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 for $i = 1, \ldots, n+1$.

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

Remark. A proof by induction would require a relationship between the 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 argument above, when n_0 is composite, we instead use two arbitrary smaller integers $a, b < n_0$ with $n_0 = ab$. Since such information does not follow from the case $n_0 - 1$, an inductive hypothesis would not be strong enough. A least-counterexample argument is therefore more appropriate here.

Exercise 3:

Assume all a_i and a are real numbers, and any bases appearing in exponents are positive to avoid complex number.

Part I.

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

$$b(a_1 + a_2 + \cdots + a_n) = ba_1 + ba_2 + \cdots + ba_n.$$

Proof. This can be proved with induction. *Base case ($n = 1$):* When the sum has only one term, the expression becomes

$$b(a_1) = ba_1,$$

which is true by the ordinary distributive law. Thus the statement holds for $n = 1$.

Inductive step: Assume that the distributive property holds for a sum of n terms; that is,

$$b(a_1 + \cdots + a_n) = ba_1 + \cdots + ba_n.$$

We must show that it then holds for a sum of $n + 1$ terms. Starting with the longer sum,

$$b(a_1 + \cdots + a_n + a_{n+1}),$$

we group the first n terms together:

$$b\big((a_1 + \cdots + a_n) + a_{n+1}\big).$$

Using the distributive law,

$$b(a_1 + \cdots + a_n) + ba_{n+1}.$$

Now we apply the inductive hypothesis to the first part:

$$(ba_1 + \cdots + ba_n) + ba_{n+1},$$

which is exactly what we want for $n + 1$ terms.

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

Part II.

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

$$(a_1 a_2 \cdots a_n)^b = a_1^b a_2^b \cdots a_n^b.$$

Proof. This can also be proved by induction.

Base case ($n = 1$): When there is only one factor,

$$(a_1)^b = a_1^b,$$

which is true by definition.

Inductive step: Assume the identity holds for a product of n terms:

$$(a_1 \cdots a_n)^b = a_1^b \cdots a_n^b.$$

Want to show that it then holds for $n+1$ terms. Consider the product with one additional factor:

$$(a_1 a_2 \cdots a_n a_{n+1})^b.$$

Group first n terms together:

$$\big((a_1 \cdots a_n)\, a_{n+1}\big)^b.$$

Using the rule $(xy)^b = x^b y^b$ for positive x, y,

$$(a_1 \cdots a_n)^b\, a_{n+1}^b.$$

Finally, apply the inductive hypothesis to the first factor:

$$(a_1^b \cdots a_n^b)\, a_{n+1}^b,$$

which is the desired expression.

Thus, by induction, the identity holds for all $n \in \mathbb{Z}^+$.