What is a Proof?

Andrew Sack

September 15, 2019

Math is not science. How you come to knowledge in science is through experimentation and observing trends, sometimes known as deductive reasoning. For example, in science we may observe swans throughout our lives and see that they are always white and hence reasonably conjecture "All swans are white." Unfortunately although you have never seen a black swan, they could still exist and just be rare or not be in the part of the world you live in. In fact, there exists a species of swan in Australia that is black.

Let us consider instead a mathematical claim: If a and b are rational numbers (fractions) and if $a \cdot b = 0$ then $a = 0$ or $b = 0$. (In mathematics we consider the statement "A or B is true" to include the possibility that both A and B are true.) If math was science, we may take a bunch of pairs of rational numbers, multiply them together, and notice that the only times we get 0 in the product are when at least one of the factors is 0. However, as mathematicians we are not satisfied. There are infinitely many rational numbers and we have not checked them all. There may be a black swan hidden among them.

To soothe our anxieties, we use so-called "deductive reasoning." In this mode of thought we start with specific assumptions and any claim we make must be shown to be a result of these assumptions by a sequence of logical steps. We call such a sequence a proof because they prove a claim beyond any doubt. Importantly, proofs are arguments and are done in English. (Or any other language, but I only know English.)

Here is an example:

> **Claim:** If a and b are rational numbers then if $a \cdot b = 0$ then $a = 0$ or $b = 0$.
>
> Proof:
>
> If $a = 0$ then we are done.
> If $a \neq 0$ then we can divide by a on both sides of the equation to have $(ab)/a = 0/a$.
> However $(ab)/a = b = 0/a = 0$.
>
> Hence $b = 0$.

As you can see, we have now handled all possible cases in one fell swoop. For the brevity, I did not define what it means to be a rational number within the proof or what it means to divide by a rational number. We in fact used several definitions and other facts implicitly, which you can work out in full details if you feel so inclined or you may see me during office hours if you want me to do it instead.

When we make claims about infinitely many things, an example is insufficient as was the case above. When we make a claim about a finite number of things, examples can be all that is necessary for proof. Sometimes we can also reduce a claim about infinitely many things to a claim about finitely many things and then just use examples.

Here are examples:

> We say that an integer a divides an integer b if there exists an integer c such that $a \cdot c = b$.
>
> We say that a positive integer is *prime* if there are exactly two distinct positive integers that divide it.
>
> Claim: 4 is not prime.
>
> Proof:
>
> $1, 2,$ and 8 all divide 8. (We give 3 examples of distinct integers that divide 8. Although there are more examples, this is sufficient for the proof)
>
> Claim: 5 is prime.
>
> Proof:
>
> 1 and 5 both divide 5.
>
> Now we must show that no other positive integers that divide 5.
> We note that if n is an integer and $n > 5$ then:
>
> - $n \cdot 0 = 0$
> - If $m \geq 1$ then $n \cdot m \geq n \cdot 1 = n > 5$, so $n \cdot m \neq 5$.
> - If $m < 0$ then $n \cdot m < 0$ so $n \cdot m \neq 5$.
>
> Then if 5 has any positive divisors they must be among $1, 2, 3, 4,$ and 5.
>
> $2, 3,$ and 4 do not divide 5 so we are done.

While inductive reasoning does not suffice within mathematics, it still has value. In math research we frequently consider specific examples as inspiration for things to prove or even

for approaches to prove things. Even in your homework you may find it useful to write out some examples when attempting to prove something. They may inspire you.

Some courses in discrete structures like to categorize different proof techniques for pedagogical purposes. I think that this can be useful, but be aware that not all proofs can be categorized so cleanly and many proofs will use many techniques within them. The rest of this page will be examples of proofs of various facts using various techniques, with some commentary. I have attempted to categorize them.

1 Direct Proof

Direct proofs are proofs that come directly from the definitions of things. They tend to follow a pattern like $A \Rightarrow B$. We know A, therefore B. Sometimes there may be many steps such as $A \Rightarrow B$ and $B \Rightarrow C$. We prove A, and therefore we have C.

Here are some examples:

Claim: The sum of an even integer and an odd integer is odd.

Proof.
Recall that we say an integer n is even if $n = 2k$ for some integer k and n is odd if $n = 2k+1$ for some integer k.
Let n be even and m be odd. Then there exist integers k and ℓ such that $n = 2k$ and $m = 2\ell + 1$.
Then $n + m = 2k + 2\ell + 1 = 2(k + \ell) + 1$.
As $k + \ell$ is an integer, $n + m$ is odd. □

Claim: If n is even then n^2 is even. If n is odd then n^2 is odd.

