

Induction I

1 Induction

A professor brings to class a bottomless bag of assorted miniature candy bars. She offers to share in accordance with two rules. First, she numbers the students 0, 1, 2, 3, and so forth for convenient reference. Now here are the two rules:

1. Student 0 gets candy.
2. For all $n \in \mathbb{N}$, if student n gets candy, then student $n + 1$ also gets candy.

You can think of the second rule as a compact way of writing a whole sequence of statements, one for each natural value of n :

- If student 0 gets candy, then student 1 also gets candy.
- If student 1 gets candy, then student 2 also gets candy.
- If student 2 gets candy, then student 3 also gets candy, and so forth.

Now suppose you are student 17. By these rules, are you entitled to a miniature candy bar? Well, student 0 gets candy by the first rule. Therefore, by the second rule, student 1 also gets candy, which means student 2 gets candy as well, which means student 3 get candy, and so on. So the professor's two rules actually guarantee candy for *every* student, no matter how large the class. You win!

This reasoning generalizes to a principle called *induction*:

Principle of Induction. Let $P(n)$ be a predicate. If

- $P(0)$ is true, and
- for all $n \in \mathbb{N}$, $P(n)$ implies $P(n + 1)$,

then $P(n)$ is true for all $n \in \mathbb{N}$.

Here's the correspondence between the induction principle and sharing candy bars. Suppose that $P(n)$ is the predicate, "student n gets candy". Then the professor's first rule asserts that $P(0)$ is true, and her second rule is that for all $n \in \mathbb{N}$, $P(n)$ implies $P(n + 1)$. Given these facts, the induction principle says that $P(n)$ is true for all $n \in \mathbb{N}$. In other words, everyone gets candy.

The intuitive justification for the general induction principle is the same as for everyone getting a candy bar under the professor's two rules. Mathematicians find this intuition so compelling that induction is always either taken as an axiom or else proved from more primitive axioms, which are themselves specifically designed so that induction is provable. In any case, the induction principle is a core principle of mathematics.

2 Using Induction

Induction is by far the most important proof technique in computer science. Generally, induction is used to prove that some statement holds for all natural values of a variable. For example, here is a classic formula:

Theorem 1. For all $n \in \mathbb{N}$:

$$1 + 2 + 3 + \dots + n = \frac{n(n + 1)}{2}$$

The left side of the equation represents the sum of all the numbers from 1 to n . You're supposed to guess the pattern and mentally replace the \dots with the other terms. We could eliminate the need for guessing by rewriting the left side with *summation notation*:

$$\sum_{i=1}^n i \quad \text{or} \quad \sum_{1 \leq i \leq n} i \quad \text{or} \quad \sum_{i \in \{1, \dots, n\}} i$$

Each of these expressions denotes the sum of all values taken on by the expression to the right of the sigma as the variable i ranges from 1 to n . The meaning of the sum in Theorem 1 is not so obvious in a couple special cases:

- If $n = 1$, then there is only one term in the summation, and so $1 + 2 + 3 + \dots + n = 1$. Don't be misled by the appearance of 2 and 3 and the suggestion that 1 and n are distinct terms!
- If $n \leq 0$, then there are no terms at all in the summation, and so $1 + 2 + 3 + \dots + n = 0$.

The \dots notation is convenient, but watch out for these special cases where the notation is misleading!

Now let's use the induction principle to prove Theorem 1. Suppose that we define predicate $P(n)$ to be " $1 + 2 + 3 + \dots + n = n(n + 1)/2$ ". Recast in terms of this predicate, the theorem claims that $P(n)$ is true for all $n \in \mathbb{N}$. This is great, because the induction principle lets us reach precisely that conclusion, provided we establish two simpler facts:

- $P(0)$ is true.
- For all $n \in \mathbb{N}$, $P(n)$ implies $P(n + 1)$.

So now our job is reduced to proving these two statements. The first is true because $P(0)$ asserts that a sum of zero terms is equal to $0(0 + 1)/2 = 0$.

The second statement is more complicated. But remember the basic plan for proving the validity of any implication: *assume* the statement on the left and then *prove* the statement on the right. In this case, we assume $P(n)$:

$$1 + 2 + 3 + \dots + n = \frac{n(n + 1)}{2}$$

in order to prove $P(n + 1)$:

$$1 + 2 + 3 + \dots + n + (n + 1) = \frac{(n + 1)(n + 2)}{2}$$

These two equations are quite similar; in fact, adding $(n + 1)$ to both sides of the first equation and simplifying the right side gives the second equation:

$$\begin{aligned} 1 + 2 + 3 + \dots + n + (n + 1) &= \frac{n(n + 1)}{2} + (n + 1) \\ &= \frac{(n + 2)(n + 1)}{2} \end{aligned}$$

Thus, if $P(n)$ is true, then so is $P(n + 1)$. This argument is valid for every natural number n , so this establishes the second fact required by the induction principle. In effect, we've just proved that $P(0)$ implies $P(1)$, $P(1)$ implies $P(2)$, $P(2)$ implies $P(3)$, etc. all in one fell swoop.

