The twelve minutes of Christmas!

More favourites from our "Maths in a Minute" library

By Marianne Freiberger
and Rachel Thomas

http://plus.maths.org

On the first day of Christmas, my true love gave to me…

… Perfect numbers!

A perfect number is a natural number whose divisors add up to the number itself. The number 6 is a perfect example: the divisors of 6 are 1, 2 and 3 (we exclude 6 itself, that is, we only consider *proper* divisors) and

1+2+3 = 6.

Hooray! People have known about perfect numbers for millennia and have always been fascinated by them. Saint Augustine (354–430) thought that the perfection of the number 6 is the reason why god chose to create the world in 6 days, taking a rest on the 7th. The Greek Nicomachus of Gerasa (60-120) thought that perfect numbers produce virtue, just measure, propriety and beauty. Numbers that are not perfect, for example numbers whose proper divisors add up to more than the number itself, Nichomachus found very disturbing. He accused them of producing excess, superfluity, exaggerations and abuse, and of being like animals with "ten mouths, or nine lips, and provided with three lines of teeth; or with a hundred arms, or having too many fingers on one of its hands."

If you play around with numbers for a while you will see why people have always been so fond of perfect numbers: they are very rare. The next one after 6 is 28, then it's 496, and for the fourth perfect number we have to go all the way up to 8128. Throughout antiquity, and until well into the middle ages, those four were the only perfect numbers that were known. Today we still only know of 48 of them, even though there are fast computers to help us find them. The largest so far, discovered in January 2013, has over 34 million digits.

Will we ever find another one? We can't be sure — mathematicians believe that there are infinitely many perfect numbers, so the supply will never run out, but nobody has been able to prove this. It's one of the great mysteries of mathematics. You can find out more in Number mysteries.

On the second day of Christmas, my true love gave to me…

… One of our favourite proofs!

Here's one of the most elegant proofs in the history of maths. It shows that $\sqrt{2}$ is an *irrational* number, in other words, that it cannot be written as a fraction a/b where a and b are whole numbers.

We start by assuming that $\sqrt{2}$ can be written as a fraction a/b and that a and b have no common factor — if they did, we could simply cancel it out. In symbols,

$$a/b = \sqrt{2}$$

Squaring both sides gives

$$a^2/b^2 = 2$$

and multiplying by b^2 gives

$$a^2 = 2b^2.$$

This means that a^2 is an even number: it's a multiple of 2. Now if a^2 is an even number, then so is a (you can check for yourself that the square of an odd number is odd). This means that a can be written as $2c$ for some other whole number c. Therefore,

$$2b^2 = a^2 = (2c)^2 = 4c^2.$$

Dividing through by 2 gives

$$b^2 = 2c^2.$$

This means that b^2 is even, which again means that b is even. But then, both a and b are even, which contradicts the assumption that they contain no common factor. This contradiction implies that our original assumption, that $\sqrt{2}$ can be written as a fraction a/b, must be false. Therefore, $\sqrt{2}$ is irrational.

On the third day of Christmas, my true love gave to me…

… Complex numbers!

Solving equations often involves taking square roots of numbers and if you're not careful you might accidentally take a square root of something that's negative. That isn't allowed of course, but if you hold your breath and just carry on, then you might eventually square the illegal entity again and end up with a negative number that's a perfectly valid solution to your equation.

