Step by Step

Definition 4.1. ***Mathematical induction*** *is the process of proving a statement of the form* $\forall n \in \mathbb{N}, F(n)$.

Note 4.2. *This is a lie. It will be corrected within this 300 course, but not immediately.*

The idea is this. I want to prove that a statement is true for all natural numbers. The first thing I will do is prove the base case; for now, I will say that I am simply going to prove $F(1)$ is true. The second thing I will do, is show that for any natural n, if $F(n)$ is true, then $F(n+1)$ must also be true.

It helps to think of it like a line of dominoes. Imagine that I have an infinite chain of dominoes, and I knock the first one over. Knocking the first one over is like proving $F(1)$. Then, the resulting chain reaction is the result of proving $\forall n \in \mathbb{N}, F(n) \Rightarrow F(n+1)$. Each domino will knock over the next one, and therefore at some point all dominoes will have been knocked over.

The basic template is as follows.

Step 1: Prove $F(1)$, $F(2)$, $\ldots$, $F(k)$, for some k, by hand.

Step 2: Pick some natural $n \geq k$, and assume $F(n)$ is true. Then prove that $F(n+1)$ is true.

Congrats - You now have pretty much all the standard proof techniques under your belt! The only thing we will in the rest of the course is expand on induction until you have the full definition, and of course, do many, many more proofs.

Example: Prove that for any natural n, there is a set $S \subseteq \mathbb{N}$ where $|S| = n$.

Obviously, $\forall n \in \mathbb{N}$, we could just pick $S = [n]$. But to show you how the template works, we will use induction.

Step 1: I will pick $k = 1$. $F(1)$ is true, because if I pick $S = \{1\}$, $|S| = 1$. So $F(1)$ is true.

Step 2: Let $n \geq k = 1$. Assume that $F(n)$ is true. Therefore, there is a set S with size n. Let m be the largest natural number contained by S. Then, I will pick $S' = S \cup \{m+1\}$. Since $m+1$ is bigger than any element in S, I know that $|S'| = |S| + 1$. Therefore, $|S'| = n + 1$, so there is a set of size $n+1$, which is also a subset of $\mathbb{N}$. This means that $F(n+1)$ is true, so I am done.

Example: Prove that $\forall n \in \mathbb{N}$, $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ `(\sum _{i = 1} ^n i = \frac{n(n+1)}{2})`.

Step 0: Define $F(n) := \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Step 1: Pick $k = 1$. Prove $F(1)$. $1 = 1 \cdot 2/2$.

Step 2: Pick $n \geq 1$. Assume $F(n)$, in other words, that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. Then,

$$\sum_{i=1}^{n+1} i = n + 1 + \sum_{i=1}^{n} i = n + 1 + \frac{n(n+1)}{2} = \frac{2n + 2 + n(n+1)}{2} = \frac{(n+1)(n+2)}{2}.$$

Proposition 4.3. $\gcd(a, b) = \gcd(b - a, b)$.

Proof. Claim: A number is a divisor of a and b iff it is a divisor of $b - a$ and b.

($\Rightarrow$) Suppose that g is a divisor of a and b. Then there are integers k and k' such that $gk = a$ and $gk' = b$. Then, $g(k' - k) = gk' - gk = b - a$, so g divides $b - a$. We already assumed that g is a divisor of b, so this direction is done.

($\Leftarrow$) Suppose that g is a divisor of $b - a$ and b. Then there are integers k and k' such that $gk = b - a$ and $gk' = b$. Then, $g(k' - k) = gk' - gk = b - (b - a) = a$, so g divides a. We already assumed that g is a

divisor of b, so this direction is done.

Now using this claim, we find that the set of all divisors of a and b, is exactly equal to the set of divisors of $b-a$ and b. Therefore the greatest divisor of a and b must be the same as the greatest divisor of $b-a$ and b. So $\gcd(a,b) = \gcd(b-a,b)$. □

Definition 4.4. *The **Fibonacci** sequence is defined as follows: $f_1 = 0$, $f_2 = 1$, and for every $n \geq 3$, $f_n = f_{n-1} + f_{n-2}$.*

Example: Prove that for every natural n, f_n and f_{n+1} are coprime.

