Math 127: Induction

Mary Radcliffe

1 Induction Fundamentals

The moment we've all been waiting for: a full treatment of proof by induction! Before we get into the technique, here, let us first understand what kinds of propositions we wish to treat using induction. As a first understanding, we will consider propositions that take the basic form:

$$\forall n \in \mathbb{N},\ p(n) \tag{1}$$

where $p(n)$ is a proposition about n. For example, suppose we wish to prove something like the following:

$$\forall n \in \mathbb{N},\ 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

Using the techniques we previously developed in the notes about logic and proof, you might find yourself at something of a loss. While we are able to prove this proposition directly, let's imagine we don't see a way forward with direct proof. Contradiction and contrapositive seem pretty infeasible here, since assuming that two numbers are not equal doesn't really give us much to work with. So we'd like to develop a different path.

But, ah! We remember something useful: the Induction Axiom from the Peano Axioms! In case you've forgotten, let's restate it here:

> If S is a set of natural numbers, having the property that $1 \in S$ and that if $a \in S$, then the successor a^+ of a is also in S, then $S = \mathbb{N}$. (2)

To apply that to our current situation, we can look to where we wish to have all of $\mathbb{N}$: we wish that every number in $\mathbb{N}$ makes the proposition true. So we could imagine that we have a set S, where we define S by saying that $n \in S$ if and only if $p(n)$ is true. The proposition we wish to prove, then, is that $S = \mathbb{N}$, so that $p(n)$ is true for every $n \in \mathbb{N}$.

This, now, can be done using (2). If we can show that $1 \in S$ and also that whenever $a \in S$, we have also $a + 1 \in S$, then (2) implies that $S = \mathbb{N}$, so that $p(n)$ is true for all $n \in \mathbb{N}$. Let's do a proof from this interpretation.

Example 1. Use the Inductive Axiom stated in (2) to prove

$$\forall n \in \mathbb{N},\ 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

Proof. Define S to be the set of natural numbers n such that $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$.
First, note that for $n = 1$, this equation states $1 = \frac{1(2)}{2}$, which is clearly true. Therefore, $1 \in S$.

Now, suppose that $n \in S$. We wish to prove that the successor n^+ of n is also in S. Recalling that $n^+ = n + 1$, we wish to prove that $n + 1$ is also in S; that is to say, we wish to prove that $1 + 2 + 3 + \cdots + (n + 1) = \frac{(n+1)((n+1)+1)}{2}$. Consider:

$$\begin{aligned} 1 + 2 + 3 + \cdots + (n + 1) &= 1 + 2 + 3 + \cdots + n + (n + 1) \\ &= (1 + 2 + 3 + \cdots + n) + (n + 1) \\ &= \frac{n(n + 1)}{2} + (n + 1) \quad (\text{since } n \in S) \\ &= (n + 1)\left(\frac{n}{2} + 1\right) \\ &= (n + 1)\left(\frac{n + 2}{2}\right) \\ &= \frac{(n + 1)((n + 1) + 1)}{2}. \end{aligned}$$

Therefore, by definition of S, we have that $n + 1 \in S$.
Thus, we have that S is a set such that $1 \in S$ and S contains all its successors. By the Inductive Axiom, we therefore have that $S = \mathbb{N}$, so every natural number n satisfies the equation

$$1 + 2 + 3 + \cdots + n = \frac{n(n + 1)}{2}.$$

□

We can simplify this technique to apply to the general statement in (1). Let's think carefully about what we really needed to prove in the above example. I will refer to the statement $1+2+\cdots+n = \frac{n(n+1)}{2}$ as $p(n)$ here. We specifically proved the following things:

- $1 \in S$, i.e., $p(1)$ is true.
- If $n \in S$, then we also have $n^+ \in S$, i.e., if $p(n)$ is true, then $p(n + 1)$ is also true.

You can sort of view this strategy as a domino effect. Given that $p(1)$ is true, the second statement allows us to conclude that $p(2)$ is true. Then we use the second statement again to conclude $p(3)$ is true, then $p(4)$, etc., etc. The first bullet point, $p(1)$, sets up the first domino, and the second bullet point ensures that each domino knocks down the next one.

