in factoring techniques, as well as the increased availability of computational hardware (both in terms of speed and low cost), make the security of the algorithms that underpin cryptologic systems more susceptible. These dangers to the security of cryptologic systems are mitigated in some ways by ongoing developments in the construction of powerful computers capable of generating bigger keys by multiplying very large primes. Despite breakthroughs in number theory, bigger composite numbers are still simpler to produce than they are to factor.

Many cryptography standards are developed under the supervision of the National Institute of Standards and Technology (NIST). The Data Encryption Standard was created in the 1970s by private firms and the United States National Security Agency (NSA) (DES). In anticipation of increased security requirements, NIST began working late in the twentieth century on the deployment of the Advanced Encryption Standard (AES) to replace DES. Despite efforts to liberalize trade regulations, the United States government classed security algorithms used in PGP-type applications as weapons near the close of the twentieth century. As a result, they remained subject to stringent export controls and prohibitions, limiting their extensive distribution and usage.

The applications of number theory in computer science:

The study of integers and their characteristics is known as number theory. Number theory is used in computer science in a variety of ways, including data compression, encryption, and error-correcting codes. Amount theory, for example, is utilized in data compression to identify effective methods to encode data with a restricted number of bits. Number theory is utilized in cryptography to build difficult-to-break codes. Number theory is also employed in error-correcting codes to create codes that can identify and rectify faults.

The study of integers is central to number theory in mathematics. It has a wide range of applications, including cryptography, computing, and numerical analysis. We will investigate the uses of number theory in engineering problems. A Mechanical Engineer from the SASTRA Deemed University's Audhithya S V School of Mechanical Engineering in Tamil Nadu, India. The paper discusses number theory applications in engineering. Cryptography, which is concerned with internet security, is one of the most essential areas in the digital era. A semiprime number is an ordinary number formed by combining two prime numbers.

Semiprimes are a good tool for cryptography due of their utility. Previously, the exploration of elliptic curves and number theory inquiries was purely for entertainment purposes. These questions have lately received a great deal of attention in a variety of domains, including coding theory, pseudorandom number generation, and cryptography. Fibonacci numbers can be utilised in Fibonacci searches to identify sorted collections. This phrase is significant since it refers to the connection between normal and shear stresses. This component is known as the defining factor for beam stress analysis. The Pythagorean Theorem is applicable to any field that contains triangles.

Mathematicians and physicists employ this theorem to determine a range and sound source. We will investigate the use of limited partition functions to compute algebraically independent degree invariants that occur as a result of a finite group action on the vector space over the field of complex numbers. In their research, Krishnaswami Alladi and Alexander Berkovich employed identical units of Jacobi's triple product. The number theory is thoroughly explained, as are applications in numerous domains. The article would not have been possible without

the financial help of TATA REALTY and Infrastructure Limited. More study and development on the theory has enhanced the prospect of broadening its applications to both pure mathematics and engineering mathematics. The apps were also praised for their adaptability.
IEEE Transactions on Signal Processing, 2014, 62, 16, 4145-4157; Ramanujan sums in the context of signal processing -part I: foundations; Vaidyanathan P. P. This work investigates the features of a multi-agent inverse reinforcement learning (MIRL) problem in two-player general-sum stochastic games. We show in this study that the smooth counting function of a set of points encapsulates information equal to the points' n-level density. We show that if the points are the eigenvalues of matrices formed from classical compact groups with Haar measure, the first few moments are Gaussian, but the distribution is not. A shakedown hypothesis is founded on data collected from a genuine structure or laboratory specimen. One of its main features is to undertake a direct analysis of an issue utilising the limit analysis approach. A novel test has been designed to answer the problem of statistical features of quantum system wave function components. This research looks at the issue of message coding and decoding.
This sequence's logarithmic decline results in a zero density. The leg sequence is comparable in terms of even limbs, as seen in the diagram. The upper bound is assumed to be stable, as is the Erd*H*o*s-Ford-Tenenbaum constant. It is a sequence with periodicity $q in which one leq q leq infty$ is made up of a series of linear combinations of $c q(n), 1 leq q leq infty$ for any given q sequence. Ramanujan exemplified These sums have been used to show the extraction of periodic components from discrete-time signals. Because the total of K indicates x *q *i* (n) in S *q i* $. It is feasible to discover hidden periodicities by defining the Ramanujan Periodic Transform (RPT). It is feasible to determine whether an irreversible chain of cycles exists using Davenport Hasse's Theorem.

IV. CONCLUSION

Every Number Theory technique is significant in cryptography for concealing information. Many methods from Number Theory, such as primes, divisors, congruencies, and Euler's " function, are used in cryptography for security purposes. Congruencies are utilized in both Caesar ciphering key cryptography and RSA public key cryptography. This illustrates the concept of a cryptosystem in the context of Algebra and Number Theory.

REFERENCES

1. David, M. Burton, Elementary Number Theory, 2nd Edition, UBS Publishers.
2. G. H. Hardy, and E. M. Wright, An Introduction to the Theory of Numbers, 5th ed., Clarendon Press, 1979
3. Gilles Brassard, Modern Cryptography: A Tutorial , Lecture Notes in Computer Science, Vol.325, Springer-verlag,1988
4. Niven, Zuckerman and Montgomery, An Introduction to the Theory of Numbers, 5th ed., New York: John Wiley and Sons,1991
5. Neal Koblitz, A course in Number Theory and Cryptography, New York: Springer Verlag,1994
6. R. Cramer and V. shoup, A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Cipher Text Attack. In crypto'98, LNCS1716, pages13-25, Springer-Verlag, Berlin,1998
7. Simon Singh, The codebook, Anchor Books, 1999.
8. T. M. Apostol, Introduction to Analytic Number Theory, Springer-Verlag (New York),1976
9. The Trustees of Princeton University. (n.d.). Number theory – princeton university math club. Princeton University. Retrieved October 14, 2022, from https://blogs.princeton.edu/mathclub/guide/courses/number-theory/ Authors
10. Number theory and applications. (2009). https://doi.org/10.1007/978-93-86279-46-0
11. *Analytic number theory*. Analytic Number Theory | Department of Mathematics. (1970, January 1). Retrieved October 14, 2022, from https://math.yale.edu/analytic-number-theory

12. Rosen, K. H. Elementary Number Theory and Its Applications. Addision-Wesley, 1986.
13. Beckett, B. Introduction to Cryptology. Blackwell Scientific, 1988.
14. Seberry, J., and J. Pieprzyk. Cryptography: An Introduction to Computer Security. Prentice-Hall, 1989
15. Vinogradov, Ivan Matveevich. Elements of Number Theory. Dover Publications, 2003.
16. Weisstein, Eric W. The CRC Concise Encyclopedia of Mathematics. Boca Raton, FL: Chapman & Hall/CRC Press, 2003.