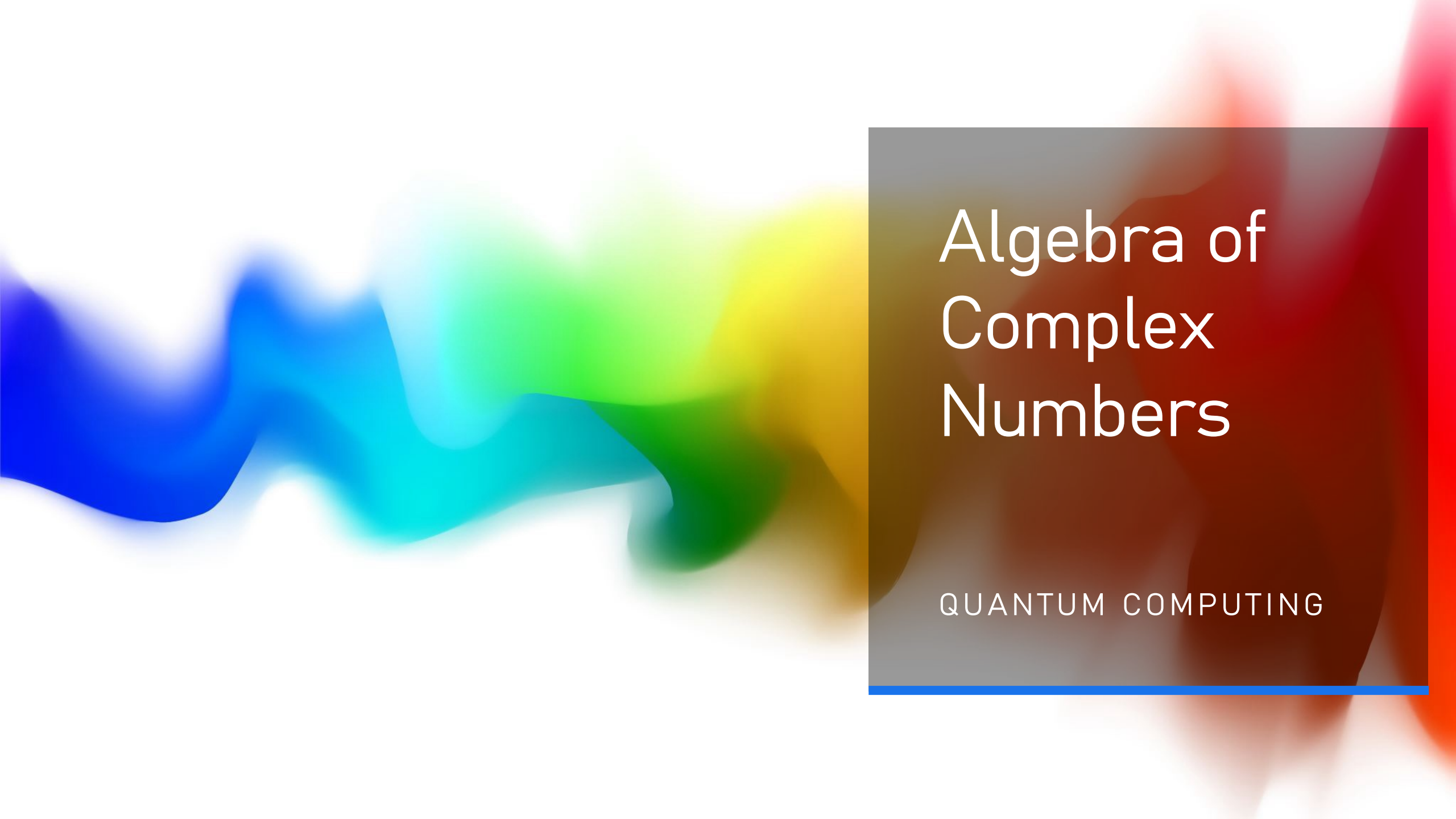




Algebra of Complex Numbers

QUANTUM COMPUTING



Math Tools

- Quantum computing does not require new mathematics.
- Instead, it uses a small collection of ideas from classical mathematics:
 - · complex numbers
 - · vectors in complex space
 - · inner products and geometry
 - · linear operators
 - · eigenvalues and eigenvectors
- Together these form the mathematical language of **Hilbert spaces**.
- Over the next few lectures we will build these tools step by step.

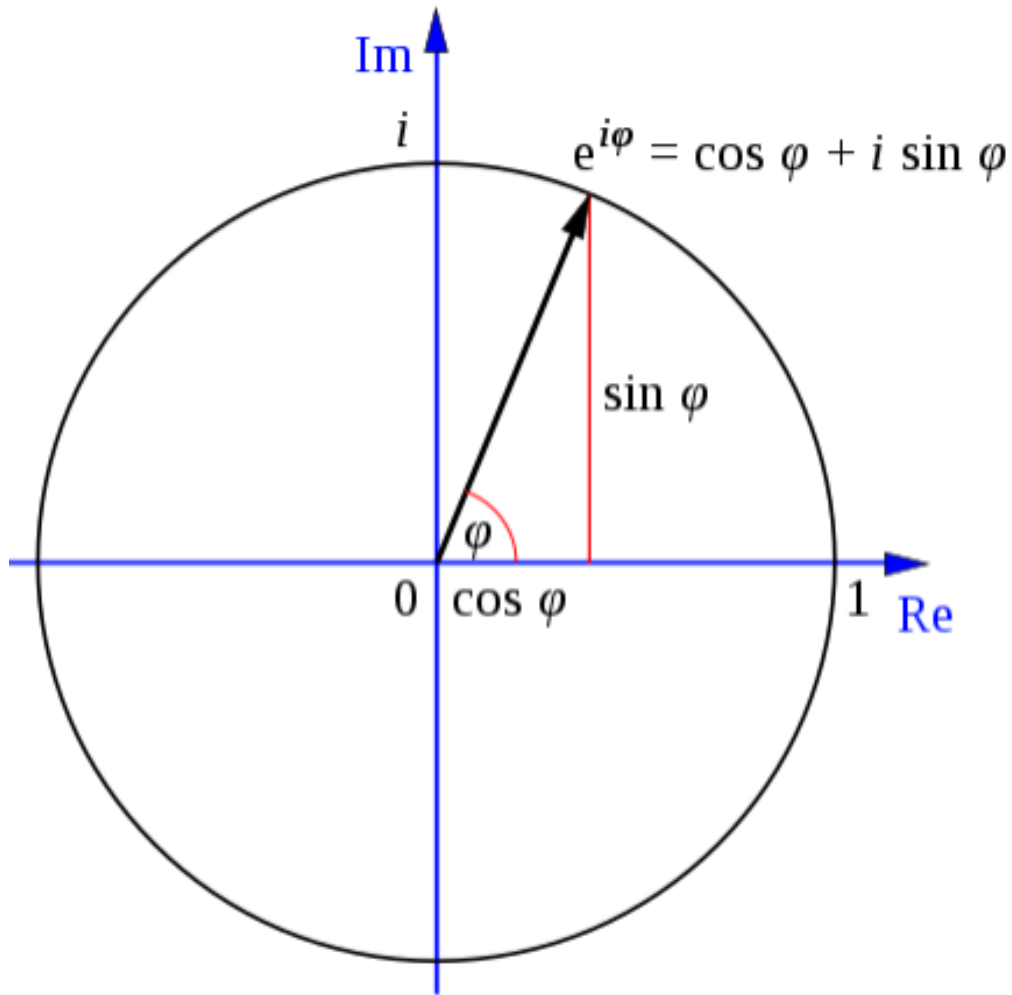


Why Complex Numbers

- There is much debate about whether complex numbers are needed to represent quantum physics.
- The truth is that complex numbers are an elegant and useful way to do the math.
- https://www.feynmanlectures.caltech.edu/I_22.html