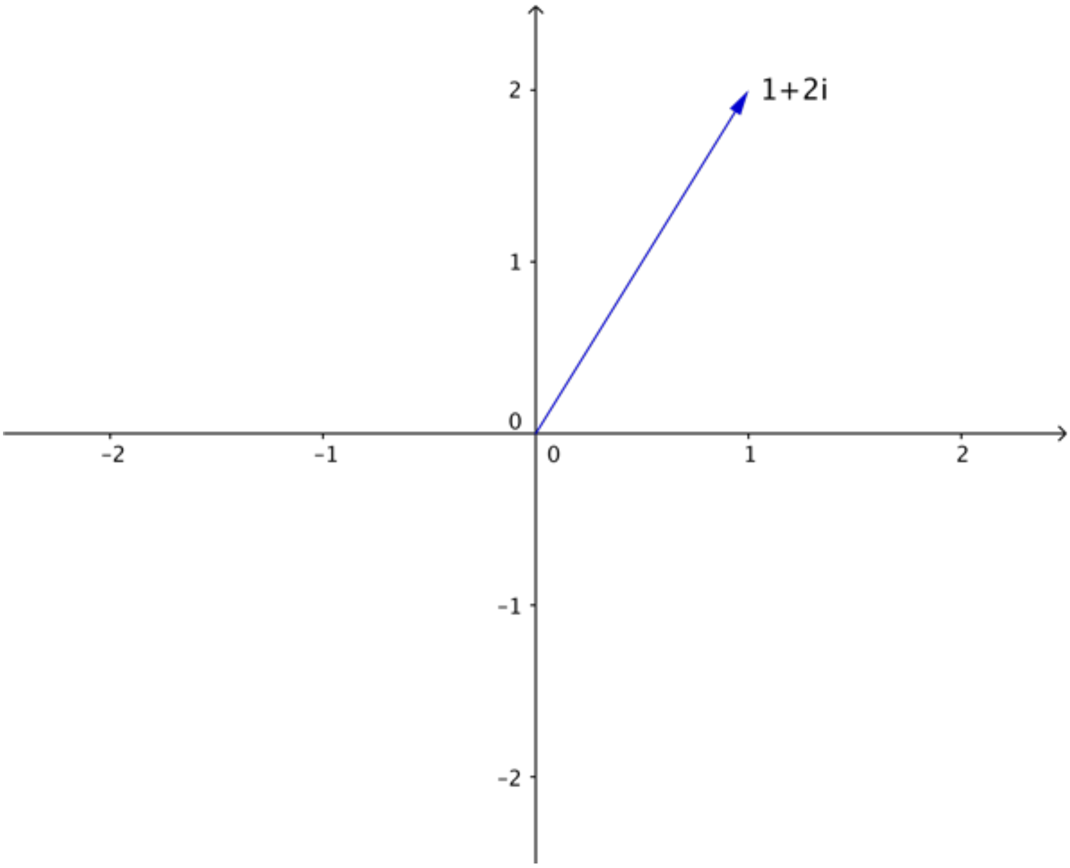
People first noticed this fact in the 15th century. A lot later on, in the 19th century, William Rowan Hamilton noticed that the illegal numbers you come across in this way can always be written as $x + iy$ where x and y are ordinary numbers and i stands for the square root of -1 The number i itself can be represented in this way with $x = 0$ and $y = 1$. Numbers of this form are called *complex numbers*.

You can add two complex numbers like this:

$$(x + iy) + (u + iv) = (x + u) + i(y + v)$$

And you multiply them like this:

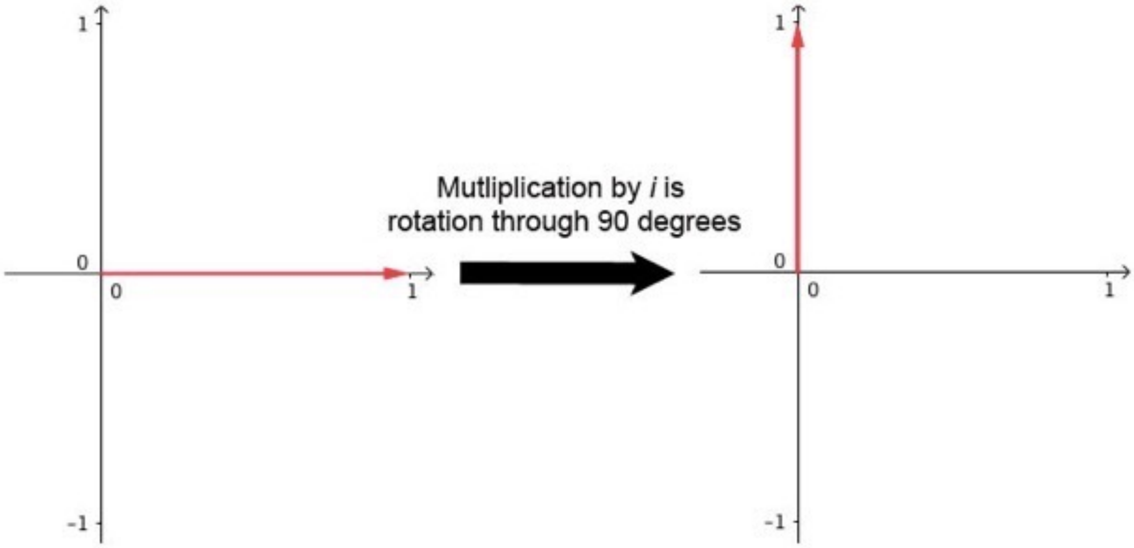
$$(x + iy)(u + iv) = xu + i(xv + yu) + i^2yv = xu - yv + i(xv - yu).$$



The complex number *1+2i*.

