Masterclass Summary: Fundamentals of Arithmetic

Professor of Mathematics
ExamBhai Academic Board

August 10, 2026

Abstract

This document provides an elite, rigorous overview of core arithmetic principles, designed for advanced learners and competitive examination aspirants. We cover number systems, fundamental operations, divisibility theory, and modular arithmetic.

1 The Number Hierarchy

Arithmetic begins with the foundational structure of number systems. Let us review the primary sets of numbers:

- **Natural Numbers ($\mathbb{N}$):** $\{1, 2, 3, 4, \dots\}$
- **Whole Numbers ($\mathbb{W}$):** $\{0, 1, 2, 3, \dots\}$
- **Integers ($\mathbb{Z}$):** $\{\dots, -2, -1, 0, 1, 2, \dots\}$
- **Rational Numbers ($\mathbb{Q}$):** $\left\{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\right\}$
- **Real Numbers ($\mathbb{R}$):** The union of rational and irrational numbers.

2 Fundamental Theorem of Arithmetic

Every integer strictly greater than 1 either is a prime number itself or can be represented as a unique product of prime numbers, up to the order of the factors.

Theorem 2.1 (Unique Factorization)**.** *For any integer $n > 1$, there exist distinct primes $p_1 < p_2 < \cdots < p_k$ and positive integers $a_1, a_2, \dots, a_k$ such that:*

$$n = \prod_{i=1}^{k} p_i^{a_i} = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

and this representation is unique.

3 Divisibility and Greatest Common Divisor (GCD)

Definition 3.1 (Divisibility)**.** *We say that an integer a divides an integer b (denoted $a \mid b$) if there exists an integer c such that $b = ac$.*

The Euclidean Algorithm is an efficient method for computing the greatest common divisor of two integers a and b:

$$\gcd(a, b) = \gcd(b, a \pmod b)$$

Example 3.1 (Applying Euclidean Algorithm)**.** *Find* $\gcd(252, 105)$*:*

$$\begin{aligned} 252 &= 2 \times 105 + 42 \\ 105 &= 2 \times 42 + 21 \\ 42 &= 2 \times 21 + 0 \end{aligned}$$

Thus, $\gcd(252, 105) = 21$.

4 Modular Arithmetic Essentials

Modular arithmetic is a system of arithmetic for integers, where numbers "wrap around" upon reaching a certain value—the modulus.

Definition 4.1 (Congruence Modulo n)**.** *Let* n *be a positive integer. Two integers* a *and* b *are congruent modulo* n *(written* $a \equiv b \pmod{n}$*) if* n *divides their difference* $a - b$*.*

$$\forall a, b \in \mathbb{Z}, \quad a \equiv b \pmod{n} \iff n \mid (a - b)$$

4.1 Properties of Modular Addition and Multiplication

If $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then:

$$\begin{aligned} (a + b) &\equiv (c + d) \pmod{n} \\ (a \times b) &\equiv (c \times d) \pmod{n} \end{aligned}$$

5 Summary Visualized via TikZ

Below is a conceptual map of number systems generated programmatically: