Complex factoring

Jonathan Dushoff

I factored a Composite of the Day by using imaginary numbers, which I think is pretty cool.

The number was 9509, which I noticed immediately is

$$97^2 + 10^2.$$

Once I know this, I know how to factor it in the "complex plane" (that is, using numbers that have an imaginary part): $9509 = (97 + 10i) * (97 - 10i)$, where $i = \sqrt{-1}$. Numbers like $97 + 10i$ are called [http://en.wikipedia.org/wiki/Gaussian_integer Gaussian integers]. If you don't understand why $9509 = (97 + 10i) * (97 - 10i)$, but are still interested in this post, you should take a minute to figure it out.

Once I noticed that $9509 = 97^2 + 10^2$, I thought that if I could find another way to write it as the sum of two squares, this would give me an easy way to factor the Composite of the Day (which is of course an important goal). You'll see below why two decompositions allow me to find the factors.

I found $9509 = 95^2 + 22^2 = (95 + 22i) * (95 - 22i)$ pretty easily, using a counting trick that I happen to know.

Once I had these two decompositions, I was very happy, because I also happen to know that the Gaussian integers have "unique factorization": each Gaussian integer can be written as the product of Gaussian integers in a unique(-ish) way. So it must be possible to break down the two products above — $(97 + 10i) * (97 - 10i)$ and $(95 + 22i) * (95 - 22i)$ — into the same list of smaller factors, which can then be rearranged and multiplied to find the real factors.

This means, in turn, that (for example) $97 + 10i$ must be factorable. We write $9509 = (95 + 22i)(95 - 22i) = x\bar{x}$, where the bar refers to the complex conjugate (that is, the relationship between $95 + 22i$ and $95 - 22i$). Then we know that $x\bar{x}$ can be factored into $a\bar{a}b\bar{b}$, and that these factors can be rearranged to make the product $(97 + 10i)(97 - 10i) = a\bar{b} * b\bar{a}$, or to make the unknown ''real" factors of 9509 (which will come out as $a\bar{a} * b\bar{b}$, since we know that we can always get a real by multiplying a complex number by its conjugate.

So if $95 + 22i$ is ab, and $97 + 10i$ is $a\bar{b}$ (for example), then we should be able to find a by finding their common factor. The way to find common factors is by using linear combinations to make smaller numbers. For example, we can subtract one number from the other to get $2 - 12i$. From there, we could keep going to get the common factor (this is called the Division algorithm), but we're really already done. $2 - 12i$ is $2 * (1 - 6i)$ Since we know 2 doesn't divide 9509, the common factor must be in $1 - 6i$. And since that number times its complex conjugate is 37, a prime, 37 must be the factor we're looking for.

We could now divide 9509 by 37, to finish factoring the composite of the day. But that would be a bit boring. The other thing we could do is the same trick over again. Starting instead with $95 - 22i$ and $97 + 10i$, we subtract to get $2 + 32i$. Factoring out 2 again, we notice we have a prime product again: $1 + 16i$ times its complex conjugate is 257. So we conclude that 9509=37*257.

I find it pretty cool that this works.