MTH 331 - Homework #5 Draft

Joe White

October 17, 2025

Exercise 2: Euclid's Lemma and Prime Factorization

Euclid's Lemma for Finite Products

Statement. If p is prime and p divides a product of positive integers,

$$p \mid a_1 a_2 \cdots a_n,$$

then p divides at least one of the a_i.

Proof. We prove this by induction on n.

Base case ($n = 2$): This is the usual Euclid's Lemma: if $p \mid a_1 a_2$, then $p \mid a_1$ or $p \mid a_2$.

Inductive step: Assume the result holds for a product of n factors. Now suppose $p \mid a_1 a_2 \cdots a_{n+1}$. Let $b = a_1 a_2 \cdots a_n$, so that $p \mid b a_{n+1}$. By the base case, either $p \mid b$ or $p \mid a_{n+1}$. If $p \mid a_{n+1}$, we are done. If $p \mid b$, then by the inductive hypothesis p divides one of $a_1, a_2, \ldots, a_n$. Thus p divides at least one of the a_i's for $i = 1, 2, \ldots, n+1$.

Therefore, by induction, the statement holds for all $n \in \mathbb{Z}^+$. □

Existence of Prime Factorizations

Statement. Every integer $n > 1$ can be written as a product of primes.

Proof (by least counterexample). Suppose not, and let $n_0 > 1$ be the smallest integer that cannot be written as a product of primes.

If n_0 is prime, then it already has a prime factorization, a contradiction. If n_0 is composite, then $n_0 = ab$ for some integers a, b with $1 < a, b < n_0$. By minimality of n_0, both a and b can be written as products of primes:

$$a = p_1 p_2 \cdots p_r, \qquad b = q_1 q_2 \cdots q_s.$$

Multiplying gives

$$n_0 = ab = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s,$$

which is also a product of primes, again a contradiction. Hence, every integer $n > 1$ can be expressed as a product of primes.

Remark. This proof doesn't work well by induction, since it relies on choosing the smallest counterexample and reasoning downward. In contrast, induction proceeds forward from smaller to larger values, so the least-counterexample argument fits better here.