Masterclass Summary: Advanced Foundations of Arithmetic

Prof. Alexander Wright, Ph.D.

August 10, 2026

Abstract

This lecture summary covers the rigorous foundations of arithmetic, exploring the algebraic properties of numbers, divisibility theory, fundamental theorem of arithmetic, and modular congruences. Designed for elite scholars seeking a deep, axiomatic understanding of elementary operations.

1 Axiomatic Foundations of Numbers

Arithmetic begins with the natural numbers $\mathbb{N} = \{1, 2, 3, \dots\}$, extended through the integers $\mathbb{Z}$, rational numbers $\mathbb{Q}$, and real numbers $\mathbb{R}$. The fundamental operations of addition $(+)$ and multiplication $(\times)$ satisfy the field axioms:

$$\begin{aligned} \text{Associativity:} \quad & (a+b)+c = a+(b+c) \\ \text{Commutativity:} \quad & a+b = b+a \\ \text{Distributivity:} \quad & a \cdot (b+c) = a \cdot b + a \cdot c \end{aligned}$$

2 Divisibility and the Euclidean Algorithm

An integer a is divisible by a non-zero integer b (denoted $b \mid a$) if there exists an integer k such that $a = bk$.

The **Division Algorithm** states that for any integers a and b with $b > 0$, there exist unique integers q and r such that:

$$a = bq + r, \quad 0 \le r < b$$

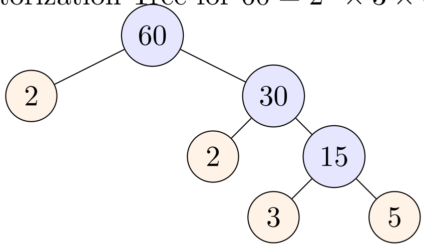
The Greatest Common Divisor ($\gcd(a, b)$) can be efficiently computed using the Euclidean Algorithm, relying on the principle that $\gcd(a, b) = \gcd(b, a \pmod b)$.

3 The Fundamental Theorem of Arithmetic

Every integer $n > 1$ can be represented uniquely as a product of prime numbers, up to the order of the factors. Let $p_1 < p_2 < \cdots < p_k$ be distinct primes and $a_i \ge 1$ be integers:

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

Prime Factorization Tree for $60 = 2^2 \times 3 \times 5$



4 Modular Arithmetic

Let m be a positive integer called the modulus. We say that a is congruent to b modulo m, written as:

$$a \equiv b \pmod{m} \iff m \mid (a - b)$$

This equivalence relation preserves sums and products, serving as the backbone for modern cryptography and number theory.