Proof.
If n is even then $n = 2k$ for some integer k.
Then $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.
As $2k^2$ is an integer, n^2 is even.

If n is odd then $n = 2k + 1$ for some integer k.
Then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.
As $2k^2 + 2k$ is an integer, n^2 is odd. □

Claim: If $p, r \in \mathbb{Q}$ and $p < r$ then there exists $q \in \mathbb{Q}$ such that $p < q < r$.

Proof.
Let $p = \frac{a}{b}$ and $r = \frac{x}{y}$ with $a, x \in \mathbb{Z}$ and $b, y \in \mathbb{Z} \setminus \{0\}$

Let $q = \frac{p+r}{2} = \frac{ay+bx}{2by}$. As $ay + bx$ and $2by$ are both integers, q is a rational number.
Then $q - p = \frac{p+r}{2} - \frac{2p}{2} = \frac{r-p}{2}$
As $r - p > 0$, $\frac{r-p}{2} > 0$ so $q - p > 0$ and $q > p$.
Similarly, $r - q = \frac{q-p}{2} > 0$ so $r > q$.
Hence $p < q < r$. □

Claim: If $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$.

Proof.
Recall that we say $X \subseteq Y$ if $\forall x \in X, x \in Y$.
Let $a \in A$.
Then as $a \in A$ and $A \subseteq B$ then $a \in B$.
Then as $a \in B$ and $B \subseteq C$ then $a \in C$.
As a was arbitrary, we have $\forall a \in A, a \in C$. □

Claim: If $f : A \to B$ is injective and $g : B \to C$ is injective then $g \circ f$ is injective.

Proof.
Recall that we say a function $h : X \to Y$ is injective if $h(a) = h(b) \Rightarrow a = b$.
Let $(g \circ f)(a) = (g \circ f)(b)$
Then $g(f(a)) = g(f(b))$. As g is injective, this implies $f(a) = f(b)$.
As f is injective, this implies that $a = b$.
Hence $g \circ f$ is injective. □

2 Proof by Contradiction

Before discussing proof by contradiction, I should talk about the contrapositive. Given a statement $A \Rightarrow B$, there is an equivalent statement $\neg B \Rightarrow \neg A$. If I say "If it is raining then the street is wet", it is equivalent to saying "If the street is not wet, then it is not raining." **Importantly**, this is not equivalent to saying "If it is not raining then the street is not wet." After all, the street may be wet for other reasons.

Proof by contradiction uses the fact that if $\neg A$ is false then A is true. This is known as the law of excluded middle. The negation of $A \Rightarrow B$ is $A \wedge \neg B$. To prove $A \Rightarrow B$ by contradiction we prove that $A \wedge \neg B$ is false.

Proofs using these techniques have a similar feeling and it's common for mathematicians to refer to both as "proof by contradiction." Here are some examples:

Claim: If $a, b \in \mathbb{Q}$ and $a \cdot b = 0$ then $a = 0$ or $b = 0$.

Proof.
Assume by way of contradiction that $a \neq 0$ and $b \neq 0$, but $a \cdot b = 0$.
Then $a \cdot b \cdot \frac{1}{b} = 0 \cdot 1b \Rightarrow a = 0$, a contradiction. □

Claim: Show that an integer n cannot be both odd and even.

Proof.
Assume by way of contradiction that n is both odd and even.
Then there exists an integer k such that $n = 2k$ and an integer ℓ such that $n = 2\ell + 1$.
Then $0 = n - n = 2\ell + 1 - 2k = 2(\ell - k) + 1$.
Then $1 = 2(k - \ell)$.
However if $k - \ell = 0$ then we would have $1 = 0$ a contradiction.
Alternatively if $|k - \ell| \geq 1$ then $1 = 2|k - \ell| \geq 2$, so $1 \geq 2$, a contradiction.
Hence n cannot be both odd and even. □

Claim: If a is rational and b is irrational then $a + b$ is irrational.

Proof.
Assume by way of contradiction that $a + b$ is rational.
Then $b = a + b - a = a + b + (-a)$.
As the sum of two rational numbers is rational, and $-a$ is rational, this implies that b is rational, a contradiction.
Hence $a + b$ is irrational. □

3 Induction/Well-ordering Principle

Ironically I started off this page discussing that math is not inductive and now we come to mathematical induction. While the words are similar, mathematical induction is different from inductive reasoning. Earlier I talked about how the issue with inductive reasoning in mathematics is that you may not handle all examples. But what if you could?