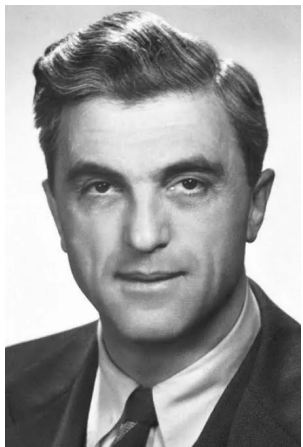
Wigner's question: Why does abstract mathematics describe nature so well?

Eugene P. Wigner (1960), "The Unreasonable Effectiveness of Mathematics in the Natural Sciences." Communications on Pure and Applied Mathematics 13, 1–14.
<https://doi.org/10.1002/cpa.3160130102>

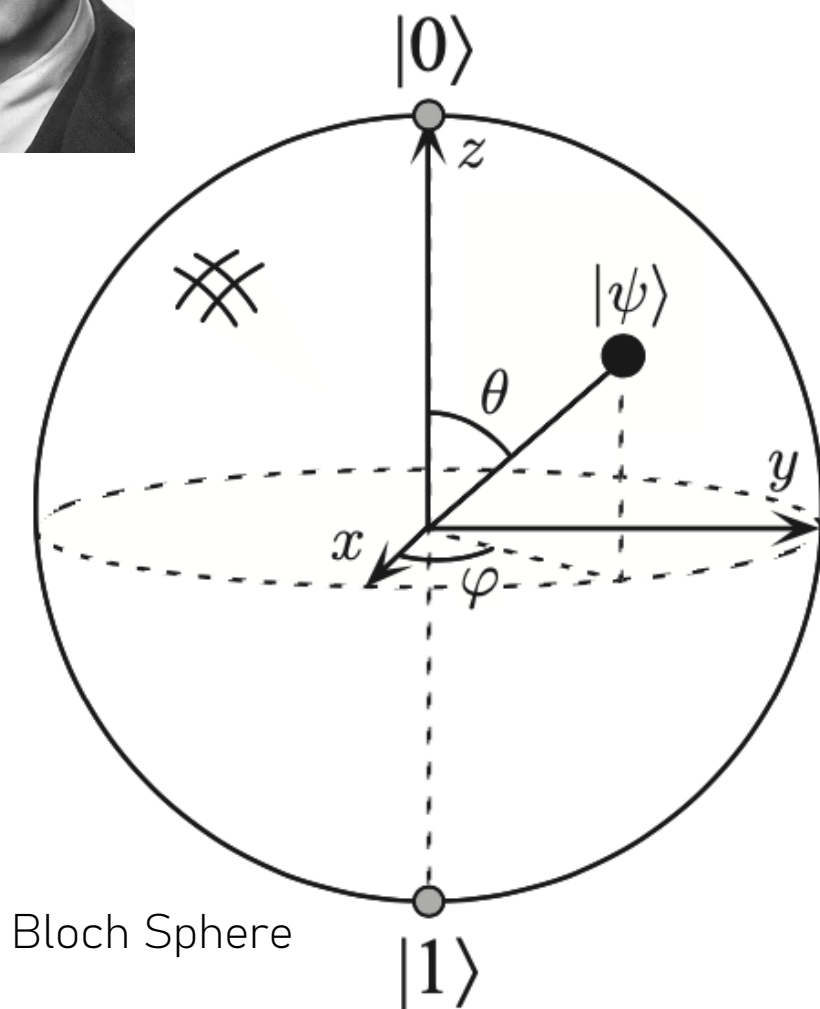


Complex Numbers are Essential to Quantum Computing

- It is possible to use math that doesn't involve complex numbers to reason about quantum computing, but in all cases you have to emulate what complex numbers give you for free.
- Learning complex number algebra is central to understanding quantum computing because quantum systems evolve by manipulating *amplitudes*, not probabilities, and amplitudes are inherently complex quantities whose phase and magnitude together determine all observable outcomes.



Felix Bloch (Swiss)
Stanford University
Nobel Prize in Physics in 1952



Complex Numbers are Essential to Quantum Computing

- Quantum computation exploits superposition and interference in a continuous state space.
- For a single qubit, that state space is a sphere.
- Complex numbers are essential because they turn quantum evolution into rotations on that sphere.

A bit of History

The following equation is unsolvable in the domain of real numbers.

$$x^2 + 1 = 0$$

In the 16th century, [Gerolamo Cardano](#) and [Rafael Bombelli](#) independently encountered the square root of -1 while solving polynomial equations.

Cardano famously described these quantities as “*as subtle as they are useless*,” reflecting the deep unease mathematicians felt toward them.

At the time, there was a serious philosophical debate about whether such values were meaningful mathematics or merely algebraic absurdities.

Bombelli took a different view. He argued that if these quantities obeyed **consistent rules of algebra**, then they deserved to be treated as legitimate mathematical objects, regardless of their lack of geometric interpretation.

A bit of History

The following equation is unsolvable in the domain of real numbers.

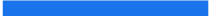
$$x^2 + 1 = 0$$

In the 17th century, René Descartes dismissed the square root of -1 as “*imaginary*.” The term was intended as an insult, but the name stuck.

It was Leonhard Euler in the **18th century** who fully rehabilitated these numbers. Euler showed that the number system could be extended naturally by introducing a new fundamental quantity and demonstrated its deep connection to trigonometry and exponential functions. He introduced the symbol i treating it as no less fundamental to this extended number system than 1, 2, or $1/2$ are to the real numbers.

$$e^{i\theta} = \cos \theta + i \sin \theta.$$

Much later, Richard Feynman would call Euler's identity “*the most remarkable formula in mathematics*.”



