M1C03 Lecture 16

Prime Numbers and the Fundamental Theorem of Arithmetic

Jeremy Lane

Oct 21, 2021

Announcement(s)

1. Quiz 5 and Assignment 2 are due Friday.
2. Test 1 details are on Avenue.

Overview

Prime numbers.

The fundamental theorem of arithmetic.

Strong induction.

Reference: Lakins, Section 3.2 and 2.3.

A useful fact

Theorem

For all positive integers a and n, if a divides n, then $a \leq n$.

Prime numbers

Definition (Lakins, Definition 2.1.7)

A positive integer p is *prime* if:

1. $p > 1$ AND
2. For all positive integers a and b, if $p = ab$, then $a = 1$ or $b = 1$.

Some reasons to care about prime numbers

- Number theory (Riemann hypothesis).
- Modern cryptography (e.g. RSA encryption).
- Computer science (e.g. hash tables).

"Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reason to believe that it is a mystery into which the human mind will never penetrate."

- Leonhard Euler

Theorem (The fundamental theorem of arithmetic, Lakins, Theorem 3.2.3)

For all positive integers $n > 1$, there exists a positive integer s and prime numbers $p_1, \ldots, p_s$ such that

$$n = p_1 \cdot p_2 \cdots p_s.$$

Moreover, the list of prime numbers with this property is unique (up to reordering).

Theorem (The fundamental theorem of arithmetic, Lakins, Theorem 3.2.3)

For all positive integers $n > 1$, there exists a positive integer s and prime numbers $p_1, \dots, p_s$ such that

$$n = p_1 \cdot p_2 \cdots p_s.$$

Strong Induction

Let $P(n)$ be a statement that depends on an arbitrary positive integer n.

IF

1. $P(1)$ AND
2. For all positive integers n, if for all positive integers k with $1 \leq k \leq n$, $P(k)$, then $P(n+1)$

THEN for all positive integers n, $P(n)$.

Induction does not have to start at $n = 1$

Let n_0 be an integer and let $P(n)$ be a statement that depends on an arbitrary integer $n \geq n_0$.

IF

1. $P(n_0)$ AND
2. For all integers $n \geq n_0$, if $P(n)$, then $P(n+1)$

THEN for all integers $n \geq n_0$, $P(n)$.

Let n_0 be an integer and let $P(n)$ be a statement that depends on an arbitrary integer $n \geq n_0$.

IF

1. $P(n_0)$ AND
2. For all integers $n \geq n_0$, if for all integers k with $n_0 \leq k \leq n$, $P(k)$, then $P(n+1)$

THEN for all integers $n \geq n_0$, $P(n)$.

Infinitude of the primes

Theorem (Euclid, Lakins, Theorem 2.3.4)

There are infinitely many prime numbers.