Gaussian Integers, Week 1

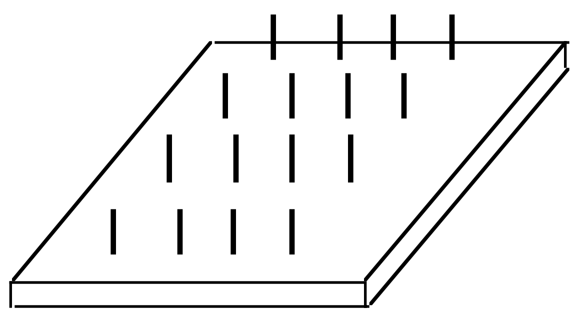
Contents

1 Day 1: The Geoboard Problem

Notes: *This is what's known as a "launch" problem. We'll work on it today and then return to it throughout the course, gaining more insight as we develop more machinery.*

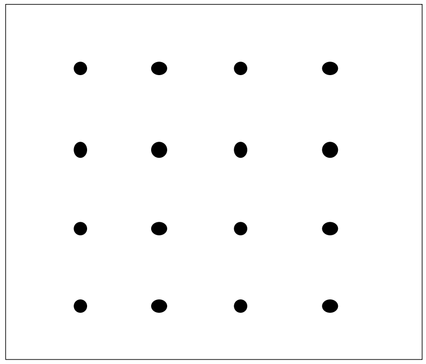
A *geoboard* is a device used by many teachers in geometry. It's a square grid of pegs, stuck in a board, like this:

This one contains 4 rows of 4 pegs, so it's called a "4 by 4" geoboard. They come in all sizes.



A 4×4 geoboard

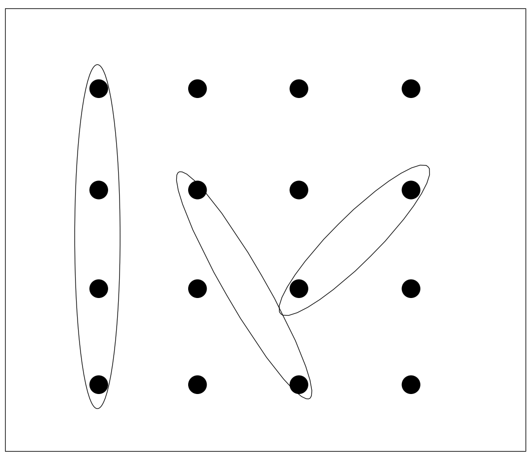
Looking down from the top, you see this:



A 4×4 geoboard, top view

One thing teachers do with geoboards is snap elastic bands around the pegs to make segments:

The elastics snap tight, so, in real life, these really do look like segments.



Three segments on a geoboard

1. Suppose you had a 2×2 geoboard (4 pegs total). What different lengths can you make?

2. Suppose you had a 3×3 geoboard (9 pegs total). What different lengths can you make?

3. Suppose you had a 4×4 geoboard. What lengths can you make? How many different ways can you make the length $\sqrt{2}$?

4. Suppose you had a 5×5 geoboard. What *integer* lengths can you make?

PROBLEM

If you know the size of a geoboard, can you tell how many *different* peg-to-peg lengths there are?

You might want to consider a 1×1 geoboard, and work up to at least a 6×6 board. Look for ways to shorten your work.

2 *Day 2: The Gaussian Integers*

We left at the end of yesterday with a number of unanswered questions:

- Given a distance, can it be made on a (potentially infinite) Geoboard? If so, what is the *smallest* square Geoboard that can be used to make the distance?
- What numbers can be expressed as the sum of the squares of two integers? How many different ways are there to express a particular number as the sum of two squares?
- Which numbers cause "problems" for our Geoboard pattern? These are numbers that can be expressed as the sum of squares in "different" ways. For example, $25 = 4^2 + 3^2 = 5^2 + 0^2$. The numbers we have found so far that do this are 25, 50, 100, 169, and 225.

