The Theory of Numbers, from Ancient Greece to the 21st Century

Matthew Emerton

University of Chicago

July 19, 2024

“There is an underlying timelessness in the basic conversation that is mathematics” — Barry Mazur (1938 –)

What are numbers?

Numbers (as we all know from experience) have many uses. For example:

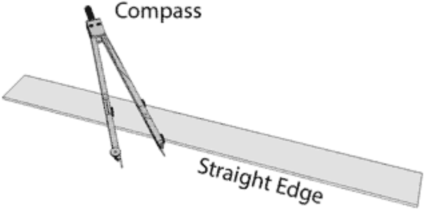
- As labels
- More powerfully, for counting
- But also, for measuring

By constructing a length first, and measuring it afterwards, we can sometimes discover numbers we didn't previously know.

Ruler and compass construction

A technique introduced in ancient Greek geometry.

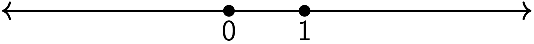
- A ruler is a long, unmarked straight edge (alternatively called a “straight edge”, for this reason).
- A compass lets you draw circles.



Ruler and compass construction

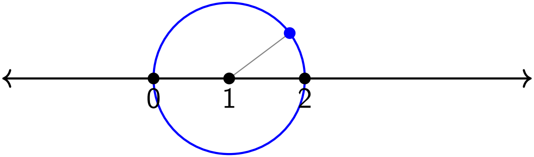
We start with two points one unit apart (labelled as ‘0’ and ‘1’):

and then use our ruler to draw a line passing through them:



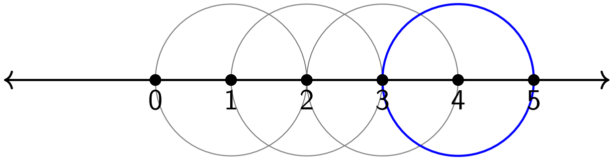
Ruler and compass construction

Now we can use our compass to draw a circle of radius 1, centered at 1. It intersects our line at 0 and another point, labelled 2:



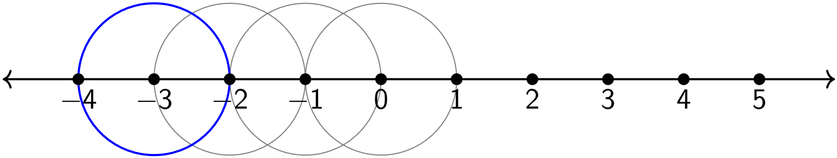
Constructing whole number lengths

If we continue, drawing a circle of radius 1 centered at 2 (letting us construct 3), then at 3, and so on, we produce more points on the line.



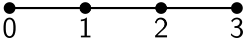
Constructing whole number lengths

We can similarly construct points to the left of 0, labelled with negative signs:



Numbers and harmony

The ancient Greeks liked the fact that whole numbers are in proportion to each other. E.g. consider just this portion of our line:

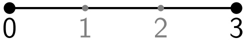


The distance between 0 and 1 is

- $1/2$ of the distance between 0 and 2;
- $1/3$ of the distance between 0 and 3.

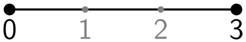
Numbers and harmony

Our line segment visualized as a string with frets:



We can play three notes, by fretting at either 1, 2, or 3, and then plucking the string.

Numbers and harmony



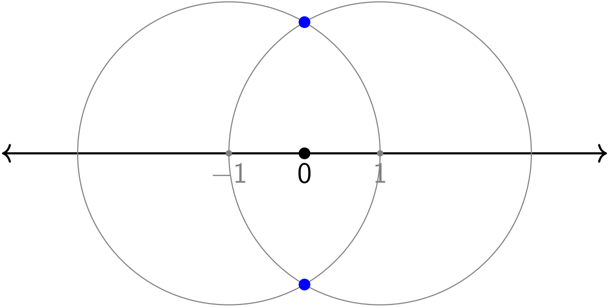
We produce three notes:

- The A above middle C (say);
- The A below middle C;
- The D below that.

The first two notes are the same (just differing by an octave). The second and third are in harmony (a perfect fifth).

