COMPUTATIONAL MATHEMATICS AND ANALYSIS

# FUNDAMENTAL PERCEPTIONS IN CONTEMPORARY NUMBER THEORY

J. Kannan
Manju Somanath

NOVA

# Computational Mathematics and Analysis

# Computational Mathematics and Analysis

**Fundamental Perceptions in Contemporary Number Theory**
J. Kannan, PhD and Manju Somanath, PhD
2023. ISBN: 979-8-88697-794-3 (Hardcover)
2023. ISBN: 979-8-88697-864-3 (eBook)

**Internet of Things and Machine Learning in Agriculture**
Jyotir Moy Chatterjee and Vishal Jain, PhD (Editors)
2021. ISBN: 978-1-68507-192-9 (Hardcover)
2021. ISBN: 978-1-68507-216-2 (eBook)

**Decision-Making with Neutrosophic Set: Theory and Applications in Knowledge Management**
Harish Garg (Editor)
2021. ISBN: 978-1-53619-419-7 (Hardcover)
2021. ISBN: 978-1-53619-522-4 (eBook)

**Perturbation Methods in Matrix Analysis and Control**
Mihail M. Konstantinov and Petko H. Petkov
2020. ISBN: 978-1-53617-470-0 (Hardcover)
2020. ISBN: 978-1-53617-471-7 (eBook)

**Understanding Eigenvalues**
Ty L. Henson (Editor)
2020. ISBN: 978-1-53617-357-4 (eBook)

**Image Recognition: Progress, Trends and Challenges**
Charles Z. Liu and S. Ramakrishnan (Editors)
2020. ISBN: 978-1-53617-258-4 (Hardcover)
2020. ISBN: 978-1-53617-259-1 (eBook)

More information about this series can be found at
https://novapublishers.com/product-category/series/computational-mathematics-and-analysis/

**J. Kannan, PhD**
**and**
**Manju Somanath, PhD**

# Fundamental Perceptions in Contemporary Number Theory

DOI: https://doi.org/10.52305/RRCF4106



## Library of Congress Cataloging-in-Publication Data

ISBN: 979-8-88697-864-3(eBook)

Published by Nova Science Publishers, Inc. † New York

# Contents

*Dedicated to All My Teachers and Students*

# Preface

Number theory is indeed an area of mathematics that investigates the attributes of positive integers like $1, 2, 3 \cdots$ Often alluded to as "higher arithmetic," it is one of the most natural and historical mathematical disciplines. This theory of numbers has long held a special place in the field of mathematics. This is as a result of the theory's undeniable historical importance. Both professional and amateur mathematicians have always been attracted by number theory. Although solutions to the issues and proofs of the theorems frequently need for a sophisticated mathematical background, number theory problems and theorems can often be grasped by laypeople, in contrast to other disciplines of mathematics.

Number theory, which has no direct applications to the actual world, was thought to be the most pure area of mathematics until the middle of the $20^{th}$ century. The development of digital computers and communications showed that number theory may offer novel solutions to practical issues. At the same time, breakthroughs in computer technology allowed number theorists to make outstanding progress in tackling numerical problems that were previously thought to be insurmountable, including factoring big numbers, figuring out primes, testing hypotheses, and more.

Elementary number theory, algebraic number theory, analytic number theory, geometric number theory, and probabilistic number theory are some of the sub-fields of modern number theory. The approaches taken to solve integer-related problems are reflected in these categories. Counting has existed since the beginning of time. Archaeological artefacts, such a bone from the Congo region of Africa that is 10,000 years old and has tally marks etched on itsigns of an unidentified ancestor tallying somethingevidence this. People had begun to understand the concept of "multiplicity" very early on in the history of civilization, opening the door to the study of numbers.

Because ancient tablets, papyri, and temple carvings from Mesopotamia, Egypt, China, and India have survived, it is certain that these civilizations had a mathematical understanding at the time. A good example is the Plimpton 322 tablet, which was discovered in Babylonia around $1700\ BCE$. Pythagoras $(c.\ 580 - 500BCE)$ supposedly worked in southern Italy among loyal followers. His thought emphasised the importance of number as the overarching idea required to comprehend everything from celestial mechanics to artistic melody.

Euclid, on the other hand, introduced number theory plainly. He described a number as "a plurality constituted of units" at the beginning of Book VII of his Elements. The plural in this instance left out 1; according to Euclid, 2 was the smallest "number." Later, he went on to define a perfect number as one that equals the sum of its proper divisors, a composite as a number that is not prime, and a prime as a number "measured by a unit alone" (i.e., whose only proper divisor is 1). From then, Euclid established a series of theorems that serve as the foundation for number theory as a branch of mathematics.

