The Two Most Important Numbers: Zero and One

R (Chandra) Chandrasekhar

2023-10-31 | 2023-11-08

The unique properties of the numbers zero and one make them mathematically interesting and indispensable. In this slow-paced stroll though the ideas streaming out of these two numbers, we uncover well-known as well as relatively obscure facts about them. It is hoped that in the process we may discover how they cement together disparate areas of Mathematics.

Starting at the beginning

At first, I thought I would skirt around the formal sets of numbers, and concepts like commutativity and associativity, and keep this blog very informal. But I found that each time I tried that approach, I would have to furtively sneak in a paragraph here, or a footnote there, to explain these ideas. In the end, I decided to start at the beginning, and work my way through the natural numbers, the integers, the rationals, etc., and broach ideas like commutativity and associativity.

Counting

Aeons ago, a shepherd with five sheep might have counted, "one sheep, two sheep, three sheep, four sheep, and five sheep." But wait! Since he did not have the names for numbers—nor indeed the abstract concept of a number—he could not have done that. So, what did he do? Let us speculate.

Naming sheep

He could have given *unique* names to each of his five sheep and developed enough familiarity with them to identify them by name. Then all he needed to do was to check that his entire flock was home by sundown. But such a method would have become cumbersome and error-prone as his sheep multiplied.

One-to-one correspondence

The later, and more likely, alternative was to use stones to correspond to sheep. He could have taken a leather bag and dropped a stone in it—one for each sheep that he owned. He did not need to learn counting. All he needed to do was to establish a one-to-one correspondence[1] between sheep and stone. As long as he had the right number of stones in his bag, he could account for each one of his sheep.

---

[1] One-to-one correspondence is a simple but extremely powerful idea which guided Georg Cantor to develop his radical but consistent ideas about types of infinity.

The Latin word for *stone* is calculus, and from the stone has come the whole science of *calculation*.

Measurement

When we *count,* as with sheep, where do we start? We start with one. We do not start with zero, because we cannot point to any sheep or other object and say "zero".

Nevertheless, zero has fundamental importance when we start *measuring*. When the petrol tank in a car is empty, we can fill it up and measure the volume of petrol for which we have to pay.

When we count, we start with 1.

When we measure, we start with 0.

Sets of numbers

Although Mathematics has rigorous foundations, at the very bottom, its notions are not defined explicitly. One such notion is that of a *set*, which is loosely defined as a collection of objects that can either be enumerated or described clearly. The *sets of numbers* we will deal with have names, symbols, and definitions as shown below.

Table 1: Sets of numbers

Name	Symbol	Definition
Natural numbers	$\mathbb{N}$	$\{1, 2, 3, 4, ...\}$
Integers	$\mathbb{Z}$	$\{..., -3, -2, -1, 0, 1, 2, 3, ...\}$
Rational numbers	$\mathbb{Q}$	$\{x : x = \frac{p}{q} \text{ where } p, q \in \mathbb{Z} \text{ and } q \neq 0\}$
Irrational numbers		$\{\text{The numbers which are not rational}\}$
Real numbers	$\mathbb{R}$	$\{\text{The rationals and the irrationals}\}$
Complex numbers	$\mathbb{C}$	$\{a + ib : a, b \in \mathbb{R} \text{ and } i^2 = -1\}$

While it is premature to talk about these sets and their peculiarities in this blog, it is worth making some points about them.

1. The symbols in the second column are called blackboard bold letters.

2. A set is traditionally enclosed in a pair of *braces*: {}.

3. Zero is neither positive nor negative. It is simply its unique self. As a set on its own, zero is often denoted {0}.

4. The numbers we use for counting, starting from 1, and never ending, are—naurally enough—called the *natural numbers*, denoted $\mathbb{N}$. There is no agreement on whether or not to include zero as a member of $\mathbb{N}$. I have chosen not to, because we start counting with one.

5. The *integers* are named $\mathbb{Z}$ after the German word *Zahlen* which stands for "numbers" (singular *Zahl*). The integers include positive and negative whole numbers as well as zero.

6. The *rational numbers* are so named because they are really *ratios* of whole numbers with the proviso that the denominator cannot be zero. The symbol $\mathbb{Q}$ is used because it denotes *quotient*—the result of *division.*

7. There is no symbol for the *irrationals*, which are simply defined as numbers which are *not rational.* In fact, the set of irrationals may be shown, using set notation only indirectly as $\mathbb{R} \setminus \mathbb{Q}$, which means the set of real numbers, excluding the rational numbers.

8. The *real numbers*, with symbol $\mathbb{R}$ for real, are glibly described as the union of the rational numbers and the irrational numbers[2] [1].

9. The *complex* numbers incorporate a non-real entity, called i the *imaginary unit*, which is defined as $i^2 = -1$. Since every real number when squared is greater than or equal to zero, this i is not a real number, and therefore demands its own symbol, arithmetic, and set, $\mathbb{C}$.

