Introduction to Mathematical Proofs

School of Mathematics and Actuarial Science University of Leicester

This document is meant to be used in conjunction with "What to expect from Leicester Maths" or "Transition from A-level to Univesity Mathematics: your initial guide".

Proof is an important part of mathematics which allows mathematicians to say that something is absolutely true and will be true forever, even if we invent some new machinery or technology or... This is what distinguishes (pure) maths from empirical sciences. You will meet proofs, in the context of mathematically exact definitions and results which hold within the corresponding mathematical theory, in many of your first year lecture courses. There are many different kinds of proofs, and this document will introduce some of them, using material you know from school. Our aim is for you to meet the idea of proof in the context of familiar material, so you are not overwhelmed with an "everything is new" situation in the first weeks of your lectures. Therefore it is in your own interest that you should work through at least a part of this document:

Aim to try at least the tasks and exercises from the section "Direct proof", and ideally a little more.

Note that each section in this document is very short, and that is on purpose. It's just to get you thinking a bit about these concepts. If you want to delve more deeply into proof and different forms of proof, we recommend the Tarquin book "Understanding Proof", given in the resources list in "Transition from A-level to University Mathematics: your initial guide".

This document is just meant to give you a taster of what is to come. Don't worry if you find the concepts hard. They are hard, and you will keep learning more and more about them throughout your studies. But having a little taster of some of the concepts now, even if you do not fully understand them, will help you when you get here, exactly because the concepts are hard. So seeing them several times in different ways can be very helpful.

What are we proving?

Proof is needed when we make mathematical statements that we claim are always true (rather than just for one specific example, say). Usually these will be statements that are useful in other contexts. It includes statements of formulae for calculations, but also other types of statement, as you will see in the examples.
In mathematics, we always first have to say what we *assume*. What is our starting point? And then a result, which we can call **Theorem** or **Proposition**, is a statement of the form "If we make the assumption P, then Q will always be true.", or said shortly: "If P, then Q", or "P implies Q", written often as "$P \Rightarrow Q$". You will see lots of examples in the document. So a result has two parts: the **assumption**, which is our starting point, setting out which situation we are in, and the **conclusion**, telling us something that is true within the context of that starting point/assumption.

Why precision is important

In our everyday language, we are not very careful about the uses of "if ... then ... " and their meaning. For example, a parent might say to their child: "You can have ice-cream if you eat your dinner." Now what they *actually* mean is "You can have ice-cream *only if* you eat your dinner." or *if and only if*. Meaning: if you don't eat your dinner, you cannot have ice-cream. In maths, if we are imprecise like that, we get into a lot of trouble. Consider two examples: a non-maths one and a maths one.

Example: We know that
- ◇ Every cat is a mammal.
- ◇ There are other mammals that are not cats.

So we can say: *If Miri is a cat, then Miri is a mammal.*
But we cannot say: *If Miri is a mammal, then Miri is a cat.*
(She might be a dog or a whale or...)
We can also not say *If Miri is not a cat, then Miri is not a mammal.*
(She might be a dog or a whale or...)
So we can only make a deduction in one direction.
We can also say: *If Miri is not a mammal, then Miri is not a cat.*
Since every cat is a mammal, without being a mammal, Miri has no chance of being a cat.

Look at the section "proving the contrapositive" to explore this idea more.
If you compare this to the ice-cream example, if we were strictly mathematical about it, then "if you eat your dinner then you can have ice-cream" does not say anything about the situation when you don't eat your dinner: maybe you can have ice-cream anyway! (Though children know very well that parents don't mean it that way...)

Task: Which of the following statements is true? (Look at the end of the document for the correct answers after you have thought about this.)
In all of them, n is some integer.
- ◇ If n is a multiple of 4, then n is even.
- ◇ If n is even, then n is a multiple of 4.
- ◇ If n is not a multiple of 4, then n is not even.
- ◇ If n is not even, then n is not a multiple of 4.