Now, of course, there's no particular reason to start the domino chain at $n = 1$. We can also begin in any case we like, and sometimes (as we will see) this will be necessary, as we can have statements that do not apply to small values of n. But the principle here works just the same in those cases. This principle is known as the Principle of Weak Induction.

Theorem 1 (Principle of Weak Induction.)**.** *Let $p(n)$ be a proposition about n. Let $a \in \mathbb{N}$. Suppose that*

- *$p(a)$ is true, and*
- *for all $n \geq a$, $p(n)$ is true $\Rightarrow p(n + 1)$ is true.*

Then $p(n)$ is true for all $n \geq a$.

Proof. Suppose that $p(n)$ and a are as defined in the statement of the theorem. We consider two cases, according as whether $a = 1$ or $a > 1$.

Case 1: $a = 1$. Define S to be the set of all natural numbers n for which $p(n)$ is true. Note that the first item above yields that $a = 1 \in S$, and moreover, the second item yields that $n \in S \ \Rightarrow \ n + 1 \in S$. By the Inductive Axiom, then $S = \mathbb{N}$, and therefore $p(n)$ is true for all $n \geq 1$.

Case 1: $a > 1$. Define $q(n)$ to be the proposition $p(n + a - 1)$. Notice that $q(1) \equiv p(1 + a - 1) = p(a)$, and hence by the first assumption, $q(1)$ is true. Moreover, for any $n \geq 1$, we have

$$\begin{aligned} q(n) \text{ is true} &\equiv p(n + a - 1) \text{ is true} \\ &\Rightarrow p(n + a) \text{ is true} \\ &\equiv q(n + 1) \text{ is true,} \end{aligned}$$

where the implication follows from the second assumptions, and the logical equivalences follow from the definition of $q(n)$.

Therefore, $q(n)$ satisfies the conditions stated for the case that $a = 1$, and hence by applying Case 1 to $q(n)$, we obtain that $q(n)$ is true for all $n \geq 1$. Therefore, since $q(n) \equiv p(n + a - 1)$, we therefore have that $p(n)$ is true for all $n \geq a$. □

This simplifies the procedure we used in Example 1. We can now perform that procedure simply by verifying the two bullet points listed in the theorem. This procedure is called Mathematical Induction. In general, a proof using the Weak Induction Principle above will look as follows:

Mathematical Induction
To prove a statement of the form $\forall n \geq a,\ p(n)$ using mathematical induction, we do the following.

1. Prove that $p(a)$ is true. This is called the "Base Case."
2. Prove that $p(n) \Rightarrow p(n + 1)$ using any proof method. What is commonly done here is to use Direct Proof, so we assume $p(n)$ is true, and derive $p(n + 1)$. This is called the "Inductive Step."

The Base Case and Inductive Step are often labeled as such in a proof. The assumption that $p(n)$ is true, made in the inductive step, is often referred to as the Inductive Hypothesis.

Let's look at a few examples of proof by induction. In these examples, we will structure our proofs explicitly to label the base case, inductive hypothesis, and inductive step. This is common to do when first learning inductive proofs, and you can feel free to label your steps in this way as needed in your own proofs.

1.1 Weak Induction: examples

Example 2. Prove the following statement using mathematical induction:

For all $n \in \mathbb{N}$, $1 + 2 + 4 + \cdots + 2^n = 2^{n+1} - 1$.

Proof. We proceed using induction.

Base Case: $n = 1$. In this case, we have that $1 + \cdots + 2^n = 1 + 2 = 2^2 - 1$, and the statement is therefore true.

Inductive Hypothesis: Suppose that for some $n \in \mathbb{N}$, we have $1 + 2 + 4 + \cdots + 2^n = 2^{n+1} - 1$.

Inductive Step: Consider

$$\begin{aligned} 1+2+4+\cdots+2^{n+1} &= 1+2+4+\cdots+2^n+2^{n+1} \\ &= (2^{n+1}-1)+2^{n+1} \quad \text{(by the Inductive Hypothesis)} \\ &= 22^{n+1}-1 \\ &= 2^{(n+1)+1}-1. \end{aligned}$$

Therefore, we have that if the statement holds for n, it also holds for $n+1$.
By induction, then, the statement holds for all $n \in \mathbb{N}$. □

Note that in both Example 1 and Example 2, we use induction to prove something about summations. This is often a case where induction is useful, and hence we will here introduce formal summation notation so that we can simplify what we need to write.

