# Induction and Well-Ordering

Joseph R. Mileti

April 8, 2017

## 1 Mathematical Induction

Suppose that we want to prove that a certain statement is true for all natural numbers. In other words, we want to do the following:

- Prove that the statement is true for 0.
- Prove that the statement is true for 1.
- Prove that the statement is true for 2.
- Prove that the statement is true for 3.
- ....

Of course, since there are infinitely many natural numbers, going through each one in turn does not work because we will never handle them all this way. How can we get around this? Suppose that when we examine the first few proofs above that they look the same except that we replace 0 by 1 everywhere, or 0 by 2 everywhere, etc. In this case, one is tempted to say that "the pattern continues" or something similar, but that is not convincing because we can't be sure that the pattern does not break down when we reach 5419. One way to argue that the "the pattern continues" and handle all of the infinitely many possibilities at once is to take an arbitrary natural number $n$, and prove that the statement is true for $n$ using *only* the fact that $n$ is a natural number (but *not* any particular natural number).

This method of taking an arbitrary $n \in \mathbb{N}$ and proving that the statement is true for $n$ is the standard way of proving a statement involving a "for all" quantifier. This technique also works to prove that a statement is true for all real numbers or for all matrices, as long as we take an *arbitrary* such object. However, there is a different method one can use to prove that every natural number has a certain property, and this one does not carry over to other settings like the real numbers. The key fact is that the natural numbers start with 0 and proceed in discrete steps forward. With this in mind, consider what would happen if we could accomplish each of the following:

- Prove that the statement is true for 0.
- Prove that if the statement is true for 0, then the statement is true for 1.
- Prove that if the statement is true for 1, then the statement is true for 2.
- Prove that if the statement is true for 2, then the statement is true for 3.
- ....

Suppose that we are successful in proving each of these. From the first line, we then know that the statement is true for 0. Since we now know that it's true for 0, we can use the second line to conclude that the statement is true for 1. Since we now know that it's true for 1, we can use the second line to conclude that the statement is true for 2. And so on. In the end, we are able to conclude that the statement is true for all natural numbers.

Let's examine this situation more closely. On the fact of it, each line looks more complicated than the corresponding line for for a direct proof. However, the key fact is that from the second line onward, we now have an additional assumption! Thus, instead of proving that the statement is true for 3 without any help, we can now use the assumption that the statement is true for 2 in that argument. Extra assumptions are always welcome because we have more that we can use in the actual argument.

Of course, as in our discussion at the beginning of this section, we can't hope to prove each of these infinitely many things one at a time. In an ideal world, the arguments from the second line onward all look exactly the same with the exception of replacing the number involved. Thus, the idea is to prove the following:

- Prove that the statement is true for 0.
- Prove that if the statement is true for $n$, then the statement is true for $n + 1$.

Notice that for the second line, we would need to prove that it is true for an arbitrary $n \in \mathbb{N}$, just like we would have to in a direct argument. An argument using these method is called a proof by (mathematical) *induction*, and it is an extremely useful and common technique in mathematics. We can also state this approach formally in terms of sets, allowing us to bypass the vague notion of "statement" that we employed above.

**Fact 1.1** (Principle of Mathematical Induction on $\mathbb{N}$)**.** *Let $X \subseteq \mathbb{N}$. Suppose that the following are true:*

- $0 \in X$ *(the* base case*).*
- $n + 1 \in X$ *whenever* $n \in X$ *(the* inductive step*).*

*We then have that $X = \mathbb{N}$.*

Once again, here's the intuitive argument for why induction is valid. By the first assumption, we know that $0 \in X$. Since $0 \in X$, the second assumption tells us that $1 \in X$. Since $1 \in X$, the second assumption again tells us that $2 \in X$. By repeatedly applying the second assumption in this manner, each element of $\mathbb{N}$ is eventually determined to be in $X$. Notice that a similar argument works if we start with a different base case, i.e. if we start by proving that $3 \in X$ and then prove the inductive step, then it follows that $n \in X$ for all $n \in \mathbb{N}$ with $n \geq 3$.

Although we have stated induction with a base case of 0, it is also possible to give an inductive proof that starts at a different natural. For example, if we prove a base case the $4 \in X$, and we prove the usual inductive step that $n + 1 \in X$ whenever $n \in X$, then we can conclude that $n \in X$ for all $n \in \mathbb{N}$ with $n \geq 4$, i.e. that $\{n \in \mathbb{N} : n \geq 4\} \subseteq X$.