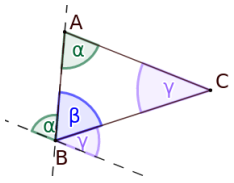
This should show you that it is very important to get the direction of "if ... then ..." right!

Direct proof

A direct proof is the most straight-forward way of proving something. It starts with the assumption and goes with logical deductions directly to the conclusion.

Proposition: *The sum of the angles in any triangle (in the plane) is* 180°.

Proof. Take any triangle ABC. Extend the sides at one vertex, and draw a line through the vertex parallel to the third side. Then all three angles appear next to each other and on one side of a straight line, so they add up to 180°. □



Remark: This result doesn't look much like "If P then Q". To make it look like that, we can rewrite it as "If T is a triangle in the plane, then the angles of T add up to 180°." So the assumption is that T is a triangle, and the conclusion is that its angles add up to 180°. This makes it a bit more clunky as a sentence, but it does make very clear what we are given and what we are trying to show.

Many proofs in Euclidean geometry are direct proofs. Here is another example, not with geometry:

Proposition: *The sum and product of two rational numbers are rational.*

Proof. Let $a = \frac{m}{n}$ and $b = \frac{k}{l}$ be two rationals, with m, n, k, l integers and $n, l \neq 0$. Then we have

$$a + b = \frac{ml + kn}{nl} \qquad \text{and} \qquad ab = \frac{mk}{nl}$$

where ml, kn, nl and mk are products of integers, so integers, and $nl \neq 0$ as the product of non-zero numbers. So the sum and product are again quotients of integers, so they are rational. □

You see that we are being very direct: just take the two numbers, add them, and see that the result is still rational.

Task: What is the assumption here and what is the conclusion? Think about this yourself, and then have a look at the end to see what we think.

Your turn

Using the above as a guide, try if you can find a direct proof for these statements. It does not matter if you can't immediately do it, or if you get completely stuck, the important point is just for you to think about it. We won't give solutions (you don't *need* to know these proofs, that's not the point), but we'll give some hints at the end which you can look up if you're really stuck and want to get a little bit further yourself.

1. Prove that if n is even then n^2 is even.
2. Prove that for all natural numbers n, $4(n^2 + n + 1) - 3n^2$ is a perfect square.

Showing the contrapositive

Remember that in the "Miri is a mammal" example, there was one version of rewriting the sentence that was still true. Was it an accident, or will that always be the case? Let's explore.
Let us write "$P \Rightarrow Q$" for "The statement P implies the statement Q", and "not P" for "the opposite of P". Then if $P \Rightarrow Q$ is our original statement, the statement "not $Q \Rightarrow$ not P" is called the **contrapositive**. Let's see some examples:

- ◇ The contrapositive of "If Miri is cat then Miri is a mammal" is "If Miri is not a mammal, then Miri is not a cat".
- ◇ The contrapositive of "If n is a multiple of 4 then n is even" is "If n is not even, then n is not a multiple for 4".

In both of those examples, both the statement and its contrapositive are true. Let's have some other examples.

- ◇ The contrapositive of "If Koko is a gecko then Koko is a mammal" is "If Koko is not a mammal then Koko is not a gecko".
- ◇ The contrapositive of "If n is a multiple of 3 then n is even" is "If n is even then n is a multiple of 3".

In these two examples, both statements are false. Geckos are not mammals, and if Koko is not a mammal, he might well be a gecko. Or of course he might be a crocodile. Similarly if n is a multiple of 3, we cannot say for sure whether it is even or not, so the "If P then Q" statement is false. n might be 3, or it might be 6. So it might be even, but we can't say for sure.
In all these examples, the statement and its contrapositive are either both true or both false. Let's see if we can explain why this is:

The only way we know that $P \Rightarrow Q$ is *false* is if we can show an example where P is true but Q is false. So for $P \Rightarrow Q$ to be a true statement, if Q is false, then P definitely also has to be false. So "not Q implies not P" must be true for $P \Rightarrow Q$ to be true. And if "not Q implies not P" is true, then by the same argument, "not not P implies not not Q" must be true, in other words $P \Rightarrow Q$ must be true. So both of these statements always have the same truth value (true or false).
So we can use this to prove "$P \Rightarrow Q$" by actually proving "not $Q \Rightarrow$ not P".
To see an example of this proof method, we will need to know what a prime number is.

