11 Mathematical Induction

In philosophy, *deduction* is the process of taking a general statement and applying it to a specific instance. For example: all students must do homework, and I am a student; therefore, I must do homework. In contrast, *induction* is the process of creating a general statement from observations. For example: all cars I have owned need to be repaired at some point; therefore, all cars will need to be repaired at some point. A similar concept is used in mathematics to prove that a statement is true for all integers. To distinguish it from the less specific philosophical notion, we call it *mathematical induction* of which we will introduce two forms. We begin by considering an example from Section 4, showing that the idea behind Mathematical Induction is a familiar one.

Euclid's Division Theorem. We find the smallest counterexample in order to prove the following theorem.

EUCLID'S DIVISION THEOREM. Letting $n \geq 1$, for every non-negative integer m there are unique integers q and $0 \leq r < n$ such that $m = nq + r$.

PROOF. Assume the opposite, that is, there is a non-negative integer m for which no such q and r exist. We choose the smallest such m. Note that m cannot be smaller than n, else we have $q = 0$ and $r = m$, and m cannot be equal to n, else we have $q = 1$ and $r = 0$. It follows that $m' = m - n$ is a positive integer less than m. Thus, there exist integers q' and $0 \leq r' < n$ such that $m' = nq' + r'$. If we add n on both sides, we obtain $m = (q' + 1)n + r'$. If we take $q = q' + 1$ and $r = r'$, we get $m = nq + r$, with $0 \leq r < n$. Thus, by the Principle of Reduction to Absurdity, such integers q and r exist. $\square$

Let $p(k)$ be the statement that there exist integers q and $0 \leq r < n$ with $k = nq + r$. Then, the above proof can be summarized by

$$p(m-n) \wedge \neg p(m) \implies p(m) \wedge \neg p(m).$$

This is the contradiction that implies $\neg p(m)$ cannot be true. We now focus on the statement $p(m - n) \Rightarrow p(m)$. This is the idea of Mathematical Induction which bypasses the construction of a contradiction.

Example: sum of integers. We consider the familiar problem of summing the first n positive integers. Recall that $\binom{n+1}{2} = \frac{n(n+1)}{2}$.

CLAIM. For all $n \geq 0$, we have $\sum_{i=0}^{n} i = \binom{n+1}{2}$.

PROOF. First, we note that $\sum_{i=0}^{0} i = 0 = \binom{1}{2}$. Now, we assume inductively that for $n > 0$, we have

$$\sum_{i=0}^{n-1} i = \binom{n}{2}.$$

If we add n on both sides, we obtain

$$\begin{aligned}\sum_{i=0}^{n} i &= \binom{n}{2} + n \\ &= \frac{(n-1)n}{2} + \frac{2n}{2}\end{aligned}$$

which is $\frac{(n+1)n}{2} = \binom{n+1}{2}$. Thus, by the Principle of Mathematical Induction,

$$\sum_{i=0}^{n} i = \binom{n+1}{2}$$

for all non-negative integers n. $\square$

To analyze why this proof is correct, we let $p(k)$ be the statement that the claim is true for $n = k$. For $n = 1$ we have $p(1) \wedge [p(1) \Rightarrow p(2)]$. Hence, we get $p(2)$ by Modus Ponens. We can see that this continues:

$$\begin{array}{rcc} p(1) \wedge [p(1) \Rightarrow p(2)] & \text{hence} & p(2); \\ p(2) \wedge [p(2) \Rightarrow p(3)] & \text{hence} & p(3); \\ & \vdots & \\ p(n-1) \wedge [p(n-1) \Rightarrow p(n)] & \text{hence} & p(n); \\ & \vdots & \end{array}$$

Thus, $p(n_0)$ and $p(n-1) \Rightarrow p(n)$ for all $n > n_0$ implies $p(n)$ for all $n \geq n_0$.

The weak form. We formalize the proof technique into the first, weak form of the principle. The vast majority of applications of Mathematical Induction use this particular form.

MATHEMATICAL INDUCTION (WEAK FORM). If the statement $p(n_0)$ is true, and the statement $p(n-1) \Rightarrow p(n)$ is true for all $n > n_0$, then $p(n)$ is true for all integers $n \geq n_0$.

