Mathematical Induction

Our next method of proof, the principle of mathematical induction, arises in a variety of situations throughout mathematics and computer science. Often, in the course of analyzing a mathematical phenomenon, we encounter statements of the following form:

1. For every positive integer n, $1 + 2 + \cdots + n = n(n+1)/2$.
2. For any positive integer n, $1 + x + \cdots + x^n = (1 - x^{n+1})/(1 - x)$ for any real number x not equal to 1.

Each of these statements entails an assertion about every positive integer. For example, when $n = 5$, statement 1 says that $1 + 2 + \cdots + 5 = 5 \cdot 6/2$, which happens to be true. When $n = 2$, statement 2 reads: $1 + x + x^2 = (1 - x^3)/(1 - x)$ for each real number $x \neq 1$. This equality does indeed hold for all $x \neq 1$.

Returning to statement 1, we ask: Is it true that for each positive integer n, $1 + 2 + \cdots + n = n(n+1)/2$? To investigate the matter further, we can calculate $1 + 2 + \cdots + n$ for $n = 1, 2, \ldots, 10$. Doing so, we obtain the sequence 1, 3, 6, 10, 15, 21, 28, 36, 45, 55. If we calculate $n(n+1)/2$ for $n = 1, 2, \ldots, 10$, then we obtain the identical list of ten integers. By now we probably believe that statement 1 is true for every positive integer n. To confirm our belief a bit more, we can check more cases such as $n = 11$ and $n = 12$ and we find that statement 1 is also true in these instances. Thus, for any positive integer $n \leq 12$, $1 + 2 + \cdots + n = n(n+1)/2$. But how can we show that this equality holds *for every positive integer n*?

To prove statements 1 and 2, we appeal to a property of the set of positive integers known as the *Principle of Mathematical Induction* (PMI). We state PMI in a general form and show how it applies to statements 1 and 2. Later we consider a slightly different (but logically equivalent) version of mathematical induction called the Principle of Strong Induction.

Excerpts from Galovich, S. (1989). *Introduction to Mathematical Structures*.
San Diego, CA. Harcourt Brace Jovanovich.

Principle of Mathematical Induction. Let $S(1), S(2), \ldots, S(n), \ldots$ be a list of statements, one for each positive integer. Then every statement on the list is true if the following two conditions hold:

(i) $S(1)$ is a true statement,
(ii) For each positive integer k, if $S(k)$ is true, then $S(k+1)$ is true.

PMI can be regarded as a proof technique that is applicable whenever one is attempting to prove that each statement in an infinite list of statements is true. Why are conditions (i) and (ii) sufficient to imply that $S(n)$ is true for all positive integers n? The first statement merely says that statement $S(1)$ is true. The second asserts that if any particular statement is true, then the next statement on the list is also true. Therefore, knowing by (i) that $S(1)$ is true and using (ii), we can conclude that $S(2)$ is true. From (ii) it follows that since $S(2)$ is true, $S(3)$ is true. By another application of (ii), one sees that $S(4)$ is true and so on.

Analogously, we might imagine an infinite staircase. Evidently, we can climb the staircase indefinitely if we know that (i) we can step on the first step and (ii) whenever we are on a given step, we can climb to the next step.

Henceforth, we refer to the first step of PMI, the assertion that $S(1)$ is true, as the *basis step* of the proof by mathematical induction, and the second step, the proof that for each positive integer k, $S(k)$ implies $S(k+1)$, as the *inductive step* of the proof by mathematical induction. In most, but not all, proofs by mathematical induction, the basis step is the easier of the two steps to establish. In proving that the inductive step holds, two general strategies are usually used. The first is to produce a direct proof that $S(k)$ implies $S(k+1)$. The second strategy is to reduce $S(k+1)$ back to $S(k)$. Some examples will illustrate these two strategies.

59

Example 1.3.8 Show that for each positive integer n, $1 + \cdots + n = n(n+1)/2$.

Proof For each positive integer n, let $S(n)$ be the statement $1 + \cdots + n = n(n+1)/2$.