In this new number system the solution to

$$x^2 + 1 = 0$$

Is,

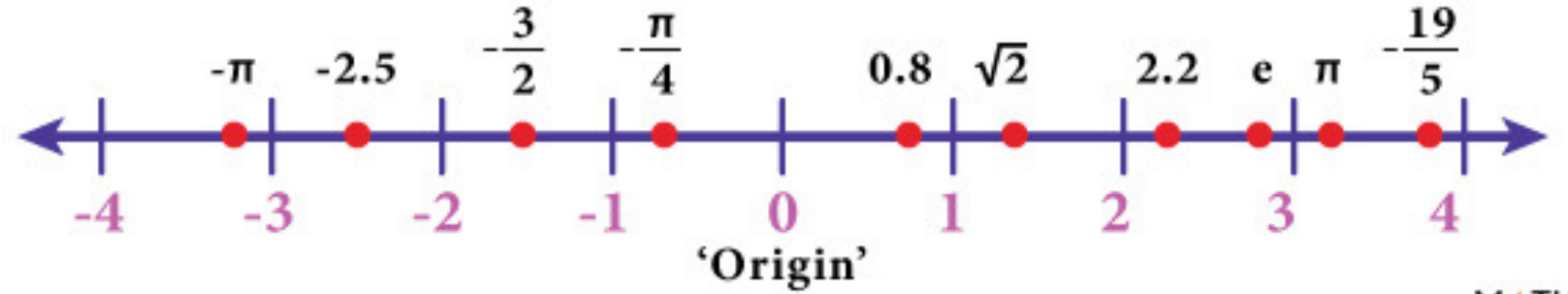
$$x^2 + 1 = 0$$

$$x^2 = -1$$

$$x = \sqrt{-1}$$

$$x = i$$

Real number line ($\mathbb{R}$)



MATH
MONKS

Purely imaginary numbers follow the same rules of algebra as real numbers::

Scalar multiplication rules are the same. For real numbers a and b :

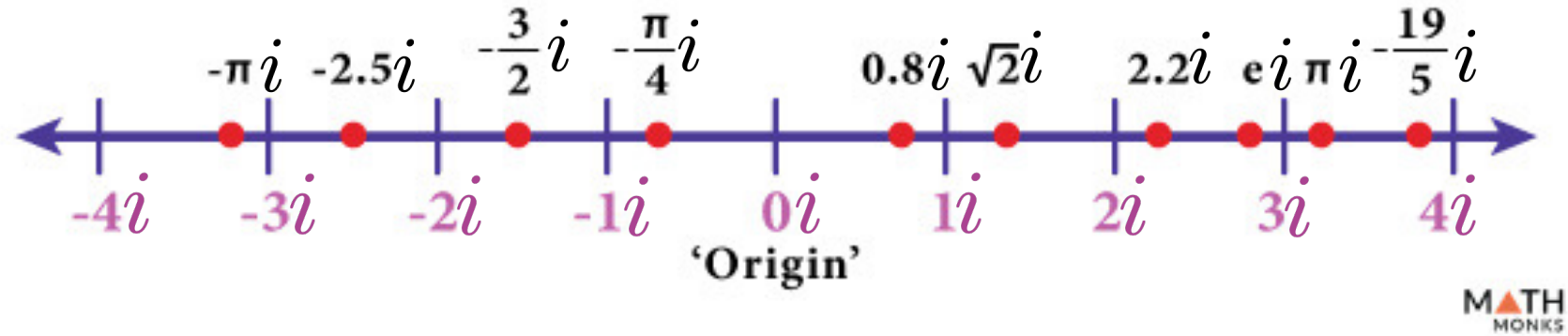
$$a(bi) = (ab)i$$

Addition rules are the same':

$$bi + ci = (b + c)i$$

closure, associativity, commutativity, identity, and additive inverses are all identical to algebra with real numbers

Imaginary number line ($i\mathbb{R} = \{bi \mid b \in \mathbb{R}\}$)



Purely imaginary numbers follow the same rules of algebra as real numbers;:

Scalar multiplication rules are the same. For real numbers a and b : $a(bi) = (ab)i$

Addition rules are the same':

$$bi + ci = (b + c)i$$

closure, associativity, commutativity, identity, and additive inverses are all identical to algebra with real numbers.

But notice that when we multiply to imaginary numbers, we don't necessarily get an imaginary number back.

$$(bi)(ci) = bc i^2 = bc(-1) = -bc$$



But notice that when we multiply two imaginary numbers, we don't necessarily get an imaginary number back.

$$(bi)(ci) = bc i^2 = bc(-1) = -bc$$

In other words, imaginary numbers are not closed under imaginary number multiplication.

When you multiply imaginary numbers you get kicked back onto the real number line but with a negative sign:

$$(bi)(ci) = -(bc)$$



Division follows the same pattern but without the minus sign

$$\frac{bi}{ci} = \frac{b}{c}$$

$$i^0 = 1$$

$$i^1 = i$$

Exponentiation:

$$i^2 = -1$$

:

$$i^3 = -i$$

$$i^4 = 1$$

$$i^5 = i$$

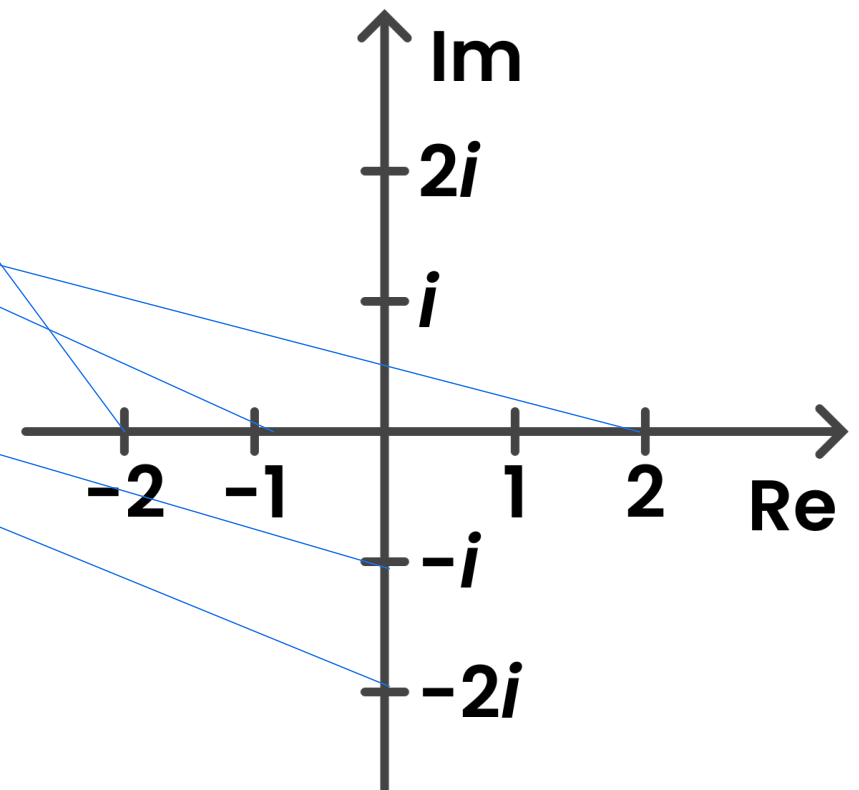
Quantum mechanics becomes elegant once we allow exponentials and logarithms of imaginary numbers, because they turn time evolution, phase, and interference into simple geometric operations.

