

## NUMBER THEORY AND ITS APPLICATIONS IN CYBERSECURITY: A REVIEW

ROMAN BOGOTYREV<sup>1</sup>

**ABSTRACT.** Modern number theory is a broad and fundamental branch of mathematics that studies the properties of integers and their relationships. This article provides an overview of the main topics and advancements in number theory, along with a discussion of practical applications of this theory in cybersecurity and cryptography.

### 1. INTRODUCTION

Modern mathematics provides a unique set of tools for understanding the deep structures and patterns that underlie many phenomena in our world. One of the most important fields in this context is number theory, which deals with the study of the basic properties of integers and their relationships. Great mathematicians such as Leonhard Euler, Pierre Fermat, Carl Friedrich Gauss, Terence Tao, Hermann Minkowski, Pafnutiy Chebyshev, and Hugo Riemann made significant contributions to the development of this field, discovering new laws and closely connecting number theory with other mathematical disciplines.

Number theory is concerned with numbers and their properties, i.e. numbers act here as the object of study. Natural series

$$1, 2, 3, 4, 5, \dots, 99, 100, 101, \dots$$

-the set of natural numbers is the most important area of research. The beginnings of the study of natural numbers date back to Ancient Greece. In the 17th century, P. Fermat, and in the 18th century, L. Euler, made huge contributions to the knowledge of natural numbers. While Fermat left many discoveries without proof, Euler created new methods and techniques, attaching proofs to them [17].

Number theory is one of the oldest branches of mathematics. These studies served as the basis for many branches of mathematics; number theory also uses analytical, algebraic, geometric, and many other methods to solve number-theoretic problems. Attempts to solve Fermat's theorem and problems related to the distribution of prime numbers stimulated the development of several branches of algebra [17].

Despite its ancient origins, the field of number theory has continued to be a hot topic in modern research. Its applications in constacyclic codes [2], investigations

---

*Date:* Received: Sep 12, 2024; Accepted: Nov 8, 2024.

\* Corresponding author.

2010 *Mathematics Subject Classification.* Primary 46L55; Secondary 44B20.

*Key words and phrases.* Prime numbers, Fermat's theorem, Cryptography, Euler's theorem.

into the properties of prime numbers [13, 14, 15], integral points [23], and other topics have attracted continuous interest among the researchers.

Our goal in this study is to provide an overview of the major existing results in number theory, as well as describe its key applications in computer science and other fields. We present both statements and proofs of the theorems for the benefit of the reader. In Section 2, together with proofs, we will analyze in detail one of the most important theorems in number theory: Fermat’s Theorem and Euler’s Theorem, which follows from it.

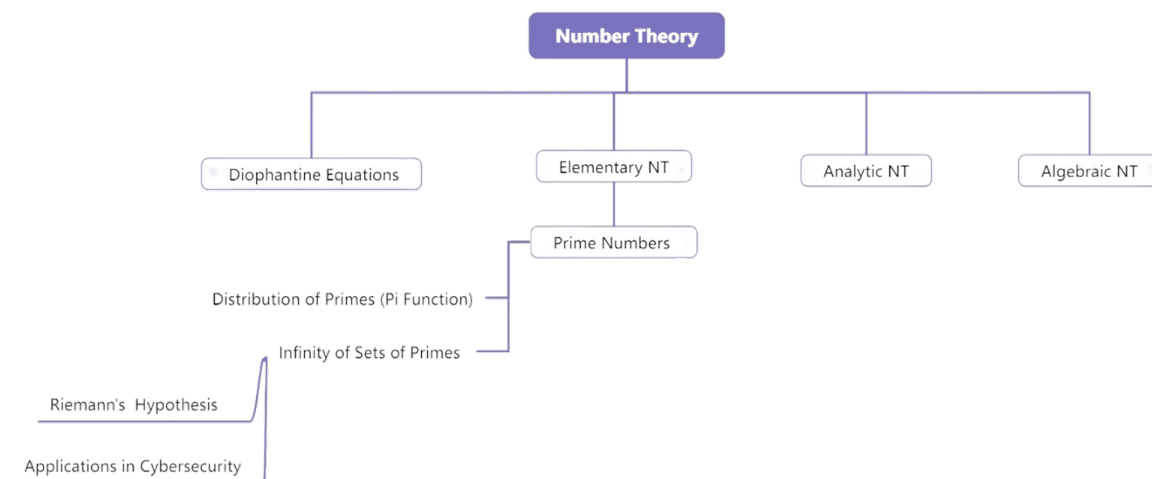


FIGURE 1. Main sections and subsections in number theory

## 2. MAIN RESULTS

Number theory, the branch of mathematics focused on the properties and relationships of numbers, forms the foundation of many modern cybersecurity methods. Cryptographic algorithms, which protect data, heavily rely on number theory to create secure encryption, authentication systems, and network security. Let’s explore how key mathematical concepts are applied to safeguard information.

