Math 8: Induction and the Binomial Theorem

Spring 2011; Helena McGahagan

Induction is a way of proving statements involving the words "for all $n \in \mathbb{N}$," or in general, "for all integers $n \geq k$." Think of some statement that depends on n. For example, consider the statement $P(n)$: "$3 \mid (1 + 2^{2n-1})$" Of course, each one of the statements $P(1)$, $P(2)$, $P(3)$, ... will be either true or false. If your goal is to prove they are all true, you might imagine starting by checking *finitely* many of them (e.g., $P(1)$: '$3 \mid 3$" is clearly true, and $P(2)$: "$3 \mid 9$" is clearly true.) No matter how many you check, though, this will never be a proof that *all* of the statements are true. (There are infinitely many of them; you'll never finish checking!) Induction is the simple observation that it is enough to prove an implication for all n – and this is often easier than just trying to prove $P(n)$ itself, because proving an if-then statement gives you a hypothesis to use!

If we show that $P(1)$ is true, and we show that the chain of implications $P(1) \Rightarrow P(2) \Rightarrow P(3) \Rightarrow ... \Rightarrow P(n) \Rightarrow P(n+1) \Rightarrow ...$ is true, then we have really proven that we can always start with knowing $P(1)$ and follow this chain until we find out that *any* $P(n)$ is true! You can imagine induction as a way to prove we can climb as high as we want to on a ladder. Rather than climbing all the way to the top, we simply say: "I can get on the first rung of the ladder" and "If I'm on a rung of the ladder, I know how to climb up to the next one." Then, if someone asks you if you can climb to any rung n, you can say yes and tell them the algorithm for doing it: "Get on the ladder, then climb to the next rung n times." Some people like to think of each statement as being a domino (rather than a rung of the ladder). If you want to use this analogy, think of each domino as being one of the statements $P(n)$ – so you're imagining an infinite chain of dominos. Knocking a domino over is equivalent to proving that the statement it represents is true. To prove the entire chain will fall down, you just need to point out that each domino will automatically push over the next one as it falls. All you need to do then is make sure you can knock over the first one.

Principle of Mathematical Induction Fix an integer $k \in \mathbb{Z}$. Let $P(n)$ be a statement for each $n \geq k$. If both of the following are true:

(a) $P(k)$ is true

(b) for all $n \geq k$, $P(n) \Rightarrow P(n+1)$,

then $P(n)$ is true for all integers $n \geq k$.

Proof: Even though this is a fairly intuitive principle, we can provide a proof (*based on the well-ordering property of the integers*). As you might expect, the proof is by contradiction. For simplicity, we will assume $k = 1$ in the proof (it would work for any k, though).

Notice that this theorem is an implication: We want to show that ((a) and (b)) $\Rightarrow$ ($P(n)$ is true for all $n \in \mathbb{N}$.) Assume that we know both (a) and (b) are true. For a contradiction, assume that there exists an integer $m \in \mathbb{N}$ such that $P(m)$ is false. Consider the set

$$S = \{n \in \mathbb{N} : P(n) \text{ is false}\}$$

S is a subset of the natural numbers; also, note that $m \in S$ so that S is nonempty. Then, consider m_1, the *smallest* natural number that is in S. Since by (a) we know that $P(1)$ is true, it must be that $m_1 \geq 2$; this guarantees that $m_1 - 1$ is a natural number. Since m_1 is the smallest element in S, $m_1 - 1 \notin S$, which means that $P(m_1 - 1)$ is true. But (b) tells us that $P(m_1 - 1) \Rightarrow P(m_1)$. Therefore, $P(m_1)$ is true, which means $m_1 \notin S$. This is a contradiction. Our assumption that such an m exists must have been wrong, and hence, $P(n)$ is true for every $n \in \mathbb{N}$. $\square$.

To prove a statement $P(n)$ is true for all $n \in \mathbb{N}$ by induction, we simply prove the statements (a) and (b) above. The outline of a proof by induction looks like this:

> Base case: Check that $P(k)$ is true.
>
> Inductive step: Fix any $n \geq k$. Assume $P(n)$ is true. ..... use this hypothesis and any other true facts or logic that you need ..... Conclude that $P(n+1)$ is true.

The base case shows that $P(k)$ is true, and the inductive step proves that "for all $n \geq k$, $P(n) \Rightarrow P(n+1)$." Once we have done both these steps, applying the Principle of Mathematical Induction allows us to conclude that $P(n)$ is true for every integer $n \geq k$. $\square$

DEFINITIONS

Base case: The step in a proof by induction in which we check that the statement is true a specific integer k. (In other words, the step in which we prove (a).)

