Gaussian Integers, Week 2

Contents

5. Day 5: Proofs, Primes, and Pythagoras **2**

6. Day 6: Congruences **6**

7. Day 7: Division Algorithm **12**

8. Day 8: GCD and Factorization **16**

9. Day 9: Congruences **18**

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.