

A Mathematician's View of Proof Professor Sarah Hart 4 June 2024

In this, my final lecture as Gresham Professor of Geometry, I wanted to take a look at the thing that makes mathematics different from perhaps all other subjects: proof. If we were in Ancient Greece, the latest science would tell us that four elements make up all things: fire, water, earth and air. In China at a similar time, there are known to be five agents of change in the universe: earth, wood, metal, fire, and water. But both cultures also knew that the square on the hypotenuse is the sum of the squares on the other two sides. And that's something we still know. The difference is proof. We have proved Pythagoras's Theorem mathematically, and so it's true for all time. Today we're going to explore the mathematical idea of proof, and I'm going to show you some of my all-time favourite proofs. We'll talk as we go about what counts as a "good proof", but the ones I'll show you today all involve a flash of genius that makes them truly delightful. Let's begin, since I have already mentioned it, with Pythagoras's Theorem.

Pythagoras's theorem

Possibly the most proved theorem of all time, it has been discovered and rediscovered multiple times throughout history. I know you know it, but just to be sure, it states that in a right angled triangle with sides a, b and c, where c is the hypotenuse, we have that $a^2 + b^2 = c^2$. That is, "the square on the hypotenuse is the sum of the squares on the other two sides". Special cases, such as the right-angled triangle whose sides are 3, 4, and 5, were known thousands of years ago, for example in Ancient Egypt and China. Later, we have proofs from the Ancient Greek, Indian and Chinese mathematical traditions, and many hundreds since. Here I'll give you my favourite two proofs. In each case we imagine a right-angled triangle with sides a, b, and hypotenuse c.





The first proof is almost purely visual. In the above pictures we see that the same square is made of four copies of our triangle, plus, in the first picture a square of side *c*, and in the second two squares of sides *a* and *b* respectively. Therefore $a^2 + b^2 = c^2$.

I like the second proof for the element of surprise: it seems to have nothing to do with squares or areas. In our given triangle, we drop a perpendicular to the hypotenuse, dividing the triangle into two smaller ones which are both similar (in the mathematical sense) to the original triangle. Ratios of corresponding sides in similar triangles are equal. Hence $\frac{a}{x} = \frac{c}{a}$ and $\frac{b}{y} = \frac{c}{b}$.



Rearranging a bit gives us $a^2 = cx$ and $b^2 = cy$, and so $a^2 + b^2 = c(x + y) = c^2$.

Before we have a proof, of course, we have to have a "conjecture" – after the first hundred or so rightangled triangles have this Pythagorean property, we get to be pretty sure that it must always be true. So how do we make conjectures? Well, it's all about pattern spotting. Let's see how good you are at that.

Here's a question about points on a circle. Draw *n* points on the circumference of a circle and join every pair of points with a chord. What is the greatest number of regions into which the circle can be divided? The answer isn't obvious, so we try some examples. For 1, 2, 3, 4, 5 points respectively, the answer is 1, 2, 4, 8, 16. Seems pretty obvious that we're getting the powers of 2 here. But in fact, however you place 6 points on the circle, you can never create more than 31 regions. (For 7 and 8 the answers are 57 and 99.) And this is why we need proofs!

This wasn't in the lecture, but there is a formula for the number of regions, which I'll explain here briefly. To follow it you need to know that the number of ways of choosing *k* objects from a set of *n* objects, known as "*n* choose *k*" and written $\binom{n}{k}$, is $\frac{n!}{k!(n-k)!}$ for $0 \le k \le n$ and 0 otherwise. (By convention 0! = 1.)

Let R(n) be the maximum number of regions into which we can divide the circle by joining n points. To get the maximum number of regions, we must arrange the points in such a way that no three chords all meet at a point, because if they didn't meet we could get an additional region, one bordered by the three chords. Let's assume we do that, and then imagine what happens when we draw the chords one at a time. We start with one region, the whole circle. Each chord we draw starts at the circumference. As soon as it hits another chord, what was previously one region is now divided into two. So every time our chord crosses another chord, we add one to our region count. The last thing to happen to the chord is that it reaches the circumference again. This also divides an existing region into two regions, so again we have to add one to the region count. Therefore, we start with 1 region, and then each new chord we draw adds (to the existing region count) the number of existing chords it intersects with, plus 1 (for the final "circumference" region). Importantly each intersection of chords arises exactly once in this way – whichever of the two chords is drawn second will use up that intersection for its region count. So we have the following formula:

