5. Prove the Fundamental Theorem of Arithmetic, that every integer $n \geq 2$ has a unique prime factorization (i.e. prove that the prime factorization from the last proof is unique).

We have already shown (in lecture) that each integer $n \geq 2$ has a prime factorization. It remains to show that this factorization is unique.

Suppose in order to derive a contradiction that the prime factorization is not unique. Then there exists a least integer $n \geq 2$ such that

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell \quad \text{where } p_i, q_j,\ 1 \leq i \leq k,\ 1 \leq j \leq \ell \text{ are prime numbers}$$

This equality gives us that the p_i divide $q_1 q_2 \cdots q_\ell$. Without loss of generality, we focus on p_1.

$p_1 | q_1 q_2 \cdots q_\ell$ implies that p_1 divides one of $q_1, q_2, \ldots, q_\ell$, since they are prime.

Without loss of generality, $p_1 | q_1$. Since both are prime, this means $p_1 = q_1$.

Thus $\cancel{p_1} p_2 \cdots p_k = \cancel{q_1} q_2 \cdots q_\ell \Rightarrow p_2 \cdots p_k = q_2 \cdots q_\ell$

This contradicts our assumption that n was the <u>least</u> integer that could be written as the product of two sets of primes.

Therefore there does not exist such a $n \Rightarrow$ prime factorizations are unique.