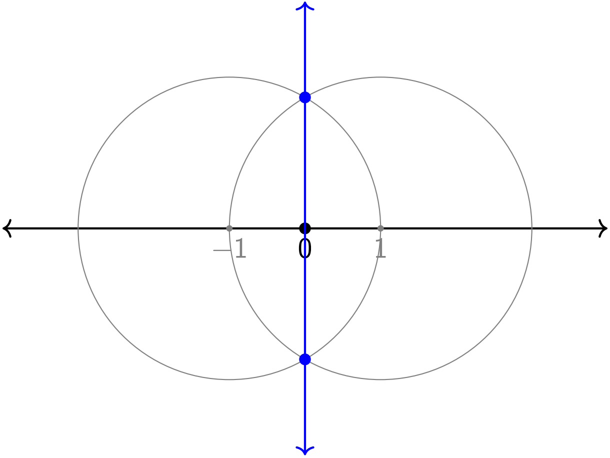
More constructions

Returning to our ruler and compass, we can also construct points not on the line, by drawing circles and looking at the points where they intersect.



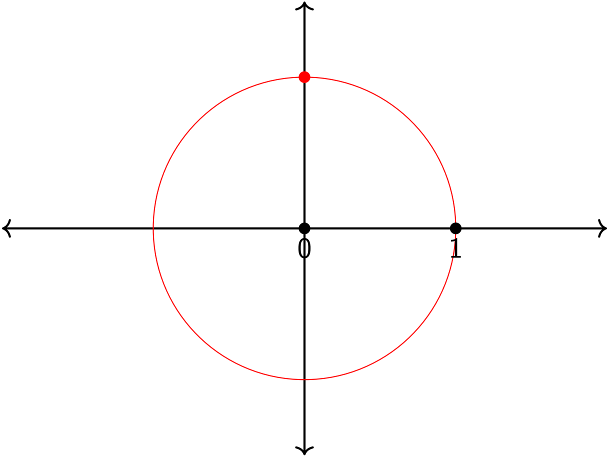
More constructions

Using our straightedge to draw the line through these points, we obtain a new line at right angles to our original line.



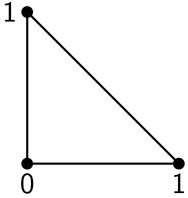
More constructions

Now we can draw a radius 1 circle centred at 0, and mark the point where it intersects the vertical line.



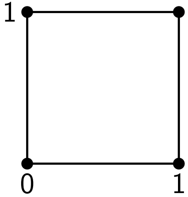
More constructions

Drawing one more line (the hypotenuse), we have constructed a triangle with horizontal and vertical sides of length 1:



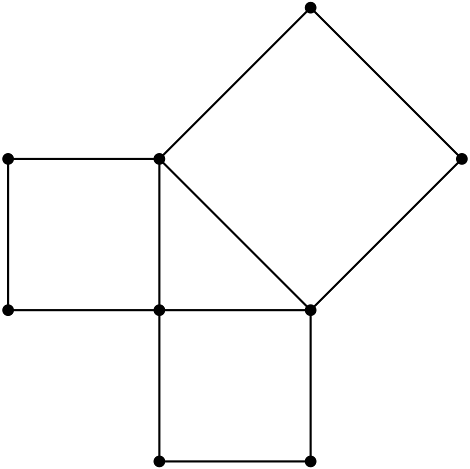
More constructions

Drawing a few more circles and lines, we can also construct a square with side lengths 1:

