Mathematical Induction

Ryan C. Daileda

Trinity University

Intro to Abstract Mathematics

Introduction

Let $P(n)$ be a statement in the (free) variable n.

In its most basic form, *(mathematical) induction* is a proof technique that may be applied to statements of the form

$$\forall n \in \mathbb{N}\,(P(n)). \tag{1}$$

The basic form easily generalizes to handle statements of the form

$$\forall n \geq a\,(P(n)), \tag{2}$$

in which the universe of discourse is $\mathbb{Z}$.

Warning: Induction *is not* the only way to prove statements of the form (1) or (2). It is just one potential option.

PMI

Induction as a proof technique follows from the following fact, which is a consequence of the Well-Ordering Principle.

Theorem 1 (Principle of Mathematical Induction)

Let $S \subset \mathbb{N}$. Suppose S has the following two properties:

1. $0 \in S$;
2. $\forall n \in \mathbb{N} \, (n \in S \to n+1 \in S)$.

Then $S = \mathbb{N}$.

Proof. Assume, for the sake of contradiction, that $S \neq \mathbb{N}$.

Then $\mathbb{N} \setminus S \neq \varnothing$. So WOP implies there is a least $m \in \mathbb{N} \setminus S$.

Since $0 \in S$, we have $0 \notin \mathbb{N} \setminus S$. Therefore $m > 0$.

In particular, $m-1 \in \mathbb{N}$. But $m-1 \notin \mathbb{N} \setminus S$, so $m-1 \in S$.

Property **2** of S then implies $m = (m-1)+1 \in S$.

Hence $m \in S \cap (\mathbb{N} \setminus S) = \varnothing$, a contradiction. $\square$

The Principle of Mathematical Induction (PMI) has the following corollary.

Theorem 2

Let $P(n)$ be a statement in the (free) variable n. Suppose that:

1. $P(0)$ *is true;*
2. $\forall n \in \mathbb{N}\,(P(n) \to P(n+1))$ *is true.*

Then $\forall n \in \mathbb{N}\,(P(n))$ is true. That is, $P(n)$ is true for every $n \in \mathbb{N}$.

Proof. Apply PMI to the truth set S of $P(n)$. $\square$

Mathematical Induction

If $P(n)$ is a statement in the (free) variable n, the preceding result gives a procedure for proving $\forall n \in \mathbb{N}\,(P(n))$:

1. (*Base Case*) Prove $P(0)$.
2. (*Inductive Step*) Let $n \in \mathbb{N}$ and prove $P(n) \Rightarrow P(n+1)$.

This process is called *(mathematical) induction*.

Intuitively, induction results in a chain of implications

$$P(0) \Rightarrow P(1) \Rightarrow P(2) \Rightarrow P(3) \Rightarrow \cdots .$$

If $P(0)$ is true, then $P(1)$ is true, and so $P(2)$ is true, and so $P(3)$ is true, etc.

Remarks

1. Proving the base case is *essential*, since the truth of $P(0)$ is what causes the truth of the remaining statements.
2. To prove $P(n) \Rightarrow P(n+1)$ we begin by assuming $P(n)$, and deduce $P(n+1)$ as a consequence.
3. When we assume $P(n)$, we *are not* assuming the conclusion. We are simply proving an implication with hypothesis $P(n)$.
4. In the inductive step, $P(n)$ is called the *inductive hypothesis*.
5. We can replace $n \in \mathbb{N}$ with $n \geq a$ $(n, a \in \mathbb{Z})$, but the base case becomes $P(a)$.

Examples

Example 1

Prove that for all $n \in \mathbb{N}$, $0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

Scratch Work.

Let $P(n)$ denote the equation $0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

We are trying to prove that $P(n)$ is true for all $n \in \mathbb{N}$. Let's try induction.

Base Case: $(n = 0)$ $P(0)$ is the statement $0 = \frac{0(0+1)}{2}$. This is true.

<u>Inductive Step:</u> We want to prove $\forall n \in \mathbb{N}(P(n) \Rightarrow P(n+1))$.

We begin with "Let $n \in \mathbb{N}$" and try to prove $P(n) \Rightarrow P(n+1)$.