**2.1. Diophantine Equations in Cybersecurity.** Diophantine equations are equations where the solutions must be integers. These equations are widely used in cybersecurity, particularly in cryptography, where they help create encryption algorithms.

- (1) **Cryptography (Data Encryption):** One of the most widely used encryption methods is **RSA**. It relies on the difficulty of factoring large numbers into prime factors and uses a Diophantine equation to compute the private key:

$$d \times e \equiv 1 \pmod{\phi(n)}$$

Here,  $e$  is the public key, which is known to everyone, and  $d$  is the private key, known only to the owner.  $\phi(n)$  is Euler's totient function, crucial in RSA calculations. This equation ensures that  $d$  and  $e$  are linked via the modulus  $\phi(n)$ , and only  $d$  can decrypt the data [22].

**Example 2.1.** : Let  $e = 7$ ,  $\phi(n) = 40$ . We need to find  $d$  such that  $d \times 7 \equiv 1 \pmod{40}$ . This implies that  $7d - 1$  must be divisible by 40. Solving this, we find  $d = 23$ .

This equation ensures the security of the RSA system because finding the private key  $d$  without knowing the prime factors of  $n$  is computationally difficult.

- (2) **Authentication and Authorization:** Diophantine equations also play a role in authentication systems. They are used to create complex access keys that allow systems to verify whether a user is authorized to access the data. For instance, some systems use mathematical challenges to verify user identity, ensuring only the rightful user can log in [22].
- (3) **Network Security Analysis:** Integer arithmetic helps in analyzing network traffic and detecting anomalies. For example, if the structure of data changes in an unusual way, it may indicate an attack, and number theory helps identify such shifts.[1]

**2.2. Fermat's Last Theorem in Cybersecurity.** Fermat's Last Theorem states that there are no positive integers  $a$ ,  $b$ , and  $c$  that satisfy the equation:

$$a^n + b^n = c^n$$

for any value of  $n > 2$ . While this theorem was proven in 1994, it has significant implications for cryptography and data security [24].

- (1) **Cryptography (Data Protection):** Fermat's Last Theorem strengthens cryptographic algorithms like RSA. The principles of the theorem show that it is impossible to easily find solutions to certain types of equations, which makes cryptographic systems more resistant to attacks. For example, breaking RSA requires factoring the product of two large prime numbers, which is computationally hard. The principles behind Fermat's Last Theorem reinforce the difficulty of finding solutions to these types of problems [5, 3].
- (2) **Digital Signatures:** Fermat's Last Theorem also helps in developing digital signature systems, which are used to verify the authenticity of data. These systems rely on the complexity of mathematical problems, and only someone with the private key can create the correct signature [10].

Fermat's theorem continues to attract the interest of researchers [11].

**2.3. RSA Encryption.** RSA is one of the most widely used public-key encryption methods, and its security is deeply tied to number theory, especially prime numbers and modular arithmetic.

2.3.1. *Key Generation.*

- (1) **Step 1: Choosing Prime Numbers** RSA starts by selecting two large prime numbers  $p$  and  $q$ . The security of RSA depends on the difficulty of factoring their product.
- (2) **Step 2: Calculating the Modulus** The modulus  $n$  is computed as the product of the two primes:

$$n = p \times q$$

This number  $n$  is used in both the public and private keys.

- (3) **Step 3: Euler's Totient Function** Euler's totient function  $\phi(n) = (p - 1)(q - 1)$  is used to compute the private key. This function counts the number of integers less than  $n$  that are coprime with  $n$ .
- (4) **Step 4: Choosing the Public Key** The public key  $e$  is chosen such that  $\gcd(e, \phi(n)) = 1$ . This ensures that  $e$  does not share common factors with  $\phi(n)$ , allowing secure encryption of data.
- (5) **Step 5: Calculating the Private Key** The private key  $d$  is found by solving the Diophantine equation:

$$d \times e \equiv 1 \pmod{\phi(n)}$$

This equation ensures that the private key can decrypt messages encrypted with the public key.

2.3.2. *Encryption and Decryption.*

- (1) **Encryption** A message  $M$  is encrypted using the public key  $e$  and modulus  $n$  by the formula:

$$C = M^e \pmod{n}$$

where  $C$  is the ciphertext.

- (2) **Decryption** Decryption uses the private key  $d$  and the formula:

$$M = C^d \pmod{n}$$

to recover the original message  $M$ .

2.3.3. *RSA Security.* RSA's security relies on the difficulty of factoring  $n = p \times q$  into its prime factors. If  $n$  consists of very large primes, factoring it and finding the private key without knowing  $p$  and  $q$  is practically impossible.

2.4. **Hashing in Cryptography.** **Hashing** is the process of converting input data into a fixed-length string called a "hash." Hashes are used to store passwords, create digital signatures, and index databases [19].

