CS 173 Episode V — The Recursion Fairy Strikes Back

Part A: Fundamental Theorem of Arithmetic, Again

Theorem (Fundamental Theorem of Arithmetic)
Every integer greater than 1 has a unique prime factorization

up to rearrangement of factors

Lemma (Euclid's Lemma).
If $a|bc$, then $a|b$ or $a|c$.

Proof. First, we prove existence of a factorization by induction.

Base Case: $n=2$, $2=2$ ← prime factorization

Base case: n is prime, n=n.

IH: For $2 \le k < n$, k has a prime factorization.

IS: Case n prime: $n=n$ ← prime factorization.

Case n composite: $n=ab$ where $2 \le a, b < n$.

By IH, a & b have prime factorizations

$a = p_1 p_2 \cdots p_k$ for primes p_1 to p_k,

$b = q_1 q_2 \cdots q_\ell$ for primes q_1 to q_ℓ.

Then $n = ab = p_1 \cdots p_k q_1 \cdots q_\ell$.

So n has a prime factorization.

Now, prove uniqueness, also by induction.

Base Case: n is prime, then the only factors of n are 1 & n, so $n=n$ is the only possible prime factorization of n.

IH: For $0 \le k < n$, k has a unique prime factorization.

IS: Let n be composite. Let $p_1 \cdots p_k$ & $q_1 \cdots q_\ell$ be two prime factorizations of n, such that

be two prime factorizations of n, such that

$p_1 \le p_2 \le \cdots \le p_k$ & $q_1 \le q_2 \le \cdots \le q_\ell$.

$p_1 p_2 \cdots p_k = n = q_1 q_2 \cdots q_\ell$, so $p_1 \mid q_1 \cdots q_\ell$.

By Euclid's Lemma, $\exists i$ s.t. $p_1 \mid q_i$.

Since q_i is prime, $p_1 = q_i$.

$p_1 (p_2 \cdots p_k) = p_1 (q_1 \cdots q_{i-1} q_{i+1} \cdots q_\ell)$.

Set $m = p_2 \cdots p_k = q_1 \cdots q_{i-1} q_{i+1} \cdots q_\ell$.

By the I.H., m has a unique factorization,

so $(p_2, p_3 \cdots, p_k) = (q_1, \cdots, q_{i-1}, q_{i+1}, \cdots q_\ell)$.

In fact, $q_i = q_1$ and

$(p_2, p_3 \cdots, p_k) = (q_2, q_3 \cdots q_\ell)$.

So $(p_1, p_2 \cdots p_k) = (q_1, q_2 \cdots q_\ell)$.

So $k = \ell$, & $p_i = q_i$ $\forall i$ $\square$