Complex numbers

It probably does the imaginary number $i = \sqrt{-1}$ a disservice to call it an imaginary number; numbers are all to a certain extent imaginary. It is easy to think there is something concrete about the idea of say ‘five’, but it is a concept not a thing, it is the number of elements in sets that have five elements, or some such piece of semi-philosophical legerdemain. Negative numbers, or real numbers such as $\sqrt{2}$ are even less obviously ‘real’ despite the advertizing given by calling real numbers by that name. However, there is a long history of adding new types of numbers because they are demanded by the algebraic or arithmetical rules that have been discovered; so, if you have subtraction and are able to do $7 - 5 = 2$ you immediately wonder what $5 - 7$ is and hence invent negative numbers; if you have division and know $6/3 = 2$ you wonder what $5/2$ is and invent rationals, when you know about Pythagoras’s theorem and can work out $\sqrt{25} = 5$ you get worried about $\sqrt{2}$ and invent irrational numbers. Similarly we have known how to solve quadratic equations $ax^2 + bx + c = 0$ using

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \tag{1}$$

since the dawn of cities in Babylon, and that immediately raises the question of what $\sqrt{-1}$ is and leads to the so called imaginary number and complex numbers. In fact, complex numbers turn out to be a very powerful and useful mathematical construction, extremely helpful in, to give a computer science example, signal processing.

So a complex number has a real part and an imaginary part:

$$z = x + iy \tag{2}$$

examples would be $1 + 2i$ or $-3i$ or whatever. You can add them:

$$x_1 + iy_1 + x_2 + iy_2 = (x_1 + x_2) + (y_1 + y_2)i \tag{3}$$

so $3 + 2i$ added to $-2 + 5i$ is $1 + 7i$. You can multiply them, rather than getting tangled up in symbols, lets just do a specific example:

$$(1 + 3i)(2 - 5i) = 2 + 6i - 5i - 15i^2 = 17 + i \tag{4}$$

where we have used that $i^2 = -1$; this is, after all, sort of the point of i.

There is some complex number specific algebraic manipulations, the **conjugate** of a complex number is the complex number you get by switching the sign of the imaginary part, so if $z = x + iy$ then the conjugate is

$$z^* = x - iy \tag{5}$$

There are actually two notations often used for the conjugate, z^* and $\bar{z}$; you see both used, sometimes by the same person; while we are talking notation, you should note that electronic engineers sometimes use j for the complex number instead of i; so they use $j = \sqrt{-1}$; this is because the use i for current. The absolute value of a complex number is

$$|z| = \sqrt{zz^*} \tag{6}$$

This is a real number, if $z = x + iy$ then, if you expand out the bracket you can see

$$zz^* = (x + iy)(x - iy) = x^2 + y^2 \tag{7}$$

One perhaps surprising thing is that you can divide two complex numbers; a complex number has the form $x + iy$ but dividing $z_1 = x_1 + iy_1$ by $z_2 = x_2 + iy_2$ seems to give something that doesn't have this form

$$\frac{z_1}{z_2} = \frac{x_1 + iy_1}{x_2 + iy_2} \tag{8}$$

However, you can get rid of the complexness of the denominator by multiplying by z_2^*/z_2^*; you can do this because it is actually just one. Hence

$$\frac{z_1}{z_2} = \frac{x_1 + iy_1}{x_2 + iy_2} = \frac{x_1 + iy_1}{x_2 + iy_2}\frac{x_1 - iy_1}{x_2 - iy_2} = \frac{(x_1 + iy_1)(x_2 + iy_2)}{x_2^2 + y_2^2} \tag{9}$$

and if you multiply out the numerator, this does indeed have the form $x+iy$. Lets do an example@

$$z = \frac{1 + i}{3 - 2i} \tag{10}$$

Now the conjugate of the denominator is $3 + 2i$ so

$$z = \frac{1 + i}{3 - 2i}\frac{3 + 2i}{3 + 2i} = \frac{(1 + i)(3 + 2i)}{13} = \frac{1}{13} + \frac{5}{13}i \tag{11}$$

Now, this ability to divide complex numbers is interesting. Complex numbers are somewhat akin to two dimensional vectors, you can map from one to the other:

$$z = x + iy \leftrightarrow \mathbf{z} = x\mathbf{i} + y\mathbf{j} \tag{12}$$

However, while you can add two dimensional vectors, you can't divide them, the complex structure is an additional structure beyond the geometrical structural of two-dimensional space. In fact, the ability to add a structure that allows division is only possible in certain numbers of dimensions, in two-dimensions there are complex numbers, in four there are another type of number called quoternions and in eight dimensions a very difficult structure called and octonion algebra.