... but we aren't ready for that yet.

Not being closed under multiplication results in a choice. Either we forbid multiplication or we recognize that imaginary numbers and real numbers are related under basic algebraic operations.

If we choose the latter, we have to go beyond number lines to a number cross. Eg

$$i \cdot 2i = 2i^2 = 2(-1) = -2$$



Mixing Real and Imaginary Numbers

- We looked at the algebra of imaginary numbers and found it maps to the imaginary number line but also the real number line forming a cross.
- A natural extension is to see what happens when we add, multiply, and divide numbers that contain both imaginary and real numbers. Eg.

$$a + bi$$

$$a(bi)$$

- Any finite length combination of imaginary and real numbers can be reduced to just:

$$a + bi$$

Mixing Real and Imaginary Numbers

- We looked at the algebra of imaginary numbers and found it maps to the imaginary number line but also the real number line forming a cross.
- A natural extension is to see what happens when we add, multiply, and divide numbers that contain both imaginary and real numbers.
- If we include in this new set of numbers

$$bi = 0 + bi$$

$$a = a + 0i$$

- We can see that it includes all the imaginary numbers and real numbers.

Mixing Real and Imaginary Numbers

When we do arithmetic with numbers that have a real term and an imaginary term we find that the result is always another number with a real and imaginary part.

Under addition: $(a + bi) + (c + di) = (a + c) + (b + d)i$

Under multiplication;

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i$$

Mixing Real and Imaginary Numbers

When we do arithmetic with numbers that have a real term and an imaginary term we find that the result is always another number with a real and imaginary part.

Division is more complicated but just as mechanical:

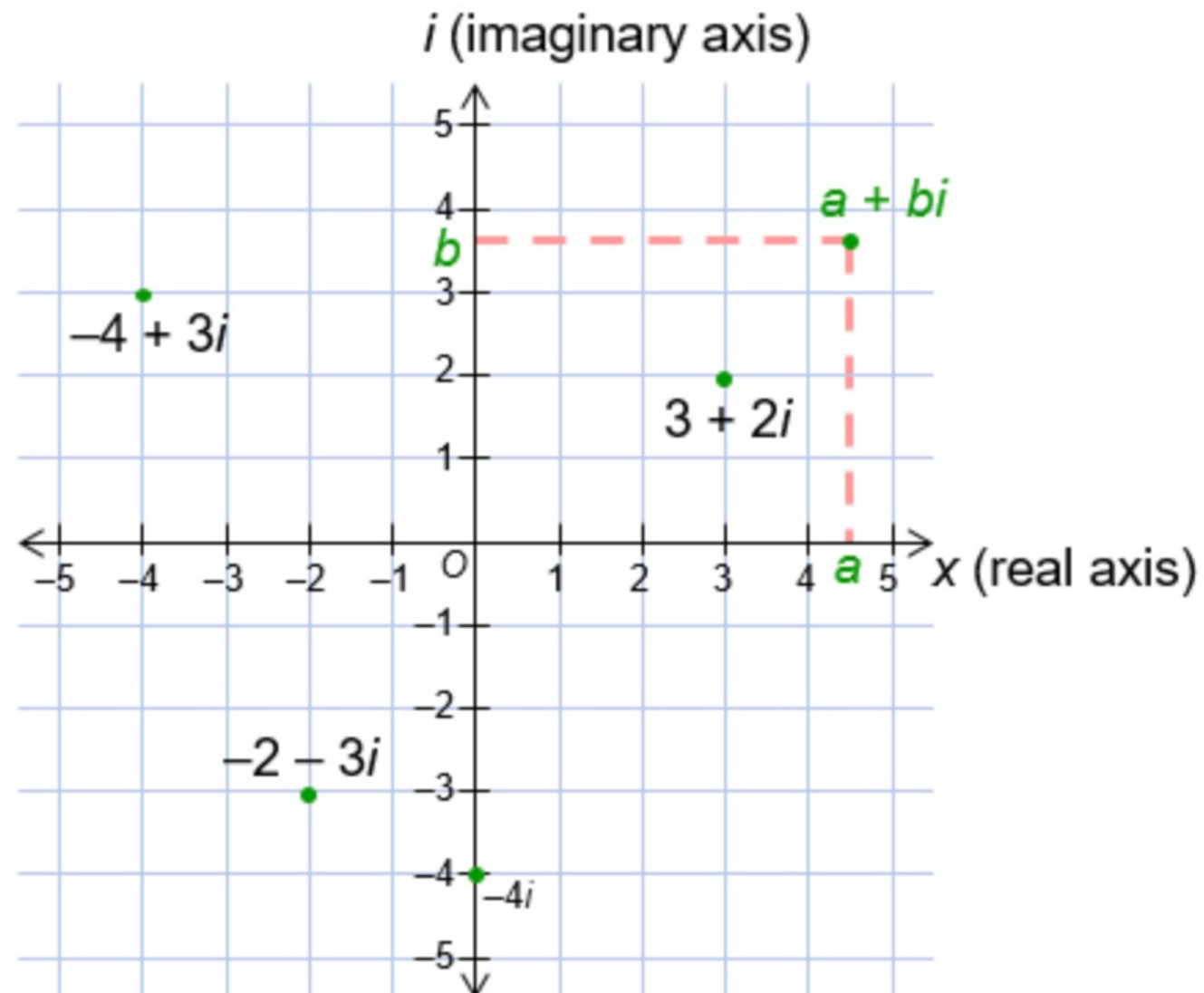
$$\frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{c^2 + d^2} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}i$$

Assuming we don't divide by 0, since division by 0 gives infinity which isn't a number at all.

$$\forall (c + di) \neq 0$$

Fundamental Theorem of Algebra

- The operations applied to numbers with a real part and an imaginary part seem to behave really well. Addition, multiplication, and division of these numbers always results in a number with a real and imaginary part as the result.
- The results that are possible with these numbers are not just limited to the number line cross we saw with pure real or pure imaginary numbers.
- Now our results form a plane.



Complex Numbers



Friedrich Gauss
University of Göttingen

In the 19th century, Carl Friedrich Gauss recognised that these new numbers were exceptionally well behaved, and that Leonhard Euler had already shown how elegantly they relate to the real numbers. Gauss concluded that they deserved a name of their own, and called them **complex numbers**.

Complex Numbers

Nearly a hundred years before the development of quantum physics, complex numbers were already being used to solve problems in engineering, geometry, acoustics, optics, and other areas of classical science. In many cases, mathematics that is cumbersome or even blocked when restricted to real numbers becomes simple and tractable when extended to the complex numbers. The intermediate steps of a calculation may involve complex values, but the final result often lies on the real number line and is therefore physically observable.