With these two facts in hand, the induction principle says that the predicate $P(n)$ is true for all natural n . And so the theorem is proved!

2.1 A Template for Induction Proofs

The proof of Theorem 1 was relatively simple, but even the most complicated induction proof follows exactly the same template. There are five components:

1. **State that the proof uses induction.** This immediately conveys the overall structure of the proof, which helps the reader understand your argument.
2. **Define an appropriate predicate $P(n)$.** The eventual conclusion of the induction argument will be that $P(n)$ is true for all natural n . Thus, you should define the predicate $P(n)$ so that your theorem is equivalent to (or follows from) this conclusion. Often the predicate can be lifted straight from the claim, as in the example above. The predicate $P(n)$ is called the "induction hypothesis".

3. **Prove that $P(0)$ is true.** This is usually easy, as in the example above. This part of the proof is called the “base case” or “basis step”.
4. **Prove that $P(n)$ implies $P(n + 1)$ for every natural number n .** This is called the “inductive step” or “induction step”. The basic plan is always the same: assume that $P(n)$ is true and then use this assumption to prove that $P(n + 1)$ is true. These two statements should be fairly similar, but bridging the gap may require some ingenuity. Whatever argument you give must be valid for every natural number n , since the goal is to prove the implications $P(0) \rightarrow P(1)$, $P(1) \rightarrow P(2)$, $P(2) \rightarrow P(3)$, etc. all at once.
5. **Invoke induction.** Given these facts, the induction principle allows you to conclude that $P(n)$ is true for all natural n . This is the logical capstone to the whole argument, but many writers leave this step implicit.

Explicitly labeling the *base case* and *inductive step* may make your proofs more clear.

2.2 A Clean Writeup

The proof of Theorem 1 given above is perfectly valid; however, it contains a lot of extraneous explanation that you won’t usually see in induction proofs. The writeup below is closer to what you might see in print and should be prepared to produce yourself.

Proof. We use induction. Let $P(n)$ be the predicate:

$$1 + 2 + 3 + \dots + n = \frac{n(n + 1)}{2}$$

Base case: $P(0)$ is true, because both sides of the equation are zero.

Inductive step: Assume that $P(n)$ is true, where n is any natural number. Then $P(n + 1)$ is also true, because:

$$\begin{aligned} 1 + 2 + 3 + \dots + n + (n + 1) &= \frac{n(n + 1)}{2} + (n + 1) \\ &= \frac{(n + 1)(n + 2)}{2} \end{aligned}$$

The first step uses the assumption $P(n)$, and the second follows by simplification. Therefore, $P(n)$ is true for all natural n by induction. \square

Induction was helpful for *proving the correctness* of this summation formula, but not helpful for *discovering* the formula in the first place. There are some tricks for finding such formulas, which we’ll show you in a few weeks.

3 A Divisibility Theorem

An integer a *divides* an integer b if b is a multiple of a . This is denoted $a \mid b$. For example, $3 \mid (5^3 - 5)$, since $5^3 - 5 = 120$ is a multiple of 3. More generally, we have the following theorem:

Theorem 2. $\forall n \in \mathbb{N} \quad 3 \mid (n^3 - n)$

Let's try to prove this with induction. The first challenge is always selecting the right induction hypothesis, $P(n)$. Your first instinct should be to lift the induction hypothesis directly from the claim. Thus, in this case, we should first try letting $P(n)$ be the predicate " $3 \mid (n^3 - n)$ ". (This doesn't always work out – as we'll see in a later example – but it does work in this case.)

Now we must address the base case by proving that $P(0)$ is true. As is often the case, this is easy: $3 \mid (0^3 - 0)$, since 0 is a multiple of 3. (Specifically, $3 \cdot 0 = 0$.)

Our next task, the inductive step, is typically the most difficult part of an induction proof. We must show that $P(n)$ implies $P(n + 1)$. Thus, as usual when proving an implication, we *assume* $P(n)$ in order to *prove* $P(n + 1)$. Writing out what these two expressions actually mean is often helpful. In this case, we assume $P(n)$:

$$3 \mid (n^3 - n)$$

in order to prove $P(n + 1)$:

$$3 \mid ((n + 1)^3 - (n + 1))$$

These two statements look somewhat similar, but how can we use the first to prove the second? For lack of any other ideas, let's multiply out the expression in the second statement:

$$\begin{aligned} 3 \mid ((n + 1)^3 - (n + 1)) &\Leftrightarrow 3 \mid (n^3 + 3n^2 + 3n + 1 - n - 1) \\ &\Leftrightarrow 3 \mid (n^3 + 3n^2 + 2n) \end{aligned}$$

Aha! Notice that the last expression is equal to $n^3 - n$ plus $3n^2 + 3n$. Since $3n^2 + 3n$ is a multiple of 3 and $n^3 - n$ is a multiple of 3 by the assumption $P(n)$, their sum must also be a multiple of 3. Therefore, $((n + 1)^3 - (n + 1))$ is a multiple of 3.