Definition: A **prime number** is a positive integer $p > 1$ whose only (positive) integer factors are 1 and p.

Proposition: *Every prime number is either odd or* 2.

Here P is "n is prime", and Q is "n is odd or $n = 2$".

Proof. Let $n > 0$ be an integer. If n is neither odd nor 2 (not Q), then $n = 2k$ for some integer $k \neq 1$. So n is not prime. (not P). □

Your turn

Using the above as a guide, try if you can find a "proof by proving the contrapositive" for these statements. Again: It does not matter if you can't immediately do it, or if you get completely stuck, the important point is just for you to think about it. We won't give solutions, but we'll give some hints at the end which you can look up if you're really stuck and want to get a little bit further yourself.

1. Prove that if n^2 is odd then n is odd.
2. Prove that if $a + b$ is even, then a and b have the same parity (they are both even or both odd).

Just to wrap up this section or point out common mistakes: we saw that "If Miri is a mammal then Miri is a cat" is not the same statement as "If Miri is a cat then Miri is a mammal". So given $P \Rightarrow Q$, turning it round the other way to $Q \Rightarrow P$ is not the same statement! This $Q \Rightarrow P$ is called the **converse** of $P \Rightarrow Q$. The converse and the original statements are different statements. Sometimes they may both be true, but sometimes not!

Example:
- ◇ If P is "$n = 2k$ for some integer k" and Q is "n is even", then both $P \Rightarrow Q$ and its converse $Q \Rightarrow P$ happen to be true.
- ◇ But if P is "n is a multiple of 4" and Q is "n is even", then the statement $P \Rightarrow Q$ is true, but it's converse $Q \Rightarrow P$ is not true! Think of $n = 2$ to show that it is not.

Confusing a statement with its converse is a very common mistake in maths, so keep it in mind for your studies.

Proof by contradiction

This type of proof is also called "Reductio ad absurdum". We claim a statement P. To prove it by contradiction, we assume "not P" and deduce a contradiction (to something we know is true).
Or: We claim $P \Rightarrow Q$. We assume "P and not Q" and show a contradiction.
When we get this contradiction to something we know, the world collapses... but of course it actually doesn't, so our assumption must have been wrong all along.

Proposition: *Let $n \geq 0$ be an integer. If n^2 is even (P) then n is even (Q).*

Proof. Suppose n^2 is even and n is odd. (P and not Q). So $n = 2k + 1$ for some integer k. But then

$$n^2 = (2k+1)^2 = 2(2k^2 + 2k) + 1$$

is odd. Contradiction to P.
So we know our assumption must be false, so in fact if n^2 is even then n is even. □

Task: Think about: what is the difference between this and showing the contrapositive?

Another example uses rational and irrational numbers.

Definition: An **irrational number** is a real number which is not a rational, i.e. a fraction.

Proposition: *$\sqrt{2}$ is irrational.*

Proof. Suppose $\sqrt{2} = \frac{m}{n}$ is rational. (not P). Then we can assume wlog (without loss of generality) that $m, n > 0$ do not share any factors (as we could just cancel those out of the fraction). (Something we know is true.) Then

$$\begin{aligned} & 2 = \frac{m^2}{n^2} \\ \iff \quad & 2n^2 = m^2 \end{aligned}$$

So m^2 is even, and we have shown that this means that m is even. So $m = 2k$ for some integer k. Then

$$\begin{aligned} & 2n^2 = 4k^2 \\ \iff \quad & n^2 = 2m^2 \end{aligned}$$

so n is also even. This is a contradiction to the fact we know that m and n don't share a factor.
So in fact our assumption was wrong, and $\sqrt{2}$ is not a rational, so an irrational. □

Task: Could we have done this proof by contrapositive instead? It does look different to the first example.