We now give many examples of proofs by induction. For our first example, we establish a formula for the sum of the first $n$ positive natural numbers.

**Proposition 1.2.** *For any $n \in \mathbb{N}^+$, we have*

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2},$$

*i.e.*

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

We give two proofs. The first is a clever argument that avoids induction, while the second is a typical application of induction.

*Proof 1.* We first give a proof with induction. Let $n \in \mathbb{N}^+$ be arbitrary. Let $S = 1 + 2 + \cdots + (n-1) + n$. We also have $S = n + (n-1) + \cdots + 2 + 1$. Adding both of these we conclude that

$$2S = (n+1) + (n+1) + \cdots + (n+1) + (n+1)$$

and hence

$$2S = n(n+1).$$

Dividing both sides by 2, we conclude that

$$S = \frac{n(n+1)}{2}$$

so $1 + 2 + \cdots + (n-1) + n = \frac{n(n+1)}{2}$. Since $n \in \mathbb{N}^+$ was arbitrary, the result follows. □

*Proof 2.* We now give a proof using induction. Since we are proving something about all elements of $\mathbb{N}^+$, we start with a base case of 1.

- *Base Case:* For $n = 1$, the sum on the left-hand side is 1, and the right-hand side is $\frac{1 \cdot 2}{2} = 1$. Thus, that statement is true when $n = 1$.
- *Inductive Step:* Assume that the statement is true for some fixed $n \in \mathbb{N}^+$, i.e. suppose that $n$ is a number for which we know that

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

  We then have

  $$\begin{aligned} 1 + 2 + \cdots + n + (n+1) &= \frac{n(n+1)}{2} + (n+1) && \text{(by the inductive hypothesis)} \\ &= \frac{n^2 + n + 2n + 2}{2} \\ &= \frac{n^2 + 3n + 2}{2} \\ &= \frac{(n+1)(n+2)}{2} \\ &= \frac{(n+1)((n+1)+1)}{2}. \end{aligned}$$

  Thus, the statement is true for $n + 1$.

By induction, we conclude that

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

for all $n \in \mathbb{N}^+$. □

In the previous proof, we could have written it using the set-theoretic form of induction by letting

$$X = \left\{ n \in \mathbb{N}^+ : \sum_{k=1}^{n} i = \frac{n(n+1)}{2} \right\},$$

and then used the principle of induction to argue that $X = \mathbb{N}^+$. Typically, we will avoid formally writing the set, and working in this way, but it is always possible to translate arguments into the corresponding set-theoretic approach.

**Proposition 1.3.** *For any $n \in \mathbb{N}^+$, we have*

$$\sum_{k=1}^{n}(2k-1) = n^2,$$

*i.e.*

$$1 + 3 + 5 + 7 + \cdots + (2n-1) = n^2.$$

*Proof.* We give a proof by induction.

- *Base Case:* Suppose that $n = 1$. We have

  $$\sum_{k=1}^{1}(2k-1) = 2 \cdot 1 - 1 = 1,$$

  so the left hand-side is 1. The right-hand side is $1^2 = 1$. Thus, the statement is true when $n = 1$.

- *Inductive Step:* Assume that the statement is true for some fixed $n \in \mathbb{N}^+$, i.e. suppose that $n$ is a number for which we know that

  $$\sum_{k=1}^{n}(2k-1) = n^2.$$

  Notice that $2(n+1) - 1 = 2n + 2 - 1 = 2n + 1$, hence

  $$\begin{aligned}
  \sum_{k=1}^{n+1}(2k-1) &= [\sum_{k=1}^{n}(2k-1)] + [2(n+1) - 1] \\
  &= [\sum_{k=1}^{n}(2k-1)] + (2n+1) \\
  &= n^2 + (2n+1) && \text{(by induction)} \\
  &= (n+1)^2.
  \end{aligned}$$

  Thus, the statement is true for $n + 1$.

By induction, we conclude that

$$\sum_{k=1}^{n}(2k-1) = n^2$$

for all $n \in \mathbb{N}^+$. □

Although induction is a useful tool for proving certain equalities, it can also be used in much more flexible ways. We now give several examples of proving divisibility and inequalities by induction.