Playing around with $P(n)$ and $P(n + 1)$ in this way, trying to understand how the two are related, is pretty typical when one is searching for an induction argument. However, what we've done so far is only scratchwork. What remains is to organize our reasoning into a clear proof.

Proof. We use induction. Let $P(n)$ be the proposition that $3 \mid (n^3 - n)$.

Base case: $P(0)$ is true because $3 \mid 0^3 - 0$.

Inductive step: Assume that $P(n)$ is true, where n is any natural number. Then:

$$\begin{aligned} 3 \mid (n^3 - n) &\Rightarrow 3 \mid (n^3 - n) + 3(n^2 + n) \\ &\Rightarrow 3 \mid n^3 + 3n^2 + 3n + 1 - n - 1 \\ &\Rightarrow 3 \mid (n + 1)^3 - (n + 1) \end{aligned}$$

The first implication relies on the fact that $3(n^2 + n)$ is divisible by 3. The remaining implications involve only rewriting the expression on the right. The last statement is $P(n + 1)$, so we've proved that $P(n)$ implies $P(n + 1)$ for all $n \in \mathbb{N}$.

By the principle of induction, $P(n)$ is true for all $n \in \mathbb{N}$, which proves the claim. \square

This proof would look quite mysterious to anyone not privy to the scratchwork we did beforehand. In particular, one might ask how we had the foresight to introduce the magic term $3(n^2 + n)$. Of course, this was not foresight at all; we just worked backward initially!

4 A Faulty Induction Proof

Sometimes we want to prove that a statement is true for, say, all integers $n \geq 1$ rather than all integers $n \geq 0$. In this circumstance, we can use a slight variation on induction: prove $P(1)$ in the base case and then prove that $P(n)$ implies $P(n + 1)$ for all $n \geq 1$ in the inductive step. This is a perfectly valid variant of induction and is *not* the problem with the proof below.

False Theorem 3. *All horses are the same color.*

Proof. The proof is by induction. Let $P(n)$ be the proposition that in every set of n horses, all are the same color.

Base case: $P(1)$ is true, because all horses in a set of 1 must be the same color.

Inductive step: Assume that $P(n)$ is true, where n is a positive integer; that is, assume that in every set of n horses, all are the same color. Now consider a set of $n + 1$ horses:

$$h_1, h_2, \dots, h_n, h_{n+1}$$

By our assumption, the first n horses are the same color:

$$\underbrace{h_1, h_2, \dots, h_n}_{\text{same color}}, h_{n+1}$$

Also by our assumption, the last n horses are the same color:

$$h_1, \underbrace{h_2, \dots, h_n, h_{n+1}}_{\text{same color}}$$

Therefore, horses h_1, h_2, \dots, h_{n+1} must all be the same color, and so $P(n+1)$ is true. Thus, $P(n)$ implies $P(n+1)$.

By the principle of induction, $P(n)$ is true for all $n \geq 1$. The theorem is a special case where n is equal to the number of horses in the world. \square

We've proved something false! Is math broken? Should we all become poets?

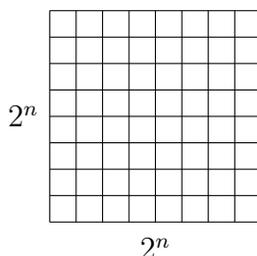
The error in this argument is in the sentence that begins, "Therefore, horses $h_1, h_2, \dots, h_n, h_{n+1}$ must all be the same color." The " \dots " notation creates the impression that the sets h_1, h_2, \dots, h_n and h_2, \dots, h_n, h_{n+1} overlap. However, this is not true when $n = 1$. In that case, the first set is just h_1 and the second is h_2 , and these do not overlap at all!

This mistake knocks a critical link out of our induction argument. We proved $P(1)$ and we proved $P(2) \Rightarrow P(3)$, $P(3) \Rightarrow P(4)$, etc. But we failed to prove $P(1) \Rightarrow P(2)$, and so everything falls apart: we can not conclude that $P(3)$, $P(4)$, etc. are true. And, of course, these propositions are all false; there are horses of a different color.

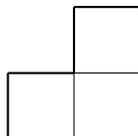
5 Courtyard Tiling

Induction served purely as a proof technique in the preceding examples. But induction sometimes can serve as a more general reasoning tool.