Definition 1. Let $a_1, a_2, \ldots, a_n$ be real numbers. For $m \geq 1$, recursively define $\sum_{k=m}^{n} a_k$ as follows:

$$\text{if } n < m, \text{ then } \sum_{k=m}^{n} a_k = 0, \quad \text{otherwise } \sum_{k=m}^{n} a_k = \sum_{k=m}^{n-1} a_k + a_n.$$

A few comments on this definition. First, this is consistent with previous definitions you may have seen for summation notation. If $n \geq m$, the recursive definition will add up all the a_k having k between m and n (inclusive). In the case that $n < m$, though, we refer to this as an *empty sum*; that is, you are adding up no numbers at all. In that case, the default is 0; if you have added nothing, you are at nothing.

While we're at it, we can also use induction to state and prove theorems about products of a bunch of numbers, so let's define product notation as well.

Definition 2. Let $a_1, a_2, \ldots, a_n$ be real numbers. For $m \geq 1$, recursively define $\prod_{k=m}^{n} a_k$ as follows:

$$\text{if } n < m, \text{ then } \prod_{k=m}^{n} a_k = 1, \quad \text{otherwise } \prod_{k=m}^{n} a_k = \left(\prod_{k=m}^{n-1} a_k\right) a_n.$$

Again, this does what you expect it should. If $n \geq m$, the recursive definition will multiply all the a_k having k between m and n (inclusive). In the case that $n < m$, we have the *empty product*. In this case, however, instead of taking the empty product to be 0, we take it to be 1. There are a few reasons for this, but the clearest may be to consider what happens recursively. As you follow the recursive definition, peeling off and multiplying one number at a time, eventually you arrive at an empty product. So what should happen? If we define the empty product to be 0, then all the numbers you've already multiplied in just vanish away (sad!). So 0 doesn't really make sense. Another way to think about it is that when we add, 0 is the number that "does nothing" (aka it is the additive identity, so $x + 0 = x$ always), and when we multiply, 1 is the number that "does nothing" (aka it is the multiplicative identity, so $x1 = x$ always). Hence, we choose the do-nothing number as our empty sum/product, according to which operation we are using.

Let's take a look at another example of induction, using the summation notation we have just developed.

Example 3. Prove the following statement using mathematical induction:

Let $n \in \mathbb{N}$. Then $\displaystyle\sum_{k=1}^{n} k(k+1) = \frac{n(n+1)(n+2)}{3}$.

Proof. We proceed using induction.

Base Case: $n = 1$. In this case, we have $\displaystyle\sum_{k=1}^{n} k(k+1) = 1(2) = 2 = \frac{1(2)(3)}{3}$, so the result holds.

Inductive Hypothesis: Suppose, for some $n \in \mathbb{N}$, we have $\displaystyle\sum_{k=1}^{n} k(k+1) = \frac{n(n+1)(n+2)}{3}$.

Inductive Step: Consider the case of $n+1$. In this case, we have

$$\begin{aligned}
\sum_{k=1}^{n+1} k(k+1) &= \sum_{k=1}^{n} k(k+1) + (n+1)(n+2) \\
&= \frac{n(n+1)(n+2)}{3} + (n+1)(n+2) \quad \text{(by the Inductive Hypothesis)} \\
&= \frac{n(n+1)(n+2) + 3(n+1)(n+2)}{3} \\
&= \frac{(n+1)(n+2)(n+3)}{3} \quad \text{(by factoring out } (n+1)(n+2)\text{)}.
\end{aligned}$$

Therefore, we have that if the statement holds for n, it also holds for $n+1$.

Hence, by induction, $\displaystyle\sum_{k=1}^{n} k(k+1) = \frac{n(n+1)(n+2)}{3}$ for all $n \in \mathbb{N}$. □

In the following example, we consider a case where we do not wish to prove a statement for all $n \in \mathbb{N}$, but for all $n \geq a$, as in the original statement in Theorem 1.

