Numbers - the evolution of an idea

The first numbers that we encounter as children are the positive integers, or counting numbers, which we often learn by numbering off the fingers on one hand, one two, three, four, five - and, not long after, the fingers on both hands 1, 2, 3, 4, 5, 6, 7, 8, 9, 10. It's interesting that our most familiar counting mode, and representation of numbers is determined by our biology. If we only had 4 digits on each hand, we would probably be living in an octal world rather than a decimal one. A little while later, we learn to do arithmetic on those numbers, usually in the context of counting some objects Starting with **addition**, for example " 5 bananas plus 3 bananas = 8 bananas ", which we can make more abstract by writing " 5 + 3 = 8", because we know that we will get the same result whether we are adding bananas, or fingers, or apples.

Often we learn the notion of **subtraction** in a similar context: " 5 bananas take away 3 bananas leaves 2 bananas", or abstracting again, " 5 - 3 = 2 " And if you are old like me, you will remember the song " yes, we have no bananas..." and in mathematics we introduce the symbol "zero, or 0", so that we could sing instead "yes, we have zero bananas" or write " yes, we have 0 bananas".

So far, so good, then someone asks us "3 - 5 = what?". If we refer back to our concrete example, and ask the question " 3 bananas take away 5 bananas leaves what?" then clearly the only sensible answer is that we can't do it. So, as mathematicians, how do we proceed? Well, we invent a whole set of **negative integers** " -1, -2 , -3, -4, ... " with the property that for each positive integer "n", there is a matching integer "-n", with the property that "n + (-n) = 0". Armed with this new invention we can say " 3 - 5 = -2 ", even though it still won't make any

sense to go into the fruit shop and try to buy " -2 bananas". The place where you might see both positive and negative numbers in the "real world" might be in your bank account, where the total might be "+ $100 ", written "$100 CR", or " - $100 " written "$100 DR" or "$100" in red ink.

The next invention of the mathematician is **multiplication**, which embodies the idea of repeated addition. Thus, we write "8 + 8 + 8 + 8 + 8 = 5 times 8 = 5 * 8". I am using the " * " symbol to represent multiplication, because it is the common multiplication symbol in all computer languages, where " x " is likely to be the name of a variable. I imagine that you all learnt the "times tables" in primary school which make mental arithmetic so much easier than it would be if we had to do repeated addition. Once we want to apply multiplication to zero and the negative integers, we need some new rules to ensure that our expanded arithmetic remains consistent. The extra rules we live by are:

- " 1 * n = n " for any n. "1 " is called the "multiplicative identity" in the same way as "0" is called the additive identity because " 0 + n = n " but you don't have to remember these names for now.
- "m * (-n) = - (m * n)" for any m and n.
- and of course you know from counting, and from your tables, that " m + n = n + m" and "m * n = n * m".

Now we come to a familiar problem at birthday parties. There are 6 lollies left, and 3 children at the party, so we can **divide** them equally and give 2 lollies to each child: " 6 / 3 = 2 " However there are only 5 balloons. "5 / 3 = what? " This presents an insoluble problem to the party organiser, but none to the visiting mathematician, who says" No problem: we will invent **fractions** or **rational numbers** and give each child $\frac{5}{3}$ balloons. I know

some people find fractions harder to deal with, because we have to invent a number of new rules to process them, and there is just more arithmetic involved.

- **addition** $\frac{m}{n} + \frac{p}{q} = \frac{m*q+n*p}{n*q}$
- **subtraction** $\frac{m}{n} - \frac{p}{q} = \frac{m*q-n*p}{n*q}$
- **multiplication** $\frac{m}{n} * \frac{p}{q} = \frac{m*p}{n*q}$
- **division** $\frac{m}{n} / \frac{p}{q} = \frac{m*q}{n*p}$

The one fraction that we cannot manage is $\frac{m}{0}$ for any non-zero m. We say that the result is **infinite** and use the symbol ∞ to represent it.

The other way that we represent numbers is as a decimal expansion, for example 12.345 which we interpret as $1 * 10^1 + 2 * 10^0 + 3 * 10^{-1} + 4 * 10^{-2} + 5 * 10^{-3}$

We can recognise any fraction as a repeating decimal expansion. For example

- $\frac{1}{4} = 0.2500000000\ldots$
- $\frac{5}{3} = 1.666666666666\ldots$

If we see a repeating decimal expansion, we can turn that into its fractional form fairly easiiy:

- $x = 0.123123123123\ldots$
- $1000 * x = 123,123123123\ldots$
- so $999 * x = 123$ and $x = \frac{123}{999} = \frac{41}{333}$

Just as an aside, how did we know that 123 was divisible by 3 ? 999 is pretty obvious. Well, if we did not see it straight away, we could have used the rule "An integer is divisible by 3 if the sum

of its decimal digits is divisible by 3". Have you ever wondered why that rule is true? If you look at the following, it should be fairly clear:

$$123 = 1*100+2*10+3*1 = 1*(99+1)+2*(9+1)+3 = 1*99+2*9+(1+2+3)$$

and 3 divides each term on the right. This immediately suggests the way to show a second rule that you might not be familiar with: " An integer is divisible by 9 if the sum of its decimal digits is divisible by 9." Try it for 34254.

