Math 220 Fall 2021, Lecture 13: Mathematical induction

1. Mathematical induction (cont'd)

1.1. What is induction? (cont'd)

Recall the Principle of Mathematical Induction:

> **Principle of Mathematical Induction** (or, short, **Principle of Induction**):
>
> Let $P(n)$ be a predicate that depends on a variable n, which is supposed to be a nonnegative integer.
>
> Assume that you have proved $P(0)$.
>
> Assume further that you have proved
>
> $$\forall n \in \mathbb{N} : (P(n) \Longrightarrow P(n+1)).$$
>
> Then, you can deduce that
>
> $$\forall n \in \mathbb{N} : P(n).$$

Recall also the Fibonacci sequence $(f_0, f_1, f_2, \ldots)$, which is defined by $f_0 = 0$ and $f_1 = 1$ and $f_n = f_{n-1} + f_{n-2}$ for all $n \geq 2$. Here are its first few values:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f_n	0	1	1	2	3	5	8	13	21	34	55	89	144	233

.

We now shall finish the proof that we started at the end of last lecture:

Theorem 1.1.1 (addition theorem for Fibonacci numbers)**.** We have

$$f_{n+m+1} = f_n f_m + f_{n+1} f_{m+1} \qquad \text{for any } n, m \in \mathbb{N}.$$

Proof. Induct on n. In other words, we apply the Principle of Induction to the predicate

$$P(n) = \text{“}\forall m \in \mathbb{N} : f_{n+m+1} = f_n f_m + f_{n+1} f_{m+1}\text{”}.$$

Base case: We must show that the theorem holds for $n = 0$. In other words, we must show that

$$f_{0+m+1} = f_0 f_m + f_{0+1} f_{m+1} \qquad \text{for any } m \in \mathbb{N}.$$

But this follows by comparing

$$f_{0+m+1} = f_{m+1} \qquad \text{with}$$
$$\underbrace{f_0}_{=0} f_m + \underbrace{f_{0+1}}_{=f_1=1} f_{m+1} = 0 f_m + 1 f_{m+1} = f_{m+1}.$$

Induction step: Let $n \in \mathbb{N}$. We assume (as our induction hypothesis) that $P(n)$ holds, i.e., that

$$f_{n+m+1} = f_n f_m + f_{n+1} f_{m+1} \qquad \text{for any } m \in \mathbb{N}.$$

Let us rewrite this as

$$f_{n+q+1} = f_n f_q + f_{n+1} f_{q+1} \qquad \text{for any } q \in \mathbb{N}. \tag{1}$$

We need to show that $P(n+1)$ holds, i.e., that

$$f_{(n+1)+m+1} = f_{n+1} f_m + f_{(n+1)+1} f_{m+1} \qquad \text{for any } m \in \mathbb{N}.$$

For any $m \in \mathbb{N}$, we have

$$\begin{aligned}
f_{(n+1)+m+1} &= f_{n+m+2} = f_{n+(m+1)+1} \\
&= f_n f_{m+1} + f_{n+1} f_{(m+1)+1} \qquad \text{(by (1), applied to } q = m+1) \\
&= f_n f_{m+1} + f_{n+1} \underbrace{f_{m+2}}_{=f_{m+1}+f_m} = f_n f_{m+1} + f_{n+1}\left(f_{m+1} + f_m\right) \\
&= f_n f_{m+1} + f_{n+1} f_{m+1} + f_{n+1} f_m = \underbrace{\left(f_n + f_{n+1}\right)}_{\substack{=f_{n+2} \\ =f_{(n+1)+1}}} f_{m+1} + f_{n+1} f_m \\
&= f_{(n+1)+1} f_{m+1} + f_{n+1} f_m = f_{n+1} f_m + f_{(n+1)+1} f_{m+1},
\end{aligned}$$

and we are done – i.e., we have proved that $P(n+1)$ holds. So the theorem is proved. □

Note that the theorem we just proved had two $\forall$-quantified variables n and m. We chose to induct on n. We could just as well have inducted on m. We cannot, however, induct on both n and m at the same time (unless we nest two inductions into one another – which is called a "double induction").

Theorem 1.1.2. If $a, b \in \mathbb{N}$ satisfy $a \mid b$, then $f_a \mid f_b$.

