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 $\mathbb{Z}_n = \{0, 1, 2, \ldots, n - 1\}$ 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. In these notes I will use “%” to represent “mod” but you can write “mod” on tests if you prefer it.

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 $a \oplus b = (a + b) \mod n$, and $a \otimes b = (a \cdot b) \mod n$

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

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

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

$$3 \oplus 6 = (3 + 6) \mod 8 = 9 \mod 8 = 1$$
$$3 \otimes 6 = (3 \cdot 6) \mod 8 = 18 \mod 8 = 2$$
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 \( \mathbb{Z}_5 \)

<table>
<thead>
<tr>
<th>( a )</th>
<th>( b )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \oplus_5 )</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>( a )</th>
<th>( b )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \otimes_5 )</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
</tr>
</tbody>
</table>

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 \textbf{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.

The $\otimes_5$ table is a little more complicated but there are certainly patterns there 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 $\otimes_4$

<table>
<thead>
<tr>
<th></th>
<th>$b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a$</td>
<td>0 1 2 3</td>
</tr>
<tr>
<td>0</td>
<td>0 0 0 0</td>
</tr>
<tr>
<td>1</td>
<td>0 1 2 3</td>
</tr>
<tr>
<td>2</td>
<td>0 2 0 2</td>
</tr>
<tr>
<td>3</td>
<td>0 3 2 1</td>
</tr>
</tbody>
</table>

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 $\oplus$: $0 \oplus a = a \oplus 0 = a \ \forall a$

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

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

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

We didn’t do this in class, but 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

$(a \oplus b) \oplus c = ((a + b) \%n) \oplus c$

$\quad = ((a + b)\%n + c) \%n$

$\quad = (a + b + c) \%n$

$\quad = (a + (b + c) \%n) \%n$

$\quad = a \oplus ((b + c) \%n)$

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

$$x \ominus y = (x - y) \mod n$$

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 $\ominus$ (modular division)

---------- Brief side trip: refresher on how “mod” works for negative numbers ----------

Let $n$ be a positive integer $\geq 2$

If $p$ is a positive integer, we all know that $p \mod n$ is just the remainder when $p$ is divided by $n$. For example, $8 \mod 5 = 3$

But what if $p$ is a negative integer? For example, what is $-8 \mod 5$? It can’t be -3 because the answer has to be in the set $\{0, 1, 2, 3, 4\}$ - these are the only values we accept as remainders when dividing by 5.

The formal way to solve this is to give a precise definition of “mod”:

$$p \mod n = x \text{ where } x \in \{0, 1, \ldots, n - 1\} \text{ and } p = k \cdot n + x \text{ for some integer } k$$

Now we can solve $-8 \mod 5$ by trying different values of $k$:

- $k = 0$ gives $-8 = 0 + x$, giving $x = -8$. This fails because -8 is not in $\{0, 1, \ldots, 7\}$
- $k = -1$ gives $-8 = -5 + x$, giving $x = 3$. This fails because -3 is not in $\{0, 1, \ldots, 7\}$
- $k = -2$ gives $-8 = -10 + x$, giving $x = 2$. This works.

So $-8 \mod 5 = 2$

A little bit of thought and algebra shows that for any $n \geq 2$ and any $p$, there is exactly one $(x,k)$ pair that satisfies the requirement, so $p \mod n$ is well-defined.
A more constructive way to think of how we find \( p \% n \) is this:
Find the largest multiple of \( n \) that is \( \leq p \). Call this multiple \( m \). Then \( p \% n = p - m \)

Example: \( 32 \% 9 \): the largest multiple of 9 that is \( \leq 32 \) is 27, so \( m = 27 \).
So \( 32 \% 9 = 32 - 27 = 5 \)

Example: \( -32 \% 9 \): the largest multiple of 9 that is \( \leq -32 \) is -36, so \( m = -36 \).
So \( -32 \% 9 = -32 - (-36) = -32 + 36 = 36 - 32 = 4 \)

In class I drew figures for treating modular numbers as “clock numbers” ... but those are too hard to draw in these notes. The truth is, I prefer the computational method I just described.

---------- Brief side trip ends here ----------------------------------------------------------

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 \( a \oplus b = x \), 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

<table>
<thead>
<tr>
<th></th>
<th>( \oplus_5 )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>( a )</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>

From our definition of \( \oplus \) we can compute \( 2 \oplus 3 \) as

\[
2 \oplus 3 = (2 - 3) \% 5 \\
= -1 \% 5 \\
= 4
\]
but we can also get this directly from the table for $\oplus_5$

Letting $x = 2 \oplus 3$, 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. 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 $a \oplus b$ 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 $a \oplus b = (a - b) \% n$

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 $\otimes$ (repeating this: $a \ominus b = \text{the value of } x \text{ that satisfies } b \ominus x = a$)

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