Induction

Mathematical induction is a technique for showing that a statement P(n) is true for all natural numbers n, or for some infinite subset of the natural numbers (e.g. all positive even integers).

A proof by induction has the following outline:

Claim: P(n) is true for all positive integers n.
Proof: We'll use induction on n. ← induction variable

Base: We need to show that P(1) is true.
Induction: Suppose that P(n) is true for n = 1, 2, . . . , k–1.
We need to show that P(k) is true.

inductive hypothesis

Simple Example

Claim *For any positive integer n, $\Sigma_{i=1}^{n} i = \frac{n(n+1)}{2}$.*

Proof: We will show that $\Sigma_{i=1}^{n} i = \frac{n(n+1)}{2}$ for any positive integer n, using induction on n.

Base: We need to show that the formula holds for $n = 1$. $\Sigma_{i=1}^{1} i = 1$. And also $\frac{1 \cdot 2}{2} = 1$. So the two are equal for $n = 1$.

Induction: Suppose that $\Sigma_{i=1}^{n} i = \frac{n(n+1)}{2}$ for $n = 1, 2, \ldots, k-1$. We need to show that $\Sigma_{i=1}^{k} i = \frac{k(k+1)}{2}$.

By the definition of summation notation, $\Sigma_{i=1}^{k} i = (\Sigma_{i=1}^{k-1} i) + k$

Our inductive hypothesis states that at $n = k-1$, $\Sigma_{i=1}^{k-1} i = (\frac{(k-1)k}{2})$.

Combining these two formulas, we get that $\Sigma_{i=1}^{k} i = (\frac{(k-1)k}{2}) + k$.

But $(\frac{(k-1)k}{2}) + k = (\frac{(k-1)k}{2}) + \frac{2k}{2} = (\frac{(k-1+2)k}{2}) = \frac{k(k+1)}{2}$.

So, combining these equations, we get that $\Sigma_{i=1}^{k} i = \frac{k(k+1)}{2}$ which is what we needed to show.

Why is the induction legit?

Domino Theory (intuitively):

- Imagine an infinite line of dominoes.
- The base step pushes the first one over.
- The inductive step claims that one domino falling down will push over the next domino in the line.
- So dominos will start to fall from the beginning all the way down the line.
- This process continues forever, because the line is infinitely long.
- However, if you focus on any specific domino, it falls after some specific finite delay.

Another example

Claim *For any natural number n, $n^3 - n$ is divisible by 3.*

Proof: By induction on n.

$\boxed{\text{Base:}}$ Let $n = 0$. Then $n^3 - n = 0^3 - 0 = 0$ which is divisible by 3.

$\boxed{\text{Induction:}}$ Suppose that $n^3 - n$ is divisible by 3, for $n = 0, 1, \ldots, k$. We need to show that $(k+1)^3 - (k+1)$ is divisible by 3.

$$(k+1)^3 - (k+1) = (k^3 + 3k^2 + 3k + 1) - (k+1) = (k^3 - k) + 3(k^2 + k)$$

From the inductive hypothesis, $(k^3 - k)$ is divisible by 3. And $3(k^2 + k)$ is divisible by 3 since $(k^2 + k)$ is an integer. So their sum is divisible by 3. That is $(k+1)^3 - (k+1)$ is divisible by 3.

Variation in notation

Certain details of the induction outline vary, depending on the individual preferences of the author and the specific claim being proved.

- Some folks prefer to assume the statement is true for k and prove it's true for k + 1.
- Other assume it's true for k – 1 and prove it's true for k.
- For a specific problems, sometimes one or the other choice yields a slightly simpler proofs.
- Folks differ as to whether the notation n = 0, 1, . . . , k implies that k is necessarily at least 0, at least 1, or at least 2.

Recursive Definition

Recursive function definitions in mathematics are basically similar to recursive procedures in programming languages

A recursive definition always has two parts:

- Base case or cases
- Recursive formula

For example, the summation $\sum_{i=1}^{n} i$ can be defined as:

- $g(1) = 1$
- $g(n) = g(n - 1) + n$, for all $n \geq 2$

Both the base case and the recursive formula must be present to have a complete definition

The true power of recursive definition is revealed when the result for n depends on the results for more than one smaller value, as in the strong induction examples.

For example, the famous Fibonacci numbers are defined:

- $F_0 = 0$
- $F_1 = 1$
- $F_i = F_{i-1} + F_{i-2}, \quad \forall i \geq 2$

So $F_2 = 1$, $F_3 = 2$, $F_4 = 3$, $F_5 = 5$, $F_6 = 8$, $F_7 = 13$, $F_8 = 21$, $F_9 = 34$.

It isn't at all obvious how to express this pattern non-recursively.

Finding closed forms (1)

The simplest technique for finding closed forms is called "unrolling".

For example, suppose we have a function T : N → Z defined by

$$\begin{aligned} T(1) &= 1 \\ T(n) &= 2T(n-1)+3, \quad \forall n \geq 2 \end{aligned}$$

The values of this function are T(1) = 1, T(2) = 5, T(3) = 13, T(4) = 29, T(5) = 61.

It isn't so obvious what the pattern is.

