M1C03 Lecture 29

Relatively prime integers and the Fundamental Theorem of Arithmetic

Jeremy Lane

Nov 24, 2021

Announcement(s)

1. Test 2 Friday
2. No quiz this week

Overview

Reference: Lakins, section 6.3.

Relatively prime integers

Definition: An integer a *divides* an integer b if there exists an integer k such that $b = ka$. We write $a|b$.

Definition: A positive integer p is *prime* if $p > 1$ and for all positive integers a and b, if $p = ab$, then $a = 1$ or $b = 1$.

Definition: The *greatest common divisor* of two integers a and b is the largest positive integer c such that $c|a$ and $c|b$. We denote this number $\gcd(a, b)$.

Definition: Two integers a and b, not both equal to zero, are *relatively prime* if $\gcd(a, b) = 1$.

Theorem (Lakins, Theorem 6.3.2)

Let a and b be integers that are not both 0. Then a and b are relatively prime if and only if there exists $x, y \in \mathbb{Z}$ such that

$$1 = xa + yb.$$

Example

Show that if $d = \gcd(a, b)$, then $\gcd(a/d, b/d) = 1$.

Euclid's Lemma

Theorem (Lakins, Lemma 6.3.3)

Let $a, b, c \in \mathbb{Z}$. *If* $\gcd(a, c) = 1$ *and* $c|ab$, *then* $c|b$.

Euclid's Lemma

Corollary (Lakins, Lemma 6.3.5)

Let p be a prime number and let $b_1, \ldots, b_r$ be integers. If $p | b_1 \ldots b_r$, then there exists $i \in \{1, \ldots, r\}$ such that $p | b_i$.

The Fundamental Theorem of Arithmetic

Theorem

Every positive integer larger than 1 can be written uniquely (up to reordering) as a product of primes.