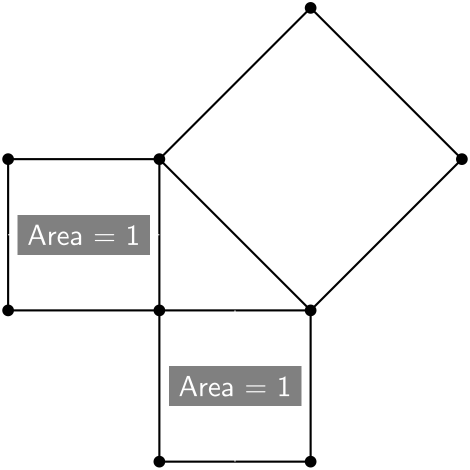


More constructions

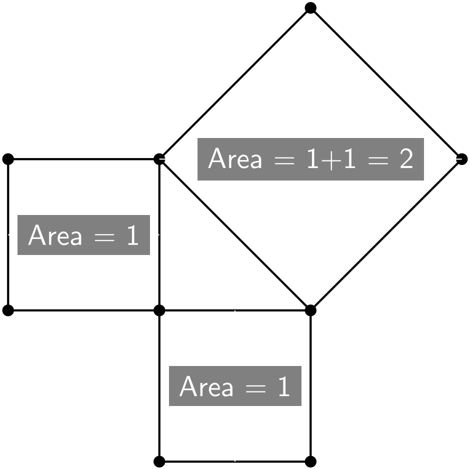
It is more interesting to construct a square like this on each side of our triangle:



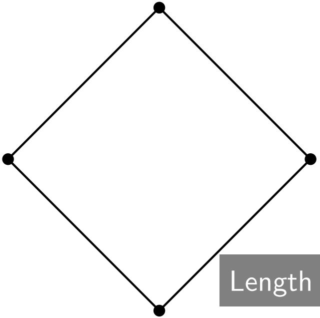
Pythagoras



Pythagoras

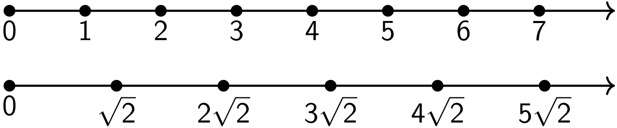


Pythagoras



Length $= \sqrt{2}$

Irrationality of $\sqrt{2}$



Once they move past 0, the two sequences of points never overlap!

Irrationality of $\sqrt{2}$

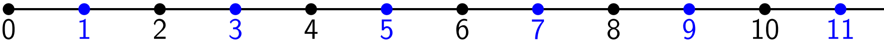
The note played by a string of length $\sqrt{2}$ does not harmonize with a note played by a string of length 1.

(The tritone, or, the Devil in music!)

Even and odd numbers

A whole number is *even* if it is a multiple of 2, and *odd* otherwise.

Any odd number is always 1 more than a multiple of 2.



Multiplication rules:

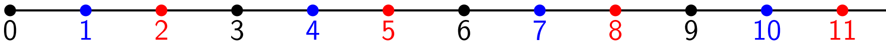
$$\text{even } x \text{ anything} \;=\; \text{anything} \times \text{even} \;=\; \text{even}$$

$$\text{odd } x \text{ odd} \;=\; \text{odd}$$

Congruence modulo 3

Any whole number is either:

- A multiple of 3 (black dots)
- 1 more than a multiple of 3 (blue dots)
- 1 less than a multiple of 3 (red dots)



We say that a number is:

- Congruent to 0 modulo 3 (or 0 mod 3)
- Congruent to 1 modulo 3 (or 1 mod 3)
- Congruent to -1 modulo 3 (or -1 mod 3)

according to which of these cases is it in.

Congruence modulo 3

Multiplication follows the usual rules for multiplying 0 and ± 1:

- $(0 \bmod 3) \times \text{anything} = \text{anything} \times (0 \bmod 3) = 0 \bmod 3$
- $(1 \bmod 3) \times (1 \bmod 3) = 1 \bmod 3$
- $(1 \bmod 3) \times (-1 \bmod 3) = (-1 \bmod 3) \times (1 \bmod 3) = -1 \bmod 3$
- $(-1 \bmod 3) \times (-1 \bmod 3) = 1 \bmod 3$

Congruence modulo 3

- $(0 \bmod 3) \times \text{anything} = \text{anything} \times (0 \bmod 3) = 0 \bmod 3$

  (Any multiple of a multiple of 3 is again a multiple of 3)

- $(1 \bmod 3) \times (1 \bmod 3) = 1 \bmod 3$

  (E.g. $4 = 3 + 1$, $7 = 6 + 1$, and $4 \times 7 = 28 = 27 + 1$)

