Foundational Mathematical Reasoning

Matias Frank Jensen - Århus University

November 3, 2017

Direct proof

A direct proof uses two propositions A, B and show that

$$A \Rightarrow B$$

To do this one almost always goes through a chain of reasoning showing that

$$A \Rightarrow A_1 \Rightarrow ... \Rightarrow A_n \Rightarrow B$$

and by the transitive property of implication one has shown the goal of

$$A \Rightarrow B$$

Example 1

A right-angled XYZ with side lengths x, y, z has area $\frac{1}{4}z^2$. Show that the remaining angels of XYZ is 45°
In this example, the propositions A and B are:

A: The triangle is rightangled with area $\frac{1}{4}z^2$
B: $\angle X = \angle Y = 45°$

It can be proven from the following chain of reasoning starting from both A and B:
The triangle being rightangled implies $z^2 = x^2 + y^2$. For any right triangle the area is $\frac{1}{2}xy$, hence this gives that $\frac{1}{4}z^2 = \frac{1}{4}(x^2 + b^2) = \frac{1}{2}xy$
If a triangle has to equal sides the corresponding angels are equal. Hence, for B to be true it must be true that $x = y \Leftrightarrow x - y = 0$. If A implies that $x - y = 0$, we are done. But

$$\frac{1}{4}(x^2 + y^2) = \frac{1}{2}xy \Leftrightarrow x^2 + y^2 - 2xy = 0 \Leftrightarrow (x - y)^2 = 0 \Leftrightarrow x - y = 0$$

The full chain of reasoning is then

$$A \Rightarrow \frac{1}{4}z^2 = \frac{1}{4}(x^2 + y^2) = \frac{1}{2}xy \Rightarrow x^2 + y^2 - 2xy = 0 \Rightarrow (x - y)^2 = 0 \Rightarrow x - y = 0 \Rightarrow x = y \Rightarrow B$$

Example 2

If n is a odd number, then $4|n^2 - 1$ In this example the propositions A and B are:

A: n is a odd number
B: $4|n^2 - 1$

We will prove this in two different ways.

Proof 1

First we will look at what it requires for B to be true. By the definition of divisibility we have that $4|n^2-1 \Leftrightarrow \exists k \in \mathbb{N} : 4k = n^2 - 1$. So if we can proof the existence of this k, we are done.
Now lets look at what A can tell us. If n is an odd number, there must exist a natural number n' such that $n = 2n' + 1$. This rewriting of n gives that

$$n^2 = (2n'+1)^2 = 4n'^2 + 4n' + 1 \Leftrightarrow n^2 - 1 = 4(n'^2 + n')$$

and we are done. Here we again both analyzed A and B and followed a chain of reasoning from A and B that met in the middle, proving what we needed to prove.

Proof 2

We again start this proof by looking at B and making a factorization:

$$4|n^2 - 1 = (n+1)(n-1)$$

For 4 to divide this product it is enough to show that 2 divides each of the terms. Now we look at A and see if this proposition can help us show that. If n is odd, then surely both $n+1$ and $n-1$ are even, hence they are divisible by 2 and it follows 4 divides $(n+1)(n-1) = n^2 - 1$ which we wanted to show.
The complete chain of reasoning can be written as

$$A \Rightarrow n+1, n-1 \text{ are even} \Rightarrow 4|(n+1)(n-1) \Rightarrow 4|n^2 - 1$$

Proof by contradiction

Proof by contradiction is an extremely powerful proof technique. Given a proposition P, instead of actually proving P, you assume $\neg P$, show that this leads to a contradiction and from that it must follow that $\neg P$ cannot be true, hence P is true.

Example 3

To illustrate proving by contradiction we will look at Euclid's classic and beautiful proof that there are an infinite number of primes.

So, *assume for contradiction* that there are *not* an infinite number of primes. Then there must exist a natural number n such that all primes can be listed as $\mathbb{P} = \{p_1, p_2, ...p_n\}$.
Now we will search for a contradiction. Sometimes you have a good idea beforehand what the contradiction will be, other times you happen to stumble upon it after enough looking. At this point a good idea for a contradiction would be to show that there must be another prime $p \notin \mathbb{P}$. If this p exists, then our assumption that there are only a finite number of primes must be false.
To prove this p exists one needs a good idea. The idea in this case is to look at the number $P = p_1 p_2 \cdots p_n$. Remember that every natural number larger than 1 has at least one prime divisor, so if we find a number where none of the primes in $\mathbb{P}$ divides it, we cannot have accounted for all of them.I postulate that no prime in $\mathbb{P}$ divides $P + 1$.
The question is then how do one prove a property for *all* the members of a set? We do not even now how large n is. n could be 1, it could be 1000, it could be the factorial of the number of particles in

