In mathematics, the truth of propositions is established by giving a mathematical proof. If there is no proof, then we do not regard the proposition as true, no matter how "obvious" it may look. Today we will talk about what a mathematical proof is and how you may go about finding one.

The good news is that there are very clear and stringent rules about what qualifies as a mathematical proof. Two economists may debate vigorously about economic truth: One could make a case that raising taxes would improve the economy, while the other one might argue that lowering them would have that effect. A prosecution lawyer might try to convince a jury that the accused broke the law, while a defence lawyer would argue that he didn't. In contrast, mathematicians do not have unsettled debates about the *truth* of propositions.[1] If a proposition is claimed to be true, it better come with a proof. Any mathematician (with sufficient training in his or her specialty) ought to be able to verify this proof as correct.

While *verifying* the correctness of a proof is a skill you can master with some effort and self-discipline, *creating* proofs is a completely different story. Mathematics is full of propositions that nobody knows how to prove. For some, like Goldbach's conjecture, the search for a proof has been going on for hundreds of years. In 1998 the Clay Mathematics Institute collected seven famous propositions and offered a 1 million US Dollar prize for each proof. So far only one has been proven. (The prize money was refused.)

Coming up with proofs is not completely dark magic. There are general guidelines for what kind of strategy might help with what type of proposition. However, it is important to remember that — unlike, say, the recipe you learn in school for calculating square roots — these are not guaranteed to succeed.

1 What is a proof?

A *proof* of a proposition is a sequence of *logical deductions* from *axioms* and previously proved propositions that concludes with the proposition in question.

Instead of trying to explain, in general, what axioms and logical deductions are, let us see an example of a proof. Do not worry how someone came up with this proof. For now, let's just contemplate it.

First we need to state the proposition that we intend to prove. A proposition for which a (correct) proof is given is called a *theorem*. Before we state our theorem, we need to *define* a few concepts that will show up in it.

The theorem I have in mind is about friendships. Let's call two people *strangers* if they are not friends. A *group of friends* is a collection of people in which every two of them are friends, and a *group of strangers* is a collection of people in which every two are strangers.

[1] Mathematicians do argue about all sorts of things, it is just that the truth of propositions is not one of them.

Theorem 1. *Every collection of 6 people includes a group of 3 friends or a group of 3 strangers.*

Proof. Let a denote one of the six people. The proof is by case analysis. We consider two cases:

- **Case 1:** a is friends with at least 3 other people in the collection.
- **Case 2:** a is a stranger to at least 3 other people in the collection.

One of these two cases must hold: There are 5 people besides a, and these are divided into friends of a and strangers to a. The bigger group has at least 3 people.

Now let's discuss Case 1. Let's give the collection of people who are friends with a a name – call it F. We consider two subcases:

- **Subcase 1.1:** At least two people within F are friends. Let's call them b and c. Then a, b, and c form a group of 3 friends.
- **Subcase 1.2:** No two people within F are friends. Take any three people in F. They form a group of 3 strangers.

We conclude that the Theorem holds in Case 1.

We are left with Case 2. Let's give the collection of people who are strangers to a a name – call it S. We consider two subcases:

- **Subcase 2.1:** At least two people within S are strangers. Let's call them b and c. Then a, b, and c form a group of 3 strangers.
- **Subcase 2.2:** No two people within S are strangers. Take any three people in S. They form a group of 3 friends.

The theorem also holds in Case 2, and so it holds in all the cases. □

Theorem 1 talks about *collections* of people and *friendships* among people. The axioms are true propositions about collections and friendships that we view as self evident. For example, two axioms about friendships are

Axiom 1. *For every person x, x is not friends with x.*

Axiom 2. *For any two people x and y, if x and y are friends, then y and x are also friends.*

Axioms about collections of people might say things like

Axiom 3. *For all collections X and Y, if Y has more people then X, then there exists a person in Y that is not in X.*

Axiom 4. *For all collections X and Y,*

$$(\text{number of people in } X \text{ or } Y) \leq (\text{number of people in } X) + (\text{number of people in } Y).$$

Let us now look at the proof. The first sentence says "Let a denote one of these six people". Who is this a? it is some fixed person – could be Alice, could be Bob – someone in the collection. How do we know that this a exists? Well, clearly we have six people so we can take one of them. Indeed, this follows from one of our axioms. Can you tell which one?

