Gaussian Integers, Week 1

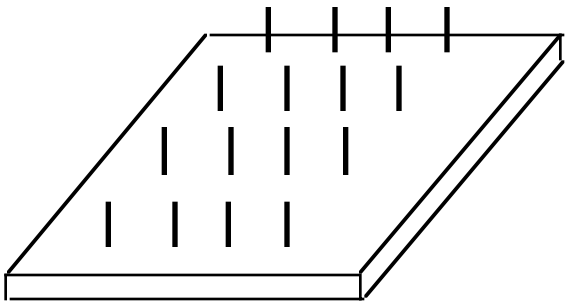
Contents

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.*

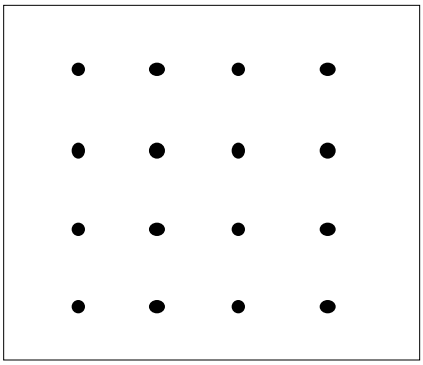
A *geoboard* is a device used by many teachers in geometry. It's a square grid of pegs, stuck in a board, like this:

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

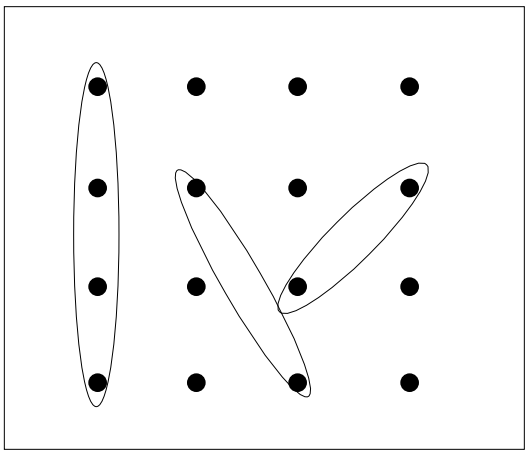
Looking down from the top, you see this:



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*.

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

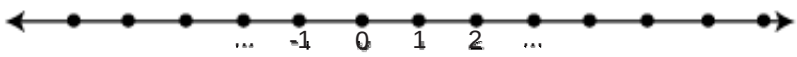
The system of Gaussian integers is denoted by $\mathbb{Z}[i]$. This means "the integers ($\mathbb{Z}$) adjoin the number i." So you can create sums and products of integers and powers of i—that is, all *polynomials* in i—and look at all the numbers you get. They all turn out to be of the form $a + bi$ 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?.

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) $\frac{w^2}{w}$		

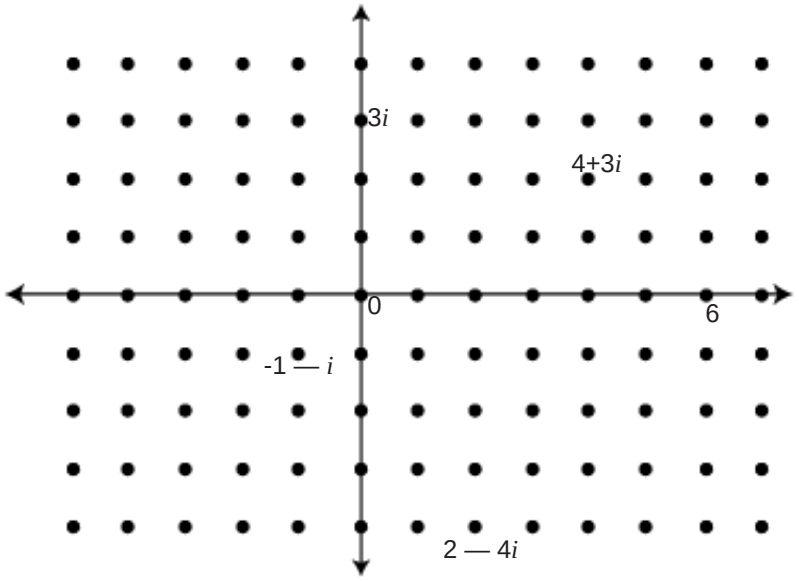
You can think of $\mathbb{Z}$ (the integers) as a set of distinct points on the number line.



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

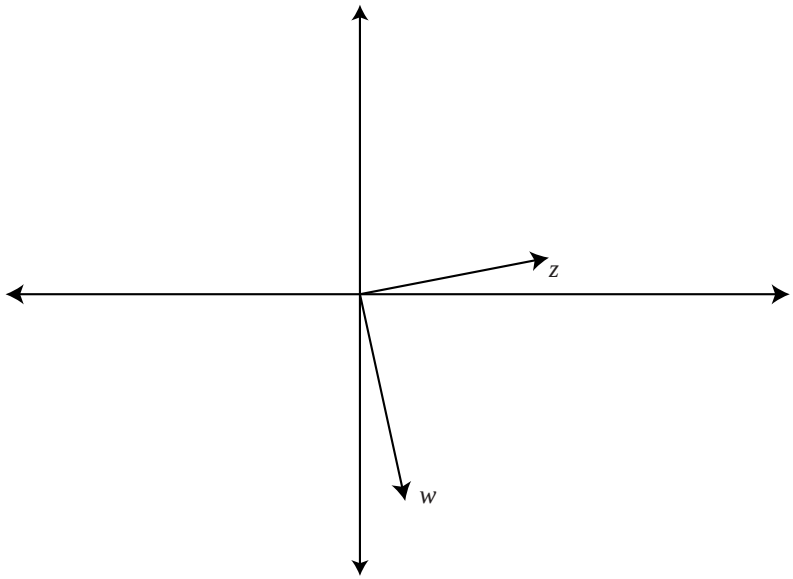
5. Let $z = 3 + i$, $w = 1 + i$, and $v = 2 - 3i$. Plot z, w, and v on the same set of axes. Which number is "biggest"? Can you make some logical order for them, smallest to largest?

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:

(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?

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.

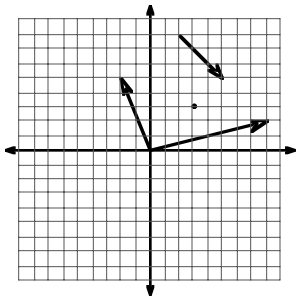
22. Closure under addition: If a and b are integers, then $a+b$ is also an integer.