Your turn

Using the above as a guide, try if you can find a proof by contradiction for these statements.

1. Prove $\sqrt{3}$ is irrational.
2. Prove that there is no greatest even integer.

Proof by Induction

Some of you may have met this in school, and you will definitely meet it again at university. It will be part of at least one, maybe two courses in your first semester, so you have time to learn it then; but any headstart can do you no harm. But don't worry if you don't understand this now: you will have plenty of time to learn it.

We want to prove a statement $A(n)$ for all natural numbers n. We do two steps:

Induction beginning (Anchor, or base case): Prove $A(1)$ is true. (or maybe $A(0)$).

Induction step: Assume that $A(n)$ is true (**Induction hypothesis**) and prove $A(n+1)$. I.e. prove $A(n) \Rightarrow A(n+1)$.
Then $A(n)$ is true for all natural numbers n.

Task: At the moment, perhaps we just take for granted that this works, and use it as a kind of "incantation". Think about *why* this proof method works! This is the kind of questions mathematicians like to ask and answer. You will learn this at Uni, so don't be worried if you can't come up with the reason on your own. Just thinking about it a little bit can help you understand it later.

Proposition: *For any natural number* n, $\sum_{k=1}^{n} k = \frac{1}{2}n(n+1)$.

We expect you to be comfortable with the sigma sum notation. If you are not, you should go back to your school material and look at it.

Proof. **Induction beginning** $n = 1$: We have $\frac{1}{2} \cdot 1 \cdot 2 = 1$ so this is true.
Induction step $A(n) \Rightarrow A(n+1)$: Assume $\sum_{k=1}^{n} k = \frac{1}{2}n(n+1)$. (Induction hypothesis). Then

$$\begin{aligned}\sum_{k=1}^{n+1} k &= \sum_{k=1}^{n} k + (n+1) = \frac{1}{2}n(n+1) + (n+1) \\ &= (n+1)(\frac{1}{2}n + 1) = \frac{1}{2}(n+1)(n+2).\end{aligned}$$

So by induction we are done. □

You will notice that when we are proving the induction step, we are using a direct proof. So these proof techniques are not all disjoint, some may have subparts where we use a different technique.

Your turn

Using the above as a guide, try if you can find a proof by induction for these statements.

1. (Sum of odd squares) Prove that for any natural number n,

$$\sum_{k=1}^{n}(2k-1)^2 = \frac{1}{3}(4n^3 - n).$$

2. (Sum of geometric progression) Prove that for all natural numbers n,

$$\sum_{k=1}^{n} ar^{k-1} = a\frac{1-r^n}{1-r}.$$

If and only if

What does "P if and only if Q" mean? It is also written as "$P \iff Q$" or as "P iff Q".
It is really two statements: $P \Rightarrow Q$ and $Q \Rightarrow P$. That means you have to prove both. Or you have to make sure that all the steps in your proof work both ways round, which is sometimes harder to convince oneself of.

Proposition: *Let $n \geq 0$ be an integer. Then n^2 is even if and only if n is even.*

Proof. We have already proved that n^2 even $\Rightarrow$ n even.
If n is even, then $n = 2k$ for some integer k. Then $n^2 = 4k^2$ is also even. □

Proposition: *Let x be a real number. Then $x^2 + 2x - 15 - 0$ if and only if $x = 3$ or $x = -5$.*

Proof. $x^2 + 2x + 15 = (x + 5)(x - 3)$, so if $x = 3$ or $x = -5$, then definitely $x^2 + 2x + 15 = 0$.
For the other direction, we use a proof by contrapositive: if x is not 3 or -5, then $x^2+2x+15 = (x + 5)(x - 3)$ is definitely not 0.
Notice that what we are really using here is that if you multiply two non-zero numbers, you still get a non-zero number. □

Giving Counterexamples

To prove that something is always true, or true for any number n, or something of that kind, we can't just use an example. (Though examples might help us to find a proof.) To show that something is *not* true, it is enough to give *one* concrete counterexample.

Question: Is $n^2 + n + 41$ prime for all posititive integers n?