Basis step. $S(1)$ is the statement: $1 = 1(1+1)/2$. Thus $S(1)$ is true.

Inductive step. We suppose that $S(k)$ is true and prove that $S(k+1)$ is true. Thus we assume that

$$1 + \cdots + k = k(k+1)/2$$

and prove that $1 + \cdots + k + (k+1) = (k+1)(k+1+1)/2$. If we add $k+1$ to both sides of the equality in $S(k)$, then on the left side of the sum we obtain the left side of the equality in $S(k+1)$. Our hope is that the right of the sum equals the right side of $S(k+1)$. Let us check: Adding $k+1$ to both sides of $1 + \cdots + k = k(k+1)/2$, we see that

$$\begin{aligned} 1 + \cdots + k + (k+1) &= k(k+1)/2 + (k+1) \\ &= (k+1)(k/2 + 1) \\ &= (k+1)(k/2 + 2/2) \\ &= (k+1)(k+2)/2 \\ &= (k+1)(k+1+1)/2. \end{aligned}$$

Hence, if $S(k)$ is true, then $S(k+1)$ is true.

We can prove this statement by induction. Let $S(n)$ be the statement: For each positive integer n, $1 + \cdots + (2n-1) = n^2$.

Basis step. $S(1)$ holds since $1 = 1^2$.

Inductive step. Suppose $S(n)$ is true. We must show that $S(n+1)$ is true. Thus we must show that

$$1 + \cdots + (2(n+1) - 1) = (n+1)^2.$$

Since $S(n)$ is true,

$$1 + \cdots + (2n-1) = n^2.$$

Hence

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

Therefore, $S(n+1)$ is true.

The inductive proof is now complete. ∎

60

Theorem 1.3.6 Division Algorithm. *Let a and b be positive integers. There exist integers q and r such that $a = b \cdot q + r$, where $0 \le r \le b - 1$.*

Remark The statement asserts that b can be "taken out" of a several times (q times to be exact) in such a way that the remainder is less than b but is at least 0. Here is a quick example: Let $a = 61$ and $b = 13$. Then $61 = 13 \cdot 4 + 9$. Here, $q = 4$ and $r = 9$.

Proof For each positive integer a let $S(a)$ be the statement: For each positive integer b there exist integers q and r such that $a = b \cdot q + r$ where $0 \le r \le b - 1$.

Basis step. To prove $S(1)$ we let b be an arbitrary positive integer, and we must find integers q and r such that $1 = b \cdot q + r$ where $0 \le r \le b - 1$. We observe that if $b = 1$, then we can satisfy the desired condition by taking $q = 1$ and $r = 0$. If $b > 1$, then we satisfy the conditions by setting $q = 0$ and $r = 1$.

Inductive step. Suppose $S(a)$ is true. We show $S(a+1)$ is true. Because $S(a)$ is true, there exist integers q and r such that $a = b \cdot q + r$ where $0 \le r \le b - 1$. To show that $S(a+1)$ holds, we must find integers q_1 and r_1 such that $a + 1 = b \cdot q_1 + r_1$ where $0 \le r_1 \le b - 1$.

We know that $a = b \cdot q + r$ where $0 \le r \le b - 1$. Thus $a + 1 = b \cdot q + r + 1$. If $0 \le r \le b - 2$, then $1 \le r + 1 \le b - 1$, and $a + 1 = b \cdot q_1 + r_1$ where $q_1 = q$, $r_1 = r + 1$, and $0 \le 1 \le r_1 \le b - 1$. On the other hand, if $r = b - 1$, then $r + 1 = b$ and $a + 1 = bq + r + 1 = bq + b = b \cdot (q+1) = b \cdot q_1 + r_1$ where $q_1 = q + 1$ and $r_1 = 0$. Therefore, in every possible case, $S(a+1)$ holds.

The inductive step is thus established. ∎

Excerpts from Galovich, S. (1989). *Introduction to Mathematical Structures*. San Diego, CA. Harcourt Brace Jovanovich.