2.4.1. *Hash Functions and Prime Numbers.* Prime numbers play a crucial role in creating secure hash functions. Using prime numbers helps minimize **collisions**—cases where two different inputs produce the same hash.

**Example 2.2.** Let's consider a simple example of hashing a string using modular arithmetic. Suppose we want to hash the string "hello". The process could be as follows:

- (1) Convert each character to its ASCII code: "h" = 104, "e" = 101, "l" = 108, "l" = 108, "o" = 111.
- (2) Sum the codes:

$$104 + 101 + 108 + 108 + 111 = 532.$$

- (3) Take the result modulo a prime number, say 13:

$$532 \bmod 13 = 12.$$

Thus, the hash value for the string "hello" is 12. This process can be made more complex to enhance security, but the core idea involves using prime numbers and modular arithmetic to create a hash.

### 3. PRIME NUMBERS

**3.1. Distribution of prime numbers.** A natural number is called prime if it is greater than 1 and cannot be represented as a product of smaller natural numbers. A prime number  $p$  has only two positive divisors: 1 and  $p$ .

The distribution of prime numbers refers to the asymptotic behavior of the function  $\pi(x)$ , where  $\pi(x)$  is the number of prime numbers less than or equal to  $x$ , for  $x \geq 0$ , as  $x \rightarrow \infty$ . Studying the initial segments of a sequence of prime numbers shows that as  $x$  increases, primes become rarer on average. There are long segments of natural numbers among which no primes exist. However, there are also prime numbers whose difference is two, called twin primes. For example, the numbers 10,006,427 and 10,006,429 are twin primes (Curtis Cooper, 2012).

Theorem Euclid asserts that  $\pi(x) \rightarrow \infty$  as  $x \rightarrow \infty$ . L. Euler introduced the zeta function in 1737.

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}, \quad \text{where } s = \sigma + it, \sigma > 0.$$

Euler proved that:

$$\sum_{n=1}^{\infty} n^{-s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1},$$

where the summation is carried out over all natural numbers, and the product is carried out over all prime numbers [24]. This formula belongs to Euler, who proved it himself in 1737 [17]. This identity and its generalizations play a fundamental role in the theory of distribution of prime numbers. Based on it, Euler proved that the series  $\sum \frac{1}{p}$  and the product  $\prod \left(1 - \frac{1}{p^s}\right)^{-1}$  with respect to prime  $p$  diverge, from which Euclid's theorem follows. Moreover, Euler established that there are "many" prime numbers, since  $\pi(x) > \ln(x) - 1$ , and at the same time, almost all natural numbers are composite, since  $\frac{\pi(x)}{x} \rightarrow 0$  as  $x \rightarrow \infty$ .

In 1837, while studying the question of the infinity of prime numbers in arithmetic progressions  $nk+l$ ,  $n=0,1,\dots$ , where  $k, l$  are coprime, P. Dirichlet considered an analogue of the Euler product

$$\prod_p \left(1 - \frac{x(p)}{p^s}\right)^{-1},$$

where  $\chi(p)$  satisfies the conditions: not identically zero, periodic with period  $k$  and completely multiplicative, i.e.  $\chi(nm) = \chi(n)\chi(m)$  for any integers  $n, m$  [6, 9]. For  $s > \theta$ , an analogue of Euler's identity is valid:

$$\sum_{n=1}^{\infty} \frac{(n)X}{n^s} = \prod_p \left(1 - \frac{x(p)}{p^s}\right)^{-1}.$$

The series on the left is called the Dirichlet series. By studying the behavior of such series as  $s \rightarrow 1 + \theta$ , Dirichlet proved his theorem on the infinity of the number of prime numbers in arithmetic progressions.

P. L. Chebyshev in 1851 proved that there are constants  $a$  and  $b$  such that

$$a \frac{x}{\ln x} < \pi(x) < b \frac{x}{\ln x},$$

where he established that if there is a limit  $\frac{2}{\ln 2} < ab < 2 \ln 2$

$$\frac{\pi(x) \ln x}{x}$$

for  $x \rightarrow \infty$ , then it is equal to 1 [24].

**3.2. The infinity of the set of prime numbers.** Factors whose product is decomposed into a certain composite number are its divisors. If a natural number is divisible by some smaller number other than 1, then it follows that the natural number is composite. Since all even numbers greater than 2 are divisible by 2, they are all composite. And the number 7 is not divisible by any of the numbers 2, 3, 4, 5, 6, then it is prime. In this way, you can check any number, for example 1009, but it will need to be divided by the entire number from the series 2, 3, 4, 5, ..., 1008. This is a very long and irrational solution; a simpler solution will be if you use the following statement [6, 9].

**Lemma 3.1.** (Euclid, 300 BC) Let  $N$  be a composite number and  $p$  the smallest of its divisors satisfying the condition  $p > 1$ . Then  $p$  is a prime number and  $p^2 \geq N$ .