Abstract Algebra

In the nineteenth century, mathematicians contemplated the then extant mathematical systems and recognized certain commonalities. Whether it was arithmetic or geometry, or some other branch of mathematics, they were able to distil certain underlying principles behind the common practices of mathematics. By systematizing and classifying what they observed, they were able to *invent* names for the *classes of objects* they discerned, along with their properties. Thus was born abstract algebra. The ideas of commutativity, associativity, the additive and multiplicative identities, and the additive and multiplicative inverses were born from this exercise in classification. If you wish to know more, I strongly recommend this short video on abstract algebra to whet your appetite.

The Four Arithmetic Operations

Each of the four basic arithmetic operations–addition, multiplication, subtraction, division—are binary operations and may *only* be performed between *two* numbers. The ability to *add* multiple numbers—as in determining the total sum to be paid at the checkout counter while shopping—is made possible by the commutativity and associativity of addition, which also applies to multiplication. Subtraction and division are neither commutative nor associative.[3]

Commutativity and Associativity

Let us add three numbers, 2, 3, and 5. It is common to write this as $2 + 3 + 5 = 10$. The sum 10 is correct, but its correctness is derived from the commutativity and associativity of addition.

In commutativity, we have

$$2 + 3 = 3 + 2.$$

The order of the two operands may be interchanged.

---

[2]Richard Dedekind with his *Schnitt* or cut, showed that the rationals and irrationals comprise $\mathbb{R}$, but that is a story for another day and another blog.
[3]For a start, subtraction is not commutative: $3 - 2 = 1 \neq -1 = 2 - 3$.

In associativity, we have *three operands*. We use parentheses to denote the operation we perform first. Associativity means that it does not matter which pair we add initially:

$$(2 + 3) + 5 = 2 + (3 + 5).$$

Together, commutativity and associativity allow us to be casual about the order in which we add several numbers.

Multiplication is repeated addition. It is thus both commutative and associative. Figure 1 gives a geometric perspective of multiplication.
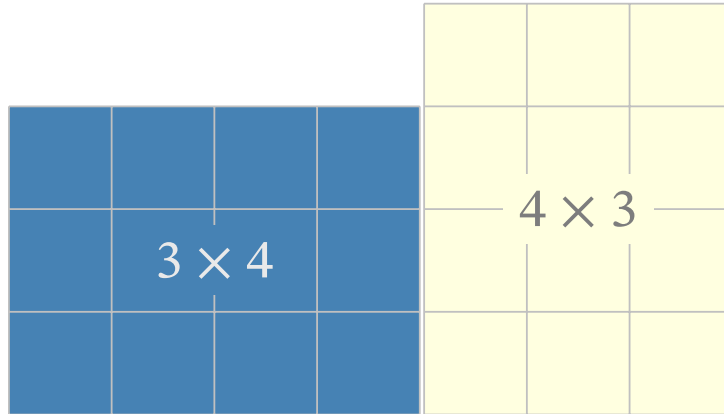

Figure 1: The products 4×3 and 3×4 amount to repeated additions and yield the same result of 12.

Talking about commutativity and associativity might seem like overkill for the addition and multiplication of real numbers. But, identifying these properties is a useful insight, as the more sophisticated mathematical objects we will encounter later may not obey either or both properties.

The additive and multiplicative identity elements in $\mathbb{R}$

When zero is added to any real number, a, we get the original number a back as the sum:

$$a + 0 = 0 + a = a. \tag{1}$$

We call 0 the *additive identity* for $\mathbb{R}$.

Likewise, when we multiply a by 1, the original number is returned as the product:

$$a \times 1 = 1 \times a = a \tag{2}$$

The number 1 is called the *multiplicative identity* in $\mathbb{R}$.

Zero and one enjoy their coign of vantage as the *unique* additive and multiplicative identities respectively for the real numbers in $\mathbb{R}$. But are their roles generalizable to cover a larger variety of mathematical objects?

Mathematics as a discipline tends to generalize and extend simple ideas to increasing levels of complexity, while at the same time maintaining consistency in definition and behaviour across these disparate domains. The additive and multiplicative identities may be so generalized, where applicable.

Varieties of additive and multiplicative identity elements

The zero of the complex numbers is $0 + i(0) = 0$ as well. And adding it to any complex number returns the original complex number.

Polynomials are expressions like $x^2 + 3x + 1$ where x is some real or complex variable. The zero polynomial is simply the constant polynomial $P(x) = 0$, and adding it to any polynomial again gives us back the original polynomial.

A matrix is a rectangular array of numbers, treated as a single unit mathematically. I facetiously call matrices *numbers in teabags*. Operations on matrices follow their own rules, but for addition, they are intuitively apparent.