One of the trickier ideas associated with the fractions, or rationals, comes when we try to count how many of them there are. If we think about the number of positive integers that there are, we can start counting $1, 2, 3, 4, 5, 6 \ldots$ and we say that there are a **countable infinity** of these positive integers. Now, obviously there are more rationals than there are positive integers, but if we can find a way of writing the rationals down in an order where we can say where each appears, we say that we can find a mapping from the rationals to the integers. Here is such a mapping : $\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{2}{2}, \frac{3}{1}, \frac{1}{4}, \frac{2}{3}, \frac{3}{2}, \frac{4}{1}, \frac{1}{5} \ldots$ Having found that mapping, we can say there are a countable infinity of rational numbers as well. Obviously the term **countable infinity** is somewhat elastic. If you have trouble getting your head around this idea, join the other 99.9% of the population, including me.

We will need to use the notion of **prime integers** before we go too much further, so we might as well talk a little about them now. There is a lot known about primes, so we will just mention a few ideas. Firstly, an integer n is prime, if the only integers that divide it with no remainder, are 1 and the number n itself. The first few prime numbers are $2, 3, 5, 7, 11, 13, 17, 19, 23 \ldots$ In fact we know that this sequence of primes goes on forever, and that there are a countable infinity of primes, because again we can lay them out in order to define a mapping from the integers. The

proof is interesting, because you might not already have encountered a **proof by contradiction**. Assume that there only a finite number M of primes $p_1, p_2, p_3, \ldots p_M$ Consider the integer $p_1 p_2 p_3 \ldots p_m + 1$ It is not exactly divisible by any of the primes p_i , which all leave a remainder of 1, so it must be prime itself. But this contradicts our assumption that there are only a finite number M of primes, so that assumption must be false. That is to say, there must be an infinite number of primes.

We can write any integer as the product of its prime factors. For example, we can write $3600 = 2^4 * 3^2 * 5^2$, or $343 = 7^3$. Looking at these two prime factorisations, we can see immediately that the highest common factor of the two is 1. Whereas, if we compare 3600 with $375 = 3 * 5^3$ we can read off the common factor as $3 * 5^2 = 75$. There are many fascinating properties of primes that mathematicians over the centuries have been able to prove, but there is one fairly simple proposition that people have been unable to prove or disprove. The **Goldbach conjecture** is that any even integer can be written as the sum of two primes. For example $6 = 3 + 3$, $8 = 3 + 5$, $10 = 5 + 5$, or $10 = 3 + 7$, $12 = 5 + 7$, and so on. If you can't go to sleep at night, you can see how far up the chain of even numbers you can get, instead of counting sheep.

One of the important uses of prime numbers that we rely on increasingly, is the RSA algorithm that secures our internet transactions when we make a https:// connection. I hope we might have time to look at the RSA algorithm one day. It relies on the fact that if we generate two very large primes and multiply them together, it will be beyond the capability of present-day computers to find those two factors, whch can be used to decrypt messages encoded with the composite product number. If you follow the popular press, you might see that quantum computers might one day be able to break the composite number into its prime factors

using an algorithm already described by Peter Shor. So the race to build a quantum computer is not entirely academic, and Microsoft is already specifying a computer language with which to program them.

One of the important numerical operators we use regularly is the **square root**. For example, $\sqrt{9} = 3$, which we can define to be the number, which when multiplied by itself, gives us the number we started with. That is to say, x solves the equation $x^2 = y$ where y is any number. Just introducing this one operator forces us to expand our whole idea of what a number can be. For example, consider $\sqrt{2} = 1.41421\ldots$. If you have a calculator, or computer, it will give you lots more digits than I have quoted, but because it doesn't give you an infinite number of digits, you can't tell whether we can write $\sqrt{2} =$ a rational, m/n, but we can fairly easily establish that it is not, by another proof by contradiction. Suppose $m = 2^{p_2} * 3^{p_3} * 5^{p_5} * \ldots$ and $n = 2^{q_2} * 3^{q_3} * 5^{q_5} \ldots$.

- $\sqrt{2} = m/n$
- $n * \sqrt{2} = m$
- $2 * n^2 = m^2$
- $2 * 2^{2q_2} * 3^{2q_3} * 5^{2q_5} \ldots = 2^{2p_2} * 3^{2p_3} * 5^{2_5} \ldots$

and we see that on one side the power of 2 is even, while on the other side it is odd, which gives us our contradiction. So $\sqrt{2}$ cannot be rational. In fact $\sqrt{2}$ is just one of the uncountably infinite family of **irrational numbers** which do not have a repeating decimal representation. I won't burden you with the proof that it's an uncountably infinite set. You can look it up if you want to. Together the integers, rationals, and irrationals, make up the set of **real numbers** which you can imagine stretched out along a line from $-\infty$ to $+\infty$. Two of the most notable irrational

numbers are π, known for millenia as the ratio of the circumference of a circle to its diameter, and e the factor underlying the term exponential growth, so beloved of our politicians.