To prove the implication (directly), we suppose $P(n)$ is true and deduce $P(n+1)$.

That is, we assume $0+1+2+\cdots+n=\frac{n(n+1)}{2}$ and use this to conclude $0+1+2+\cdots+n+(n+1)=\frac{(n+1)((n+1)+1)}{2}$.

To do this, we look for a connection between $P(n)$ and $P(n+1)$.

In this case, notice that the LHS of $P(n+1)$ is the LHS of $P(n)$ *plus* $n+1$.

So with the hypothesis $P(n)$ we have

$$\underbrace{0+1+2+\cdots+n}_{\frac{n(n+1)}{2}} + (n+1) = \frac{n(n+1)}{2} + (n+1) = (n+1)\left(\frac{n}{2}+1\right)$$

$$= (n+1)\frac{n+2}{2} = \frac{(n+1)((n+1)+1)}{2},$$

which shows that $P(n+1)$ is true! Let's get formal now.

Proof. We prove that $0+1+2+\cdots+n = \frac{n(n+1)}{2}$ for all $n \in \mathbb{N}$ by induction.

When $n = 0$, the equation in question becomes $0 = \frac{0(0+1)}{2}$, which is true.

Now let $n \in \mathbb{N}$ and suppose that $0+1+2+\cdots+n = \frac{n(n+1)}{2}$ holds.

We then have

$$\begin{aligned}0+1+2+\cdots+n+(n+1) &= \frac{n(n+1)}{2}+(n+1)\\ &= (\text{as above}) = \frac{(n+1)(n+2)}{2},\end{aligned}$$

which shows that the $n+1$ case holds as well.

By mathematical induction, the equation

$$0+1+2+\cdots+n=\frac{n(n+1)}{2}$$

holds for all $n \in \mathbb{N}$. □

Example 2

Prove that for all $n \in \mathbb{N}$, $5 | n^5 - n$.

Proof. We induct on $n \in \mathbb{N}$.

When $n = 0$, we must prove that $5 | 0^5 - 0$, which is clearly true.

Now let $n \geq 0$ and suppose that $5 | n^5 - n$. Write $n^5 - n = 5k$ for some $k \in \mathbb{N}$.

We have (using Pascal's triangle)

$$\begin{aligned}(n+1)^5 - (n+1) &= n^5 + 5n^4 + 10n^3 + 10n^2 + 5n + 1 - n - 1 \\ &= \underbrace{n^5 - n}_{5k} + 5(n^4 + 2n^3 + 2n^2 + n)\end{aligned}$$

$$= 5(\underbrace{k + n^4 + 2n^3 + 2n^2 + n}_{m \in \mathbb{N}}) = 5m,$$

which shows that $5 | (n+1)^5 - (n+1)$, as needed.

By mathematical induction, we find that $5 | n^5 - n$ for all $n \in \mathbb{N}$. □

Remark. This result is an instance of *Fermat's Little Theorem*, which states that if p is prime, then

$$p | n^p - n \text{ for all } n \in \mathbb{N}.$$

Example 3

Prove that for all $n \geq 4$, $n! > 2^n$.

Proof. We induct on $n \geq 4$.

When $n = 4$, we have $n! = 4! = 24$ and $2^n = 2^4 = 16$, so that $4! > 2^4$.

Now let $n \geq 4$ and suppose that $n! > 2^n$.

We then have

$$(n+1)! = (n+1)n! > (n+1)2^n \geq (4+1)2^n > 2 \cdot 2^n = 2^{n+1}.$$

By induction, the inequality $n! > 2^n$ holds for all $n \geq 4$. □

When do I use induction?

Consider a statement of the form $\forall n \in \mathbb{N}(P(n))$. Let $n \in \mathbb{N}$.

1. If you can prove $P(n)$ directly, there's no need for induction
2. If you see a connection between $P(n)$ and $P(n+1)$, then induction may be an option.

Identifying the connection between $P(n)$ and $P(n+1)$ is the key to every induction proof!

More Examples

Example 4

For $n \in \mathbb{N}$, let $F_n = 2^{2^n} + 1$ (the nth *Fermat number*). Prove that for all $n \geq 1$, $F_n = (F_0 F_1 F_2 \cdots F_{n-1}) + 2$.