Friedrich Gauss
University of Göttingen

Let's look at an example:



Remember [Gerolamo Cardano](#) who was the first person to write about imaginary numbers?

He lived in what is now Italy. At the time mathematicians would challenge each other to “mathematical duals”.

These were sometimes conducted in public with an audience. Each mathematician would challenge the other with, say 30 problems they knew how to solve. Whichever dualist solved the problems they were given first won.

The methods these mathematicians used were often closely guarded secrets. These were high stakes duals with cash prizes and huge boosts or loss of reputation. These duals could make or break careers.

Cardanao participated in these duals and was able to very quickly solve cubic equations of the form:

$$x^3 - 15x - 4 = 0$$

To be clear this was long before Rene Descarte invented the algebraic notation we use now. The math of the 16th C was largely devoid of symbols.

Let's look at an example:

[Cardano](#) revealed much later how he solved these kinds of problems in his 1545 book.

Let's solve

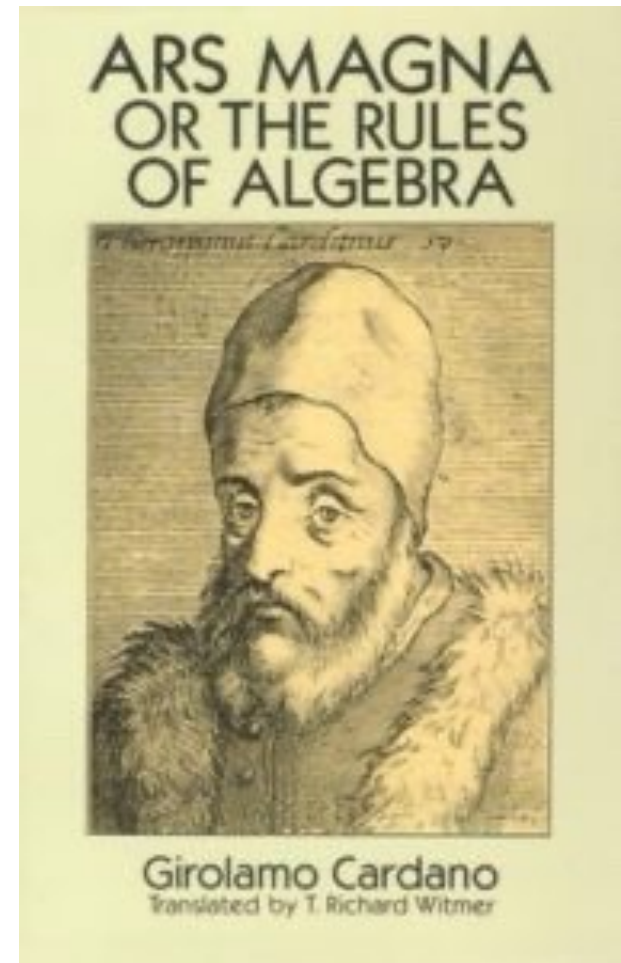
$$x^3 - 15x - 4 = 0$$

Cardano showed that cubic equations of the form:

$$x^3 + px + q = 0$$

can be written as:

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$



Let's look at an example:

$$x^3 + px + q = 0$$

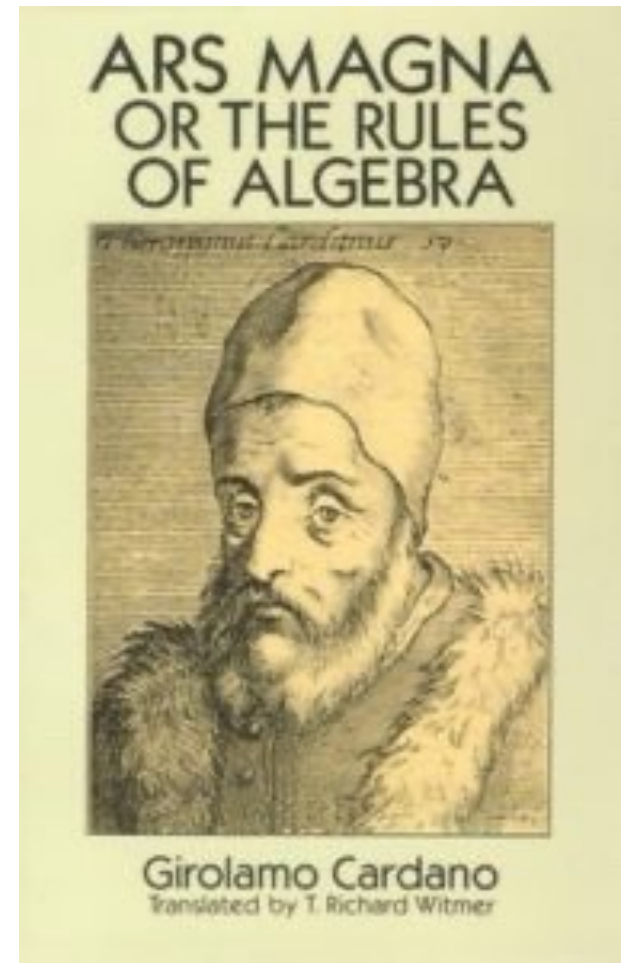
$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

So far so good as long as the numbers don't go negative under the square root.

At this time numbers were thought of as real things that mapped to physical reality.

The problem with a negative root is that there is no real number that multiplied by itself equals -1, so negative roots were just treated as wrong.

Cardano's trick was to hold his nose and just pretend that the nonsense values were OK and work through the math anyway. He seems quite embarrassed by the process in his later writing, calling them "useless numbers"



Let's look at an example:

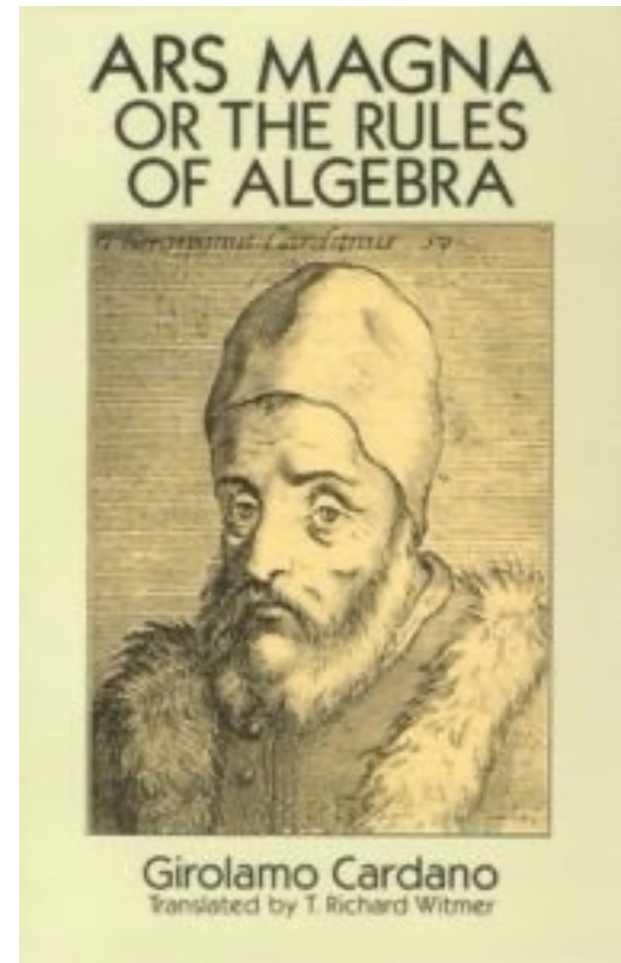
$$x^3 - 15x - 4 = 0 \quad x^3 + px + q = 0$$

$$p = -15, \quad q = -4$$

$$\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3 = (-2)^2 + (-5)^3 = 4 - 125 = -121$$