1. Find all numbers less than 100 that can be expressed as the sum of the squares of two integers. What *types* of numbers show up in this list? Can you find any underlying structure?

2. Find at least three more examples of numbers (like 50) that are not perfect squares, but can be expressed as the sum of squares in "different" ways. Hint: There are two examples between 60 and 90, and one that is 4 less than one of the ones we've already found.

3. Find all *twelve* ways to write 25 as the sum of the squares of two integers.

The third problem should suggest a Geoboard with a center at (0,0) and pegs extending vertically and horizontally in both directions. This is a picture of the *Gaussian integers*. This session focuses on the structure of the Gaussian integers, and forms the ground work we will need to properly connect the mathematics of the Gaussian integers to our unsolved Geoboard problems.

A *Gaussian integer* is a complex number of the form $a + bi$ where a and b are *integers*.

The system of Gaussian integers is denoted by $\mathbb{Z}[i]$. This means "the integers ($\mathbb{Z}$) adjoin the number i." So you can create sums and products of integers and powers of i—that is, all *polynomials* in i—and look at all the numbers you get. They all turn out to be of the form $a + bi$ where a and b are integers (why?). You can create other systems by adjoining numbers besides i. For example, $\mathbb{Z}[\sqrt[3]{2}]$ would be all the numbers that looked like $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ (why?). What would $\mathbb{Z}[\pi]$ look like?.

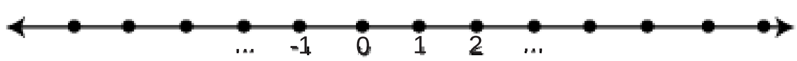
Example: $3 + 2i$. Non-example: $\frac{1}{2} + i\sqrt{2}$.

Important Stuff It's time to add, subtract, multiply, and divide!

4. Let $z = 3 - i$ and $w = -1 + 7i$. Find:

(a) $z + w$	(b) $w + z$	(c) $z - w$	(d) $w - z$
(e) $2z$	(f) $-z$	(g) $-2z + 3w$	(h) iz
(i) iw	(j) iwi	(k) wz	(l) zw
(m) w^2	(n) $\frac{w^2}{w}$		

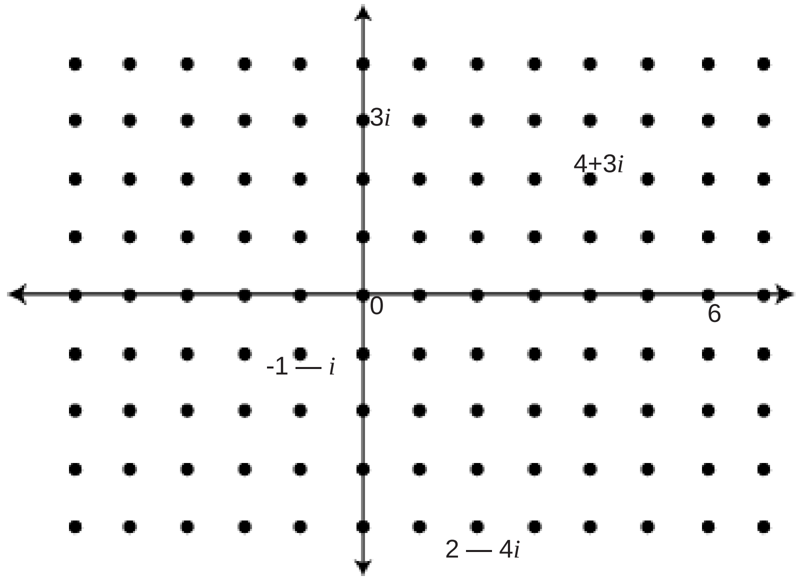
You can think of $\mathbb{Z}$ (the integers) as a set of distinct points on the number line.



The Integers

In the same way, you can think of $\mathbb{Z}[i]$ (the Gaussian Integers) as a set of distinct points in the plane. These are the *lattice points*, where both coordinates are integers.