$$R(n) = 1 + (no. of chords) + (no. of intersections)$$

Since each chord is specified by its endpoints, the number of chords is the number of ways of choosing two points from the *n* points we have. So it is $\binom{n}{2}$. The number of chord intersections is slightly harder to work out. Two chords that intersect arise from 4 endpoints (one chord from the first pair, one from the second pair). But is this condition sufficient? Is it possible for four points to produce more than one pair of intersecting chords? Or no intersecting chords? No, because any four points on a circle define six chords, making up the sides and diagonal of a quadrilateral, and there is exactly one intersection point among these chords. So any four points on a circle really do define exactly one intersection point. Thus, the number of intersecting chords is precisely the number of ways of choosing 4 points from *n*, which is $\binom{n}{4}$. Therefore, $R(n) = 1 + \binom{n}{2} + \binom{n}{4}$. If you plug in the formulae for $\binom{n}{2}$ and $\binom{n}{4}$, after some work you get $R(n) = \frac{1}{24}(n^4 - 6n^3 + 23n^2 - 18n + 24)$. Not as nice as 2^{n-1} , which we wanted the answer to be, but it does have the virtue of being correct! You might wonder why these numbers start off looking like powers of 2. The reason relates to some properties of binomial coefficients that you might remember from Pascal's triangle. Firstly, $\binom{n-1}{0} + \binom{n-1}{1} + \binom{n-1}{n-1} + \binom{n-1}{2} + \binom{n-1}{3} + \binom{n-1}{4}$. For $n \le 5$ this is 2^{n-1} . But as soon as $n \ge 6$, we are missing $\binom{n-1}{5}$ and subsequent terms, and so that's where the patterns stop agreeing.

What are the ingredients of a "good" proof?

Once there is a valid proof of a theorem, then that is sufficient, in purely mathematical terms. We don't need to prove it again, and doing so doesn't make it "extra true". So why do some results have many proofs? Pythagoras's Theorem is a case in point. With hundreds of proofs, it may be the most proved theorem of all time. A mixture of things is going on here. Firstly, the theorem was noticed in many different cultures. Even in Ancient Egypt, though they probably didn't know the general result, they do appear to have known and used the fact that a 3-4-5 triangle will have a right angle opposite the longest side. Later on, in the Greek, Indian and Chinese traditions we see different proofs being found. But even when proofs of the result were well known, people kept finding new ones. It's something of a mathematical hobby at this

point in the case of Pythagoras's Theorem, but sometimes finding a different proof of a result can shed new light on it, showing connections that hadn't previously been noticed, potential generalisations, or using a new technique that can be applied more widely. Also, often the first proof of a theorem is not the best – it gets the job done but later people find clearer arguments and shorter ways through. The first explorers may take a meandering path but of course once you have a map you can easily find shorter, better routes. Over the years, proofs can be refined and simplified so that eventually a beautiful, crystalline kernel remains where the exquisite genius of the underlying idea is shown to its best effect.

Here's an example of turning a bad proof into a good one. Calculate the expression $n^2 + n + 41$ for different values of n. When n = 0, 1, 2, 3 respectively, we get 41, 43, 47, 53: all prime. We also get prime numbers for n = 4, 5, 6, 7, 8, 9, 10, Do we always get a prime number? It turns out the answer is no. A bad proof of this would be to list all the values until we hit one that isn't prime. A good way would be to notice that if we put n = 41, then every term will have a factor of 41, and so the result cannot be prime (it will be 41×43 , whatever that is). However, that observation may only have come from us doing those calculations first. Once we have noticed this "41" trick, we can then immediately generalize it and get:

Theorem No expression $an^2 + bn + c$ (with *a*, *b*, *c* positive integers) gives prime numbers for every $n \ge 0$.

Proof Let $f(n) = an^2 + bn + c$. If c > 1 then f(c) = c(ac + b + 1); both factors are greater than 1 and f(c) is not prime. If c = 1 then f(0) = 1, which is not prime.