*Proof.* Since  $N$  is a composite number, then by definition  $N = u \times v$ , provided that  $1 < u < N$  and  $1 < v < N$ . By the conditions of 3.1, it follows that  $p^2 \geq u \times v = N$ .

Let  $d$ -divisor  $p$ , different from 1, having properties  $d|p, p|N$  it follows that  $d$  is a divisor of  $N$ , by the definition of  $p$ , we have  $d \geq p$ . So, the number  $p$  has no divisors, satisfying the condition  $1 < d < p$ . This means  $p$  is a prime number.

**Corollary 3.2.** [17] Every integer  $N > 1$  has a prime divisor.

*Proof.* If  $N$  is a prime number, then the statement is true, since  $N|N$ . But if  $N$  is a composite number, the statement holds by Lemma 2.1.

*Theorem 1 states that if 1009 is a composite number, then it has a prime divisor  $p$ , satisfying the condition  $2 \leq p \leq 31$ . Since all even numbers other than 2 are not prime, and the numbers divisible by 3 are 9, 15, 21, 27, as well as the number  $25 = 5 \times 5$ , it follows that the possible divisors 1009 is contained among the numbers*

*2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31.*

*Now we can find that none of them is a divisor of 1009, so it is a prime number.*

**Theorem 3.3.** (Euclid, 300 BC) The set of prime numbers is infinite.

*Proof. Let us assume that prime numbers form a finite set  $\{p_1, p_2, \dots, p_m\}$ . Consider the natural number  $N = p_1 p_2 \dots p_m + 1$ . According to Corollary 2.1, it has a prime divisor  $p$ . If the number  $N$  is not divisible by any of the numbers  $p_1, p_2, \dots, p_m$ , but is divisible by  $p$ , then the prime number  $p$  is different from each of the numbers  $p_1, p_2, \dots, p_m$ . The resulting contradiction completes the proof of Euclid's prime number theorem [6].*

**3.3. The Riemann Hypothesis in Cybersecurity.** The Riemann Hypothesis is considered one of the most famous problems in mathematics, especially in number theory. The hypothesis is fundamental to the distribution of prime numbers. Although it is mostly theoretical and may initially seem useless, its potential proof could have a significant impact on cryptography and cybersecurity in general, as the distribution of prime numbers underpins RSA encryption. This section explores how the Riemann Hypothesis could be applied in cybersecurity and how it might affect existing cryptographic methods.

**3.3.1. Overview of the Riemann Hypothesis.** The Riemann zeta function is defined for complex numbers  $s = \sigma + it$  (where  $\sigma$  and  $t$  are real numbers) as:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

The Riemann Hypothesis posits that all non-trivial zeros of this function have a real part equal to  $\frac{1}{2}$ , meaning:

$$\operatorname{Re}(s) = \frac{1}{2}$$

This hypothesis is deeply connected to the distribution of prime numbers through the prime-counting function  $\pi(x)$ , which estimates the number of primes less than or equal to a given number  $x$ . The relationship between the zeta function and prime numbers is expressed in the following formula:

$$\pi(x) = \operatorname{Li}(x) - \sum_{\rho} \operatorname{Li}(x^{\rho})$$

where  $\operatorname{Li}(x)$  is the logarithmic integral, and  $\rho$  represents the non-trivial zeros of the zeta function. The accuracy of this formula depends on the location of these zeros. If the Riemann Hypothesis is proven true, it would provide a more precise understanding of how prime numbers are distributed [18].

3.3.2. *Impact on Cryptography.* Present-day cryptographic techniques such as RSA only function due to the fact that it is difficult to find the prime numbers needed. Securely encrypting data relies on the assumption that other party is not able to foresee the series of prime numbers and that given a very huge number which is a product of two other prime number (a semi-prime number) one cannot break it itself into its component prime numbers. On one hand, the prime number theorem suggests there are few large primes; on the other, it means that attempts to locate such heads of long lists of primes are normally futile. Should the converse of the Riemann zeta hypothesis be established, this would further clarify the once-puzzling question of the distribution of prime numbers as well as the viability of prime-based encryption [12, 5].

3.3.3. *RSA Encryption and the Riemann Hypothesis.* RSA encryption's security relies on the difficulty of factoring a large number  $n$ , which is the product of two primes,  $p$  and  $q$ :

$$n = p \times q$$

The time required to factor  $n$  into  $p$  and  $q$  increases significantly as  $p$  and  $q$  grow larger. The Riemann Hypothesis could provide more precise bounds on the distribution of primes, which may impact the assumptions we make about the density and location of large primes. This could either:

- **Strengthen RSA:** If the Riemann Hypothesis confirms that primes are more evenly distributed than previously thought, it could boost confidence in RSA's security by reinforcing the difficulty of prime factorization.
- **Weaken RSA:** On the other hand, proving the Riemann Hypothesis could lead to new mathematical insights that make factoring large numbers easier. For instance, more efficient algorithms might emerge that exploit the refined distribution of primes, potentially making RSA vulnerable to faster factoring techniques [18].

