16. Equivalence Relations, Equivalence Classes, & Partitions

- An **equivalence relation** on a set A is a relation that is reflexive, symmetric, and transitive.
- Suppose $\mathcal{R}$ is an equivalence relation on A. For each element $a \in A$, the **equivalence class of** a is the set $[a]_{\mathcal{R}} = \{x \in A : a \,\mathcal{R}\, x\}$

CONGRUENCE MODULO m: AN EQUIVALENCE RELATION ON INTEGERS

Let m be a positive integer, and let $x \in \mathbb{Z}$ be any integer.

- The **remainder of** $x \pmod{m}$ is the unique integer r such that $0 \leq r < m$ and

$$\boxed{x = km + r} \qquad (k \in \mathbb{Z})$$

- We call m the **modulus**.
- Two integers a and b are called **congruent modulo** m if the remainder of $a \pmod{m}$ equals the remainder of $b \pmod{m}$.

Notation: For short, we write $a \equiv b \pmod{m}$ whenever a and b are congruent moduluo m.

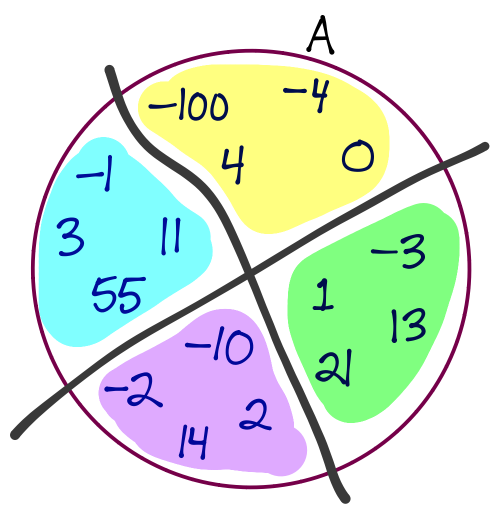
Example 16.1. Let $m = 4$ be our modulus. For each element of the following set A, compute its remainder $\pmod{4}$. Determine which integers in A are congruent to each other modulo 7.

$$A = \{-100,\ -10,\ -4,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ 4,\ 11,\ 13,\ 14,\ 21,\ 55\}$$

remainder (mod 4) 0 2 0 1 2 3 0 1 2 3 0 3 1 2 1 3

x	$=$	$km + r$
-100	$=$	$(-25)(4)+0$
-10	$=$	$(-3)(4)+2$
-4	$=$	$(-1)(4)+0$
-3	$=$	$(-1)(4)+1$
-2	$=$	$(-1)(4)+2$
-1	$=$	$(-1)(4)+3$
0	$=$	$(0)(4)+0$
1	$=$	$(0)(4)+1$

x	$=$	$km + r$
2	$=$	$(0)(4)+2$
3	$=$	$(0)(4)+3$
4	$=$	$(1)(4)+0$
11	$=$	$(2)(4)+3$
13	$=$	$(3)(4)+1$
14	$=$	$(3)(4)+2$
21	$=$	$(5)(4)+1$
55	$=$	$(13)(4)+3$



Theorem 16.2. Let a and b be integers, and let m be a positive integer.

Then $a \equiv b \pmod{m}$ if and only if m divides $a - b$.

Exercise 16.3. Prove Theorem 16.2.

* These notes are solely for the personal use of students registered in MAT1348.

Example 16.4. Let m be a positive integer.

a) Prove that $\equiv \pmod{m}$ is an equivalence relation on $\mathbb{Z}$.

We will use the fact that $a \equiv b \pmod{m} \Longleftrightarrow m \mid (a-b)$ (Theorem 16.2)

[reflexive] Let $x \in \mathbb{Z}$.

Then $x - x = 0 = (0)(m) + 0$ $\therefore$ $m \mid (x-x)$ $\therefore$ $x \equiv x \pmod{m}$

we proved $[x \in \mathbb{Z}] \rightarrow [x \equiv x \pmod{m}]$ $\therefore$ $\equiv \pmod{m}$ is reflexive.

[Symmetric] Let $x, y \in \mathbb{Z}$.

Assume $x \equiv y \pmod{m}$ (goal: prove $y \equiv x \pmod{m}$).

Then $m \mid (x-y)$ (by Theorem 16.2)

$\Longrightarrow$ $x - y = km$ for some integer k (def of divides)

$\Longrightarrow$ $y - x = (-k)m$. Since $k \in \mathbb{Z}$, so too is $-k \in \mathbb{Z}$

$\therefore$ $m \mid (y-x)$ $\therefore$ $y \equiv x \pmod{m}$ (by Theorem 16.2)

we proved $[x \equiv y \pmod{m}] \longrightarrow [y \equiv x \pmod{m}]$ $\therefore$ $\equiv \pmod{m}$ is symmetric.

[transitive] Let $x, y, z \in \mathbb{Z}$

Assume $x \equiv y \pmod{m}$ and $y \equiv z \pmod{m}$. (goal: prove $x \equiv z \pmod{m}$).

