Pledge: *I pledge my honor that I have abided by the Stevens Honor System.* -Eric Altenburg

---

1: The statement of the fundamental theorem of arithmetic given above is somewhat vague. What is a prime number? What is a product of primes? And what does it mean for such a product to be unique? Explain.

A natural number p is prime if its only divisors are 1 and p, and $p \neq 1$.
A product of primes can be written as $n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k$ where $n, k \in \mathbb{N}$
For a product to be unique, it means that when writing the product of primes as $n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k$ where $n, k \in \mathbb{N}$, no two or more p_k's can be the same number. For example, $20 = 2 \cdot 2 \cdot 5 = 2^2 \cdot 5$ would not be unique as there are two 2's.

2: Our first goal will be to prove the existence of a factorization into primes. Write down a strategy for doing so, and be prepared to explain it in class.

We can assume that there exists a number that does not have a factorization into primes. Let n be the smallest such number that cannot be factored into primes. Since n is not prime, then it is composite and can be factored as such $n = a \cdot b$ such that $1 < a$ and $b < n$. However, since we assumed that n was the smallest such number that was unable to be factored into primes, then a and b must be products of primes. With this, $a \cdot b$ is a product of primes and so n is a product of primes as well. This contradicts the initial assumption.

3: Our next goal will be to prove the uniqueness of a factorization into primes, which will entail several steps. For each of these steps, write down another proof strategy, and be prepared to explain it in class.

(Step 1: Prove Bézout's theorem, namely that if two integers a and b are coprime, then there exist integers x and y such that $ax + by = 1$.)

If a and b are coprime, then we can use the idea that $\gcd(a, b) = 1$ to show that $\gcd(a, b) = ax + by$ which would show that x and y exist. Assume there is a common divisor c for a and b. c would then divide ax and by or $ax + by$ which we know to be 1. That means c divides 1 so $c = 1$. Since $c = 1$, this shows that x and y exist.

(Step 2: Prove Euclid's lemma, namely that if P is prime and $p \mid ab$, where $a, b \in \mathbb{Z}$, then $p \mid a$ or $p \mid b$)

We can use Bézout's theorem for this where $ax + by = 1$ and a, b are relatively prime. In the context of this problem, let's assume n and a are relatively prime numbers and $n \mid ab$. Then with Bézout's theorem, we can say $nx + ay = 1$. Multiplying both sides by b would give $nxb + ayb = b$. This means that n divides (nxb) and it divides (ayb) because of the assumption, and because of this, that means b is also divisible by n. This proves that $n \mid b$ which is the lemma.

(Step 3: Prove uniqueness with the help of the previous two results.)

Assume we have the smallest number that can be written as two distinct prime factorizations, call it s. Then $s = p_1 \cdot p_2 \cdot \ldots \cdot p_m = q_1 \cdot q_2 \cdot \ldots \cdot q_n$. From Euclid's lemma, we know that the prime number $p_1 \mid q_1$ or $p_1 \mid q_2 \cdot \ldots \cdot q_n$. So we can then say that $p_1 = q_k$ for some k. So by removing these items from the equation we now have $s' = p_2 \cdot \ldots \cdot p_m = q_1 \cdot q_2 \cdot \ldots \cdot q_n$ but with some q_k missing in the second factorization as well. Because these were removed, we are left with another number s' where $s' < s$ which contradicts the initial assumption, so no such smallest number can exist proving uniqueness.