ROSSIISKAYA ISTORIYA
ISSN: 0869-5687
No. 2 (2026)
https://rossiiskaya.com

Number Theory and Its Applications in Cryptography and Information Security

Jonas R. Feldmann
Institute for Computational Biology, Rheinwald Technical University, Munich, Germany

Received: 12/01/2026 ; Accepted : 03/05/2026 ; Published : 05/07/2026

Abstract
Number theory is one of the oldest and most fundamental branches of mathematics, concerned primarily with the properties and relationships of integers. Traditionally regarded as a field of pure mathematics, number theory has acquired enormous practical significance through its applications in computer science, cryptography, coding theory, information security, and digital communication. Concepts such as prime numbers, divisibility, modular arithmetic, congruences, greatest common divisors, Euler's theorem, Fermat's little theorem, and discrete logarithms provide the mathematical foundations for many modern cryptographic systems. Public-key cryptography, in particular, transformed information security by making it possible to communicate securely over insecure networks without requiring the prior exchange of a secret key. The RSA cryptosystem relies on properties of large integers and the computational difficulty associated with integer factorization, while Diffie-Hellman key exchange and related systems rely on modular arithmetic and discrete logarithm problems. This paper examines the fundamental concepts of number theory and their role in modern cryptography. It discusses prime numbers, modular arithmetic, congruences, Euclidean algorithms, finite structures, computational complexity, RSA, public-key cryptography, digital signatures, and cryptographic security. The paper also examines limitations of classical cryptographic methods in the context of quantum computing and considers the development of post-quantum cryptography. The analysis demonstrates that number theory represents an important connection between abstract mathematical theory and practical technological security. The continuing development of secure digital communication will require both classical mathematical knowledge and new mathematical approaches capable of addressing emerging computational threats.

Keywords: Number theory, prime numbers, modular arithmetic, cryptography, RSA, public-key cryptography, discrete logarithms, information security, digital signatures

1. Introduction

Number theory is the mathematical study of integers and their properties. Questions concerning divisibility, prime numbers, factors, and integer equations have fascinated mathematicians for centuries. Historically, many number-theoretical problems were considered purely theoretical because they did not appear to have direct practical applications.

The twentieth century dramatically changed this perception. The development of computers and digital communication created a need for mathematical techniques capable of protecting

information. Number theory provided many of the mathematical structures required for modern cryptography.

Cryptography is concerned with protecting information through mathematical transformations. Its objectives include confidentiality, integrity, authentication, and non-repudiation. Modern digital systems require these properties because sensitive information is routinely transmitted and stored electronically.

Classical symmetric cryptography requires communicating parties to share a secret key. Public-key cryptography introduced a different approach in which each participant can have a public key and a corresponding private key. The mathematical relationship between these keys allows secure communication without directly transmitting the private key.

The security of several public-key systems is based on computational problems that are easy to perform in one direction but difficult to reverse without special information. Integer factorization and discrete logarithms are important examples.

Number theory therefore provides not only abstract mathematical results but also practical mechanisms for protecting financial transactions, digital identities, electronic communication, and computer networks.

This paper examines the mathematical foundations of number theory and explains how these concepts contribute to cryptography and information security.

2. Historical Development of Number Theory

Number theory has ancient origins. The study of prime numbers, divisibility, and integer relationships appears in the mathematical traditions of ancient Greece and other civilizations.

Euclid's work established important results concerning prime numbers and divisibility. His proof that there are infinitely many primes remains one of the most famous arguments in mathematics.

Later mathematicians developed more sophisticated results. Pierre de Fermat contributed important theorems concerning modular arithmetic and prime numbers. Leonhard Euler generalized several of Fermat's results and made major contributions to arithmetic functions.

Carl Friedrich Gauss played a particularly important role in formalizing number theory. His work *Disquisitiones Arithmeticae* established systematic methods for studying congruences and quadratic forms.

Although these developments were initially theoretical, they eventually became central to computational mathematics and cryptography.

3. Prime Numbers

A prime number is an integer greater than one that has exactly two positive divisors: one and itself. Examples include

2,3,5,7,11,13,17,…2,3,5,7,11,13,17,\ldots

Every integer greater than one can be expressed as a product of prime numbers. This is the fundamental theorem of arithmetic.

Prime factorization is straightforward for relatively small integers. However, factoring extremely large integers can be computationally difficult using known classical methods.

This difference between the ease of multiplying large primes and the difficulty of recovering those primes from their product is central to RSA cryptography.