The Gaussian integers where $a \geq 0$ and $b \geq 0$ are like pegs on a geobaord. That might help later!



The Gaussian Integers

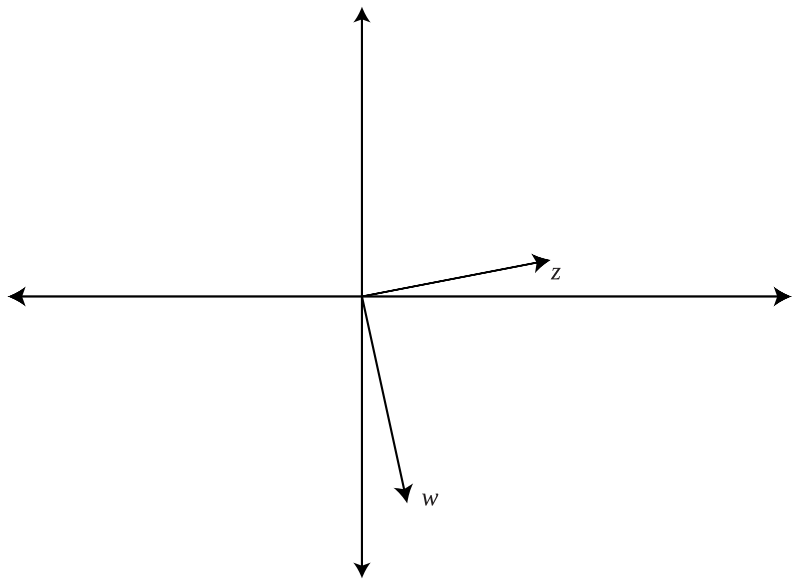
5. Let $z = 3 + i$, $w = 1 + i$, and $v = 2 - 3i$. Plot z, w, and v on the same set of axes. Which number is "biggest"? Can you make some logical order for them, smallest to largest?

What could $z < w$ mean in $\mathbb{Z}[i]$? Come up with a definition of the "size" of a Gaussian Integer.

6. Again, let $z = 3+i$, $w = -1+4i$, and $v = 2-i$. Plot each of the following on the same set of axes:

(a) z, i, $z + i =$ ____
(b) z, 1, $z + 1 =$ ____
(c) z, w, $z + w =$ ____
(d) z, v, $z + v =$ ____
(e) w, v, $w + v =$ ____

7. In general, what is the geometric interpretation of adding complex numbers? In particular, two complex numbers, z and w, are shown below. Find their sum without calculating.



8. Again, let $z = 3 + i$, $w = 1 + i$, and $v = 2 - i$. Plot each of the following on the same set of axes:

We'll come back to this, but any idea about a geometric interpretation of multiplying complex numbers?

(a) z, i, $iz =$ ____
(b) w, i, $iw =$ ____
(c) v, i, $iv =$ ____
(d) z, -1, $-z =$ ____
(e) z, $-i$, $-iz =$ ____
(f) z, 2, $2z =$ ____
(g) w, 3, $3w =$ ____
(h) v, $2i$, $2iv =$ ____
(i) z, w, $zw =$ ____
(j) z, v, $zv =$ ____
(k) w, v, $wv =$ ____

9. Plot at least 8 integral multiples of -6 on a number line. Use your picture to decide which multiple of -6 is closest to 27.

10. Let's see if we can make a picture in $\mathbb{Z}[i]$ analogous to the one we made in problem 9, by plotting the multiples of $(2 - i)$. First calculate and then plot each of the following multiples of $(2 - i)$:

(a) $(2-i)1$	(b) $(2-i)2$	(c) $(2-i)3$	(d) $(2-i)(-1)$
(e) $(2-i)i$	(f) $(2-i)2i$	(g) $(2-i)3i$	(h) $(2-i)(-i)$
(i) $(2-i)(1+i)$	(j) $(2-i)(2+2i)$	(k) $(2-i)(3+3i)$	(l) $(2-i)(-1-i)$
(m) $(2-i)(-1+i)$	(n) $(2-i)(-2+2i)$	(o) $(2-i)(1-i)$	(p) $(2-i)(1-2i)$