Let us consider an arbitrary 2×2 *square matrix* like $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$. It has two horizontal rows and two vertical columns, and therefore 4 elements. The additive identity for this matrix is a 2×2 square matrix, all of whose entries are zero:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} \tag{3}$$

The matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the *multiplicative identity* for matrix multiplication for 2×2 matrices.[4] Note that its elements are solely ones and zeroes, with ones on the principal-diagonal from top left to bottom right.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} \tag{4}$$

This is a simple example of how the seed ideas of the additive and multiplicative identities, sown far and wide, germinate into shoots that are surprisingly similar to the original ones. The numbers 0 and 1 do indeed rule the roost for the simple reason that the original object remains unchanged under the respective operation. Obviously, the identity matrices will change with the matrix sizes, but the principles remain the same.

---

[4]The rules of matrix multiplication are a little involved and will not detain us here. The interested reader is referred to another blog of mine for details.

The additive inverse in $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$

The negative integers arose from subtractions like $(3 - 5)$, whose result was not a positive integer, and therefore lay outside the confines of $\mathbb{N}$. The negative numbers were introduced to rectify this deficit. The sets $\mathbb{Z}$, $\mathbb{Q}$, and and $\mathbb{R}$ all contain negative numbers, and can therefore lay claim to an additive inverse. Every integer or real number a has an *additive inverse*, a' such that:

$$a + a' = a' + a = 0.$$

Any guesses as to what a' is? It is the number a prefixed with a negative sign and written as $-a$, i.e., $a' = -a$. It is noteworthy, that when we subtract any real number from itself, we get zero, by the property of the additive inverse:

$$a - a = a + (-a) = 0 = (-a) + a. \tag{5}$$

If you have heard of matter and antimatter annihilating each other in real life or Science Fiction [2], you can metaphorically think of a and $-a$ as one such pair, giving rise not to energy, but to zero.☺

The multiplicative inverse in $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$

Suppose we ask the question, "If we have an arbitrary number a, what number should it be multiplied by to get 1?" Let us denote this number by a''. Then, we have:

$$a \times a'' = a'' \times a = 1 \tag{6}$$

If you know how to solve simple equations, you would suggest that we divide Equation (6) by a on *both sides*, like so:

$$
\begin{aligned}
a \times a'' &= 1; \text{ divide both sides by } a \\
a'' &= \frac{1}{a}.
\end{aligned}
\tag{7}
$$

The number $\frac{1}{a}$ is called the *reciprocal* of a and it is the multiplicative inverse of a. But there is one important restriction: $a \neq 0$. See Why is division by zero disallowed?

The rational numbers $\mathbb{Q}$ arose to accommodate the results of division. Note the hierarchy $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ where the symbol $\subset$ may be spoken as "is a subset of" or "is contained in".

The Arithmetic Four Revisited

Addition

If we start with 0 and add 1 to it, we get 1. If we add 1 to that we get 2. In this fashion, all the natural numbers may be generated successively by adding 1. The *next number* is called the *successor*. Even if we did not start with 0, but started with 1 instead, we can still generate the entire set $\mathbb{N}$ by adding 1 successively.

This method shows that there is no largest natural number. If there were such a number, say p, we could always add one to it and show the assumption to be false, since $(p + 1) > p$. In this sense, the number 1 helps us to understand countable infinity.

Subtraction

Subtracting zero from a number leaves it unchanged: $a - 0 = a$.

By convention, when a sign is not prefixed to a number, we assume it to be positive. If a negative sign is prefixed to a number, it is a negative number. This is indicated by a pair of parentheses—surrounding the number and its sign—in expressions. When the number is featured alone, these parentheses are dropped.

With signed numbers, from $\mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{R}$, we may convert any subtraction into an addition thus:

$$3 - 5 = -2 = 3 + (-5) = (-5) + 3. \tag{8}$$

And those additions would still be commutative. This does not mean that subtraction has suddenly become commutative; it has not. It simply means that subtraction can be morphed into the (commutative) addition of signed numbers.

Multiplication

Multiplying any number a by zero yields zero: $a \times 0 = 0 \times a = 0$. This might be a little difficult to grasp. To see why this is the case, let us be a little sneaky and write zero as $(p + (-p))$, for some $p \in \mathbb{R}$, because

$$(p + (-p)) = p - p = 0.$$

Then, we may write, for arbitrary $a \in \mathbb{R}$,

$$\begin{aligned}
a \times 0 &= a \times (p + (-p)) \\
&= a \times p + a \times (-p) \\
&= ap - ap \\
&= 0.
\end{aligned} \tag{9}$$

Here, I have applied the rule that the product of a positive and a negative number is negative. I have also silently invoked the distributivity of multiplication over addition.

Zero was a problematic number that had been introduced into Europe from India via the Arabs. Can you imagine the effort that must have gone into understanding and justifying that multiplication of any number by zero yielded zero? Zero, one, and infinity are a daunting triad. Mastering them takes time, practice, and familiarity, and stretches both human logic and imagination.