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).

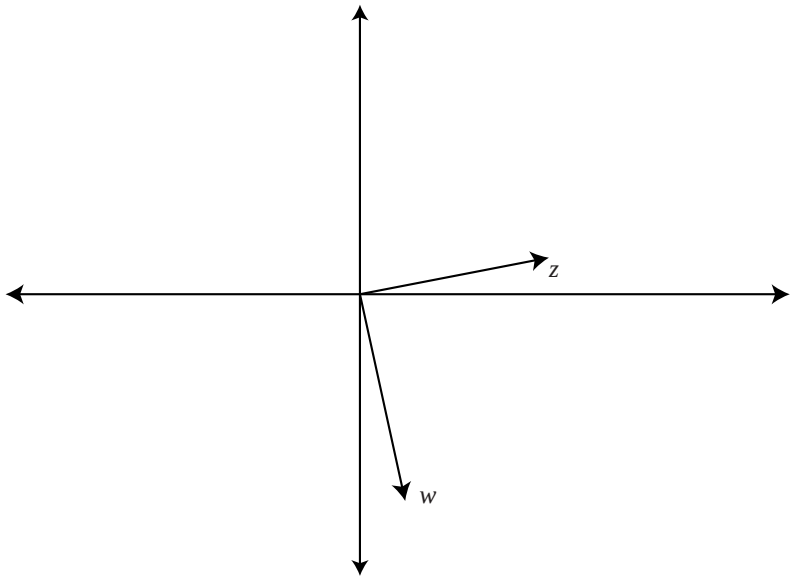
1. Let $z = 3 + i$, $w = 1 + i$, and $v = 2 - 3i$. Plot z, w, and v on the same set of axes. Which number is "biggest"? Can you make some logical order for them, smallest to largest?

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 $6 \not| 2$.

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) $5|1$

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

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!

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) $(26 + 41i)|0$

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

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.

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

(a) $z = -3 + 4i$ (b) $z = 2i$ (c) $z = 2 - i$
(d) $z = 3 + 2i$ (e) $z = -5 - 12i$ (f) $z = -25$

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) $z = -11 + 2i$

Gaussian Integers, Week 2

Contents

5 Day 5: Proofs, Primes, and Pythagoras

Throughout our work in the first week, we have come up with a number of conjectures. Some of them have been proved, some have been disproved, and some are still undecided. We'll start today by focusing on proof; in particular we will try to prove some of the things we have observed about $\mathbb{Z}[i]$.

Some of these proofs will be about divisibility, so it will help to have a definition of "divides" to work with. Here is the definition introduced in Friday's notes.

DEFINITION

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

This definition of $a|b$ works for both $\mathbb{Z}$ and $\mathbb{Z}[i]$, or any other number system where multiplication is defined.

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.

Many of these proofs rely on definitions, so make sure you know the defintions of divisibility and norm.

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

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

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

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

5. If $a|b$ then $ai|b$.

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

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

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

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

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

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

11. A Gaussian integer is prime if and only if its norm is prime.

Roger Howe's definition of prime may be helpful in the previous problem and in the next few. A Gaussian integer is *prime* if it has no proper factorization. Another useful definition involving the norm is that a Gaussian integer p is prime if there are no Gaussian integers z with $z|p$ and $1 < N(z) < N(p)$.

12. Find all divisors of $3+i$. Find an element of $\mathbb{Z}[i]$ that does not divide $3+i$. Is $3+i$ prime in $\mathbb{Z}[i]$?

13. Find all divisors (in $\mathbb{Z}[i]$) of the Gaussian integer 2. Find an element of $\mathbb{Z}[i]$ that does not divide 2. Is 2 prime in $\mathbb{Z}[i]$?

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

15. If a Gaussian integer z is prime, what other Gaussian integers related to z would you expect to be prime? You may find your work from Problem 5 useful, but this is not a proof.

Back to the Geoboard? Remember the original Geoboard problem? It came down to asking two important questions:

- Which integers can be expressed as the sum of two squares?
- Given an integer, in how many ways can it be expressed as the sum of two squares?

Well, remember that the norm of a Gaussian integer is a sum of two squares:

$$N(a+bi) = a^2 + b^2$$

so that should certainly help us with the investigation. Let's focus on sums of two squares and norms. First, a couple of problems to review what we've done to this point:

16. If possible, find a Gaussian integer with the given norm:

(a) $N(z) = 1$	(b) $N(z) = 2$	(c) $N(z) = 3$
(d) $N(z) = 4$	(e) $N(z) = 5$	(f) $N(z) = 6$
(g) $N(z) = 7$	(h) $N(z) = 25$	(i) $N(z) = 31$
(j) $N(z) = 221$	(k) $N(z) = 235$	(l) $N(z) = 290$

17. Which prime numbers in $\mathbb{Z}$ are the norm of some element in $\mathbb{Z}[i]$?

18. Pick several Gaussian integers $a + bi$ (make $a > b > 0$) and **square** them. Write down the results. Conjectures?

19. Find the norm of each of each squared Gaussian integer you found in problem 18.

20. Use properties of the norm to show that if z is a Gaussian integer, then

$$N(z^2) = (N(z))^2$$

Notice that the right side of this equation is a *perfect square* (it is the square of an integer).

Problem 20 is a key to one of the nicest ways around for generating Pythagorean triples. The idea goes like this:

- The equation $a^2 + b^2 = c^2$ can be written $N(z) = c^2$ where $z = a + bi$. So, we are looking for Gaussian integers whose norms are perfect squares.
- Problem 20 says that the norm of a Gaussian integer will be a perfect square if the Gaussian integer is itself a perfect square.
- So, to generate Pythagorean triples, pick a Gaussian integer at random, and square it. The square will be a Gaussian integer $a + bi$ whose norm, $a^2 + b^2$ will be a perfect square.

So, there are infinitely many triples of integers that satisfy the equation $x^2 + y^2 = z^2$. What about $x^3 + y^3 = z^3$?

That is, $a^2 + b^2$ will equal c^2 for some integer c, and (a, b, c) will be a Pythagorean triple.

21. Generate half a dozen Pythagorean triples in this way.

22. Use the method to establish the following identity that is often used for generating Pythagorean triples:

$$(r^2 + s^2)^2 = (r^2 - s^2)^2 + (2rs)^2$$

Challenges... There are some details that need to be taken care of to refine our algorithm...:

23. If we pick a Gaussian integer "at random" using this method, we sometimes produce duplicate triples, and sometimes the "legs." produced are negative. Refine the algorithm so that it produces only positive triples and produces no duplicates.