3.3.4. *Prime Number Generation and the Riemann Hypothesis.* The role of prime numbers is indispensable in any cryptographic protocol which is true for RSA as well as for many other protocols including Diffie-Hellman key exchange, and ECC. Specifically these protocols need the generation of large random primes. Technically speaking the Riemann Hypothesis about the zeros of the Riemann zeta-function could impact on the algorithms for generating such primes.

3.3.5. *Faster Prime Generation.* Should the Riemann Hypothesis be confirmed, advances in the algorithms for producing large prime numbers may also take place for more than one reasons, including the better understanding of the distances between successive prime numbers. As of now, the existing procedures use random numbers and carry out what is known as number testing to determine whether the generated number is a prime or not. The premise of the Riemann Hypothesis is correct, such deterministic algebraic principles for generating long single digit primes could be better augmented and the prediction of such single digit primes would become less time consuming catering to the need of shortening the key generation time of cryptography [17].

**Example 3.4.** : if we denote the gap between consecutive prime numbers  $p_n$  and  $p_{n+1}$  as  $g_n = p_{n+1} - p_n$ , the Riemann Hypothesis could offer tighter bounds on  $g_n$ . These bounds would allow us to predict the next prime's location more accurately, making prime generation more efficient.

3.3.6. *Hash Functions and the Riemann Hypothesis.* Hash functions have significant implications in cybersecurity since they enable the manipulation of data into a collection of characters that are of a specific length. Secure hashing techniques are often considered along with the use of prime numbers. Although the Riemann Hypothesis has no direct bearing on the design and implementation of hashing it is possible that in the future it might influence the development of methods for generating prime numbers for cryptographic systems [8, 20].

**Example 3.5.** Cryptographic hash functions like SHA-256 require several mathematical computations for encryption, e.g., prime numbers. A real proof of the Riemann hypothesis could greatly advance knowledge on the use of modulo arithmetic and also divide methods, which contribute to production of better and effective hashing algorithms [12, 19].

3.3.7. *Future Directions: Post-Quantum Cryptography.* Moreover, it is worthwhile to remember that post-quantum cryptography might have some links with the Riemann Hypothesis. This is an active direction of research, aimed primarily at the creation of such encryption algorithms, the security of which will be quantum computer resistant. Quantum computers could render traditional cryptosystems such as RSA ineffective by, for instance, decrypting traffic using p-1 method. Knowledge gained from the Riemann Hypothesis could assist in the very design of the construction of the encryption schemes immune to such conditions.

**Example 3.6.** Both lattice and elliptic curve cryptosystems depend on different algebro-geometric structures, including number theory. Thus, an effective rationale for decreases in the distribution of primes factors in case of smaller prime numbers precludes facilitation of these systems also for post-quantum use.[21]

## 4. FERMA'S LITTLE THEOREM AND ITS GENERALIZATIONS

### 4.1. Little theorem Ferma's.

**Theorem 4.1. *Ferma's theorem.*** [24] *Let p be a prime number. As is known, Fermat's little theorem states that*

$$a^{p-1} \equiv 1 \pmod{p} \tag{4.1}$$

*for every integer a not divisible by p, or, equivalently,*

$$a^p \equiv a \pmod{p} \tag{4.2}$$

*for every integer a.*

*Proof.* [24] Let there be  $p$  objects arranged in a circle, each of which must be painted in one of a colors. The number of all colorings is obviously equal to  $a^p$ .

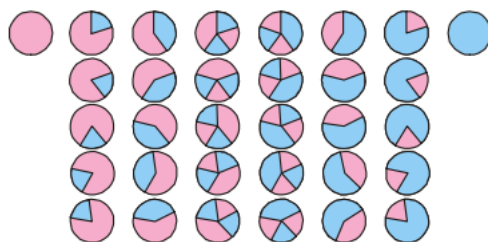


FIGURE 2. Circle colorings

Suppose that a certain coloring transforms into itself when rotated through some angle,  $\frac{2\pi d}{p}$   $0 < d < p$ . We will consider  $d$  to be the smallest possible and divide  $p$  by  $d$  with  $a$  remainder:

$$p = qd + r, \quad 0 \leq r < p.$$

It is clear that this coloring transforms into itself when rotated by an angle  $\frac{2\pi qd}{p} = 2\pi - \frac{2\pi r}{p}$  and, therefore, - and when turning through an angle  $\frac{2\pi r}{p}$ . Due to the choice of  $d$ , we obtain that  $r = 0$ , i.e.,  $d$  divides  $p$ . Since  $p$  is a prime number, then  $d = 1$ , i.e. this coloring is one-color.