- $(1 \bmod 3) \times (-1 \bmod 3) = (-1 \bmod 3) \times (1 \bmod 3) = -1 \bmod 3$

  (E.g. $4 = 3 + 1$, $2 = 3 - 1$, and $4 \times 2 = 8 = 9 - 1$)

- $(-1 \bmod 3) \times (-1 \bmod 3) = 1 \bmod 3$

  (E.g. $2 = 3 - 1$, $5 = 6 - 1$, and $2 \times 5 = 10 = 9 + 1$)

Congruence modulo 3

In particular, any *square* is either:

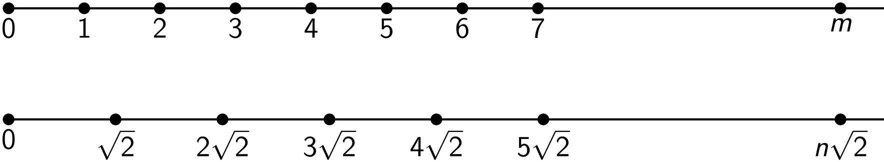
- 0 mod 3

  or

- 1 mod 3

Proof of irrationality of $\sqrt{2}$

Suppose that two points in the two sequences coincide:



So $m = n\sqrt{2}$, for some whole numbers m and n. We'll show this is impossible!

Proof of irrationality of $\sqrt{2}$

$$m = n\sqrt{2} \quad \overset{\text{square both sides}}{\Longrightarrow} \quad m^2 = n^2 \times 2$$

Look at the right hand equation modulo 3:

$$(0 \text{ or } 1 \bmod 3) = (0 \text{ or } -1 \bmod 3)$$

The only consistent possibility is both sides are 0 mod 3.

Proof of irrationality of $\sqrt{2}$

We've shown $m = n\sqrt{2}$ implies $m = 3p$, $n = 3q$.

$$3p = 3q\sqrt{2} \quad \overset{\text{cancel 3 from both sides}}{\Longrightarrow} \quad p = q\sqrt{2}.$$

Same reasoning implies $p = 3s$, $q = 3t$, and that $s = t\sqrt{2}$.

Continuing on like this, we find that our original numbers m and n are both infinitely divisible by 3, an obvious impossibility.

We conclude that it's impossible to have $m = n\sqrt{2}$.

Proof of irrationality of $\sqrt{2}$

We could have used other primes besides 3.

For example:

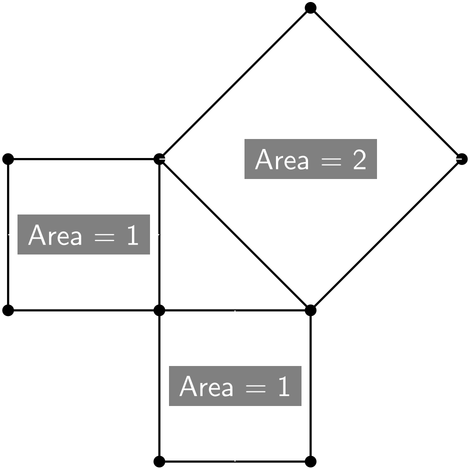
- Integers are congruent to $-2, -1, 0, 1$, or 2 modulo 5.
- Integer squares are congruent to $-1, 0$, or 1 modulo 5.
- So 2 is not a square modulo 5.

Proof of irrationality of $\sqrt{2}$

But not *every* prime would work. E.g.:

- Integers are congruent to $-3, -2, -1, 0, 1, 2$, or 3 modulo 7.
- Integer squares are congruent to $-3, 0, 1$, or 2 modulo 7.
- E.g. $3^2 \bmod 7 = 9 \bmod 7 = 2 \bmod 7$.

Doubling the square



Given a square of some area, we have found a way to construct (with ruler and compass) a square of twice its area.

Doubling the cube

The Delian problem: construct (using ruler and compass) a cube with twice the volume of a given one.

- To double a square, we constructed a segment of length $\sqrt{2}$ (starting from a segment of length 1).
- To double a cube, we must construct a segment of length $\sqrt[3]{2}$.

