Introduction to Number Theory

Jose Chavez

August 9, 2023

1 Introduction

Number theory is a branch of mathematics that deals with the properties and relationships of numbers, both integers and rational numbers. Its origins can be traced back to ancient civilizations, but it gained prominence in the late 19th and early 20th centuries through the works of mathematicians like Carl Friedrich Gauss and Pierre de Fermat. Number theory has applications in cryptography, coding theory, and more.

2 Basic Concepts

3 Applications

4 History

5 Group Theory Basics

A group is a set G equipped with a binary operation $\cdot$ that satisfies the following properties:

1. **Closure**: For all $a, b \in G$, $a \cdot b \in G$.
2. **Associativity**: For all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
3. **Identity Element**: There exists an element $e \in G$ such that for all $a \in G$, $a \cdot e = e \cdot a = a$.
4. **Inverse Element**: For each $a \in G$, there exists an element $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

[Lagrange's Theorem] In a finite group, the order of any subgroup divides the order of the group.

6 Ring Theory

A ring is a set R equipped with two binary operations, addition ($+$) and multiplication ($\cdot$), satisfying the following axioms:

1. R is an abelian group under addition.
2. Multiplication is associative.
3. The distributive laws hold: $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(a+b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in R$.

Let R and S be rings. A function $\varphi : R \to S$ is a ring homomorphism if it preserves both addition and multiplication.

7 Divisibility and Primes

An integer a is said to divide an integer b (denoted $a \mid b$) if there exists an integer c such that $b = ac$.

[Fundamental Theorem of Arithmetic] Every positive integer greater than 1 can be uniquely factored into prime numbers.

8 Modular Arithmetic

Given an integer $m > 1$, two integers a and b are said to be congruent modulo m (denoted $a \equiv b \pmod{m}$) if $a - b$ is divisible by m.

[Chinese Remainder Theorem] Given pairwise coprime integers m and n, any system of congruences $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ has a unique solution modulo mn.

9 Number Theory Examples (continued)

9.1 Fermat's Little Theorem

[Fermat's Little Theorem] If p is a prime number and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.

9.2 Euler's Totient Function

The Euler's totient function $\phi(n)$ is the number of positive integers less than or equal to n that are coprime to n.

9.3 Primitive Roots

An integer g is a primitive root modulo n if every positive integer coprime to n is congruent to a power of g modulo n.

9.4 Quadratic Residues

Let p be a prime number and a an integer not divisible by p. a is called a quadratic residue modulo p if there exists an integer x such that $x^2 \equiv a \pmod{p}$.

9.5 Quadratic Reciprocity

[Quadratic Reciprocity] Let p and q be distinct odd prime numbers. Then, the congruence $x^2 \equiv p \pmod{q}$ has a solution if and only if the congruence $x^2 \equiv q \pmod{p}$ has a solution.

9.6 Diophantine Equations

A Diophantine equation is an equation where the solutions are sought among integers.

9.7 Pell's Equation

The Pell's equation is a Diophantine equation of the form $x^2 - ny^2 = 1$, where n is a non-square positive integer.

9.8 Continued Fractions

A continued fraction is an expression of the form $[a_0; a_1, a_2, a_3, \ldots]$, where a_i are integers and a_0 is a whole number.

9.9 Farey Sequences

A Farey sequence of order n is the sequence of all reduced fractions between 0 and 1 whose denominators do not exceed n.

9.10 Perfect Numbers

A positive integer n is said to be perfect if the sum of its proper divisors equals n.

9.11 Mersenne Primes

A Mersenne prime is a prime number of the form $2^p - 1$, where both p and $2^p - 1$ are prime.

10 Number Theory Examples (continued)

10.1 Goldbach's Conjecture

[Goldbach's Conjecture] Every even integer greater than 2 can be expressed as the sum of two prime numbers.

10.2 Riemann Zeta Function

The Riemann zeta function is defined as $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ for complex numbers s with real part greater than 1.

10.3 Prime Number Theorem

[Prime Number Theorem] The prime number theorem states that the limit of the ratio of the number of primes up to x and $x/\log x$ is 1 as x approaches infinity.

10.4 Distribution of Prime Gaps

The distribution of prime gaps follows a logarithmic pattern. The average gap between consecutive primes near x is approximately $\log x$.

10.5 Hardy-Littlewood Conjectures

[Hardy-Littlewood Conjectures] The Hardy-Littlewood prime tuples conjecture predicts the distribution of prime constellations, such as twin primes, prime quadruplets, and other patterns.

10.6 Analytic Number Theory

Analytic number theory uses methods from analysis to study the distribution of prime numbers and related number-theoretic functions.

10.7 Dirichlet's Theorem on Arithmetic Progressions

[Dirichlet's Theorem] For any two positive coprime integers a and d, there are infinitely many primes of the form $a + nd$, where n is a non-negative integer.

