20200128

Modular Arithmetic

We are accustomed to performing arithmetic on infinite sets of numbers. But sometimes we need to perform arithmetic on a finite set, and we need it to make sense and be consistent (as far as possible) with normal arithmetic. In this unit we will discuss versions of addition, multiplication, subtraction and division for finite sets of numbers.

We will focus on the sets defined by $\mathbb{Z}_n = \{0, 1, 2, 3, ..., n-1\}$ where $n \geq 2$

$\mathbb{Z}_n$ is just the set of remainders we can get when we divide integers by n

One of the important features we want to build into our mathematical operations for finite sets is **closure**: the property that when we apply an operation to two elements of the set, the result is also an element of the set. Note that we have encountered closure before ... when we apply the composition operation to two permutations, the result is another permutation.

Since we are working now with $\mathbb{Z}_n$, it seems reasonable to use "mod n" as part of our definitions of addition, multiplication, subtraction and division (because if we end each calculation with "mod n" we are guaranteed that our results will be in $\mathbb{Z}_n$, so we will have closure). In these notes I will occasionally use "%" to represent "mod" .

Since we will be doing ***a lot*** of mod operations in this unit, it makes sense to explore the properties of this. Much of this is review – none of the new material is difficult.

When we write the expression "$a \mod n$" (where a and n are both integers) we mean "the unique integer r such that

$a = q * n + r$ for some integer q

and

$0 \leq r < n$ "

The easy way to see that r must exist and must be unique is to visualize a on a number line where all the multiples of n are marked. We can think of r as the "offset" from the closest multiple of n that is $\leq a$. It should be clear that for each value of a, there is exactly one r in the range $[0 \dots n-1]$ that works as this offset.

When we write the statement "$a \equiv b \pmod{n}$" we mean "$a \mod n = b \mod n$"

Some people get confused by "$a \equiv b \pmod{n}$" because it looks like the "$\mod n$" is only being applied to one side. I have to agree .... it would make more sense to write "$a \equiv_{\text{mod n}} b$" to show that the "$\mod n$" applies to the $\equiv$, and not just to b ...... but nobody is going to listen to me so we are stuck with the standard notatoin.

So "$9 \equiv 17 \pmod{4}$" is a true statement because $9 \mod 4 = 1$ and $17 \mod 4 = 1$

All of the examples we have looked have involved positive integers. What happens if we try to include negative integers?

For example, what is $-13 \mod 8$? It turns out that our definition of $a \mod n$ works perfectly well if $a < 0$ and $n > 0$

We can see that $-13 = -2 * 8 + 3$ and there is no other value of r in the range $[0 \ldots 7]$ that lets us write $-13 = q * 8 + r$ .... so $-13 \mod 8 = 3$

What if we let n be negative? What is $13 \mod -8$? What is $-13 \mod -8$? There is no universally accepted definition for these situations. Some mathematicians suggest we should just use the absolute value of n, regardless of whether it is negative or positive (so $n = -8$ and $n = 8$ are handled the same way) but others suggest that when n is negative, the remainders should be in the range $[-(n-1) \ldots 0]$

Fortunately this burning controversy will not be an issue for us ... we will always use values of n that are > 1

We will use the symbols $\oplus, \otimes, \ominus$ and $\oslash$ to represent addition, multiplication, subtraction and division on $\mathbb{Z}_n$

$\oplus$ and $\otimes$ are very easy to define, and we start with them:

Let a and b be elements of $\mathbb{Z}_n$. Then $a \oplus b = (a+b)\ \ \%\ \ n$, and $a \otimes b = (a \cdot b)\ \%\ n$

Example: Let n = 7, a = 3, b = 6.

$$3 \oplus 6 = (3+6)\ \ \%\ 7 = 9\ \%\ 7 = 2$$
$$3 \otimes 6 = (3 \cdot 6)\ \%\ 7 = 18\ \%\ 7 = 4$$

Let n = 8, a = 3, b = 6

$$3 \oplus 6 = (3+6)\ \ \%\ 8 = 9\ \%\ 8 = 1$$
$$3 \otimes 6 = (3 \cdot 6)\ \%\ 8 = 18\ \%\ 8 = 2$$

It's useful to look at the full $\oplus$ and $\otimes$ tables for a couple of small values of n.

Here is the $\oplus$ table for $\mathbb{Z}_5$

	b						
a	$\oplus_5$		0	1	2	3	4
	0		0	1	2	3	4
	1		1	2	3	4	0
	2		2	3	4	0	1
	3		3	4	0	1	2
	4		4	0	1	2	3

Here is the $\otimes$ table for $\mathbb{Z}_5$

	b						
a	$\otimes_5$		0	1	2	3	4
	0		0	0	0	0	0
	1		0	1	2	3	4
	2		0	2	4	1	3
	3		0	3	1	4	2
	4		0	4	3	2	1

A brief examination of these two tables reveals some interesting patterns. For example, both are symmetric about their main diagonal (that is, the top right "triangle" is the mirror image of the bottom left "triangle"). This is because $\oplus$ and $\otimes$ are both **commutative**, which means that $x \oplus y = y \oplus x$ and $x \otimes y = y \otimes x$.

Let's prove that $\oplus$ is commutative. The proof is based on the fact that ordinary addition is commutative (ie $x + y = y + x$):

$$x \oplus y = (x + y) \ \% \ n = (y + x) \ \% \ n = y \oplus x$$

The proof that $\otimes$ is commutative is just as easy.

We can also see that in the $\oplus_5$ table, each row is a permutation of $\mathbb{Z}_5$. It's not hard to see why this happens: clearly the first row is just a copy of the "axis row" since we are just adding 0 to each element of $\mathbb{Z}_5$. Then in each subsequent row the a value increases by 1, so the $a + b$ value increases by 1, so the remainder when we divide by n goes up by 1 ... until it drops back down to 0.

We can see that the same thing would happen for $\oplus$ on any $\mathbb{Z}_n$, so every $\oplus$ table is going to look a lot like the one we just did.