## Math 3200: Day 28

Recall the theorem from last time:

**Thm:** Let $R$ be an equivalence relation on a set $A$ & let $a,b \in A$. Then $[a]=[b]$ if & only if $aRb$.

Notice that, writing the contrapositive of each direction of the biconditional, we see that $[a] \cap [b] = \emptyset$ if & only if $a \not R b$.

This means that the equivalence classes of $R$ give a partition of $A$ since every element is in some equivalence class (e.g. its own) & equivalence classes are disjoint.

In turn, it's often useful, given a set & an equivalence relation, to think about the set of equivalence classes.

**Examples:**
- The set of equivalence classes of triangles with respect to congruence or similarity.
- The set of equivalence classes of rational numbers w.r.t. equality (like we want to treat $\frac{2}{1}$ & $\frac{4}{2}$ as the same thing).

One that we'll think about a little more carefully is the set of equivalence classes of integers w.r.t. congruence mod $n$, called $\mathbb{Z}_n$.

Namely, $\mathbb{Z}_n = \{[0],[1],[2],\ldots,[n-1]\}$.

Now here's something slightly awesome: in principle, elements of $\mathbb{Z}_n$ are sets, so there's no reason to think you can do anything to them but take unions, intersections, etc.

However, it turns out we can define addition & multiplication on $\mathbb{Z}_n$ in a sensible way.

**Def:** Define the operation $+_n$ on $\mathbb{Z}_n$ as follows: for any $[a],[b] \in \mathbb{Z}_n$, define

$$[a] +_n [b] = [a+b].$$

Likewise, define $\cdot_n$ on $\mathbb{Z}_n$ by

$$[a] \cdot_n [b] = [a \cdot b].$$

Addition & Multiplication tables:

on $\mathbb{Z}_3$:

| $+_3$ | [0] | [1] | [2] |
|---|---|---|---|
| [0] | [0] | [1] | [2] |
| [1] | [1] | [2] | [0] |
| [2] | [2] | [0] | [1] |

| $\cdot_3$ | [0] | [1] | [2] |
|---|---|---|---|
| [0] | [0] | [0] | [0] |
| [1] | [0] | [1] | [2] |
| [2] | [0] | [2] | [1] |

on $\mathbb{Z}_4$:

| $+_4$ | [0] | [1] | [2] | [3] |
|---|---|---|---|---|
| [0] | [0] | [1] | [2] | [3] |
| [1] | [1] | [2] | [3] | [0] |
| [2] | [2] | [3] | [0] | [1] |
| [3] | [3] | [0] | [1] | [2] |

| $\cdot_4$ | [0] | [1] | [2] | [3] |
|---|---|---|---|---|
| [0] | [0] | [0] | [0] | [0] |
| [1] | [0] | [1] | [2] | [3] |
| [2] | [0] | [2] | [0] | [2] |
| [3] | [0] | [3] | [2] | [1] |

Notes: ① Notice that an element of $\mathbb{Z}_n$ can be its own additive inverse, as in the case of $[2] \in \mathbb{Z}_4$

② Also, it's possible for 2 nonzero elements of $\mathbb{Z}_n$ to multiply to give $[0]$. So $[x] \cdot_n [y] = [0]$ does not necessarily mean $[x]=[0]$ or $[y]=0$. Solving equations can be tricky modulo $n$!