**Proposition 1.4.** *For all $n \in \mathbb{N}$, we have $3 \mid (4^n - 1)$.*

*Proof.* We give a proof by induction.

- *Base Case:* Suppose that $n = 0$. We have $4^0 - 1 = 1 - 1 = 0$, hence $3 \mid (4^0 - 1)$ because $3 \cdot 0 = 0$. Thus, the statement is true when $n = 0$.

- *Inductive Step:* Assume that the statement is true for some fixed $n \in \mathbb{N}^+$, i.e. suppose that $n$ is a number for which we know that $3 \mid (4^n - 1)$. Fix $k \in \mathbb{Z}$ with $3k = 4^n - 1$. We then have

$$\begin{aligned} 4^{n+1} - 1 &= 4 \cdot 4^n - 1 \\ &= 4 \cdot (3k + 1) - 1 \\ &= 12k - 3 \\ &= 3 \cdot (4k - 1). \end{aligned}$$

  Since $4k - 1 \in \mathbb{Z}$, we conclude that $3 \mid (4^{n+1} - 1)$. Thus, the statement is true for $n + 1$.

By induction, we conclude that $3 \mid (4^n - 1)$ for all $n \in \mathbb{N}$. □

**Proposition 1.5.** *We have $2n + 1 < n^2$ for all $n \in \mathbb{N}$ with $n \geq 3$.*

*Proof.* We give a proof by induction.

- *Base Case:* Suppose that $n = 3$. We have $2 \cdot 3 + 1 = 7$ and $3^2 = 9$, so $2 \cdot 3 + 1 < 3^2$. Thus, the statement is true when $n = 3$.
- *Inductive Step:* Assume that the statement is true for some fixed $n \in \mathbb{N}$ with $n \geq 3$, i.e. suppose that $n \geq 3$ is a number for which we know that $2n + 1 < n^2$. Since $2n + 1 \geq 2 \cdot 3 + 1 = 7 > 2$, we then have

$$\begin{aligned} 2(n + 1) + 1 &= 2n + 3 \\ &= (2n + 1) + 2 \\ &< n^2 + 2 \\ &< n^2 + 2n + 1 \\ &= (n + 1)^2. \end{aligned}$$

  Thus, the statement is true for $n + 1$.

By induction, we conclude that $2n + 1 < n^2$ for all $n \in \mathbb{N}$ with $n \geq 3$. □

**Proposition 1.6.** *We have $n^2 < 2^n$ for all $n \geq 5$.*

*Proof.* We give a proof by induction.

- *Base Case:* Suppose that $n = 5$. We have $5^2 = 25$ and $2^5 = 32$, so $5^2 < 2^5$. Thus, the statement is true when $n = 5$.
- *Inductive Step:* Assume that the statement is true for some fixed $n \in \mathbb{N}$ with $n \geq 5$, i.e. suppose that $n \geq 5$ is a number for which we know that $n^2 < 2^n$. Since $n^2 = n \cdot n \geq 3n = 2n + n > 2n + 1$, we have then have

$$\begin{aligned} (n + 1)^2 &= n^2 + 2n + 1 \\ &< n^2 + n^2 \\ &= 2n^2 \\ &< 2 \cdot 2^n \\ &= 2^{n+1}. \end{aligned}$$

  Thus, the statement is true for $n + 1$.

By induction, we conclude that $n^2 < 2^n$ for all $n \geq 5$. □

**Proposition 1.7.** *For all $x \in \mathbb{R}$ with $x \geq -1$ and all $n \in \mathbb{N}^+$, we have $(1+x)^n \geq 1 + nx$.*

On the face of it, this problem looks a little different because we are also quantifying over infinitely many real numbers $x$. Since $x$ is coming from $\mathbb{R}$, we can't induct on $x$. However, we *can* take an arbitrary $x \in \mathbb{R}$ with $x \geq -1$, and then induct on $n$ for this particular $x$. We now carry out that argument.

*Proof.* Let $x \in \mathbb{R}$ be arbitrary with $x \geq -1$. For this $x$, we show that $(1+x)^n \geq 1 + nx$ for all $n \in \mathbb{N}^+$ by induction.

