The International Conference on Computing Innovation and Applied Physics (CONF-CIAP 2022)
DOI: 10.54254/2753-8818/2/20220139

Development of Number Theory and the Application in Cryptography

Wenchao Shang

Shouguang modern high school, Shouguang, Shandong province, China, 262700

18266116699@163.com

Abstract. The primary focus of number theory, one of the fields of fundamental mathematics, is on the characteristics of integers. The development of cryptography also benefited greatly from the contributions of number theory. The paper primarily examines the evolution of number theory and its use in cryptography using a method of literature review. The study discovers that number theory development in the East reached a prosperous phase in the 1930s. From the 15th and 16th centuries through the 19th century, number theory flourished in the first. Number theory is still being developed, as demonstrated by the discovery of the biggest known prime number by American mathematician Curtis Cooper. Numerology is also extensively employed in cryptography, including the RSA technique and digital signatures. Numerous algorithms used in cryptography mostly depend on a working understanding of number theory.

Keywords: number theory, cryptography, application.

1. Introduction

Passwords have a long history in both ancient and modern times, and cryptography is a science with a rich past. Nearly all cryptographic algorithms require an understanding of number theory, hence it is crucial to advance this field. This work employs the method of a literature review to examine the history of number theory and how it is used in cryptography because few papers specifically address this aspect. Number theory is the study of properties of whole numbers. The core of number theory is the study of the properties of prime numbers because they are the fundamental units of integers. Integers are one of the earliest branches of mathematics. There are numerous intriguing problems and theories. The Goldbach conjecture serves as the best illustration. Number theory is the "queen of mathematics," lamented Gauss, the greatest mathematician of the 19th century [1]. The linkages between number theory and cryptography as well as their historical evolution are covered in this study to help readers better grasp these two fields.

2. Number theory

2.1. Number theory in the west

2.1.1. Number theory in the west around 300BC. The Elements of Euclid was a mathematical work written by the Greek mathematician Euclid around 300 BC. He talked about the knowledge of number

DOI: 10.54254/2753-8818/2/20220139

theory in the seventh, eighth, and ninth volumes of this book. The propositions are of pioneering significance to the development of number theory.

In the first proposition of book 7, Euclid puts forward the proposition that two numbers are prime to each other. When you have two unequal numbers, subtract the smaller number from the larger number until the remainder is less than the smaller number, then subtract the remainder from the smaller number until the remainder is less than the previous remainder, and so on, and if the remainder does not measure the previous number until the remainder is one unit, then the two numbers are prime to each other [1]. For example, 36and5, 36-5-5-5-5-5-5-5=1, which is less than 5, and the remainder is 1, so 36 and 5 are prime to each other.

The greatest common divisor of two numbers that are not prime to one another can be discovered using the method Euclid suggested in his second statement in Book Seven. The algorithm is known as "Euclidean's algorithm" to recognize and praise his efforts. For instance, the gcd for 30 and 54 is 6, since 30=24x1+6, 24=6x4=0, and 54=30x1+24.

Euclid demonstrated that the collection of prime numbers is infinite in book 9, statement 20. Assume that the number of primes a, b, c, etc. is finite. Euclid thought that N = (abc...n) + 1 was the result of multiplying their products. He then considered the following two options:

First, N is a new prime, which is larger than any element in the collection, if it is prime.

Second, N must have a prime factor, which cannot be one of the originals, in order for it to be composite. Start with the prime numbers 2 and 18 to get N = (2x19) + 1 = 40 as an example. This is a composite, although the originals don't contain its prime components, 3, or 13. The set of prime numbers is endless because a finite set of primes can never be exhausted.

The ideal number was proposed by Euclid in Book IX's final statement. 2k (2+4+6+8+10+..+2k) is a perfect number if the sum of its divisors is a prime number. For instance, the prime number 1 + 2 + 4 = 7, making the perfect number 1 + 2 + 4 = 28.