Multiplying a number by 1 is comparatively simpler: it leaves the original number unchanged. The number 1 is the *multiplicative identity* element for the real numbers. So, $5 \times 1 = 1 \times 5 = 5$.

Multiplying a by -1 yields the additive inverse of a, namely $-a$.

Division

If multiplication can be thought of as repeated addition, division can equally be thought of as repeated subtraction. Dividing 6 by 2 may be understood as "How many times can we subtract 2 from 6 before we hit zero?" Stated a little more mathematically, $6 \div 2 = 3$, and the steps are:

$$
\begin{array}{l|l}
6 - 2 = 4 & \text{First lot of two} \\
4 - 2 = 2 & \text{Second lot of two} \\
2 - 2 = 0 & \text{Third lot of two}
\end{array}
$$

The result or *quotient* is 3 because our subtraction algorithm terminated in 3 steps with a remainder of 0. Because division is the inverse of multiplication, we can also understand the result as the number by which we must multiply the *divisor* 2 to obtain the *dividend* 6. In this case, the *remainder* is zero, to better illustrate what is happening.

If the division gives rise to a remainder, we stop when we get a remainder that is less than the divisor. For example, with $7 \div 2$, we get:

$$
\begin{array}{l|l}
7 - 2 = 5 & \text{First lot of two} \\
5 - 2 = 3 & \text{Second lot of two} \\
3 - 2 = 1 & \text{Third lot of two}
\end{array}
$$

That last number 1 is the remainder and the number of steps before stopping is still the quotient, which is again 3.

Just as subtraction may be thought of as the addition of signed numbers, so also may division be thought of as the multiplication by reciprocals. If some real a is divided by another real $b \neq 0$, we may write this as $a \div b$ or equivalently, we may also express it as $a \times \frac{1}{b} = \frac{1}{b} \times a = \frac{a}{b}$.

Why is division by zero disallowed?

Now, what happens if we divide by zero? To keep matters simple, let us keep the same dividend, namely 6. If we subtract 0 from 6, we end up with 6. Subtracting another 0 from this 6 still leaves us with 6. By now, you should have cottoned on to the fact that we are not making any progress.

$$
\begin{array}{l|l}
6 - 0 = 6 & \text{First lot of zero} \\
6 - 0 = 6 & \text{Second lot of zero} \\
6 - 0 = 6 & \text{Third lot of zero} \\
\cdots & \cdots
\end{array}
$$

Each time we subtract zero, the remainder equals the dividend, and we end up where we started. Thus, this process never ends, and therefore cannot be an algorithm, which by definition, must terminate in a *finite* number of steps. Sometimes, this is stated as "dividing by zero gives infinity," which is a mathematically less acceptable, but intuitively more friendly, way of stating that it is an unending process. This is why division by zero is not permitted.

The most basic justification for not permitting division by zero is given here. With increasing mathematical sophistication, increasingly recondite reasoning may be given for why division by zero is not permitted. For example, *any number* multiplied by zero gives zero. Therefore, dividing by zero will give us *any number*, which is a non-unique answer. Allowing such an operation will destroy the predictability on which mathematical operations are built.

Exponentiation

Exponentiation may also be called *raising (something) to a power*. It is a short form for repeated multiplication by the *same* number. For example, if we multiply 5 by itself three times, we write it so:

$$5 \times 5 \times 5 = 5^1 \times 5^1 \times 5^1 = 5^{(1+1+1)} = 5^3 = 125 \tag{10}$$

The number 5 is called the *base* and the power 3 is called the *exponent*. Note that $5^1 = 5$ and the exponent 1 is omitted.

The reciprocal of an arbitrary non-zero real number a is $\frac{1}{a}$. The product of the two is 1. So, a and $\frac{1}{a}$ are multiplicative inverses. Written with an exponent,

$$\frac{1}{a} = a^{-1}.$$

Continuing with the number 5 in our example, its reciprocal is $\frac{1}{5} = 5^{-1}$. What do we get if we multiply 5 by its reciprocal? We already know the answer to be 1. Let us do the multiplication using exponents:

$$5 \times \frac{1}{5} = 1 = 5^1 \times 5^{-1} = 5^{1+(-1)} = 5^0. \tag{11}$$

The astounding conclusion from Equation (11) is that 5 raised to the exponent zero is 1. I will hand-wave here and assert that this will apply to any base $a \in \mathbb{R}$, i.e., $a^0 = 1$ for $a \in \mathbb{R}$: something that will be understood better after we encounter logarithms in this series of blogs or elsewhere. The consequence is that the logarithm of 1 to any base b is 0:

$$\log_b 1 = 0. \tag{12}$$

Equation (12) is yet another memorable equation linking 1 and 0. When the domain of mathematics expands to take on new numbers, new objects, and new notations, the need for consistency with the existing body of mathematics gives us pearls such as Equation (12).