- *Base Case:* Suppose that $n = 1$. We then have that $(1+x)^1 = 1 + x = 1 + 1x$, so certainly $(1+x)^1 \geq 1 + 1x$.
- *Inductive Step:* Assume that the statement is true for some fixed $n \in \mathbb{N}^+$, i.e. suppose that $n$ is a number for which we know that $(1+x)^n \geq 1 + nx$. Since $x \geq -1$, we have $1 + x \geq 0$, so we can multiply both sides of this inequality by $(1+x)$ to conclude that

$$(1+x)^n \cdot (1+x) \geq (1+nx) \cdot (1+x).$$

We then have

$$\begin{aligned}
(1+x)^{n+1} &= (1+x)^n \cdot (1+x) \\
&\geq (1+nx) \cdot (1+x) && \text{(from above)} \\
&= 1 + nx + x + nx^2 \\
&= 1 + (n+1)x + nx^2 \\
&\geq 1 + (n+1)x. && \text{(since } nx^2 \geq 0\text{)}
\end{aligned}$$

Hence, we have shown that $(1+x)^{n+1} \geq 1 + (n+1)x$, i.e. that the statement is true for $n+1$.

By induction, we conclude that $(1+x)^n \geq 1 + nx$ for all $n \in \mathbb{N}^+$. Since $x \in \mathbb{R}$ with $x \geq -1$ was arbitrary, the result follows. □

# 2 Strong Induction and Well-Ordering

Remember our original model for induction:

- Prove that the statement is true for 0.
- Prove that if the statement is true for 0, then the statement is true for 1.
- Prove that if the statement is true for 1, then the statement is true for 2.
- Prove that if the statement is true for 2, then the statement is true for 3.
- Prove that if the statement is true for 3, then the statement is true for 4.
- ....

In the previous section, we argued why this model was sound and gave many examples. However, upon closer inspection, it appears that we can assume more. In the second line, when proving that the statement is true for 1 we are allowed to assume that the statement is true for 0. Now in the third line, when proving that the statement is true for 2, we only assume that it is true for 1. If we are knocking down the natural numbers in order, then we've already proved that it's true for 0, so why can't we assume that as well? The answer is that we can indeed assume it! In general, when working to prove that the statement is true for a natural number $n$, we can assume that the statement is true for all smaller natural numbers. In other words, we do the following:

- Prove that the statement is true for 0.
- Prove that if the statement is true for 0, then the statement is true for 1.
- Prove that if the statement is true for 0 and 1, then the statement is true for 2.
- Prove that if the statement is true for 0, 1, and 2, then the statement is true for 3.
- Prove that if the statement is true for 0, 1, 2, and 3, then the statement is true for 4.
- ....

Suppose that we are successful in doing this. From the first line, we then know that the statement is true for 0. Since we now know that it's true for 0, we can use the second line to conclude that the statement is true for 1. Since we now know that it's true for both 0 and 1, we can use the second line to conclude that the statement is true for 2. And so on. In the end, we are able to conclude that the statement is true for all natural numbers.

As usual, we can't hope to prove each of these infinitely many things one at a time. In an ideal world, the arguments from the second line onward all look exactly the same with the exception of replacing the number involved. Thus, the idea is to prove the following.

- Prove that the statement is true for 0.
- Prove that if the statement is true for each of $0, 1, 2, \ldots, n$, then the statement is true for $n + 1$.

Alternatively, we can state this as follows:

- Prove that the statement is true for 0.
- Prove that if the statement is true for each of $0, 1, 2, \ldots, n - 1$, then the statement is true for $n$ (for $n \geq 1$).

An argument using these method is called a proof by *strong induction*. As we will see in the examples below, sometimes we need to modify this simple structure to include several base cases in order to get the argument going. Rather than going through a theoretical discussion of how and why one would do this, it's easier to illustrate the technique by example.

We start with an example where we verify a simple closed formed formula for a recursively defined sequence. Since the sequence uses the past two values to define the current value, regular induction does not give enough power to complete the proof.

**Proposition 2.1.** *Define a sequence $a_n$ recursively by letting $a_0 = 0$, $a_1 = 1$, and*

$$a_n = 3a_{n-1} - 2a_{n-2}$$

*for $n \geq 2$. Show that $a_n = 2^n - 1$ for all $n \in \mathbb{N}$.*

*Proof.* We prove that $a_n = 2^n - 1$ for all $n \in \mathbb{N}$ by strong induction.