Hint: If $N(z) = N(w)$, what do you know about z and w?

24. Even after you eliminate duplicates, there are annoying triples like $(6, 8, 10)$ that show up and are simple multiples of a "primitive" triple (this one is twice $(3, 4, 5)$). Characterize those z so that z^2 will generate a *primitive* Pythagorean triple.

25. Find all numbers less than 250 that cause "problems" for the Geoboard counting algorithm. We have found a few such "problem" numbers: 25, 50, 65, 85, 100, 169, 221, 225. Try to find a way to generate these numbers without relying on trial and error.

26. Use the results of problem 25 to determine the number of different distances that can be measured on a 15×15 Geoboard.

6 Day 6: Congruences

By "$a \equiv b \pmod{n}$" (read this as "a and b are congruent modulo n"). we mean a and b differ by a multiple of n.

1. Which of the following pairs of numbers are congruent modulo 5? Justify your answers.
(a) 2 and 12 (b) 4 and 444 (c) 2 and -2 (d) 0 and 15
(e) 1 and -14 (f) 4 and -1 (g) a and $5a$ (h) a and $6a$

2. List seven pairs of numbers that are congruent to -3 modulo 13.

3. Draw a number line. On the number line,
(a) Color all of the numbers congruent to 0 modulo 6 one color.
(b) Color all of the numbers congruent to 1 modulo 6 another color.
(c) Color all of the numbers congruent to 2 modulo 6 another color.
(d) Keep going. How many different colors do you need?

$\mathbb{Z}_n$ is the system of remainders modulo n. There are lots of potential sets we could use, but the standard set we use is $0, 1, 2, \ldots, n-1$.

4. Find the following in $\mathbb{Z}_8$:

(a) $7+6$,	$5 \cdot 3$,	4^2,	$6-2$,	$2-7$,
(b) 16,	32,	40,	88,	800,
(c) -4,	-13,	$800+3$,	$800+7$,	8005
(d) 9,	17,	25,	33,	41

Why are the ones in 4.d all the same?

5. Without finding their actual values, explain why, in $\mathbb{Z}_8$, we have

$$\begin{aligned} 165 &= 157 \\ 519 &= 503 \\ 415 &= 15 \end{aligned}$$

Saying "$165 = 157$ in $\mathbb{Z}_8$" is the same as saying "$165 \equiv 157 \pmod 8$."

6. Reduce the following mod 8 without a calculator: 8029, 451, 323, and -406.

Hint: Find a nearby multiple of 8.

7. (a) Find $(16 + 20)$ in $\mathbb{Z}_{15}$.
(b) Find 16 in $\mathbb{Z}_{15}$ and 20 in $\mathbb{Z}_{15}$. Add the two.
(c) Compare your answers to 7a and 7b. Any conjectures?
(d) Repeat 7a and 7b with $(29 + 36)$ and $(9 + 23)$. Does your conjecture hold?

8. (a) Find $(16 \cdot 20)$ in $\mathbb{Z}_{15}$.
(b) Find 16 in $\mathbb{Z}_{15}$ and 20 in $\mathbb{Z}_{15}$. Multiply the two.
(c) Compare your answers to 8a and 8b. Any conjectures?
(d) Repeat 8a and 8b with $(4 \cdot 18)$ and $(7 \cdot 50)$. Does your conjecture hold?

9. It is true that you can multiply, add, and reduce in any order you want, in any modulus. Use that fact to find the following in $\mathbb{Z}_{13}$ without a calculator.

Prove it!

(a) $(14 \cdot 15 \cdot 16)^2$ (b) 28^4 (c) $12 \cdot 11 \cdot 10$
(d) $(12 \cdot 15)^3$ (e) $14^{5,067,293}$ (f) $12^{5,067,293}$
(g) $(128(132 + 35))^2$ (h) $(12^3 \cdot 14 \cdot 3 + 13(500)^{299})^2$

10. Suppose I was really tired and fell asleep at 8:00pm. If I slept for 499 hours, what time of day would I wake up?

11. Suppose my birthday fell on a Saturday in 2001.
(a) What day will it fall on this year?
(b) What day did it fall on in 1997? (Note: 2000 was a leap year.)

12. In this problem you will establsih one of the "famous" divisibilty tests.
(a) Find 1, 10, 100, 1000, and 10000 in $\mathbb{Z}_3$.
(b) Explain why any power of 10 reduces to 1 in $\mathbb{Z}_3$.
(c) Use 12a and 12b to quickly find the following in $\mathbb{Z}_3$:
4631 5973 2217

Hint: $4631 = 4 \cdot 1000 + 6 \cdot 100 + 3 \cdot 10 + 1$

(d) Explain why a number is divisible by 3 if the sum of its digits is divisible by 3.

(e) Show that a number is divisible by 4 if the sum of its units digit and twice its ten's digit is divisible by 4.

Hint: Look at the numbers from 12a in $\mathbb{Z}_4$.

13. Carefully complete the following multiplication table for $\mathbb{Z}_{10}$.

·	0	1	2	3	4	5	6	7	8	9
0										
1										
2										
3			6							
4										
5										
6										
7					8					
8										
9										

(a) Does $\mathbb{Z}_{10}$ (using $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$) have a largest number? Explain.

(b) Can you find two nonzero numbers in $\mathbb{Z}_{10}$ whose produce is zero. If so, list all of the pairs that work.

14. Use your multiplication table for $\mathbb{Z}_{10}$ to find the following:

$\sqrt{6}$ $\quad \frac{1}{3}$ $\quad \frac{1}{7}$ $\quad \frac{1}{2}$

$\sqrt{5}$ $\quad \sqrt{3}$ $\quad \sqrt{-1}$ $\quad \frac{4}{7}$

Note: Some may have multiple answers, and some may not exist.

15. In $\mathbb{Z}_n$, a nonzero number a is called a *zero divisor* if there exists a nonzero number b such that $ab = 0$. Use your multiplication table for $\mathbb{Z}_{10}$ to list all of the zero divisors. Do they have anything in commeon with each other? With the number 10?

For example, in $\mathbb{Z}_4$, 2 is a zero divisor because $2 \cdot 2 = 0$.

16. In $\mathbb{Z}_n$, a number a is called a *unit* if there exists a number b such that $ab = 1$. Use your multiplication table for $\mathbb{Z}_{10}$ to list all of the units. Conjectures?

For example, in $\mathbb{Z}_3$, 2 is a unit because $2 \cdot 2 = 1$.