11. Without calculating, plot another 20 (or more!) multiples of $(2-i)$.

12. Use your picture from problem 10 to find the multiple of $(2-i)$ that is "closest" to $(2+6i)$.

More Stuff

13. Evaluate the following:
(a) $(3-2i)+(3+2i)$
(b) $(3-2i)-(3+2i)$
(c) $(3-2i)\times(3+2i)$

14. Evaluate $(5-3i)\div(3-2i)$. Is this quotient an element of $\mathbb{Z}[i]$?

How do we get rid of i in the denominator?

15. Calculate the value and plot each of the following:
(a) i (b) i^2 (c) i^3 (d) i^4
(e) i^5 (f) i^6 (g) i^{10} (h) i^{127}

16. Suppose $z=3+4i$ and $w=1-i$. *Without calculating*, locate each Gaussian integer on the complex plane.
(a) $3z$ (b) $-2w$ (c) $z+w$
(d) $3z-2w$ (e) $2w-3z$ (f) iz
(g) $3iz$ (h) $-iw$ (i) zw

17. Describe each of the following operations geometrically — what effect do they have on a Gaussian Integer in the plane?
(a) multiplying by i
(b) multiplying by -1
(c) multiplying by any real number

18. Use your answer from problem 5 to explain why it makes sense *geometrically* that $i^2=-1$.

19. Create a picture of all the multiples of these Gaussian integers:

(a) $2+4i$ (b) 5

20. Using your picture from problem 19.a of all the multiples of $2+4i$, find the multiple that is "closest" to $7+9i$. Why did this ambiguity *not* occur with the multiples of $2-i$?

21. Let $z = 7+6i$ and $w = 2-i$. Plot all of the points that look like $z+wt$ where t is in $\mathbb{Z}[i]$. That is, plot all the points that are z plus some multiple of w.

An idea: first restrict t to be an *integer*. Then look at the picture when t is "pure imaginary" (of the form bi where b is an integer). Then "mix."

Properties of the Gaussian Integers Here is a list of statements that are true about the integers. For each one, decide if an equivalent statement would be true about the Gaussian Integers. If it is true, craft the statement and then try to prove it.

Your proofs will probably use the fact that these statements are true in the integers.

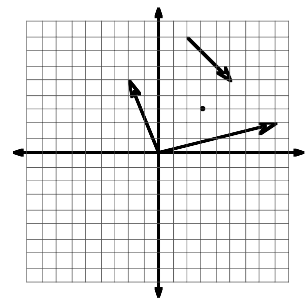
22. Closure under addition: If a and b are integers, then $a+b$ is also an integer.

23. Closure under multiplication: If a and b are integers, then ab is also an integer.

24. Commutativity: If a and b are integers, then $a+b=b+a$. Likewise, $ab=ba$.

25. Zero property: If a and b are integers, then $ab=0$ if and only if either a or b is zero.

3 Day 3: Geometry of Gaussian Integers



$\mathbb{Z}[i]$ as vectors at 0, points, and vectors.

This session will focus primarily on the geometric interpretation of Gaussian integers as an infinite Geoboard. You might still have to do some adding and multiplying, though!

We typically draw a Gaussian integer as a *vector* starting from the origin (0, 0). However, it is sometimes just as useful to think of the Gaussian integer as the point corresponding to the end of that vector, and the vector does not necessarily need to start at (0, 0).