But how can we visualise these numbers and their addition and multiplication? The x and y components are normal numbers so we can associate to them the point with coordinates (x, y) on the plane, which is where you get to if you walk a distance x in the horizontal direction and a distance y in the vertical direction. So the complex number $(x+u) + i(y + v)$, which is the sum of $(x + iy)$ and $(u + iv)$, corresponds to the point you get to by walking a distance $x + u$ in the horizontal direction and a distance $y + v$ in the vertical direction. Makes sense.

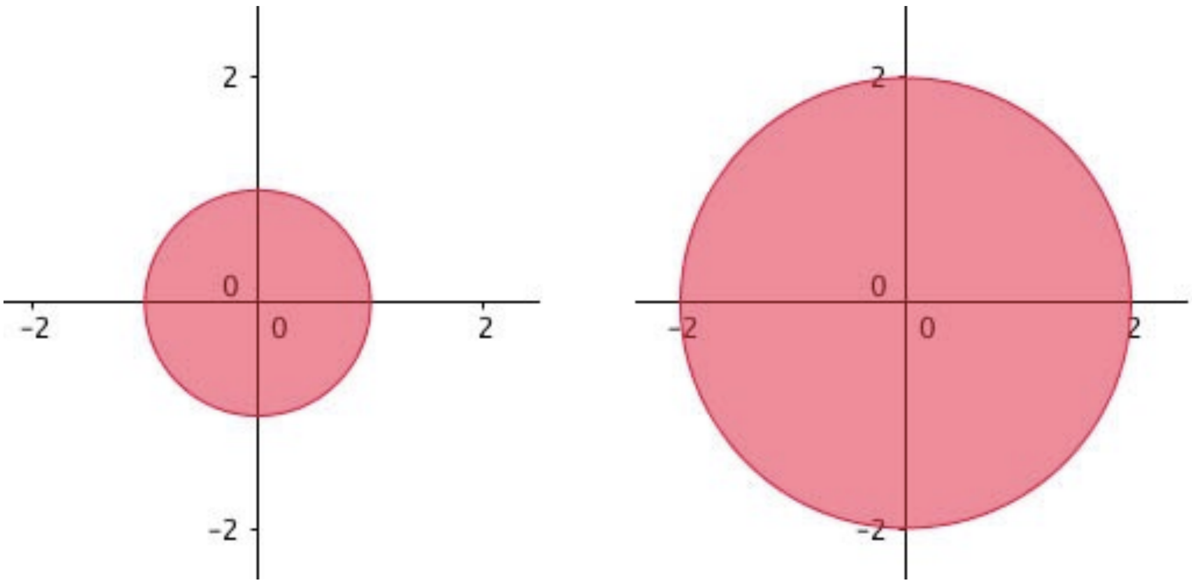
What about multiplication? Think of the numbers that lie on your horizontal axis with coordinates $(x, 0)$ Multiplying them by -1 flips them over to the other side of the point (0,0): (1,0) goes to (-1,0), (2,0) goes to (-2,0), and so on. In fact, you can think of multiplication by -1 as a rotation: you rotate the whole plane through 180 degrees about the point (0,0).



Multiplying by *i*.

What about multiplication by *i,* the square root of -1? Multiplying twice by *i* is the same as multiplying by -1. So if the latter corresponds to a rotation through 180 degrees, the former should correspond to rotation by 90 degrees. And this works. Try multiplying any complex number, say 2 + 5*i* by *i* and you will see that the result corresponds to the point you get to by rotating through 90 degrees (counter-clockwise) about (0,0)

And what about multiplying not just by *i* but by a more difficult complex number *u* + *iv*? Well, multiplying by an ordinary positive number corresponds to stretching or shrinking the plane: multiplication by 2 takes a point (*x,y*) to (2*x*, 2*y*) which is further away from (0,0) (that's stretching) and multiplication by 1/2 takes it to (*x*/2, *y*/2) which is closer to (0,0) (shrinking).