17. Compare your lists from problems 15 and 16. Any conjectures?

18. Make a multiplication table for $\mathbb{Z}_9$.

·	0	1	2	3	4	5	6	7	8
0									
1									
2									
3									
4									
5									
6									
7									
8									

19. Using your multiplication table for $\mathbb{Z}_9$:

(a) Find the following:
$\frac{1}{5}$ $\frac{1}{3}$ $\frac{1}{2}$ $\sqrt{4}$ $\sqrt{-2}$

(b) List all of the zero divisors

(c) List all of the units.

20. (a) Based on the results of problems 16 and 19, what do you think the zero divisors in $\mathbb{Z}_{21}$ are? Why?

(b) Without doing the multiplication, explain why $14 \cdot 3$ must be zero in $\mathbb{Z}_{21}$.

Hint: $14 \cdot 3 = (2 \cdot 7) \cdot 3$.

(c) Without multiplying, how can we tell that $18 \cdot 7$ will be zero in $\mathbb{Z}_{21}$?

(d) Explain why any nonzero number that has 3 or 7 as a factor will be a zero divisor in $\mathbb{Z}_{21}$.

21. Based on the previous problems, how many zero divisors would you expect to find in the following: $\mathbb{Z}_3$, $\mathbb{Z}_7$, and $\mathbb{Z}_p$ where p is a prime number?

22. Find all solutions to these equations in $\mathbb{Z}_{10}$:

(a) $3x = 2$ (b) $2x - 3 = 0$

(c) $9x - 2 = 4$ (d) $3x^2 + 5 = 3$

23. Find all solutions to these equations in $\mathbb{Z}_9$:

(a) $3x = 2$ (b) $2x - 3 = 0$

(c) $5(x^2 - 3) = 3$ (d) $(x - 3)^3 = 8$

Hint: Cube each number in $\mathbb{Z}_9$ to make sure you find *all* cube roots of 8.

24. (a) Solve the quadratic equation $x^2 - x = 0$ in ordinary arithmetic. How did you solve it?

(b) Now solve it in $\mathbb{Z}_{10}$. How many solutions does it have here?

(c) We now have a quadratic equation with *four* solutions. Why is this happening? Why *can't* this happen in ordinary arithmetic?

25. Consider the equation $2x = 4$ in $\mathbb{Z}_{10}$.

- Al says that if you multiply both sides by $\frac{1}{2}$, you get $x = 2$. So $x = 2$ is the solution.
- Betty says that if $2x = 4$, then $2x-4 =$, so $2(x-2) = 0$. This can only happen if $x - 2 = 0$, so she agrees that $x = 2$ is the only solution.
- Chris says that in his table, $2 \cdot 2 = 4$ and $2 \cdot 7 = 4$, so there are two solutions: $x = 2$ and $x = 7$.

Al and Betty somehow missed the solution $x = 7$. Find the mistake in their logic.

26. Find all solutions to these equations:
(a) $5x = 5$ in $\mathbb{Z}_{10}$
(b) $6x - 2 = 2$ in $\mathbb{Z}_{10}$
(c) $3x = 6$ in $\mathbb{Z}_9$

In $\mathbb{Z}[i]$, $a \equiv b \pmod{z}$ if (and only if) a and b differ by a multiple of z.

27. Use the definition of $a \equiv b \pmod{z}$ to find four Gaussian integers that are congruent to $2 - i$ modulo $7 + 3i$.

28. Use the definition of $a \equiv b \pmod{z}$ to find four Gaussian integers that are congruent to i modulo $1 + 2i$.

29. Plot multiples of $(1 + 2i)$ in the plane. Remember that these "multiples" have the form $(1 + 2i)z$ where z is in $\mathbb{Z}[i]$.

30. Using your graph from Problem 29, explain why $(1 + 3i)$ is congruent to i modulo $(1 + 2i)$. Name at least two other Gaussian integers that are congruent to i modulo $(1 + 2i)$.

31. Plot all the multiples of $2 - i$ in the plane.

32. Show that each of the following numbers is congruent to 1 modulo $(2 - i)$.

$$(3 - i), \quad (5 - 2i), \quad (2 + 2i), \quad -2i$$

Plot each of these numbers on your picture from problem 31. Plot 10 more numbers congruent to 1 mod $(2 - i)$.

Take It Further

33. Consider the following "system of modular equations":

$$x = 2 \pmod 3$$

$$x = 3 \pmod 4$$

A "solution" to this system is defined to be any integer that reduces to 2 in $\mathbb{Z}_3$ and reduces to 3 in $\mathbb{Z}_4$.

(a) List the first 15 integers that reduce to 2 mod 3.
(b) List the first 15 integers that reduce to 3 mod 4.
(c) Find four solutions to the modular system.
(d) Without listing out any more terms, what do you think the next solution will be? Check your answer by reducing it mod 3 and mod 4.
(e) Explain why if n is a solution, $n+12$ must be another.

34. When a bag of candy is divided among 6 people, there is one left over. When it is divided among 7 people, there are 3 left over. If there are less than 150 pieces of candy in the bag, what are the possible amounts?

35. When my age is divided by 5, there is a remainder of 4. When divided by 3, there is a remainder of 2, when divided by 7 there is a remainder of 5. How old am I?

7 Day 7: Division Algorithm

As you probably remember, there is a division algorithm in $\mathbb{Z}$ (the integers). The division algorithm can be expressed in a few ways. One way is this:

> **Division Algorithm, Version 1:** Given two integers a and b, $b \neq 0$, there exist unique integers q and r such that $a = qb + r$, and $0 \leq r < |b|$

Here's another version, maybe not the one you are familiar with:

> **Division Algorithm, Version 2:** Given two integers a and b, $b \neq 0$, there exist unique integers q and r such that $a = qb + r$, and $|r| \leq |\frac{b}{2}|$

In both algorithms, there are two important conclusions. First, q and r *exist*, so a solution to the division can always be found. Second, q and r are *unique*, so there is exactly one solution to the division.

1. For each of the following a and b pairs, find q and r for
   (a) The version 1 algorithm
   (b) The version 2 algorithm

$$(13, 3), \quad (15, 24), \quad (-17, 5),$$
$$(45, -8), \quad (59, -8), \quad (231, -8)$$

2. Plot all of the integral multiples of -8 on a number line and explain how this picture can help justify the version 2 division algorithm for $b = -8$.

How can it help justify the version 1 algorithm?

3. For what kinds of pairs (a, b) do the version 1 and version 2 algorithms produce the same q and r?

4. Give a quick justification of why you think either algorithm works (pick your favorite). Try drawing a number line to help.

