Math/CS 120: Intro. to Math | Professor: Padraic Bartlett

Lecture 10: Complex Numbers

Week 10 | *UCSB 2014*

> The shortest route between two truths in the real domain passes through the complex domain.
>
> Jacques Hadamard, mathematician

1 Complex Numbers

1.1 Introduction; basic definitions.

In mathematics classes, we often run into the following question: "Given some polynomial $P(x)$, what are its roots?" Depending on the polynomial, we had several techniques for finding these roots (Rolle's theorem, quadratic/cubic formulas, factorization;) however, we at times would encounter polynomials that have no roots at all, like

$$x^2 + 1.$$

Yet, despite the observation that this polynomial's graph never crossed the x-axis, we *could* use the quadratic formula to find that this polynomial had the "formal" roots

$$\frac{-0 \pm \sqrt{-4}}{2} = \pm\sqrt{-1}.$$

The number $\sqrt{-1}$, unfortunately, isn't a real number (because $x^2 \geq 0$ for any real x) — so we would usually conclude that this polynomial has no roots over $\mathbb{R}$. This is a rather frustrating block to run into; often, we like to factor polynomials entirely into their roots, and it would be quite nice if we could always do so, as opposed to having to worry about irreducible polynomials like $x^2 + 1$.

Motivated by this, we can create the **complex numbers** by just throwing $\sqrt{-1}$ into the real numbers. Formally, we define the set of complex numbers, $\mathbb{C}$, as the set of all numbers $\{a + bi : a, b \in \mathbb{R}\}$, where $i = \sqrt{-1}$.

On a previous homework, we did this in a somewhat more formal fashion:

Problem. Consider the collection of all polynomials with real-valued coefficients, which we denote as $\mathbb{R}[x]$. Take any polynomial $h(x) \in \mathbb{R}[x]$, and define the following relation:

$$\equiv_h := \{(f(x), g(x)) \mid \exists q(x) \in \mathbb{R}[x], f(x) - g(x) = q(x)h(x)\}.$$

For example, if $h(x) = x - 2$, we would say that $f(x) = x^2 - 4$ is equivalent to $g(x) = x^2 - 3x + 2$, because

$$f(x) - g(x) = x^2 - 4 - (x^2 - 3x + 2) = 3x - 6 = 3(x - 2) = 3h(x).$$

1. Prove that $\equiv_h$ is an equivalence relation on the collection of all polynomials.

2. Denote any equivalence class containing a polynomial $f(x)$ as $[f(x)]_h$: this represents the collection of all of the polynomials equivalent to $f(x)$ under $\equiv_h$. We can define $+, \cdot$ on these equivalence classes as follows: $[f(x)]_h + [g(x)]_h = [f(x) + g(x)]_h$, and $[f(x)]_h \cdot [g(x)]_h = [f(x) \cdot g(x)]_h$.

   Set $h(x) = x^2 + 1$ for this problem, and let $(\mathbb{R}[x]/h(x))$ denote the collection of equivalence classes for $\mathbb{R}[x]$ under h.

   Show that $[x]_h \cdot [x]_h + [1]_h = [0]_h$.

3. Keep $h(x) = x^2 + 1$, and consider the map $\varphi : \mathbb{C} \to (\mathbb{R}[x]/h(x))$ defined by $h(a + ib) = [a + bx]_h$. Is φ a bijection? Does φ preserve addition and multiplication: in other words, for any $a, b, c, d \in \mathbb{R}$, do we have

   - $h((a + ib) + (c + id)) = [a + bx]_h + [c + dx]_h$, and
   - $h((a + ib) \cdot (c + id)) = [a + bx]_h \cdot [c + dx]_h$?

Solution.
1. This is straightforward. We simply take any polynomial $h(x)$, and verify that $\equiv_h$ is indeed an equivalence relation by checking for reflexivity, symmetry and transitivity.

Reflexivity: For any $f(x)$, we want $f(x) \equiv_h f(x)$ to hold. But this is equivalent to asking that for any $f(x)$, $f(x) - f(x) = 0$ is a multiple of $h(x)$, which is true!

Symmetry: We want to show that if $f(x) \equiv_h g(x)$, then $g(x) \equiv_h f(x)$. But this is easy to check: if $f(x) \equiv_h g(x)$, then we can write $f(x) - g(x)$ as some multiple $q(x)h(x)$ of $h(x)$. But this means that $g(x) - f(x) = -q(x)h(x)$ is also a multiple of $h(x)$: in other words, that $g(x) \equiv_h f(x)$.

Transitivity: Suppose that $f(x) \equiv g(x)$ and $g(x) \equiv_h j(x)$. We want to show that $f(x) \equiv_h j(x)$. This is similar to the above. Notice that by definition, there must be two polynomials $q(x), r(x)$ such that $f(x) - g(x) = q(x)h(x)$ and $g(x) - j(x) = r(x)h(x)$. Consequently, we have $f(x) - g(x) + g(x) - j(x) = f(x) - j(x) = (q(x) + r(x))h(x)$. In other words, $f(x) - j(x)$ is a multiple of $h(x)$: so we have $f(x) \equiv_h j(x)$, as desired!

