What is proof?

Lesson 1

The topic for this Math Explorer Club is mathematical proof. In this post we will go over what was covered in the first session.

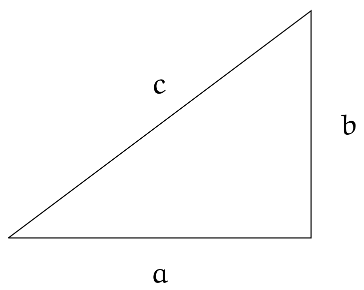
The word proof is a normal English word that you might hear in normal speech. Here are some examples.

- A physicist might say that they have proved the existence of the Higgs boson
- A teacher might ask for a proof that you have done all your homework
- Even a baker might tell you that they have proved a loaf of bread

In mathematics when we use the word proof we mean something different. Consider the following familiar theorems of mathematics.

1 Pythagoras' theorem

Consider the right-angled triangle with side lengths a, b and c as below.



Then Pythagoras' theorem says that

$$a^2 + b^2 = c^2$$

Or in words; the square of the hypotenuse is equal to the sum of the squares of the other two sides. Pythagoras' theorem was known to the ancient Greeks, over 2000 years ago!

2 The Quadratic formula

Given a quadratic polynomial

$$ax^2 + bx + c = 0$$

the solutions are given by the following formula.

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Quadratic equations have been studied as far back as the Babylonians. General solutions to quadratics were known by ancient Greeks, and are thus also thousands of years old.

This begs an important question. Why is it that these results, which are thousands of years old, are still to this day being taught in schools all over the world? The ancient Greeks used to think the world was flat and that Zeus lived atop Mt. Olympus. Why is it that some of their ideas remain true today, while others have long been replaced? The answer is mathematical proof. Before we say what a proof is, we must actually start by saying what a proof is not.

A non-proof that the world is flat. Why did people believe that the world was flat? Well if you look around the world does usually look flat. Okay, perhaps there are some hills nearby, but generally speaking the world doesn't look like a sphere to us. In fact, everyone you meet would also probably have experienced a flat world (unless you find yourself having lunch with an astronaut!). This led people to thinking the world was flat because every example they had showed it to be so.

What would be the equivalent non-proof of Pythagoras' theorem? We could draw lots of right-angled triangles and measure their side lengths and see if they satisfied the equation $a^2 + b^2 = c^2$. If this works for every example we do (and it would!) then would we be satisfied that we had proved the theorem? The answer is no - this is not something a mathematician considers as a mathematical proof. And it is because our examples could be misleading. Perhaps there are some examples for which the formula doesn't hold. If mathematicians accepted proofs like this we would end up proving things like 'the world is flat', and that, as we know, is not okay. So lesson 1 is the following.

It is not okay to prove something by doing examples

What we need to do to give a mathematical proof is to provide an argument that works in general. Something that works for all possible right-angled triangles. That is exactly what we will try and do in this next worksheet.

[Worksheet on Pythagoras' Theorem]

Well done! We just proved Pythagoras' theorem. This proof means that this theorem was true 2000 years ago, it is true now, and it will still be true in 2000 years time! Isn't that amazing?

Proof by contradiction

Lesson 2

The proof we just saw of Pythagoras' theorem is an example of a direct proof. We gave a general argument that directly showed that $a^2 + b^2 = c^2$ for all right-angled triangles. In this section we are going to look at a different type of proof, called a proof by contradiction. The idea is a subtle one, so think about it carefully. The general outline is as follows.

1. We want to prove a certain mathematical statement.
2. Start by assuming that the statement we want to prove is false.
3. Use that assumption to show something impossible, or contradictory.
4. Conclude that our original assumption must have been incorrect.

To see this in action we are going to think about prime numbers.

Prime Numbers

Prime numbers are the building blocks of whole numbers. They are the smallest parts into which we can break numbers down. For example, we can break down the number 15 as follows.

$$15 = 5 \times 3$$

The point is that we can't break these numbers down any further. We call numbers like this prime. So in this example we see that 5 and 3 are prime numbers, and that 15 is not (because it could be broken down into smaller pieces). Here are some of the smallest prime numbers.

$$2, 3, 5, 7, 11, 13, 17$$

Think about some of the numbers that have been missed out on this list and check to see why they aren't prime e.g. $4 = 2 \times 2$. You may have noticed that we skipped over 1. Well 1 is a bit weird because we can do silly things like write $3 = 3 \times 1 = 3 \times 1 \times 1$ and so on. For this reason we just choose to ignore 1 and say that it is not prime.