the universe.
The trick is to choose an *arbitrary* element and then proving the property must hold for this. This can actually be reformulated as another proof by contradiction. We want to show that *no* prime p_i in $\mathbb{P}$ divides $P+1$, so for contradiction we assume the opposite. What is the opposite? That for at least one prime $p_i \in \mathbb{P}$, $p_i|P+1$.
So *assume for contradiction* that $\exists p_i \in \mathbb{P} : p_i|\ P+1$. It is not entirely clear by this point what exactly our contradiction is going to be, but hopefully we will find one.
The definition of divisibility gives that $p_i|P+1 \Leftrightarrow \exists k \in \mathbb{N} : p_i k = P+1$. Remember that $p_i|P$, so $P = P'p_i$ for some natural number P'. This results in

$$p_i|P+1 \Leftrightarrow p_i k = P+1 = P'p_i + 1 \Leftrightarrow p_i k - P'p_i = p_i(k-P') = 1$$

However this cannot be the case since $p_i > 1$ and we have our contradiction.
Now we have shown that there cannot exist a prime $p_i \in \mathbb{P}$ so that $p_i|P+1$, hence there must exist at least one other prime p so $p|P+1$, but $p \notin \mathbb{P}$, which is a contradiction to the assumption that we had listed all the primes.
So by contradiction we have now proven that the original assumption that there only are a finite number of primes is false, so there must be an infinite number.

0.1 Example 4

This pro*of is really interesting and very vividly illustrates the concepts a non-constructive proof.
A non-constructive proof shows indirectly that a certain mathematical object must exist but without actually giving an example of such an object.
We are going to show that there exists to irrational numbers x and y such that x^y is rational. This might not be a proof by contradiction but I just had to include it because it is so cool.
Consider the number $\sqrt{2}^{\sqrt{2}}$. If this is rational then we are done. But what if it is irrational? Then consider

$$\sqrt{2}^{\sqrt{2}^{\sqrt{2}}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2$$

which most certainly is rational. So either way one of the two is an example of what we wanted to show, but we have no idea which one it is. It turns out that $\sqrt{2}^{\sqrt{2}}$ is irrational but proving it requires a lot of rather deep mathematical theory first which could take years to understand but our little non-constructive proof here can be fully understood in a few minutes.

Proof by induction

Induction is also one of the fundamental cornerstones of mathematical reasoning. It is a very clever way of proving a property of elements of a countable infinite set.
If you want to show a proposition holds for every $n \in \mathbb{N}$ it is infeasible to prove it for every n individually. Instead, you prove it for some base case n, and then you (usually) show that implies the property holds for $n+1$. Thereby it must also hold for $n+2, n+3, ...$ and must therefore hold for every single $m \geq n$. If you base case is $n = 1$, the property holds for all $n \in \mathbb{N}$.

Example 4

The sum of the first n numbers is n(n+1)/2
To show this by induction we first choose a base case. For $n = 1$ it certainly holds, since $1 =$

$1 \cdot (1+1)/2$

Now for the induction step. Assume for a given n that

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

. Then we want to show this implies that

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

By the induction hypothesis we have that

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

This shows what we needed. So because we explicitly showed sum formula was true for $n = 1$ it must be true for all $n \in \mathbb{N}$.

In this case we actually had a goal already, we had been given the correct formula to show and then we could prove it. But what about a different situation where you do not know what you want to prove beforehand? Then it is usually about looking for a specific pattern and see if you can spot the general formula/property.

Example 5

What is the last digit of $3^{1,000,000}$*?*
This might not at first hand seem like a problem induction could solve since we are not looking at any property to hold for all natural n. But what if we by induction could calculate the last digit of $3^n, \forall n \in \mathbb{N}$. Then we certainly would also be able to calculate the last digit of $3^{1,000,000}$.
The first powers of 3 are $1, 3, 9, 27, 81, 243, 729, 2187, 6561$ so the last digits are $1, 3, 9, 7, 1, 3, 9, 7, 1$. It certainly looks like there is a pattern where the last digits cycles between $1, 3, 9, 7$ in that order. Now to prove this is the case by induction!
What can we say about a number k that ends in a 1? That means k is of the form $k = 10k' + 1$. Then $3k = 3(10k' + 1) = 30k' + 3$. Notice that the $30k'$ term does not have an effect on the last digit since this ends in a 0. So the last digit of a number ending in 1 is always 3. What about a generel last digit of d? Assume the number k ends in a $d, 0 \leq d \leq 9$, then $k = 10k' + d$ for some natural number k'. $3k = 3(10k' + d) = 30k' + 3d$ and again, the $30k'$ has no contribution to the last digit, the last digit is completely determined by $3d$. So to determine the last digit of $3k$ one only needs to know the last digit of k.
That means we are almost done. But what is our induction hypothesis precisely? We want to show the last digits has a cycle of 4 through the numbers $1, 3, 9, 7$, here is a way to formalize that notion and formulate a proof.