To write a proof using the weak form of Mathematical Induction, we thus take the following four steps: it should have the following components:

Base Case: $p(n_0)$ is true.

Inductive Hypothesis: $p(n-1)$ is true.

Inductive Step: $p(n-1) \Rightarrow p(n)$.

Inductive Conclusion: $p(n)$ for all $n \geq n_0$.

Very often but not always, the inductive step is the most difficult part of the proof. In practice, we usually sketch the inductive proof, only spelling out the portions that are not obvious.

Example: sum of powers of two. If we can guess the closed form expression for a finite sum, it is often easy to use induction to prove that it is correct, if it is.

CLAIM. For all integers $n \geq 1$, we have $\sum_{i=1}^{n} 2^{i-1} = 2^n - 1$.

PROOF. We prove the claim by the weak form of the Principle of Mathematical Induction. We observe that the equality holds when $n = 1$ because $\sum_{i=1}^{1} 2^{i-1} = 1 = 2^1 - 1$. Assume inductively that the claim holds for $n-1$. We get to n by adding 2^{n-1} on both sides:

$$\begin{aligned} \sum_{i=1}^{n} 2^{i-1} &= \sum_{i=1}^{n-1} 2^{i-1} + 2^{n-1} \\ &= (2^{n-1} - 1) + 2^{n-1} \\ &= 2^n - 1. \end{aligned}$$

Here, we use the inductive assumption to go from the first to the second line. Thus, by the Principle of Mathematical Induction, $\sum_{i=1}^{n} 2^{i-1} = 2^n - 1$ for all $n \geq 1$. ◻

The strong form. Sometimes it is not enough to use the validity of $p(n-1)$ to derive $p(n)$. Indeed, we have $p(n-2)$ available and $p(n-3)$ and so on. Why not use them?

MATHEMATICAL INDUCTION (STRONG FORM). If the statement $p(n_0)$ is true and the statement $p(n_0) \wedge p(n_0+1) \wedge \cdots \wedge p(n-1) \Rightarrow p(n)$ is true for all $n > n_0$, then $p(n)$ is true for all integers $n \geq n_0$.

Notice that the strong form of the Principle of Mathematical Induction implies the weak form.

Example: prime factor decomposition. We use the strong form to prove that every integer has a decomposition into prime factors.

CLAIM. Every integer $n \geq 2$ is the product of prime numbers.

PROOF. We know that 2 is a prime number and thus also a product of prime numbers. Suppose now that we know that every positive number less than n is a product of prime numbers. Then, if n is a prime number we are done. Otherwise, n is not a prime number. By definition of prime number, we can write it is the product of two smaller positive integers, $n = a \cdot b$. By our supposition, both a and b are products of prime numbers. The product, $a \cdot b$, is obtained by merging the two products, which is again a product of prime numbers. Therefore, by the strong form of the Principle of Mathematical Induction, every integer $n \geq 2$ is a product of prime numbers. ◻

We have used an even stronger statement before, namely that the decomposition into prime factors is unique. We can use the Reduction to Absurdity to prove uniqueness. Suppose n is the smallest positive integer that has two different decompositions. Let $a \geq 2$ be the smallest prime factor in the two decompositions. It does not belong to the other decomposition, else we could cancel the two occurrences of a and get a smaller integer with two different decompositions. Clearly, $n \bmod a = 0$. Furthermore, $r_i = b_i \mod a \neq 0$ for each prime factor b_i in the other decomposition of n. We have

$$\begin{aligned} n \bmod a &= \left(\prod_i b_i \right) \bmod a \\ &= \left(\prod_i r_i \right) \bmod a. \end{aligned}$$

Since all the r_i are smaller than a and a is a prime number, the latter product can only be zero if one or the r_i is zero. But this contradicts that all the b_i are prime numbers larger than a. We thus conclude that every integer larger than one has a unique decomposition into prime factors.

Summary. Mathematical Induction is a tool to prove that a property is true for all positive integers. We used Modus Ponens to prove the weak as well as the strong form of the Principle of Mathematical Induction.