Proof. We might try to induct on a. So we apply the Principle of Induction to the predicate

$$P(a) := \left(\forall b \in \mathbb{N} : (a \mid b) \Longrightarrow (f_a \mid f_b)\right).$$

Unfortunately, it is not clear how to do the induction step here. Indeed, $a \mid b$ has nothing to do with $a+1 \mid b$. So inducting on a does not work.

Inducting on b does not work either.

Fortunately, we can induct on variables that are not in the statement (as long as these variables are nonnegative integers). All we have to do is restate the claim. In our current case, we restate the claim as follows: We define $P(n)$ to be the statement

$$(\forall a \in \mathbb{N} : (f_a \mid f_{na})) \qquad \text{for each } n \in \mathbb{N}.$$

If we can prove this statement $P(n)$ for all $n \in \mathbb{N}$, then the theorem will follow, because $a \mid b$ entails that $b = na$ for some $n \in \mathbb{N}$.

Now, this statement $P(n)$ is susceptible to induction. Namely, we prove it by inducting on n.

Base case: We must prove $P(0)$. In other words, we must prove $\forall a \in \mathbb{N} : (f_a \mid f_0)$. But this is clear, since $f_0 = 0$ is divisible by every integer.

Induction step: Let $n \in \mathbb{N}$. Assume that $P(n)$ is true. We must prove $P(n+1)$.

We have assumed that $P(n)$ is true, i.e., that $\forall a \in \mathbb{N} : (f_a \mid f_{na})$.

We must prove that $P(n+1)$ is true, i.e., that $\forall a \in \mathbb{N} : \left(f_a \mid f_{(n+1)a}\right)$.

Let $a \in \mathbb{N}$ be arbitrary. By our assumption, we have $f_a \mid f_{na}$. Thus, $f_{na} = f_a c$ for some integer c.

We want to show that $f_a \mid f_{(n+1)a}$. In other words, we want to show that $f_{(n+1)a} = f_a d$ for some integer d.

We have

$$\begin{aligned} f_{(n+1)a} &= f_{na+a} = f_{na+(a-1)+1} = \underbrace{f_{na}}_{=f_a c} f_{a-1} + f_{na+1} f_a \\ &\qquad \left(\begin{array}{c} \text{by the addition formula } f_{x+y+1} = f_x f_y + f_{x+1} f_{y+1}\text{, which} \\ \text{holds for all } x, y \in \mathbb{N} \text{ by the previous theorem} \end{array} \right) \\ &= f_a c f_{a-1} + f_{na+1} f_a = f_a \left(c f_{a-1} + f_{na+1} \right). \end{aligned}$$

Thus, $f_{(n+1)a} = f_a d$ for some integer d (namely, for $d = c f_{a-1} + f_{na+1}$). Therefore, $f_a \mid f_{(n+1)a}$. We have thus proved $P(n+1)$. Hence, the theorem is proved.

Did you spot the little mistake? We have applied the addition formula $f_{x+y+1} = f_x f_y + f_{x+1} f_{y+1}$ to $x = na$ and $y = a-1$. However, $a - 1 \notin \mathbb{N}$ when $a = 0$. So we need to treat the case $a = 0$ separately. Fortunately, this case is trivial: In this case, $f_{na} = f_{n \cdot 0} = f_0 = 0$, which is divisible by every integer, including f_a.

So the correct proof of $P(n+1)$ would look as follows:

"Let $a \in \mathbb{N}$ be arbitrary. We are in one of the following two cases:

Case 1: We have $a = 0$.

Case 2: We have $a \neq 0$.

In Case 1, we have $a = 0$. Therefore, $f_{na} = f_{n \cdot 0} = f_0 = 0$ is divisible by f_a. Hence, $P(n+1)$ is proved.

In Case 2, we have $a \neq 0$. Therefore, $a \geq 1$ (since $a \in \mathbb{N}$). Hence, $a - 1 \in \mathbb{N}$. By our assumption, we have $f_a \mid f_{na}$. Thus, $f_{na} = f_a c$ for some integer c.

We want to show that $f_a \mid f_{(n+1)a}$. In other words, we want to show that $f_{(n+1)a} = f_a d$ for some integer d.

