

Session 12, July 24

Properties of Gaussian Integers

For starters, a quick sampling of two problem types we did yesterday.

1. Use the Chinese Remainder Theorem to find all numbers x where $x = 23 \pmod{97}$ and $x = 17 \pmod{103}$.
2. Use Lagrange Interpolation (the method similar to the CRT) to find a fourth degree polynomial for which $f(0) = 1$, $f(1) = 1$, $f(3) = 61$, $f(-1) = 5$, and $f(-3) = 121$.

And now, for something completely different. Or is it...? Often we encounter topics in mathematics that seem completely independent at first, and some initial discovery can be guided by trying to decide how the new thing is similar to or different from whatever else we've encountered. Furthermore, it's always been difficult for mathematicians to see in advance how a new branch of mathematics will relate to its precursors.

Consider the “imaginary” number i , which was initially noticed in the 16th century in calculations to solve cubic equations. People studying cubic equations (specifically, Cardano and Bombelli) found that allowing i to exist as a “fictitious” or “imaginary” number, with its only property being that $i^2 = -1$, allowed them to solve equations that were otherwise unsolvable. This is not dissimilar to the “discovery” of fractions, irrational numbers, zero, and negative numbers, which were all found to be useful in a particular way, then, later, useful in plenty of other ways. The same is true for i , and we'll be getting a taste of this today and tomorrow. Since i is not a real number, we're going to define a new set of numbers to include it, which are called the *Gaussian integers*.

$\mathbf{Z}[i]$ is the set whose elements have the form $x = a + bi$, where a and b are integers. The pronunciation is **Z** *adjoint* i , which means that you take **Z** and add all the multiples of i into the mix.

Elements of $\mathbf{Z}[i]$ include $2 + 3i$, $-5 + 4i$, $3i$, and -6 . ($3i = 0 + 3i$ and $-6 = -6 + 0i$.) $\mathbf{Z}[i]$ is not the same as the complex numbers, **C**, just as the integers are not the same as the real numbers.

Here, have some quick experience with operations in $\mathbf{Z}[i]$: don't forget $i^2 = -1$.

3. Find the values of:
 - (a) $(3 + 2i) + (5 - 3i)$
 - (b) $(3 + 2i) - (5 - 3i)$
 - (c) $(3 + 2i) \times (5 - 3i)$
 - (d) $(3 + 2i) \div (5 - 3i)$ (Give your answer with an integer denominator.)
4. Are all the answers you got in Problem 3 elements of $\mathbf{Z}[i]$? More generally, is $\mathbf{Z}[i]$ closed under addition, subtraction, multiplication, division?
5. Repeat the addition, subtraction, multiplication, and division for $(4 + 3i)$ and $(4 - 3i)$. Does anything unusual happen in any of the calculations?

Elements of $\mathbf{Z}[i]$ such as $(4 + 3i)$ and $(4 - 3i)$ are called *conjugates*. They have the same real part and opposite imaginary parts.

6. Think a little more about division in $\mathbf{Z}[i]$. Can one “divide” into another in the way that it can happen in \mathbf{Z} ? Give examples, both of elements of $\mathbf{Z}[i]$ that will divide, and of those that will not. For example, does $(3 + 2i)$ divide $(21 + i)$? When an element of $\mathbf{Z}[i]$ does *not* divide into another, can we do what we do in the division algorithm and write a quotient and remainder?

Problem 6 allows us to think of the divisors of an element in $\mathbf{Z}[i]$, just as we did in \mathbf{Z} . In fact, a lot of the concepts in \mathbf{Z} can be extended to $\mathbf{Z}[i]$. Some do not. These problems get progressively more difficult, so don't worry if you don't get to every last one of them. But *be sure to work on Problem 14*, which will apply heavily tomorrow.

7. Is $\mathbf{Z}[i]$ commutative for both addition and multiplication? Is the distributive property true? Is there an identity for addition? Does every element in $\mathbf{Z}[i]$ have an opposite under addition? Is there an identity for multiplication? Does every element in $\mathbf{Z}[i]$ have an inverse under multiplication? For each answer, search for an understanding of the reasons behind the answers, but don't worry about full, formal proofs.
8. Recall that a unit is any element of a set which has a multiplicative inverse. Which elements of $\mathbf{Z}[i]$ are units? Do they have anything in common?
9. How might you find the greatest common divisor (GCD) of two elements in $\mathbf{Z}[i]$? Think about how we do it in \mathbf{Z} (there is more than one way!), and adapt. Try it on $(1 + 5i)$ and $(6 + 4i)$, then try it again on your own example.
10. What does it mean for an element in $\mathbf{Z}[i]$ to be “greater than” another? You may not have noticed this in Problem 9, but this is essential for dealing with the GCD. Without such a relation, it's impossible to say that a GCD is “greatest.” In particular, which would you say is “larger”: $(7 + i)$ or $(6 + 5i)$? Consider graphing a member of $\mathbf{Z}[i]$. How would you do it?
11. Bob and Ray were asked to find the GCD of $(3 + 5i)$ and $(3 + i)$. Bob claims the GCD is $(1 + i)$, and Ray claims the GCD is $(1 - i)$. Who's right? What is going on here? Does anything similar happen in \mathbf{Z} ?

At this point, it is important to introduce the *norm* of a number in $\mathbf{Z}[i]$. (“Norm!” ... sorry, Boston humor.) The *norm* is the product of itself and its conjugate. Remember: conjugates have the same real part, and opposite imaginary parts.

12. Find the conjugate of $(3 + 4i)$, then find the norm. Repeat for $(3 + i)$, for $(-4 + 3i)$, for $(a + bi)$. Does this give you any help or perspective on Problem 10?
13. Can the norm of a number in $\mathbf{Z}[i]$ ever be prime (in \mathbf{Z})? Conversely, is every prime number (in \mathbf{Z}) the norm of some element in $\mathbf{Z}[i]$? If you answered “no” to either of these, what are the exceptions?

Hopefully, you now have a picture that many more properties of \mathbf{Z} than you might have expected carry over, in some way, into $\mathbf{Z}[i]$. Here are some more examples.

14. Which elements of $\mathbf{Z}[i]$ are perfect squares? Is there a way to find them, like there is in \mathbf{Z} ? What are the norms of the perfect squares? (For example, $15 + 8i$ is a perfect square. Can you see why?)

15. Adapt the methods we used in \mathbf{Z} to find a solution to the Diophantine equation $(3 + 5i)x + (5 + 2i)y = 1$. Here, x and y will be elements of $\mathbf{Z}[i]$. When using the division algorithm, don't forget that the remainder must be "smaller" than the divisor.
16. Do any of the following examples show that there is no unique prime factorization in $\mathbf{Z}[i]$? Why or why not? A related question: is every number in $\mathbf{Z}[i]$ either prime or composite? (Is that true in \mathbf{Z} ?)
- (a) $2 = (1 + i)(1 - i) = i(1 - i)^2$
- (b) $5 = (2 + i)(2 - i) = (1 + 2i)(1 - 2i)$
- (c) $4 + 7i = (2 + i)(3 + 2i) = (2 - 3i)(-1 + 2i)$
17. The norm is often written as $N(z)$, where $z = (a + bi)$. Can you prove that if x and y are elements of $\mathbf{Z}[i]$, then $N(xy) = N(x)N(y)$? There is more than one way to do this.
18. What are the prime numbers in $\mathbf{Z}[i]$? What are their norms? Look especially at any primes within $\mathbf{Z}[i]$ which do *not* have prime norms, and numbers (like 5) which are prime in \mathbf{Z} but *not* prime in $\mathbf{Z}[i]$.