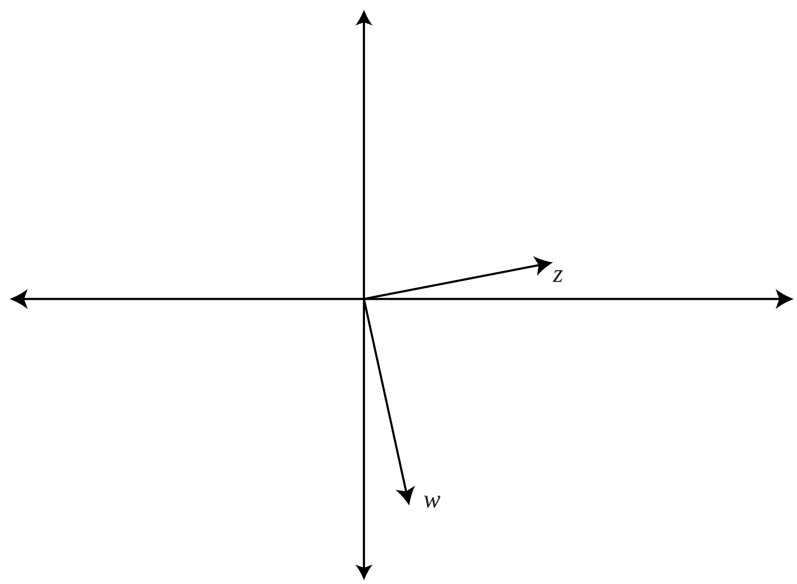
1. Let $z = 3 + i$, $w = 1 + i$, and $v = 2 - 3i$. Plot z, w, and v on the same set of axes. Which number is "biggest"? Can you make some logical order for them, smallest to largest?

What could $z < w$ mean in $\mathbb{Z}[i]$? Come up with a definition of the "size" of a Gaussian Integer.

2. Again, let $z = 3+i$, $w = -1+4i$, and $v = 2-i$. Plot each of the following on the same set of axes:

(a) z, i, $z + i =$ ____
(b) z, 1, $z + 1 =$ ____
(c) z, w, $z + w =$ ____
(d) z, v, $z + v =$ ____
(e) w, v, $w + v =$ ____

3. In general, what is the geometric interpretation of adding complex numbers? In particular, two complex numbers, z and w, are shown below. Find their sum without calculating.



4. Again, let $z = 3 + i$, $w = 1 + i$, and $v = 2 - i$. Plot each of the following on the same set of axes:

(a) z, i, $iz =$ ____
(b) w, i, $iw =$ ____
(c) v, i, $iv =$ ____
(d) z, -1, $-z =$ ____
(e) z, $-i$, $-iz =$ ____
(f) z, 2, $2z =$ ____
(g) w, 3, $3w =$ ____
(h) v, $2i$, $2iv =$ ____
(i) z, w, $zw =$ ____
(j) z, v, $zv =$ ____
(k) w, v, $wv =$ ____

We'll come back to this, but any idea about a geometric interpretation of multiplying complex numbers?

5. Describe each of the following operations geometrically — what effect do they have on a Gaussian integer in the plane?

(a) multiplying by i
(b) multiplying by -1
(c) multiplying by any real number

6. Use your answer from problem 5 to explain why it makes sense *geometrically* that $i^2 = -1$.

7. Suppose $z = 3 + 4i$ and $w = 1 - i$. *Without calculating*, locate each of these Gaussian integers:

(a) $3z$	(b) $-2w$	(c) $z+w$
(d) $3z-2w$	(e) $2w-3z$	(f) iz
(g) $3iz$	(h) $-iw$	(i) zw

8. Evaluate $(2+6i) \div (2-i)$. Is this quotient an element of $\mathbb{Z}[i]$? How do you know?

When performing division in the integers, we usually talk about the *quotient* and *remainder* of a division. For the division to work properly, the remainder should be less than the divisor.

9. Plot at least 8 integral multiples of -6 on a number line. Use your picture to decide which multiple of -6 is closest to 29.