- The idea behind unrolling is to substitute a recursive definition into itself,
- so as to re-express T(n) in terms of T(n−2) rather than T(n−1).
- We keep doing this, expressing T(n) in terms of the value of T for smaller and smaller inputs,
- until we can see the pattern required to express T(n) in terms of n and T(0).
- So, for our example function, we would compute:

$$
\begin{aligned}
T(n) &= 2T(n-1)+3 \\
&= 2(2T(n-2)+3)+3 \\
&= 2(2(2T(n-3)+3)+3)+3 \\
&= 2^3T(n-3)+2^2\cdot 3+2\cdot 3+3 \\
&= 2^4T(n-4)+2^3\cdot 3+2^2\cdot 3+2\cdot 3+3 \\
&\dots \\
&= 2^kT(n-k)+2^{k-1}\cdot 3+\ldots+2^2\cdot 3+2\cdot 3+3
\end{aligned}
$$

$$
\begin{aligned}
T(n) &= 2^k T(n-k) + 2^{k-1} \cdot 3 + \ldots + 2^2 \cdot 3 + 2 \cdot 3 + 3 \\
&= 2^k T(n-k) + 3(2^{k-1} + \ldots + 2^2 + 2 + 1) \\
&= 2^k T(n-k) + 3 \sum_{i=0}^{k-1} (2^i)
\end{aligned}
$$

Now, we need to determine when the input to T will hit the base case.

In our example, the input value is $n - k$ and the base case is for an input of 1.

So we hit the base case when $n - k = 1$. i.e. when $k = n - 1$

Substituting this value for k back into our equation, and using the fact that T(1) = 1, we get

$$\begin{aligned} T(n) &= 2^k T(n-k) + 3\sum_{i=0}^{k-1}(2^i) \\ &= 2^{n-1}T(1) + 3\sum_{i=0}^{n-2}(2^i) \\ &= 2^{n-1} + 3\sum_{k=0}^{n-2}(2^k) \\ &= 2^{n-1} + 3(2^{n-1}-1) = 4(2^{n-1}) - 3 = 2^{n+1} - 3 \end{aligned}$$

Finding closed forms (2)

The second technique for finding closed forms is using "induction" starting with a guess or claim for the solution.

Claims involving recursive definitions often require proofs using a strong inductive hypothesis.

For example, suppose that the function f : N → Z is defined by

$$f(0) = 2$$

$$f(1) = 3$$

$$\forall n \geq 1,\ f(n+1) = 3f(n) - 2f(n-1)$$

Claim $\forall n \in \mathbb{N}, f(n) = 2^n + 1$

Claim $\forall n \in \mathbb{N}, f(n) = 2^n + 1$

Proof: by induction on n.

Base: $f(0)$ is defined to be 2. $2^0+1 = 1+1 = 2$. So $f(n) = 2^n+1$ when $n = 0$.

$f(1)$ is defined to be 3. $2^1 + 1 = 2 + 1 = 3$. So $f(n) = 2^n + 1$ when $n = 1$.

Induction: Suppose that $f(n) = 2^n + 1$ for $n = 0, 1, \ldots, k$.

$f(k + 1) = 3f(k) - 2f(k - 1)$

By the induction hypothesis, $f(k) = 2^k+1$ and $f(k-1) = 2^{k-1}+1$. Substituting these formulas into the previous equation, we get:

$f(k+1) = 3(2^k+1) - 2(2^{k-1}+1) = 3 \cdot 2^k + 3 - 2^k - 2 = 2 \cdot 2^k + 1 = 2^{k+1} + 1$

So $f(k + 1) = 2^{k+1} + 1$, which is what we needed to show.

We need to use a strong induction hypothesis, as well as two base cases, because the inductive step uses the fact that the formula holds for two previous values of n (k and $k - 1$).

Proof by Contradiction

Contradiction is a powerful proof technique that can be extremely useful in the right circumstances.

However, contradiction proofs tend to be less convincing and harder to write than direct proofs.

In proof by contradiction, we show that a claim P is true by showing that its negation ¬P leads to a contradiction.

If ¬P leads to a contradiction, then ¬P can't be true, and therefore P must be true.

- A contradiction can be any statement that is well-known to be false or
- a set of statements that are obviously inconsistent with one another. e.g.
  - ✓ n is odd and n is even, or
  - ✓ $x < 2$ and $x > 7$.

Simple Example

Claim There is no largest even integer.

Proof:

- Suppose not. That is, suppose that there were a largest even integer. Let's call it k.
- Since k is even, it has the form $2n$, where n is an integer.
- Consider $k + 2$. $k + 2 = (2n) + 2 = 2(n + 1)$.
- So $k + 2$ is even. But $k + 2$ is larger than k.
- This contradicts our assumption that k was the largest even integer. So our original claim must have been true.

Another Example: $\sqrt{2}$ is irrational

Proof:

Suppose not. That is, suppose that $\sqrt{2}$ were rational.

- Then we can write $\sqrt{2}$ as a fraction $\frac{a}{b}$, where a and b are integers with no common factors.
- Since $\sqrt{2} = \frac{a}{b}$, $2 = \frac{a^2}{b^2}$. So $2b^2 = a^2$.
- By the definition of even, this means a^2 is even.
- But then a must be even. So $a = 2n$ for some integer n.
- If $a = 2n$ and $2b^2 = a^2$, then $2b^2 = 4n^2$. So $b^2 = 2n^2$. This means that b^2 is even, so b must be even.
- We now have a contradiction. a and b were chosen not to have any common factors. But they are both even, i.e. they are both divisible by 2.
- Because assuming that $\sqrt{2}$ was rational led to a contradiction, it
- must be the case that $\sqrt{2}$ is irrational.

Philosophy

- Proof by contradiction strikes many people as mysterious, because the argument starts with an assumption known to be false.
- The whole proof consists of building up a fantasy world and then knocking it down.
- Although the method is accepted as valid by the vast majority of theoreticians, these proofs are less satisfying than direct proofs which construct the world as we believe it to be.

There is, in fact, a minority but long-standing thread within theoretical mathematics, called “constructive mathematics,” which does not accept this proof method.