The number of one-color colorings is equal to  $a$ . We divide all other  $p$ - $a$  colorings into classes, assigning to one class the colorings obtained from each other by rotations. By virtue of the previous, each class consists of  $p$  colorings. Hence comparison (4.2) follows.  $\square$

**4.2. Euler's theorem.** For any natural number  $m$ ,  $\varphi(m)$  denotes the number of natural numbers not exceeding  $m$  and relatively prime to  $m$ . The function  $\varphi$ , called the Euler function, has the following multiplicative property: if  $m_1$  and  $m_2$  are relatively prime natural numbers, then

$$\varphi(m_1 m_2) = \varphi(m_1) \varphi(m_2). \tag{4.3}$$

If  $m = p$  is a prime number, then  $\varphi(m) = p - 1$ . If  $m = p^n$ , then  $\varphi(m) = p^n - p^{n-1}$ .

Euler's theorem (Euler, 1736) states that

$$a^{\varphi(m)} \equiv 1 \pmod{m} \tag{4.4}$$

for any integer  $a$  coprime to  $m$ . This is obviously a generalization of Fermat's little theorem.

If  $m = m_1 m_2$ , where  $m_1$  and  $m_2$  are coprime, then to prove comparison (4.4) it is enough to check that

$$a^{\varphi(m)} \equiv 1 \pmod{m_1} \text{ and } a^{\varphi(m)} \equiv 1 \pmod{m_2}. \tag{4.5}$$

Taking into account (4.3), we obtain that

$$a^{\varphi(m)} = (a^{\varphi(m_2)})^{\varphi(m_1)} = (a^{\varphi(m_1)})^{\varphi(m_2)} \tag{4.6}$$

and, therefore, comparisons (3) follow from Euler's theorem for modules  $m_1$  and  $m_2$ . This reasoning shows that it is enough to prove Euler's theorem for  $m = p^n$ , where  $p$  is a prime number. In this case it takes the form

$$a^{p^n - p^{n-1}} \equiv 1 \pmod{p^n} \quad (4.7)$$

for any integer  $a$  not divisible by  $p$ . Comparison (4.7) is equivalent to comparison

$$a^{p^n} \equiv a^{p^{n-1}} \pmod{p^n} \quad (4.8)$$

Moreover, the last comparison is obviously true for  $a$  that is a multiple of  $p$ , since in this case both of its parts are divisible by  $p^n$ . We present three proofs of Euler's theorem, generalizing the corresponding proofs of Fermat's little theorem.

*Proof (Euler, 1736).* Consider the ring  $\mathbb{Z}_m$  of residues modulo  $m$ . We will denote the reduction of an integer  $a$  by  $\alpha$ . The invertible elements of the ring  $\mathbb{Z}_m$  form a group under multiplication. As is known, the element  $\alpha$  is invertible in  $\mathbb{Z}_m$  if and only if the number  $a$  is coprime to  $m$ . This means that the order of the group of invertible elements is equal to  $\varphi(m)$ . From here, as in the first proof of Fermat's little theorem, comparison (4.4) follows.

## 5. DIOPHANTINE EQUATIONS

**Definition 5.1.** A Linear Diophantine equation with two unknowns is called an equation of the form

$$Ax + By = C,$$

where  $A$ ,  $B$ , and  $C$  are given non-zero integers, and  $x$  and  $y$  are unknown integers. If the number  $C$  is not divisible by  $\gcd(|A|, |B|)$ , then the equation has no solutions, since in this case the left side is divisible by  $\gcd(|A|, |B|)$  but the right side is not. Otherwise, the equation can be divided by  $\gcd(|A|, |B|)$  to obtain the equation

$$ax + by = c,$$

in which the numbers  $a$  and  $b$  have no common divisor other than 1. Assume that  $(x_0, y_0)$  is a solution. We will show how to obtain all other solutions (and there are infinitely many) of the Diophantine equation. Since

$$ax_0 + by_0 = c,$$

for any pair of numbers  $(x, y)$  satisfying the equation  $ax + by = c$ , the following identity holds:

$$ax + by = ax_0 + by_0.$$

Therefore,  $a(x - x_0) = b(y_0 - y)$ . But since  $a$  and  $b$  have no common divisor other than 1, it follows that  $x - x_0$  is divisible by  $b$ . Let  $x - x_0 = kb$ , then  $y_0 - y = ka$ .

As a result, we get the entire set of solutions:  $x = x_0 + kb$ ,  $y = y_0 - ka$ , where  $k$  is any integer.

