You proved that every natural number n such that $n \geq 2$ has a prime factorization. This begs the question: can a natural number posess more than one prime factorization? The answer is complicated by the fact that our definition of a prime factorization seems to depend on the order:

$$10 = 2 \cdot 5 \qquad \text{and} \qquad 10 = 5 \cdot 2$$

are two different factorizations. To deal with this, we define an ordered prime factorization of n to be a sequence $p_1, \ldots, p_k$ of primes such that $p_1 \leq p_2 \leq \cdots \leq p_k$ and such that

$$n = p_1 \cdot \cdots \cdot p_k.$$

Given a prime factorization, we can always obtain an ordered prime factorization simply by rearranging the factors. Making this absolutely precise is a little subtle and involves tacking down the notion of rearranging a set. We might address this a little later.

Assuming we can do the rearranging, one way to approach the uniqueness question is to show that every $n \in \mathbb{Z}_{\geq 2}$ has no more than one ordered prime factorization.

Proposition 6.D: Suppose $(p_1, \ldots, p_k)$ and $(q_1, \ldots, q_\ell)$ are finite sequences of primes such that

$$p_1 \cdot \cdots \cdot \cdots \cdot p_k = q_1 \cdot \cdots \cdot \cdots \cdot q_\ell$$

and such that $p_1 \leq \cdots \leq p_k$ and $q_1 \leq \cdots \leq q_\ell$. Then $k = \ell$ and $p_i = q_i$ for $1 \leq i \leq k$.

Proof. Let $P(K)$ be the statement that if $(p_1, \ldots, p_k)$ and $(q_1, \ldots, q_\ell)$ are finite sequences of primes such that $k \leq K$ and $\ell \leq K$, and such that

$$p_1 \cdot \cdots \cdot \cdots \cdot p_k = q_1 \cdot \cdots \cdot \cdots \cdot q_\ell,$$

then $k = \ell$ and $p_i = q_i$ for $1 \leq i \leq k$. We will show that $P(K)$ is true for all $K \in \mathbb{N}$ by induction on K. The case $K = 1$ is obvious.

Suppose for some $K \in \mathbb{N}$ that $P(K)$ is true. Now suppose $(p_1, \ldots, p_k)$ and $(q_1, \ldots, q_\ell)$ are finite sequences of primes such that $k \leq K + 1$ and $\ell \leq K + 1$, and such that

$$p_1 \cdot \cdots \cdot p_k = q_1 \cdot \cdots \cdot q_\ell$$

Now either $k = 1$ or $k > 1$. Suppose $k = 1$. Then

$$p_1 = q_1 \cdot \cdots \cdot q_\ell.$$

Since p_1 is prime, and since each factor on the right-hand-side is a natural number larger than 1, each one must be p_1. So $p_1 = q_1^\ell$. But $p_1^\ell > p_1$ if $\ell > 1$. Hence $\ell = 1$ and $p_1 = q_1$.

The result is proved similarly if $\ell = 1$, so we turn to the case where $k > 1$ and $\ell > 1$ as well. Without loss of generality, we may assume $p_k \geq q_\ell$. Since p_k is prime, and since it divides the product on the left, our corollary of Euclid's lemma implies that p_k divides the product on the right. Thus $p_k = q_i$ for some i. Now $q_j \leq q_\ell$ for all j, so $p_k \leq q_\ell$. Since $p_k \geq q_\ell$ as well we conclude that $p_k = q_\ell$. Since $p_k \neq 0$, we can apply Axiom 1.5 and conclude

$$p_1 \cdot \cdots \cdot \cdots \cdot p_{k-1} = q_1 \cdot \cdots \cdot \cdots \cdot q_{\ell-1}$$

Applying the induction hypothesis we conclude that $k - 1 = \ell - 1$ and hence $k = \ell$. Moreover, $p_i = q_i$ for $1 \leq i \leq k - 1$. Since $p_k = q_\ell = q_k$ as well, we have established that $P(K + 1)$ is also true. $\square$

We can now establish existence and uniqueness of ordered prime factorizations as follows. Let $n \in \mathbb{Z}$ with $n \geq 2$. Given a prime factorization of it, rearrange it to obtain an ordered prime factorization. (Mild hole here!) This establishes existence. Uniqueness follows immediately from Proposition 6.D.