5. Suppose we continued dividing, using the previous divisor as the new dividend, and the previous remainder as the new divisor. For example, let's use 125 and 55 as a starting point:
$125 = 2 \times 55 + 15$
Then 55 becomes the new dividend, and 15 becomes the new divisor:
$55 = 3 \times 15 + 10$
What happens as this process is continued? Try this again, starting with a new pair of numbers. What happens to the remainder after each step? What happens to the remainder *eventually*?

Can the division algorithm we stated earlier be re-written replacing $\mathbb{Z}$ with $\mathbb{Z}[i]$? What should $|\ |$ be translated to? The next few problems should help you with those questions.

6. For each of the following pairs a and b, decide if $a|b$.

Which ones are easy to dismiss, and which ones must be tested?

(a) $(2+i, 8-i)$ (b) $(2-i, 8+i)$ (c) $(3-2i, 8+i)$

(d) $(2-i, i)$ (e) $(i, 2-i)$ (f) $(3, 6+9i)$

(g) $(3, 6+10i)$ (h) $(4+3i, 5+12i)$ (i) $(4+3i, 8-6i)$

(j) $(2+3i, 2-3i)$ (k) $(2+i, 5)$ (l) $(5, 7)$

7. See if you can find q and r for each of the (a, b) pairs in problem 6.

8. Draw a lattice of multiples of $(1 + 2i)$. Then, use the lattice to find the multiple of $(1 + 2i)$ that is "closest" to $(2+6i)$. Write a division algorithm-like equation using this multiple.

9. Al and Betty are arguing over the answer to problem 8 in $\mathbb{Z}[i]$. Steve claims that

$$(2 + 6i) = (1 + 2i)(3) + (-1)$$

Melanie claims that

$$(2+6i) = (1+2i)(2) + (2i)$$

Verify that in both cases, the norm of the remainder is less than the norm of the divisor $(1+2i)$. So who is correct?

10. Plot a lattice of multiples of $(2-i)$ to find the multiple of $(2-i)$ that is "closest" to $(3+4i)$, then write a division algorithm-like equation using this multiple. How many multiples of $(2-i)$ could qualify as multiples that produce remainders whose norms are less than that of the divisor?

11. Use division of Gaussian integers to directly find the quotient and the "smallest" possible remainder when $(3+4i)$ is divided by $(2-i)$. Is the remainder in fact "less than" the divisor $(2-i)$?

12. Do you think it will always be possible to find a remainder that is "less than" the divisor when performing the division algorithm in $\mathbb{Z}[i]$? Try to come up with a convincing geometric argument that supports your claim (yes or no).

13. Find the quotient and remainder when $(5-3i)$ is divided by $(3+2i)$. You can do this either by creating a lattice of multiples of $(3+2i)$ or by directly dividing and finding the nearest Gaussian integer for the quotient.

14. Suppose we try the algorithm described in problem 5 with elements of $\mathbb{Z}[i]$. What do you think will happen *eventually* to the remainder? Try this out with a few examples. Be careful to choose the "smallest" possible remainder at each step of the division process.

It's a Mod, Mod World? In any ring, a number is a *unit* if it has a reciprocal. That is, if it divides evenly into 1. If a is an element of a number system (like $\mathbb{Z}[i]$ or $\mathbb{Z}_n$), and you can find an element b in the same system so that $ab = 1$,then a is a unit. For example, 2 is a unit in $\mathbb{Z}_3$ since $2 \cdot 2 \equiv 1 \pmod 3$.

. . . groan . . .

15. What are all of the units in $\mathbb{Z}$? in $\mathbb{Z}[i]$? in $\mathbb{Z}_{10}$?

16. Find all of the units in $\mathbb{Z}_{15}$. Find all of the zero divisors in $\mathbb{Z}_{15}$. How are these lists related to the number 15?

17. Consider the number 2. In which modular rings is 2 a unit? In which modular rings is 2 a zero divisor?

18. Suppose u is a unit. Then there exists v so that $uv = 1$. Now consider $(-u)$, the opposite of u. Can you find a number in the system so that $(-u) \cdot \_\_\_\_ = 1$?

We're going to try and prove Art's conjecture...

19. Find all possible numbers in $\mathbb{Z}_{10}$ which equal the following:
(a) $\sqrt{6}$ (b) $\frac{1}{3}$ (c) $\frac{1}{7}$ (d) $\frac{1}{2}$

(e) $\sqrt{5}$ (f) $\sqrt{3}$ (g) $\sqrt{-1}$ (h) $\frac{4}{7}$

One way to do these problems is to translate each into an equation. For example, if $x = \frac{1}{3}$, then $3x = 1$. Equations without fractions or roots tend to be much more solvable!

20. In $\mathbb{Z}_{10}$, what numbers satisfy the following equations?
(a) $3x = 2$ (b) $2x - 3 = 0$

(c) $9x - 2 = 4$ (d) $3x^2 + 5 = 3$

(e) $5x + 5 = 0$ (f) $x^4 = 7$

Consider the equation $2x = 4$ in $\mathbb{Z}_{10}$.

- Beavis says that if you multiply both sides by $\frac{1}{2}$, you get $x = 2$. So $x = 2$ is the solution.
- Butthead says that if $2x = 4$, then $2x - 4 = 0$, so $2(x-2) = 0$. This can only happen if $x-2 = 0$, so he agrees that $x = 2$ is the only solution.
- Cato says that in her table, $2 \cdot 2 = 4$ and $2 \cdot 7 = 4$, so there are two solutions: $x = 2$ and $x = 7$.

Beavis and Butthead somehow missed the solution $x = 7$ (go figure). Find the mistake in their logic.

Prove or Disprove and Salvage if Possible...

21. u is a unit in $\mathbb{Z}[i]$ if and only if $N(u) = 1$.

22. u is a unit in $\mathbb{Z}_n$ if and only if u does not divide n.

8 Day 8: GCD and Factorization

Sample test #1

1. List all divisors of $33 + 4i$.

2. List all of the units in each of the following systems: $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}_7$, $\mathbb{Z}_8$

3. List all primes in $\mathbb{Z}[i]$ with norm less than 50.

4. How many ways can each of the following numbers be expressed as the sum of two squares? 595, 1885, 585, 80

5. Plot on a complex number plane 10 numbers congruent to 1 modulo $(3 + i)$.

Stuck? Maybe try this first: Plot on a number line 10 numbers congruent to 1 modulo 5

GCD and Factorization

6. Find a valid quotient and remainder when each of the following numbers are divided by $(3 + i)$: $(7 + 5i)$, 13, $(-2 + 4i)$, $(-3 - 3i)$, $(2 + i)$

Use your lattice!

