MAS 4301 – Modular Arithmetic

Let $n \in \mathbb{N}$ and $n > 1$. Recall that
$$n\mathbb{Z} = \{x \in \mathbb{Z} : \exists k \in \mathbb{Z}, x = nk\}.$$
We showed that $n\mathbb{Z} \leq \mathbb{Z}$.

So what does it mean in other words for an integer to belong to $n\mathbb{Z}$?

Recall that a relation on $\mathbb{Z}$ is a subset of $\mathbb{Z} \times \mathbb{Z}$. Here we define the relation R as those
$$R = \{(a, b) \in \mathbb{Z}^2 : a - b \in n\mathbb{Z}\}.$$
We can write $a \sim b$ to mean that $(a, b) \in R$. We also say that a **is congruent to** b **modulo** n when this happens.

We show that R is an equivalence relation, that is, it is *reflexive, symmetric, and transitive.*

Reflexive Is $a \sim a$?

This is asking whether $a - a \in n\mathbb{Z}$. Find a $k \in \mathbb{Z}$ such that $a - a = kn$.

$$k = \underline{\hspace{3cm}}.$$

Symmetric If $a \sim b$, then $b \sim a$.

So we assume that $a \sim b$. By definition, this means $\forall$ / $\exists$ ____ $\in \mathbb{Z}$ such that __________ $= nk$. Next, find a $j \in \mathbb{Z}$ such that $b - a = nj$.

Transitive If $a \sim b$ and $b \sim c$, then $a \sim c$.

We suppose that $a \sim b$ and $b \sim c$. This means that there exist $j, k \in Z$ such that $a - b =$ _______ and ___________ $= nk$. Next, add $(a - b)$ and $(b - c)$ together in two ways. The first way is the easy way and results in $(a - b) + (b - c) =$___________. Add them together a second way by substituting in what they equal and then factor out n. Write this out.

We have thus shown that $\sim$ is an equivalence relation. For an $a \in \mathbb{Z}$, we let $[a] = \{b \in \mathbb{Z} : a \sim b\}$ and call this the **congruence class modulo** n **containing** a**.** The set of all equivalence classes modulo n is denoted by $\mathbb{Z}/n\mathbb{Z}$.

Let $i, j \in \mathbb{N}$ satisfy $0 \le i < j < n$. Can it be the case that $j \sim i$?

It follows that

$$[0], [1], \ldots [n-2], [n-1]$$

are distinct equivalence classes modulo n.

Next, let $a \in Z$. The Division Algorithm states that we can divide a by n and get a remainder that is between 0 and $n-1$. In particular, there are unique $q, r \in Z$ such that

$$a = nq + r$$

and $0 \le r < n$. Subtract r from both sides to get

$$a - r = nq.$$

Do you see then $a \sim r$?

Thus,

$$[0] \cup [1] \cup \ldots \cup [n-1] = \underline{\hspace{3cm}}.$$

You should be able to conclude that $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$ and so

$$|\mathbb{Z}/n\mathbb{Z}| = \underline{\hspace{3cm}}$$

We define an addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$ by

$$[a] \oplus [b] = [a+b]$$

and

$$[a] \otimes [b] = [ab]$$

.

The goal is always to take an equivalence class $[a]$ and find $0 \le r < n$ such that $[a] = [r]$. (Divide a by n and let r be the remainder.)

Example 0.1. Let $n = 7$. What is $[6] \otimes [5]$? Multiply $6 \cdot 5$ and then divide by 7 to be left with a

remainder of ___________. So $[6] \otimes [5] =$ ___________