Multiplying by 2 is stretching.

It turns out that multiplication by a complex number $u + iv$ corresponds to a combination of rotation and shrinking/stretching. For example, multiplication by $-1 + 1.732i$ is rotation through 120 degrees followed by stretching by a factor of 2. So complex numbers are not just weird figments of the imagination designed to help you solve equations, they've got a geometric existence in their own right.

You can find out more about complex numbers and things you can do with them in the *Plus* articles Curious quaternions, Unveiling the Mandelbrot set, Non-Euclidean geometry and Indra's pearls and Maths goes to the movies.

On the fourth day of Christmas, my true love gave to me…

…A greedy algorithm!

Vending machines that don't return change are annoying, especially if the prices they demand aren't nice round figures you can make up with a single coin. If that's the case, then there's nothing but to hunt through your wallet, fishing out the right coins to make up the amount exactly. What's the best way of doing that? Without noticing many of us probably follow this recipe: find the biggest (as in largest denomination) coin that fits into the amount, then the next-biggest that fits into the remainder, and so on, until you (hopefully) hit the required sum. As an example, if you're being asked for 85p, you probably fish a 50p coin out first, then a 20p coin, then a 10p coin, and finally a 5p coin. And what if you haven't got all of the coins just mentioned in your wallet? In that case you follow the same recipe using what you've got.

This *greedy* recipe (greedy because you always go for the biggest coin that fits) seems to offer the best solution in that it seems to involve the fewest number of coins to make up the amount you need. For example, supposing you do have a 20p coin, but decide to go for two 10p coins instead, you increase the number of coins to make up 85p from four to five. So the greedy algorithm seems useful, not just for people struggling with vending machines, but also for cashiers returning change to customers.

But is greed really always the best option? It turns out that this depends on the coins that are available. Imagine, for example, you need to make up 8p. Greed would tell you to go for a 5p coin, then a 2p coin and then a 1p coin. And that's indeed the smallest number of coins to make up 8p with if you are using Pound Sterling, Euros, US Dollars, and most other currencies. But now imagine a currency that in addition to these denominations also has a 4p coin. Then you could make up 8p with two of those, beating the greedy strategy by one. Such a currency system might seem silly but it's not unheard-of: the pre-decimal British coinage system was one for which the greedy recipe failed when it came to minimising the number of coins needed to make up a given amount.

On the fifth day of Christmas, my true love gave to me…

…Countable infinity!

An infinite set is called *countable* if you can count it. In other words, it's called countable if you can put its members into one-to-one correspondence with the natural numbers 1, 2, 3, ... For example, a bag with infinitely many apples would be a countable infinity because (given an infinite amount of time) you can label the apples 1, 2, 3, etc.

Two countably infinite sets A and B are considered to have the same "size" (or *cardinality*) because you can pair each element in A with one and only one element in B so that no elements in either set are left over. This idea seems to make sense, but it has some funny consequences. For example, the even numbers are a countable infinity because you can link the number 2 to the number 1, the number 4 to 2, the number 6 to 3 and so on. So if you consider the totality of even numbers (not just a finite collection) then there are just as many of them as natural numbers, even though intuitively you'd think there should only be half as many.

Something similar goes for the rational numbers (all the numbers you can write as fractions). You can list them as follows: first write down all the fractions whose denominator and numerator add up to 2, then list all the ones where the sum comes to 3, then 4, etc. This is an unfailing recipe to list all the rationals, and once they are listed you can label them by the natural numbers 1, 2, 3, ... So there are just as many rationals as natural numbers, which again seems a bit odd because you'd think that there should be a lot more of them.

It was Galileo who first noticed these funny results and they put him off thinking about infinity. Later on the mathematician Georg Cantor revisited the idea. In fact, Cantor came up with a whole hierarchy of infinities, one "bigger" than the other, of which the countable infinity is the smallest. His ideas were controversial at first, but have now become an accepted part of pure mathematics.

