The number system $\mathbf{Z}_n$

MTH 350 -- Module 5A

Agenda

- Daily Prep 5A review: Congruence classes mod n, equivalence relations
- The set $\mathbf{Z}_n$ and addition, multiplication on this set
- Main activity: Constructing operation tables for $\mathbf{Z}_n$
- What axioms are satisfied by the number system $\mathbf{Z}_n$?

Below are some relations (all denoted $\sim$) on the set of integers. Which ones are REFLEXIVE? Select all that apply.

- $a \sim b$ if and only if $a < b$
- $a \sim b$ if and only if $a \leq b$
- $a \sim b$ if and only if $a | b$
- $a \sim b$ if and only if a and b have the same ones digit

Tc 0

Below are some relations (all denoted $\sim$) on the set of integers. Which ones are SYMMETRIC? Select all that apply.

- $a \sim b$ if and only if $a < b$
- $a \sim b$ if and only if $a \leq b$
- $a \sim b$ if and only if $a | b$
- $a \sim b$ if and only if a and b have the same ones digit

Below are some relations (all denoted $\sim$) on the set of integers. Which ones are TRANSITIVE? Select all that apply.

$a \sim b$ if and only if $a < b$

$a \sim b$ if and only if $a \leq b$

$a \sim b$ if and only if $a | b$

$a \sim b$ if and only if a and b have the same ones digit

Tc 0

Recall that $[a]_n$ means the congruence class of integers modulo n where n is a natural number. The congruence class $[7]_3$ is

- 1
- 7
- $\{1\}$
- $\{7\}$
- $\{1, 4, 7, 10, 13, \cdots\}$
- $\{\cdots, -5, -2, 1, 4, 7, 10, 13, \cdots\}$

To 0

Which of the following is/are equal to $[7]_3$? Select all that apply.

- $[1]_3$
- $[3]_7$
- $[7]_6$
- $[13]_3$
- (Select this if none of these are equal to $[7]_3$)

To 0

The set $\mathbb{Z}_5$ is

$\{0, 1, 2, 3, 4\}$

$\{0, 1, 2, 3, 4, 5\}$

$\{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$

$\{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5, [5]_5\}$

$\{\cdots, -15, -10, -5, 0, 5, 10, 15, \cdots\}$

Tc 0

SMQ’s of note

Facts about equivalence relations

Definition 5.5. Let $\sim$ be an equivalence relation on a nonempty set S, and let $a \in S$. The **equivalence class of** a (with respect to $\sim$), denoted $[a]_\sim$, is the set of all elements of S that are related to a by $\sim$. More precisely,

$$[a]_\sim = \{x \in S : x \sim a\}.$$

The equivalence class of a is the set of everything that is related to a.

If a *belongs to* [b], then a and b have equal classes.

Theorem 5.6. *Let S be a nonempty set, and let $\sim$ be an equivalence relation on S. Then S can be written as the disjoint union of the distinct equivalence classes corresponding to $\sim$. That is, the equivalence classes corresponding to $\sim$ are pairwise disjoint, and every element of S belongs to exactly one equivalence class. In particular:*

(i) *For all $a, b \in S$, if $[a] \neq [b]$, then $[a] \cap [b] = \emptyset$.*

(ii) *For all $a \in S$, $a \in [a]$.*

(iii) *For all $a \in S$, if $a \in [b]$ for some $b \in S$, then $[a] = [b]$.*

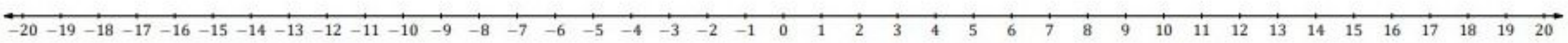
Two equivalence classes must either be equal or have no elements in common. ("disjoint")

There's no such thing as an "empty class" because [a] must always at least contain a itself.

Lemma 5.7. *Let S be a nonempty set, and let $\sim$ be an equivalence relation on S. Then for all $a, b \in S$, $[a] = [b]$ if and only if $a \sim b$.*

If two objects are "related" then their classes are equal, and vice versa.

Example: Integer congruence modulo 5



Arithmetic in $\mathbf{Z}_n$

The number system $\mathbf{Z}_n$

Example: $\mathbf{Z}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$
or just $\{[0], [1], [2], [3], [4]\}$ if the context makes it clear

Definition 5.10. For every integer $n \geq 2$, the **integers modulo** n, denoted $\mathbb{Z}_n$, is the set of the n distinct congruence classes of $\mathbb{Z}$ modulo n, *i.e.*,

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

We can make $\mathbb{Z}_n$ into a number system by defining an addition and multiplication on the set. There is a seemingly natural way to do this:

$$[a] + [b] = [a+b] \text{ and } [a] \cdot [b] = [a \cdot b]$$

Example: In $\mathbf{Z}_5$:
$[4] + [3] = [7] = [2]$. ← The result can always be written as an element of $\mathbf{Z}_5$
$[4] * [2] = [8] = [3]$ ← Ditto

Quick practice

Perform all the following calculations and reduce each answer appropriately:

$[1]_3 + [2]_3$		$[2]_3 \cdot [2]_3$	
$[1]_{10} + [2]_{10}$		$[4]_5 \cdot [3]_5$	
$[0]_9 + [8]_9$		$[9]_{10} \cdot [8]_{10}$	
$[1]_9 + [8]_9$		$[2]_4 \cdot [2]_4$	
$[15]_{26} + [22]_{26}$		$[13]_{26} \cdot [5]_{26}$	

Operation tables

Question: Is this [1]+[2] or [2]+[1]? Does it matter? Will it *ever* matter?

Since $\mathbf{Z}_n$ is finite, we can write down **all possible sums and products** in **tables.**

For $\mathbf{Z}_3$:

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

·	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Theorem: Addition and multiplication in $\mathbf{Z}_n$ are commutative.

ACTIVITY: Write out the operation tables for $\mathbf{Z}_n$, n = 4, 5, …, 11. $\mathbf{Z}_2$ and $\mathbf{Z}_3$ are provided.

Group 1:

What symmetries, patterns, etc. do you notice that might help?

ACTIVITY

Write out the operation tables for $\mathbf{Z}_n$, n = 4, 5, …, 11 on the spreadsheet. $\mathbf{Z}_2$ and $\mathbf{Z}_3$ are provided.

- Group 1: n = 4 and 11
- Group 2: n = 5 and 10
- Group 3: n = 6 and 9
- Group 4: n = 7 and 8

This is a lot of typing 😩 Do you notice any patterns or symmetries that could help?

What do you notice? What do you wonder about?