From the foregoing, note that

$$a \times \frac{1}{a} = a \times a^{-1} = a^0 = 1.$$

Constants in polynomials may be written using x^0 in place of one. For example,

$$2x^2 + 3x + 2 = 2x^2 + 3x^1 + 2x^0. \tag{13}$$

Equation (13) shows how consistent the terms in a polynomial are. They are all powers of x written in descending fashion, although by convention, certain terms are understood and therefore implicit. The omission of the index in the term $3x^1$ and the x^0 in the term $2x^0$ could cause disquiet in the newcomer to polynomials. It is best to dispel that unease right away, by understanding that it is a mere convention that has led to this departure from absolute consistency.

In the succeeding sections, we take a look a some lesser known aspects of zero and one.

The shy one

The number one is often implicit in mathematical notation. While we may write $2x$ to denote $2 \times x$, or two multiplied by x, we *do not* write $1x$, even if it is literally correct, because of convention. In instances like this, the number one is implicit, and assumed to be understood by those who know. If you happen to be one of those *not* in the know, here's your chance to join the other side.

When we write a fraction as $\frac{3}{4}$ we mean the decimal 0.75 and matters are clear. But all whole numbers are also fractions with the denominator being 1. So, the fraction $\frac{3}{1}$ is rarely written in that form, even if syntactically correct, because usage dictates that whole numbers are written to stand on their own, as 3, in this case. Again, the 1 in the denominator is assumed to be unobtrusively present: out of sight but *not* out of mind.

One consequence of this is that $\mathbb{Z} \subset \mathbb{Q}$ which, in plain English, reads as "the set of integers is a (proper) subset of the set of rationals".

When we write 4^2, spoken out as "four squared" we mean the number obtained by multiplying 4 by itself. This nomenclature arose because, if 4 was associated with the *length* of, say, a piece of string, the number "four squared" was used to denote the *area* of a square that had a side of length 4. So, $4^2 = 4 \times 4 = 16$.

Likewise, the expression 7^3 or "seven cubed" denoted the volume of a cube of side 7. Beyond the third dimension, this naming scheme faded out, because we cannot percieve dimensions higher than three.

Therefore, 6^4 is spoken as "six raised to the fourth (power)" or "six to the four". As we have seen before, in such statements, the number 6 is called the base and the number 4 is called the exponent.

We have already seen that $5^1 = 5$ and, while that is perfectly correct, convention intrudes to say that we write it simply as 5. *Any number raised to the power of* 1 *equals itself.*

The notation making 1 implicit in these scenarios reduces clutter and simplifies notation. The absence of the implicit 1 might trouble the heart of the sincere young mathematician, but familiarity with these conventions will make for comfort and confidence in using them.

The interval $[0, 1]$

If the reals are thought of as a line, the segment from 0 to 1 can serve as a microcosm of all the real numbers. It is as densely populated with rational and irrational numbers as the entire real number line. This almost holographic property is a consequence of what "infinity" is, and is again a concept that might be difficult to accept, let alone understand.

In any case, our interest in the closed interval $[0, 1]$ is for a different purpose now. The numbers in $\mathbb{Q}$ and $\mathbb{R}$ have an interesting property when they lie in the interval $[0, 1]$. If we raise such numbers to integer powers, they become progressively smaller in value. This may easily be seen using the rules of exponentiation, or by successive multiplication.

Let $a = 0.9$. Then the successive integral powers of a are as tabulated below:

a	0.9^1	0.9
a^2	0.9^2	0.81
a^3	0.9^3	0.729
a^4	0.9^4	0.6561
a^5	0.9^5	0.59049

It is clear that the powers of a^n diminish with increasing n when $a \in [0, 1]$. This is peculiar to the interval $[0, 1]$, because when $a > 1$, the powers of a^n increase with increasing n, as tabulated below for $a = 1.1$.

a	1.1^1	1.1
a^2	1.1^2	1.21
a^3	1.1^3	1.331
a^4	1.1^4	1.4641
a^5	1.1^5	1.61051

The pivot at $a = 1$ is rock steady because $1^n = 1$ for all $n \in \mathbb{N}$. When a is 10% less, we see a steady decline in a^n as n increases. But when a is 10% more than 1, we see a growth in a^n and n increases. This wondrous behaviour contributes to the magic of the number 1.

Figure 2 shows graphs of x^n for $x \in [0, 1]$ and $n \in \{0, 1, 2, 4, 8, 16, 32, 64, 128, 512\}$. As n increases and x approaches 1, the graphs exhibit an almost perpendicular change in direction like a laterally inverted L. I find this behavior fascinating, and it explains why geometric series converge when the common ratio $|r| < 1$.

Rotation on the complex plane

The two-dimensional plane may be pressed into service in a variety of contexts to serve different ends. One such use is the Argand diagram in which the x axis represents the real part and the y axis the imaginary part of a complex number, $z = x + iy$; $x, y \in \mathbb{R}$; $z \in \mathbb{C}$.

