Number Theory and Cryptography

Number theory is the branch of mathematics devoted to studying integers and their properties. This fundamental area forms the backbone of modern cryptography - the science of secure information transmission.

From divisibility and modular arithmetic to prime numbers and complex algorithms, number theory provides the mathematical tools that enable secure digital communications, data protection, and verification systems used worldwide.

Divisibility and Modular Arithmetic

Division

When one integer is divided by a nonzero integer, we say that a divides b if there exists an integer c such that b = ac. We denote this as a | b, and call a a divisor or factor of b.

Division Algorithm

For any integer a and positive integer d, there exist unique integers q (quotient) and r (remainder), with $0 \leq r < d$, such that a = dq + r.

Modular Arithmetic

We say a is congruent to b modulo m, written $a \equiv b \pmod{m}$, if m divides a - b. This creates equivalence classes of integers with the same remainder when divided by m.

Integer Representations and Algorithms

Binary Representation

Every integer can be uniquely represented in base 2 using only 0s and 1s. This is the foundation of computer arithmetic.

Base Conversion

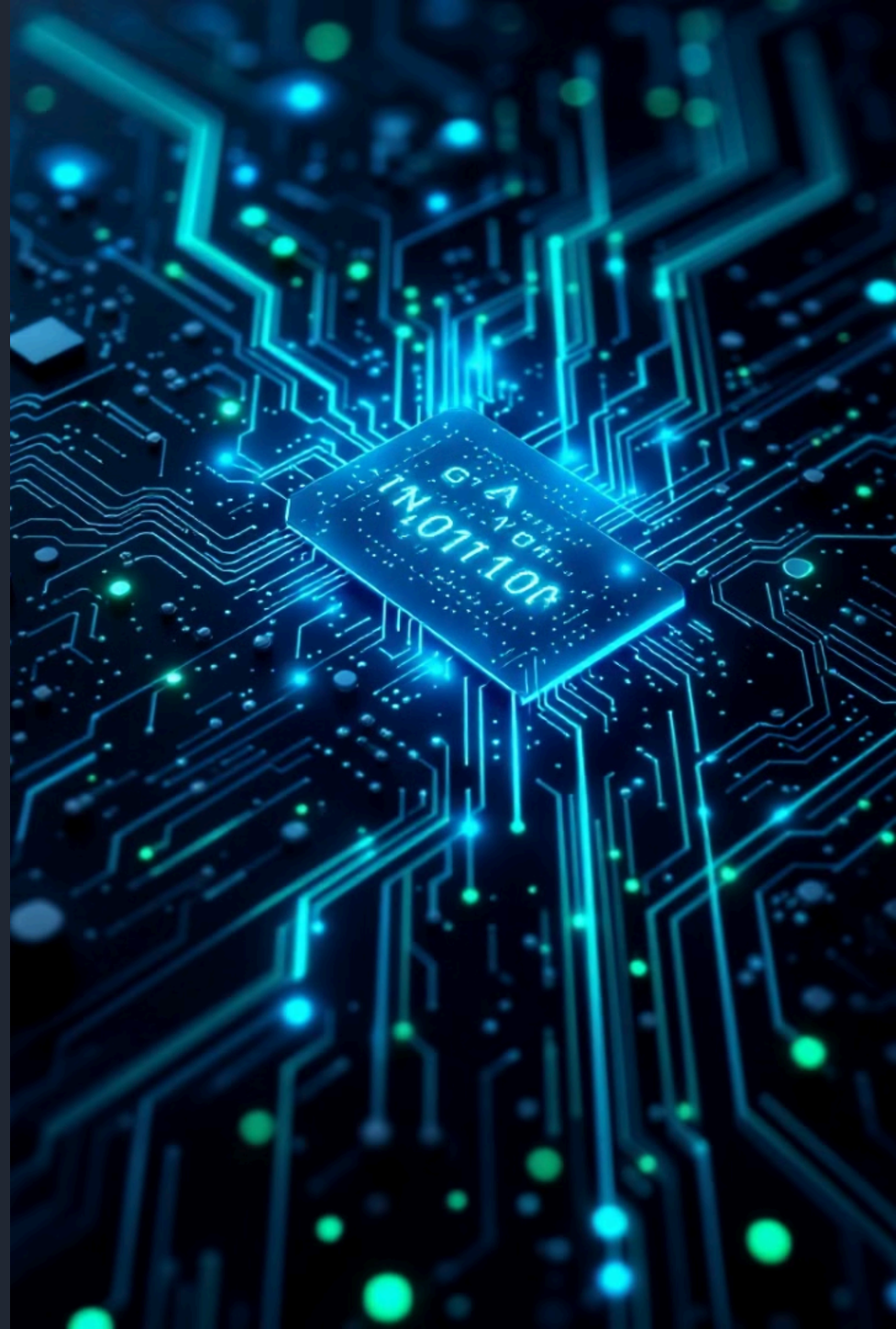
To convert from decimal to another base b, repeatedly divide by b and collect the remainders from right to left.