Prime numbers are therefore not only mathematically interesting but also computationally significant.

4. Divisibility and the Euclidean Algorithm

Divisibility is one of the basic concepts of number theory. If an integer aa divides bb, there exists an integer kk such that

b=ak.b=ak.

The greatest common divisor of two integers aa and bb, denoted gcd⁡(a,b)\gcd(a,b), is the largest positive integer dividing both.

The Euclidean algorithm provides an efficient method for computing the greatest common divisor.

For example,

gcd⁡(48,18)\gcd(48,18)

can be calculated using

48=2(18)+12,48=2(18)+12, 18=1(12)+6,18=1(12)+6, 12=2(6)+0.12=2(6)+0.

Therefore,

gcd⁡(48,18)=6.\gcd(48,18)=6.

The Euclidean algorithm is important in cryptography because modular inverses and key-generation procedures frequently require efficient computation of greatest common divisors.

5. Modular Arithmetic

Modular arithmetic is one of the most important mathematical foundations of cryptography.

Two integers aa and bb are congruent modulo nn if nn divides their difference:

a≡b(modn).a\equiv b\pmod n.

For example,

17≡5(mod12).17\equiv5\pmod{12}.

Modular arithmetic resembles ordinary arithmetic but operates within a finite set of residue classes.

Addition, subtraction, and multiplication can all be performed modulo nn. Modular exponentiation is especially important in cryptography.

For example,

ak(modn)a^k\pmod n

can be calculated efficiently even when kk is extremely large by using repeated squaring.

Efficient modular exponentiation is fundamental to RSA and Diffie-Hellman cryptographic systems.

6. Euler's Totient Function

Euler's totient function, denoted by φ(n)\varphi(n), counts the positive integers up to nn that are relatively prime to nn.

For a prime pp,

φ(p)=p−1.\varphi(p)=p-1.

If pp and qq are distinct primes,

φ(pq)=(p−1)(q−1).\varphi(pq)=(p-1)(q-1).

Euler's theorem states that if gcd⁡(a,n)=1\gcd(a,n)=1, then

aφ(n)≡1(modn).a^{\varphi(n)}\equiv1\pmod n.

This theorem plays an important role in the mathematical structure of RSA.
The totient function illustrates how an apparently abstract arithmetic function can become part of a practical security system.

7. Fermat's Little Theorem

Fermat's little theorem states that if pp is prime and aa is not divisible by pp, then
ap−1≡1(modp).a^{p-1}\equiv1\pmod p.
This theorem is closely related to Euler's theorem.
Fermat's little theorem has applications in primality testing and modular arithmetic. Probabilistic primality tests use related ideas to determine whether very large numbers are likely to be prime.
Since cryptographic systems require large prime numbers, efficient primality testing is an important computational problem.

8. Modular Inverses

An integer aa has a multiplicative inverse modulo nn if there exists an integer bb such that
ab≡1(modn).ab\equiv1\pmod n.
Such an inverse exists precisely when
gcd⁡(a,n)=1.\gcd(a,n)=1.
The extended Euclidean algorithm can efficiently calculate modular inverses.
For example, if
3b≡1(mod7),3b\equiv1\pmod7,
then b=5b=5, since
3(5)=15≡1(mod7).3(5)=15\equiv1\pmod7.
Modular inverses are central to RSA key generation and many other cryptographic algorithms.

9. Public-Key Cryptography

Traditional symmetric cryptography uses the same secret key for encryption and decryption. This creates a key-distribution problem: communicating parties must find a secure way to exchange the secret key.
Public-key cryptography addresses this challenge using a pair of mathematically related keys. The public key can be distributed openly, while the private key is kept secret.
A cryptographic system generally requires a mathematical transformation that is easy to perform using public information but difficult to reverse without the private key.
The development of public-key cryptography represented a major transformation in information security. It enabled secure communication across networks where users may not have previously established a shared secret.