7. Find the GCD of each of the following pairs of numbers:
(a) 24 and 56
(b) $(33 + 4i)$ and $(38 + 44i)$
(c) 483 and 391
(d) 11,413 and 11, 289
(e) $(63 + 49i)$ and $(39 + 3i)$

8. Use Euclid's algorithm to find the GCD of $(63 + 49i)$ and

$(39+3i)$

A calculator will probably be helpful. You will probably also want to frequently check you work with those around you (How many times do we say that to our students?)

9. Al and Bowen each did the previous problem. Al's algorithm yielded the following result:

$$\begin{aligned}(63+49i) &= (2+i)\times(39+3i)+(-12+4i)\\ (39+3i) &= (-3-i)\times(-12+4i)+(-1+3i)\\ (-12+4i) &= (2+3i)\times(-1+3i)+(-1+i)\\ (-1+3i) &= (2-i)\times(-1+i)+0\end{aligned}$$

Bowen's algorithm went as follows:

$$\begin{aligned}(63+49i) &= (1+i)\times(39+3i)+(27+7i)\\ (39+3i) &= 1\times(27+7i)+(12-4i)\\ (27+7i) &= (2+i)\times(12-4i)+(-1+3i)\\ (12-4i) &= (-2-3i)\times(-1+3i)+(1-i)\\ (-1+3i) &= (-2+i)\times(1-i)+0\end{aligned}$$

Al claims the GCD of $(63+49i)$ and $(39+3i)$ is $(-1+i)$, but Bowen disagrees, and claims that his calculation shows the GCD to be $(1-i)$. Who is right? Did your calculation look exactly like either of theirs?

10. If z is in $\mathbb{Z}[i]$, when is $(z,\overline{z})=1$?

Some Challenges and Extensions

11. Find integers x and y which satisfy each of the following equations:
(a) $24x+56y=1$
(b) $11,413x+11,289y=1$

. . . back substitution?

12. Find Gaussian Integers z and w which satisfy each of the following equations:
(a) $(2+i)z+(3-2i)w=1$
(b) $(1+3i)z+(5+i)w=1$

13. Betty has a supply of five-cent and eight-cent stamps. What is the largest denomination of postage she can't make?

Be thankful that Betty doesn't have current postage denominations: 23 and 37 cents!

14. Jim has a supply of 8-cent and 12-cent stamps. What is the largest denomination of postage he can't make?

15. Prove, or Disprove and Salvage if Possible: If $(a,b)=1$ and $a|bc$ then $a|c$.

This statement is equivalent to the statement that each number has a unique prime factorization

9 Day 9: Congruences

1. Turn to the person next to you and explain why the Euclidean Algorithm works.

Also explain how you feel about the Euclidean Algorithm.

2. Find a valid quotient and remainder when $(16 + 11i)$ is divided by $(5 + i)$.

3. Al claims that the Gaussian Integers have unique prime factorization, just like the integers. Betty claims Al is wrong, and as evidence, shows him the following examples:

$$2 = (1 + i)(1 - i) = i(1 - i)^2$$

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

$$(4 + 7i) = (2 + i)(3 + 2i) = (2 - 3i)(-1 + 2i)$$

What do you think?

4. Find the number of elements in each of the following: $\mathbb{Z}_7$, $\mathbb{Z}_{51}$, $\mathbb{Z}[i]_{(2+i)}$, $\mathbb{Z}[i]_{(5+i)}$, $Z[i]_7$

Any Conjectures?

5. What is Pick's Theorem, and what does it have to do with the last problem?

6. List all of the elements of $\mathbb{Z}_7$, $\mathbb{Z}[i]_{(2+i)}$.

7. Al and Betty agree (for once!) that there are five elements in $\mathbb{Z}[i]_{(2+i)}$. However, Al thinks the five elements are $\{0, (-1 + i), i, 1 + i, 2i\}$ while Betty says the elements are $\{0, 1, 2, (1+i), (1-i)\}$. Help them resolve their dispute.

8. Fred names the elements of $\mathbb{Z}[i]_{(2+i)}$ $\{0, 1, 2, 3, 4\}$. Is he correct? Can any five Gaussian Integers be chosen?

In Problems 9–10**:** Prove, or Disprove and Salvage if Possible.

9. If an integer a is the sum of 2 squares, then a must be the norm of some Gaussian Integer.

10. If an integer is congruent to 3 (mod 4), then it is prime in$\mathbb{Z}[i]$.

11. Find a prime in $\mathbb{Z}[i]$ whose norm is not a prime in $\mathbb{Z}$

12. In how many different ways can 1105 be expressed as the sum of two squares?

Hint: Day 8, Problem 1

13. In how many different ways can 225 be expressed as the sum of two squares?

In Problems 14–16**:** p is an odd prime integer. Prove, or Disprove and Salvage if Possible.

14. If p is the sum of two squares, then -1 is a square in $\mathbb{Z}_p$.

I'll prove it... I'll prove it like a theorem!
—-Ross from "Friends"

15. If -1 is a square in $\mathbb{Z}_p$, then p is the sum of two squares.

16. -1 is a square in $\mathbb{Z}_p$ if and only if p is congruent to 1 (mod 4).

17. Characterize all Gaussian Integers a and b such that dividing a by b will give you "the worst-case scenario."

18. Generalize Pick's Theorem to three dimensions.

Gaussian Integers, Week 3

Contents

10 Day 10: Sums of Two Squares

1. Define what it means for a number to be:
(a) prime in $\mathbb{Z}$
(b) prime in $\mathbb{Z}[i]$
(c) prime in the sums of squares

In Problems 7–9**:** Prove, or Disprove and Salvage if Possible.

2. If an integer is congruent to 3 (mod 4), then it cannot be expressed as the sum of two squares.

3. If a prime integer is congruent to 3 (mod 4), then it is prime in $\mathbb{Z}[i]$.

4. If a Gaussian Integer is prime in $\mathbb{Z}[i]$, then its norm is a prime in $\mathbb{Z}$.

5. If each of two integers is the sums of two squares, then so is their product.

One way to think about problem 5: use norm.