Induction essentially provides a technique for doing so, at least in some circumstances. The way this works is you have a list of statements $S_1, S_2, ...$ You show that S_1 is true and then you show that $S_n \Rightarrow S_{n+1}$. Then you can assert that S_n is true for all n. This is because if $S_n \Rightarrow S_{n+1}$ and S_1 is true then we have $S_1 \Rightarrow S_2 \Rightarrow ...$

Related to induction is the Well-ordering Principle. This states that if S is a non-empty set of positive integers then S has a least element. When trying to prove that P_n holds for all positive integers n, we can say "Let $\mathcal{S}$ be the set of all positive integers such that S_n is false. Assume by way of contradiction that S is non-empty and let k be the least integer in $\mathcal{S}$." Then we show that there is some other integer smaller than k such that S_k is false, which

contradicts the minimality of k. These two techniques are equivalent and we sometimes use whichever is more convenient.

If these descriptions are confusing here is a simple example:

Claim: All natural numbers are even or odd.

Proof.
We handle the base case of 0 first: 0 is even because $0 = 0 \cdot 2$.
Now assume that n is even or odd.
If n is even then $n = 2k$ for some integer k. Hence $n + 1 = 2k + 1$ so $n + 1$ is odd.
If n is odd then $n = 2k + 1$ for some integer k. Hence $n + 1 = 2k + 2 = 2(k + 1)$ so $n + 1$ is even.
Hence $n + 1$ is either even or odd.
By induction, all natural numbers are even or odd. □

Here are some more examples:

Claim: If $a, b \in \mathbb{N}$ and $a \cdot b = 0$ then $a = 0$ or $b = 0$.

Proof.
We will instead prove the contrapositive: If $a \neq 0$ and $b \neq 0$ then $a \cdot b \neq 0$.
Note that $a \neq 0 \Rightarrow a > 0$.
We will do induction on a.
The base case is $a = 1$. If $a = 1$ then $a \cdot b = 1 \cdot b = b \neq 0$.
Now assume that $a \cdot b \neq 0$. Then $(a + 1) \cdot b = ab + b$.
As $ab > 0$ and $b > 0, ab + b > 0$.
Hence $(a + 1) \cdot b \neq 0$.
By induction, the claim is proven. □

Sometimes it's useful to first prove something with induction and then extend it to more general cases:

Claim: If $a, b \in \mathbb{Z} \setminus \{0\}$ then $a \cdot b \neq 0$

Proof.
If $a < 0$ and $b < 0$ then $a \cdot b = (-a)(-b) \neq 0$ and by the case above. (Because $-a, -b \in \mathbb{Z}^+$)
If exactly one of a or b is less than 0, without less of generality assume it is a.
Then $-1 \cdot a \cdot b = (-a)(b) \neq 0$ by the case above. □

Claim: $\forall n \in \mathbb{N}, \sum_{k=0}^{n} k = \frac{n(n+1)}{2}$

Proof.
When $n = 0$ the equation is true because $0 = 0$.
If $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$ then :

$$\begin{aligned}\sum_{k=0}^{n+1} k &= \left(\sum_{k=0}^{n} k\right) + n + 1 \\ &= \frac{n(n+1)}{2} + n + 1 \\ &= \frac{n^2+n}{2} + \frac{2n+2}{2} \\ &= \frac{n^2+3n+2}{2} \\ &= \frac{(n+1)(n+2)}{2}\end{aligned}$$

Hence by induction the claim is true for all $n \geq 0$. □

Claim: $\forall n \in \mathbb{N}, \sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$

Proof.
When $n = 0$ the equation is true because $0 = 0$.
If $\sum_{k=0}^{n} k^2 = \frac{n(n+1)}{2}$ then :

$$\begin{aligned}\sum_{k=0}^{n+1} k^2 &= \left(\sum_{k=0}^{n} k^2\right) + (n+1)^2 \\ &= \frac{n(n+1)(2n+1)}{6} + n^2 + 2n + 1 \\ &= \frac{2n^3+3n^2+n}{6} + \frac{6n^2+12n+6}{6} \\ &= \frac{2n^3+9n^2+13n+6}{6} \\ &= \frac{(n+1)(n+2)(2n+3)}{6}\end{aligned}$$