2.1.2. Number theory in the west around 250 BC. The ancient Greek mathematician Eratosthenes invented a way to find prime numbers. This way is called the sieve of Eratosthenes. If you want to find all primes up to n, you must subtract out all multiples of primes not greater than the square root of n, and what is left is a prime.

Given the range "n" of values to be screened, find the prime numbers within. Given the range "n" of values to be screened, find the prime numbers within. Then, the author uses 2 to sieve, that is, leave the 2 and the multiples of 2 out; then, the author takes the next prime number, which is 3, and keeps the 3, and gets rid of the multiples of 3; and then we use the next prime number, 5, and we keep the 5, and we get rid of the multiples of 5; Continue to repeat...

For example, when we look for all primes up to 25, we first list all the numbers: 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25. Then, the first prime in this set is 2, so keep 2 and delete multiples of 2. If the largest number in the sequence is less than the square of the prime chosen in the previous step, then all numbers in the remaining sequence are prime numbers. Otherwise, go back to step 2. In this case, 25 is greater than 2 squared, so we are going to go back to step 2. The first prime of the remaining numbers is 3, so we keep 3 and delete multiples of 3. In addition, 25 is also greater than 3 squared, so we're going to go back to step 2. The first prime of the remaining numbers is 5, so we keep 5 and delete multiples of 5. Lastly, because 23 is less than 5 squared, we stop the cycle. The prime numbers between 2 and 25 are 2, 3, 5, 7, 11, 13, 17, 19, and 23.

2.1.3. Number theory in the West around 15th,16th century to 20th century. Between early and medieval times, over 2000 years, number theory hardly advanced. It was the middle stage of the evolution of number theory from the 15th, 16th, and up until the 20th century.

Pierre de Fermat: Arithmetic, which the Greek mathematician Diophantine wrote about in the third century AD, was in use in Europe at the start of the seventh century. Fermat focused his research on the indefinite equations in the book and limited his study of them to the integer range.

Fermat made significant advances in number theory, including the following:

DOI: 10.54254/2753-8818/2/20220139

(1) Fermat's Last Theorem

When the integer n> 2, the equation x^n+y^n=z^n of x y z has no positive integer solution.

There is no positive integer solution to the equation x^n+y^n=z^n when the integer n > 2.

(2) Fermat's little theorem

If p is a prime number and the integer a is not a multiple of p, then a^（p-1）≡1（mod p). For example, when p is 3, a is 5. Then 5^(3-1)≡1(mod 3), it means 25-1=3x8.

In actuality, Fermat's Little Theorem is a specific case of Euler's Theorem. The formula for Euler's theorem is a^φ(n)-1≡0(mod n), where a and n are both positive integers and φ(n) is the Euler function, which denotes the quantity of prime to n positive integers that are less than n.

Euler's Theorem is actually an instance of Fermat's Little Theorem. The Euler theorem has the formula a^φ(n)-1≡0(mod n), where a and n are both positive numbers, and φ(n) is the Euler function, which denotes the number of prime to n positive integers fewer than n.

Adrien-Marie Legendre: Legendre was a pioneer of analytic number theory. I n 1798, he proposed a preliminary form of the distribution law of prime numbers. He made it more precise in 1808. Presented in the following form, if y is a prime and less than x, then $y=x/(\log_x -1.08366)$. He claimed and emphasized in 1830 that he had discovered this law by induction.

There were a lot of mathematicians in this period who were really driving the development of number theory, which will be revealed in future studies.

2.2. The development of number theory in the east

China was the first country in the world to adopt the decimal system, and mathematical tools such as arithmetical methods and abacus discs began to emerge, apply, and develop very early [2]. The ninety-ninth table and some contents of number theory were recorded in ancient arithmetic books, which were an important part of the brilliant achievements of ancient Chinese mathematics [3].