To find out more about uncountable infinities, see Counting numbers. You can find out more about infinity in general in our collection of articles on infinity.

On the sixth day of Christmas, my true love gave to me…

…Counting numbers!

Are there more irrational numbers than rational numbers, or more rational numbers than irrational numbers? Well, there are infinitely many of both, so the question doesn't make sense. It turns out, however, that the set of rational numbers is infinite in a very different way from the set of irrational numbers.

As we saw here, the rational numbers (those that can be written as fractions) can be lined up one by one and labelled 1, 2, 3, 4, etc. They form what mathematicians call a *countable infinity*. The same isn't true of the irrational numbers (those that cannot be written as fractions): they form an uncountably infinite set. In 1873 the mathematician Georg Cantor came up with a beautiful and elegant proof of this fact. First notice that when we put the rational numbers and the irrational numbers together we get all the real numbers: each number on the line is either rational or irrational. If the irrational numbers were countable, just as the rationals are, then the real numbers would be countable too — it's not too hard to convince yourself of that.

So let’s suppose the real numbers are countable, so that we can make a list of them, for example

1. 0.1234567…
2. 1.4367892…
3. 2.3987851…
4. 3.7891234…
5. 4.1415695…

and so on, with every real number occurring somewhere in the infinite list. Now take the first digit after the decimal point of the first number, the second digit after the decimal point of the second number, the third digit after the decimal point of the third number, and so on, to get a new number 0.13816… .

Now change each digit of this new number, for example by adding 1 (and changing a 9 to a 0). This gives the new number 0.24927… . This new number is not the same as the first number on the list, because their first decimal digits are different. Neither is it the same as the second number on the list, because their second decimal digits are different. Carrying on like this shows that the new number is different from every single number on the list, and so it cannot appear anywhere in the list.

But we started with the assumption that every real number was on the list! The only way to avoid this contradiction is to admit that the assumption that the real numbers are countable is false. And this then also implies that the irrational numbers are uncountable.

It's easy to see that an uncountable infinity is "bigger" than a countable one. An uncountable infinity can form a continuum, such as the number line, in a way that a countable infinity can't. Cantor went on to define all sorts of other infinities too, one bigger than the other, with the countable infinity at the bottom of the hierarchy. When he first published these ideas, Cantor faced strong opposition from some of his colleagues. One of them, Henri Poincaré, described Cantor's ideas as a "grave disease" and another, Leopold Kronecker, went so far as to denounce Cantor as a "scientific charlatan" and "corrupter of youth". Cantor suffered severe mental health problems which may have resulted in part from the rejection his work had met with. But we now know that his work had simply come too soon: 150 years on, Cantor's ideas form a central pillar of mathematics and many of his results can be found in standard textbooks.

See our infinity page to find out more about this and other things to do with infinity.

On the seventh day of Christmas, my true love gave to me…

…The perfect voting system!

Is there a perfect voting system? In the 1950s the economist Kenneth Arrow asked himself this question and found that the answer is no, at least in the setting he imagined.

Kenneth defined a voting system as follows. There is a population of voters each of whom comes up with a preference ranking of the candidates. A voting system takes these millions of preference rankings as input and by some method returns a single ranking of candidates as output. The government can then be formed on the basis of this single ranking.

For a voting system to make any democratic sense, Kenneth required it to satisfy each of the following, fairly basic constraints:

1. The system should reflect the wishes of more than just one individual (so there's no dictator).
2. If all voters prefer candidate x to candidate y, then x should come above y in the final result (this condition is sometimes called *unanimity*).
3. The voting system should always return exactly one clear final ranking (this condition is known as *universality*).

He also added a fourth, slightly more subtle condition:

4. In the final result, whether one candidate is ranked above another, say x above y, should only depend on how individual voters ranked x compared to y. It shouldn't depend on how they ranked either of the two compared to a third candidate, z. Arrow called this condition *independence of irrelevant alternatives*.

Arrow proved mathematically that if there are three or more candidates and two or more voters, no voting system that works by taking voters' preference rankings as input and returns a single ranking as output can satisfy all the four conditions. His theorem, called *Arrow's Impossibility Theorem* helped to earn him the 1972 Nobel Prize in Economics.

You can find out more in the *Plus* articles Which voting system is best? and Electoral impossibilities.

