369 Prove that every positive integer is a product of primes. By “product” we mean the result of multiplying together any natural number of (not necessarily distinct) numbers. By “prime” we mean a natural number with exactly two factors.

After trying the question, scroll down to the solution.

§ 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

$\forall n: nat\cdot \exists m: nat\cdot m>n$

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

$\forall n: nat\cdot (\forall m: nat\cdot m<n \Rightarrow P\ m) \Rightarrow P\ n \implies \forall n: nat\cdot P\ n$

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 $n\ge 2$, 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 $a, b: 2,..n$. 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

$prime = \langle p: nat\cdot (¢§n: nat\cdot p: n\times nat) = 2\rangle$

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

$P\ 1 = \top$

$\forall n: nat+2\cdot (P\ n = prime\ n \lor \exists a, b: 2,..n\cdot P\ a \land P\ b \land n=a\times b)$

We want to prove $\forall n: nat+1\cdot P\ n$. 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".

$P\ 0 = \top$

$\forall n: nat+1\cdot (P\ n = prime\ (n+1) \lor \exists a, b: 2,..n+1\cdot P\ a \land P\ b \land n+1=a\times b)$

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

$\forall n: nat\cdot P\ n$ induction

$\Leftarrow$ $\forall n: nat\cdot (\forall m: nat\cdot m<n \Rightarrow P\ m) \Rightarrow P\ n$ divide first domain: $nat = 0, nat+1$

$=$ $((\forall m: nat\cdot m<0 \Rightarrow P\ m) \Rightarrow P\ 0) \land (\forall n: nat+1\cdot (\forall m: nat\cdot m<n \Rightarrow P\ m) \Rightarrow P\ n)$

The left conjunct simplifies to $P\ 0$ and then to $\top$.

$=$ $\forall n: nat+1\cdot (\forall m: nat\cdot m<n \Rightarrow P\ m) \Rightarrow P\ n$ divide second domain: $nat = 0, nat+1$

$=$ $\forall n: nat+1\cdot (0<n \Rightarrow P\ 0) \land (\forall m: nat+1\cdot m<n \Rightarrow P\ m) \Rightarrow P\ n$ Left conjunct is $\top$.

$=$ $\forall n: nat+1\cdot (\forall m: nat+1\cdot m<n \Rightarrow P\ m) \Rightarrow P\ n$ idempotence

$=$ $\forall n: nat+1\cdot (\forall m: nat+1\cdot m<n \Rightarrow P\ m) \land (\forall m: nat+1\cdot m<n \Rightarrow P\ m) \Rightarrow P\ n$

rename local variables

$=$ $\forall n: nat+1\cdot (\forall a: nat+1\cdot a<n \Rightarrow P\ a) \land (\forall b: nat+1\cdot b<n \Rightarrow P\ b) \Rightarrow P\ n$

Now we need to use the definition of P and then $prime$ and it's going to be a lot of hard work and then eventually we get

$=$ $\top$