Induction hypothesis

For all $n \in \mathbb{N}$ the last digit of

$$3^{4n} \text{ is } 1$$
$$3^{4n+1} \text{ is } 3$$
$$3^{4n+2} \text{ is } 9$$
$$3^{4n+3} \text{ is } 7$$

Base case
For $n = 0$ we have that $3^0 = 1, 3^1 = 3, 3^2 = 9, 3^3 = 27$, so the induction hypothesis is true for $n = 0$.

Induction step
Assume the induction hypothesis is true for n. Then we need to show it is true for $n + 1$. By the induction hypothesis the last digit of 3^{4n+3} is 7. But we argued before that the last digit of $3k$ is completely determined by the last digit of k, so the last digit of $3^{4(n+1)} = 3 \cdot 3^{4n+3}$ is 1 because the last digit of 3^{4n+3} is 7. By the same argument the last digit of $3^{4(n+1)+1} = 3 \cdot 3^{4(n+1)}$ is 3, the last digit of $3^{4(n+1)+2} = 3 \cdot 3^{4(n+1)+1)}$ is 9 and the last digit of $3^{4(n+1)+3} = 3 \cdot 3^{4(n+1)+2}$ is 7.
This proves the desired.

Now we have a complete formula for the last digit of 3^n. Since $1,000,000 = 4 \cdot 250,000$ the last digit of $3^{1,000,000}$ must be 1.

Proving intuitions from axioms/definitions

All math is build upon axioms and definitions. That is, we assume or decide something is true, and then from that discover the consequences from those definitions and thereby build our mathematical knowledge.
These axioms and definitions usually comes from an intuition we have about something that must be true. Then the mathematician formalizes this intuition and finds a small set of definitions that (usually) forces one's intuitions to be true. From that a slew of other facts and connections tend to follow and one has developed a deeper and broader understanding of the subject at hand. I will now illustrate this through an elaborate example.

The goal of this sections is to prove the well-known rules of exponentiation such as $a^{\frac{1}{2}} = \sqrt{a}$, $a^{-n} = \frac{1}{a^n}$ and so forth only from two simple definitions. The following two definitions alone are enough to be able to define $a^{\frac{n}{m}}$ for all real a and natural numbers n, m and in the process of discovering this one will (hopefully) develop a good understanding of exponentiation.

Intuitively exponentiation is first defined only for positive natural numbers such that $a^n = \underbrace{a \cdot a \cdots a}_{n}$ and ecapsulating this behavior can be done by the following definitions:

$$a^1 = a \tag{1}$$
$$a^{p+q} = a^p \cdot a^q \tag{2}$$

As of now we can only give meaning to a^1, for all other $p \neq 1$, a^p makes no sense. Lets fix that one step at a time.

First note that $a^2 = a^{1+1} = a^1 \cdot a^1 = a \cdot a$ where the second equality comes from 2 and third from 1, so the definitions force our intuition to be true for a^2. This can be used to deduce that $a^3 = a^{2+1} = a^2 \cdot a^1 = a \cdot a \cdot a^1 = a \cdot a \cdot a$ so our intuition is true for a^3 as well. We are now ready to prove the general fact that

$$a^n = \underbrace{a \cdot a \cdots a}_{n}$$

which will be done by induction.

Induction base
$a^1 = a$ by rule 1

Induction hypothesis
Assume for some positive natural number n that $a^n = \underbrace{a \cdot a \cdots a}_{n}$

Induction step

$$a^{n+1} = a^n \cdot a^1 = a^n \cdot a = \underbrace{a \cdot a \cdots a}_{n} \cdot a = \underbrace{a \cdot a \cdots a}_{n+1}$$

First equality follows from 2, second equality from 1 and third from the induction hypothesis.