6. If z is any Gaussian Integer, then $N(z^2)$ is a square in $\mathbb{Z}$.

7. If a prime integer is congruent to 1 (mod 4) , then it is the norm of a prime Gaussian Integer.

Remember the Geoboard Problem? To solve this problem, it might be useful to know how many ways a given number can be written as the sum of two squares. We will investigate this today. In our investigation, we'll need to decide what we mean

Why might this be useful?

by "different." For instance, if $n = 25$,

$$\begin{aligned} 25 &= 3^2 + 4^2 \\ 25 &= 4^2 + 3^2 \\ 25 &= (-3)^2 + 4^2 \\ 25 &= 0^2 + 5^2 \\ 25 &= (-5)^2 + 0^2 \\ 25 &= 5^2 + 0^2 \quad \textit{et cetera} \end{aligned}$$

Are all of these different? How would you like us to count? We will come to a consensus in class.

Define $S(n)$ to be the number of ways an integer n can be expressed as the sum of two squares.

8. Find the values of $S(n)$ for all values of n from 1 to 100. Any Conjectures?

9. For which n is $S(n) = 0$?

10. For which n is $S(n) > 1$?

11. Find a value of n for which $S(n) > 5$

12. List all divisors of 5 in $\mathbb{Z}[i]$. How may are there? Can you find a prime factorization for 5?

13. List all divisors of $(8+i)$ in $\mathbb{Z}[i]$. How may are there? Can you find a prime factorization for $(8+i)$?

14. List all divisors of 25 in $\mathbb{Z}[i]$. How may are there? Can you find a prime factorization for 25?

15. Prove that at least one number in every pythagorean triple must be even.

16. Find a non-right triangle with vertices at lattice points, all of whose sides have integer lengths.

17. Find all units and zero-divisors in each of the following systems: $\mathbb{Z}_7$, $\mathbb{Z}_{12}$, $\mathbb{Z}[i]_{(2+i)}$, $\mathbb{Z}[i]_{(5+i)}$

11 Day 11: S(n), Lagrange, and Nice Triangles

1. List at least three integers n for which:
(a) $S(n) = 3$
(b) $S(n) = 4$
(c) $S(n) = 5$
(d) $S(n) = 8$
(e) $S(n) = 32$

2. List all divisors of 5 in $\mathbb{Z}[i]$. How may are there? Can you find a prime factorization for 5?

3. List all divisors of $(8+i)$ in $\mathbb{Z}[i]$. How may are there? Can you find a prime factorization for $(8+i)$?

4. List all divisors of 25 in $\mathbb{Z}[i]$. How may are there? Can you find a prime factorization for 25? What is $S(625)$?

5. Find a prime factorization in Z[i] for $(88 + 154i)$

6. Calculate $S(31, 460)$.

In Problems 7–9: Prove, or Disprove and Salvage if Possible.

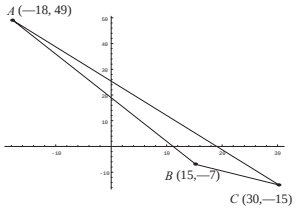
7. If $ab = c$, and a and b are both perfect squares, then c is a perfect square.

8. If $ab = c$, and a and b are not both perfect squares, then c is not a perfect square.

9. If $ab = c$, and a and b are not both perfect cubes, then c is not a perfect cube.

10. Find the length of each side of the triangle whose vertices

Problems 7–9: Are these true in $\mathbb{Z}$? In $\mathbb{Z}[i]$?



Picture for problem 7

are at $(-18, 49)$, $(15, -7)$, and $(30, -15)$:

Problem 7: Did the numbers come out nicely? Why? Can we easily make other triangles that work out nicely?
Problem 8: Hmm. A nice distance. Why? What else do we use || to represent

11. If $r = (3 + 2i)$, calculate $q = r^2$, and the length of the vector which represents q. We often denote this distance by $|q|$.

12. State a formula which will produce Pythagorean triples. Use this formula to generate a Pythagorean triple of integers which you have never seen before. Use this formula to generate a Pythagorean triple of Gaussian Integers.

Day 5, Problem 22

13. Now, let's make one of these nice triangles. Let $r = (3 + 2i)$, and $s = (2 + i)$ Calculate $a = r^2 + s^2$, and $b = r^2 - s^2$. Calculate $z = a^2$, and $w = b^2$. Find $|z|$, $|w|$, and $|z - w|$. Use z, w, and $z - w$ to create a nice triangle!

Does this look familiar?

Why does this procedure work?
Amaze your friends!

14. Create another nice triangle using this procedure.

A taste of $\mathbb{Z}[\sqrt{-2}]$:

15. List five elements of $\mathbb{Z}[\sqrt{-2}]$.

16. By analogy to $\mathbb{Z}[i]$, define conjugate and norm in $\mathbb{Z}[\sqrt{-2}]$. What is the norm of $a+b\sqrt{-2}$? Is norm still multiplicative?

17. How many units can you find in $\mathbb{Z}[\sqrt{-2}]$? List them.

18. We use the lattice point (a, b) to represent the Gaussian Integer $(a + bi)$, and all Gaussian Integers with the same norm lie on a circle centered at the origin. If we use the lattice point (a, b) to represent $a + b\sqrt{-2}$ in $\mathbb{Z}[\sqrt{-2}]$, what can you say about where points which share the same norm lie?

19. Partition the natural numbers into two sets so that neither set contains a Pythagorean triple.

12 Day 12: "Teacher Problems"

1. Calculate each of the following:
(a) $S(2), S(4), S(8), ...$
(b) $S(3), S(9), S(27), ...$
(c) $S(4), S(16), S(64), ...$
(d) $S(5), S(25), S(125), ...$
(e) $S(13), S(169), S(2197), ...$

Can you generalize?

Justify these using prime factorizations.

2. Find a prime factorization in $\mathbb{Z}[i]$ for 221. What is $S(221)$? List all ways that 221 can be written as the sum of two squares.

3. Find a prime factorization in $\mathbb{Z}[i]$ for 1885. What is $S(1885)$?

4. Find a prime factorization in $\mathbb{Z}[i]$ for $83,521$. What is $S(83,521)$?

5. Find a prime factorization in $\mathbb{Z}[i]$ for $98,260$. What is $S(98,260)$? List all ways that $98,260$ can be written as the sum of two squares.