The second sentence says "The proof is by case analysis." Case analysis is a logical *deduction rule*. It says that we can prove a proposition P like this: Split all logical possiblities into two cases C_1 and C_2, prove that C_1 and C_2 cover all possiblities, prove that C_1 implies P, and prove that C_2 implies P.

$$\frac{C_1 \text{ OR } C_2 \qquad C_1 \longrightarrow P \qquad C_2 \longrightarrow P}{P}$$

It should be clear that this deduction rule is *sound* – it only proves true statements – but if in doubt you can always write out a truth table. Let's do it just this once. Here, $\star$ is shorthand for $(C_1 \text{ OR } C_2) \text{ AND } (C_1 \longrightarrow P) \text{ AND } (C_2 \longrightarrow P)$.

P	C_1	C_2	$\star$	$\star \longrightarrow P$
T	**T**	**T**	**T**	**T**
T	**T**	**F**	**T**	**T**
T	**F**	**T**	**T**	**T**
T	**F**	**F**	**F**	**T**
F	**T**	**T**	**F**	**T**
F	**T**	**F**	**F**	**T**
F	**F**	**T**	**F**	**T**
F	**F**	**F**	**F**	**T**

Next, the proof has to tell us what the two cases (C_1 and C_2) are. Here, C_1 is the predicate "a is friends with at least 3 people" and C_2 is the predicate "a is strangers to at least 3 people."

Now, we expect to be given proofs of the predicates C_1 OR C_2 (the cases cover all possibilities), $C_1 \longrightarrow P$ (the theorem holds in case 1) and $C_2 \longrightarrow P$ (the theorem holds in case 2). By the case analysis deduction rule, once we validate these proofs we'll be sure to have a valid proof.

Let's start with C_1 OR C_2. This says "a is friends with 3 people, or a is strangers with 3 people". The next sentence explains why this must be true: Among the friends of a and the strangers of a there are at least 5 people, so the bigger of the two groups must contain at least $5/2 = 2.5$ people. As 2.5 is not an integer, there must be at least 3 people in one of the two groups.

This appears like a sensible argument – but how does it, exactly, follow from our axioms? We will see so shortly. For now let us "package" this intermediate statement C_1 OR C_2 as a *lemma* and give its proof later, which we must:

> **Lemma 2.** *For every collection of six people, and every person a within that collection, a is friends with at least three people or a is strangers to at least three people.*

A lemma is just like a theorem – a proposition with a proof. Usually, the theorems are the ones we are really interested in, and lemmas are intermediate propositions that are used in the proofs of theorems or of other lemmas.

Chugging along, now comes the proof of the theorem in Case 1. For this part, we can *assume* C_1: a is friends of at least 3 people. You can think of it as another axiom, but just for this part of the proof. We divide C_1 into two subcases: Those 3 contain a pair of friends (C_{11}), or they are all strangers to one another (C_{12}). Clearly, C_{11} OR C_{12} always holds. Next, we see that C_{11} implies the theorem (analysis of Subcase 2.1) and C_{12} implies the theorem (anaysis of Subcase 2.2). So the theorem holds in all subcases of Case 1.

The last part of the proof is structurally similar: By the same type of reasoning, the theorem is shown to hold in all subcases of Case 2. A mathematics book may omit this part altogether and say "Case 2 is proved analogously to Case 1". Before you become practiced at proofs, I suggest that you refrain from doing this and work out all the cases in detail.

Before we embark on the challenging task of discovering proofs, let us have one final word about axioms. What, exactly, are we allowed to assume as an axiom or as a previously proved proposition when we prove a theorem? For us, this will consist of the "common sense" facts you have learned in school, as well as propositions we have previously proved in class. For example, if you are asked to prove a theorem in your homework, it is okay to use Theorem 1 as a previously proved statement.

In the beginning of the 20th century logicians spent considerable effort trying to agree on a small collection of axioms that ought to be enough to prove all known mathematics. One of the proposals are the so-called ZFC axioms of set theory; you can read about them in the textbook. While, in principle, you can write any proof relying on just these nine axioms, in practice deriving a proposition as simple as $1 + 1 = 2$ from the ZFC axioms may take dozens of pages of proof and explanations, so we won't be doing that.