Number theory got little serious attention as mathematics spread from the Islamic world to Renaissance Europe. Important developments in geometry, algebra, and probability occurred between $1400$ and $1650$, as well as the discovery of logarithms and analytic geometry. However, number theory was viewed as just a small discipline with mostly recreational significance.

The current state and future directions of numerous facets of contemporary number theory are examined in this book "Fundamental Perceptions in Contemporary Number Theory" from a unified standpoint. The theoretical foundations of contemporary theories are unveiled as a consequence of simple challenges. Additionally, this book makes an effort to present the contents as simply as possible. It is primarily intended for novice mathematicians who have tried reading other works but have struggled to comprehend them due to complex reasoning.

In this book, there are eight chapters. An overview of the initial stages of Divisibility is given in the introduction of Chapter 1. In-depth discussion is given on the division and the fundamental theorem of arithmetic. The Greatest Integer Function and other Classical Functions of Number Theory are discussed in Chapter 2. Congruence theory, along with some of its fundamental characteristics and theorems, are covered in Chapter 3. Primitive roots and indices are discussed in Chapter 4 with emphasis on the Primitive Root Theorem. Quadratic reciprocity and its features are covered in Chapter 5. Chapter 6 defines and discusses special numbers. Waring's Problem and Sum of Squares are presented in Chapter 7. Also, the questions from CSIR- NET Mathematics examination

(conducted by National Testing Agency, Govt. of India) are included at the end of each chapter.

# List of Symbols

| | |
|---|---|
| $\mathbb{N}$ | Set of all natural numbers |
| $\mathbb{Z}$ | Set of all integers |
| $\mathbb{R}$ | Set of all real numbers |
| $x \in S$ | $x$ belongs to the set $S$ |
| $x \notin S$ | $x$ does not belong to the set $S$ |
| $\|x\|$ | Absolute value of $x$ |
| $n!$ | $n$ Factorial |
| $\binom{n}{r}$ | Binomial coefficient |
| $a \mid b$ | $a$ divides $b$ |
| $a \nmid b$ | $a$ does not divide $b$ |
| $(a, b)$ | GCD of $a$ and $b$ |
| $[a, b]$ | LCM of $a$ and $b$ |
| $a \equiv b \pmod{m}$ | $a$ is congruent to $b$ modulo $m$ |
| $a \not\equiv b \ (m)$ | $a$ is not congruent to $b$ modulo $m$ |
| $F_n$ | Fermat Number |
| $M_n$ | Mersenne Number |
| $P_n$ | Pell Number |
| $\mu(n)$ | Mobius Function |
| $\phi(n)$ | Euler Totient Function |
| $f * g$ | Dirichlet Product of $f$ and $g$ |
| $f^{-1}$ | Dirichlet inverse of $f$ |
| $\tau(n)$ | Number of positive divisors of $n$ |
| $\sigma_\alpha(n)$ | Sum of $\alpha^{th}$ power of positive divisors of $n$ |
| $ind_g(a)$ | Index of $a$ to the base $g$ |
| $\left(\frac{a}{p}\right)$ | Legendre Symbol |
| $(a\|m)$ | Jacobi Symbol |
| $mRp$ | $m$ is a quadratic residue modulo $p$ |
| $m\bar{R}p$ | $m$ is a quadratic non residue modulo p |
| $ord_m(a)$ | Order of $a$ modulo $m$ |
| $[a]_m$ | Residue class $a$ modulo $m$ |
| $a^*$ | Modulo inverse of $a$ |
| $[x]$ | Greatest integer less than or equal to $x$ |

# Chapter 1

# Divisibility

"Mathematics is the language with which God wrote the universe"

- Galileo

The fundamental ideas of elementary number theory are addressed in this chapter, encompassing divisibility, GCD, LCM, Primes. Principles of induction, Division and Euclidean Algorithms, Fundamental Thoerem of Arithmetic are the ultimate aim in this chapter. The following integer properties are used extensively in many of the proofs.

## 1.1. Preliminaries

The fundamental concepts required to comprehend basic number theory are covered in this part. That includes, what are integers and their properties, principles involoving natural numbers.

The set of all integers is denoted by $\mathbb{Z}$. That is, $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3 \cdots, \}$.

**Properties of Integers**. Let $a, b, c \in \mathbb{Z}$. Then

(i) $a + b = b + a$

(ii) $a - b = -(b - a)$

(iii) $ab = ba$

(iv) $a + (b + c) = (a + b) + c$

(v) $a(bc) = (ab)c$

(vi) $|a| = \begin{cases} a, \text{if } a \geq 0 \\ -a, \text{if } a < 0 \end{cases}$

(vii) $a + 0 = 0 + a = a$

(viii) $a - a = 0$

**Principle of Weak Induction**. Let $P(n)$ be a statement regarding a positive integer $n$ and let $a \in \mathbb{N}$ be fixed. If

(i) $P(a)$ is true

(ii) for every $m \geq a$, if $P(m)$ is true, then $P(m+1)$ is true,

then $P(n)$ is true for all $n \geq a$.