2. This is an easy check. By our definitions above, we have

$$[x]_h \cdot [x]_h + [1]_h = [x^2]_h + [1]_h = [x^2 + 1]_h.$$

But $x^2 + 1 \equiv_{x^2+1} 0$, because it clearly differs from 0 by a multiple of $x^2 + 1$; so we actually have

$$[x]_h \cdot [x]_h + [1]_h = [x^2]_h + [1]_h = [x^2 + 1]_h = [0]_h,$$

as claimed.

3. We first check bijectivity. First, notice that for any two linear polynomials $ax + b, cx + d$, we have that

$$(ax + b \equiv_{x^2+1} cx + d) \Rightarrow (a - c)x + (b - d) \text{ is a multiple of } x^2 + 1.$$

But any non-zero multiple of x^2+1 has a term of degree 2 or higher! Therefore, the only way this can hold is if $(a-c)x+(b-d)=0$; in other words, if $ax+b=cx+d$. Therefore no two linear polynomials are in the same equivalence class mod h!

Conversely, take any degree-n polynomial $p(x)=a_0+a_1x+\ldots a_nx^n$. I claim that this polynomial is equivalent to some linear polynomial under the $\equiv_{x^2+1}$ relation, and justify this with induction on the degree of $p(x)$. Note that our claim is clearly true for degree 0 and 1 polynomials, which gives us a base case.

Inductively, then, assume our claim is true for degree $n-1$ polynomials; we seek to show it holds for degree-n polynomials. To see this, simply note that for any degree-n $p(x)=a_0+a_1x+\ldots a_nx^n$, we have

$$a_0+a_1x+\ldots a_nx^n \equiv_{x^2+1} a_0+a_1x+\ldots a_nx^n - a_nx^{n-2}\big(x^2+1\big)$$

because their difference is $a_nx^{n-2}(x^2+1)$, a multiple of x^2+1. But the right-hand-side is just

$$a_0+a_1x+\ldots (a_{n-2}-a_n)x^{n-2}+a_{n-1}x^{n-1},$$

a degree-$n-1$ polynomial, which we know by induction is equivalent to some linear polynomial.

Therefore, we have shown the following:

- Any polynomial is equivalent to some linear polynomial.
- No two linear polynomials are equivalent.

Consequently, we can uniquely label each of our equivalence classes with the unique linear polynomial that is in this class! In other words, we have formed a bijection from our equivalence classes to the collection of all linear polynomials $\{(a+bx) \mid a,b\in\mathbb{R}\}$.

From here, it is easy to see that our map $\varphi:\mathbb{C}\to(\mathbb{R}/\equiv_h)$ is a bijection. It hits each linear polynomial exactly once, as for any $a+bx$ there is exactly one $a+bi\in\mathbb{C}$; so, by our earlier observations, it hits each equivalence class exactly once!

Furthermore, we claim that this map is an isomorphism: in other words, that

- $\varphi((a+ib)+(c+id))=[a+bx]_h+[c+id]_h$, and
- $\varphi((a+ib)\cdot(c+id))=[a+bx]_h\cdot[c+id]_h$.

The first is immediate: $\varphi((a+c)+i(b+d))$ is just $[(a+c)+(b+d)x]_h$, while $[a+bx]_h+[c+id]_h=[(a+b)+(c+d)x]_h$, by our earlier definitions.

Similarly, $\varphi((a+ib)\cdot(c+id))=\varphi((ac-bd)+i(bc+ad))=[(ac-bd)+(bc+ad)x]_h$, while

$$[a+bx]_h+[c+id]_h=[ac+(bc+ad)x+bdx^2]_h.$$

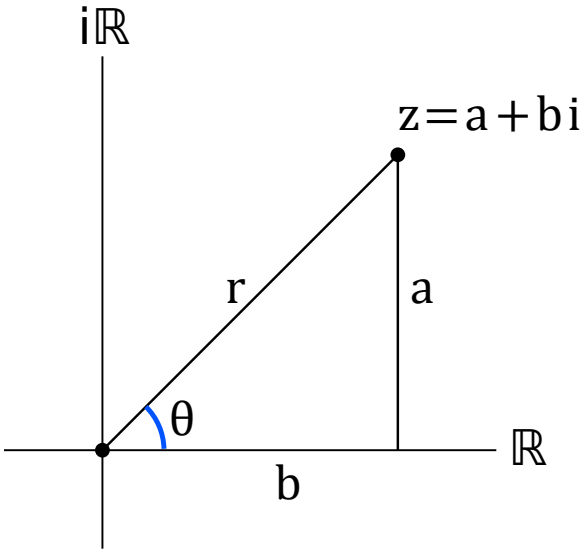
Because $x^2\equiv_h -1$ (this follows because x^2+1 is, um, a multiple of x^2+1), we can replace the x^2 with a -1 above to get that

$$[a+bx]_h+[c+id]_h=[ac+(bc+ad)x+bdx^2]_h=[ac-bd+(bc+ad)x]_h.$$

So our operation is an isomorphism!