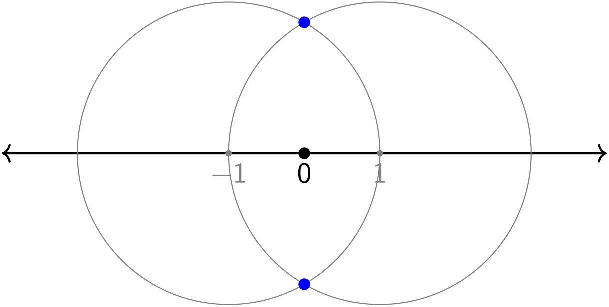
Doubling the cube

It turns out that this is *impossible*!

This impossibility is explained by symmetry.

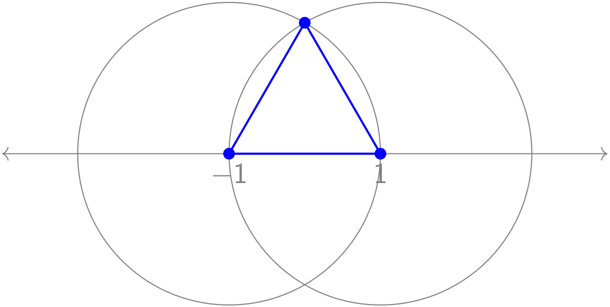
Symmetries in geometry

Earlier, we constructed this figure, involving two circles each of radius 2:



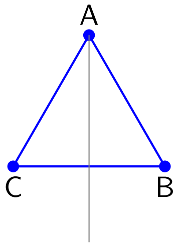
Symmetries in geometry

Drawing the indicated lines yields an equilateral triangle:



Symmetries in geometry

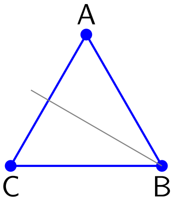
We can reflect through this vertical line of symmetry:



$$A \mapsto A$$
$$B \mapsto C$$
$$C \mapsto B$$

Symmetries in geometry

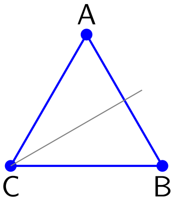
. . . and through this line of symmetry:



$$A \mapsto C$$
$$B \mapsto B$$
$$C \mapsto A$$

Symmetries in geometry

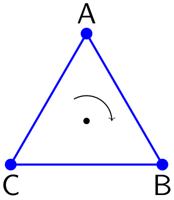
. . . and through this line of symmetry:



$$A \mapsto B$$
$$B \mapsto A$$
$$C \mapsto C$$

Symmetries in geometry

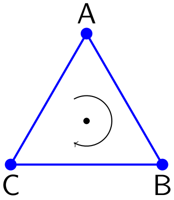
We can also rotate clockwise 120°:



$$A \mapsto B$$
$$B \mapsto C$$
$$C \mapsto A$$

Symmetries in geometry

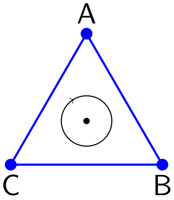
. . . or 240°:



$$A \mapsto C$$
$$B \mapsto A$$
$$C \mapsto B$$

Symmetries in geometry

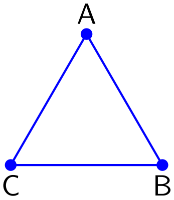
If we rotate all the way around 360°, then nothing changes. We call this the *identity* symmetry:



$$A \mapsto A$$
$$B \mapsto B$$
$$C \mapsto C$$

Symmetries in geometry

Altogether we have 6 symmetries of the triangle:



Identity (All of A, B, and C fixed),

$B \longleftrightarrow C$ (A is fixed),

$A \longleftrightarrow C$ (B is fixed),

$A \longleftrightarrow B$ (C is fixed),

$$\begin{tikzcd} A \arrow[r] & B \arrow[r] & C \arrow[ll, bend left] \end{tikzcd},$$

$$\begin{tikzcd} A \arrow[r] & C \arrow[r] & B \arrow[ll, bend left] \end{tikzcd}$$