**Principle of Strong Induction**. Let $P(n)$ be a statement regarding a positive integer $n$ and let $a \in \mathbb{N}$ be fixed. If

(i) $P(a)$ is true

(ii) for every $m \geq a$, if $P(a), P(a+1), \cdots, P(m)$ are true, then $P(m+1)$ is true,

then $P(n)$ is true for all $n \geq a$.

**Theorem 1.1** (Well-Ordering Principle)**.** *Every non-empty set of positive integers contains a least element.*

*Proof.* Let $A$ be a non- empty subset of $\mathbb{N}$ and that has no least element and $B = \mathbb{N} \backslash A$. Let us prove that if $n \in \mathbb{N}$, then $n \in B$. If $1 \in A$, then 1 is the least element in the set $A$. But this is not possible by the construction of A. Thus $1 \notin A$ and so $1 \in B$. Assume that $n \in B$. If $2, 3, \cdots, n-1 \in A$, then $A$ contains a least element. Hence $2, 3, \cdots, n-1 \notin A$ and so $2, 3, \cdots, n-1 \in B$. If $n+1 \in A$, then it is the least element in $A$. Thus $n+1 \notin A$ and so $n+1 \in B$. Hence $n \in B$ for all $n \in \mathbb{N}$. That is, $B = \mathbb{N}$ and hence $A$ must be empty, a contradiction. □

**Problem 1.1.** *Let $a$ and $b$ be integers such that $a > b > 0$. Then the set $\{a - b, a - 2b, \cdots\}$ contains a least positive integer.*

**Solution.** *Suppose the set* $\{a-b, a-2b, a-3b, \cdots\}$ *contains no positive integer. Then* $a - nb \leq 0$, *for all* $n \geq 1$. *But we have* $a > b$. *This implies* $a - b > 0$. *This is a contradiction to* $a - nb \leq 0$, *for all* $n \geq 1$. *Therefore, there exist* $n \in \mathbb{N}$ *such that* $\{a-b, a-2b, \cdots, a-nb\}$ *is a set of positive integers. By well ordering principle* $\{a-b, a-2b, \cdots, a-nb\}$ *contains a least positive integer and it is the least positive integer in* $\{a-b, a-2b, a-3b, \cdots\}$.

**Problem 1.2.** *Let* $a$ *be a negative integer and* $b$ *be a positive integer. Then the set* $\{a+b, a+2b, a+3b, \cdots\}$ *contains a least positive integer.*

**Solution.** *Since* $a < 0$, *let it be* $a = -a_1,\ a_1 > 0$. *We have to find* $n \in \mathbb{N}$ *such that* $a + nb > 0$.

*Case 1. If* $a_1 = b$, *then we have* $n = 2$, *since* $a + nb = -a_1 + 2a_1 = a_1 > 0$.

*Case 2. If* $a_1 > b$, *then we have* $n = a_1 + b$, *Since* $a + nb = a_1(b-1) + b^2 > 0$, *for all* $b \in \mathbb{N}$.

*Case 3. If* $a_1 < b$, *then we have* $n = 1$, *Since* $a + nb = b - a_1 > 0$.

*Thus in all cases, we can find* $n$ *such that* $a + nb > 0$. *Since* $n < n + 1$, *we must have* $a + nb < a + (n+1)b$. *Thus* $0 < a + nb < a + (n+1)b < \cdots$ *and so* $\{a+nb, a+(n+1)b, \cdots\}$ *is a set of positive integers. By well ordering principle* $\{a + nb, a + (n+1)b, \cdots\}$ *contains a least positive integer and it is the least positive integer of the given set.*

## 1.2. Division Algorithm

The most crucial and frequently applied notion relating to integers (divisibility) is covered in this section. Additionally, examples are provided that address the quotient and remainders while dividing as well as the parity of integers and their divisibility. The division algorithm, which provides the path to acquire quotient and remainders, is the major subject of this section.

**Definition 1.1.** *An integer* $b$ *is said to be divisible by an integer* $a(\neq 0)$, *if* $b$ *is a multiple of* $a$.
*If* $b$ *is divisible by* $a$, *we write* $a \mid b$, *(i.e.* $a$ *divides* $b$*) and otherwise we write* $a \nmid b$ *(i.e.* $a$ *does not divide* $b$*).*

**Example.** *1. If* $a = 5,\ b = 10$, *then* $b = 2a$ *and so* $a \mid b$.

2. *If* $a = 3,\ b = 4$, *then* $a \nmid b$.

**Note.** 1. $1 \mid a$ *for any* $a \in \mathbb{Z}$.

2. $a \mid 0$ *for any* $a \in \mathbb{Z}$.

