Lecture 3.4: Divisibility and primes

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 4190, Discrete Mathematical Structures

Divisibility

Definition

Let $n, d \in \mathbb{Z}$, with $d \neq 0$. We say d divides n, written $d \mid n$, if $n = dk$ for some $k \in \mathbb{Z}$, i.e.,

$$d \mid n \quad \Leftrightarrow \quad \exists k \in \mathbb{Z} \text{ such that } n = dk.$$

Other ways to say this are:

- n is divisible by d,
- n is a multiple of d,
- d is a divisor of n,
- d is a factor of n.

Key point

If d does not divide n, we write $d \nmid n$. Note that

$$d \nmid n \quad \Leftrightarrow \quad \frac{n}{d} \text{ is not an integer.}$$

Examples

(i) Every positive integer divides 0.

(ii) Every positive integer is divisible by 1 and itself.

(iii) The only divisors of 1 are 1 and -1.

Divisibility and primes

Recall that an integer $p > 0$ is prime if $p = ab$ implies either $p = a$ or $p = b$.

Proposition

An integer $p > 0$ is prime iff its only positive divisors are 1 and p.

Proof

Divisibility and primes

Proposition

Every positive integer is divisible by a prime.

Proof

Transitivity of divisibility

Statements

Let a, b, c be integers.

(i) If $a \mid b$ and $b \mid c$, then $a \mid c$.

(ii) If $a \mid b$ and $b \mid a$, then $a = b$.

Proof

(i)

(ii) This is false. Let $a = 2$, $b = -2$.

The fundamental theorem of arithmetic

Theorem

Given any integer $n > 1$, there exists $k \in \mathbb{N}$, distinct prime numbers $p_1 < \cdots < p_k$, and positive integers $e_1, \ldots, e_k$ such that

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

Moreover, the the sequence of p_i's and e_i's is unique.

Remark

Though unique factorization seems "obvious", there are other sets of numbers for which it fails. For example:

(i) The rational numbers do not have primes, or unique factorization.

(ii) In the set of numbers $R_{-5} := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$,

$$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$