Consider the point P in Figure 3 with coordinates $(1, 0)$ which denotes the real number 1 in $\mathbb{C}$. P has no imaginary component. If we multiply it by i, we get to Q, $(0, 1)$, which is purely imaginary and has no real component. Another multiplication by i sends Q to R, which is $(-1, 0)$, a purely real number. A third multiplication transforms R into S at $(0, -1)$ which is purely imaginary. A fourth and final multiplication maps S back to P.

The upshot of this is that each multiplication by i rotates the point P counterclockwise by $\frac{\pi}{2}$ or 90°. Four consecutive multiplications restore the rotated point to itself. The multiplicative identity element is therefore

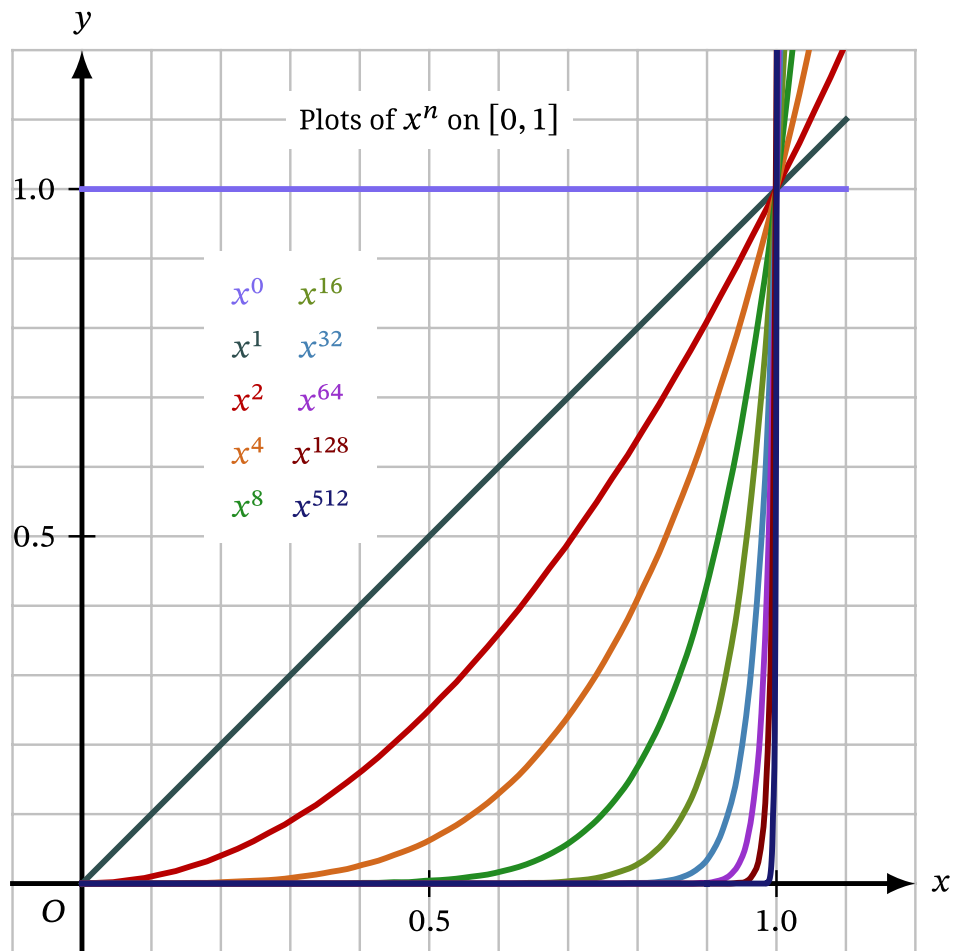$$i^4 = (i^2)(i^2) = (-1)(-1) = 1$$

Figure 2: Graphs of $y = x^n$ for $x \in [0, 1]$ and $n \in \{0, 1, 2, 4, 8, 16, 32, 64, 128, 512\}$. Note that all curves pass through $(1, 1)$.

$$
\begin{aligned}
i^1 &= i \\
i^2 &= -1 \\
i^3 &= -i \\
i^4 &= 1
\end{aligned}
$$