Mathematicians' favourite proofs have certain qualities (in addition, of course, to being correct!): they are ingenious, they are clear, and they are elegantly concise. They may also give you extra insight into the question, or involve a surprising idea. One of the false messages about mathematics is that only geniuses can do it, so I want to stress that almost always, our first proofs are workmanlike, roundabout, too long, badly expressed, with woefully unhelpful and inconsistent notation, and often wrong. The polishing process takes a long time, but don't be fooled by the presentation of the final perfect gem into thinking it came directly from our brains onto the page like that! So let's sit back and enjoy these lovely proofs, but remember that, like any good selfie, it took a lot of work time to make it look that effortless. Here are two more proofs that rely on an insight that makes everything simple.

How many different sums add up to n?

For example, there are four ways to make 3:	3	2 + 1	1 + 2	1 + 1 + 1
---	---	-------	-------	-----------

You can make 4 in eight ways:

4; 3+1; 1+3; 2+2; 2+1+1; 1+2+1; 1+1+2; 1+1+1+1

Is the number of ways doubling each time? If so, why? We could try and make the sums for 4 out of the sums for 3. For instance we could add 1 to the first term: 4; 3 + 1; 2 + 2; 2 + 1 + 1. That gives us half the answers. We could instead add an extra 1 to get 3 + 1; 2 + 1 + 1; 1 + 2 + 1; 1 + 1 + 1 + 1. But we've now got 3 + 1 and 2 + 1 + 1 twice and haven't got 1 + 3 or 1 + 1 + 2. It's looking horribly complicated. Until a fabulous insight saves us.

There are 2^{n-1} sums that add to n

Proof Start with *n* lots of 1. Between each pair of 1's put either *g* or +. The *g* means "glue them together", so 1g1 + 1g1g1 means 2 + 3. This will give us all the ways to make *n* with no repetitions or omissions. So, the number of possibilities is the number of ways to make n - 1 choices of *g* or +. Which is 2^{n-1} .

Incidentally, if we don't care about the order the numbers appear in, then there's one way to make 1, two ways to make 2 (namely 2 and 1 + 1), and three ways to make 3 (namely 3, 2 + 1, and 1 + 1 + 1). By now you know it's risky to imagine there are four ways to make 4. And you'd be right to be suspicious. There are five ways: 4; 3 + 1; 2 + 2; 2 + 1 + 1; 1 + 1 + 1 + 1. Aha, so it's the Fibonacci sequence, you cry? Well, the possibilities for 5 are 5; 4 + 1; 3 + 2; 3 + 1 + 1; 2 + 2 + 1; 2 + 1 + 1 + 1 + 1 + 1. So it's not the Fibonacci sequence either. The first few terms are 1, 2, 3, 5, 7, 11, 15, 22, 30, 42, 56, 77, 101. This is called the partition function. We can work each term out recursively from earlier terms in the sequence, but there's no known closed form expression for it (that is, something just in terms of *n*, like 2^n).

The following argument uses a very powerful tool called the *Pigeonhole Principle*: if we have m boxes and n > m things to put in the boxes, then at least one box will contain more than one thing.

What follows is just an illustrative example – in that it doesn't prove anything particularly profound – but there are some deep theorems in mathematics that deploy the pigeonhole principle as part of their proofs.



There is a multiple of 42 which consists just of 0's and 1's.

Proof (This proof works, suitably modified, for any *n*, not just 42.) Write a list of numbers: 1, 11, 111, 1111, 1111, 11111, ... Each of these numbers on division by 42 gives a remainder. Possible remainders: 0, 1, 2, 3, ..., 41. There are 42 possible remainders. If we continue our list of numbers 1, 11, ... until we have a string of 43 1's, we will have: 43 numbers and 42 possible remainders. By the Pigeonhole Principle, there must be two of these numbers with the same remainder. If we subtract the smaller from the larger, we'll get a multiple of 42. Therefore 42 divides some number of the form 1111...10...0.

A picture speaks a thousand words

Sometimes, the right picture is all you need to make a great proof. Here are some examples.

Viviani's Theorem Whatever point you choose inside an equilateral triangle, the sum of the distances from that point to the three sides is equal to the height of the triangle.



Proof Suppose the triangle has height *h* and base *b*. The area of the triangle is $\frac{1}{2}bh$. Since it's equilateral, the other sides also have length *b*.

