Lecture 7

\[ \mathbb{Z} \not\ni 0 \implies \text{Relation on } A \implies \sim \text{ is an e.r.} \implies A/\sim = \{ [a] \mid a \in A \} \]  
\[ \checkmark \text{Reflexive} \]
\[ \checkmark \text{Symmetric} \]
\[ \checkmark \text{Transitive} \]

\[ A = \{8, 11, 17, 32, 52\} \implies a \sim b \iff a, b \text{ belong to the same subset in } A \]

\[ P = \{\{8, 11\}, \{17, 32\}, \{52\}\} \]

\[ A/\sim = \{ [8], [17], [52] \} = P \]

\[ [8] = \{8, 11\} \]
\[ [17] = \{17, 32\} \]
\[ [52] = \{52\} \]
\[
\begin{align*}
[0]_2 &= \{ 2k \mid k \in \mathbb{Z} \} & [1]_2 &= \{ 1 + 2k \mid k \in \mathbb{Z} \} \\
& \text{even} & & \text{odd}
\end{align*}
\]

\[
[0]_3 = \{ 3k \mid k \in \mathbb{Z} \} \quad \text{multiples of 3} \quad [0]_3 = \{ \ldots, -9, -6, -3, 0, 3, 6, 9, \ldots \}
\]

\[
[1]_3 = \{ 1 + 3k \mid k \in \mathbb{Z} \}
\]

\[
[2]_3 = \{ 2 + 3k \mid k \in \mathbb{Z} \} = \{ \ldots, -7, -4, -1, 2, 5, 8, 11, \ldots \}
\]

\[
[3]_3 = \{ 3 + 3k \mid k \in \mathbb{Z} \} = [0]_3
\]
Proposition 13: Let \( n \in \mathbb{N} \setminus \{0,1\} \). There are exactly \( n \) distinct congruence classes; namely \([0], [1], [2], \ldots, [n-1]\).

Proof: Let \( a \in \mathbb{Z} \). By the Division Algorithm \( a = nq + r \) for some \( q, r \in \mathbb{Z} \) and \( 0 \leq r < n \). Therefore, \([a] = [r]\) for some \( r = 0, 1, 2, \ldots, n-1\).

Need to proof that the \( n \) classes above are all distinct (this means, we wish that no two of \( 0, 1, 2, \ldots, n-1 \) are congruent module \( n \)).

Let \( \alpha, \beta \in \{0, 1, 2, \ldots, n-1\} \) so that \( \alpha \neq \beta \). WLOG (without loss of generality) say \( 0 \leq \alpha < \beta \leq n-1 \). Then \( \beta - \alpha > 0 \) and \( \beta - \alpha < n \), i.e. \( n \nmid (\beta - \alpha) \), thus by definition \( \beta \not\equiv_n \alpha \). Then, \([0], [1], [2], \ldots, [n-1]\) are all distinct.
Def: The quotient set of \( \mathbb{Z} \) by \( \equiv_n \) is denoted by \( \mathbb{Z}/n \) (or \( \mathbb{Z}_n \)) and it is read \( \mathbb{Z} \mod n \).

Remarks:
1. \( a \equiv_n b \) iff \( [a]_n = [b]_n \)

\[ \{ a + nk \mid k \in \mathbb{Z} \} = \{ b + nk \mid k \in \mathbb{Z} \} \]

2. Two classes modulo \( n \) are either disjoint or identical.

3. \( \mathbb{Z}/n = \{ [0], [1], [2], \ldots, [n-1] \} \) is a partition of \( \mathbb{Z} \). Exactly \( n \) elements

\[
\mathbb{Z} = \bigcup_{a=0}^{n-1} [a] = [0] \cup [1] \cup [2] \cup \ldots \cup [n-1]
\]
4. Each congruence class can be written in infinitely many ways.

\[ \mathbb{Z}/2 = \{ [0], [1] \} \quad [0] = [2] = [-4] = [2k] \quad \text{for all } k \in \mathbb{Z} \]

\[ \mathbb{Z}/7 = \{ [0], [1], \ldots, [6] \} \quad [1] = [8] = [-6] = [1 + 7k] \quad \text{for all } k \in \mathbb{Z} \]

5. Be careful! The elements of \( \mathbb{Z}/n \) are classes (i.e. subsets of \( \mathbb{Z} \)), not single integers.

5 \notin \mathbb{Z}/6 \quad \text{[5] \in \mathbb{Z}/6}

**Question:** Do we have addition in \( \mathbb{Z}/n \)?

**Do we have multiplication in \( \mathbb{Z}/n \)?**

~

That’d be weird!

Addition and multiplication between sets.

**Answer:** Yes, we do!!!
Let \([a], [b] \in \mathbb{Z}/n\). We define

**Addition in \(\mathbb{Z}/n\):** \([a] \oplus [b] := [a+b]\)

**Multiplication in \(\mathbb{Z}/n\):** \([a] \odot [b] := [a \cdot b]\)

**Ex:** Consider \(\mathbb{Z}/5 = \{[0], [1], [2], [3], [4]\}\)

\([0] \oplus [1] = [0+1] = [1]\)
\([4] \odot [4] = [16] \equiv [1]\)

Possible problem: Do we get the same answer if we use different representatives? For instance,

\([5] \oplus [6] = [11] = [1]\)
\([9] \odot [-1] = [-9] = [1]\)

11 \equiv 1
-9 \equiv 1

Apparently, we do. But we must prove it!
Theorem 14: The operations of addition and multiplication in \( \mathbb{Z}/n \) are well-defined.

Explicitly: They do not depend on the choices of representatives for the classes involved:

If \( a, b, c, d \in \mathbb{Z} \) with \([a] = [b]\) and \([c] = [d]\),

then \([a] \oplus [c] = [b] \oplus [d]\) and \([a] \odot [c] = [b] \odot [d]\).

Proof: Read Thm 2.1 and Thm 2.6 in Hungerford's book.

Definition: Let \( k \in \mathbb{N} \) and \([a] \in \mathbb{Z}/n\).

\[
[k][a] := \underbrace{[a] \oplus \ldots \oplus [a]}_{k\text{-times}} \quad [a]^k := \underbrace{[a] \odot \ldots \odot [a]}_{k\text{-times}}
\]

\([0][a] := [0]\) \quad [a]^0 := [1]\]
Ex.: In $\mathbb{Z}/7$:

$$3 [1] = [1] \oplus [1] \oplus [1] = [1+1+1] = [3]$$


$$0 [6] = [0]$$

$$[3]^0 = [1]$$

Remark: $k [a] = [ka]$  \hspace{1cm} 0 [a] = [0\cdot a]$

$$[a]^k = [a^k]$$  \hspace{1cm}  $[a]^0 = [a^0]$  

As you would expect!