2.2.1. The decimal system. The universal decimal numeration system was first developed in China, and the earliest information about decimal numeration was found in the oracle bones of the Shang Dynasty. By the Spring and Autumn Period at the latest, the decimal value system had been quite perfect.[2] After that, the creation of Indian Arabic numerals became the world's easiest calculation tool and the most advanced numeration system.

2.2.2. The Pythagorean theorem. A right triangle in the plane has two sides and a hypotenuse that are equal in their squared lengths. In terms of math, if a right triangle has sides a and b and a and c is the hypotenuse, then a^2+b^2=c^2.

An exchange between Shang Gao and Zhou Gong is described in the pre-first century BC text Chou Pei Suan Ching. The hypotenuse of a right triangle is five when its two sides are three and four, respectively. The Pythagorean Theorem was developed by Chou Pei Suan Ching in the third century BC, and Zhao Shuang of the Three Kingdoms period elaborated on it and recorded it in The Nine Chapters on the Mathematical Art. He also provided a thorough demonstration of the theorem by mixing numbers and figures. The mathematician HuaHengfang proposed more than twenty proofs of the Pythagorean Theorem in the last stages of the Qing Dynasty.

2.2.3. Chinese remainder theorem. There is a classic problem in the Sun Zi sutra, which is that there are things you don't know how to count: Three three leaves two, five five leaves three, seven seven leaves two, ask geometry?

In this book, Sun Zi first proposed the congruence equations problem and the solution of the above problems.

In terms of congruence, it can be expressed as:

$x \equiv 2(\mod 3)$

$x \equiv 3(\mod 5)$

$x \equiv 2(\mod 7)$

DOI: 10.54254/2753-8818/2/20220139

2.2.4. The development of number theory in Modern China. From the 1930s, he made important contributions to analytic number theory, the Diophantine equation, uniform distribution, and so on. First-class number theory experts such as Hua Luogeng, Min Sihe, Ke Zhao, Chen Jingrun, and Pan Chengdong emerged. Since 1949, the study of number theory has been further developed. Chen Jingrun, Wang Yuan and others have made world-leading achievements in their research on the "sieve method" and "Goldbach conjecture". Zhou Haizhong has made outstanding achievements in the study of Mersenne prime distribution, a famous number theory problem.

3. Application of number theory in cryptography

3.1. The meaning of cryptography

The study of how to convey information covertly is known as cryptography. In the field of information coding known as cryptography, research is primarily concerned with how to transfer information covertly in the presence of adversaries. One of the most important research objectives of cryptography is confidentiality, realizing secret encoding of sensitive information, so it is called cryptography. They have a long history and were used in ancient times to transmit secret messages. The history of human use of passwords can be traced back to the ancient Babylonian clay tablets. Almost all civilizations in the history of the world have used passwords.

3.2. Application of number theory in cryptography

3.2.1. RSA algorithm. The RSA cryptosystem is an early example of a public key cryptosystem. In their article titled "Method of Obtaining Digital Signature and Public Key Cryptosystem" from 1978, MIT researchers Rivest, Shamir, and Adleman proposed the RSA cryptosystem, an asymmetric (public key) cryptosystem based on number theory. The foundation of the block cipher RSA is the idea that "the prime factorization of huge numbers is a daunting problem [3]." The difficulty of breaking apart large integers is the foundation of the RSA block encryption method. Its cornerstone is the generalized Euler theorem.

In order to make n a positive integer, ψ (n) =1 {0≤x≤n} x | 1 with the greatest common divisor n is 1. ψ (1) =1, ψ (2) =1, ψ (3) =2... ψ (p) =p-1 (p is prime). ψ is called the Euler theorem in number theory of euler functions. If omega and n are prime, then ω^ψ (n) must be several times the sum of n, plus the cryptography is a numeric language, but this time we're using decimal numbers. For example, consider the letters "S" and "A." Since S and A are ranked 19th and 1st, respectively, the corresponding numeric language for S and A is 1901 [4].