In fact, the punchline of this exercise is that if you wanted, you could take $\mathbb{R}[x]/\equiv_{x^2+1})$ as your **definition** for the complex numbers, and that in a very real sense this is what we mean by i in the complex numbers — it's not just that we've randomly decided to throw in $\sqrt{-1}$ into the reals, but rather that we've decided to look at equivalence classes of polynomials, and x^2+1 is a irreducible polynomial (and thus, by our work with field extensions earlier, yields a field!)

Graphically, we can visualize the complex numbers as a plane, where we identify one axis with the real line $\mathbb{R}$, the other axis with the imaginary-real line $i\mathbb{R}$, and map the point $a+bi$ to (a,b):



One natural question to ask, when introducing a new object, is **what sorts of properties does it satisfy?** We answer this in the following theorem:

Theorem. $\mathbb{C}$, as defined above, is a field.

Proof. In our definition above, we defined the operations $+,\cdot$ for any two $a+ib, c+id \in \mathbb{C}$ as follows:

$$(a+bi)+(c+di) = (a+c)+(b+d)i,$$
$$(a+bi)\cdot(c+di) = (ac-bd)+(bc+ad)i.$$

It is not hard to see that $\langle \mathbb{C}, + \rangle$ forms an abelian group with respect to this operation:

1. **Identity**: $0 = 0+0i$ is clearly the identity, as $(a+bi)+(0+0i) = (a+0)+(b+0)i = a+bi$. Notice how in this sense identity was "inherited" from $\mathbb{R}$, as we used the fact that $0+x=0$ for any real x to conclude that $0+0i$ was our identity. Almost all of our properties here will follow in the same way!

2. **Inverses**: For any $a+bi$, we know that $-a, -b \in \mathbb{R}$ and therefore that $(-a)+(-b)i \in \mathbb{C}$; moreover, we can see that $(a+bi)+((-a)+(-b)i) = (a+(-a))+(b+(-b))i = 0+0i =$ the identity. Consequently every element has an inverse!

3. **Associativity**: Inherited from $\mathbb{R}$, in the same way that this has happened throughout this class! To be formal: suppose that you take any three $a+bi, c+di, e+fi \in \mathbb{C}$; then by definition

   $$(a+bi)+((c+di)+(e+fi)) = (a+(c+e))+(b+(d+f))i, \text{ and} ((a+bi)+(c+di))+(e+fi) \quad = (($$

   The two RHS above are equal because the real numbers are associative; therefore, we have established associativity.

4. **Commutativity**: Inherited from $\mathbb{R}$, in the same way as above.

It is not much harder to see that $\langle \mathbb{C}^\times, \cdot \rangle$, the complex numbers without $0+0i$ under the multiplication operation also forms an abelian group, and that the operations $+, \cdot$ satisfy the distributive property. Indeed, the identity $1+0i$, associativity, commutativity, and distributivity properties will all fall out from $\mathbb{R}$ being a field in the same way that they did above. The only interesting property to check, then, is whether or not we have multiplicative inverses.

To start finding an inverse, notice that for any $a+bi$ we can at the least simplify it by multiplying it by its **conjugate** $a-bi$; this idea lets us write

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

Consequently, if $a+bi \neq 0+0i$, at least one of $a, b \neq 0$, and therefore we have $a^2+b^2 > 0$; this lets us claim that $\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i \in \mathbb{C}$, and moreover that

$$(a+bi)\left(\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i\right) = \frac{a^2+b^2}{a^2+b^2} = 1.$$

So we have inverses for all of our nonzero elements, and are thus a field! □

As you may have noticed in the above proof, two useful concepts when working in the complex plane are the ideas of **norm** and **conjugate**:

Definition. If $z = x+iy$ is a complex number, then we define $|z|$, the **norm** of z, to be the distance from z to the origin in our graphical representation; i.e. $|z| = \sqrt{x^2+y^2}$.

As well, we define the **conjugate** of $z = x+iy$ to be the complex number $\overline{z} = x-iy$. Notice that $|z| = \sqrt{x^2+y^2} = \sqrt{z\overline{z}}$.

In the real line, recall that we had $|x \cdot y| = |x| \cdot |y|$; this still holds in the complex plane! In particular, we have $|w \cdot z| = |w| \cdot |z|$, for any pair of complex numbers w, z. (If you don't believe this, prove it! – it's not a difficult exercise to check.)

So: we have this set, $\mathbb{C}$, that looks like the real numbers with i thrown in. Do we have any way of extending any of the functions we know and like on $\mathbb{R}$, like $\sin(x), \cos(x), e^x$ to the complex plane?

At first glance, it doesn't seem likely: i.e. what should we say $\sin(i)$ is? Is cos a periodic function when we add multiples of $2\pi i$ to its input? Initially, these questions seem unanswerable; so (as mathematicians often do when faced with difficult questions) let's try something easier instead!

In other words, let's look at **polynomials**. These functions are much easier to extend to $\mathbb{C}$: i.e. if we have a polynomial on the real line

$$f(x) = 2x^3 - 3x + 1,$$

the natural way to extend this to the complex line is just to replace the x's with z's: i.e.

$$f(z) = 2z^3 - 3z + 1.$$

This gives you a well-defined function on the complex numbers (i.e. you put a complex number in and you get a complex number out,) such that if you restrict your inputs to the real line $x + i \cdot 0$ in the complex numbers, you get the same outputs as the real-valued polynomial.