2 How to prove it

Let's start by proving a simple theorem:

Theorem 3. *The sum of two even integers is even.*

How do we go about proving such a theorem? First, let us unwind this statement in terms of quantifiers:

> For all integers m and n, if m is even and n is even, then $m + n$ is even.

This is a universal statement about two integers, which we call m and n. We need to show that following implication:

$$(m \text{ is even}) \text{ AND } (n \text{ is even}) \longrightarrow (m + n \text{ is even}).$$

Let's assume that m is even and n is even. This means there exist integers a and b such that $m = 2a$ and $n = 2b$. But then $m + n = 2a + 2b = 2(a + b)$, so $m + n$ is also twice an integer, and therefore even.

This is a common method for proving a statement of the form "If P then Q". We assume P, do a bit of reasoning, see what consequences we get, and eventually hope to end up with Q.

Once you figured out the reasoning, here is how you may *write* this proof:

Proof of Theorem 3. Let us call the two integers m and n. Assume m is even and n is even. Then there exist integers a and b such that $m = 2a$ and $n = 2b$. It follows that $m + n = 2a + 2b = 2(a + b) = 2c$, where $c = a + b$. Therefore m is also even. □

Let's do another one:

Theorem 4. *The product of two odd integers is odd.*

We follow the same pattern.

Proof. Call the integers m and n. Since m and n are both odd, we can write $m = 2a + 1$ and $n = 2b + 1$ for some integers a and b. Then

$$mn = (2a + 1)(2b + 1) = (2a)(2b) + 2a + 2b + 1 = 2(2ab + a + b) + 1 = 2c + 1$$

where $c = 2ab + a + b$. It follows that mn is also odd. □

In these examples, the path to the proof was clear; we just need to move along (and avoid making mistakes in the process). Other times we need to do some "scratch work," that is reasoning which won't make it into the proof but helps us figure things out. Here is one such example:

Theorem 5. *The square of an odd number is of the form $8k + 1$ for some integer k.*

Let's call our number n. Since n is odd, we can write $n = 2t + 1$ for some integer t. Then

$$n^2 = (2t + 1)^2 = 4t^2 + 4t + 1.$$

Why should this be of the form $8k + 1$? We want to show that given t, we can always find a k such that

$$4t^2 + 4t + 1 = 8k + 1$$

which we can simplify to $t^2 + t = 2k$. Namely, we are now left to show that $t^2 + t$ is always even. To make sure we are on the right track, we can try some examples: $1^2 + 1 = 2$, $2^2 + 2 = 4 + 2 = 6$, $3^2 + 3 = 9 + 3 = 12$, all even.

It seems there are two cases: t is even, in which case so is t^2 and also $t^2 + t$, or t is odd, in which case so is t^2, and so $t^2 + t$ is also even. This covers all possibilities. We now need to summarize them nicely into a proof.

Before we do so, let's revisit the last step and see if there is an easier way to explain why $t^2 + t$ is always even. If we factor this expression, we get $t^2 + t = t(t + 1)$. Now if t is even, so is $t(t + 1)$, and if t is odd, then $t + 1$ is even and so is $t(t + 1)$. This simplifies our case analysis a bit.

Proof of Theorem 5. Assume n is odd, so we can write $n = 2t + 1$ for some integer t. Then

$$n^2 = (2t + 1)^2 = 4t^2 + 4t + 1 = 4t(t + 1) + 1$$

We now prove the theorem by case analysis.

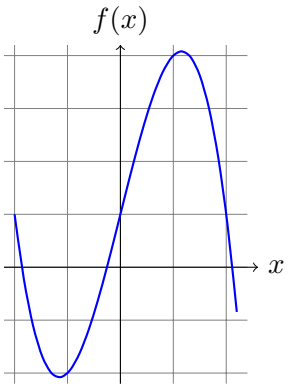
- **Case 1:** t is even. Then we can write $t = 2r$ for some r and $4t(t+1)+1 = 8r(t+1)+1 = 8k+1$ for $k = r(t + 1)$.
- **Case 2:** t is odd. Then $t + 1 = 2r$ for some r and $4t(t + 1) + 1 = 8tr + 1 = 8k + 1$ for $k = tr$.