Apart from this musing about division and geometry, thinking of complex numbers as points in two-dimensional space leads to an important idea: the polar representation. Polar coordinates are an alternative coordinate system for two dimensions. Instead of writing the position as (x, y) where x is the distance in the x direction and y the distance in the y direction you can write the position in polar coordinates as (r, θ) where r is the distance from the origin and θ is the angle the line to the position makes with the x axis. It is easy to translate between the two, a little bit of trigonometry tells us that $r = \sqrt{x^2 + y^2}$ and $\theta = \arctan{(y/x)}$ and, conversely, $x = r\cos\theta$ and $y = r\sin\theta$.

The same thing can be done with complex number, this is called the **polar representation** and relies on the Euler formula

$$e^{i\theta} = \cos\theta + i\sin\theta \tag{13}$$

It might seem that almost everything is named after Euler! There are lots of ways to derive this formula, including using the Taylor series; but we will just accept it here. This means there are two ways to write a complex number:

$$z = x + iy = re^{i\theta} \tag{14}$$

where $r = \sqrt{zz^*} = \sqrt{x^2 + y^2}$ and $\theta = \arctan{(y/x)}$. As an example,

$$1 + i = \sqrt{2}e^{i\pi/4} \tag{15}$$

One advantage of the polar representation is that it allows you to find powers of complex numbers, if

$$z = re^{i\theta} \tag{16}$$

then

$$z^n = r^n e^{in\theta} \tag{17}$$

This has a slightly surprising result when applied to roots. Recall the way there are two solutions to $x^2 = a$, you have $x = \sqrt{a}$ obviously, but also $x = -\sqrt{a}$. When you include complex numbers this is only the first in a whole series of similar examples, so, consider the equation:

$$z^n = a \tag{18}$$

in polar form this give

$$\left(re^{i\theta}\right)^n = a \tag{19}$$

or

$$r^n e^{in\theta} = a \tag{20}$$

so, first off $r = \sqrt[n]{a}$, so the interesting bit is the **n-th root of unity**:

$$e^{in\theta} = 1 \tag{21}$$

Now, obviously, $\theta = 0$ is a solution, but so is $\theta = 2\pi/n$ since

$$e^{in2\pi/n} = e^{2\pi i} = \cos 2\pi + i \sin 2\pi = 1 \tag{22}$$

In fact there are n solution: 0, $2\pi/n$, $4\pi/n$ and so on until you get to 2π, that isn't a new solution, it is equivalent to $\theta = 0$; for example

$$e^{3i\theta} = 1 \tag{23}$$

has solutions $\theta = 0$, $\theta = 2\pi/3$ and $\theta = 4\pi/3$, or

$$e^{4i\theta} = 1 \tag{24}$$

has solutions $\theta = 0$, $\theta = \pi/2$, $\theta = \pi$ and $\theta = 3\pi/2$. For

$$e^{2i\theta} = 1 \tag{25}$$

the two solutions are $\theta = 0$ and $\theta = \pi$ and since

$$e^{\pi i} = \cos \pi + i \sin \pi = -1 \tag{26}$$

this is the $x^2 = 1$ means $x = 1$ or $x = -1$ we mentioned earlier.

Modular arithmetic

Arithmetic should be thought of as the basic mathematical operations such as addition, subtraction, multiplication, and division. This is something with which you are very familiar with in the sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, but there are many more ways of constructing sets of numbers on which there exist consistent arithmetic laws. The arithmetic of a clock is especially interesting because we can construct a consistent set of arithmetic laws on the *finite* set of hours.

Let us start by studying 'clock addition'. If you add 4 hours to 10 o'clock, then you get 2 o'clock (rather than 14 o'clock, since we will work here with the 12-hour clock). The way that we will write this is:

$$10 + 4 \equiv 2 \pmod{12}.$$

The $\equiv$ sign should be read as 'is equivalent to', and the notation $\pmod{12}$ tells us that we should reset when we get to the number 12, or if you like that our day is split into 12 hours.