10.8 Dedekind Zeta Function

The Dedekind zeta function associated with an algebraic number field K is a complex function that encodes information about the distribution of prime ideals in the ring of integers of K.

10.9 Elliptic Curves over Q

An elliptic curve over the rational numbers Q is a smooth projective curve with a specified point at infinity, and it can be defined by an equation of the form $y^2 = x^3 + ax + b$.

10.10 Modular Forms and L-Functions

A modular form is a complex function that satisfies certain transformation properties under modular substitutions. L-functions are associated with modular forms and encode arithmetic information.

10.11 Birch and Swinnerton-Dyer Conjecture

[Birch and Swinnerton-Dyer Conjecture] For an elliptic curve E over Q, the rank of the group of rational points on E is related to the order of vanishing of its L-function at its central critical point.

10.12 ABC Conjecture

[ABC Conjecture] The ABC conjecture, proposed by Joseph Oesterlé and David Masser, states that for any positive integers a, b, c that are coprime and satisfy $a + b = c$, the product of the distinct prime factors of abc is usually much larger than c.

10.13 Quadratic Forms

A quadratic form is a homogeneous polynomial of degree 2 in several variables. It plays a crucial role in number theory, algebra, and geometry.

10.14 Class Numbers and Units

The class number of an algebraic number field is a measure of the failure of unique factorization into prime elements. Units are invertible elements in the ring of integers of a number field.

10.15 L-functions of Algebraic Number Fields

An L-function associated with an algebraic number field encodes information about the distribution of prime ideals in its ring of integers and reflects deep arithmetic properties.

10.16 Quadratic and Higher Reciprocity Laws

[Quadratic Reciprocity Law] Let p and q be distinct odd prime numbers. The Legendre symbol $\left(\frac{p}{q}\right)$ determines whether p is a quadratic residue modulo q.

10.17 Artin's Conjecture on Primitive Roots

[Artin's Conjecture] Artin's conjecture states that for any non-square integer a and a positive integer n coprime to a, there are infinitely many primes p such that a is a primitive root modulo p.

10.18 Langlands Program

The Langlands program is a vast and influential web of conjectures connecting number theory, representation theory, and harmonic analysis.

10.19 Algebraic Independence

Algebraic numbers $\alpha_1, \alpha_2, \ldots, \alpha_n$ are said to be algebraically independent if no non-trivial polynomial equation with integer coefficients relates them.

10.20 Mahler's Method

Mahler's method is a technique used to prove transcendence and algebraic independence results, based on the construction of linear forms in logarithms.

10.21 Diophantine Approximation

Diophantine approximation deals with approximating irrational numbers by rational numbers with a specified level of accuracy.

10.22 Transcendental Numbers

A real or complex number is called transcendental if it is not the root of any non-zero polynomial equation with integer coefficients.

10.23 Skolem's Problem

Skolem's Problem concerns whether certain algebraic equations have integer solutions and is closely related to Diophantine equations and number theory.

10.24 S-unit Equations

An S-unit equation is a Diophantine equation involving integers from a fixed finite set of prime factors.

10.25 Exponential Diophantine Equations

Exponential Diophantine equations involve variables in exponent positions and are characterized by their intricate and challenging solutions.

10.26 Solving Polynomial Equations in Integers

For a given polynomial equation with integer coefficients, determining whether it has integer solutions is a fundamental problem in number theory.

10.27 Gaps Between Consecutive Prime Powers

The study of prime gaps includes understanding the distribution and size of gaps between consecutive prime numbers and prime powers.

10.28 Prime Constellations

Prime constellations are patterns in the distribution of primes, such as twin primes, prime quadruplets, and other related structures.

10.29 Prime k-tuples Conjecture

[Prime k-tuples Conjecture] The prime k-tuples conjecture predicts the existence of infinitely many prime constellations of a certain form.

10.30 Automorphic Forms and Representations

Automorphic forms are complex functions that satisfy certain transformation properties under a group of linear fractional transformations. They have deep connections with number theory, representation theory, and geometry.

10.31 Lang's Conjectures

Lang's conjectures are a series of far-reaching conjectures that propose connections between algebraic number theory, transcendence theory, and Diophantine geometry.

10.32 Subconvexity Bounds for L-functions

Subconvexity bounds are estimates of the behavior of L-functions in the critical strip that provide important information about the distribution of their zeros.

10.33 Arithmetic Dynamics

Arithmetic dynamics is the study of number-theoretic properties of iterative processes and their relationships with algebraic number theory and geometry.

10.34 Sums of Squares and Waring's Problem

Waring's problem seeks to represent every positive integer as a sum of a fixed number of kth powers of positive integers, for a given k.

10.35 Arithmetic Combinatorics

Arithmetic combinatorics explores the additive and multiplicative structures of integers and their relationships with combinatorial principles.