- *Base Case:* We handle two bases where $n = 0$ and $n = 1$ because our inductive step will use the result for two steps back. When $n = 0$, we have $a_0 = 0$ and $2^0 - 1 = 1 - 1 = 0$, so $a_0 = 2^0 - 1$. When $n = 1$, we have $a_1 = 1$ and $2^1 - 1 = 2 - 1 = 1$, so $a_1 = 2^1 - 1$.
- *Inductive Step:* Let $n \geq 2$ and assume that the statement is true for $0, 1, 2, \ldots, n - 1$, i.e. assume that $a_m = 2^m - 1$ for all $m \in \{0, 1, 2, \ldots, n - 1\}$. We prove that the statement is true for $n$. Notice that

since $n \geq 2$, we have $0 \leq n-1 < n$ and $0 \leq n-2 < n$, so we know that $a_{n-1} = 2^{n-1} - 1$ and $a_{n-2} = 2^{n-2} - 1$. Now

$$\begin{aligned} a_n &= 3a_{n-1} - 2a_{n-1} && \text{(by definition since } n \geq 2) \\ &= 3 \cdot (2^{n-1} - 1) - 2 \cdot (2^{n-2} - 1) && \text{(by the inductive hypothesis)} \\ &= 3 \cdot 2^{n-1} - 3 - 2 \cdot 2^{n-2} + 2 \\ &= 3 \cdot 2^{n-1} - 2^{n-1} - 1 \\ &= (3-1) \cdot 2^{n-1} - 1 \\ &= 2 \cdot 2^{n-1} - 1 \\ &= 2^n - 1. \end{aligned}$$

Thus, $a_n = 2^n - 1$ and so the statement is true for $n$.

Using strong induction, we conclude that $a_n = 2^n - 1$ for all $n \in \mathbb{N}$. □

We now turn to an interesting example of using strong induction to establish when we can solve an equation in the natural numbers.

**Proposition 2.2.** *If $n \in \mathbb{N}$ and $n \geq 12$, then there exist $k, \ell \in \mathbb{N}$ with $n = 3k + 7\ell$.*

*Proof.* We give a proof by strong induction.

- *Base Case:* We first prove that the statement is true for all $n \in \{12, 13, 14\}$ (we will see why we need so many base cases in the inductive step below). We have the following cases:
  - $12 = 3 \cdot 4 + 7 \cdot 0$.
  - $13 = 3 \cdot 2 + 7 \cdot 1$.
  - $14 = 3 \cdot 0 + 7 \cdot 2$.

  Thus, the statement is true for all $n \in \{12, 13, 14\}$.

- *Inductive Step:* Let $n \geq 15$ and assume that the statement is true for all $k \in \mathbb{N}$ with $12 \leq k < n$, i.e. assume that the statement is true for $12, 13, 14, \ldots, n-1$. We prove that the statement is true for $n$. Since $n \geq 15$, we have $12 \leq n - 3 < n$, so we can use the inductive hypothesis to fix $k, \ell \in \mathbb{N}$ with

  $$n - 3 = 3k + 7\ell.$$

  Adding 3 to both sides, we see that

  $$\begin{aligned} n &= 3k + 7\ell + 3 \\ &= 3(k+1) + 5\ell. \end{aligned}$$

  Since $k + 1, \ell \in \mathbb{N}$, we conclude that the statement is true for $n$.

By strong induction, we conclude that for all $n \in \mathbb{N}$ with $n \geq 12$, there exist $k, \ell \in \mathbb{N}$ with $n = 3k + 7\ell$. □

We can also use strong induction to establish bounds for recursively defined sequences.

**Proposition 2.3.** *Define a sequence recursively by letting $f_0 = 0$, $f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$ for all $n \geq 2$. We have*

$$f_n \leq 2^n$$

*for all $n \in \mathbb{N}$.*

*Proof.* We prove the result by strong induction.

- *Base Case:* We first handle the cases when $n = 0$ and $n = 1$.
  - Notice that $2^0 = 1 > 0$, so $f_0 \leq 2^0$.
  - Notice that $2^1 = 2 > 1$, so $f_1 \leq 2^1$.

  Thus, the statement is true for $n = 0$ and $n = 1$.

