Number theorists call this “the fundamental theorem of arithmetic”, or maybe this plus the words “unique factorization”. But I think there are much more fundamental theorems than this one. How about
\[ \forall n: \text{nat} . \exists m: \text{nat} . m > n \]
which says “for every natural number, there's a bigger one”. I think that's more fundamental.

The plan is to prove that every positive integer is a product of primes by using
\[ \forall n: \text{nat} . (\forall m: \text{nat} . m < n \Rightarrow P m) \Rightarrow P n \Rightarrow \forall n: \text{nat} . P n \]
which is a consequence of induction, sometimes called “course-of-values induction”; it is in Subsection 6.0.0 of the textbook. The number 1 is the empty product, and every element of the empty bunch is prime, so 1 is a product of primes. For each \( n \geq 2 \), if \( n \) is prime, then it's the product of one prime (itself). If \( n \) is non-prime, then it's a product \( ab \) where \( a, b : 2,..n \). By the induction hypothesis, both \( a \) and \( b \) are products of primes. So \( ab \) is also a product of primes. That's an informal proof, or proof plan. Now we need to formalize it.

The question says a prime is a natural with exactly two factors. So define
\[ \text{prime} = \langle p: \text{nat} \rightarrow (\forall n: \text{nat} . p \times n \text{nat}) = 2 \rangle \]

The proof plan says we need \( P n \) to mean “\( n \) is a product of primes” for positive integers \( n \), and that can be defined as
\[ P 1 = \top \]
\[ \forall n: \text{nat}+2 . (P n = \text{prime} n \lor \exists a, b: 2,..n . P a \land P b \land n = a \times b) \]

We want to prove \( \forall n: \text{nat}+1 . P n \). That's almost the consequent of induction, except for the +1. So we redefine \( P n \) to mean “\( n+1 \) is a product of primes”.
\[ P 0 = \top \]
\[ \forall n: \text{nat}+1 . (P n = \text{prime} (n+1) \lor \exists a, b: 2,..n+1 . P a \land P b \land n+1 = a \times b) \]

Now we want to prove \( \forall n: \text{nat} . P n \).

\[
\begin{align*}
\forall n: \text{nat} . P n & \quad \text{induction} \\
\iff & \quad \text{divide first domain: } \text{nat} = 0, \text{nat}+1 \\
= & \quad ((\forall m: \text{nat} . m < 0 \Rightarrow P m) \Rightarrow P 0) \land (\forall n: \text{nat} . m < n \Rightarrow P m) \Rightarrow P n \\
= & \quad \forall n: \text{nat}+1 . (\forall m: \text{nat} . m < n \Rightarrow P m) \Rightarrow P n \quad \text{divide second domain: } \text{nat} = 0, \text{nat}+1 \\
= & \quad \forall n: \text{nat}+1 . (0 < n \Rightarrow P 0) \land (\forall m: \text{nat}+1 . m < n \Rightarrow P m) \Rightarrow P n \quad \text{Left conjunct is } \top \\
= & \quad \forall n: \text{nat}+1 . (\forall m: \text{nat}+1 . m < n \Rightarrow P m) \Rightarrow P n \quad \text{idempotence} \\
= & \quad \forall n: \text{nat}+1 . (\forall a: \text{nat}+1 . a < n \Rightarrow P a) \land (\forall b: \text{nat}+1 . b < n \Rightarrow P b) \Rightarrow P n \quad \text{rename local variables} \\
= & \quad \top 
\end{align*}
\]

Now we need to use the definition of \( P \) and then \( \text{prime} \) and it's going to be a lot of hard work and then eventually we get