Now we want to prove the +1. So we rede

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

$$\forall n: \text{nat} \exists m: \text{nat} \cdot m > n$$

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

$$\forall n: \text{nat} \cdot (\forall m: \text{nat} \cdot m < n \Rightarrow Pm) \Rightarrow Pn \Rightarrow \forall n: \text{nat} \cdot Pn$$

which is a consequence of induction, sometimes called “course-of-values induction”, or “Noetherian induction”; it is near the bottom of page 92 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 $a \times b$ where $a, b: 2, \ldots, n$. By the induction hypothesis, both $a$ and $b$ are products of primes. So $a \times b$ 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

$$\text{prime} = \langle p: \text{nat} \rightarrow (\forall \exists n: \text{nat} \cdot p \cdot n \cdot \text{nat}) = 2 \rangle$$

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

$$P 1 = \top
\forall n: \text{nat}+2 \cdot (P n \Rightarrow \text{prime} n \lor \exists a, b: 2, \ldots, n \cdot P a \land P b \land n = a \times b)$$

We want to prove $\forall n: \text{nat}+1 \cdot P n$. 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”.

$$P 0 = \top
\forall n: \text{nat}+1 \cdot (P n \Rightarrow \text{prime} (n+1) \lor \exists a, b: 2, \ldots, n+1 \cdot P a \land P b \land n+1 = a \times b)$$

Now we want to prove $\forall n: \text{nat} \cdot P n$.

$$\forall n: \text{nat} \cdot P n
\iff \forall n: \text{nat} \cdot (\forall m: \text{nat} \cdot m < n \Rightarrow Pm) \Rightarrow Pn
\quad \text{divide first domain: } \text{nat} = 0, \text{nat}+1
\iff ((\forall m: \text{nat} \cdot m < 0 \Rightarrow Pm) \Rightarrow P0) \land (\forall n: \text{nat}+1 \cdot (\forall m: \text{nat} \cdot m < n \Rightarrow Pm) \Rightarrow Pn)
\quad \text{Left conjunct simplifies to } P0 \text{ and then to } \top .
\iff \forall n: \text{nat}+1 \cdot (\forall m: \text{nat} \cdot m < n \Rightarrow Pm) \Rightarrow Pn
\quad \text{divide second domain: } \text{nat} = 0, \text{nat}+1
\iff \forall n: \text{nat}+1 \cdot (0 < n \Rightarrow P0) \land (\forall m: \text{nat}+1 \cdot m < n \Rightarrow Pm) \Rightarrow Pn
\quad \text{Left conjunct is } \top .
\iff \forall n: \text{nat}+1 \cdot (\forall m: \text{nat}+1 \cdot m < n \Rightarrow Pm) \Rightarrow Pn
\quad \text{idempotence}
\iff \forall n: \text{nat}+1 \cdot (\forall m: \text{nat}+1 \cdot m < n \Rightarrow Pm) \land (\forall m: \text{nat}+1 \cdot m < n \Rightarrow Pm) \Rightarrow Pn
\quad \text{rename local variables}
\iff \forall n: \text{nat}+1 \cdot (\forall a: \text{nat}+1 \cdot a < n \Rightarrow Pa) \land (\forall b: \text{nat}+1 \cdot b < n \Rightarrow Pb) \Rightarrow Pn
\quad \text{Now we need to use the definition of } P \text{ and then } \text{prime} \text{ and it's going}
\quad \text{to be a lot of hard work and then eventually we get}
\iff \top