10. RSA Cryptography

RSA is one of the best-known public-key cryptosystems. Its mathematical structure depends strongly on number theory.
The RSA key-generation process begins by selecting two large prime numbers pp and qq. Their product is
n=pq.n=pq.
The value
φ(n)=(p−1)(q−1)\varphi(n)=(p-1)(q-1)

is then calculated.
A public exponent ee is selected such that
gcd(e,φ(n))=1.\gcd(e,\varphi(n))=1.
The private exponent dd is chosen to satisfy
ed≡1(modφ(n)).ed\equiv1\pmod{\varphi(n)}.
The public key consists of nn and ee, while dd is kept secret.
RSA encryption can be represented conceptually as
c≡me(modn),c\equiv m^e\pmod n,
where mm is the message and cc is the ciphertext.
Decryption uses
m≡cd(modn).m\equiv c^d\pmod n.
The mathematical correctness of this transformation is based on modular arithmetic and number-theoretical results.
The security of appropriately implemented RSA relies on the difficulty of factoring large integers, although the precise security considerations are more complicated than simply stating that “factoring is difficult.”

11. Diffie-Hellman Key Exchange

Diffie-Hellman key exchange is another important application of number theory. It allows two parties to establish a shared secret over an insecure communication channel.
The basic idea uses modular exponentiation. Two parties agree publicly on a suitable modulus and generator. Each party selects a private value and computes a corresponding public value.
The parties then combine their private values with the other's public value to obtain a common shared secret.
The security is related to the computational difficulty of the discrete logarithm problem in suitable mathematical groups.
The conceptual importance of Diffie-Hellman lies in its demonstration that two parties can establish a common secret without directly transmitting that secret.

12. Discrete Logarithms

The discrete logarithm problem can be viewed as the inverse of modular exponentiation.
Given
gx≡y(modp),g^x\equiv y\pmod p,
the problem is to determine xx.
Computing yy from gg and xx can be efficient using repeated squaring, while determining xx from gg and yy can be computationally difficult in appropriately chosen groups.
This asymmetry provides the basis for several cryptographic systems.
The difficulty of discrete logarithms depends on the mathematical group and algorithm being used. Therefore, cryptographic security requires careful parameter selection.

13. Digital Signatures

Digital signatures provide mechanisms for authentication and integrity. A signature allows a recipient to verify that a message was associated with a particular private key and has not been modified.

Public-key mathematics makes this possible. The signer uses a private key to generate a signature, while others use the corresponding public key to verify it.

Digital signatures are important for electronic documents, software distribution, financial systems, digital certificates, and secure communication.

Number-theoretical concepts such as modular arithmetic, finite groups, and computational hardness contribute to the mathematical foundations of signature schemes.

14. Cryptographic Hashing and Number Theory

Cryptographic hash functions are not simply applications of classical number theory in the same way as RSA, but mathematical structures remain important in their design and analysis.

A cryptographic hash function maps input data to a fixed-length output. A secure hash function should make it computationally difficult to find collisions and should exhibit strong diffusion properties.

Hash functions are used in password protection, digital signatures, blockchain systems, data integrity verification, and many other applications.

Although their security properties differ from those of public-key cryptography, hash functions demonstrate the broader relationship between mathematical theory and information security.

15. Number Theory and Primality Testing

Cryptographic systems often require large prime numbers. Therefore, efficient primality testing is essential.

A deterministic test can establish whether a number is prime, while probabilistic tests determine whether a number is probably prime with extremely high confidence.

Tests based on modular exponentiation can rapidly eliminate many composite numbers. More advanced algorithms can provide deterministic primality testing within theoretical complexity bounds.

The practical generation of cryptographic primes therefore represents an intersection of number theory, algorithms, probability, and computational complexity.

16. Computational Complexity and Cryptographic Security

Cryptography depends on computational difficulty. A mathematical problem is useful for security when legitimate users can perform required operations efficiently, while an adversary without secret information would require an impractical amount of computational effort to reverse or attack the system.

This concept connects number theory with computational complexity.

The security of a cryptographic algorithm must be evaluated against known mathematical algorithms and realistic computational resources. Increasing computer power can weaken systems that were previously considered secure.

Consequently, cryptographic parameters must be periodically reassessed.

17. Number Theory in Coding and Error Correction

Number theory also contributes to coding theory. Error-correcting codes allow information to be recovered even when transmission introduces errors.

Finite fields, which are algebraic structures containing finitely many elements, are particularly important in coding theory.

Polynomial arithmetic over finite fields supports several error-correcting codes used in digital communication and data storage.

Applications include satellite communication, wireless systems, optical storage, QR codes, and digital broadcasting.

This demonstrates that the mathematical structures underlying cryptography also interact with communication theory.

18. Applications in Blockchain Technology

Blockchain systems employ cryptographic methods for authentication, integrity, and transaction security. Digital signatures help users authorize transactions, while cryptographic hash functions help create tamper-evident chains of records.