In other words, we know how to work with polynomials. Does this help us work with more general functions?

The answer (if you remember calculus) is yes! More specifically, the answer here is to use **power series**. Specifically, in your AP Calculus classes, you've likely shown that

$$\begin{aligned}
\sin(x) &= x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \frac{x^9}{9!} - \dots, \\
\cos(x) &= 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \frac{x^8}{8!} - \dots, \text{and} \\
e^x &= 1 + x + \frac{x^2}{2} + \frac{x^3}{3!} + \frac{x^4}{4!} + \frac{x^5}{5!} + \dots
\end{aligned}$$

for all real values of x. Therefore, we can choose to **define**

$$\begin{aligned}
\sin(z) &= z - \frac{z^3}{3!} + \frac{z^5}{5!} - \frac{z^7}{7!} + \frac{z^9}{9!} - \dots, \\
\cos(z) &= 1 - \frac{z^2}{2!} + \frac{z^4}{4!} - \frac{z^6}{6!} + \frac{z^8}{8!} - \dots, \text{and} \\
e^z &= 1 + z + \frac{z^2}{2} + \frac{z^3}{3!} + \frac{z^4}{4!} + \frac{z^5}{5!} + \dots,
\end{aligned}$$

for all $z \in \mathbb{C}$. This extension has the same properties as the one we chose for polynomials: it gives a nice, consistent definition of each of these functions over all of $\mathbb{C}$, that agrees with the definitions they already had on the real line $\mathbb{R}$.

The only issue with these extensions is that we're still not entirely quite sure what they mean. I.e.: what **is** $\sin(i)$, apart from some strange infinite power series? Where does the point e^z lie on the complex plane?

To answer these questions, let's look at e^z first, as it's arguably the easiest of the three (its terms don't do the strange alternating-thing, and behave well under most algebraic manipulations.) In particular, write $z = x + iy$: then we have

$$e^z = e^{x+iy} = e^x \cdot e^{iy},$$

where e^x is just the real-valued function we already understand. So, it suffices to understand e^{iy}, which we study here:

$$e^{iy} = 1 + iy + \frac{(iy)^2}{2} + \frac{(iy)^3}{3!} + \frac{(iy)^4}{4!} + \frac{(iy)^5}{5!} + \frac{(iy)^6}{6!} + \frac{(iy)^7}{7!} + \frac{(iy)^8}{8!} + \dots$$

If we use the fact that $i^2 = -1$, we can see that powers of i follow the form

$$i, -1, -i, 1, i, -1, -i, 1, \dots$$

and therefore that

$$e^{iy} = 1 + iy - \frac{y^2}{2} - i\frac{y^3}{3!} + \frac{y^4}{4!} + i\frac{y^5}{5!} - \frac{y^6}{6!} - i\frac{y^7}{7!} + \frac{y^8}{8!} + \dots$$

If we split this into its real and imaginary parts, we can see that

$$e^{iy} = \left(1 - \frac{y^2}{2} + \frac{y^4}{4!} - \frac{y^6}{6!} + \dots\right) + i\left(y - \frac{y^3}{3!} + \frac{y^5}{5!} \dots\right).$$

But wait! We've seen those two series before: they're just the series for $\sin(y)$ and $\cos(y)$! In other words, we've just shown that

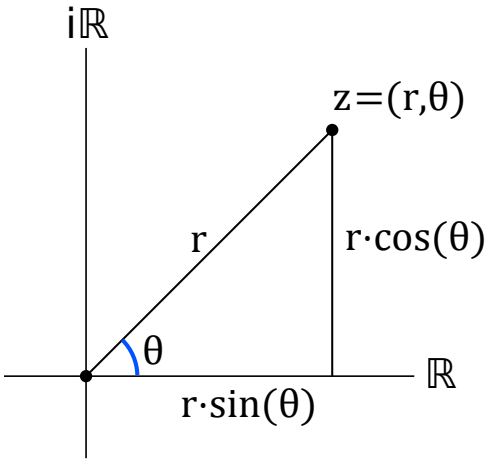
$$e^{iy} = \cos(y) + i\sin(y).$$

One famous special case of this formula is when $y = \pi$, in which case we have $e^{i\pi} = \cos(\pi) + i\sin(\pi) = -1$, or

$$e^{i\pi} + 1 = 0.$$

Which is *amazing*. In one short equation, we've discovered a fundamental relation that connects five of the most fundamental mathematical constants, in a way that – without this language of power series and complex numbers – would be unfathomable to understand. Without power series, the fact that a constant related to the area of a circle (π), the square root of negative 1, the concept of exponential growth (e) and the multiplicative identity (1) can be combined to get the additive identity (0) would just seem absurd; yet, with them, we can see that this relation was inevitable from the very definitions we started from.