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{-121}} + \sqrt[3]{-\frac{q}{2} - \sqrt{-121}}$$

$$x = \sqrt[3]{-\frac{-4}{2} + \sqrt{-121}} + \sqrt[3]{-\frac{-4}{2} - \sqrt{-121}}$$



Let's look at an example:

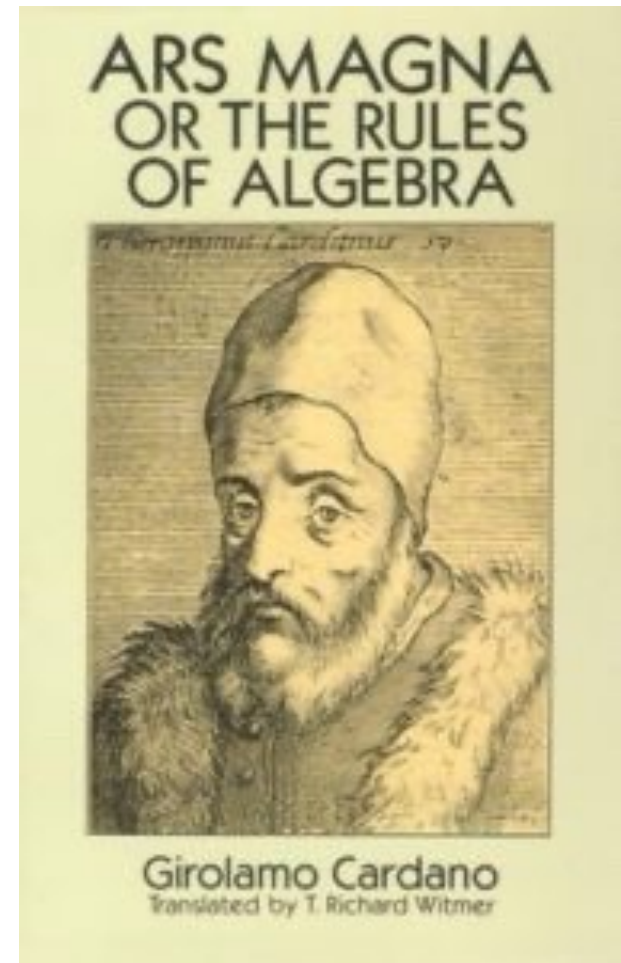
$$x^3 - 15x - 4 = 0 \quad x^3 + px + q = 0$$

$$p = -15, \quad q = -4$$

$$x = \sqrt[3]{-\frac{-4}{2} + \sqrt{-121}} + \sqrt[3]{-\frac{-4}{2} - \sqrt{-121}}$$

$$x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}$$

$$\sqrt{-121} = \sqrt{121}\sqrt{-1} = 11i$$



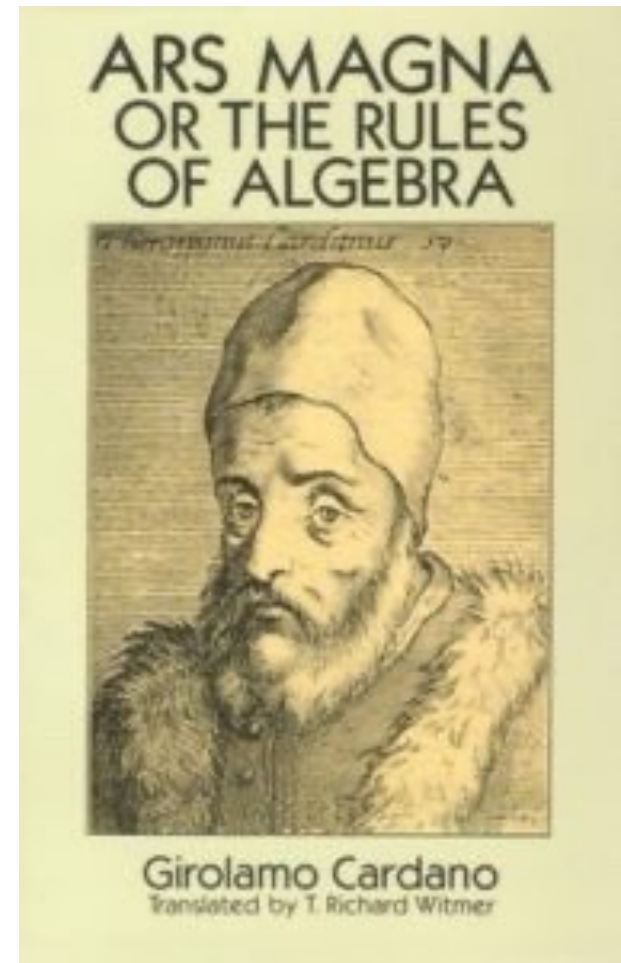
Let's look at an example:

$$x^3 - 15x - 4 = 0 \quad x^3 + px + q = 0$$

$$p = -15, \quad q = -4$$

$$\sqrt{-121} = \sqrt{121}\sqrt{-1} = 11i$$

$$x = \sqrt[3]{2 + 11i} + \sqrt[3]{2 - 11i}$$



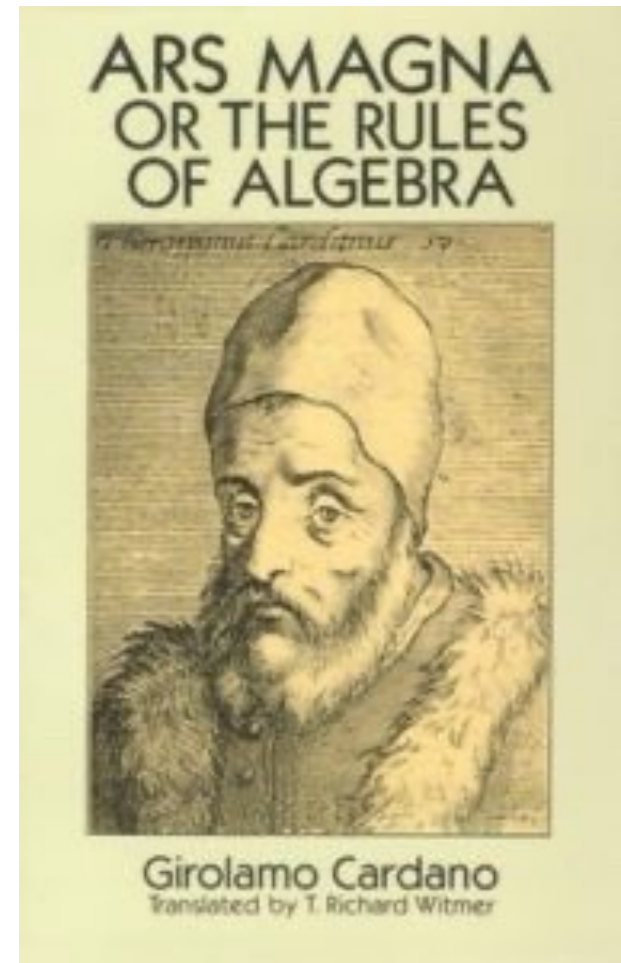
Let's look at an example:

$$x^3 - 15x - 4 = 0 \quad x^3 + px + q = 0$$

$$p = -15, \quad q = -4$$

$$x = \sqrt[3]{2 + 11i} + \sqrt[3]{2 - 11i}$$

Without a systematic way to extract cube roots of complex numbers, Cardano would have relied on trial, pattern recognition, and verification to see whether any simple complex number cubed to $2 + 11i$



Let's look at an example:

We know the answer to these cube roots must be some number with a real and/or Imaginary part.

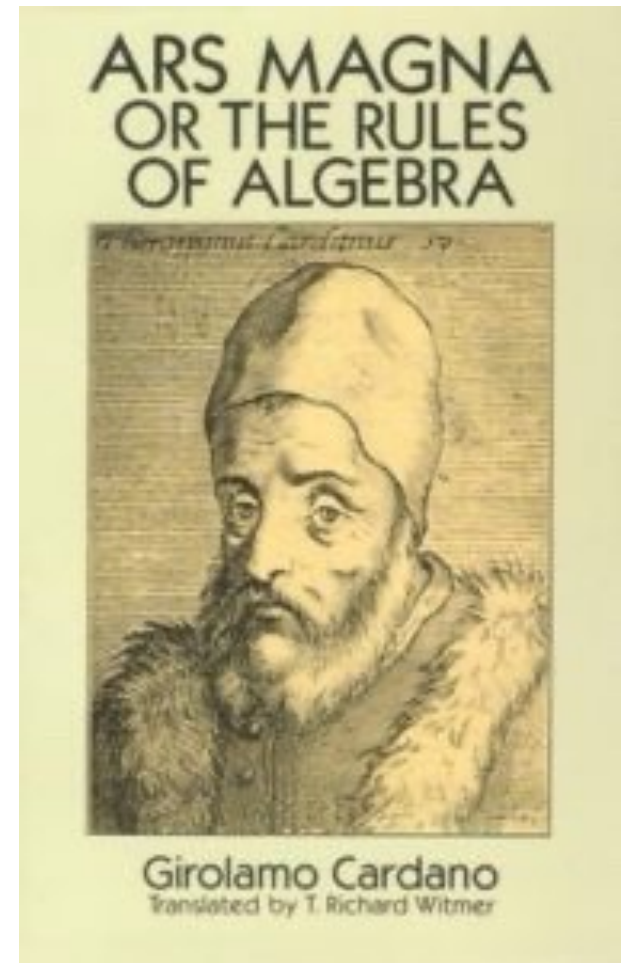
$$\sqrt[3]{2 + 11i} = a + bi, \quad \sqrt[3]{2 - 11i} = c + di$$

At this point Cardano would have tried small integer solutions:

$$a = 2$$

$$b = 1$$

$$\begin{aligned}(2 + i)^3 &= (2 + i)(2 + i)(2 + i) \\ &= (2 + i)(3 + 4i) = 6 + 8i + 3i + 4i^2 \\ &= 6 + 11i + 4(-1) \\ &= 2 + 11i\end{aligned}$$



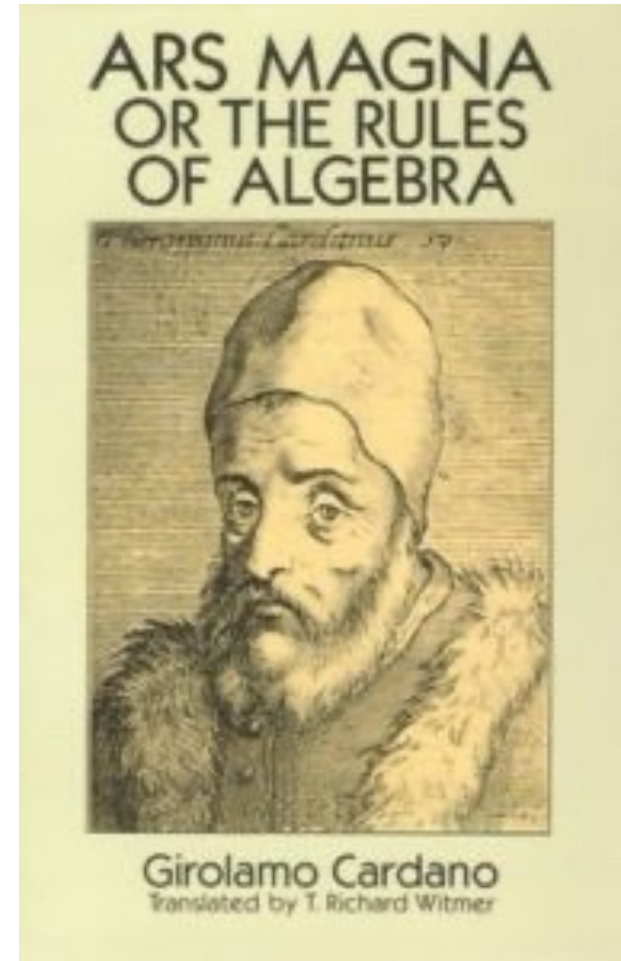
Let's look at an example:

We know the answer to these cube roots must be some number with a real and/or Imaginary part.

$$\sqrt[3]{2 + 11i} = a + bi, \quad \sqrt[3]{2 - 11i} = c + di$$

At this point Cardano would have tried small integer solutions:

$$\begin{aligned} c &= 2 \\ d &= -1 \end{aligned} \quad \begin{aligned} (2 - i)^3 &= (2 - i)(2 - i)^2 \\ &= (2 - i)(3 - 4i) \\ &= 6 - 8i - 3i + 4i^2 \\ &= 2 - 11i \end{aligned}$$