On the eighth day of Christmas, my true love gave to me…

…The truth behind an important fallacy!

A woman's DNA matches that of a sample found at a crime scene. The chances of a DNA match are just one in two million, so the woman must be guilty, right?

Wrong. But it's a common mistake to make, known as the *prosecutor's fallacy*. It mistakes the one in two million for the probability of the woman's innocence. In order to assess the woman's guilt properly, we need to take the fact that she matched the sample as a given, and see how much more likely this makes her to be guilty than she was before the DNA evidence came to light.

A result called *Bayes' theorem* is useful in this context. The matching probability above implies that the woman's DNA is two million times more likely to match the sample if she is guilty, than if she is innocent. Bayes' theorem now says that:

Odds of guilt after DNA evidence = 2,000,000 x Odds of guilt before DNA evidence.

If our woman comes from a city of 500,000 people, and we think each of them is equally likely to have committed the crime, then her odds of guilt before the DNA evidence are about 1 in 500,000. Therefore:

Odds of guilt after DNA evidence = $2,000,000 \times 1/500,000 = 4$.

These are odds as we're used to them from the races. Translating the result into probabilities, this gives an 80% chance of guilt. Definitely not beyond reasonable doubt!

You can read more about the prosecutor's fallacy in *It's a match!*, which explores DNA evidence, and *Beyond reasonable doubt*, which explores a miscarriage of justice based on the fallacy.

On the ninth day of Christmas, my true love gave to me…

…Modular arithmetic!

You do modular arithmetic several times every day when you are thinking about time. Imagine, for example, you're going on a train trip at 11pm that lasts three hours. What time will you arrive? Not at 11+3 = 14 o'clock, but at 2 o'clock in the morning. That's because, on a 12-hour clock, you start counting from the beginning again after you get to 12. (On a 24-hour clock, you start again after you get to 24.) So, on a 12-hour clock you have:

4 + 9 = 1,
7 + 7 = 2,
5 + 12 = 5,

and so on. When you are subtracting hours, you do the same but backwards:

4 - 7 = 9
1 - 11 = 2
6 - 12 = 6.

You could play the same game using other numbers, apart from 12 and 24, to define your cycle. For example, in modular arithmetic *modulo* 5 you have

4 + 2 = 1
3 + 4 = 2
1 - 4 = 2
3 - 5 = 3.

These sums can be a little tedious to work out if you're counting on your fingers, but luckily there is a general method. Let's say you're doing arithmetic modulo some natural number p and you're looking at some other natural number x. To find the value of x modulo p (the value of x on a clock with p hours), compute the remainder when dividing x by p: that's your result.

This also works when x is negative (noting that the remainder is defined to be always positive). For example, for $p = 12$ and $x = -3$ we have

-3 = (-1) x 12 + 9,

so the remainder is 9. Therefore -3 modulo 12 is equal to 9. (If you use the modulus function in some computer languages you have to be a little careful though, as some return a different value for negative numbers.)

If you want to add or subtract two numbers module some natural number p, you simply work out the result, call it x, in ordinary arithmetic and then find the value of x modulo p.

There is clearly something very cyclical about modular arithmetic. Whatever number p defines your arithmetic, you can think of it as counting forward or backward in clock with p hours. To put this in technical maths language, modular arithmetic modulo p gives you a cyclic group of order p. You can find out more about group theory in this *Plus* article and about modular arithmetic on our sister site NRICH.

On the tenth day of Christmas, my true love gave to me…

…The fundamental group!

Topologists famously think that a doughnut is the same as a coffee cup because one can be deformed into the other without tearing or cutting. In other words, topology doesn't care about exact measurements of quantities like lengths, angles and areas. Instead, it looks only at the overall shape of an object, considering two objects to be the same as long as you can morph one into the other without breaking it. But how do you work with such a slippery concept?

One useful tool is what's called the *fundamental group* of a shape. Take the sphere as an example. Pick a point *A* on the sphere and consider all the loops through that point - i.e. you look at all the paths you can trace out on the sphere which start and end at your point *A*. You consider two loops to be equivalent if you can morph one into the other without cutting either of them. You can combine two loops *p* and *q* to get a third one by simply going around *p* first and then going around *q*. Also, if you traverse a loop in the clockwise direction, then this movement has an opposite, or an *inverse*, which is traversing it in the counterclockwise direction.