The two cases cover all possibilities and the claim holds in each case. □

Here is another one where some scratch work of a different sort is helpful:

Theorem 6. *If x is a real number with $0 \leq x \leq 2$, then $-x^3 + 4x + 1 > 0$.*

This is a universal statement and there are infinitely many x to check, so we need to be a bit clever here. Fortunately, we live in an age of computers so we start by plotting the graph of $f(x) = -x^3 + 4x + 1$:



This picture is not a proof; we must derive the theorem by logical deduction. So where do we start?

From the picture we can see that in the range of interest $0 \leq x \leq 2$, $f(x)$ is not only greater than zero, but always exceeds 1, namely

$$\text{If } 0 \leq x \leq 2, \text{ then } -x^3 + 4x + 1 \geq 1.$$

The statement $-x^3 + 4x + 1 \geq 1$ is the same as $-x^3 + 4x \geq 0$. But now we can *factor* the left hand side as

$$-x^3 + 4x = x(4 - x^2) = x(2 - x)(2 + x).$$

When x is between 0 and 2, all of the terms $x, 2 - x, 2 + x$ are nonnegative, and so must be their product. There!

We are not finished yet – we must now summarize our conclusions neatly into a proof with clear logical deductions.

Proof of Theorem 6. Assume x is a real number such that $0 \leq x \leq 2$. Then all of the numbers x, $2-x$, and $2+x$ must be nonnegative. It follows that $x(2-x)(2+x) \geq 0$. Multiplying out the left hand side, we obtain $-x^3 + 4x \geq 0$. Therefore $-x^3 + 4x + 1 \geq 1 > 0$, as claimed. □

3 Some proof patterns

The contrapositive

The *contrapositive* of a proposition of the form $P \longrightarrow Q$ is the proposition (NOT Q) $\longrightarrow$ (NOT P). The two are logically equivalent. You can draw your own truth table to verify this.

A number r is *rational* if we can write $r = n/d$ where both m and n are integers, e.g. 1/2, 3/2, 5/17, 8/16. A number is *irrational* if it is not rational.

Theorem 7. *Assume $r \geq 0$. If r is irrational, then $\sqrt{r}$ is irrational.*

Let us try to prove this theorem. We assume r is irrational. So r cannot be written as a fraction n/d for any integers n and d. Where do we go from here? An assumption like this doesn't tell us much about $\sqrt{r}$, so it is not clear how to reach any conclusion about it. Instead, let us try the contrapositive:

> Assume $r \geq 0$. If $\sqrt{r}$ is rational, then r is rational.

This is now much easier to prove.

Proof of Theorem 7. We prove the contrapositive. Assume $r \geq 0$ and $\sqrt{r}$ is rational. Then we can write $\sqrt{r} = n/d$ for some integers n and d. It follows that $r = n^2/d^2$, and so r is also rational. □

Proving equivalences

A common way to prove a statement of the form P IFF Q, that is, an equivalence, is to prove separately that P implies Q and that Q implies P:

$$\frac{P \longrightarrow Q \qquad Q \longrightarrow P}{P \text{ IFF } Q}$$

Here is an example.

Theorem 8. *For every integer n, n^2 is even if and only if n is even.*

Proof. First, we prove that if n is even then n^2 is even. If n is even, we can write $n = 2k$ for some integer k, so $n^2 = 4k^2 = 2(2k^2)$, which is also even.

Now, we prove that if n^2 is even then n is even. We prove the contrapositive: If n is odd, then n^2 must also be odd. In Theorem 5 we showed that if n is odd then n^2 is of the form $8k+1 = 2(4k)+1$, which is an odd number. □

Proof by contradiction

Say you want to prove a proposition P. In a proof by contradiction, you start by assuming P is *false*, and then you deduce that this assumption applies a falsehood. So P must have been true:

$$\frac{(\text{NOT } P) \longrightarrow \mathbf{F}}{P}$$

We will now prove Lemma 2 using this method. Recall what the lemma says:

> *For every collection of six people, and every person a within that collection, a is friends with at least three people or a is strangers to at least three people.*

In the proof, we will assume the negation of the statement, and then show that something false must follow.