Since we have a base case and proved the induction step from the induction hypothesis we have shown the desired.
Take a little moment to appreciate the fact that we have now expanded our understanding of a^k from only knowing what it meant for $k = 1$ to now understanding it for all $k \in \mathbb{N}$.
What about 0? The first intuition one has about exponentiation doesn't help to define a^0, but when intuition fails our definitions should hopefully help. Notice that

$$a = a^1 = a^{1+0} = a^1 \cdot a^0 = a \cdot a^0$$

using rule 2 and 1 at equality 3 and 4 respectively. So $a^0 = 1$. We have now taken the first step away from the original intuition and expanded our understanding beyond that. But what about negative integers. What does a^{-1} mean? Using the fact that $a^0 = 1$ one get that

$$1 = a^0 = a^{1+(-1)} = a^1 \cdot a^{-1} = a \cdot a^{-1} = 1 \Leftrightarrow a^{-1} = \frac{1}{a}$$

Reusing this trick for a^{-2} we can deduce that

$$1 = a^0 = a^{2+(-2)} = a^2 \cdot a^{-2} = 1 \Leftrightarrow a^{-2} = \frac{1}{a^2}$$

and for a generel n we get

$$1 = a^0 = a^{n+(-n)} = a^n \cdot a^{-n} = 1 \Leftrightarrow a^{-n} = \frac{1}{a^n}$$

(Notice that this fact holds for all real numbers, not just integers)
Now we can define a^n for ever integer, positive, negative or 0!
Turning to fractions we will look at $a^{\frac{1}{2}}$. This is another great example of how ones original intuition do not really help. But by clever use of rule 1 and 2 we can deduce

$$a = a^1 = a^{\frac{1}{2}+\frac{1}{2}} = a^{\frac{1}{2}} \cdot a^{\frac{1}{2}} = a \Leftrightarrow a^{\frac{1}{2}} = \sqrt{a}$$

By induction on $n \in \mathbb{N}$ one can prove that generally $(a^m)^n = a^{mn}$. Using this fact gives

$$a = a^1 = a^{\frac{n}{n}} = (a^{\frac{1}{n}})^n = a \Leftrightarrow a^{\frac{1}{n}} = \sqrt[n]{a}$$

Going from unit fractions to arbitrary fractions is now easy

$$a^{\frac{m}{n}} = (a^{\frac{1}{n}})^m = (\sqrt[n]{a})^m$$

and for negative fractions using the results we have discovered so far we end with

$$a^{-\frac{m}{n}} = \frac{}{a^{\frac{m}{n}}} = \frac{1}{(\sqrt[n]{a})^m}$$

At the beginning we only had two rules and could only explicitly give meaning to a^1, for all other exponents p we did not know what to make of a^p. By first expanding our knowledge to a^n for all natural n, then to a^0, then to all negative integers to a^{-n}, then unit fractions $a^{\frac{1}{n}}$ we ended up with being able to define a^q for every single rational number q.
This is the power of mathematical reasoning. One can start with a simple intuition, formalize it and then discover a whole new landscape in the world of mathematics.

Problems

Direct proofs

Definition
A natural number n is odd if there exists a natural number k such that $n = 2k + 1$. A natural number is even if there exists a natural number k such that $n = 2k$

Problem 1
If a number n is even, then n^2 is also even

Problem 2
The sum of two odd numbers is even

Problem 3
The sum of an odd and even number is odd

Problem 4
The square of an odd number is odd

Problem 5
Proof that $\sum_{i=0}^{n} a^i = \frac{a^{n+1}-1}{a-1}$

Problem 6
The sum of two rational numbers are rational

Problem 7
Every odd number is the difference of two square numbers

Proof by Contradiction

Problem 8
Prove there is no smallest, positive rational number

Problem 9
If $b \in \mathbb{Z}$ and $k|b$ for every $k \in \mathbb{N}$, then $b = 0$

Problem 10
If a and b are positive real numbers, then $a + b \geq 2\sqrt{ab}$

Induction proofs

Problem 11
Every tree with n nodes has exactly $n - 1$ edges

Problem 12
A full binary tree of height h has $2^h - 1$ nodes and $2^h - 2$ edges

Problem 13
Prove by induction on n that $(a^m)^n = a^{mn}$ for all $n \in \mathbb{N}$

Problem 14
Prove by induction on n that $a^{-n} = \frac{1}{a^n}$ for all $n \in \mathbb{N}$

0.2 Miscellaneous

Problem 15
Prove that $a^{p-q} = \frac{a^p}{a^q}$

Problem 16
Prove that $a^{\frac{p}{n}} = \sqrt[n]{a^p}$ for $p \in \mathbb{Q}$ and $n \in \mathbb{N}$