You might think at this stage our zoo of numbers is now fully occupied, but nothing could be further from the truth. Mathematicians over the centuries have continued to exercise their imaginations, and many of our modern day physical phenomena, such as electromagnetic radiation, or the quantum mechanical behaviour of atoms can be described mathematically using their next invention. You all know the formula for solving for the roots of a quadratic equation $a * x^2 + b * x + c = 0$ The roots are $x = \frac{-b \pm \sqrt{(b^2 - 4 * a * c)}}{2 * a}$

What happens when we apply that formula to the quadratic equation $x^2 - 2 * x + 2 = 0$? If you graph the function $y(x) = x^2 - 2 * x + 2$, you will see that the graph never crosses the x axis so there are no real roots. " No problem, says the Italian mathematician Cardano, visiting from the 16th century. We will invent a new **imaginary number** $i = \sqrt{-1}$, and **complex numbers** with the form $z = x + i * y$ with a real and an imaginary part. This new invention immediately gives us an answer to our quadratic equation problem.

- $x = \frac{-(-2) \pm \sqrt{(-2)^2 - 4 * 1 * 2}}{2 * 1} = \frac{2 \pm \sqrt{4 * i^2}}{2}$
- $x = 1 \pm i$

Of course, once Cardano had invented these complex numbers he had to define a whole set of arithmetic operations for these entities which were consistent with the arithmetic operations on real numbers. The theory of complex numbers is too large to explore here, so I will show the simple set of operations, and we will stop. If we had more time we could explore the Argand diagram and the (r, θ) representation of complex numbers.

- $z_1 = x_1 + i * y_1$
- $z_2 = x_2 + i * y_2$
- $z_2^* = x_2 - i * y_2$, the **complex conjugate** of z_2 which helps with division.
- $z_1 + z_2 = (x_1 + x_2) + i * (y_1 + y_2)$
- $z_1 - z_2 = (x_1 - x_2) + i * (y_1 - y_2)$
- $z_1 * z_2 = (x_1 * x_2 - y_1 * y_2) + i * (x_1 * y_2 + x_2 * y_1)$
- $z_1/z_2 = (z_1 * z_2^*)/(z_2 * z_2^*) = (z_1 * z_2^*)/(x_2^2 + y_2^2)$

Long after complex numbers were defined, and used over the centuries, people like Babbage, Alan Turing, and John von Neumann came up with the invention of digital computation, and Ada, the Countess of Lovelace, and others, started to program them. Modern electronic computers use transistors which essentially can store binary information as a 0 or a 1. So to represent the decimal numbers we are more familiar with, we have to follow the arithmetic that we would have used if we only had 2 fingers and not 10, and learn to play with **binary numbers**.

When we write a decimal integer like 1234 we mean

$$1234 = 1 * 10^3 + 2 * 10^2 + 3 * 10^1 + 4 * 10^0$$

In binary arithmetic, we only have the digits 0 and 1 at our disposal, and powers of 2 and not powers of 10, so to represent the decimal number 1234 in binary, we have to say:

$$\begin{aligned} 1234 &= 1024 + 128 + 64 + 16 + 2 \\ &= 1 * 2^{10} + 0 * 2^9 + 0 * 2^8 + 1 * 2^7 + 1 * 2^6 + 0 * 2^5 + 1 * 2^4 + 0 * 2^3 + 0 \\ &= 10011010010 \end{aligned}$$

You can see that binary representations of large integers will quickly became unmanagable by us poor humans, so it's lucky that

they are childs play for the modern digital computer, whether it's in your laptop or iphone. To make binary numbers produced by computers more readable, we often print them out in groups of three (octal) or groups of four (hexadecimal). These are summarised in the tables below:

binary	octal
000	0
001	1
010	2
011	3
100	4
101	5
110	6
111	7

binary	hexadecimal
0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	A
1011	B
1100	C
1101	D
1110	E
1111	F

You should try writing the decimal number 1234 in octal and hexadecimal just to see that you have the hang of it. If we have more time, we can explore how negative integers are stored (two's complement), and and real numbers like 12345.6789 are stored, using Kahan's IEEE754 format. Of course digital computers also have to store alphanumeric data, such as peoples' names, and web addresses, and these have specially defined formats like ASCII. You should google "character encoding" if you want to know more about how different character sets in different languages are handled.

Finally, you might occasionally wonder, when we have chosen to embrace the metric system of weights and measures, and decimal currency, why we still have 60 seconds in a minute, 60 minutes in an hour, 360 in degrees in a circle. We have to thank the ancient Sumerians and Babylonians for handing us this legacy. 60 is a very useful number to use as a base. We can divide it exactly by $2, 3, 4, 5, 6, 10, 15, 20$ and 30, as we routinely do every day with time and angles.