'Clock subtraction' works in much the same way. If you subtract 6 hours from 1 o'clock, then you get 7 o'clock. The way that we will write this is:

$$1 - 6 \equiv 7 \pmod{12}.$$

'Clock multiplication' can be thought of just as repeated addition, so can as be defined in a natural way. For example,

$$5 \times 3 = 5 + 5 + 5 \equiv 3 \pmod{12}.$$

Division is a little more complicated, so we will return to that later.

A natural question that arises when studying clock arithmetic is: what if the day was not split into sets of 12 hours, but some other number, like 7? We can of course set up addition, subtraction, and multiplication $\pmod 7$ in just the same way as $\pmod{12}$. Formally, we define the notation $\equiv$ and $\pmod n$ as follows.

Let $n \in \mathbb{Z}_{>1}$ and let $a, b \in \mathbb{Z}$. We say that

$$a \equiv b \pmod n$$

if there exists $k \in \mathbb{Z}$ such that $a = b + kn$.

We refer to basic arithmetic $\pmod{n}$ as *modular arithmetic*. Suppose now that we want to compute $10 \times 11 \pmod{12}$. We would like to find $a \in \mathbb{Z}$ such that $1 \leq a \leq 12$ and $10 \times 11 \equiv a \pmod{12}$. One way to do this is to first compute $10 \times 11 = 110$, and then divide 110 by 12 and take a to be the remainder. Try to prove for yourself that this will give the right answer.

Finally, let us turn to division. Suppose that you want to divide 3 by 4 on our 7-hour clock. It turns out that the best way to think of this is as 3×4^{-1}– we already have a notion of multiplication (and of 3), so it remains to understand the notion of inverses[1]: Let $a \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>1}$. If there exists $b \in \mathbb{Z}$ such that

$$ab \equiv 1 \pmod{n}$$

then we say that $b \pmod{n}$ is the *inverse* of $a \pmod{n}$.

Notice the 'if there exists' part of this definition. Consider $a = n = 12$. No matter how many multiples of 12 you take, you are always going to land back at the 12 o'clock position on the clock, or more formally, for every $b \in \mathbb{Z}$ we have that $12b \equiv 12 \pmod{12}$, so in particular 12 has no inverse mod 12. In fact, since $12 \equiv 0 \pmod{12}$, this isn't so surprising, since we are used to the idea of 0 having no inverse. There are however other numbers by which we cannot divide $\pmod{12}$. Consider $a = 6$ and $n = 12$. For every $b \in \mathbb{Z}$ we have that either $6b \equiv 6 \pmod{12}$ or $6b \equiv 0 \pmod{12}$. So $6 \pmod{12}$ also has no inverse. When does an integer mod n have an inverse?

To understand when the inverse exists, we first need to understand in which situations the inverse of $a \pmod{b}$ exist for any a and b. Let's look at a couple of examples.

Examples

- The inverse of $4 \pmod{7}$ is $2 \pmod{7}$ because $4 \cdot 2 \pmod{7} \equiv 1 \pmod{7}$.
- $4 \pmod{8}$ has no inverse because for every $n \in \mathbb{Z}$ we know that

  $$4 \cdot n \pmod{8} \in \{0 \pmod{8}, 4 \pmod{8}\},$$

  so in particular there does not exist any $n \pmod{8}$ such that $4 \cdot n \equiv 1 \pmod{8}$.

[1] Technically we are introducing *multiplicative* inverses here (analogous to the additive inverse that we saw in Worksheet 1). As multiplicative inverses are clearly more interesting that additive inverses, we tend to drop the adjective.

- Exercise: generalise the above example. That is, show that if m and n are not coprime then m does not have an inverse mod n.

Summary

Complex numbers have the form $z = x + iy$; the conjugate is

$$z^* = x - iy \tag{27}$$

while the absolute value is

$$|z| = \sqrt{zz^*} = \sqrt{x^2 + y^2} \tag{28}$$

To divide two complex numbers you multiple above and below by the conjugate of the denominator, this will get rid of the is below the bar:

$$\frac{z_1}{z_2} = \frac{z_1}{z_2}\frac{z_2^*}{z_2^*} = \frac{z_1 z_2^*}{|z_2|^2} \tag{29}$$

You can rewrite a complex number in polar form

$$z = re^{i\theta} \tag{30}$$

using the Euler formula

$$e^{i\theta} = \cos\theta + i\sin\theta \tag{31}$$

This is particularly useful when calculating powers of complex numbers. When taking roots of complex numbers, remember there are n n-roots of unity.