3. $a \mid a$ *for any* $a \in \mathbb{Z}$.

**Properties.** *For any integers* $a(\neq 0), b, c, d$, *the following hold:*

1. *If* $a \mid b$ *and* $a \mid c$, *then* $a \mid (b + c)$.

2. *If* $a \mid b$, *then* $a \mid bc$.

3. *If* $a \mid b$ *and* $b \mid c$, *then* $a \mid c$.

4. *If* $a \mid b$ *and* $a \mid c$, *then* $a \mid (mb + nc)$ *whenever* $m \ \& \ n$ *are integers.*

5. $a \mid 1$ *iff* $a = \pm 1$.

6. *If* $a \mid b$ *and* $c \mid d$, *then* $ac \mid bd$.

7. $a \mid b$ *and* $b \mid a$ *if and only if* $a = \pm b$.

8. *If* $a \mid b$ *and* $b \neq 0$, *then* $|a| \leq |b|$.

*Proof.* 1. Suppose $a \mid b$ and $a \mid c$. Then $b = k_1 a$ and $c = k_2 a$ for some $k_1, k_2 \in \mathbb{Z}$. Now, $b + c = (k_1 + k_2)a$. Since $k_1 + k_2 \in \mathbb{Z}$, we can conclude that $a \mid (b + c)$.

2. Suppose $a \mid b$. Then $b = ka$ for some $k \in \mathbb{Z}$. Multiply both sides by $c$, we have $bc = (kc)a$. Since $kc \in \mathbb{Z}$, we have $a \mid bc$.

3. Suppose $a \mid b$ and $b \mid c$. Then $b = k_1 a,\ c = k_2 b$ for some $k_1, k_2 \in \mathbb{Z}$. Now,

$$\begin{aligned} c &= k_2 b \\ &= k_2(k_1 a) \\ c &= (k_2 k_1)a \end{aligned}$$

Therefore, $a|c$.

4. Suppose $a \mid b$ and $a \mid c$. Then $b = k_1 a$ and $c = k_2 a$ for some $k_1 k_2 \in \mathbb{Z}$. Let $m, n \in \mathbb{Z}$. Then $b = k_1 a \implies mb = m(k_1 a) = m_1 a$, where $m_1 = mk_1 \in \mathbb{Z}$ and $c = k_2 a \implies nc = n(k_2 a) = n_1 a$, where $n_1 = nk_2 \in \mathbb{Z}$. Thus we obtain $mb = m_1 a$ and $nc = n_1 a$. Therefore, $a \mid mb$ & $a \mid nc$ and so $a \mid (mb + nc)$

5. Suppose $a \mid 1$. Then $1 = ka$ for some $k \in \mathbb{Z}$. Since $k$ and $a$ are integer, this is possible only if $k = 1,\ a = 1$ or $a = -1,\ k = -1$. That is, $a = \pm 1$.
   Conversely, suppose that $a = \pm 1$. Then $1 = ka$, where $k = 1,\ a = 1$ and $-1 = ka$ where $k = 1,\ a = -1$. Therefore, $a \mid 1$.

6. Suppose $a \mid b$ and $c \mid d$. $b = k_1 a$ and $d = k_2 c$ for some $k_1, k_2 \in \mathbb{Z}$. Then

$$\begin{aligned} b = k_1 a \implies bd &= (k_1 a)d \\ bd &= (k_1 k_2)ac \end{aligned}$$

   Therefore, $ac \mid bd$.

7. Suppose $a \mid b$ and $b \mid a$. Then $b = k_1 a$ and $a = k_2 b$ where $k_1, k_2 \in \mathbb{Z}$. Now,

$$\begin{aligned} b = k_1 a &\implies b = k_1(k_2)b \\ &\implies b = (k_1 k_2)b \\ &\implies k_1 k_2 = 1 \\ &\implies k_1 = 1 = k_2 \text{ or } k_1 = -1 = k_2 \end{aligned}$$

   Therefore, $a = k_2 b \implies a = \pm b$. Conversely, suppose that $a = \pm b$. Then $a = b \implies a = 1(b) \implies b \mid a$.
   $a = -b \implies b = -a \implies b = (-1)a \implies a \mid b$. Therefore, $b \mid a$ & $a \mid b$.

8. Suppose $a|b$ and $b \neq 0$. Then $b = ka$, for some $k \in \mathbb{Z}$. Taking modulus on both sides, we get $|b| = |ka| = |k||a| \geq |a|$. Therefore, $|a| \leq |b|$.

□

**Definition 1.2** (Even Integer )**.** *An integer $a$ is said to be even if* $2 \mid a$.

**Definition 1.3** (Odd Integer)**.** *An integer $a$ is said to be odd if* $2 \nmid a$.