Suppose the distances to the sides from our chosen points are *x*, *y*, *z*. We can split the triangle into three smaller triangles with heights *x*, *y*, *z* and base *b*. Therefore, $\frac{1}{2}bh = \frac{1}{2}b(x + y + z)$. Hence h = x + y + z.

The sum of the first n odd numbers is n^2



(We may not have time for this in the lecture, so think of this bonus content if you bothered to read this transcript!) The first few sums are 1, then 1 + 3 = 4, then 1 + 3 + 5 = 9, and then 1 + 3 + 5 + 7 = 16, and so on. We appear to be getting square numbers. A diagram makes this obvious. We can be a bit more rigorous if we like: to get from n^2 to $(n + 1)^2$ we wrap 2n + 1 unit squares around the square of side n, and we could do it algebraically: $(n + 1)^2 = n^2 + 2n + 1$. But the picture really helps us to see this relationship.

The n^{th} triangular number is $\frac{1}{2}n(n+1)$.



The n^{th} triangular number T_n is the number of dots we need to make a triangle with base n, that is, $1 + 2 + \dots + n$.

Again, a visual argument helps. The rectangle shown contains two copies of T_n . Its area is n(n + 1). And so $T_n = 1 + 2 + \dots + n = \frac{1}{2}n(n + 1)$.

The sum of the first *n* square numbers is $\frac{1}{6}n(n+1)(2n+1)$

Let's write $S_n = 1 + 4 + 9 + \dots + n^2$. Imagine a triangle of numbers, but we put 1's in the first row, 2's in the second row, and so on down to *n*. That means the sum of the numbers in the triangle is S_n . Make three copies of this triangle, each one starting the counting from a different vertex. Then the sum of the numbers in all three triangles put together is $3S_n$.



But if we superimpose the three separate triangles, we have a triangle with 2n + 1 at each entry (the j^{th} entry of the i^{th} row is i + (n - i + j) + (n + 1 - j). The n^{th} triangle number is $\frac{1}{2}n(n + 1)$, meaning there are $\frac{1}{2}n(n + 1)$ entries. Adding all these entries gives us $3S_n = \frac{1}{2}n(n + 1)(2n + 1)$, and the result follows.



Proof by contradiction

The following proof dates back to Euclid and would probably come in most mathematician's list of the top ten proofs of all time.

There are infinitely many prime numbers

Proof Suppose that there are only finitely many primes. Then we can make a list of them: 2, 3, 5, up to the biggest prime p, say. Let $n = (2 \times 3 \times 5 \times \cdots \times p) + 1$. Now n is one more than a multiple of 2, so clearly 2 does not divide n. Similarly 3 doesn't divide n, nor does 5, and nor do any of the prime numbers on our list. But that implies n is either prime or has a prime factor not on our allegedly complete list of primes. So that list cannot have been complete – there can't be only finitely many prime numbers.

What a wonderful idea – a thought experiment that imagines the consequences of assuming the opposite of what you actually want to prove! This is a technique called "proof by contradiction" (or *reductio ad absurdum*, if you prefer). It's a kind of Sherlock Holmesian approach: once you have eliminated the impossible, whatever remains, however improbable, must be the truth. The great mathematician G. H. Hardy called this technique "one of a mathematician's finest weapons. It is a far finer gambit than any chess gambit: a chess player may offer the sacrifice of a pawn or even a piece, but a mathematician offers the game". The final proof I'll show you involves one of the most important early realisations that Ancient Greek mathematicians had, namely that there are numbers that cannot be written as a ratio, or fraction, of whole numbers. Such numbers are called *irrational*. The square root of 2 is an example. But how do you prove something can never be done – isn't there always the chance that you've just not found a solution yet? The answer is this ingenious proof by contradiction.

$\sqrt{2}$ is irrational

Proof Suppose $\sqrt{2}$ is rational. Then we can write $\sqrt{2} = \frac{a}{b}$, where *a*, *b* are whole numbers, and by cancelling

any common factors we can assume they are coprime. Now square both sides: $\frac{a^2}{b^2} = 2$. This implies that $a^2 = 2b^2$. If *a* were an odd number, then a^2 would be odd, because the product of two odd numbers is odd. So *a* must be even, and we can write a = 2c for some integer *c*. Now a = 2c, so $2b^2 = (2c)^2 = 4c^2$. Cancelling the 2 we get $b^2 = 2c^2$. As before, this forces *b* to be even. But we said that *a* and *b* were coprime – and now we've shown they are both even, which is a contradiction. Thus, there is no expression for $\sqrt{2}$ as a fraction, and it is therefore irrational.