Addition Algorithm

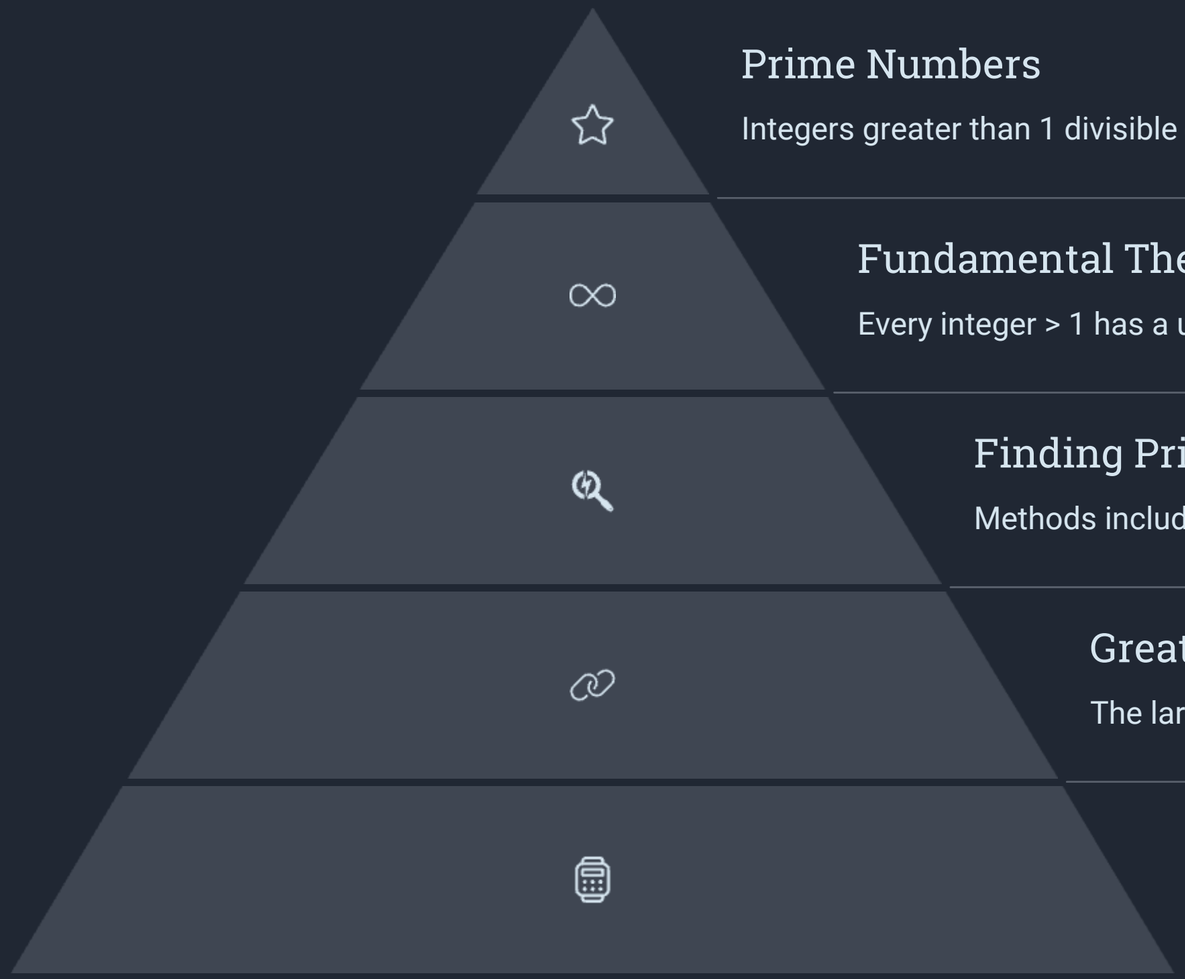
Binary addition follows similar rules to decimal addition but with carrying when the sum exceeds 1.

Modular Exponentiation

Computing b^n mod m efficiently by reducing intermediate results modulo m, crucial for cryptography.



Primes and Greatest Common



Prime Numbers

Integers greater than 1 divisible only by 1 and themselves

Fundamental Theorem of Arithmetic

Every integer > 1 has a unique prime factorization

Finding Primes

Methods include trial division and the Sieve of Eratosthenes

Greatest Common

The largest integer that divides two numbers

Euclidean Algorithm

An efficient method to compute GCDs

Prime numbers are the building blocks of integers, and their properties make them essential for cryptography. The Euclidean algorithm provides an efficient way to find the GCD without needing to factor the numbers.

Solving Congruences

Linear Congruences

Solving equations of the form $ax \equiv b \pmod{m}$

Modular Inverses

Finding a^{-1} such that $a \cdot a^{-1} \equiv 1 \pmod{m}$

Chinese Remainder Theorem

Solving systems of congruences with different moduli

Solving congruences is a fundamental skill in number theory with direct applications to cryptography. The Chinese Remainder Theorem allows us to solve systems of congruences efficiently, which is particularly useful for handling large numbers in computer arithmetic.

Computer Arithmetic with Large Integers

Representing Large Numbers

Using remainders with respect to multiple moduli to represent large integers efficiently. Any number less than the product of the moduli can be uniquely represented.

