

# Prime Numbers Aren't

*Math 3*

Today, in “lies you’ve been told all your lives:” *not all prime numbers are prime!!!* Your teachers told you 5 was prime. It’s not:

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

We can’t factor 5 using integers—but using complex numbers, we can!!!

$$\begin{aligned}(2 + i)(2 - i) &= 2^2 + 2i - 2i - i^2 \\&= 4 - (-1) \\&= 4 + 1 \\&= 5\end{aligned}$$

Are the prime numbers no longer prime? Can we all of a sudden factor every prime number using complex numbers? Now that we’ve gone so deep into our imagination, *is anything real anymore?!?*

What about non-real complex numbers? Are any of *them* prime? Or can we just keep factoring them into smaller and smaller factors? For example, here’s an non-real complex number:

$$3 + 93i$$

This isn’t prime, since we can factor out a 3:

$$3 + 93i = (3) \cdot (1 + 31i)$$

Can we factor it yet further? We know that 3 is prime as an integer, but can we factor it further in the complex numbers? What about  $1+31i$ ? Can we factor that any further, or is it prime? We can’t factor out from it any normal integers, since 1 and 31 have no factors in common (1 doesn’t really count). Can we perhaps factor it into complex integers?

We can!

$$1 + 31i = (3 + 2i)(5 + 7i)$$

Without explaining how we would *come up* with this factorization, we can check that it works:

$$\begin{aligned}(3 + 2i)(5 + 7i) &= 3 \cdot 5 + 3 \cdot 7i + 5 \cdot 2i + (2i)(7i) \\&= 15 + 21i + 10i + 14i^2 \\&= 15 + 31i - 14 \\&= (1 + 31i)\end{aligned}$$

So, I guess that  $1 + 31i$  isn’t prime! What about its factors,  $3 + 2i$  and  $5 + 7i$ ? Are they prime? Can we factor them any more? (Note that 2, 3, 5, and 7 are all prime among the integers, but that doesn’t mean that  $3 + 2i$  and  $5 + 7i$  must also be prime.)

So we have:

$$\underbrace{3 + 93i}_{\text{not prime}} = (3) \cdot (1 + 31i) = \underbrace{(3) \cdot (3 + 2i) \cdot (5 + 7i)}_{\text{are any of these prime???}}$$

Before we go totally off the deep end, let’s be a bit more clear about our definitions. When we normally talk about factoring numbers into primes, we’re talking about factoring integers. For any (positive) integer, there’s only one way to factor it into a product of prime numbers (ignoring things like negatives, extra 1s,

and ordering the factors differently). So, for example, as an integer, 5 is prime, because we can't factor it into smaller integers. 12 isn't prime (it's **composite**), because we can factor it into a bunch of primes:

$$12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$$

What about when we start talking about complex numbers? Let's define a **complex integer** as a number of the form  $a + bi$ , where  $a$  and  $b$  are both integers:

$$\text{a complex integer} = a + bi, \quad a, b \in \mathbb{Z}$$

So these are like the complex versions of integers (as opposed to the complex versions of real numbers, which is most of what we've been talking about). Most people call these the **Gaussian integers**, and while Gauss was a great guy, I think **complex integer** is a more evocative name.

So, for example, here are some complex integers:

$$5 + 2i$$

$$3 - 4i$$

$$7 \quad (\text{it's also a normal integer!})$$

$$12i \quad (\text{it's also a normal imaginary number!})$$

Every complex integer is also a normal integer:

#### VENN DIAGRAM PICTURE

Here are some complex numbers that aren't complex integers:

$$1.6 + 2.4i$$

$$8 - \pi i$$

$$11.46$$

$$-17.9i$$

Here are two overwhelming questions:

- Which complex integers are prime? Which are not prime?
- Of the numbers that are prime when considered as integers, which are still prime as complex integers?

Here are some more somewhat more specific questions:

- FACTOR SOME STUFF
  - Is every number that's prime among the integers also prime among the complex integers? Why, or why not? Can you come up with examples or counterexamples? Can you prove it?
  - Suppose we have a normal integer. If it's nonprime/composite among the integers, is it always nonprime/composite among the complex integers? Why, or why not?
  - Suppose we have a normal integer. If it's prime among the integers, is it always prime among the complex integers? Which numbers that are prime as integers are also prime as complex integers?
  - Try making a list of the normal primes (well, some of them). Which of them can you factor as complex integers? We already know that we can factor 5 in the complex integers—is it the only integer prime for which we can do that? Are there others? Do they have anything in common? Why is it, by the way, that we can factor 5 in the complex integers? What's the underlying reason?
- The powers of  $i$  repeat every four. In other words, if we want to simplify  $i^n$ , all we have to do is find the remainder of  $n$  when it's divided by 4. Think about the primes that aren't prime as complex integers—what's their remainder when divided by 4?
- Suppose we have a complex integer,  $a + bi$ , with  $a$  and  $b \in \mathbb{Z}$ . When is it prime?