6. Calculate $S(1,768,680)$, $S(177,625)$, and $S(7,420,530,600)$

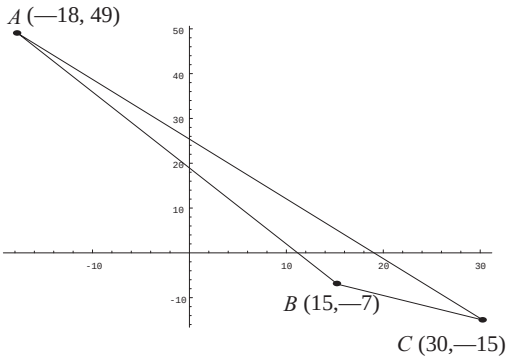
Once you have agreed on a method, you might want to divide the calculations among your group.

And now...

Making Nice Triangles

7. Find the length of each side of the triangle whose vertices are at $(-18, 49)$, $(15, -7)$, and $(30, -15)$:

Problem 7: Did the numbers come out nicely? Why? Can we easily make other triangles that work out nicely?



Picture for problem 7

8. If $r = (3 + 2i)$, calculate $q = r^2$, and the length of the vector which represents q. We often denote this distance by $|q|$.

Problem 8: Hmm. A nice distance. Why? What else do we use || to represent

9. State a formula which will produce Pythagorean triples. Use this formula to generate a Pythagorean triple of integers which you have never seen before. Use this formula to generate a Pythagorean triple of Gaussian Integers.

Day 5, Problem 22

10. Now, let's make one of these nice triangles.
Let $r = (3+2i)$, and $s = (2+i)$ Calculate $a = r^2 + s^2$, and $b = r^2 - s^2$. Calculate $z = a^2$, and $w = b^2$. Find $|z|$, $|w|$, and $|z - w|$. Use z, w, and $z - w$ to create a nice triangle!

Does this look familiar?

11. Create another nice triangle using this procedure.

Why does this procedure work?
Amaze your friends!

More "Teacher Problems"

12. If you want to create a lattice point in 3-space (x, y, z) which is an integer distance away from the origin, what criteria must x, y, and z meet? What kind of distances are possible?

This might lead to an investigation.

13. A "congruent number" is an integer which is the area of a right triangle with rational side lengths. Show that 6 is a congruent number, but 1 is not. What other numbers are congruent numbers?

13 *Day 13: The Geoboard Strikes Back*

1. For each of the following integers calculate the number of divisors which are 1 (mod 4) and 3 (mod 4):

n	1	2	3	5	18	25	49	54	65	70	85	100
1 mod 4												
3 mod 4												

2. Explain why, if an integer n has an odd power of a 3 (mod 4) prime in its prime factorization, then it has the same number of divisors which are 1 (mod 4) and 3 (mod 4).

3. Can an integer ever have more divisors which are 3 (mod 4) than 1 (mod 4)? Explain.

Recall our question from Day 1: If you know the size of a Geoboard, can you tell how many different peg-to-peg lengths there are?

4. Let $G(n) =$ the number of peg-to-peg lengths one can make on an $n \times n$ Geoboard. Calculate $G(n)$ for $n = 1, \ldots, 10$

n	1	2	3	4	5	6	7	8	9	10
$G(n)$										

5. How many integral peg-to-peg lengths are possible on an $n \times n$ Geoboard?

OK, problem 5 is a hard problem. Maybe start with $n = 1, 2, 3, ...$

6. Find three integers n for which the "almost solution" to the $n \times n$ Geoboard problem does not give the correct number for $G(n)$. In these cases, is the "almost solution" too big

or too small?

7. Calculate the average value of $S(n)$ for the sets {1–10}, {1–20}, {1–30}, {1–40}, {1–50}, {1–60}, {1–70}, {1–80}, {1–90}, {1–100}. Does the average seem to get bigger, smaller, converge on a value, or none of the above? What do you think will happen to the average as our sets get bigger and bigger?

The average value of S between 1 and N is

$$\frac{1}{N}\sum_{k=1}^{N} S(k)$$

N	10	20	30	40	50	60	70	80	90	100
$\frac{1}{N}\sum_{k=1}^{N} S(k)$										

8. Calculate the number of lattice points contained in a circle of radius 5, 10, 100, 1000, and 10,000.

These last three might require a computer program. How close are these to πr^2

9. Are there any integers which can be expressed as an integral power of a Gaussian Integer?

Extension: Another Route to Pythagorean Triples

10. What is the equation of the unit circle?

11. Find a point on the unit circle where:
(a) Both coordinates are rational and non-zero.
(b) One coordinate is rational and the other is irrational.

12. Consider the line with slope $5/2$, passing through the point $(0, -1)$. Find the other intersection of this line with the unit circle. Use the intersection point to create a Pythagorean triple.

13. Given a rational point on the unit circle, show how to derive a Pythagorean triple.

A rational point is a point where both coordinates are rational numbers

14. Consider the line with slope r/s, passing through the point $(0, -1)$. Find the other intersection of this line with the unit circle. Can we always the intersection point to create a Pythagorean triple?

Did this circular route lead us back to a place we've already been?

15. Can you create all possible Pythagorean Triples using the "unit circle method?"

16. Prove that every integer is an element of at least one Pythagorean triple.

14 Day 14: So Long, and Thanks for All the Fish

1. Use the "almost solution" to the Geoboard problem to calculate G(5). What's wrong with this solution?

2. Calculate the number of lattice points in a circle of radius 7 centered at the origin.

3. Calculate the average value of $S(n)$ for the sets {1–10}, {1–20}, {1–30}, {1–40}, {1–50}, {1–60}, {1–70}, {1–80}, {1–90}, {1–100}. Does the average seem to get bigger, smaller, converge on a value, or none of the above? What do you think will happen to the average as our sets get bigger and bigger?

The average value of S between 1 and N is

$$\frac{1}{N}\sum_{k=1}^{N} S(k)$$

N	10	20	30	40	50	60	70	80	90	100
$\frac{1}{N}\sum_{k=1}^{N} S(k)$										

4. Calculate the number of lattice points contained in a circle of radius 5, 10, 100, 1000, and 10,000, each centered at the origin.

Problem 4: The last three (100,1000,10000) might require a computer program. How close are these to πr^2?

5. Are there any integers which can be expressed as an integral power of a Gaussian Integer?

6. Which ordinary integers can be expressed as the product of two primes in the Gaussian Integers?

7. Which ordinary integers are prime in the Gaussian Integers?

8. Find a formula for the number of different peg-to-peg lengths possible on an $n \times n$ Geoboard.

9. Please write down any that apply to you. We really appreciate any feedback. If anything occurs to you after today,

please email!

(a) Something you learned, or something which changed your understanding of a concept.

(b) A question you don't know the answer to but would like to explore.

(c) A change or suggestion you might have if this class were to be offered again.

(d) Anything else you wish to add.