Proof. No: $n = 41$ gives $41(41 + 1 + 1) = 41 \cdot 43$ which is not prime. □

If you start trying the first few values of n, as one would do, you might be a false impression:

- $1^2 + 1 + 41 = 43$ is prime.
- $2^2 + 2 + 41 = 47$ is prime.
- $3^2 + 3 + 41 = 53$ is prime.
- $4^2 + 4 + 41 = 61$ is prime.
- $5^2 + 5 + 41 = 71$ is prime.

So this is also a very good example for you to see that you can't prove a general statement by looking at some cases. As an additional challenge, you might want to find out what is the smallest n such that $n^2 + n + 41$ is not a prime.

Finding mistakes

When you are learning maths, it is important that you can read through your own argument again and find any mistakes. Everyone makes mistakes, this is fine, and in fact helps us learn. But spotting mistakes is also a very good skill to practise.
What is wrong with the following argument?

Proposition: *Every bear has the same colour.*

"Proof" by induction
Induction beginning $n = 1$: One bear has the same colour as itself. Correct.
Induction step $A(n) \Rightarrow A(n+1)$: Suppose any n bears have the same colour, and now we have $n+1$ bears. Take the first n bears: they all have the same colour. Now take the last n bears: they also have the same colour. But these two sets overlap, so that tells us that all bears have the same colour.

We know that there are Grizzy bears, brown bears, black bears and polar bears, so clearly the statement is not true. But where did we make our mistake? It is very easy to make such a mistake, so part of studying maths at university is also to train your brain so that eventually you are tuned into these sorts of subtleties and can find out where this went wrong.

If you can't work it out by yourself or discussing with friends once you get here, ask either the Elements of Number Theory lecturer, or your personal tutor, to discuss it with you.

Hints

Why precision is important

- ◇ *If n is a multiple of 4, then n is even.* This is true. If you work through the "Direct Proof" section, you should be able to prove this.
- ◇ *If n is even, then n is a multiple of 4.* This is not true. A counterexample is 2: 2 is even, but not a multiple of 4. (This statement is the converse of the first statement.)
- ◇ *If n is not a multiple of 4, then n is not even.* This is not true. A counterexample is 2: 2 is not a multiple of 4, but it is even. (This statement is the contrapositive of the second statement.)
- ◇ *If n is not even, then n is not a multiple of 4.* This is true. It is the contrapositive of the first statement.

Direct proof

- ◇ In "The sum and product of two rational numbers are rational.", the assumption is "two numbers a and b are rational numbers", and the conclusion is "the numbers $a + b$ and $a \cdot b$ are also rational numbers".
- ◇ Hint for "n even $\Rightarrow$ n^2 even": How can you write n if you know it is an even number?
- ◇ Hint for "$4(n^2 + n + 1) - 3n^2$ is a perfect square": Can you simplify this expression, until it looks like (something)^2?

Showing the contrapositive

- ◇ Hint for "n^2 even $\Rightarrow$ n even": First think about what the contrapositive is that you want to prove. Then remember the hint from previously: can you write the number in a certain way if you know it is even, and in a certain way if you know it is odd?
- ◇ Hint for "$a + b$ even $\Rightarrow$ a, b same parity": What is the contrapositive of this? So what is the opposite of "a and b have the same parity"?

Proof by contradiction

- ◇ Difference between proof by contradiction and proving the contrapositive: maybe it's sometimes just a matter of phrasing the assumption? Think about this suggestion in the two examples given so far.
- ◇ $\sqrt{3}$ is irrational: Follow the proof for $\sqrt{2}$, but be careful that you think about where you used 2 where you now have to use 3. This thinking about "where did I use this particular bit of information" is an essential attitude which you will have to learn to adopt when you look at proofs.
- ◇ What would a largest even number look like? Can you make a bigger one?

Proof by induction

You will come across these two again if you do the Elements of Number Theory course, and possibly also in other courses. So if you get too stuck, you can leave it until then.

Finding mistakes

- ◇ The bear problem: What happens when you have two bears?