Proof. **Stage 0:** Define $F(n) := \gcd(f_n, f_{n+1}) = 1$

Stage 1: Pick $k = 1$. Prove $F(1)$. $\gcd(f_1, f_2) = \gcd(0,1) = 1$.

Stage 2: Assume $F(n)$ is true, which means that $\gcd(f_n, f_{n+1}) = 1$. Then, $\gcd(f_{n+1}, f_{n+2}) = \gcd(f_{n+1}, f_n + f_{n+1}) = \gcd(f_n, f_{n+1}) = 1$. □

Humility and Why We Are Always Wrong

Source: https://www.mathcs.bethel.edu/~gossett/DiscreteMathWithProof/CommonErrorsInProofs.pdf

Example: Let $a, b, c \in \mathbb{Z}$. If $a \mid (bc)$, then either $a \mid b$ or $a \mid c$.
"Proof:" Let $a = 5, b = 3, c = 10$. Then $a \mid bc$, because 5 divides 30. Finally we see that $a \mid c$, because 5 divides 10.

Error: Incorrect universal instantiation. I put restrictions on a, b, c that are invalid.

Definition 4.5. *When working in a Euclidean domain, for every two elements a and $b \neq 0$, there exist unique q and r such that $a = bq + r$, and $0 \leq r < |b|$. This is known as **Euclidean division**.*

Note 4.6. *The integers are a Euclidean domain.*

Note 4.7. *When processing the above, you should interpret q as being "close" to the quotient a/b, or at least as close as the domain you are in allows you to be, and r is the remainder. For example, if $a = 7, b = 3$, the closest quotient we can get with $r \geq 0$, is $q = 2$. Thus we write $7 = 3 \cdot 2 + 1$.*

Definition 4.8. *$a \mod b$ is the value of r when using Euclidean division with values a and b respectively. We say that $a = k \mod b$ if $a \mod b = k$.*

Example: Let a, b be integers, where $a = 1 \mod 3$ and $b = 2 \mod 3$. Then $(a+b) = 0 \mod 3$.

"Proof:" Let a, b be arbitrary integers, such that $a = 1 \mod 3$ and $b = 2 \mod 3$. Then it follows by the division algorithm that there must exist some q such that $a = 3q + 1$. Since $b = 2 \mod 3$, we can also wrote $b = 3q + 2$. Then, $a + b = 3q + 1 + 3q + 2 = 6q + 3 = (2q+1)3$, so again by division algorithm, we find that $a + b = 0 \mod 3$.

Error: Used the same variable twice.

Definition 4.9. *The **Daikon-Raydish** number of an integer x is a number that describes the number of graphs of isomorphism class x^p, where p is the smallest prime larger than x. It is written as* $\mathrm{DR}(x)$ `(\mathrm{DR}(x))`.

Example: Prove that every set of integers of size n all have the same DR number.
"Proof:" **Stage 0:** $F(n) := \forall S \subseteq \mathbb{Z}, |S| = n \Rightarrow (\forall x, y \in S, \mathrm{DR}(x) = \mathrm{DR}(y))$.

Stage 1: $F(1)$ is true because any set of size one will only have one possible DR number.

Stage 2: Suppose that $F(n)$ is true. Then any set of size n will have the same DR number. Now take any set S of size $n+1$. Order the elements like this: $\{a_1, \ldots, a_{n+1}\}$.

Take $S_1 = \{a_1, \ldots, a_n\}$, and $S_2 = \{a_2, \ldots, a_{n+1}\}$. Since $|S_1| = n$ and $F(n)$ is true, all elements a_1 through a_n have the same DR number; call it x. But a_2 is in S_2, and $|S_2| = n$, so $\mathrm{DR}(a_2) = x$, implies $\mathrm{DR}(a_{n+1}) = x$ as well. Therefore $\forall a \in S$, $\mathrm{DR}(a) = x$, so $F(n+1)$ is true.

Error: Inductive step does not work for $n = k = 1$.

Theorem 4.10 (Fermat)**.** *Let $f : (a, b) \to \mathbb{R}$ be a function that is differentiable on (a, b). If f attains either a local extremal value at some $c \in (a, b)$, then $f'(c) = 0$.*

Example: Let $f : (-2, 2) \to \mathbb{R}$ be defined by $f(x) = (x-1)^2$. Then f attains a local extremum at $x = 1$.