Okay so we have this idea of prime numbers, and we have seen that some numbers, like 7, are prime, while others, like 4 and 15 are not. The question is, how many prime numbers are there? The periodic table is a table of elements from which all of matter is made. All of the complexity of nature is built from this list of 118 elements. So what about numbers? How many prime numbers do we need to build all the numbers in the world?

The answer is that there are infinitely many prime numbers. That is, the prime go on and on forever. If we were to extend the list above $2, 3, 5, 7, 11, 13, 17, \ldots$ it would never end. There is no last prime number. How are we going to prove something like this? The idea is, of course, to use a proof by contradiction. Let's give it a try:

Step 1. Assume the statement is false. That is, suppose we have only finitely many prime numbers. Here they are now.

$$p_1, p_2, \ldots, p_n$$

We don't know how many there are, only that the list is finite. We say there are n of them where n is some number we don't know. It could be 1,456,345, perhaps it's 73, it doesn't matter. All that matters is that we are pretending that it is finite.

Step 2. Now we need to come up with a contradiction. Consider the following number:

$$P = p_1 p_2 p_3 \cdots p_n + 1$$

That is, we just multiply all the prime numbers together and add 1. For example, if the list of all prime numbers was $2, 3, 5$ (it clearly isn't, but just for a concrete example), then this number would be 31. What happens if we try to divide our new number P by a prime number? I claim that we will always get a remainder of 1. In our example this is plain to see - 31 divided by any of our primes 2, 3 or 5, has remainder 1. This holds for our general number P too, since this is exactly how we built it!

Question: Is P a prime number? Well, observe that P is larger than any of the primes on our list $p_1, \ldots, p_n$, since we made P by multiplying all the primes together and adding 1. So P can't be on the list, and so it cannot be prime (since we assumed the list contained all the primes!).

On the other hand, if P is not a prime number, then by definition we must be able to break it down into smaller prime pieces (like we did with $15 = 5 \times 3$). So we should be able to write P as a product of primes on our list. But we just observed that no primes on our list divide P. If P was a product of primes, then those primes must divide P (just as both 5 and 3 divide 15).

Step 3. So P cannot be a prime, and cannot be a non-prime! But this cannot be - it must be one or the other. Therefore this is our contraction. It shows us that our original assumption must have been false!

Step 4. So our original assumption, that there were only finitely many primes, must be false. We can therefore conclude that there are indeed infinitely many primes!

Next lesson we will look at some graph theory and you will try and come up with your own idea of a mathematical theorem!

Graph theory and Euler characteristic

Lesson 3

Our next step in attempting to understand mathematical proof is to look at how mathematicians actually come up with theorems in the first place, and how this process can help them come up with ways to create a proof.

With that in mind, work through the following exercises in which you will come up with your own idea for a theorem, and then see how one might prove it!

[Worksheet on Euler Characteristic]

Hopefully as you went through this worksheet you came up with the following guess for a theorem:

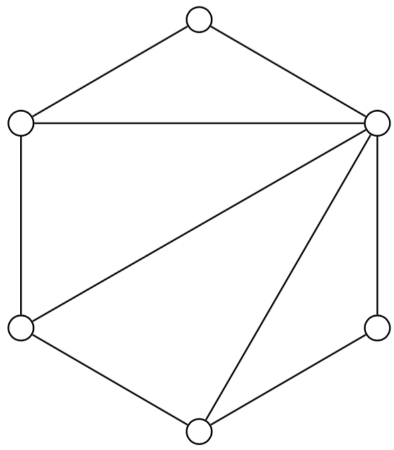
Theorem. The value of $V - E + F$ is always 1, no matter the graph.

More then that, what followed was the outline for a way to prove this via a direct proof. Remember, with a direct proof we need to give an argument that works for any graph obeying those rules (there's actually a name for such graphs, we call them planar graphs, because they can be drawn in the plane!). So our proof should start with something like:

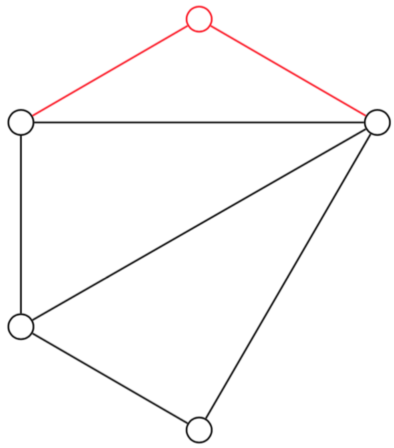
Let G be *any* planar graph. For this graph G suppose the value of

$$V - E + F = x$$

We want to show that $x = 1$. Well we saw in the worksheet that we can always cut up all the faces of G into triangles without changing the value of x.