Then $m \mid (x-y)$ and $m \mid (y-z)$ (by Theorem 16.2)

$\Longrightarrow$ $x - y = km$ and $y - z = \ell m$ for some integers $k, \ell \in \mathbb{Z}$ (def of divides)

$\therefore$ $x - z = km + y - (\ell m - y) = (k - \ell)m$. Since $k, \ell \in \mathbb{Z}$, so too is $k - \ell \in \mathbb{Z}$

$\therefore$ $m \mid (x-z)$ $\therefore$ $x \equiv z \pmod{m}$ (by Theorem 16.2)

we proved $[x \equiv y \pmod{m} \wedge y \equiv z \pmod{m}] \longrightarrow [x \equiv z \pmod{m}]$

$\therefore$ $\equiv \pmod{m}$ is transitive

Since it's reflexive, symmetric, and transitive,

$\equiv \pmod{m}$ is indeed an equivalence relation on $\mathbb{Z}$. $\blacksquare$

b) Let $m = 4$ be our modulus, and let

$$A = \{-100,\ -10,\ -4,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ 4,\ 11,\ 13,\ 14,\ 21,\ 55\}.$$

Note: Since congruence modulo 4 is an equivalence relation on the set of all integers, it follows that it also defines an equivalence relation on A.

Determine all of the distinct equivalence classes of the elements of A with respect to the equivalence relation $\equiv \pmod 4$.

$$[-100]_{\equiv (\mathrm{mod}\ 4)} = \{-100, -4, 0, 4\}$$

$$[-10]_{\equiv (\mathrm{mod}\ 4)} = \{-10, -2, 2, 14\}$$

$$[-3]_{\equiv (\mathrm{mod}\ 4)} = \{-3, 1, 13, 21\}$$

$$[-1]_{\equiv (\mathrm{mod}\ 4)} = \{-1, 3, 11, 55\}$$

b) What are the distinct equivalence classes of the equivalence relation $\equiv \pmod 4$ on the set of all integers?

$$[0]_{\equiv (\mathrm{mod}\ 4)} = \{n \in \mathbb{Z} : n \equiv 0 \pmod 4\}$$

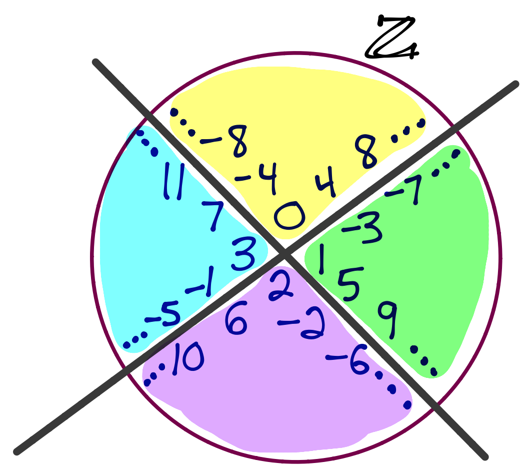
$$= \{n \in \mathbb{Z} : \text{the remainder of } n \ (\mathrm{mod}\ 4) \text{ is } 0\}$$

$$= \{\ldots, -8, -4, 0, 4, 8, 12, \ldots\}$$

Similarly, $[1]_{\equiv (\mathrm{mod}\ 4)} = \{\ldots, -7, -3, 1, 5, 9, 13, \ldots\}$

$$[2]_{\equiv (\mathrm{mod}\ 4)} = \{\ldots, -10, -6, -2, 2, 6, 10, \ldots\}$$

$$[3]_{\equiv (\mathrm{mod}\ 4)} = \{\ldots, -9, -5, -1, 3, 7, \ldots\}$$



General Observations on Equivalence Classes of an Equivalence Relation.

Let $\mathcal{R}$ be an equivalence relation on a set A. Then:

i. $a \in [a]_{\mathcal{R}}$ for all $a \in A$.

ii. $[a]_{\mathcal{R}} = [b]_{\mathcal{R}}$ if and only if $(a, b) \in \mathcal{R}$.

iii. $[a]_{\mathcal{R}} \cap [b]_{\mathcal{R}} = \emptyset$ if and only if $(a, b) \notin \mathcal{R}$.

*In fact, these properties turn out to give us what is called a **partition** of A.

Partitions

A **partition** of a set A is a collection $\mathcal{P} = \{S_1, S_2, \dots\}$ of subsets $S_i \subseteq A$ such that the following three properties hold:

i. $S_i \neq \emptyset$ for all i (Si are non-empty subsets of A)

ii. $A = S_1 \cup S_2 \cup \cdots$ (union of all Si is all of A)

iii. $S_i \cap S_j = \emptyset$ for all $i \neq j$ (pairwise disjoint)

Example 16.5. Let $A = \{1, 2, 3, 4, 5\}$

$\mathcal{P}_1 = \{\{3,4,1\}, \{2\}, \{5\}\}$ is a partition of A.

