§11.5 The Integers Modulo n

We now focus on one particular relation: $\equiv \pmod n$

Equivalence modulo n

Thm For any $n \in \mathbb{N}$, the relation $R = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} : x \equiv y \pmod n\}$

i.e. $xRy \iff x \equiv y \pmod n$

is an equivalence relation on $\mathbb{Z}$.

Proof:

Reflexivity $(\forall x \in \mathbb{Z},\ xRx)$

Let $x \in \mathbb{Z}$.

Since $x - x = 0 \cdot n$, we have $n \mid x - x$ and so $x \equiv x \pmod n$.

Symmetry $(\forall x,y \in \mathbb{Z},\ xRy \Rightarrow yRx)$

Let $x,y \in \mathbb{Z}$ and suppose $x \equiv y \pmod n$.

Then $x - y = na$, $a \in \mathbb{Z}$, and so $y - x = n(-a)$, $-a \in \mathbb{Z}$.

Therefore $y \equiv x \pmod n$.

Transitivity $(\forall x,y,z \in \mathbb{Z},\ (xRy \wedge yRz) \Rightarrow xRz)$

Let $x,y,z \in \mathbb{Z}$ and suppose $x \equiv y \pmod n$ & $y \equiv z \pmod n$.

Then $\exists a,b \in \mathbb{Z}$ such that $x - y = na$ and $y - z = nb$.

Then $x - z = (x-y) + (y-z) = na + nb = n(a+b)$.

Since $a+b \in \mathbb{Z}$, this shows $n \mid x - z$ & so $x \equiv z \pmod n$. ∎

Note: The equivalence relation $\equiv \pmod n$ on $\mathbb{Z}$ partitions $\mathbb{Z}$ into n equivalence classes:

$$[0] = \{x \in \mathbb{Z} : x \equiv 0 \pmod n\} = \{\dots, -2n, -n, 0, n, 2n, \dots\}$$
$$[1] = \{x \in \mathbb{Z} : x \equiv 1 \pmod n\} = \{\dots, -2n+1, -n+1, 1, n+1, 2n+1, \dots\}$$
$$[2] = \{x \in \mathbb{Z} : x \equiv 2 \pmod n\} = \{\dots, -2n+2, -n+2, 2, n+2, 2n+2, \dots\}$$
$$\vdots$$
$$[n-1] = \{x \in \mathbb{Z} : x \equiv n-1 \pmod n\} = \{\dots, -n-1, -1, n-1, 2n-1, 3n-1, \dots\}$$

Def: The set of n equivalence classes formed by the equivalence relation $\equiv \pmod n$ on $\mathbb{Z}$ is

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

"The integers modulo n" or "$\mathbb{Z}$ mod n"

ex. $\equiv \pmod 3$ PARTITIONS $\mathbb{Z}$ INTO 3 EQUIVALENCE CLASSES: $[0], [1], [2]$.

$\mathbb{Z}_3 = \{[0], [1], [2]\} = \{[0], [1], [-1]\}$

$= \{[27], [37], [47]\}$, ETC.

NOTE: THE ELEMENTS OF $\mathbb{Z}_n$ ARE SETS (EQUIVALENCE CLASSES), NOT INTEGERS.

HOWEVER, THERE IS A SIMPLE WAY TO DEFINE BOTH ADDITION & MULTIPLICATION OF ELEMENTS OF $\mathbb{Z}_n$:

> ADDITION: DEFINE $[a] + [b] = [a + b]$
>
> MULTIPLICATION: DEFINE $[a] \cdot [b] = [a \cdot b]$

ex. CONSIDER THE SET $\mathbb{Z}_{10} = \{[0], [1], \ldots, [9]\}$.

(EASY) $[2] + [4] = [6]$
$[2][4] = [8]$

(MEDIUM) $[8] + [6] = [14] = [4]$ WE PREFER TO STICK WITH STANDARD REPRESENTATIVES / LABELS: $0 - (n-1)$.
$[8][6] = [48] = [8]$

(HARD) $[1256] + [6739] = [6] + [9] = [15] = [5]$
$[1256][6739] = [6][9] = [54] = [4]$

WHY DOES THIS WORK?

THM: SUPPOSE $[a], [b] \in \mathbb{Z}_n$.
IF $[a] = [a']$ & $[b] = [b']$ THEN (a) $[ab] = [a'b']$, AND
(b) $[a+b] = [a'+b']$

PROOF: (a) RECALL THM 11.1: $[x] = [y] \iff x R y$.
SO, TO SHOW $[ab] = [a'b']$, IT IS ENOUGH TO SHOW $ab \equiv a'b' \pmod n$.

SINCE $[a] = [a']$ & $[b] = [b']$, BY DEFINITION,
$a \equiv a' \pmod n$ & $b \equiv b' \pmod n$.
THUS $a - a' = nx$ AND $b - b' = ny$ FOR SOME $x, y \in \mathbb{Z}$.
THAT IS $a = a' + nx$ AND $b = b' + ny$.
THEN $ab = (a' + nx)(b' + ny) = a'b' + n(a'y + b'x + nxy)$.

Set $z = a'y + b'x + nxy \in \mathbb{Z}$
Then, $ab - a'b' = nz$, i.e. $ab \equiv a'b' \pmod{n}$.
$\therefore$ It follows from Thm 11.1 that $[ab] = [a'b']$.

(b) Homework ☺

§11.6 Relations Between Sets

Please read this section on your own.

It is only 1 page.