Theorem 1：if (a,n)=1, then a＝(mod n)

Theorem 2: if (m1,m2)=1, then φ(m1·m2)=φ(m1)·φ(m2).

Theorem 3: if p is a prime, then φ(p)=p-1.

The procedure for establishing RSA is as follows:

First pick two large prime numbers at random p, q. To calculate n=p x q.

Compute the Euler function φ(n)=(p-1)(q-1)

3) Select an integer e as the public encryption key, and obtain the secret decryption key d from e :d· e=1 mod φ(n)＝ k

4) Encryption/decryption:

The plaintext is divided into plaintext blocks m of less than n bits,

The encryption process is C =M^e (mod n)

The decryption process is M = C^d (mod n)

Under RSA: D(d, E(M，e)) = M (mod n)

E(e, D(d,M)) = M(mod n)

E and D are interchangeable. When used for a digital signature, the sender only needs to "encrypt" with its own decryption key d because only the sender is aware of its own d, and the receiver can only "decrypt" with the corresponding e to obtain the plaintext and confirm the sender's identity [4].

DOI: 10.54254/2753-8818/2/20220139

3.2.2. Digital signature algorithm. We know that in modern public keys, when someone sends you a message, public key D is used to encrypt it so that only you, who have private key E, can decrypt it and receive the plaintext message. The process of digital signature is slightly opposite to the encryption algorithm, but the principle is the same.

A digital signature encrypts the information sent to others with the private key e. As long as the other party can unlock the information with the public key d, it proves that the information was sent by you, forming the signature mechanism. Normally, when encrypting a message n, divide it up into smaller than n the first data packet mi (I | mi | < Log2n, usually less than 2k bits.)

If you need to encrypt a fixed group of messages, you can fill in some zeros to the left and make sure that the number is less than n. The encrypted ciphertext c consists of ci packets of the same length. The encryption process can be simply expressed as: ci = m (ie modn). When decrypting the message, take the ci of each encrypted packet and calculate xi=mi=ci^d (id modn).

RSA digital signature algorithm process:

First, select two prime numbers, P and q. In order to obtain maximum security in practical application, the length of the two prime numbers should be consistent and above 1024 bits. Calculate n=pq and euler function φ (n) = (p-1) (q-1).

Second, select encryption key randomly. e(1<e<φ (n)) and (e,φ (n)) = 1.

Third, the decryption key d is calculated using the Euclidean extended algorithm, satisfying ed =1 (modφ (n)), that is, ed = K φ (n) +1, so d≡ e^-1 (modφ (n)), where (d, n) =1.

Fourth, use e and n as public keys and d as private keys. The two prime numbers p and q are no longer needed and should be discarded immediately without divulge [5].

3.2.3. Advanced encryption standard. The processing unit is the part of the AES algorithm that processes bytes. Enter the key K after using 128-bit input plaintext. 16 bytes can be used to represent clear text. After ten rounds, there are four additional operations in addition to byte substitution, line displacement, columns, and mixing. Mixed columns are not performed in the most recent iteration. Additionally, it is important to note that the s-box substitution employed in byte substitution uses contemporary algebraic expertise to complete the encryption calculation [6].

3.2.4. Data encryption standard. There have been two most significant achievements in the field of cryptography since the 1950s. One of them is the data encryption standard, which was established by Tuchman and Meyer in 1971 according to the multiple encryption validity theory proposed by Shannon, the founder of information theory, and promulgated by the National Bureau of Standards in 1977. The Lucifer cipher, a block cipher using conventional encryption techniques, is essentially the basis for the DES cipher. Its symmetric approach works for both encrypting and decrypting data. Block encryption is accomplished using the DES encryption algorithm.