*Remark 5.2.* To find a particular solution  $(x_0, y_0)$  of the equation  $ax + by = c$ , where  $\gcd(a, b) = 1$ , one can use the Euclidean algorithm. First, find a solution

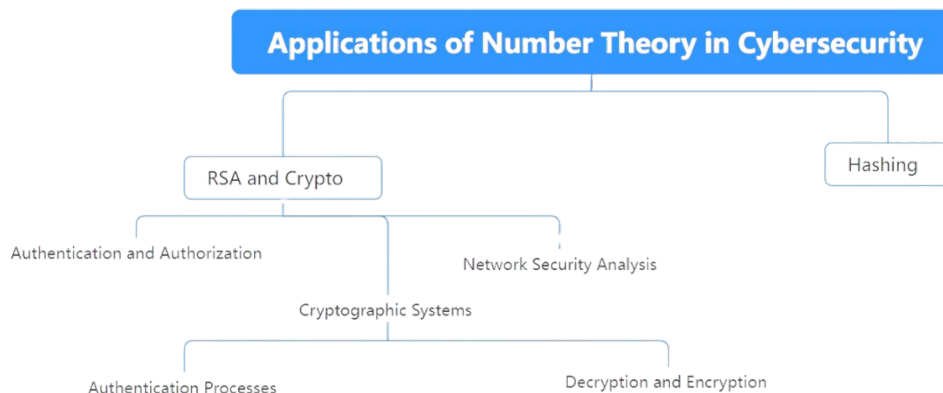


FIGURE 3. Applications of Number Theory in Cybersecurity

$(x_0, y_0)$  to the equation  $ax + by = \gcd(a, b)$  using the algorithm. Then,  $(cx_0, cy_0)$  will be a solution to the equation  $ax + by = c$ .

## 6. THE ROLE OF NUMBER THEORY IN MODERN CYBERSECURITY

As cyber threats continue to escalate, protecting sensitive information has become critically important. Number theory, a branch of pure mathematics, plays a key role in the development of cryptographic protocols essential for data security. Modern research highlights its significance in various encryption systems and security methodologies [1, 4].

**6.1. Fundamental Concepts in Number Theory.** Key concepts such as prime numbers, modular arithmetic, and discrete logarithms are foundational for cryptographic algorithms, including RSA and the Diffie-Hellman protocol. The security of RSA relies on the difficulty of factoring large composite numbers, while modular arithmetic enables efficient operations on large integers [9, 10]. These mathematical principles ensure data integrity and confidentiality.

**6.2. Applications in Cryptography.** Number theory underpins numerous cryptographic schemes, such as elliptic curve cryptography (ECC), which offers enhanced security with smaller key sizes. This efficiency makes ECC particularly advantageous in resource-constrained environments. Research is continuously adapting number-theoretic methods to address emerging cyber threats, underscoring their relevance in the digital landscape [3, 21].

**6.3. Future Directions.** The future of number theory in cybersecurity lies in its integration into composite encryption systems. Developing hybrid schemes that leverage the strengths of various number-theoretic methods will enhance information security [16, 7]. However, the complexity of these methods poses challenges for implementation, highlighting the need for ongoing research to simplify and optimize their applications.

## 7. CONCLUSION

Number theory, as one of the oldest fields in mathematics, plays a vital role in modern cryptography and cybersecurity. Concepts such as prime numbers, Diophantine equations, and Fermat's Theorem have significant applications in securing data and creating cryptographic algorithms. Prime numbers are essential in encryption methods, and Diophantine equations have practical applications in security, coding, and optimization. The proof of Fermat's Last Theorem has further strengthened cryptographic systems. The Riemann Hypothesis remains an unsolved mystery that could unlock deeper insights into the distribution of primes, impacting the future of digital security.

Fermat's Last Theorem, after a long-standing challenge, was proven in 1994 by Andrew Wiles. This result not only left a significant mark on the history of mathematics but also has applications in modern cybersecurity. The proof of Fermat's Theorem enhanced the security of cryptographic systems and data protection, as it complicated number factorization attacks.

The application of Diophantine equations and Fermat's Last Theorem in cybersecurity is a vivid example of how theoretical mathematical concepts permeate our daily lives. RSA, an algorithm that employs these mathematical principles, has become a foundational element of privacy protection on the Internet, ensuring secure encryption and authentication. Cybersecurity remains a critical aspect of the modern world, and number theory plays a vital role in its safeguarding.

In conclusion, number theory remains a cornerstone of both theoretical and applied mathematics, significantly influencing cryptography, data security, and the development of encryption technologies. The mathematical concepts explored, such as prime numbers, Diophantine equations, and Fermat's Last Theorem, illustrate the profound impact that abstract mathematics can have on modern technological advancements. As cybersecurity continues to grow in importance, the ongoing exploration of number theory will remain critical to safeguarding the digital world.