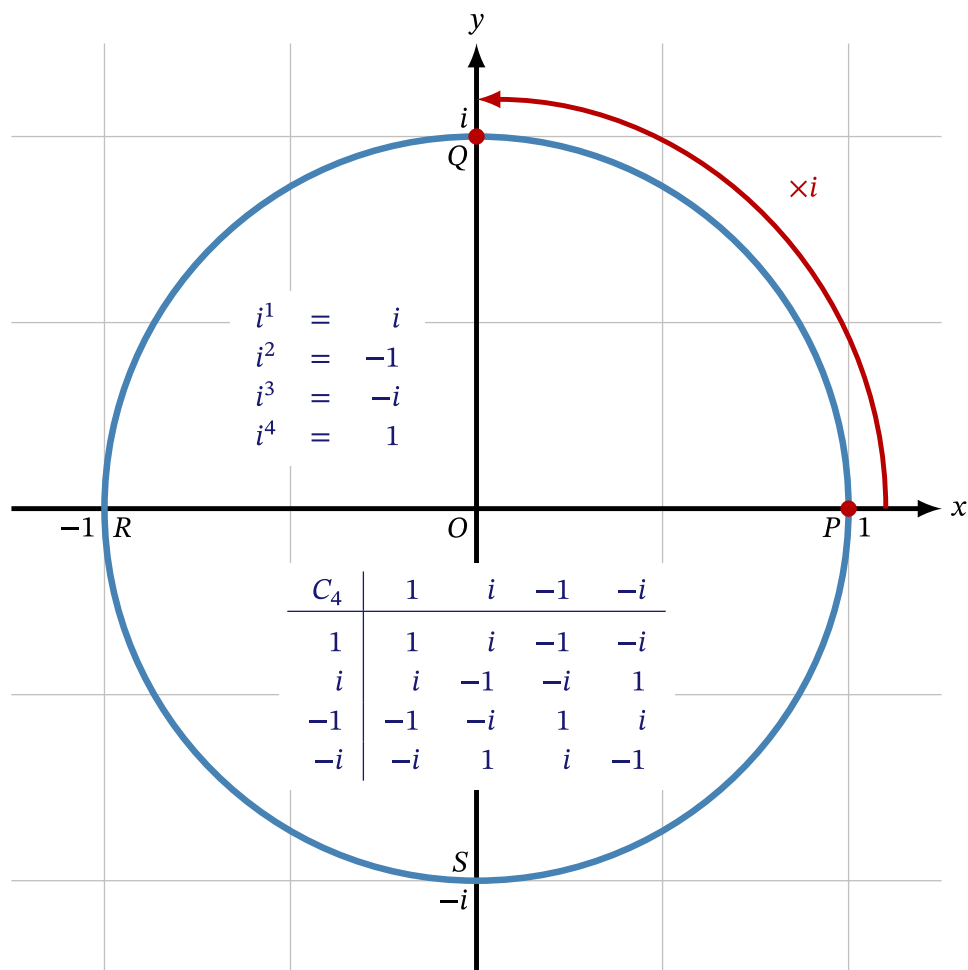| C_4	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Figure 3: Successive multiplication by i as a rotation in $\mathbb{C}$. See the text for the full explanation.

as would be expected. The multiplicative inverses for the four elements $1, i, -1, -i$ are $1, -i, -1, i$ respectively. Observe that:

1. A multiplication by i corresponds to a $\frac{\pi}{2}$ counterclockwise rotation in $\mathbb{C}$.
2. Four consecutive rotations restore the point to its original position.
3. The multiplicative identity element is $i^4 = 1$ as would be expected.
4. The multiplicative inverse for each of the four elements is also one of the four numbers $1, i, -1, -i$.
5. The starting point and the results of all rotations are points on the unit circle.

These properties are at the heart of Group Theory which is the mathematical study of symmetries. The particular group we are looking at is called the C_4 group because of its fourfold symmetry.

It is customary to enumerate the transformations in a group by displaying them in a table, called a Cayley table, not unlike a multiplication table. Such a table for the C_4 group is shown in Figure 3 as well as below:

C_4	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Some groups may not be commutative with respect to multiplication. So, the order of multiplication is "the row element multiplied by the column element". The group C_4 is a commutative or Abelian group under multiplication, so the order of multiplication may be swapped. Moreover, because all its elements may be generated from a single element, e.g., i, as shown in the second quadrant of Figure 3, it is also called a cyclic group.

The four numbers $1, i, -1, -i$ are also known as the fourth roots of unity [3]. These numbers satisfy the polynomial equation

$$z^4 = 1. \tag{14}$$

Indeed, the study of groups was motivated by mathematical questions arising from the study of polynomials, the study of integers using modular arithmetic and the study of geometric symmetries. Group theory has enabled mathematicians to distil similarities from disparate domains and thereby produce an integrated picture of their discipline. Watch this video on cyclic groups to learn more about them.

Sequences and Series

An ordered procession of numbers is called a sequence [4,5].[5] Repetitions are allowed, but the order matters. The natural numbers form the sequence $(1, 2, 3, 4, 5, \ldots)$. Note that the elements of the sequence are enclosed in parentheses, (). There is an entire website devoted to sequences, called the The On-Line Encyclopedia of Integer Sequences® (OEIS®).

---

[5] The general definition replaces *numbers* with *mathematical objects* but the former will suffice for our limited purpose here.