This formula (Euler's formula) isn't just useful for discovering deep fundamental relations between mathematical constants: it also gives you a way to visualize the complex plane! In specific, recall the concept of **polar coördinates**, which assigned to each nonzero point z in the plane a value $r \in \mathbb{R}^+$, denoting the distance from this point to the origin, and an angle $\theta \in [0, 2\pi)$, denoting the angle made between the positive x-axis and the line connecting z to the origin:



With this definition made, notice that any point with polar coördinates (r, θ) can be written in the plane as $(r\cos(\theta), r\sin(\theta))$. This tells us that any point with polar coördinates (r, θ) in the complex plane, specifically, can be written as $r(\cos(\theta) + i\sin(\theta))$; i.e. as $re^{i\theta}$.

This gives us what we were originally looking for: a way to visually interpret e^{x+iy}! In specific, we've shown that e^{x+iy} is just the point in the complex plane with polar coördinates (e^x, y).

1.2 Gaussian integers.

When we extended $\mathbb{R}$ to $\mathbb{C}$, we saw that doing this gave us a massive amount of beautiful mathematics! Naturally, then, we might wonder what adding in i to other sets of numbers might give us. This, loosely speaking, is one possible motivation for the **Gaussian integers** $\mathbb{Z}[i]$:

Definition. The **Gaussian integers**, denoted $\mathbb{Z}[i]$, are the collection of all numbers of the form

$$a + bi,$$

where $a, b \in \mathbb{Z}$ and i denotes the "square root of -1," or more formally denotes some symbol with the property that $i^2 = -1$ and that satisfies all of the other reasonable properties (commutativity, associativity, etc) that numbers satisfy.

We can define $+, \cdot$ on this set in the same way that we do for $\mathbb{C}$: that is, we can set

$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$
$$(a + bi) \cdot (c + di) = (ac - bd) + (bc + ad)i.$$

If $a, b, c, d \in \mathbb{Z}$, then the RHS above is always an integer; consequently our operations are well-defined.

Given a new object, one natural question to ask about is "what properties does it satisfy?" We answer this here:

Theorem. The Gaussian integers $\mathbb{Z}[i]$ form a **ring**: that is, they satisfy all of the properties of being a field except for having multiplicative inverses.

Proof. Notice that because $\mathbb{C} \supseteq \mathbb{Z}[i]$, the commutativity/associativity/distributivity properties are all inherited from $\mathbb{C}$, as are the identity properties once we note that $0, 1$ are actually in $\mathbb{Z}[i]$. So the only property left is additive inverses, as we're not asking for multiplicative inverses; this is immediate, as if $a + bi \in \mathbb{Z}[i]$, then $a, b \in \mathbb{Z}$, and therefore $-a, -b \in \mathbb{Z}$ and so $(-a) + (-b)i \in \mathbb{Z}[i]$. □

It is worth noting that we very much do not have multiplicative inverses for almost all of our elements; if we take $3 + 0i = 3$ for example, we can see that for any $a + bi \in \mathbb{Z}$, we have

$$3 \cdot (a + bi) = 3a + (3b)i \neq 1,$$

because there is no integer a such that $3a = 1$.

In fact, we can go further than this:

Definition. Call a number $a + bi$ in $\mathbb{Z}[i]$ a **unit** if it has an inverse.

Theorem. The only units in $\mathbb{Z}[i]$ are ± 1 and $\pm i$.

Proof. A very useful concept to use in this proof is the concept of the "squared norm" of a Gaussian integer. Specifically: take any $a+bi \in \mathbb{Z}[i]$. Define $N(a+bi) = a^2+b^2$, i.e. define $N(a+bi)$ as the squared norm of $a+bi$.

Notice that this is a function from $\mathbb{Z}[i] \to \mathbb{N}$: that is, its outputs are always integers! Also notice that this function is multiplicative, i.e.

$$\begin{aligned} N(a+bi)N(c+di) &= (a^2+b^2)(c^2+d^2) \\ &= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 \\ &= a^2c^2 + b^2d^2 - 2abcd + a^2d^2 + b^2c^2 + 2abcd \\ &= N((ac-bd)+(bc+ad)i) \\ &= N((a+bi)(c+di)). \end{aligned}$$

We can use this to prove that the only possible units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$ as follows: take any Gaussian integer $a+bi$ that has an Gaussian integer inverse $c+di$. Then, we have

$$\begin{aligned} 1 &= (a+bi)(c+di) \\ \Rightarrow N(1) = 1 &= N(a+bi)N(c+di) = (a^2+b^2)(c^2+d^2). \end{aligned}$$

The only two natural numbers whose product yields 1 are $(1,1)$; consequently we have

$$(a^2+b^2) = 1, (c^2+d^2) = 1.$$

Because $a,b,c,d \in \mathbb{Z}$, this forces one of $a,b = \pm 1$ and the other to equal 0; in other words, we have $a+bi = \pm 1$ or $\pm i$. So these are the only possible units; noting that $1^2 = 1, -1^2 = 1$ and $i(-i) = (-i)i = 1$ tells us that these elements are indeed units, as claimed. □

The fact we proved about the squared norm above is so useful, we state it as its own proposition:

Proposition. For any $a+bi, c+di$, we have $N(a+bi)N(c+di) = N((a+bi)(c+di))$.

1.3 Gaussian Primes

Given that the Gaussian integers have the word "integers" in their name, we might naturally wonder if they have some of the other same properties that integers have. Namely, integers have a notion of "primes:" that is, numbers that only have themselves and one as a factor!