"Proof:" Take the derivative $f'(x) = 2(x-1)$. This satisfies $f'(1) = 0$, and so by Fermat's Theorem, it follows that f attains a local extremum at $x = 1$.

Error: The argument does not use the statement of the theorem itself, but uses the converse of the theorem.

Definition 4.11. *If $P \implies Q$ is an implication, then we say its **converse** is $Q \implies P$.*

Note 4.12. *A statement and its converse are **not** logically equivalent. For example, take the statement "if $x > 0$, then $x^2 > 0$," which is true but its converse is false. However, if a statement $P \implies Q$ and its converse $Q \implies P$ are both true, then we have P if and only if Q, i.e., $P \iff Q$.*

Homework

1. Using induction, prove that
$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}.$$

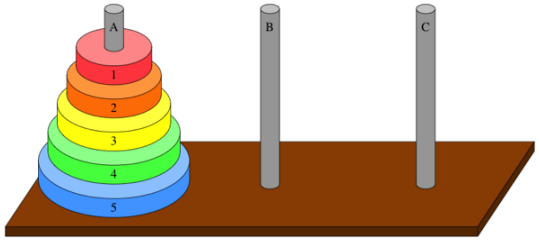
2. Using induction, show that for all $n \in \mathbb{N}$, 8 divides $5^{2n} - 1$.

3. Suppose there are n people in a room. Everyone in the room is very friendly, as it happens, and each person wants to shake every other person's hand. Show that there are $\frac{n^2-n}{2}$ handshakes that will occur. (For example, for $n = 2$, there will be one handshake that occurs between the two people).

4. **(Towers of Hanoi).** Consider the following figure, where we have three rods, and 5 disks stacked on top of each other on the leftmost rod, and the largest disk is on the bottom, and the smallest is on top. The objective of the puzzle is to move all the disks to the rightmost rod, while observing the following three rules:

   - Only one disk may be moved at a time.
   - A "move" is taking the topmost disk from one of the rods and moving it to a different rod.
   - A larger disk may not be placed on a smaller disk.

   Now consider the same game with n disks instead of 5. Show, using induction, that the puzzle may be solved in $2^n - 1$ moves.



5. Show that for any convex polygon with n vertices, the sum of interior angles is $(n-2)\pi$. A **convex polygon** is a polygon where for any two points in the interior, the line segment that joins them is contained within the polygon. However, you may use the easier definition, which is that a polygon is convex when all interior angles are less than π.

Additional Exercises for Practice

6. The Computer Science department considers induction the most important part of Math 300 (even though it *definitely* is not), and the reason why this is the case is that induction provides a way to prove that an algorithm is correct. Consider the following `Adamsort` algorithm, which takes an array of length n as input and outputs an array which contains the same elements, but sorted.

Algorithm 4.13 Adamsort

Require: A an array of length $n \geq 0$
Ensure: A is sorted at the end. That is, $i < j$, then $A[i] \leq A[j]$.
  for $1 \leq i \leq \binom{n}{2}$ **do**
    if there exist $j < k$ such that $A[j] > A[k]$ **then**
      Swap $A[j]$ and $A[k]$
    else
      Break
    end if
  end for

Prove using induction that this algorithm converges to a sorted list.

7. (a) **(Pascal's Identity).** The **binomial coefficient** is written

$$\binom{n}{k} := \frac{n!}{k!(n-k)!}$$

(`\binom{n}{k}`) and is the coefficient on x^k of the expansion of the binomial $(1+x)^n$. It is also the number of ways to choose k elements from a set with n elements. Prove that

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

[Hint: no need to use induction here, just verify using computation.]

(b) **(Leibniz Rule).** † Suppose f and g are differentiable functions. We know from high school calculus the product rule:

$$(fg)' = f'g + fg'.$$

Prove using induction the following Leibniz Rule:

$$(fg)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} f^{(n-k)} g^{(k)}.$$

Here $f^{(n)}$ denotes the nth derivative of f, with the convention that $f^{(0)} = f$. [Hint: use part (a).]