Fibonacci sequence

The Fibonacci sequence is a simple but profound sequence that is reflected in much of Nature. We start at the beginning with 0 and 1:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, \dots$$

We add them to get the next number, which is 1 again. Adding that to the previous number, we obtain 2. The algorithm is to add the two previous numbers to get the current one:

$$\begin{aligned}
F_1 &= 0 \\
F_2 &= 1 \\
F_3 &= F_2 + F_1 = 1 \\
F_4 &= F_3 + F_2 = 1 + 1 = 2 \\
F_n &= F_{n-1} + F_{n-2} \text{ for } n \in \mathbb{N} \text{ and } n > 2
\end{aligned} \tag{15}$$

We have a *recurrence relation* in Equation (15) for the nth Fibonacci term.[6] And the grist for the Fibonacci sequence mill are the two numbers, 0 and 1!

Pascal's triangle is another sequence that may be built from adjacent sums in a number pattern. It is related to the binomial coefficients which play a vital role in probability, combinatorics, and calculus. I intend to look at number patterns like the Fibonacci sequence and Pascal's triangle in another blog.

Series

A series is the (progressive) sum of an infinite sequence [6,7].

The sum of *all* the natural numbers, starting with 1 and going on without end, is written as

$$\sum_{n=1}^{\infty} n = 1 + 2 + 3 + 4 + \dots$$

It is tacitly understood that the numbers are integers from $\mathbb{N}$. The sum is unbounded or infinite. However, certain infinite sums converge to a specific number or *limit,* as our next example demonstrates.

Consider, for example the sequence that we encounter in Zeno's Dichotomy paradox: $1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \dots$. Is there a sum to infinity, and if so, what is it? The series we are after is called a *geometric series* or a *geometric progression* and the sum to infinity may be written as:

$$\sum_{n=0}^{\infty} \frac{1}{2^n} = 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \dots \tag{16}$$

---

[6]The nth Fibonacci term may be expressed in closed form without recursion using Binet's Formula but we will not go into that here

Mark that the first term is $\frac{1}{2^0} = \frac{1}{1} = 1$. Because the successive terms in this series get smaller and smaller, there is hope that it could converge to a finite limit. Using the standard notation for geometric series, we have the first term $a = 1$. The common ratio r is the ratio of the succeeding term divided by the current term. Looking at the first two terms, we have $r = \frac{\frac{1}{2}}{1} = \frac{1}{2}$.

If the absolute value of the common ratio r is less than 1, i.e.,

$$|r| < 1 \tag{17}$$

then the infinite series will converge to a finite limit. If you need to be convinced about the condition in Equation (17), take a look at Figure 2 and you will hopefully be persuaded! Again, note the vital place enjoyed by 0 and 1 in the game called mathematics.☺

So, what is the sum to infinity? The time-honoured formula is $\frac{a}{1-r}$, which in our case, works out to:

$$\sum_0^\infty \frac{1}{2^n} = \frac{1}{1 - \frac{1}{2}}$$
$$= \frac{1}{\frac{1}{2}}$$
$$= 2.$$

The problem with the paradoxes of old was that they did not allow for the fact that *infinite sums could sometimes be finite.* And that is a problem that mathematicians have been grappling with ever since the calculus was invented. But that again, is a blog for another day and another occasion.

For now, I hope that the uniqueness, utility, and ubiquity of 0 and 1 have convinced you of their indispensability in the domain of Mathematics.

Feedback

Please email me your comments and corrections.

A PDF version of this article is available for download here:

https://swanlotus.netlify.app/blogs/the-two-most-important-numbers.pdf

References

[1]   Arpita Bhattacharya. 2023. Cutting Through the Confusion: How Dedekind Cuts Build the Real Numbers. Retrieved 7 November 2023 from https://arpita95b.medium.com/cutting-through-the-confusion-how-dedekind-cuts-build-the-real-numbers-20aeaaec021d

[2]   William S Higgins. 2008. Antimatter's science fiction debut. Retrieved 5 November 2023 from https://www.symmetrymagazine.org/article/september-2008/antimatters-science-fiction-debut?language_content_entity=und

[3]   Patrick Honner. 2021. The Simple Math Behind the Mighty Roots of Unity. *Quanta Magazine* (September 2021). Retrieved 7 November 2023 from https://www.quantamagazine.org/the-simple-math-behind-the-mighty-roots-of-unity-20210923/#

[4]   Wikipedia contributors. 2023. Sequence—Wikipedia, The Free Encyclopedia. Retrieved 3 November 2023 from https://en.wikipedia.org/w/index.php?title=Sequence&oldid=1177801065

[5]   Eric W Weisstein. Sequence. From MathWorld—A Wolfram Web Resource. Retrieved 3 November 2023 from https://mathworld.wolfram.com/Sequence.html

[6]   Wikipedia contributors. 2023. Series (mathematics)—Wikipedia, The Free Encyclopedia. Retrieved 3 November 2023 from https://en.wikipedia.org/w/index.php?title=Series_(mathematics)&oldid=1174621451

[7]   Eric W. Weisstein. Series. From MathWorld—A Wolfram Web Resource. Retrieved 3 November 2023 from https://mathworld.wolfram.com/Series.html