$\mathcal{P}_2 = \{\{3,4\}, \{2\}, \{5\}\}$ is not a partition of A (fails property ii)

$\mathcal{P}_3 = \{\{3,4,1\}, \{2\}, \emptyset, \{5\}\}$ is not a partition of A (fails property i)

$\mathcal{P}_4 = \{\{3,4,1\}, \{1,2\}, \{5\}\}$ is not a partition of A (fails property iii)

Example 16.6. Here are two partitions of $\mathbb{Z}$:

$\mathcal{P}_1 = \{\mathbb{Z}^-, \{0\}, \mathbb{Z}^+\}$ is a partition of $\mathbb{Z}$

$\mathcal{P}_2 = \{\{0\}, \{1,-1\}, \{2,-2\}, \{3,-3\}, \dots\}$ is a partition of $\mathbb{Z}$

Correspondence between Equivalence Relations and Partitions

Theorem 16.7. Let A be a set.

(I) If $\mathcal{R}$ is an equivalence relation on A, then the collection of equivalence classes of $\mathcal{R}$ forms a partition of A.

(II) If $\mathcal{P} = \{S_1, S_2, \dots\}$ is a partition of A, then the relation $\mathcal{S}$ on A defined by the rule

$$\text{For all } a, b \in A \quad (a,b) \in \mathcal{S} \iff \{a,b\} \subseteq S_i \quad \text{for some } S_i \in \mathcal{P}$$

is an equivalence relation on A.

Example 16.8. Let $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ and let $\mathcal{R}$ be the relation on A defined by the rule

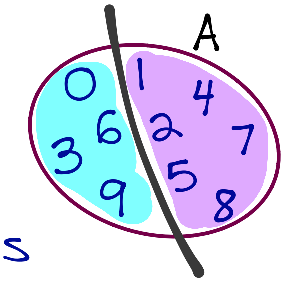
for all $x, y \in A \quad x \mathcal{R} y \quad$ if and only if $\quad 3 \mid (x^2 + 2y^2)$.

Exercise: Prove that $\mathcal{R}$ is an equivalence relation on A.

Determine the corresponding partition of A into equivalence classes.

$[0]_{\mathcal{R}} = \{0,3,6,9\}$

$[1]_{\mathcal{R}} = \{1,2,4,5,7,8\}$

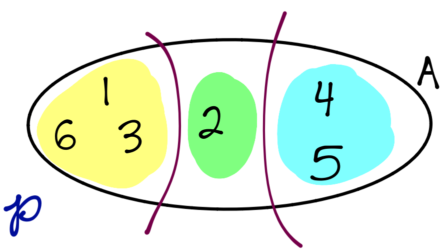


$\therefore$ the partion of A into equivalence classes of $\mathcal{R}$ is

$$\mathcal{P} = \Big\{ \{0,3,6,9\}, \{1,2,4,5,7,8\} \Big\}$$

Example 16.9. Let $A = \{1, 2, 3, 4, 5, 6\}$.

Here is a partition of A: $\mathcal{P} = \{ \overset{S_1}{\{1,3,6\}}, \overset{S_2}{\{2\}}, \overset{S_3}{\{4,5\}} \}$



Here is the corresponding equivalence relation $\mathcal{S}$ on A:

rule for $\mathcal{S}$: $\quad (a,b) \in \mathcal{S} \iff \{a,b\} \subseteq S_i$ for some $S_i \in \mathcal{P}$

$\mathcal{S}$ as a finite list:

$$\mathcal{S} = \{ \underbrace{(1,1),(1,3),(1,6),(3,1),(3,3),(3,6),(6,1),(6,3),(6,6)}_{\text{Corresponds to } \{a,b\} \subseteq S_1 = \{1,3,6\}}, \underbrace{(2,2)}_{\text{Corresponds to } \{a,b\} \subseteq S_2 = \{2\}}, \underbrace{(4,4),(4,5),(5,4),(5,5)}_{\text{Corresponds to } \{a,b\} \subseteq S_3 = \{4,5\}} \}$$

Exercise 16.10. Consider the **equivalence relation** $\mathcal{R}$ on the set $A = \{-6, -5, -2, 0, 1, 3, 5, 7\}$ defined as follows:

$$a \mathcal{R} b \quad \Longleftrightarrow \quad a \equiv b \pmod 5 \quad \text{or} \quad a \equiv -b \pmod 5$$

i. Prove that $\mathcal{R}$ is an equivalence relation on A.
ii. Determine the partition of A into equivalence classes with respect to $\mathcal{R}$

Study Guide

Important terms and concepts:	**equivalence relations:** **equivalence classes:**	reflexive, symmetric, & transitive $[a]_{\mathcal{R}} = \{x \in A : x \mathcal{R} a\}$
partition $\mathcal{P} = \{S_1, S_2, \dots\}$ **of a set** A 1. $S_i \neq \emptyset$ for all i	2. $A = S_1 \cup S_2 \cup \cdots$	3. $S_i \cap S_j = \emptyset$ for all $i \neq j$
Exercises		Sup.Ex. §7 # 1b, 2, 3, 4, 6, 8, 9, 10, 11 Rosen §9.5 # 1, 3, 7, 11, 15, 25, 26, 29, 41, 47