The following lemma will be essential to many of the computational tools we will use in this segment of the course:

Lemma: Let n be an integer ≥ 2 and let k and m be any integers.

Then $(k * n + m)\ \%\ n = m\ \%\ n$

Proof:

Let $(k * n + m)\ \%\ n = r$ this means r is the unique integer such that
$k * n + m = q * n + r$ where q is an integer and
$r \in [0 \ldots n - 1]$
We want to show $r = m \mod n$
$k * n + m = q * n + r$
$\Rightarrow m = (q - k) * n + r$
$\Rightarrow m\ \%\ n = r$ by definition
$\Rightarrow (k * n + m)\ \%\ n = m\ \%\ n$

We can put that to use in several ways!

Claim: Let a, b and n be integers, with $n \geq 2$. Then $(a + b)\%n = (a\%n + b\%n)\%n$

Proof: Let $a\%n = r_1$ and $b\%n = r_2$
$\Rightarrow a = q_1 * n + r_1$ and $b = q_2 * n + r_2$

$$\begin{aligned}\Rightarrow (a + b)\%n &= (q_1 * n + r_1 + q_2 * n + r_2)\%n \\ &= ((q_1 + q_2) * n + r_1 + r2)\%n \\ &= (r_1 + r_2)\%n \\ &= (a\%n + b\%n)\%n\end{aligned}$$

Claim: Let a, b and n be integers, with $n \geq 2$. Then $(a * b)\%n = (a\%n\ *\ b\%n)\%n$

I'll let you work out the proof of that.

The significance of these results is that if we are doing a large calculation that ends with a "%n" operation, we can add in more "%n" operations along the way without changing the result (as long as we are careful).

Here are two examples of how we can apply these equalities.

Example 1: What is the value of $(28^5)\ \%13$?

$$\begin{aligned}(28^5)\ \%13 &= (28*28*28*28*28)\ \%13 \\ &= (28\%13 * 28\%13 * 28\%13 * 28\%13 * 28\%13)\ \%13 \\ &= (2*2*2*2*2)\ \%13 \\ &= 32\%13 \\ &= 6\end{aligned}$$

Example 2: What is the value of $((87+144)*(4535+994))\ \%6$?

$$\begin{aligned}((87+144)*(4535+994))\ \%6 &= ((87\%6+144\%6)\%6 * (4535\%6+994\%6)\%6)\%6 \\ &= ((3+0)\%6 * (5+4)\%6)\%6 \\ &= (3*3)\%6 \\ &= 3\end{aligned}$$

This can be particularly useful if we attempting to code these calculations and the numbers we are adding and/or multiplying are so big that we are in danger of exceeding the MaxInt for whatever system we are using.

This is the end of our discussion of basic principles of modular operations. We now return you to your regularly scheduled notes.

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

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

The $\otimes_5$ table is a little more complicated than the $\oplus_5$ but there are certainly patterns here too. The first row is all 0's of course because each entry is just the remainder of dividing 0*b by n ... which is always 0. Each of the other rows is a permutation of $\mathbb{Z}_5$. Is that always going to be true? Also, is there any way to predict what the permutations will be?

Let's look at the table for $\otimes_4$

			b			
	$\otimes_4$		0	1	2	3
	0		0	0	0	0
a	1		0	1	2	3
	2		0	2	0	2
	3		0	3	2	1

Well there goes our idea that all the rows (except for the 0 row) would be permutations of $\mathbb{Z}_4$: the row for 2 just contains 0 2 0 2.

So what property does 5 have that 4 does not? We will see that the crucial property is that **5 is prime.** Now notice that two of the rows of the $\otimes_4$ table **are** permutations of $\mathbb{Z}_4$: the rows for 1 and 3. So what property do 1 and 3 have that 2 does not? We will see that the crucial property is that 1 and 3 are both **relatively prime with 4** (that is, the only factor they share with 4 is 1).

We will explore these relationships and properties in detail over the next couple of classes, so this is just a bit of dramatic foreshadowing.

There are some other simple properties of $\oplus$ and $\otimes$ that we can establish.

0 is the **identity element** for $\oplus$: $0 \oplus a = a \oplus 0 = a \quad \forall a$

We say that 0 is the **additive identity** for $\mathbb{Z}_n$

1 is the identity element for $\otimes$: $1 \otimes a = a \otimes 1 = a \quad \forall a$

We say that 1 is the **multiplicative identity** for $\mathbb{Z}_n$

It is also easy to show that $\oplus$ and $\otimes$ are **associative**:

$$(a \oplus b) \oplus c = a \oplus (b \oplus c)$$

$$(a \otimes b) \otimes c = a \otimes (b \otimes c)$$

I'll prove it for $\oplus$ ... at some point you should satisfy yourself that it is true for $\otimes$ also

$$\begin{aligned}
(a \oplus b) \oplus c &= ((a + b)\ \%n) \oplus c \\
&= ((a + b)\ \%n + c)\ \%n \\
&= (a + b + c)\ \%n \\
&= (a + (b + c)\ \%n)\ \%n \\
&= a \oplus ((b + c)\ \%n) \\
&= a \oplus (b \oplus c)
\end{aligned}$$

Now let's consider modular subtraction, for which we use the symbol $\ominus$

(Incidentally, the LaTeX code for $\ominus$ is "\ominus" which requires me to make the painful pun ... *modular subtraction looks ominous.)*

It would make sense to define $\ominus$ as

x $\ominus$ y = (x – y) % n

and in fact that is exactly where we are going to end up. But we are going to take a slightly round-about route because that will help us when we define $\oslash$ (modular division)

In normal arithmetic, when we write a – b = x, we understand that this is equivalent to writing a = b + x. So when we want to figure out the value of x in the equation a $\ominus$ b = x, it makes sense to say x is the element of $\mathbb{Z}_n$ such that a = b $\oplus$ x

Let's look at the $\oplus$ table for $\mathbb{Z}_5$ again

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

From our definition of $\ominus$ we can compute $2 \ominus 3$ as

$$\begin{aligned} 2 \ominus 3 &= (2 - 3) \ \% \ 5 \\ &= -1 \ \% \ 5 \\ &= 4 \end{aligned}$$

but we can also get this directly from the table for $\oplus_5$

Letting $x = 2 \ominus 3$, we can turn this around, as discussed above, to get $3 \oplus x = 2$

We can find *x* by looking at the *3* row of the table and scanning across until we see *2* . (How do we know we will find it? Because each row of the $\oplus_5$ table is a permutation of $\mathbb{Z}_5$ - so 2 must be in the row somewhere. The number at the top of this column gives us the *x* that adds to *3* to give *2* ... we see it is *4*, which exactly the same result as we got from the formula. In fact, we can show that this method of using the $\oplus$ table to compute $a \ominus b$ will always give the same result as the formula.

Which method is better? They are really both just doing the same thing. If n is small and we have the $\oplus$ table already, perhaps there is a case for using the table. But if n is large, constructing the table (or even just the relevant row of it) might take a long time – we're probably better off using the formula $a \ominus b = (a - b) \ \% \ n$

So what was the point of all of this? Why not simply define $a \ominus b = (a - b) \ \% \ n$ and move on?

The point was that we can define $\ominus$ completely in terms of $\oplus$ (repeating this :
$a \ominus b = \text{ the value of } x \text{ that satisfies } b \oplus x = a$)

Our next task will be to define modular division $\oslash$ ... and we will do it using $\otimes$.