Example 4. Prove the following statement using mathematical induction:

For all $n \geq 5$, $4n < 2^n$.

Proof. We proceed by induction.

Base Case: $n = 5$. Then $4n = 20 < 32 = 2^n$, and the result is true.

Inductive Hypothesis: Suppose, for some $n \geq 5$, that $4n < 2^n$.

Inductive Step: Consider $n+1$. We have

$$\begin{aligned}
4(n+1) &= 4n + 4 \\
&< 2^n + 4 \quad \text{(by the Inductive Hypothesis)} \\
&< 2^n + 2^n \quad \text{(since } 2^n > 4 \text{ for all } n \geq 5\text{)} \\
&= 2^{n+1}.
\end{aligned}$$

Therefore, if the result holds for n, it also holds for $n+1$.

Thus, by induction, we have that $4n < 2^n$ for all $n \geq 5$. □

In the following example, we outline an inductive proof in which the steps are not labeled, but instead

we use prose to guide the reader through the work.

Example 5. Prove the following statement using mathematical induction:

Let x be a positive real number. Then for any $n \in \mathbb{N}$, we have $(1+x)^n \geq 1 + nx$.

Proof. We work by induction on n. First, for the base case, consider $n = 1$. Then $(1+x)^n = 1 + x = 1 + nx$, and hence the result is true.

Now, suppose that the result is known for some $n \in \mathbb{N}$; that is, for some $n \in \mathbb{N}$ we have $(1+x)^n \geq 1 + nx$. Consider the case of $n+1$; in this case, we have

$$\begin{aligned}
(1+x)^{n+1} &= (1+x)(1+x)^n \\
&\geq (1+x)(1+nx) \quad \text{(by the inductive hypothesis)} \\
&= 1 + x + nx + nx^2 \\
&\geq 1 + x + nx \\
&= 1 + (n+1)x.
\end{aligned}$$

Hence, if the result holds in the case of n, it also holds in the case of $n+1$. Therefore, by induction, the result holds for all $n \in \mathbb{N}$. □

One thing to notice in all the previous proofs: if you consider the inductive hypothesis, it usually starts with a statement of the form "for some $n \in \mathbb{N}$." This is important: when you are making the inductive hypothesis, you are working with a fixed value of n and considering the specific next step. You cannot at that point pile assumptions on n; it is frozen as a specific (though unknown) integer.

1.2 Proofs of Some Proofs

As promised in lecture, let's take a look at how we can verify some of our most important proof techniques using mathematical induction. We first consider a proof that our method of direct proof works. This is of critical importance, since we use a form of direct proof inside the structures for all of our proof methods.

Theorem 2 (Proof of Direct Proof)**.** *Let $k \geq 1$, and let $p, q, r_1, r_2, \ldots, r_k$ be propositions. Then*

$$p \Rightarrow q \equiv (p \Rightarrow r_1) \wedge (r_1 \Rightarrow r_2) \wedge \cdots \wedge (r_{k-1} \Rightarrow r_k) \wedge (r_k \Rightarrow q).$$

The reason we need induction to prove this theorem is that we do not know the specific value of k. So we will use induction to break up the right hand side of the logical equivalence into two pieces, the first k implications, and then the last. The first k implications can be considered by the inductive hypothesis and then conjoined with the last to establish the result.

Proof. We work by induction on k. Note that the case of $k = 1$ has been previously proven, in Theorem 1 of the Logic and Proof notes.

Now, suppose that for some $k \geq 1$, it is known that for any propositions $p, q, r_1, \ldots, r_k$, we have $p \Rightarrow q \equiv (p \Rightarrow r_1) \wedge (r_1 \Rightarrow r_2) \wedge \cdots \wedge (r_{k-1} \Rightarrow r_k) \wedge (r_k \Rightarrow q)$. Let us consider propositions $p, q, r_1, \ldots, r_k, r_{k+1}$. Then we have