Kind-of. You see, the above definition, while seemingly correct, isn't actually what you want for $\mathbb{Z}$: on one hand, we definitely want 7 to be a prime, and yet on the other hand we can write $7 = (-1)\cdot(-7)$, neither of which are 1 or 7!

The issue with the above factorization is that we were in a sense able to "sneak" a -1 into both of our terms, because $-1 \cdot -1 = 1$ and therefore in the product it canceled out! So, when we define our notion of prime, we want it to "ignore" such cancellable terms. We do this formally via our earlier-defined notion of "units" here:

Definition. We call an element $a + bi \in \mathbb{Z}[i]$ **prime** if the following two conditions hold:

- $a + bi$ is not a unit. (This is the "1 is not a prime" rule.)
- If we can write $a + bi = z \cdot \omega$ for two $z, \omega \in \mathbb{Z}[i]$, then one of z, ω must be a unit.

We give a few examples of primes here:

Example. The numbers 3, 7 are prime.

Proof. We prove this using our "squared-norm" function. We first note that neither $3, 7$ are units, which satisfies the first of our desired properties. To see the second, notice that if we can find $a + bi, c + di \in \mathbb{Z}[i]$ such that

$$3 = (a + bi)(c + di),$$

then applying N to both sides gives us

$$\begin{aligned} N(3) &= N(a + bi)N(c + di) \\ \Rightarrow 9 &= (a^2 + b^2)(c^2 + d^2). \end{aligned}$$

(Note that because $3 = 3 + 0i$, its norm is $3^2 + 0^2$. It is a common mistake to forget to square numbers when using N!)

If neither $a + bi, c + di$ are units, then both $a^2 + b^2, c^2 + d^2$ are not equal to 1, as proven earlier. Consequently, because they are both natural numbers whose product is 9, each of them must be equal to 3; but this is impossible, as there are no two integers a, b such that $a^2 + b^2 = 3$. (This is easy to check; if either $a, b \geq 2$ then $a^2 + b^2 \geq 4$, and for the remaining few cases checking by hand verifies that this is impossible.) So at least one of $a + bi, c + di$ is a unit, which finishes our proof that 3 is a prime.

We use similar logic to show that 7 is a prime: if we can find $a + bi, c + di \in \mathbb{Z}[i]$ such that

$$7 = (a + bi)(c + di),$$

then applying N to both sides gives us

$$\begin{aligned} N(7) &= N(a + bi)N(c + di) \\ \Rightarrow 49 &= (a^2 + b^2)(c^2 + d^2). \end{aligned}$$

Again, if neither $a + bi, c + di$ are units, then both $a^2 + b^2, c^2 + d^2$ are not equal to 1; because their product is 49 and they are natural numbers, we can conclude that both $a^2 + b^2, c^2 + d^2$ are equal to 7. This too is impossible: there are no two integers a, b such that $a^2 + b^2 = 7$, which we can verify easily (if $a, b \geq 3$ then $a^2 + b^2 \geq 9$, and the remaining cases can be eliminated by casework.) So 7 is a prime! □

Perhaps more interestingly, there are several numbers that are prime in $\mathbb{Z}$ that are **not** prime in $\mathbb{Z}[i]$:

Theorem. Neither 2 nor 5 are primes in $\mathbb{Z}[i]$.

Proof. Simply notice that

$$2 = (1+i)(1-i), 5 = (1+2i)(1-2i)$$

to see that both numbers are not prime. □

However, you can easily verify that these two numbers have been decomposed above into primes: by mimicking our proofs that 3, 7 are prime, you can easily show that $(1+i), (1+2i)$ are both prime.

This raises our next question: in the integers, we know that any number can be uniquely decomposed into primes, up to multiplication by units (i.e. $21 = 3 \cdot 7 = (-3) \cdot (-7)$.) Does this happen for the Gaussian integers?

The answer is yes! Proving this is the focus of the rest of this section.

The first tool we need in this process is a way to factor Gaussian integers. We have tools for doing this in $\mathbb{Z}$, namely the Euclidean algorithm: does this carry over here?

The answer turns out to be yes! To state and prove this, it is useful to have the following lemma:

Lemma. Suppose that α, β are a pair of nonzero Gaussian integers, with $N(\alpha) \geq N(\beta)$. Then we can find Gaussian integers q, r, thought of as the "quotient" and "remainder" of $\frac{\alpha}{\beta}$, such that $\alpha = q \cdot \beta + r$, where $N(\beta) > N(r)$.

Proof. To do this, look at the fraction $\frac{\alpha}{\beta}$. Because $\beta \neq 0$, this is a well-defined number in $\mathbb{C}$: denote it as some $x + iy$ for $x, y \in \mathbb{R}$.

We want, in some sense, to capture the idea of "remainder" and "quotient" for this fraction $\frac{\alpha}{\beta}$. To do this, note that in a sense we want to set the "quotient" part of this fraction to be the closest Gaussian integer to $x + iy$; that is, we want to define

$$q = [x] + i[y],$$

where $[x], [y]$ denote the results of rounding x, y to the nearest integer.