Proof of Lemma 2. Assume, for contradiction, that there exists a collection of six people and a person a within that collection such that a is friends with at most two people and a is strangers with at most two people. Then the number of people in the collection that are friends with a or strangers to a is at most four (by Axiom 4). These make up all people in the collection apart from a. Therefore the collection has at most five people. This contradicts our assumption that the collection consists of six people. □

Here is a famous example:

Theorem 9. *$\sqrt{2}$ is irrational.*

This is a universally quantified statement: For all n and d, we cannot write $\sqrt{2}$ as n/d. You could try different choices of n and d and see for yourself that they don't work. Where to go from here?

Proof. Assume, for contradiction, that $\sqrt{2}$ is rational. Then we can write $\sqrt{2} = n/d$ where n and d are integers. Furthermore, let's take n and d so that they have no common factor greater than 1, so the fraction is written in lowest terms.

Squaring both sides, we obtain $2 = n^2/d^2$ and so $n^2 = 2d^2$. So n^2 is even. Then n must also be even (by Theorem 8), and so n^2 is a multiple of 4. Because $2d^2 = n^2$, d^2 must be even, so d is also even.

We conclude that both n and d are even. But we assumed that they have no common factor greater than 1. This contradicts our assumption that $\sqrt{2}$ is rational. □

Proofs by contradiction can be confusing because you begin by assuming a statement that is, in fact, false. So some of the statements you will be making inside the proof will also be false. You need to keep in mind at all times that you are operating under a false assumption, and intermediate claims, like "d is even", are only true within that context. Because of this confusion, I generally

recommend proofs by contradiction only as a last resort, when all your other attempts at a proof have failed.

In some cases, a proof by contradiction can be rewritten as a proof by contrapositive. Lemma 2 is one such example. Can you prove this lemma using the contrapositive?

Experiment and don't give up easily!

When you start out trying to prove a theorem, you rarely know what is the right method ahead of time. So play around, experiment, backtrack, and don't be afraid. The "correct" approach will often reveal itself after a few trials and errors.

Theorem 10. *There exist irrational numbers a and b such that a^b is rational.*

Where do we start? Let's try some examples. Well, the only number we know for sure is irrational is $\sqrt{2}$, so let's try setting $a = \sqrt{2}$ and $b = \sqrt{2}$. Is $\sqrt{2}^{\sqrt{2}}$ rational or irrational? It looks pretty irrational to me, so it doesn't seem that this should work out.[2]

Ah, but if $\sqrt{2}^{\sqrt{2}}$ is irrational, then we have one more irrational number to play with. So why don't we try $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}^{\sqrt{2}}$. Then

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}^{\sqrt{2}}} = \sqrt{2}^{\sqrt{2}\cdot(\sqrt{2})^{\sqrt{2}}} = \sqrt{2}^{\sqrt{2}^{\sqrt{2}+1}}$$

What a mess! Let's backtrack and try instead $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$. Then

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2})^2} = \sqrt{2}^2 = 2$$

which is a rational number! Let's summarize this reasoning into a proof.

Proof. The proof is by case analysis.

Case 1: $\sqrt{2}^{\sqrt{2}}$ is rational. In this case, the theorem is true for $a = \sqrt{2}$ and $b = \sqrt{2}$.

Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational. In this case, the theorem is true for $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$ because $a^b = 2$. □

This type of proof is sometimes called a *win-win proof*. It doesn't matter if $\sqrt{2}^{\sqrt{2}}$ is rational or not. In either case you win. You may not always get this lucky, but it doesn't hurt to try.

[2]This part of the argument is not conclusive: "It looks pretty irrational" doesn't make a number irrational. Perhaps we'll come back to it later, but we might as well try something easier first.

4 How to write and present a proof

For this class, it is not enough that you know how to come up with proofs. You must also write and present them properly. Writing a proof is not easy. On the one hand the proof must be clear and precise. On the other hand, it should be easy to read and understand (by humans, not by machines). For general advice on how to write proofs, see Section 2.7 in your textbook.

Presenting a proof to others is also challenging. Your listeners may not be familiar with the notation. Steps in the proof that are obvious to you may take longer for others to grasp. So start from the beginning and go slowly; do not introduce too many new concepts at once; give examples along the way; and encourage questions from your audience.

References

This lecture is based on Chapter 2 of the text *Mathematics for Computer Science* by E. Lehman, T. Leighton, and A. Meyer. Material from slides by Prof. Lap Chi Lau were also used in the preparation.