Many blockchain systems use public-key cryptography based on mathematical structures such as elliptic curves. Elliptic-curve cryptography is rooted in algebraic number theory and finite-field mathematics.

The practical security of blockchain therefore depends substantially on mathematical principles developed through number theory and related areas.

19. Limitations of Classical Cryptographic Systems

Classical cryptographic methods face several challenges.

First, security depends on mathematical assumptions. If a supposedly difficult problem becomes efficiently solvable, a cryptographic system may become vulnerable.

Second, implementation errors can undermine mathematically sound algorithms. Weak random-number generation, poor key management, side-channel leakage, and incorrect protocol design can create security weaknesses.

Third, increasing computational power requires periodic increases in cryptographic key sizes and algorithmic sophistication.

A particularly important challenge is quantum computing.

20. Quantum Computing and Post-Quantum Cryptography

Large-scale quantum computers could potentially threaten cryptographic systems based on integer factorization and discrete logarithms. Shor's algorithm provides a theoretical polynomial-time method for solving both types of problems on a sufficiently powerful quantum computer.

This has motivated research into post-quantum cryptography, which seeks cryptographic systems believed to resist quantum attacks.

Candidate mathematical foundations include lattice problems, error-correcting codes, hash functions, and other computational structures.

The development of post-quantum cryptography demonstrates that mathematical research must continuously respond to technological change.

21. Future Perspectives

Number theory is likely to remain highly important to cryptography. New mathematical structures may provide stronger security against both classical and quantum computational threats.

Research will continue in lattice-based cryptography, elliptic-curve mathematics, finite fields, computational number theory, and cryptographic protocols.

There will also be increasing interaction between pure mathematics and computer science. Problems originally studied without practical objectives may eventually become important to technology, just as number theory became central to modern cryptography.

Advances in algorithms and computing power will require continuous reassessment of cryptographic assumptions.

Mathematical education is equally important. Professionals designing secure systems require strong foundations in modular arithmetic, algebra, probability, algorithms, and computational complexity.

22. Conclusion

Number theory demonstrates exceptionally well how abstract mathematics can acquire profound practical significance. Concepts involving prime numbers, divisibility, modular arithmetic, congruences, Euler's theorem, and discrete logarithms provide foundations for important cryptographic technologies.

RSA demonstrates the role of integer factorization and modular arithmetic. Diffie-Hellman illustrates the importance of discrete logarithms. Digital signatures demonstrate how mathematical relationships can provide authentication and integrity.

The security of these systems depends not only on mathematical theory but also on computational assumptions, algorithm design, implementation quality, and key management.

The emergence of quantum computing introduces new challenges because algorithms such as Shor's algorithm could threaten some classical public-key systems. Post-quantum cryptography consequently represents an important research direction.

The continuing interaction between number theory, computer science, and information security illustrates the enduring value of mathematical research. Number theory is therefore not simply the study of integers; it is also a foundation for some of the technologies that protect modern digital society.

References

1. Hardy, G. H., & Wright, E. M. (2008). *An Introduction to the Theory of Numbers* (6th ed.). Oxford University Press.
2. Burton, D. M. (2010). *Elementary Number Theory* (7th ed.). McGraw-Hill.
3. Niven, I., Zuckerman, H. S., & Montgomery, H. L. (1991). *An Introduction to the Theory of Numbers* (5th ed.). Wiley.
4. Ireland, K., & Rosen, M. (1990). *A Classical Introduction to Modern Number Theory* (2nd ed.). Springer.
5. Koblitz, N. (1994). *A Course in Number Theory and Cryptography* (2nd ed.). Springer.
6. Stinson, D. R. (2006). *Cryptography: Theory and Practice* (3rd ed.). Chapman & Hall/CRC.
7. Katz, J., & Lindell, Y. (2020). *Introduction to Modern Cryptography* (3rd ed.). CRC Press.
8. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press.

9. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126.
10. Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), 644–654.
11. Euler, L. (1748). *Introductio in analysin infinitorum*. Lausanne.
12. Gauss, C. F. (1801). *Disquisitiones Arithmeticae*. Leipzig.
13. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, 124–134. IEEE.
14. Bernstein, D. J., Buchmann, J., & Dahmen, E. (Eds.). (2009). *Post-Quantum Cryptography*. Springer.
15. Silverman, J. H. (2009). *The Arithmetic of Elliptic Curves* (2nd ed.). Springer.