## REFERENCES

1. Abakumova, S. I. (2023). Development of Number Theory and the Application in Cryptography. <https://doi.org/10.54254/2753-8818/2/20220139>
2. Ahendouz, Y., & Ismail Akharraz. (2024). A class of constacyclic codes of length  $2p^s$  over  $F_{pm}[u,v] / \langle u^2, v^2, uv - vu \rangle$ . Gulf Journal of Mathematics, 17(2), 73-90. <https://doi.org/10.56947/gjom.v17i2.1918>
3. Arun, R., Kumar, P. (2019). Number theory: Cryptography and Security. Pharma Innovation. <https://doi.org/10.22271/tpi.2019.v8.i2n.25455>
4. Boneh, D. (1999). Twenty years of attacks on the RSA cryptosystem. Notices of the AMS, 46(2), 203-213. <https://doi.org/10.1090/S0273-0979-99-00883-7>
5. Brij, B., Gupta, D. P., Agrawal, S. Y. (2016). Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security. <https://doi.org/10.4018/978-1-5225-0105-3>
6. Bukhshtab, A. A. (2022). Number Theory. St. Petersburg: Lan'. <https://mahalex.net/151-153/Buchstab.pdf>

7. Cherckesova, L. V., Safaryan, O. A., Lyashenko, N. G., & Korochentsev, D. A. (2022). Developing a new collision-resistant hashing algorithm. *Mathematics*, 10(15), 2769. <https://doi.org/10.3390/math10152769>
8. Chi, L., & Zhu, X. (2017). Hashing techniques: A survey and taxonomy. *ACM Computing Surveys (Csur)*, 50(1), 1-36. <https://doi.org/10.1145/3047307>
9. Skabelund, D. (2022). Number Theory. <https://doi.org/10.1201/9780429354649-12>
10. Page, D., & Smart, N. P. (2014). Safety in Numbers: Modern Cryptography from Ancient Arithmetic. [https://doi.org/10.1007/978-3-319-04042-4\\_8](https://doi.org/10.1007/978-3-319-04042-4_8)
11. Gallardo, L. (2022). Special case of Fermat's Theorem. *Gulf Journal of Mathematics*, 13(2), 12-18. <https://doi.org/10.56947/gjom.v13i2.868>
12. Habr. (2023). RSA encryption. <https://habr.com/ru/articles/745820/>
13. Jakimczuk, R. (2023). Two topics in number theory: the greatest k-free number that divides n and formulas for composite and prime numbers. *Gulf Journal of Mathematics*, 14(1), 33-44. <https://doi.org/10.56947/gjom.v14i1.1089>
14. Jakimczuk, R. (2023). Some questions on the distribution of prime gaps and some formulas involving prime gaps. *Gulf Journal of Mathematics*, 15(1), 7-41. <https://doi.org/10.56947/gjom.v15i1.1380>
15. Jakimczuk, R. (2024). Square-full numbers multiple of a certain set of primes and hybrid numbers. *Gulf Journal of Mathematics*, 16(1), 136-149. <https://doi.org/10.56947/gjom.v16i1.1786>
16. Zhu, L. (2024). Profound integration of elementary number theory in composite encryption systems: A mathematical security exploration. *Theoretical and Natural Science*. <https://doi.org/10.54254/2753-8818/36/20240505>
17. Nesterenko, Y. V. (2008). Number Theory. Petrograd: Academia. <https://mmmf.msu.ru/lect/nesterenko/mainnth.pdf>
18. Orús-Lacort, M., Orús, R., Jouis, C. (2023). Analyzing Riemann's hypothesis. *Ann Math Phys*, 6(1), 075-082. <https://doi.org/10.17352/amp.000083>
19. Redaoui, A., Belalia, A., Belloulata, K. (2024). Deep supervised hashing by fusing multiscale deep features for image retrieval. *Information*, 15(3), 143. <https://doi.org/10.3390/info15030143>
20. Salakhutdinov, R., Hinton, G. (2009). Semantic hashing. *International Journal of Approximate Reasoning*, 50(7), 969-978. <https://doi.org/10.1016/j.ijar.2009.04.007>
21. Samad, A. (2023). Number Theory and Cryptography: Unraveling the Foundations of Data Security. <https://doi.org/10.31219/osf.io/5sczk>
22. Shand, M., Vuillemin, J. (1993, June). Fast implementations of RSA cryptography. In *Proceedings of IEEE 11th Symposium on Computer Arithmetic* (pp. 252-259). IEEE. <https://doi.org/10.1109/ARITH.1993.175044>
23. Undrakh, B., & Bat-Ochir, G. (2022). Refinement of the upper bound of the radius of a circular integral points set. *Gulf Journal of Mathematics*, 12(1), 28-40. <https://doi.org/10.56947/gjom.v12i1.774>
24. Vinberg, E. B. (2008). Fermat's Little Theorem and its generalizations. *Journal of Mathematical Education, Series 3, Issue 12*, 43-53.
25. Dimitrov, W. (2023). Mathematical Approaches Transform Cybersecurity from Proto-science to Science. <https://doi.org/10.3390/app13116508>

<sup>1</sup>DEPARTMENT OF COMPUTER SCIENCE, CANADIAN UNIVERSITY DUBAI, DUBAI, UAE.  
*Email address:* [bogotyrev27@gmail.com](mailto:bogotyrev27@gmail.com)