MTH 331 - Homework #5

Joe White

November 12, 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 result cannot be proved naturally by induction on n. A proof by induction would require a relationship between the prime factorization of n_0 and that of $n_0 - 1$, since the inductive hypothesis would only apply to $n_0 - 1$. However, consecutive integers do not have any simple relationship between their prime factorizations. In the least-counterexample proof, when n_0 is composite, we instead rely on two smaller numbers $a, b < n_0$ with $n_0 = ab$. Because the argument depends on such smaller factors rather than the immediately preceding integer, the inductive hypothesis would not be sufficient, and a least-counterexample argument is more appropriate here.

Exercise 1: Proofs by Least Counterexample

Sum of the First n Odd Numbers

Claim. For all $n \in \mathbb{Z}^+$,

$$1 + 3 + 5 + \cdots + (2n-1) = n^2.$$

Proof (least counterexample). Assume the set

$$S = \left\{ n \in \mathbb{Z}^+ \ : \ 1 + 3 + \cdots + (2n-1) \neq n^2 \right\}$$

is nonempty, and let n_0 be its least element. Then the statement is true for every $1 \leq k < n_0$, and in particular

$$1 + 3 + \cdots + \big(2(n_0 - 1) - 1\big) = (n_0 - 1)^2.$$

Add the next odd term $2n_0 - 1$ to both sides:

$$1 + 3 + \cdots + \big(2(n_0 - 1) - 1\big) + (2n_0 - 1) = (n_0 - 1)^2 + (2n_0 - 1) = n_0^2.$$

But the left-hand side is exactly $1 + 3 + \cdots + (2n_0 - 1)$, so the equality holds at n_0, contradicting the definition of n_0. Therefore S is empty and the formula holds for all $n \in \mathbb{Z}^+$. □

Sum of the First n Integers

Claim. For all $n \in \mathbb{Z}^+$,

$$1 + 2 + 3 + \cdots + n \ = \ \frac{n(n+1)}{2}.$$

Proof (least counterexample). Assume the set

$$T = \left\{ n \in \mathbb{Z}^+ \ : \ 1 + 2 + \cdots + n \neq \frac{n(n+1)}{2} \right\}$$

is nonempty, and let n_0 be its least element. Then for every $1 \leq k < n_0$,

$$1 + 2 + \cdots + k \ = \ \frac{k(k+1)}{2}.$$

Applying this at $k = n_0 - 1$ and then adding n_0 to both sides gives

$$1 + 2 + \cdots + (n_0 - 1) + n_0 = \frac{(n_0 - 1)n_0}{2} + n_0 = \frac{n_0(n_0 - 1 + 2)}{2} = \frac{n_0(n_0 + 1)}{2}.$$

Hence the identity also holds at n_0, contradicting the choice of n_0. Therefore T is empty and the formula holds for all $n \in \mathbb{Z}^+$. □

Which Method Feels More Natural?

For these two summation formulas, induction feels more natural: each case at $n+1$ is obtained by adding the "next term" to the case at n. Least counterexample works (and is formally equivalent to induction over $\mathbb{Z}^+$), but it is especially well-suited when a minimal failure leads you to factor or otherwise use *some* smaller numbers (not just $n - 1$), as in the existence of prime factorizations.