After doing this, if we set

$$r = \alpha - q\beta,$$

we clearly have that $\alpha = q \cdot \beta + r$. So it suffices to demonstrate that r is in fact a "remainder," in that it should be smaller than β in size.

This is not hard to see. Notice that because $q = [x] + i[y]$, we can write

$$\frac{\alpha}{\beta} = x + iy = q + (X + iY),$$

if we set $X = x - [x]$ and $Y = y - [y]$. Notice that $|X|, |Y| \leq \frac{1}{2}$, because we obtained $[x], [y]$ by rounding x, y to the nearest integers.

This means that we can write

$$q = \frac{\alpha}{\beta} - (X + iY),$$

and therefore have

$$r = \alpha - q\beta = \alpha - \beta(\frac{\alpha}{\beta} - (X + iY)) = \beta(X + iY).$$

As a consequence, we have that

$$N(r) = N(\beta)N(X + iY) = N(\beta) \cdot (X^2 + Y^2) \leq N(\beta) \cdot \left(\frac{1}{4} + \frac{1}{4}\right) = \frac{N(\beta)}{2} < N(\beta),$$

and have thus finished our proof! □

We use this lemma in our statement and proof of the Euclidean algorithm:

Algorithm. (The Euclidean Algorithm for $\mathbb{Z}[i]$.) Take any two nonzero Gaussian integers $\alpha = a + bi, \beta = c + di \in \mathbb{Z}[i]$. The following process will create the greatest common divisor (i.e. gcd) of these two numbers: i.e. it will output a Gaussian integer $\gamma = x + yi$ such that

- γ is a **divisor** of both α and β; that is, we can find Gaussian integers $e + fi, g + hi$ such that $\alpha = (x + yi)(e + fi)$, $\beta = (x + yi)(g + hi)$.
- γ is the "greatest" such common divisor; that is, for any other Gaussian integer δ that is a divisor of α and β, then δ must also be a divisor of $x + yi$ as well.

To start our process, assume that $N(\alpha) \geq N(\beta)$ without any loss of generality. Initialize $r_1 = \alpha$ and $r_2 = \beta$, and begin the following process, starting at $k = 1$:

1. If $r_{k+1} = 0$, halt our process, and output r_k.
2. Otherwise, use the lemma above to find q, r_{k+2} such that $r_k = qr_{k+1} + r_{k+2}$, with $N(r_{k+1}) > N(r_{k+2})$.
3. Increase k by 1 and return to step 1.

Theorem. The Euclidean algorithm for Gaussian integers, as described above, works.

Proof. Input any two nonzero Gaussian integers $\alpha, \beta \in \mathbb{Z}[i]$ into the above algorithm, and let r_k denote the resulting output.

We need to prove that r_k is both a divisor of α, β, and moreover that it is the greatest such divisor. We prove these claims by a series of inductive proofs:

Claim. r_k divides r_j, for any j.

Proof. By induction on r_{k-i}. For $i = 0$, this claim is trivial, as any number is a multiple of itself. For $i = 1$, we use the fact that because our process halted at r_k, we have

$$r_{k-1} = qr_k,$$

and thus that r_{k-1} is also a multiple of r_k.

Assume that we have have proven our claim for all $i \in \{0, \ldots n\}$; we seek to extend our claim to $i = n + 1$ as well. To do this, notice that by definition

$$r_{k-(n+1)} = r_{k-(n-1)} + qr_{k-n}$$

By induction, we know that the RHS is the sum of two multiples of r_k; consequently the LHS is a multiple of r_k as well, and we have finished our inductive claim. □

If we consider the special cases $j = 1, 2$ in the above proof, we have proven that r_k is a divisor of both $r_1 = \alpha$ and $r_2 = \beta$.

We now want to show that r_k is the greatest such divisor. We again do this by proving a related claim by induction:

Claim. For any $j \in \{1, \dots k\}$, we can write r_j as $A\alpha + B\beta$, for two Gaussian integers A, B.

Proof. By induction on r_i. For $i = 0, 1$, this claim is trivial, as $r_1 = \alpha, r_2 = \beta$.

Assume that we have have proven our claim for all $i \in \{0, \dots n\}$; we seek to extend our claim to $i = n + 1$ as well. To do this, notice that by definition

$$r_{n+1} = r_{n-1} - qr_n.$$

By induction, we know that the RHS has the form

$$A_{n-1}\alpha + B_{n-1}\beta - qA_n\alpha - qB_n\beta = (A_{n-1} - qA_n)\alpha + (B_{n-1} - qB_n)\beta,$$

and therefore our claim holds for r_{n+1} as well. □

As a consequence, we can see that for any divisor $\delta \in \mathbb{Z}[i]$ of both α, β, if we write

$$r_k = A_k\alpha + B_k\beta,$$

we can see that δ must also be a divisor of r_k. This finishes our claim that r_k is the greatest common divisor. □

We use the Euclidean algorithm to prove the following observation about primes, called Euclid's lemma:

Lemma 1. *(Euclid's lemma.) Suppose that p is a prime in $\mathbb{Z}[i]$ and that p divides some product $\alpha\beta$ of two Gaussian integers α, β. Then p must divide at least one of α or β.*

Proof. There are two cases to consider. If p divides α, we are done! Otherwise, p does not divide α. This means that the GCD of p, α cannot be anything other than a unit, as the GCD of p and any other number is a divisor of p, and if it's not p then it must be a unit, as p is prime.