Symmetries in geometry

$$\text{Identity (All of } A\text{, } B\text{, and } C \text{ fixed)},$$

$$B \longleftrightarrow C \ (A \text{ is fixed}),$$

$$A \longleftrightarrow C \ (B \text{ is fixed}),$$

$$A \longleftrightarrow B \ (C \text{ is fixed}),$$

$$\begin{tikzcd} A \arrow[r] & B \arrow[r] & C \arrow[ll, bend left] \end{tikzcd},$$

$$\begin{tikzcd} A \arrow[r] & C \arrow[r] & B \arrow[ll, bend left] \end{tikzcd}$$

These are just all the ways of permuting the 6 vertices A, B, and C.

We call this the *group* of symmetries of the equilateral triangle. It has *order* 6 (i.e. 6 members).

Symmetries in algebra

There are symmetries in other parts of mathematics too (though often less obvious than symmetries in geometry).

The theory of symmetries in algebra is due to *Évariste Galois* (1811 – 1832).

He showed that solutions to equations have symmetries, just like geometric figures do.

Symmetries in algebra

The quadratic formula says that the solutions to

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

are given by

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

The "±" means that there are two solutions, that are interchanged by changing the sign from $+$ to $-$ and vice versa.

Symmetries in algebra

The solutions to a quadratic have a symmetry group of order two.
(The identity, and the sign change that swaps them.)

If we describe ruler and compass constructions in terms of analytic geometry on the x-y plane, the new points we construct are obtained by solving simultaneous equations.

(Lines have equations like $y = mx + b$.)

(Circles have equations like $(x - a)^2 + (y - b)^2 = r^2$.)

The solutions of these equations have symmetry groups.

Symmetries in algebra

The equations we get are iterated quadratic equations. So the symmetry groups are built up out symmetry groups of quadratic equations, each of which has order 2.

So the symmetry groups all have order equal to a power of 2.

Symmetries in algebra

As an example, consider the number $\sqrt{5+2\sqrt{5}}$.

It is a solution to $x^2 = 5 + 2\sqrt{5}$.

$5 + 2\sqrt{5}$ is a solution to $x^2 - 10x + 5 = 0$.

So $\sqrt{5+2\sqrt{5}}$ is a solution to $x^4 - 10x^2 + 5 = 0$.

Symmetries in algebra

What are the symmetries of the solutions to $x^4 - 10x^2 + 5 = 0$?

What effect do they have on $\sqrt{5 + 2\sqrt{5}}$?

Symmetries in algebra

One symmetry (I'll call it S) is given by a sign change in the outer square root:

$$\sqrt{5+2\sqrt{5}} \xrightarrow{S} -\sqrt{5+2\sqrt{5}}$$

Symmetries in algebra

But there is also a symmetry (I'll call it T) that changes the sign of $\sqrt{5}$ (the inner square root). Then:

$$\sqrt{5+2\sqrt{5}} \xrightarrow{T} \sqrt{5-2\sqrt{5}}$$

Symmetries in algebra

Some sidework:

$$\begin{aligned}(5+2\sqrt{5})(5-2\sqrt{5}) &= 25-20 \quad \text{(Difference of perfect squares)}\\ &= 5\end{aligned}$$

So:

$$5-2\sqrt{5} = \frac{5}{5+2\sqrt{5}}$$

Taking square roots:

$$\sqrt{5-2\sqrt{5}} = \sqrt{\frac{5}{5+2\sqrt{5}}} = \frac{\sqrt{5}}{\sqrt{5+2\sqrt{5}}}$$

Symmetries in algebra

$$\begin{aligned}\sqrt{5+2\sqrt{5}} \xrightarrow{T} \sqrt{5-2\sqrt{5}} &= \frac{\sqrt{5}}{\sqrt{5+2\sqrt{5}}} \\ &\xrightarrow{T} \frac{-\sqrt{5}}{\frac{\sqrt{5}}{\sqrt{5+2\sqrt{5}}}} = -\sqrt{5+2\sqrt{5}}\end{aligned}$$

So the symmetry T^2 (applying T twice) gives the same result as S (the sign change on the outer square root).