Arithmetic with Remainders

Performing operations on the smaller remainder values instead of the original large numbers, then reconstructing the result using the Chinese Remainder Theorem.

Choosing Efficient Moduli

Selecting moduli of the form 2^k-1 (like 31, 63, 127) allows for efficient binary operations while handling numbers as large as 2^{184}.

Fermat's Little Theorem and

Fermat's Little Theorem

If p is prime and a is not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$. Alternatively, for any integer a, $a^p \equiv a \pmod{p}$.

This theorem makes calculating large exponents modulo a prime much easier. For example, to find $7^{222} \bmod 11$, we can use the fact that $7^{10} \equiv 1 \pmod{11}$ to simplify the calculation.

Pseudoprimes

Some composite numbers satisfy Fermat's condition for specific bases, making them appear prime. For example, $341 = 11 \times 31$ is composite, but $2^{340} \equiv 1 \pmod{341}$.

Carmichael numbers are special pseudoprimes that satisfy Fermat's condition for all bases relatively prime to the number, like 561, making them particularly deceptive in primality testing.

Primitive Roots and Discrete

Primitive Roots

A primitive root modulo p is a number r whose powers generate all numbers from 1 to p-1 in some order

Cryptographic Applications

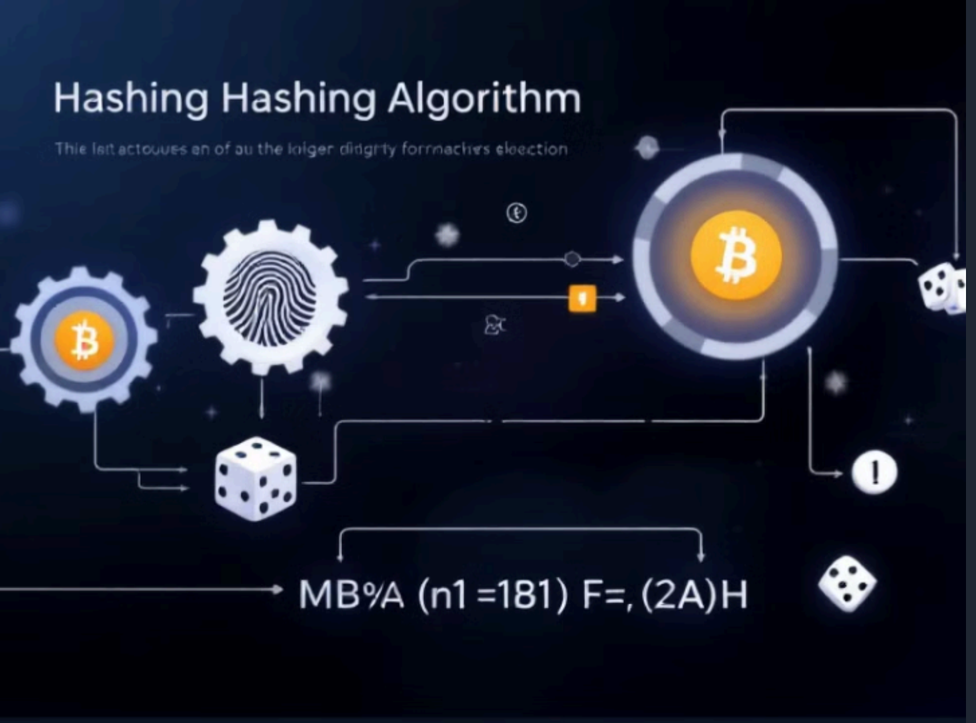
The difficulty of finding discrete logarithms forms the basis of several cryptographic systems

Power Generation

For a primitive root r of prime p, the values r^1, r^2, r^3, ..., r^{p-1} include all numbers from 1 to p-1

Discrete Logarithms

If $r^e \equiv a \pmod{p}$, then e is the discrete logarithm of a with base r



Applications of

Hashing Functions

Congruences help assign memory locations efficiently in computer systems. A simple hash function h(k) = k mod m maps large identifiers to smaller memory locations, though collisions must be handled when two keys hash to the same location.

Pseudorandom

Linear Congruential Generators create sequences that appear random using the formula $x_{n+1} = (ax_n + c) \bmod m$. These are fast to compute but have recognizable patterns, making them suitable for simulations but not cryptography.

Check Digits

Many identification numbers (ISBN, credit cards) include check digits calculated using modular arithmetic to detect errors. If a number is entered incorrectly, the check digit won't match, signaling an error.

Cryptography Systems and

Private Key Cryptography

Also called symmetric cryptography, where the sender and receiver share a single secret key for both encryption and decryption. Examples include the Shift Cipher, Affine Cipher, and AES (Advanced Encryption Standard).

Public Key

Uses two different keys: a public key for encryption that can be shared openly, and a private key for decryption that must be kept secret. The RSA cryptosystem is based on the difficulty of factoring large prime numbers.

Cryptographic Protocols

Structured procedures that ensure secure communication, including key exchange (Diffie-Hellman), digital signatures for authenticity verification, and homomorphic encryption that allows computations on encrypted data.