$$\begin{aligned}
&(p \Rightarrow r_1) \wedge (r_1 \Rightarrow r_2) \wedge \cdots \wedge (r_k \Rightarrow r_{k+1}) \wedge (r_{k+1} \Rightarrow q) \\
&\qquad \equiv [(p \Rightarrow r_1) \wedge (r_1 \Rightarrow r_2) \wedge \cdots \wedge (r_k \Rightarrow r_{k+1})] \wedge (r_{k+1} \Rightarrow q) \\
&\qquad \equiv [p \Rightarrow r_{k+1}] \wedge (r_{k+1} \Rightarrow q) \quad \text{(by the inductive hypothesis)} \\
&\qquad \equiv p \Rightarrow q \quad \text{(by Theorem 1 in Logic and Proof notes, or by the base case).}
\end{aligned}$$

Hence, by induction, the result holds for all values of k. □

Following a similar strategy, which will be left as an exercise, we can prove the following theorem establishing the validity of proof by cases:

Theorem 3 (Proof of Proof by Cases)**.** *Let $k \geq 1$, and let $p, q, r_1, r_2, \ldots, r_k$ be propositions. If $p \equiv r_1 \vee r_2 \vee \cdots \vee r_k$, then*

$$p \Rightarrow q \equiv (r_1 \Rightarrow q) \wedge (r_2 \Rightarrow q) \wedge \cdots \wedge (r_k \Rightarrow q).$$

2 Strong Induction

Now, let's look at an example where our previous structure no longer applies.

Example 6. Given $n \in \mathbb{N}$, define a_n recursively as follows:

$$a_0 = 1, \quad a_1 = 3, \quad a_n = 2a_{n-1} - a_{n-2} \text{ for } n \geq 2.$$

Prove that for all $n \geq 0$, $a_n = 2n + 1$.

Notice what will happen in the above example if we try to work by our previous strategy. After the base case, and the inductive hypothesis, we will be left looking at a_{n+1}. In our previous inductive proofs, we would use information about a_n to tell us something about a_{n+1}. But that's not quite enough here; we need information about a_{n-1} also in order to work with a_{n+1}. So it's not enough just to know something about one previous value of n, we need more. Enter the Principle of Strong Induction to save the day.

Theorem 4 (Principle of Strong Induction)**.** *Let $p(n)$ be a proposition about n. Let $a \in \mathbb{N}$. Suppose that*

- *$p(a)$ is true, and*
- *for all $n \geq a$, if $p(k)$ is true for all $a \leq k \leq n$, then $p(n+1)$ is also true.*

Then $p(n)$ is true for all $n \geq a$.

Note the distinction here with the Weak Inductive Principle. In the inductive step, we do not simply assume that the proposition is true for one choice of n, but that it is true for all k preceding that n. If we think about this from the domino analogy, with Weak Induction we show that one domino knocks down the next. With strong induction we show that if all the previous dominoes have been knocked over, the next one will also fall.

Proof of Theorem 4. Suppose that $p(n)$, a are as defined in the statement of the theorem, and that the two bullet points about $p(n)$ are true. Define $q(n)$ to be the proposition that $p(k)$ is true for all $a \leq k \leq n$ (that is to say, $q(n) \equiv \bigwedge_{k=a}^{n} p(k)$). Notice that if $q(n)$ is true, that implies that $p(n)$ is true, so it is sufficient to show that $q(n)$ is true for all $n \geq a$. We prove this using the Principle of Weak Induction.

For the base case, we note that assumption, $p(a)$ is true, and hence $q(a)$ is true.

Now, assume for induction that $q(n)$ is true. Then $p(k)$ is true for all $a \leq k \leq n$, so by the second bullet point we have also that $p(n+1)$ is true. Therefore, $p(k)$ is true for all $a \leq k \leq n+1$, and hence $q(n+1)$ is also true.

By the Principle of Weak Induction, we therefore have that $q(n)$ is true for all $n \geq a$. But for any n, if $q(n)$ is true, that implies that $p(n)$ is true, so we therefore have that $p(n)$ is true for all $n \geq a$, as desired. □

Now, let us return to Example 6 to see some strong induction in action. Here, we will use two base cases, instead of 1, since the equation about a_n is only true when $n \geq 2$. Since we cannot apply that equation to the case of $n = 0$ or $n = 1$, we separate each of these cases out.