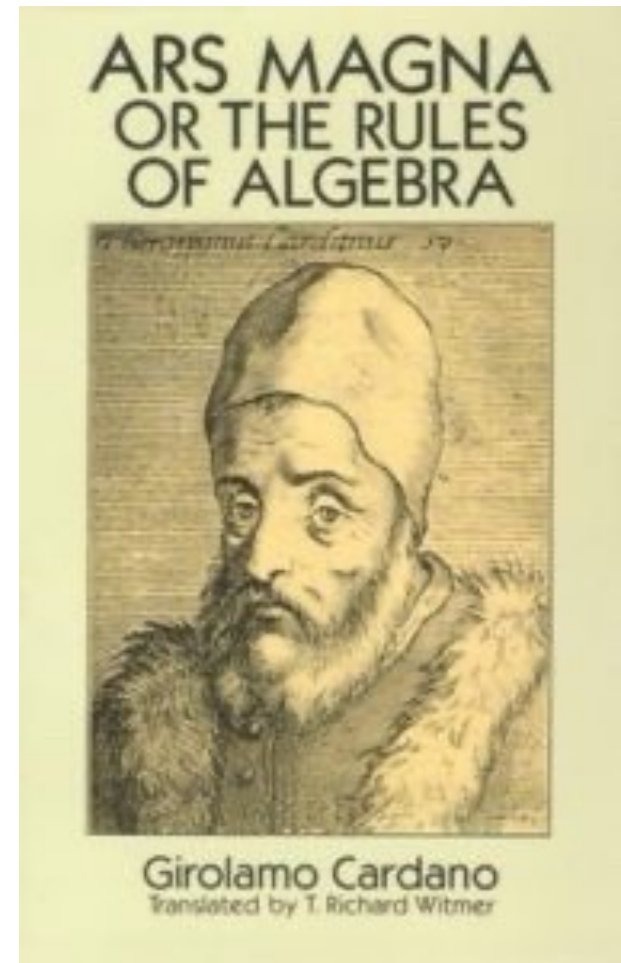
Let's look at an example:

$$x^3 - 15x - 4 = 0$$

$$x = \sqrt[3]{2 + 11i} + \sqrt[3]{2 - 11i}$$

$$x = (2 + 1i) + (2 - 1i)$$

$$x = 4$$



The mathematics we will use to describe quantum computers follows a very similar path. We use imaginary (complex) numbers to describe the state of a quantum system as it evolves, but the output of a quantum computation is always real at the end of the process.



Modulus

- Modulus answers: *how big is a complex number?*

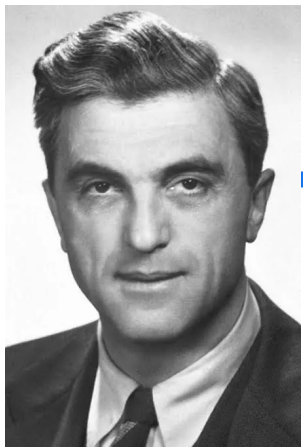
$$|a + bi| = \sqrt{a^2 + b^2}$$



Complex Conjugate

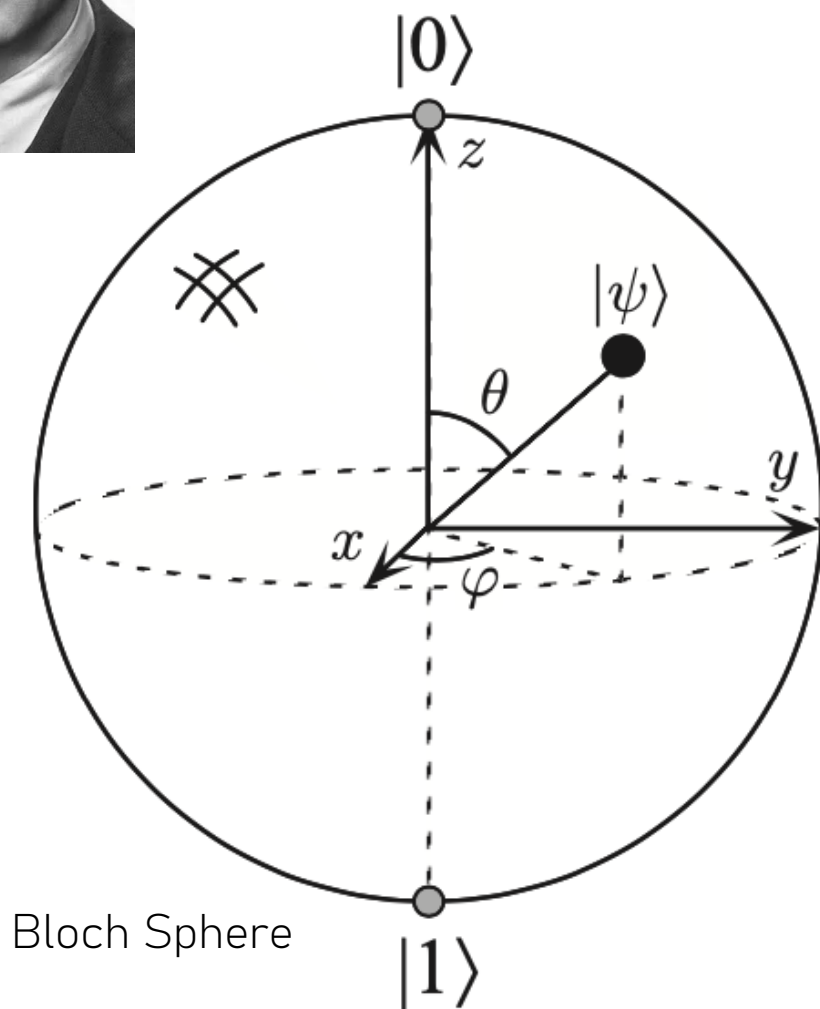
- Conjugates answer: *how do imaginary parts cancel cleanly?*

$$(a + bi)(a - bi) = a^2 + b^2$$



Felix Bloch (Swiss)
Stanford University

■ Nobel Prize in Physics in 1952



Complex Numbers are Essential to Quantum Computing

- We will use that equation to describe the state of the qubit.
- The qubit is a geometric representation described by

$$e^{i\theta} = \cos \theta + i \sin \theta.$$

Later we will use the following to reason about quantum computing (this is a preview, we will learn the notation soon)

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right) |0\rangle + e^{i\phi} \sin\left(\frac{\theta}{2}\right) |1\rangle$$

In class exercises

Using the expressions given in the slides, in any language you like write the following functions:

$$[a, b] \leftarrow \text{complex_add}(c, d)$$
$$[a, b] \leftarrow \text{complex_mult}(c, d)$$
$$[a, b] \leftarrow \text{complex_div}(c, d)$$
$$[a, b] \leftarrow \text{complex_mod}(c, d)$$
$$[a, b] \leftarrow \text{complex_conj}(c, d)$$