Solution. We induct on $n \geq 1$.

When $n = 1$, we must show that $F_1 = F_0 + 2$. Indeed,

$$F_0 + 2 = 2^{2^0} + 1 + 2 = 5 = 2^{2^1} + 1 = F_1.$$

Now let $n \geq 1$ and suppose that $F_n = (F_0 F_1 F_2 \cdots F_{n-1}) + 2$. Then $F_0 F_1 F_2 \cdots F_{n-1} = F_n - 2$. Thus

$$F_0 F_1 F_2 \cdots F_{n-1} F_n + 2 = (F_n - 2) F_n + 2$$

$$
\begin{aligned}
&= (2^{2^n} + 1 - 2)(2^{2^n} + 1) + 2 \\
&= (2^{2^n} - 1)(2^{2^n} + 1) + 2 \\
&= (2^{2^n})^2 - 1 + 2 = 2^{2^n \cdot 2} + 1 \\
&= 2^{2^{n+1}} + 1 = F_{n+1},
\end{aligned}
$$

as needed.

By mathematical induction, the proof is complete. □

Remark. The first few Fermat numbers are

$$3, 5, 17, 257, 65537, 4294967297, \ldots$$

F_0, F_1, F_2, F_3, F_4 are prime, but Euler showed F_5 is composite.

It is not known if F_n is composite for all $n > 4$, or if F_n is prime infinitely often.

Example 5

Show that for all $n \in \mathbb{N}$, $24 | (2 \cdot 7^n - 3 \cdot 5^n + 1)$.

Solution. We induct on $n \in \mathbb{N}$.

When $n = 0$, $2 \cdot 7^n - 3 \cdot 5^n + 1 = 2 - 3 + 1 = 0$, which is divisible by 24.

Let $n \in \mathbb{N}$ and suppose that $24 | (2 \cdot 7^n - 3 \cdot 5^n + 1)$.

Write $2 \cdot 7^n - 3 \cdot 5^n + 1 = 24k$ for some $k \in \mathbb{Z}$. Then

$$2 \cdot 7^n = 24k + 3 \cdot 5^n - 1.$$

Thus

$$\begin{aligned}
2 \cdot 7^{n+1} - 3 \cdot 5^{n+1} + 1 &= 7 \cdot 2 \cdot 7^n - 3 \cdot 5^{n+1} + 1 \\
&= 7(24k + 3 \cdot 5^n - 1) - 3 \cdot 5^{n+1} + 1 \\
&= 7 \cdot 24k + 7 \cdot 3 \cdot 5^n - 7 - 5 \cdot 3 \cdot 5^n + 1 \\
&= 7 \cdot 24k + 3 \cdot 5^n(7 - 5) - 6 \\
&= 7 \cdot 24k + 6 \cdot 5^n - 6 = 7 \cdot 24k + 6(5^n - 1) \\
&= 7 \cdot 24k + 6(5 - 1)(\underbrace{5^{n-1} + 5^{n-2} + \cdots + 5 + 1}_{m}) \\
&= 7 \cdot 24k + 24m = 24(7k + m),
\end{aligned}$$

where we have used the identity

$$X^n - 1 = (X - 1)(X^{n-1} + X^{n-2} + \cdots + X + 1)$$

from HW (with $X = 5$). This proves $24 | (2 \cdot 7^{n+1} - 3 \cdot 5^{n+1} + 1)$. □

Example 6

Use induction to prove that

$$X^n - 1 = (X-1)(X^{n-1} + X^{n-2} + \cdots + X + 1),$$

for all $n \geq 1$.

Remark. We have

$$X^{n-1} + X^{n-2} + \cdots + X + 1 = \sum_{k=0}^{n-1} X^k.$$

When $n = 1$, this means the sum is just $X^0 = 1$.

Solution. We induct on $n \geq 1$.

When $n = 1$, the identity in question becomes $X - 1 = (X-1) \cdot 1$, which is certainly true.

Let $n \geq 1$ and suppose that

$$X^n - 1 = (X-1)(X^{n-1} + X^{n-2} + \cdots + X + 1)$$

Then

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

Appealing to mathematical induction completes the proof. □