Example 6. Continued. Let's restate the problem to ensure we remember what we're doing: Given $n \in \mathbb{N}$, define a_n recursively as follows:

$$a_0 = 1, a_1 = 3, a_n = 2a_{n-1} - a_{n-2} \text{ for } n \geq 2.$$

Prove that for all $n \geq 0$, $a_n = 2n + 1$.

Proof. We work by strong induction on n.
For the base cases, first consider $n = 0$. We have that $a_0 = 1 = 2(0) + 1$, so the result is true when $n = 0$.
Next, consider $n = 1$. We have that $a_1 = 3 = 2(1) + 1$, so the result is true when $n = 1$.
For the strong inductive hypothesis, suppose that for some $n \geq 1$, we have that $a_k = 2k + 1$ for all $0 \leq k \leq n$. Consider a_{n+1}. We have

$$\begin{aligned} a_{n+1} &= 2a_n - a_{n-1} \qquad \text{(because } n + 1 \geq 2\text{)} \\ &= 2(2n + 1) - (2(n - 1) + 1) \qquad \text{(by the strong inductive hypothesis)} \\ &= 4n + 2 - 2n + 2 - 1 \\ &= 2n + 3 \\ &= 2(n + 1) + 1. \end{aligned}$$

Therefore, the result holds for $n + 1$ as well.
Hence, by the Principle of Strong Induction, we have $a_n = 2n + 1$ for all $n \geq 0$. □

In general, it is useful in the case of strong induction to think about how many base cases you might need. Strong induction is particularly helpful in cases where your n^{th} term is defined in terms of more than one previous term, or in cases where you may not know how many previous steps are required.

In addition to the circumstance in Example 6, there are many other cases where we might use strong induction. In particular, we can use strong induction when we know that we can reduce a problem to information about a smaller number, but we don't necessarily know which number might be involved. Consider the following example:

Example 7. Use strong induction to prove the following proposition:

> Every positive integer n can be written as a sum of distinct nonnegative integer powers of 2.

Here, we want to consider how to deal with an integer n by first stripping off one power of 2, and then using induction to write the new, smaller number as a sum of powers of 2. However, we don't know exactly what the new, smaller number will be. Hence, we can turn to strong induction to assume that we know the result for ALL preceding integers, so it doesn't really matter what the smaller number is.

Example 7. Continued.

Proof. We proceed by strong induction on n.

Base Case: $n = 1$. Then $n = 2^0$, and thus the result holds for $n = 1$.

Inductive Hypothesis. Suppose, for some $n \geq 1$ that for every $k \leq n$, we can write k as a sum

of distinct powers of 2.

Inductive Step. Consider $n+1$. Let ℓ be the largest integer such that $2^\ell \leq n+1$. Let $m = n+1-2^\ell$. Notice that since $2^\ell \geq 1$, we have that $m < n+1$. Then by the strong inductive hypothesis, there are distinct integers $r_1, r_2, \ldots, r_s$ such that we can write $m = 2^{r_1} + 2^{r_2} + \cdots + 2^{r_s}$. Note then that $n+1 = 2^\ell + 2^{r_1} + 2^{r_2} + \cdots + 2^{r_s}$, so we need only verify that $r_j \neq \ell$ for all j with $1 \leq j \leq s$. Suppose, for the sake of contradiction, that $r_j = \ell$ for some j. Then we have $m \geq 2^\ell$, and hence $n+1 = m + 2^\ell \geq 2^\ell + 2^\ell = 2^{\ell+1}$. But then ℓ is not the largest integer such that $2^\ell \leq n+1$, which is impossible due to our assumptions. Hence, $r_j \neq \ell$ for each j, and thus $n+1$ can be written as a sum of distinct nonnegative integer powers of 2.

By strong induction, then, the result holds for all $n \geq 1$. □

We close this section on strong induction with an example so wonderful that we're gonna call it a theorem.

Theorem 5 (Fundamental Theorem of Arithmetic.)**.** *Every positive integer can be written as a product of prime factors, and this product is unique up to reordering of the factors.*

Proof. We work by strong induction on positive integers. For the base case, consider the integer 1. This is the empty product of prime factors, and is clearly unique, as any product of prime factors other than the empty product is necessarily greater than 1.