By our proof above, this means that we can find Gaussian integers A, P such that

$$A\alpha + Pp = \text{some unit}.$$

Scaling both sides by the inverse of this unit gives us

$$A'\alpha + P'p = 1,$$

for some $A', P' \in \mathbb{Z}[i]$.

Multiplying both sides by β gives us

$$A'\alpha\beta + P'p\beta = \beta.$$

Both $\alpha\beta$ and p are multiples of p; therefore the LHS is a multiple of p, which forces the RHS to also be a multiple of p! In particular, this tells us that p divides β, as claimed. □

With this result, unique factorization is immediate:

Theorem. Take any Gaussian integer α. We can factor α into primes; furthermore, this factorization is unique up to the order of such primes and scaling by units.

Proof. To see that α can be factored into primes is not hard. Take α: either it is prime and we are already done, or it is not prime and we can factor it into $\beta \cdot \gamma$, where $N(\beta), N(\gamma) > 1$. As a consequence, note that because $N(\alpha) = N(\beta)N(\gamma)$, we must have $N(\alpha) > N(\beta), N(\gamma)$; i.e. the norms of these numbers have strictly decreased.

Repeat this factorization process on β, γ, and on any resulting factors of β, γ, and so on; because the norms of these numbers are positive integers and they decrease at each step, this process can only continue for at most $N(\alpha)$-many steps, and so must halt. When it does halt, we have decomposed our α into primes, as claimed.

The second part of this proof involves showing that any two such decompositions into primes are equivalent, up to the order and/or scaling by units. To see this, suppose that

$$\alpha = p_1 \cdot \ldots p_n = q_1 \cdot \ldots q_m,$$

for two collections $p_1, \ldots p_n$, $q_1, \ldots q_m$ of primes.

Take any p_i in the first collection. We know by assumption that p_i divides $q_1 \cdot \ldots q_m$; therefore, by repeated application of Euclid's lemma, we know that p_i divides some q_j. Because p_i is a prime, we know that it is not a unit; therefore, because it is a non-unit divisor of q_j, we know that it **is** q_j, up to scaling by a unit. In other words, we have $p_i = q_j \cdot$ (a unit). Cancel out p_i, q_j from both sides.

Repeat this process until we run out of either p_i's or q_j's. If we ran out of both sides simultaneously, we've proven our claim; up to the units and order, the p_i factorization was the same as the q_j factorization! Otherwise, we ran out of one side first; say that we are out of p_i's without loss of generality.

But this means that some product of units (which is itself a unit) is equal to some nontrivial product of primes. In particular, this means that the norm of a unit — namely, 1 — is equal to the norm of a product of primes, which is decidedly not 1. This is therefore impossible, so we must have ran out of our p_i, q_j's simultaneously; in other words, we've proven that we have unique factorizations into primes! □

This is really cool in of itself; we've made a new and stranger set of integers, that on one hand have many of the same concepts (Primes! Factorizations!) that the normal integers had, but that also had some strange quirks as well (2 is no longer a prime!)

However, if you're not sold on the beauty of $\mathbb{Z}[i]$, perhaps an appeal to utility may work! Here's a theorem that is almost trivial with $\mathbb{Z}[i]$, and ridiculously difficult without it:

Theorem. Suppose that p is a prime in $\mathbb{Z}$ (where we're using the $\mathbb{Z}$-definition of prime), and that p can be written in the form $a^2 + b^2$ for two integers a, b. For example, 5 is such a prime, as we can write $5 = 1^2 + 2^2$, while 7 is not, as we cannot write 7 as the sum of two squares.

Then there is only one way to write p as such a sum of squares, up to the ordering and sign of a, b.

Proof. Take p, and think of it as an element of $\mathbb{Z}[i]$. Notice that because $p = a^2 + b^2$, we can write

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

Also notice that the norm of $a \pm bi$ is p; therefore, if we write $a \pm bi$ as the product of any two other Gaussian integers α, β, we must have $N(\alpha)N(\beta) = p$, and therefore that one of $\alpha, \beta = 1$ because p is a prime in $\mathbb{Z}$. Consequently, the two numbers $a \pm bi$ are primes in $\mathbb{Z}[i]$.

Take any other two integers c, d such that $p = c^2 + d^2$; by the same logic, we have that $p = (c + di)(c - di)$, where the two numbers $c \pm di$ are primes in $\mathbb{Z}[i]$.

Because we have unique factorization, we know that these two factorizations are equivalent; that is, we have

$$(a \pm bi) = (\text{unit}) \cdot (c \pm di)$$

for some appropriate units and choice of signs. But if our unit is ± 1, this tells us that $a = \pm c, b = \pm d$, and if our unit is $\pm i$, this tells us that $a = \pm d, b = \pm c$. In other words, the pair c, d is the same as our pair a, b, up to the sign and order! This proves our claim. $\square$

Gorgeous!