These two properties, that two loops can be combined to get a third and that every loop has an inverse (together with a couple of other properties), mean that the set of loops (where you consider two loops as equivalent if the can be morphed into one another) form a neat and self-contained structure called a *group*. It turns out that as long as your object is *path-connected* (there's a path linking any two points on it) this structure is the same no matter which point *A* you used as the base for your loops.

Now on the sphere every loop can be transformed into every other loop. In particular, every loop can be contracted into the trivial loop, which goes nowhere and is just your base point *A*. The fundamental group in this case is also *trivial*, in other words it contains just one loop. This is true not only for the perfectly round sphere, but also for a deflated football, and for any other 2D surface that's topologically the same as the sphere.

But now think of the surface of a doughnut, also called a *torus*. In this case not all loops can be contracted to a point because they may wind around the hole of the torus and also around its body. A general loop may wind around the hole a total of *m* times and around the body a total of *n* times. It turns out that any two loops are equivalent if they wind around the hole the same number of times and also wind around the body the same number of times. The fundamental group of the torus is the same as a group structure you get from looking at ordered pairs of whole numbers (to be precise, it's same as the *direct product* *Z*x*Z*, where *Z* is the set of whole numbers). This is true not only for a perfectly round torus, but also for a really irregular and lumpy one. So the direct product of *Z*x*Z*, which is a well-understood structure, gives a good characterisation of tori, regardless of their exact geometry.

The concept of fundamental group is a powerful tool in topology, where you can't use precise measurements to describe an object. It's also connected to one of the trickiest problems of modern maths: the Poincaré conjecture. It seems obvious that any object with a trivial fundamental group is topologically the same as the sphere: a trivial fundamental group means that the object has no holes for the loops to wind around and if there are no holes, then the object can always be deformed into a perfect sphere. At the beginning of the twentieth century Henri Poincaré asked whether a similar statement was true for the 3D sphere (which is hard for us to visualise) and found the problem was a lot trickier. It took around 100 years to prove that the answer is yes.

Read more about the Poincaré conjecture, about topology in general and about groups on *Plus*.

On the eleventh day of Christmas, my true love gave to me…

…The catenary!

When you suspend a chain from two hooks and let it hang naturally under its own weight, the curve it describes is called a *catenary*. Any hanging chain will naturally find this equilibrium shape, in which the forces of tension (coming from the hooks holding the chain up) and the force of gravity pulling downwards exactly balance.

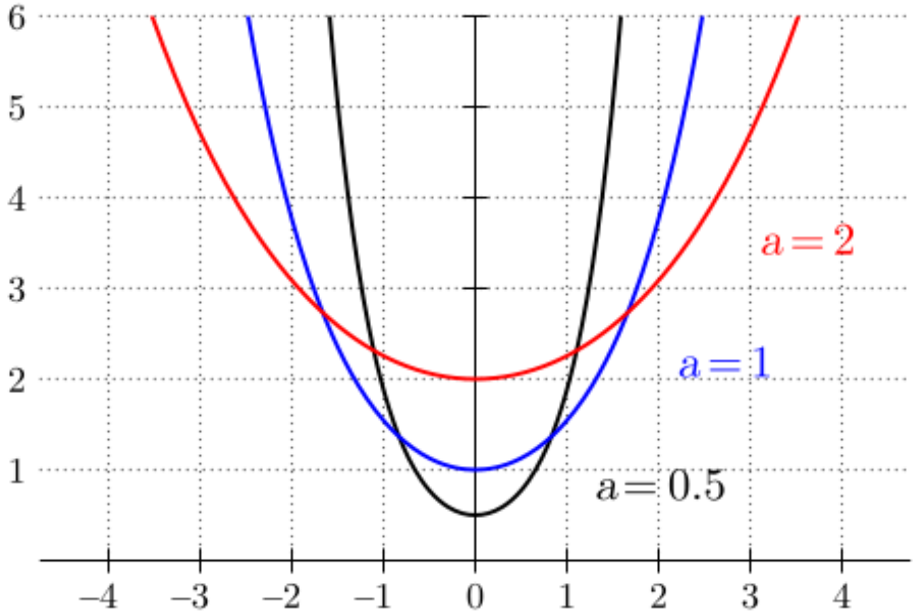
Something beautiful happens when you turn a catenary curve upside down. The inverted catenary will now describe an arch — and it turns out that it's the most stable shape an arch can have. In a hanging chain the forces of tension all act along the line of the curve. In the inverted catenary the forces of tension become forces of compression. And since these forces are directed along the line of the arch, the arch doesn't bend or buckle. If you want to build an arch, you should make sure it contains the shape of an inverted catenary. That way it will stand freely under its own weight and you'll also need to use a minimal amount of materials.

