Organizational Notes

1. A Zoom recording link and class notes will be sent out after each Zoom class.

2. Remember to send your answers to the classroom worksheets, and pdfs of your Lab work. Title your email with enough to help me record your “participation”.

Logging into Sage/CoCalc

1. Start the Chrome browser.

2. Go to http://cocalc.com and sign in.

3. You should see an existing Project for our class. Click on that.

4. Click “New”, call it c11, then click “Sage Worksheet”.

5. For each problem number, label it in the Sage cell where the work is. So for Problem 1, the first line of the cell should be #Problem 1.

6. When you are finished with the worksheet, click “make pdf”, email me the pdf (at clarson@vcu.edu, with a header that says Math 305 c11 worksheet attached).

From our Book

We defined \( a \equiv b \pmod{n} \) to mean \( n|\left(b - a\right) \) (which is equivalent to \( n|\left(a - b\right)\)). There are several related ways to think about this definition.

1. How can we check whether \( 5 \equiv 11 \pmod{3} \)? We can directly divide using the definition. Is there anything else we could do?

2. How can we check whether \( 47 \equiv 11 \pmod{3} \)?

One way to think about \( a \equiv b \pmod{n} \) is in terms of the remainders of \( a \) and \( b \) individually when you divide by \( n \) (If the remainders are the same then the difference between them must be a multiple of \( n \)).

Let’s check \( 47 \equiv 11 \pmod{3} \) by finding the remainder (or modulus when we divide my \( n \).

3. Run: \( 47 \mod(3) \).

4. Run: \( 11 \mod(3) \).

5. We see that we get the remainders. So we can test if \( 47 \equiv 11 \pmod{3} \) by checking if the remainders are the same. Run: \( 47 \mod(3)==11 \mod(3) \).
We defined $n \mathbb{Z}$ ($n \in \mathbb{N}$) to be the collection of integer multiples of $n$, and we defined $a + n \mathbb{Z}$ ($a \in \mathbb{Z}$) to be the collection \{a + n\mathbb{Z}\}, the set of integers you get by adding any multiple of $n$ to $a$. Notice that this means that these are the integers that are equivalent \mod n to $a$.

6. Is 47 in $2 + 3\mathbb{Z}$? Check if $47 \equiv 2 \pmod{3}$. Run: 47.mod(3)==2.mod(3).

Equivalently we can think of the remainder of dividing 47 by 3. $2 + 3\mathbb{Z}$ is the collection of integers whose remainder is 2 when you divide by 3.

We defined $\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} : a \in \mathbb{Z}\}$. So another way to think about this collection is that its the set of remainders you get when you divide by 3. (Really, its the collections of numbers that are equivalent \mod 3 to those remainders.)

7. Define the ring $\mathbb{Z}/3\mathbb{Z}$. Call it $R$. Run: $R = \text{Integers}(3)$.

8. List the elements of $R$ to see what we have. Run: \text{list}(R).

9. Really what we have are representatives of infinite sets. We can see that 5 for instance is in $R$. Run: 5 \text{ in } R.

10. Of course, 5 and 2 have the same remainder when you divide by 3—so they must both be in $2 + 3\mathbb{Z}$. We’ll check this by defining symbols $a$ and $b$ to represent $2 + 3\mathbb{Z}$ and $5 + 3\mathbb{Z}$ and check that these are actually equal:

    \[
    a = R(2) \\
    b = R(5) \\
    a == b
    \]

    Next class we will define $+$ and $\ast$ to show that $\mathbb{Z}/n\mathbb{Z}$ is a ring:

    \[
    (a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z} \\
    (a + n\mathbb{Z}) \ast (b + n\mathbb{Z}) = (a \ast b) + n\mathbb{Z}
    \]

    What still needs to be done is to show that the $+$ and $\ast$ have the ring properties.

    One way to think about these now is that $+$ and $\ast$ in $\mathbb{Z}/3\mathbb{Z}$ is in terms of remainders. The sum $(a + 3\mathbb{Z}) + (b + 3\mathbb{Z})$ is the set of things that are equivalent \mod 3 to $a + b$ and thus to the remainder of what you get by dividing $(a + b)$ by 3.

11. Do some experiments to see how the elements of $R$ ($\mathbb{Z}/3\mathbb{Z}$) add.

    A ring $R$ is a field if there is a multiplicative identity (or one) and every element has a multiplicative inverse, that is, for every non-zero $a \in R$ there is a $b \in R$ such that $a \ast b = 1$.

    We’ll see that for a prime $p$, $\mathbb{Z}/p\mathbb{Z}$ is not only a ring but that it is (importantly) a field.

12. Do some experiments to see how the elements of $R$ ($\mathbb{Z}/3\mathbb{Z}$) multiply. Check that every non-zero element has a multiplicative inverse.

13. Let’s try a more interesting example. Let’s define $\mathbb{Z}/17\mathbb{Z}$. Do some experiments to show that this ring is indeed a field.

**Extras**

14. If $p$ and $p + 2$ are both prime, they are called twin primes. Find the first several pairs of twin primes.