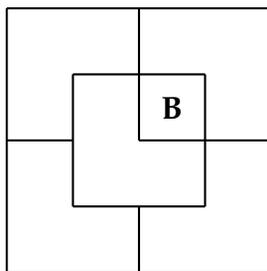
MIT recently constructed a new computer science building. As the project went further and further over budget, there were some radical fundraising ideas. One plan was to install a big courtyard with dimensions $2^n \times 2^n$:



One of the central squares would be occupied by a statue of a wealthy potential donor. Let's call him "Bill". (In the special case $n = 0$, the whole courtyard consists of a single central square; otherwise, there are four central squares.) A complication was that the building's unconventional architect, Frank Gehry, insisted that only special L-shaped tiles be used:



A courtyard meeting these constraints exists, at least for $n = 2$:



For larger values of n , is there a way to tile a $2^n \times 2^n$ courtyard with L-shaped tiles and a statue in the center? Let's try to prove that this is so.

Theorem 4. For all $n \geq 0$ there exists a tiling of a $2^n \times 2^n$ courtyard with Bill in a central square.

Proof. (doomed attempt) The proof is by induction. Let $P(n)$ be the proposition that there exists a tiling of a $2^n \times 2^n$ courtyard with Bill in the center.

Base case: $P(0)$ is true because Bill fills the whole courtyard.

Inductive step: Assume that there is a tiling of a $2^n \times 2^n$ courtyard with Bill in the center for some $n \geq 0$. We must prove that there is a way to tile a $2^{n+1} \times 2^{n+1}$ courtyard with Bill in the center... \square

Now we're in trouble! The ability to tile a smaller courtyard with Bill in the center does not help tile a larger courtyard with Bill in the center. We can not bridge the gap between $P(n)$ and $P(n + 1)$. The usual recipe for finding an inductive proof will not work!

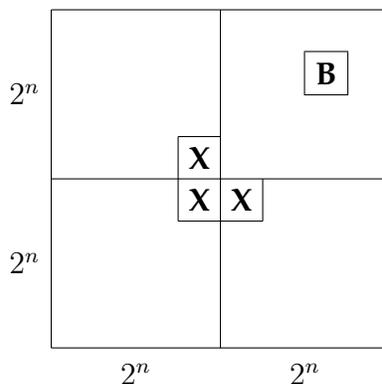
When this happens, your first fallback should be to look for a *stronger* induction hypothesis; that is, one which implies your previous hypothesis. For example, we could make $P(n)$ the proposition that for *every* location of Bill in a $2^n \times 2^n$ courtyard, there exists a tiling of the remainder.

This advice may sound bizzare: "If you can't prove something, try to prove something more grand!" But for induction arguments, this makes sense. In the inductive step, where you have to prove $P(n) \Rightarrow P(n + 1)$, you're in better shape because you can *assume* $P(n)$, which is now a more general, more useful statement. Let's see how this plays out in the case of courtyard tiling.

Proof. (successful attempt) The proof is by induction. Let $P(n)$ be the proposition that for every location of Bill in a $2^n \times 2^n$ courtyard, there exists a tiling of the remainder.

Base case: $P(0)$ is true because Bill fills the whole courtyard.

Inductive step: Assume that $P(n)$ is true for some $n \geq 0$; that is, for every location of Bill in a $2^n \times 2^n$ courtyard, there exists a tiling of the remainder. Divide the $2^{n+1} \times 2^{n+1}$ courtyard into four quadrants, each $2^n \times 2^n$. One quadrant contains Bill (B in the diagram below). Place a temporary Bill (X in the diagram) in each of the three central squares lying outside this quadrant:



Now we can tile each of the four quadrants by the induction assumption. Replacing the three temporary Bills with a single L-shaped tile completes the job. This proves that $P(n)$ implies $P(n+1)$ for all $n \geq 0$. The theorem follows as a special case. \square

This proof has two nice properties. First, not only does the argument guarantee that a tiling exists, but also it gives an algorithm for finding such a tiling. Second, we have a stronger result: if Bill wanted a statue on the edge of the courtyard, away from the pigeons, we could accommodate him!

Strengthening the induction hypothesis is often a good move when an induction proof won't go through. But keep in mind that the stronger assertion must actually be *true*; otherwise, there isn't much hope of constructing a valid proof! Sometimes finding just the right induction hypothesis requires trial, error, and insight. For example, mathematicians spent almost twenty years trying to prove or disprove the conjecture that "Every planar graph is 5-choosable"¹. Then, in 1994, Carsten Thomassen gave an induction proof simple enough to explain on a napkin. The key turned out to be finding an extremely clever induction hypothesis; with that in hand, completing the argument is easy!

¹5-choosability is a slight generalization of 5-colorability. Although every planar graph is 4-colorable and therefore 5-colorable, not every planar graph is 4-choosable. If this all sounds like nonsense, don't panic. We'll discuss graphs, planarity, and coloring in two weeks.