The English architect Robert Hooke was the first to study the catenary mathematically and in 1675 published an anagram (in Latin) of : "As hangs the flexible line, so but inverted will stand the rigid arch." The arch above Wembley Stadium has the shape of a catenary and Christopher Wren also intended to use it in St. Paul's dome (find out more about St. Paul's here).

The equation of the catenary is

$a(e^{x/a} + e^{-x/a})/2.$

This gives a whole family of curves, one for each value of the parameter *a*, which determines the width of the catenary and also its lowest point above the *x*-axis.



The catenary for different values of *a*. Image: Geek3, CC BY-SA 3.0.

On the twelfth day of Christmas, my true love gave to me…

…The second law of thermodynamics!

Occasionally our colleague Owen, who we share the *Plus* office with, despairs of our messy desk and tidies it up. Our newly tidied desk is very ordered and hence, in the language of physics, has low *entropy*. Entropy is a measure of disorder of a physical system. And, as Owen knows from personal experience, the entropy of our desk is certain to increase as it will become messier and messier each time we appear in the office. Essentially this comes down to a probabilistic argument — there are so many more ways for our desk to be messy and just a few limited ways for it to be tidy. So unless someone intervenes and tidies it up (which we must admit isn't our strong point) the entropy is certain to increase.

Really it isn't our fault — you can't fight the laws of physics and this is one of the most fundamental ones: *the second law of thermodynamics*. The entropy of an isolated system never decreases. The law explains not only why desks never tidy themselves when left alone, but also why ice melts in your drink. All systems evolve to maximal entropy: the highly structured ice-cubes in the warmer liquid form an inherently more ordered system than one where the ice has melted and all the particles of the ex-cubes and drink have mingled together. The highest entropy state of a system is also its equilibrium.

The second law of thermodynamics comes from the area of *statistical mechanics* which describes the behaviour of large numbers of objects using statistical principles. One obvious place this is useful is in the behaviour of gases or liquids. We could try to write down (or simulate in a computer) the Newtonian equations that describe each and every gas particle and all possible interactions between them, but that would just be silly: there are around $3\text{x}10^{22}$ molecules in a litre of air so we would need a huge number of equations just to describe the behaviour of each of these individually, let alone their interaction. Instead you can predict the bulk behaviour of the whole system using statistics.

For example, if you take the lid off a jar of gas in an empty box you intuitively know that the gas won't stay in the jar, it will gradually spread till it evenly fills all the space available. Out of all the possible arrangements of gas particles in the box, only a tiny number of correspond to the gas remaining inside the now open jar. These are far outnumbered by the possible arrangements of gas molecules spread through the whole box. The fact that the gas molecules invariably spread out and don't move back into the jar is not a certainty, it's just overwhelmingly more likely.

It may seem strange at first that a law of nature, such as the second law of thermodynamics, is based on statistical likelihood — after all, laws are about certainties and likelihoods incorporate the fact that there is uncertainty. To illustrate just how unlikely a violation of this law is, the French mathematician, Émile Borel, used an intriguing metaphor: he said that if a million monkeys typed for ten hours a day for a year, it would be unlikely that their combined writings would exactly equal the content of the world's richest libraries — and that a violation of the laws of statistical mechanics would be even more unlikely than that. The British physicist Arthur Eddington captured the strange link between chance and certainty beautifully when he wrote, "When numbers are large, chance is the best warrant for certainty. Happily in the study of molecules and energy and radiation in bulk we have to deal with a vast population, and we reach a certainty which does not always reward the expectations of those who court the fickle goddess."

You can read more about entropy and typing monkeys on *Plus*.

A very merry Christmas from everyone here at Plus magazine!