10. Let's see if we can make a picture in $\mathbb{Z}[i]$ analogous to the one we made in problem 9, by plotting the multiples of $(2-i)$. First calculate and then plot each of the following multiples of $(2-i)$:

(a) $(2-i)1$	(b) $(2-i)2$	(c) $(2-i)3$	(d) $(2-i)(-1)$
(e) $(2-i)i$	(f) $(2-i)2i$	(g) $(2-i)3i$	(h) $(2-i)(-i)$
(i) $(2-i)(1+i)$	(j) $(2-i)(2+2i)$	(k) $(2-i)(3+3i)$	(l) $(2-i)(-1-i)$
(m) $(2-i)(-1+i)$	(n) $(2-i)(-2+2i)$	(o) $(2-i)(1-i)$	(p) $(2-i)(1-2i)$

11. Without calculating, plot another 20 (or more!) multiples of $(2-i)$.

12. Use your picture from problem 10 to find the multiple of $(2-i)$ that is "closest" to $(2+6i)$.

Recall from last time that if $z = a+bi$, then the *conjugate* of z, written $\overline{z}$, is $a-bi$.

13. Describe the relationship, geometrically, between a Gaussian integer and its conjugate.

14. Let $z = -1+4i$ and $w = 2-i$. Find each of the following.
(a) $N(z)$ (b) $N(w)$ (c) $N(zw)$

15. How is the norm of a Gaussian integer related to its graph in the complex plane?

16. Find several Gaussian integers with norm 1. What do they all look like?

17. Find all of the Gaussian integers with the same norm as $8 + i$.

More Stuff

18. For each of the following pairs of Gaussian integers, find the *distance* between z and w.
(a) $z = -2 + i$ and $w = 4 - 3i$
(b) $z = 12 + 5i$ and $w = 2i$
(c) $z = -7 + 4i$ and $w = 7 + 4i$

19. For any two distinct integers ($a \neq b$), it is always possible to say either $a < b$ or $b < a$. Is the same true in Gaussian integers? Explain.

20. Find several (at least 7) Gaussian integers whose norms are prime (in $\mathbb{Z}$).

21. If possible, find a Gaussian integer with each norm:
(a) 11 (b) 13 (c) 21
(d) 31 (e) 85 (f) 121
(g) 215 (h) 442 (i) 1105

Powers and Roots

22. Pick several Gaussian integers $a + bi$ (make $a > b$) and **square** them. Write down the results. Conjectures?

We'll come back to this later.

23. For each Gaussian integer below, compute and then plot z, z^2, z^3, and z^4.
(a) $z = 1 + i$ (b) $z = 10 + i$

24. Using the two values of z given in problem 3, compute $N(z)$, $N(z^2)$, $N(z^3)$, $N(z^4)$, and $N(z^{17})$.

25. We say that an integer n is a perfect square if there exists some integer a such that $a^2 = n$. Likewise, a Gaussian integer z is a perfect square if there exists some Gaussian integer w such that $w^2 = z$. For each z below, decide if it is a perfect square. If it is, find its square root.
(a) $z = -3 + 4i$ (b) $z = 2i$ (c) $z = 2 - i$
(d) $z = 3 + 2i$ (e) $z = -5 - 12i$ (f) $z = -25$

To paraphrase Tina Turner, "What's Norm got to do with it?" (Feel free to groan.)

26. A Gaussian integer z is a perfect cube if there exists some Gaussian integer w such that $w^3 = z$. For each z below, decide if it is a perfect cube. If it is, find its cube root.
(a) $z = -2 - 2i$ (b) $z = 5 - 3i$ (c) $z = -11 + 2i$

Challenges

27. Find two Gaussian integers that are an integer distance apart.

28. Find three Gaussian integers so that any two of them are an integer distance apart.

29. You know about primes in $\mathbb{Z}$: they are numbers whose only divisors are themselves and 1. In $\mathbb{Z}[i]$, some integer primes can now "split" into factors. Make a table of integer primes, and for each one decide if it splits into factors over the Gaussian integers or not.

For example, $2 = (1 + i)(1 - i)$.

4 *Day 4: Divisibility in Gaussian Integers*

Let's start where we left off last time – looking at a lattice of multiples of a particular Gaussian integer.