Hence by induction the claim is true for all $n \geq 0$. □

Claim: $8^n - 3^n$ is divisible by 5 for all $n \in \mathbb{N}$

Proof.
When $n = 0$ we claim that 5 divides 0 which is true because $5 \cdot 0 = 0$.
If $8^n - 3^n = 5k$ for some integer k then

$$\begin{aligned} 8^{n+1} - 3^{n+1} &= 8 \cdot 8^n - 3 \cdot 3^n \\ &= 3 \cdot 8^n + 5 \cdot 8^n - 3 \cdot 3^n \\ &= 3(8^n - 3^n) + 5 \cdot 8^n \\ &= 5k + 5 \cdot 8^n = 5(k + 8^n) \end{aligned}$$

Hence if $8^n - 3^n$ is divisible by 5 then $8^{n+1} - 3^{n+1}$ is divisible by 5.
By induction the claim is true. □

Claim: There does not exist a rational number q such that $q^2 = 2$.

Proof.
Suppose that there exists $q \in \mathbb{Q}$ such that $q^2 = 2$.
If $q^2 = 2$ then $(-q)^2 = q^2 = 2$ so we can assume that q is non-negative. Furthermore $q \neq 0$ because $0^2 = 0 \neq 2$.
Then there exist positive integers $x, y \in \mathbb{Z}^+$such that $\left(\frac{x}{y}\right)^2 = 2$
Let $\mathcal{A}$ be the set of all positive integers n such that there exists an integer m such that $\left(\frac{n}{m}\right)^2 = 2$
By the assumption, $\mathcal{A}$ is non-empty, so by the well-ordering principle, $\mathcal{A}$ has a least element.
Let a be the least element of $\mathcal{A}$ and let b be such that $\left(\frac{a}{b}\right)^2 = 2$
Then $\frac{a^2}{b^2} = 2$ so $a^2 = 2b^2$.
Hence a^2 is even. Now we claim that if a^2 is even then a is even:

> Assume by way of contradiction that a is odd but a^2 is even.
> We showed earlier that if a is odd then a^2 is odd, a contradiction to a^2 being even.
> Hence a is even.

Then we can write $a = 2c$ for some integer c.
So $a^2 = (2c)^2 = 4c^2 = 2b^2$
So $2c^2 = b^2$ and by the same argument as earlier, this shows that b is even.
Hence $\left(\frac{a/2}{b/2}\right)^2 = 2$.
But $a/2 < a$ a contradiction to the minimality of a.
Hence there does not exist a rational number q such that $q^2 = 2$. □

Claim: If $a, b \in \mathbb{Z}^+$ then there exist unique integers q, r such that $0 \leq r < b$ and $a = bq + r$. (Existence and uniqueness of quotient and remainder)

Before I start this proof I should discuss our natural instinct on this sort of problem. Why is 13 divided by 3 equal to 4 with remainder 1. Well it's because there are no 3s left to take away from 1. We essentially want to take away the maximum number of 3s away from 13. In this proof we try to capture that intuition.

Proof.
Let $S = \{n \in \mathbb{Z}^+ | nb > a\}$.

S is non-empty because $ab > a$ (Because both a and b are positive) so $a \in S$
Hence by the well-ordering principle, S has a least element. Furthermore $0 \notin S$ because $0 \cdot b = 0 < a$.
Let $q + 1$ be the least element of S.
We claim that $0 \leq a - bq < b$.
$bq \leq a$ because $q \notin S$ so $a - bq \geq 0$.
$a < b(q + 1)$ because $q + 1 \in S$ so $a < bq + b \Rightarrow a - bq < b$.
Take $r = a - bq$ and hence two such integers q and r exist.

Now suppose $a = bq_1 + r_1$ and $a = bq_2 + r_2$ with $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ and $0 \leq r_1, r_2 < b$.
Without loss of generality assume that $r_2 \geq r_1$.
Then $0 = bq_1 + r_1 - bq_2 - r_2,$ so $r_2 - r_1 = b(q_1 - q_2)$.
Hence b divides $r_2 - r_1$. However $0 \leq r_2 - r_1 < b$ and the only integer divisible by b between 0 and $b - 1$ inclusive is 0.
Hence $r_2 - r_1 = 0$ so $r_2 = r_1$.
Furthermore, $0 = b(q_1 - q_2)$ and as $b \neq 0, q_1 - q_2 = 0$ so $q_1 = q_2$.
Hence q and r are unique. □