- *Inductive Step:* Suppose that $n \geq 2$ and the statement is true for all $k \in \mathbb{N}$ with $k < n$. In particular, we have $0 \leq n-2 < n$ and $0 \leq n-1 < n$, so the statement is true for both $n-2$ and $n-1$, and hence $f_{n-2} \leq 2^{n-2}$ and $f_{n-1} \leq 2^{n-1}$. We then have

$$\begin{aligned} f_n &= f_{n-1} + f_{n-2} && \text{(since } n \geq 2\text{)} \\ &\leq 2^{n-1} + 2^{n-2} && \text{(from above)} \\ &\leq 2^{n-1} + 2^{n-1} \\ &= 2 \cdot 2^{n-1} \\ &= 2^n. \end{aligned}$$

  Therefore, $f_n \leq 2^n$, i.e. the statement is true for $n$.

By strong induction, we conclude that $f_n \leq 2^n$ for all $n \in \mathbb{N}$. □

Once we have such a proof, it is natural to ask how it could be improved. A nearly identical argument shows that $f_n \leq 2^{n-1}$ for all $n \in \mathbb{N}$. However, if we try to show that $f_n \leq 2^{n-2}$ for all $n \in \mathbb{N}$, then the inductive step goes through without a problem, but the base case of $n = 1$ does not work. As a result, the argument fails.

Can we obtain a significantly better upper bound for $f_n$ than $2^{n-1}$? In particular, can we use an exponential whose base is less than 2? If we replace 2 with a number $\alpha > 1$, i.e. try to prove that $f_n \leq \alpha^n$ (or $f_n \leq \alpha^{n-1}$), then the base case goes through without a problem. In the inductive step, the key fact that we used was that $2^{n-1} + 2^{n-2} \leq 2^n$ for all $n \in \mathbb{N}$. If we replace 2 by and $\alpha > 1$ with the property that $\alpha^{n-1} + \alpha^{n-2} \leq \alpha^n$ for all $n \in \mathbb{N}$, then we can carry out the argument. Dividing through by $\alpha^{n-2}$, we want to find the smallest possible $\alpha > 1$ such that $\alpha + 1 \leq \alpha^2$, which is equivalent to $\alpha^2 - \alpha - 1 \geq 0$. Using the quadratic formula, the solutions to $x^2 - x - 1 = 0$ are

$$x = \frac{1 \pm \sqrt{5}}{2}.$$

Now $\frac{1+\sqrt{5}}{2} > 1$, so we now go back and check that we can use it in an inductive argument. In fact, we can use it as a lower bound too (due to the fact that we get *equality* at the necessary step), so long as we change the exponent slightly and start with $f_1$.

**Proposition 2.4.** *Define a sequence recursively by letting $f_0 = 0$, $f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$ for all $n \geq 2$. Let $\phi = \frac{1+\sqrt{5}}{2}$ and notice that $\phi^2 = \phi + 1$ (either from above, or by direct calculation). We have*

$$\phi^{n-2} \leq f_n \leq \phi^{n-1}$$

*for all $n \in \mathbb{N}^+$.*

*Proof.* We prove the result by strong induction.

- *Base Case:* We first handle the cases when $n = 1$ and $n = 2$. Notice that

$$\phi = \frac{1+\sqrt{5}}{2} > \frac{1+2}{2} = \frac{3}{2},$$

hence

$$\phi^{-1} < \frac{2}{3}.$$

We also have

$$\phi = \frac{1+\sqrt{5}}{2} < \frac{1+3}{2} = 2.$$

Since $f_1 = 1 = f_2$, we have

$$\phi^{-1} < f_1 = \phi^0$$

and

$$\phi^0 = f_2 < \phi^1.$$

Therefore, the statement is true for $n = 1$ and $n = 2$.

- *Inductive Step:* Suppose that $n \geq 3$ and the statement is true for all $k \in \mathbb{N}^+$ with $k < n$. In particular, we have $1 \leq n-2 < n$ and $1 \leq n-1 < n$, so the statement is true for both $n-2$ and $n-1$, and hence

$$\phi^{n-4} \leq f_{n-2} \leq \phi^{n-3} \qquad \text{and} \qquad \phi^{n-3} \leq f_{n-1} \leq \phi^{n-2}$$

We have

$$\begin{aligned} f_n &= f_{n-1} + f_{n-2} && \text{(since } n \geq 3\text{)} \\ &\geq \phi^{n-3} + \phi^{n-4} && \text{(from above)} \\ &= \phi^{n-4}(\phi + 1) \\ &= \phi^{n-4} \cdot \phi^2 \\ &= \phi^{n-2}, \end{aligned}$$

and also

$$\begin{aligned} f_n &= f_{n-1} + f_{n-2} && \text{(since } n \geq 3\text{)} \\ &\leq \phi^{n-2} + \phi^{n-3} && \text{(from above)} \\ &= \phi^{n-3}(\phi + 1) \\ &= \phi^{n-3} \cdot \phi^2 \\ &= \phi^{n-1}. \end{aligned}$$

Therefore, $\phi^{n-2} \leq f_n \leq \phi^{n-1}$, i.e. the statement is true for $n$.

