3 Induction

3.1 Introduction to Induction

In this section, we will explore a technique for proving statements of the form $(\forall n \in \mathbb{N})P(n)$, where $P(n)$ is some predicate. Notice that this is a statement about natural numbers and not some other set.

Consider the claims:

1. For all $n \in \mathbb{N}$, $1 + 2 + 3 + \cdots + n = \dfrac{n(n+1)}{2}$.

2. For all $n \in \mathbb{N}$, $n^2 + n + 41$ is prime.

Let's take a look at potential proofs.

"Proof" of Claim (1). If $n = 1$, then $1 = \frac{1(1+1)}{2}$. If $n = 2$, then $1 + 2 = 3 = \frac{2(2+1)}{2}$. If $n = 3$, then $1 + 2 + 3 = 6 = \frac{3(3+1)}{2}$, and so on. □

"Proof" of Claim (2). If $n = 1$, then $n^2 + n + 41 = 43$, which is prime. If $n = 2$, then $n^2 + n + 41 = 47$, which is prime. If $n = 3$, then $n^2 + n + 41 = 53$, which is prime, and so on. □

Are these actual proofs? The answer is NO! In fact, the second claim isn't even true. If $n = 41$, then $n^2 + n + 41 = 41^2 + 41 + 41 = 41(41 + 1 + 1)$, which is not prime since it has 41 as a factor.

It turns out that the first claim is true, but what we wrote cannot be a proof since the same type of reasoning when applied to the second claim seems to prove something that isn't actually true.

We need a rigorous way of capturing "and so on" and a way to verify whether it really is "and so on."

Axiom 3.1 (Axiom of Induction)**.** Let $S \subseteq \mathbb{N}$ such that both

1. $1 \in S$, and

2. if $k \in S$, then $k + 1 \in S$.

Then $S = \mathbb{N}$.

Remark 3.2. Recall that an axiom is a basic mathematical assumption. That is, we are assuming that the Axiom of Induction is true, which I'm hoping that you can agree is a pretty reasonable assumption. I like to think of the first hypothesis of the Axiom of Induction as saying that we have a first rung of a ladder. The second hypothesis says that if we have some random rung, we can always get to the next rung. Taken together, this says that we can get from the first rung to the second, from the second to the third, and so on. Again, we are assuming that the "and so on" works as expected here.

Theorem 3.3 (Principle of Mathematical Induction, *)**.** Let $P_1, P_2, P_3, \ldots$ be a sequence of statements, one for each natural number. Assume

1. P_1 is true, and

2. If P_k is true, then P_{k+1} is true.

Then P_n is true for all $n \in \mathbb{N}$.

Remark 3.4. The Principal of Mathematical Induction (PMI) provides us with a process for proving statements of the form: "For all $n \in \mathbb{N}$, P_n," where P_n is some statement involving $n \in \mathbb{N}$. Hypothesis (1) above is called the **base step** while (2) is called the **inductive step**. Here is what a proof by induction looks like (remarks are in parentheses):

Proof. We proceed by induction.

(i) Base step: (Verify that P_1 is true. This often amounts to plugging $n = 1$ into two sides of some claimed equation and verifying that both sides are actually equal. Don't assume that they are equal!)

(ii) Inductive step: (Your goal is to prove that "For all $k \in \mathbb{N}$, if P_k is true, then P_{k+1} is true.") Let $k \in \mathbb{N}$ and assume that P_k is true. (Now, do some stuff to show that P_{k+1} is true.) Therefore, P_{k+1} is true.

Thus, by the PMI, P_n is true for all $n \in \mathbb{N}$. □

Problem 3.5 (*). For all $n \in \mathbb{N}$, $\displaystyle\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. (*Note:* $\displaystyle\sum_{i=1}^{n} i = 1+2+3+\cdots+n$, by definition.)

Problem 3.6 (*). For all $n \in \mathbb{N}$, 3 divides $4^n - 1$.

Problem 3.7 (*). For all $n \in \mathbb{N}$, 6 divides $n^3 - n$.

Problem 3.8 (*). Let $p_1, p_2, \ldots, p_n$ be n distinct points arranged on a circle. Then the number of line segments joining all pairs of points is $\frac{n^2-n}{2}$.

Theorem 3.9 (*). Let A be a set with n elements. Then $\mathcal{P}(A)$ is a set with 2^n elements.[*]

---

[*]We encountered this theorem back in Section 2.2 (see Conjecture 2.33), but we didn't prove it. Proving this theorem is rather tricky. If you use induction (which I suggest), at some point, you will need to argue that if you add one more element to a finite set, then you end up with twice as many subsets.