1. Make a pretty picture in $\mathbb{Z}[i]$ by plotting the multiples of $(3+i)$. First, calculate and plot each of the following multiples of $(3+i)$ until you get the idea:

(a) $(3+i)1$	(b) $(3+i)2$	(c) $(3+i)3$	(d) $(3+i)(-1)$
(e) $(3+i)i$	(f) $(3+i)2i$	(g) $(3+i)3i$	(h) $(3+i)(-i)$
(i) $(3+i)(1+i)$	(j) $(3+i)(2+2i)$	(k) $(3+i)(3+3i)$	(l) $(3+i)(-1-i)$
(m) $(3+i)(-1+i)$	(n) $(3+i)(-2+2i)$	(o) $(3+i)(1-i)$	(p) $(3+i)(1-2i)$

Then, continue the lattice so that it extends at least as far as ± 10 in both the real and imaginary directions.

2. The lattice should suggest that the Gaussian integer $(9-i)$ is *not* a multiple of $(3+i)$. Can you think of a way to use norms to explain why $(9-i)$ cannot be a multiple of $(3+i)$?

3. Use your picture from problem 1 to find the multiple of $(3+i)$ that is "closest" to $(9-i)$.

4. What integers are multiples of $(3+i)$? Why?

The notion of divisibility is as important in $\mathbb{Z}[i]$ as it is in $\mathbb{Z}$.

The expression $a|b$ is read as "a divides b," and it means our familiar notion of "divides," as in divides evenly with no remainder. A statement about divisibility can be true or false or indeterminate, just like other types of mathematical statements.

So, for example, $2|6$ is true, but $6|2$ is not true. We sometimes write $6 \nmid 2$.

These problems are about $\mathbb{Z}$ (the integers).

5. For each statement below, decide if it is true or false. Find a way to justify your answers.
(a) $5|10$ (b) $5|-10$ (c) $10|5$ (d) $5|13$
(e) $5|5$ (f) $1|5$ (g) $5|1$

6. Propose a mathematical definition for $a|b$.

7. To decide if $a|b$ when a and b are Gaussian integers, it helps to be able to divide Gaussian integers. This problem helps review dividing Gaussian integers; if you already know how, skip it.
Let $z = 3 + 2i$ and $w = 7 - 4i$.
(a) Find $z\overline{z}$.
(b) Find $\frac{z}{w}$. Hint: use problem 7a above!

These problems are about $\mathbb{Z}[i]$, the Gaussian integers.

8. For each statement below, decide if it is true or false. Find a way to justify your answers.
(a) $5|(5 + 5i)$ (b) $-5|(5 + 5i)$ (c) $(1 + i)|(3 + 3i)$
(d) $i|(5 + 5i)$ (e) $(5 + 5i)|i$ (f) $(26 + 41i)|0$

9. Decide if each statement is true or false. Justify your answers.
(a) $(3 + 2i)|(10 + 11i)$ (b) $(3 + 2i)|(4 + 7i)$ (c) $(4 + 7i)|(10 + 11i)$
(d) $(10 + 11i)|(3 + 2i)$ (e) $(4 - i)|(10 + 11i)$

10. Find the norm of each Gaussian integer in problem 9. Any conjectures?

11. You saw in problem 9 that $(3 + 2i)|(10 + 11i)$. Does that imply that $(3-2i)|(10+11i)$? How about $(2+3i)|(10+11i)$? $(2 - 3i)|(10 + 11i)$? Any conjectures?

Recall from Roger Howe's talk that a number can be considered *prime* if it has no proper factorization; that is, it cannot be written as $z = vw$ where v and w are both less than z.

12. Find all divisors of $2 + 2i$. Find an element of $\mathbb{Z}[i]$ that does not divide $2 + 2i$. Is $2 + 2i$ prime in $\mathbb{Z}[i]$?

13. Find all divisors (in $\mathbb{Z}[i]$) of the Gaussian integer 5. Find an element of $\mathbb{Z}[i]$ that does not divide 5. Is 5 prime in $\mathbb{Z}[i]$?