By strong induction, we conclude that $\phi^{n-2} \leq f_n \leq \phi^{n-1}$ for all $n \in \mathbb{N}^+$. □

Closely related to strong induction, the following is a core fact about the ordering of the natural numbers:

**Fact 2.5** (Well-Ordering of $\mathbb{N}$)**.** *Every nonempty set $X \subseteq \mathbb{N}$ has a smallest element. That is, for all nonempty $X \subseteq \mathbb{N}$, there exists $m \in X$ such that $m \leq n$ for all $n \in X$.*

Why is this statement true? Suppose that $X \subseteq \mathbb{N}$ is nonempty. If $0 \in X$, then 0 is clearly the smallest element of $X$, and we are done. Suppose then that $0 \notin X$. If $1 \in X$, then 1 is the smallest element of $X$, and we are done. Suppose then that $1 \notin X$. If $2 \in X$, then 2 is the smallest element of $X$, and we are done. Continuing this process, we must eventually reach a point where we encounter an element $X$, because otherwise we would eventually argue that each fixed $n \in \mathbb{N}$ is not an element of $X$, which would then imply that $X = \emptyset$.

This argument, like the arguments for induction and strong induction, is intuitively reasonable and convincing. However, it is not particularly formal. It is possible to formally prove each of induction, strong induction, and well-ordering from any of the others, so in a certain precise sense the three statements are equivalent. If you're interested, think about how to prove well-ordering using induction (along with some of the other implications). However, since all three are intuitively very reasonable, and it's beyond the scope of the course to construct the natural numbers and articulate exactly what we are allowed to use in the proofs of these equivalences, we will omit the careful arguments.

Notice that the given statement is false if we consider subsets of $\mathbb{Z}$ or $\mathbb{R}$ (rather than subsets of $\mathbb{N}$). For example, $\mathbb{Z}$ is trivially a nonempty subset of $\mathbb{Z}$, but it does not have a smallest element. Even if we consider only subsets of the nonnegative reals $\{x \in \mathbb{R} : x \geq 0\}$, we can find nonempty subsets with no smallest element (for example, the open interval $(0, 1) = \{x \in \mathbb{R} : 0 < x < 1\}$ does not have a smallest element).

We can often write an inductive proof as a proof using well-ordering, by considering a smallest potential counterexample. For example, here is a proof of Proposition 2.2 (if $n \in \mathbb{N}$ and $n \geq 12$, then there exist $k, \ell \in \mathbb{N}$ with $n = 3k + 7\ell$) using a well-ordering argument.

*Proof of Proposition 2.2.* Consider the set

$$X = \{n \in \mathbb{N} : n \geq 12 \text{ and there does not exist } k, \ell \in \mathbb{N} \text{ with } n = 3k + 7\ell\}$$

of counterexamples to the given statement. It suffices to show that $X = \emptyset$. Suppose instead that $X \neq \emptyset$. By well-ordering, we can let $m$ be the smallest element of $X$. Notice that $m \notin \{12, 13, 14\}$ because we have the following:

- $12 = 3 \cdot 4 + 7 \cdot 0$.
- $13 = 3 \cdot 2 + 7 \cdot 1$.
- $14 = 3 \cdot 0 + 7 \cdot 2$.

Therefore, we must have $m \geq 15$, and hence $12 \leq m - 3 < 15$. Now $m$ is the smallest element of $X$, so we must have $m - 3 \notin X$, and hence we can fix $k, \ell \in \mathbb{N}$ with $m - 3 = 3k + 7\ell$. Adding 3 to both sides, we see that

$$\begin{aligned} m &= 3k + 7\ell + 3 \\ &= 3(k + 1) + 5\ell. \end{aligned}$$

Since $k + 1, \ell \in \mathbb{N}$, we conclude that $m \notin X$, which is a contradiction. Therefore, it must be the case that $X = \emptyset$, giving the result. □