Changing the assumptions

You can't prove something from nothing. Every proof requires assumptions: these include the hypothesis of the statement, for instance in Pythagoras's Theorem that we have a right-angled triangle, and some agreed understanding of the definitions of the words used (like what a prime number is), but also we often rely on other results, like facts about similar triangles as in the case of the second proof I gave of Pythagoras's Theorem, and, if we go far enough back, we reach the basic assumptions, or axioms. Here's an example.

The angles in a triangle add up to 180°

Proof Take the triangle *ABC*. Draw a line through *A* parallel to *BC*.



Now, because alternating angles are equal, the angles marked x are equal and the angles marked y are equal. Angles on a straight line add up to 180°, and thus $x + y + z = 180^\circ$, as required.

It's so simple, but it does use some other facts which are either axioms that Euclid assumes as self-evident, or facts that Euclid has proved earlier, like that the angles on a straight line add up to 180° , or that alternating angles are equal, as well as "common notions", for example that things that are equal to the same thing are equal to each other. In particular, this proof relies on the socalled fifth postulate, the parallel postulate of Euclid, which says that given any line *L* and any point *A* not on *L*, there is a line

through *A* parallel to *L*. What we have really proved is that, *subject to the axioms of Euclidean geometry*, the angles in a triangle add up to 180° . If we remove the parallel postulate from our geometry, the proof isn't valid and it opens up the possibility that in some geometries, the angles in a triangle don't add up to

180°. And indeed that's exactly what happens in the geometry on the surface of a sphere. Here, we use the idea that a "straight line" is really just a shortest path between points to define "lines" on a sphere as geodesics – shortest paths. It turns out that these are arcs of great circles (like the equator). Long-haul flights follow these paths because they use the least fuel. It feels like understanding this geometry must be horribly complicated, but actually there's a beautiful relationship between the angles in a spherical triangle and the area of that triangle that is wonderfully simple to prove. It was first shown to me by the then Gresham Professor of Geometry, Christopher Zeeman, when I was still at school, and it impressed me profoundly!

Angles in a spherical triangle add up to more than 180°



On a sphere, if we take two great circles, they create a shape called a lune¹ – well, two identical lunes in fact, one antipodal to the other. The area of a lune with angle x is just $\frac{x}{360}$ ths of the total surface area *S* of the sphere. For a spherical triangle with angles x, y, and z, we can see that each pair of sides creates a pair of identical lunes. The six lunes cover the whole area of the sphere, but there is some overlap. The triangle appears in three of the lunes, and an antipodal copy of it appears in the other three, as shown in the two diagrams below².



The total surface area of the sphere equals the six lunes, minus four copies of the triangle. Say the triangle has area Δ . Then $S = 2\left(\frac{x}{360} + \frac{y}{360} + \frac{z}{360}\right)S - 4\Delta$, and so $x + y + z = 180\left(1 + \frac{4\Delta}{S}\right)$. This means that every spherical triangle has angle sum greater than 180° . Moreover, the amount by which the sum exceeds 180° is proportional to the area of the triangle! If, for instance, the triangle's area is one eighth the surface area of the sphere,

we get that the angle sum is 270°, which explains the three right angles of a triangle

with one vertex at the North Pole and the others on the equator at longitudes 0 and 90. This makes a lot of sense when you think that the smaller a triangle is as a proportion of the surface of the sphere, the closer it gets to being flat, and the closer its angle sum gets to 180°. In the limit, we'd end up with a triangle on the plane (or a sphere of infinite radius, if you prefer) and the angle sum would revert to the Euclidean 180°.

The future: can computers do proofs?