14. Find all divisors of $1 - 4i$. Find an element of $\mathbb{Z}[i]$ that does not divide $1 - 4i$. Is $1 - 4i$ prime in $\mathbb{Z}[i]$?

15. Find a Gaussian integer whose norm is 13. Use that to find a factorization of 13 in $\mathbb{Z}[i]$. Can you do this in more than one way? How can this be? Does this mean there is no unique prime factorization in $\mathbb{Z}[i]$?

16. Let a and b be Gaussian integers. If $a|b$, what must be true about the graphs of a and b? Try several examples.

Prove, Disprove, or Salvage if Possible... Before going on to the proofs, it will help to have a definition of "divides" to work with. Here's a good one.

DEFINITION

We say $a|b$ ("a divides b") if and only if there is an element c in $\mathbb{Z}[i]$ such that $ac = b$.

This definition of $a|b$ works for both $\mathbb{Z}$ and $\mathbb{Z}[i]$. How close is it to the definition you proposed in problem 6?

Here is a list of conjectures about divisibility. For each conjecture:

- Decide if it is true or false.
- If it is true, try to prove it.
- If it is false, show how you know (provide a counterexample). Then try to "salvage" it — change the hypothesis or conclusion somehow to make a true statement, and then prove *that*.

Don't forget that important first step! Trying to prove something that isn't true can be difficult.

17. For any a in $\mathbb{Z}[i]$, $a|a$.

18. For any a in $\mathbb{Z}[i]$, $i|a$.

19. If $a|b$ then $N(a)|N(b)$.

20. If $N(a)|N(b)$ then $a|b$.

21. For any a, b, and c in $\mathbb{Z}[i]$: If $a|b$ and $b|c$ then $a|c$.

Here are some other conjectures about $\mathbb{Z}[i]$ that may or may not be true. Prove or disprove, and salvage if you can!

22. If q is an integer, then $N(q) = q^2$.

23. A Gaussian integer is a perfect square if and only if its norm is a perfect square.

24. If a Gaussian integer z is a perfect square, then the following are all perfect squares as well: $\overline{z}$, $-z$, and iz.

25. The norm of $(1+i)^6$ is 16.

26. A Gaussian integer is a perfect square if and only if its conjugate is a perfect square.

27. If z and w are in $\mathbb{Z}[i]$, $N(z+w) = N(z) + N(w)$.

28. The distance between two Gaussian integers z and w is $\sqrt{N(z-w)}$.

5 Leftovers and Carryovers...

1. If possible, find a Gaussian integer with each norm:
(a) 11 (b) 13 (c) 21
(d) 31 (e) 85 (f) 121
(g) 215 (h) 442 (i) 1105

2. Pick several Gaussian integers $a + bi$ (make $a > b$) and **square** them. Write down the results. Conjectures?

We'll come back to this later.

3. For each Gaussian integer below, compute and then plot z, z^2, z^3, and z^4.
(a) $z = 1 + i$ (b) $z = 10 + i$

4. Using the two values of z given in problem 3, compute $N(z)$, $N(z^2)$, $N(z^3)$, $N(z^4)$, and $N(z^{17})$.

5. We say that an integer n is a perfect square if there exists some integer a such that $a^2 = n$. Likewise, a Gaussian integer z is a perfect square if there exists some Gaussian integer w such that $w^2 = z$. For each z below, decide if it is a perfect square. If it is, find its square root.
(a) $z = -3 + 4i$ (b) $z = 2i$ (c) $z = 2 - i$
(d) $z = 3 + 2i$ (e) $z = -5 - 12i$ (f) $z = -25$

To paraphrase Tina Turner, "What's Norm got to do with it?" (Feel free to groan.)

6. A Gaussian integer z is a perfect cube if there exists some Gaussian integer w such that $w^3 = z$. For each z below, decide if it is a perfect cube. If it is, find its cube root.
(a) $z = -2 - 2i$ (b) $z = 5 - 3i$ (c) $z = -11 + 2i$