The plaintext is separated into blocks that are each 64 bits long. Following the initial transformation of the 64-bit data under the control of the 64-bit key, the 16-round encryption iteration is performed: the 64-bit data is split into left and right parts, each of which is 32 bits; the key is combined with the right part, followed by the left part, to produce the new right part; the former right half is then joined as the new left half. A round consists of these actions. 16 times are completed in this rotation. After the final round, the initial permutation's inverse is done, yielding a 64-bit cipher text. Three steps make up the DES encryption process: sub-key generation, encryption transformation, and processing [7].

3.2.5. Elgama. Cryptography involves Tahir Gaimor's 1985 Diffier-Hermann key exchange proposal, which is the foundation of the asymmetric ElGamal encryption technique. Both encryption and digital signatures can be performed with this technology. It is, along with RSA, one of the most representative public key cryptosystems [7].

The ELGamal public key cryptosystem has the following advantages: The system does not need to save secret parameters; all system parameters can be disclosed. The same plaintext encrypted by the same cipher at different times will produce different ciphertext (probabilistic cipher system), but the

DOI: 10.54254/2753-8818/2/20220139

computational complexity of the ELGamal system is greater than the RSA system. The most direct way to solve The ELGamal public key cryptosystem is to calculate the discrete logarithm, but there is no effective algorithm to solve the discrete logarithm over finite fields at present, so the ELGamal public key cryptosystem is safe when it is large enough [8].

3.2.6. Modern cryptography. The original origin of modern encryption can be found in Shannon's 1949 publication, The Communication Theory of Secure Systems. In this work, Shannon introduced information theory into the study of cryptography. He presented a model of a cryptosystem and used the concepts of probability, statistics, and entropy to mathematically describe and statistically examine the security of information sources, key sources, transmitted ciphertext, and cryptosystems. For modern cryptanalysis and cryptography, his work created a solid theoretical foundation. Modern cryptography has utilized both symmetric cryptography and public key cryptography to make mathematical applications to Shannon theory and number theory [9].

4. Conclusion

The growth of number theory and its use in cryptography are the main topics of this paper, while network security still needs to be improved through stronger cryptography. The study discovers that the 1930s marked the beginning of a prosperous phase for the development of number theory in the East. In the first, from the 15th and 16th centuries until the 19th century, number theory was in vogue. When American mathematician Curtis Cooper found the biggest known prime number, number theory was still evolving. The RSA method and digital signatures are just two examples of how frequently number theory is employed in cryptography. In cryptography, there are several algorithms that primarily depend on understanding of number theory.

Today's civilization uses encryption extensively in the network, and it is always evolving. As a result, network security has a lot to do with cryptography. The development of cryptography for network security focuses on security services, security methods, and security assaults. The author believes that the password component of network security needs to be improved more in the current era of ubiquitous networks in our daily lives.

In this paper, the introduction of the development of number theory is not very comprehensive; it only selects the key points for narration; there is no detailed investigation of the development of number theory in various periods in history, so there are shortcomings. Improvements can be made in access to data. Further research in this area will be carried out in the future.

References

[1] Euclid, *Elements of Euclid* [D]. Dent, 1993.
[2] Wangjun, On the development and influence of number theory in ancient China [J]. *Journal of Anyang Normal University*, 2014: 118-120
[3] Guohaimin. Application of number theory in cryptography [J]. *Computer Knowledge and Technology*, 2010: 4614-4618
[4] Liujia. Some applications of number theory in cryptography[J]. *New Courses' Study*, 2013：184-185
[5] Fujingbo. Application of number theory knowledge in cryptography [J]. *Scientific and Technological Innovation*, 2012: 183
[6] Huangyao. Analysis of the application of number theory in cryptography [J]. *Modern Communication,* 2017: 196
[7] Songyanhong, Kangbaoyuan. Application of number theory in cryptography [J]. *Divineland*, 2012: 30-31
[8] Chenminyi, Xiexiaojuan. Numbers and number theory [J]. *Open Class*, 2017: 94-95,112-113
[9] Zhangrong.The application of mathematics to cryptography [J]. *Telecom World*, 2016: 258