Symmetries in algebra

So the symmetry group in this case equals

$$\{\text{Identity}, T, S = T^2, T^3\}$$

It has order 4 (a power of 2).

Cube roots of 2

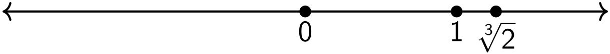
$\sqrt[3]{2}$ is a solution to $x^3 = 2$, or $x^3 - 2 = 0$.

This is a *cubic* equation. It has 3 solutions!

There is the usual cube root of 2, and also two complex number cube roots of 2.

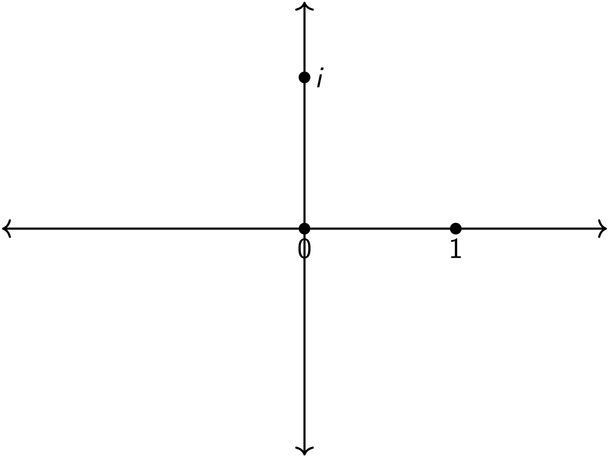
Cube roots of 2

Usual (real) numbers are represented as all the points on a line:



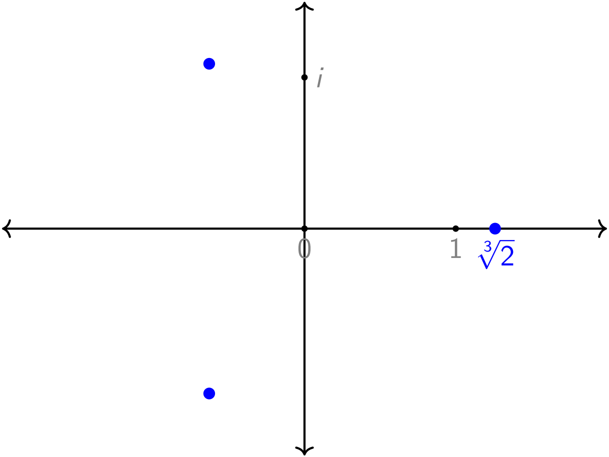
Cube roots of 2

Complex numbers are represented as the points on a plane:



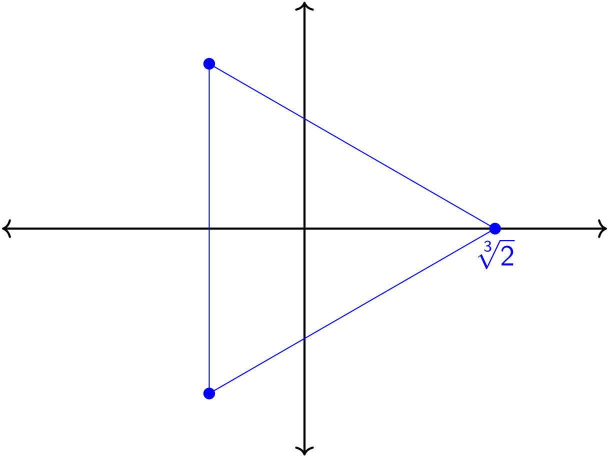
Cube roots of 2

The three complex number cube roots of 2:



Cube roots of 2

The complex cube roots of 2 are vertices of an equilateral triangle:



Cube roots of 2

The symmetries of the solutions to $x^3 - 2 = 0$ are the same as the symmetries of the equilateral triangle: they permute the three solutions.

There are 6 altogether.

Cube roots of 2

6 is *not* a power of 2, and so $\sqrt[3]{2}$ cannot be constructed by ruler and compass.

Numbers and harmony: the Langlands Program

Modern number theory studies the symmetries of algebraic equations using ideas growing out of the work of the Canadian mathematician Robert Langlands (1936–).