For the strong inductive hypothesis, suppose that for some positive integer n, every positive integer $k \leq n$ can be uniquely (up to reordering) written as a product of prime factors.

Consider the integer $n+1$. If $n+1$ is itself a prime, then we are done, as it cannot be written as any composite of factors less than $n+1$, and hence its presentation as the product of $n+1$ with nothing else is unique.

If $n+1$ is not itself a prime, then since $n \geq 1$, $n+1$ must be composite. Let a, b be positive integers, with $a, b \neq 1$, such that $ab = n+1$. By the strong induction hypothesis, each of a, b can be written as a product of prime factors, say $a = p_1 p_2 \ldots p_t$ and $b = q_1 q_2 \ldots q_s$, where all of $p_1, p_2, \ldots, p_t, q_1, q_2, \ldots, q_s$ are themselves primes. Then $n+1 = p_1 p_2 \ldots p_t q_1 q_2 \ldots q_s$, a product of primes.

Relabel these factors so that we have $n+1 = p_1 p_2 \ldots p_r$, where all of $p_1, p_2, \ldots, p_r$ are primes. Suppose that we have a second factorization of $n+1$ into primes; we label these primes as $q_1, q_2, \ldots, q_v$, so we have $n+1 = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_v$.

We wish to show that these two factorizations are in fact the same (up to the order of the primes). We consider two cases, if $p_1 = q_1$ or $p_1 \neq q_1$.

Case 1: $p_1 = q_1$. Let $k = \frac{n+1}{p_1} = \frac{n+1}{q_1}$, and note that $k = p_2 p_3 \ldots p_r = q_2 q_3 \ldots q_v$. Moreover, $k < n+1$, and hence by the strong inductive hypothesis, k has a unique factorization into primes. Therefore, we must have that $p_2, p_3, \ldots, p_r$ and $q_2, q_3, \ldots, q_v$ are the same up to reordering of the factors.

Case 2: $p_1 \neq q_1$. Then one of p_1, q_1 is larger than the other; wolog suppose that $p_1 > q_1$. Consider $c = p_1 - q_1$. Note that $c < n+1$, and hence by the strong inductive hypothesis, c can be uniquely written as a product of primes, say $c = s_1 s_2 \ldots s_u$, where all of $s_1, \ldots, s_u$ are prime. We note that we cannot have q_1 as a factor of c, because if so, we would have that $p_1 = c + q_1$ is divisible by q_1, and therefore p_1 would not be prime, a contradiction. Hence, c is not divisible by q_1.

Define $m = cp_2 p_3 \ldots p_r = s_1 s_2 \ldots s_u p_2 p_3 \ldots p_r$. Notice that

$$m = (p_1 - q_1) p_2 p_3 \ldots p_r = n + 1 - q_1 p_2 p_3 \ldots p_r,$$

so $m < n+1$. Hence, by the strong inductive hypothesis, the writing of m as $s_1 s_2 \ldots s_u p_2 p_3 \ldots p_r$ is a unique (up to ordering) prime factorization of m. On the other hand, we have that

$$m = n + 1 - q_1 p_2 p_3 \ldots p_r = q_1 (q_2 q_3 \ldots q_v - p_2 p_3 \ldots p_r),$$

and hence q_1 is a prime factor of m. Since q_1 is not a factor of c, we cannot have q_1 as one of the s_i, and hence it must be the case that there is some j, with $2 \leq j \leq r$, with $p_j = q_1$.

As in the first case, then, let $k = \frac{n+1}{p_j} = \frac{n+1}{q_1}$. Note that the product of the remaining p_i with $i \neq j$ is a prime factorization of k, as is $q_2 \dots q_v$. Moreover, $k < n + 1$, and hence these factorizations must be the same, up to reordering.

Therefore, in either case, we have that the factors $p_1, p_2, \dots, p_r$ are the same as the factors $q_1, q_2, \dots, q_v$, up to reordering. Therefore, the prime factorization of $n + 1$ is unique up to reordering, as any two factorizations must be the same.

By strong induction, then, the result is true for any positive integer n. □