Inductive step: The step in a proof by induction in which we prove that, for all $n \geq k$, $P(n) \Rightarrow P(n+1)$. (I.e., the step in which we prove (b).)

Inductive hypothesis: Within the inductive step, we assume $P(n)$. This assumption is called the inductive hypothesis.

Sigma notation: The notation $\sum_{k=1}^{n} a_k$ is short-hand for the sum of all the a_k's from $k = 1$ to n. That is, $\sum_{k=1}^{n} a_k = a_1 + a_2 + ... + a_{n-1} + a_n$. (Similarly, the **product notation** is $\prod_{k=1}^{n} a_k = a_1 \cdot a_2 \cdot ... \cdot a_{n-1} \cdot a_n$.)

Binomial coefficients: Let $n \in \mathbb{N}$. If $0 \leq r \leq n$, the binomial coefficient (often read "n choose r" is defined to be

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}.$$

Examples We used induction to prove each of the following examples in lecture.

1. Prove $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ for all $n \in \mathbb{N}$.
2. Fix a (real) number $p > -1$. Prove that $(1+p)^n \geq 1 + np$ for all $n \in \mathbb{N}$.
3. Fix $x, y \in \mathbb{Z}$. Prove that $x^{2n-1} + y^{2n-1}$ is divisible by $x + y$ for all $n \in \mathbb{N}$.
4. Prove that $10^n < n!$ for all $n \geq 25$.
5. We can partition any given square into n sub-squares for all $n \geq 6$.

The first four are fairly simple proofs by induction. The last required realizing that we could easily prove that $P(n) \Rightarrow P(n+3)$. We could prove the statement by doing three separate inductions, or we could use the Principle of *Strong* Induction.

Principle of Strong Induction Let k be an integer and let $P(n)$ be a statement for each integer $n \geq k$. If we know

(a) $P(k)$ is true.

(b) For all $n \geq k$, $(P(k)$ and $P(k+1)$ and ... and $P(n-1)$ and $P(n)) \Rightarrow P(n+1)$.

Then, $P(n)$ is true for all integers $n \geq k$.

What changes here is the inductive step: We get to assume *more* in our in our inductive hypothesis, and still need to conclude that $P(n+1)$ is true. Convince yourself that the logic of strong induction is still sound! We are still showing you can get to the next rung of the ladder once you know that you can climb the first n rungs. (We even wrote down a proof of strong induction in class! You can prove it by using regular induction on the compound statement $Q(n)$: "$P(k)$ and $P(k+1)$ ... and $P(n)$.")

Then, our proof for the squares can simply start out by checking *three* base cases ($n = 6$, $n = 7$ and $n = 8$), and then saying, for the inductive step, that if we assume $P(6), P(7), P(8), ...,$ and $P(n)$, we know $P(n-2)$ is true, so we can start by partitioning the square into $n-2$ sub-squares. Then, partitioning one of those sub-squares into four, we have shown that we can partition the original square into $n+1$ sub-squares. This proves that $(P(6), P(7), P(8), ...,$ and $P(n)) \Rightarrow P(n+1)$ is true for all $n \geq 8$. Therefore, by strong induction, we can always partition a square into n sub-squares for any $n \geq 6$. (Also see problem IV on homework 6 for an example of a proof using strong induction.)

We also proved that the *Tower of Hanoi*, the game of moving a tower of n discs from one of three pegs to another one, is always winnable in $2^n - 1$ moves. Our last proof by induction in class was the *binomial theorem*.

Binomial Theorem Fix any (real) numbers a, b. For any $n \in \mathbb{N}$,

$$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^{n-r} b^r$$

Once you show the lemma that for $1 \leq r \leq n$, $\binom{n}{r-1} + \binom{n}{r} = \binom{n+1}{r}$ (see your homework, Chapter 16, #4), the induction step of the proof becomes a simple computation. This lemma also gives us the idea of Pascal's triangle, the n^{th} row of which lists the binomial coefficients you see in this sum. The triangle is very easy to write down because you can simply add two from the previous row to find out each number in the next row: See *All You Ever Wanted to Know About Pascal's Triangle and More* (http://ptri1.tripod.com/) for lots of details!

We can also use the binomial theorem directly to show simple formulas (that at first glance look like they would require an induction to prove): for example, $2^n = (1+1)^n = \sum_{r=0}^{n} \binom{n}{r}$. Proving this by induction would work, but you would really be repeating the same induction proof that you already did to prove the binomial theorem!