They are a sophisticated reinterpretation of the ancient Greek notion that numbers should give rise to harmonies.

Numbers and harmony: the Langlands Program

Usual harmonics on a string can be written as mathematical functions:

$$e^{2\pi inx}$$

(n is an integer, i.e. whole number, and x is the variable, a real number)

These are *periodic* functions, invariant under the translation $x \mapsto x + 1$.

Numbers and harmony: the Langlands Program

The Langlands Program involves more sophisticated harmonics.

Here is the harmonic that governs $\sqrt[3]{2}$:

$$f(z) = e^{2\pi i\, z} \prod_{n=1}^{\infty} (1 - e^{2\pi i\, 6nz})(1 - e^{2\pi i\, 18nz})$$

$$= e^{2\pi i\, z} - e^{2\pi i\, 7z} - e^{2\pi i\, 13z} - e^{2\pi i\, 19z} + e^{2\pi i\, 25z} + 2e^{2\pi i\, 31z} + \cdots$$

Numbers and harmony: the Langlands Program

$$f(z) = e^{2\pi i\, z} \prod_{n=1}^{\infty} (1 - e^{2\pi i\, 6nz})(1 - e^{2\pi i\, 18nz})$$

$$= e^{2\pi i\, z} - e^{2\pi i\, 7z} - e^{2\pi i\, 13z} - e^{2\pi i\, 19z} + e^{2\pi i\, 25z} + 2e^{2\pi i\, 31z} + \cdots$$

The variable z is a complex number (with positive imaginary part), and the function $f(z)$ has periodic behaviour in two (non-commuting) directions:

$$f(z+1) = f(z)$$

$$f(\frac{-1}{108z}) = -6\sqrt{3}izf(z)$$

Numbers and harmony: the Langlands Program

(The precise mathematical description of $f(z)$ is that it is a *modular form of weight* 1 *and level* 108.)

Numbers and harmony: the Langlands Program

$$f(z) = e^{2\pi i\, z} - e^{2\pi i\, 7z} - e^{2\pi i\, 13z} - e^{2\pi i\, 19z} + e^{2\pi i\, 25z} + 2e^{2\pi i\, 31z} + \cdots$$

The most interesting coefficients are the coefficients of $e^{2\pi i\, pz}$, where p is a prime (different from 2 or 3).

This coefficient is equal to one less than the number of solutions to $x^3 - 2 = 0$ in congruences modulo p.

In particular, it encodes whether p is a prime we can use to detect irrationality of $\sqrt[3]{2}$.

Numbers and harmony: the Langlands Program

$$f(z) = e^{2\pi i\,z} - e^{2\pi i\,7z} - e^{2\pi i\,13z} - e^{2\pi i\,19z} + e^{2\pi i\,25z} + 2e^{2\pi i\,31z} + \cdots$$

E.g. the first time we get a coefficient of 2 is for $p = 31$.

Numbers and harmony: the Langlands Program

To explain this, notice that

$$\begin{aligned}(x-2)(x-10)(x+12)\\ &= x^3 - 124x + 240\\ &\qquad = x^3 - (4 \times 31)x + (8 \times 31 - 2),\end{aligned}$$

which *is*

$$x^3 - 2$$

if we ignore all the multiples of 31.

Numbers and harmony: the Langlands Program

The Langlands Program conjectures that all irrational numbers that arise as zeroes of a polynomial equation have an associated harmonic (called a *modular form* or *automorphic form*). These are like notes arising from the vibrations of higher dimensional drum skins.

Numbers and harmony: the Langlands Program

The relationship between the harmonic and the irrational number is given via congruences modulo primes.

The possible irrationalities are limited by the possible harmonics. This has implications in both directions.

E.g. if we can construct interesting irrational numbers, these should also give rise to interesting (perhaps previously unknown) harmonics.

Numbers and harmony: the Langlands Program

Many results have been proved in the Langlands Program, but many still remain to be proved.

A currently open problem: to construct the harmonics that govern solutions to a degree 5 equation

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$$

with integer coefficients, in the case when all of its solutions are real numbers.

The conversation continues . . .