Next we saw that we can remove triangles from the outside in, each time not changing the value of x.



We repeat in this way until we are left with only 1 more triangle, and because we haven't changed the value of x along the way we know that $V - E + F$ for the triangle is equal to $V - E + F$ of the original graph G! We complete the proof by verifying that any triangle has $V - E + F = 1$.

Summary

We see here that although we cannot prove something just by doing examples, it is still a very important part of the process. We not only saw that $V - E + F = 1$ in each of our examples, but by playing around with triangles we were able to gain intuition on how the proof might go.

Proof by induction

Lesson 4

So far we have seen two different types of mathematical proof:

1. Direct proof e.g. Pythagoras' theorem, Euler's formula ($V - E + F = 1$)
2. Proof by contradiction e.g. Infinitely many primes

In today's lesson we will learn a third type of proof called proof by induction. Let's motivate the idea by working through an example. We are going to try and prove the following formula for summing the first n numbers.

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

[Worksheet on Induction]

So what's the idea of proof by induction? A helpful analogy is found in dominoes. Think of each domino as representing one of the statements we want to prove. The induction argument is based on the idea that knocking one domino over (by proving that statement) causes all the other dominoes to get knocked over, one by one.

Let's recap the argument. We were able to verify that the formula for summing the first n numbers holds in some small examples by hand. However, we want to be able to use the formula for any number n, for example, to add the first 1,000,000 numbers, which we clearly don't want to do by hand. So we proved the inductive step which was to show that if the formula holds for $n = k - 1$ then the formula holds for $n = k$. This is the part which says, if one domino falls, then so does the next one.

It is important to note that there are two steps involved when doing a proof by induction.

Base Case: First we have to show that the formula holds for $n = 1$. In our example this was easy, we just verified that that formula read $1 = 1$!

Inductive step. Then we have to show that if the formula holds for $n = k - 1$ then the formula holds for $n = k$.

By the base case we know the formula holds for $n = 1$. Now by the inductive step, since we know the formula holds for $n = 1$ we can conclude that the formula must hold for $n = 2$. But since the formula holds for $n = 2$, we can deduce from the inductive step that the formula must hold for $n = 3$. But since the formula holds for $n = 3$, we can deduce from the inductive step that the formula must hold for $n = 4$. Etc, etc....

This kind of argument is very useful for proving formulas that depend on n, for example:

Formula for the sum of squares.

$$1^2 + 2^2 + 3^2 + \cdots n^2 = \frac{n(n+1)(2n+1)}{6}$$

Binomial formula.

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

The square root of 2 and a brief history of numbers

Lesson 5

In today's lesson we will learn about a new kind of number. We'll begin at the beginning with a brief history of numbers.

[Worksheet on the square root of 2 and a history of numbers]

Let's take a minute to process this; we just discovered a whole new kind of number. We call them irrational numbers, and they are numbers that cannot be written as fractions of whole numbers $\frac{a}{b}$. There are many examples of numbers like this, perhaps none more famous than the mysterious number π, that relates the diameter of a circle to its circumference.

At this point then we have considered four different types of numbers.

1. The natural numbers: 1, 2, 3, 4, etc.
2. The whole numbers, or integers: ..., -2, -1, 0, 1, 2, etc.
3. The rational numbers: fractions a/b
4. The reals numbers: these include irrational numbers like $\sqrt{2}$ and π. They can be thought of as all decimal numbers, where the decimals can be infinitely long. Irrational numbers are those whose decimals go on forever, and never repeat themselves. For example $\pi = 3.14159265...$

Cantor's Diagonal Argument - Different Sizes of Infinity

In 1874 Georg Cantor - the father of set theory - made a profound discovery regarding the nature of infinity. Namely that some infinities are bigger than others!

The story begins with the notion of a countable set, we think of the natural numbers $\{0, 1, 2, ...\}$ as being countable in that we can put them in a list and count through them (clearly we will never reach the end of the list, but the process of counting them makes sense). This is somehow the building block for defining countable sets, as we think of a general set as being countable if there exists a bijection between it and the naturals. Remember, a *bijection* just means that we can match up each element in one set with an element in the other set, without missing any elements out. Here are some examples of a bijections.