In an hour I can only show you short proofs. There are many other beautiful proofs that also involve wonderfully clear and ingenious arguments, but to experience them as "clear" you need several years of university level maths, and a "short" proof may be one that's a mere five pages instead of twenty. Some of the most famous theorems have proofs that run to hundreds of pages. There's a theorem in algebra called the Classification of Finite Simple Groups that takes up several books. Even this is a distillation of hundreds of earlier research articles. Meanwhile, proofs involving computer calculations, such as, famously, the Four Colour Theorem, are done on a machine precisely because they would take a human far too long. How do we know that these calculations are correct? Are these proofs valid? For me, yes. And the reason is that, as long as we check the program, the chance of a stray neutrino changing a 0 into a 1 and giving a false output feels to me lower than the chance that there's an error in one of the hundreds of pages of the proof of the Classification of Finite Simple Groups, or of Fermat's Last Theorem. Humans are considerably more fallible than machines, as long as we have definitely asked the machine to do what we actually want it to. I think I will always prefer proofs that I can grasp every line of for myself. But sometimes such proofs are elusive. Any proof is better than none! As well as computer-assisted proofs, where the machine carries out some of the calculations as directed by the human mathematician, another interesting development is proof-checking by machine. But can computers discover and prove entirely new theorems, unaided by humans? Sort of. There's no immediate danger of human mathematicians becoming obsolete. But it will be very interesting to see how such technology develops in the future.

¹ The lune diagram is from <u>https://commons.wikimedia.org/wiki/File:Regular digon in spherical geometry-2.svg</u> by Pbroks13, Public domain, via Wikimedia Commons.

² I've based these on a black and white diagram of a spherical triangle by Peter Mercator, usage under CC BY-SA 3.0 <u>https://commons.wikimedia.org/wiki/File:Spherical_trigonometry_Intersecting_circles.svg</u>, (Wikimedia commons)



Conclusion

The concept of proof is one of the defining characteristics of mathematics. Science, though it uses mathematics, is not itself mathematics. It's perhaps not fair to claim that the Ancient Greeks' theories about the four elements count as science. But even when what we call the scientific method got going, by which I mean conducting experiments rather than reasoning things out philosophically, we are still dealing with hypotheses continually refined by experiment. I'm not saying that Newton's laws are worthless, "F = ma" fits exceedingly well with experiment, but I also know that they cease to work so well at very high speeds, close to the speed of light. For that you need Einstein's special relativity. And there will no doubt be further refinements as time passes. In mathematics we don't have this problem of supersession because nothing is accepted into the canon until a valid proof has been found. In science there is no absolute proof – we could argue that science consists of things that have the potential to be disproved by experiment (science could never prove or disprove the existence of God, for example). Meanwhile, in a court of law, we only have to prove things "beyond reasonable doubt". In mathematics, by contrast, the burden of proof is much higher. In mathematics we prove things beyond unreasonable doubt.

I hope you've enjoyed this, and indeed all of my Gresham lectures. It's been a great honour to be the first woman to serve in this role. You can watch all my lectures online via the Gresham College website.

© Professor Sarah Hart, 2024



References and Further Reading

- You can watch this and all my other Gresham lectures online for free. The full list is at https://www.gresham.ac.uk/speakers/professor-sarah-hart
- If you want to explore just how many sequences begin 1, 2, 4, 8, 16... but are not the powers of 2, have a look at the fabulous Online Encyclopedia of Integer Sequences. You can enter any sequence of digits into the search bar and you'll get information about all the known interesting sequences containing that sequence of terms. https://oeis.org/
- There's an excellent YouTube channel dedicated entirely to visual proofs, and it has lots of really good animations and diagrams. <u>https://www.youtube.com/@MathVisualProofs</u>. One of my favourites, which I didn't have time to show today but is well worth a look, is the proof that it's possible, with a straightedge and compass construction, to divide a circle into seven (or indeed *n* for any positive integer *n*), pieces of equal area https://www.youtube.com/watch?v=KhfZK5IIK9E.
- The mathematician Paul Erdős used to say that God had a book of the best proofs of every theorem, and any exceptionally lovely proof would be referred to as a "proof from The Book". In tribute to that idea, Martin Aigner and Günter M. Ziegler assembled a collection of wonderful proofs of different theorems, including six proofs that there are infinitely many prime numbers. Most of them require university level mathematics, but if you have that, it's well worth a read. As Erdős said, "You don't have to believe in God, but you should believe in The Book".

Martin Aigner and Günter M. Ziegler. Proofs from The Book, Springer, 2009. ISBN 9783642008559.

© Professor Sarah Hart, 2024