We have

$$f_{(n+1)a} = f_{na+a} = f_{na+(a-1)+1} = \underbrace{f_{na}}_{=f_a c} f_{a-1} + f_{na+1} f_a$$

$$\left(\begin{array}{c} \text{by the addition formula } f_{x+y+1} = f_x f_y + f_{x+1} f_{y+1} \text{ (which} \\ \text{holds for all } x, y \in \mathbb{N} \text{ by the previous theorem),} \\ \text{applied to } x = na \text{ and } y = a-1 \end{array} \right)$$

$$= f_a c f_{a-1} + f_{na+1} f_a = f_a \left(c f_{a-1} + f_{na+1} \right).$$

Thus, $f_{(n+1)a} = f_a d$ for some integer d (namely, for $d = c f_{a-1} + f_{na+1}$). Therefore, $f_a \mid f_{(n+1)a}$. We have thus proved $P(n+1)$.

So we have proved $P(n+1)$ in both Cases 1 and 2. Thus, $P(n+1)$ is always true."

This is awkward to write: We needed a case distinction only to dispatch of a case that is essentially obvious. There is a shorthand for such case distinctions. It is called "**WLOG**" (short for "**without loss of generality**"). The idea is that the case $a = 0$ is so trivial that you can essentially treat it as an afterthought. If you can prove the theorem for all $a \neq 0$, then you know that the theorem is true for all $a \in \mathbb{N}$. You can reflect this in your proof by saying "We assume WLOG that $a \neq 0$ (because in the case $a = 0$, we have $f_{na} = f_{n \cdot 0} = f_0 = 0$ which is divisible by f_a)". Formally speaking, this is saying that the case $a = 0$ is clear (by the explanation provided) and therefore you will be only working in the case $a \neq 0$ from here on. □

In general, the word "WLOG" is used to dispose of cases that either are trivial, or are straightforward adaptations of other cases. Here is an example of the latter:

Theorem 1.1.3. For any two reals x and y, we have $x^2 + y^2 \geq 2xy$.

Proof. We are in one of the following two cases:

Case 1: We have $x \geq y$.

Case 2: We have $x < y$.

In Case 1, we have $x \geq y$. Now,

$$\left(x^2 + y^2 \right) - 2xy = (x-y)^2 = \underbrace{(x-y)}_{\geq 0} \underbrace{(x-y)}_{\geq 0} \geq 0.$$

Case 2 reduces to Case 1 by swapping x and y. □

Instead of splitting this proof into two cases as we just did, we could just as well have said "WLOG assume that $x \geq y$ (since the case $x < y$ can be reduced to the case $x \geq y$ by swapping x and y)".

Here are some more induction proofs:

Theorem 1.1.4. For any $n \in \mathbb{N}$, we have $2^0 + 2^1 + 2^2 + \cdots + 2^{n-1} = 2^n - 1$.

Proof. We induct on n (i.e., we apply the Principle of Mathematical Induction using the variable n).

Base case: The theorem is true for $n = 0$, since the empty sum equals 0 (and since $2^0 - 1$ also equals 0).

Induction step: Let $n \in \mathbb{N}$. Assume that

$$2^0 + 2^1 + 2^2 + \cdots + 2^{n-1} = 2^n - 1.$$

We must prove that

$$2^0 + 2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 1.$$

We have

$$\begin{aligned} &2^0 + 2^1 + 2^2 + \cdots + 2^n \\ &= \underbrace{\left(2^0 + 2^1 + 2^2 + \cdots + 2^{n-1}\right)}_{\substack{=2^n-1 \\ \text{(by the induction hypothesis)}}} + 2^n \\ &= 2^n - 1 + 2^n = \underbrace{2^n + 2^n}_{=2\cdot 2^n = 2^{n+1}} - 1 = 2^{n+1} - 1, \end{aligned}$$

which is precisely what we need. So the induction is complete. □

More generally:

Theorem 1.1.5. Let x and y be any two numbers. Then, for any $n \in \mathbb{N}$, we have

$$(x-y)\left(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + x^2y^{n-3} + xy^{n-2} + y^{n-1}\right) = x^n - y^n.$$

The big sum in the parentheses is the sum of all products of the form $x^i y^j$ where i and j are nonnegative integers with $i + j = n - 1$.

For example, for $n = 2$, this says

$$(x-y)(x+y) = x^2 - y^2.$$

For $n = 3$, this says

$$(x-y)\left(x^2 + xy + y^2\right) = x^3 - y^3.$$

For $n = 4$, this says

$$(x-y)\left(x^3 + x^2y + xy^2 + y^3\right) = x^4 - y^4.$$