1. $\{1, 2, 3, 4, 5\}$ is in bijection with $\{a, b, c, d, e\}$, but not with the set $\{a, b, c\}$

$$\begin{array}{ccccccc}
1 & \text{———} & a & \qquad & 1 & & a \\
2 & \text{———} & b & & 2 & ? & b \\
3 & \text{———} & c & & 3 & ? & c \\
4 & \text{———} & d & & 4 & ? & \\
5 & \text{———} & e & & 5 & &
\end{array}$$

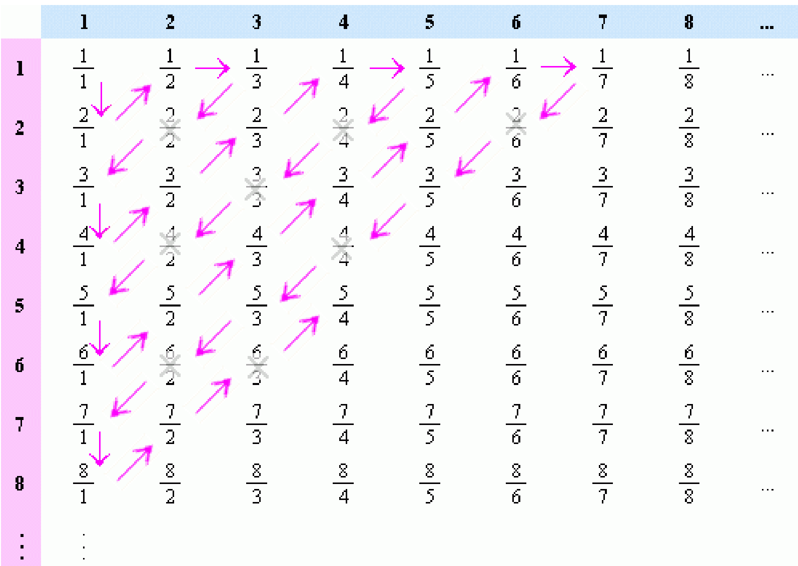
2. The natural numbers $\{1, 2, 3, \ldots\}$ are in bijection with the whole numbers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$

$$\begin{array}{ccc} 1 & \text{———} & 0 \\ 2 & \text{———} & 1 \\ 3 & \text{———} & -1 \\ 4 & \text{———} & 2 \\ 5 & \text{———} & -2 \\ \vdots & & \vdots \end{array}$$

In particular, we note that being *countable*, i.e., in bijection with the natural numbers, just means that we can write out our numbers in a list and in such a way that we don't miss any out. Let's do a harder example.

Example. The rational numbers are countable

We can show they are countable by writing them in a table as follows.



First notice that every rational number occurs in this table, and that, by snaking along the pink path we will hit every number in it. In this way we have a list with every rational number in it, and thus the rationals are countably infinite. Our list beginning

1. $\frac{1}{1} = 1$
2. $\frac{2}{1} = 2$
3. $\frac{1}{2}$
4. $\frac{1}{3}$
5. $\frac{3}{1} = 3$

This shows that the rational numbers are countable!

Are the reals countable?

The next question is: are the real numbers countable? Cantor showed that the answer is no!

Suppose that the real interval $[0, 1]$ were a countable set. That is, we could write down every real number between 0 and 1 in some list. Let me write a small section of this hypothetical list below:

1. $0.\mathbf{a_1}a_2a_3a_4a_5\ldots$
2. $0.b_1\mathbf{b_2}b_3b_4b_5\ldots$
3. $0.c_1c_2\mathbf{c_3}c_4c_5\ldots$
4. $0.d_1d_2d_3\mathbf{d_4}d_5\ldots$

$\vdots$

Now here the numbers stretch off infinitely into the right, as real numbers can have infinite decimal expansions, and obviously stretch infinitely far down. The letters a_i, b_i, c_i, d_i represent numbers between 0 and 9, so $0.a_1\ a_2\ a_3\ a_4\ a_5\ldots$ may be the number 0.12321... . It is unimportant what the specific numbers are, only that we can write them in such a list.

Now, along the diagonal of this list the numbers that have been emboldened form a number; it begins $0.a_1\ b_2\ c_3\ d_4\ldots$. With this we define a new number, called D, by adding 1 to each digit with the convention that if a digit is 9 then adding 1 goes to 0. In this way we have that the first digit of D is $a_1 + 1$. So if the first number really did start 0.12321, then D would start 0.2..., for example.

Now this number D is surely a real number, and moreover it certainly lies between 0 and 1. Thus if the above list is, as claimed, complete it should contain D.

Where does our new number D belong on this list? Is it the first number on the list? No - it can't be since they differ in the first position? The first digit of D is $a_1 + 1$ whereas the number in the list starts with a_1.

Is it the second number in the list? Again no. This time we see that it differs in the second digit. The second digit if D is defined to be $b_2 + 1$, whereas the second number in the list has second digit b_2.

Continuing in this way we see that in fact D cannot belong anywhere on the list! We have therefore found a real number that does not belong to this list. But this list was supposed to contain **all** real numbers!