Week 3

Last Friday

Theorem S a set

$\{$ equivalence relations on S $\}$

R $\longleftrightarrow$ $\{$ partitions P on S $\}$

$R \longrightarrow \{ [a]_R \}_{a \in S}$.

Def Let n be a positive integer

Define a relation $\equiv$ on $\mathbb{Z}$ ($|\mathbb{Z}|$)

$a, b \in \mathbb{Z}$

by

$$a \equiv b \pmod{n}$$

(a is congruent to b mod n)

$\Leftrightarrow$ $b - a$ is divisible by n.

(i.e. $\exists\, r \in \mathbb{Z}$ s.t.

$b - a = n \cdot r$)

Prop 10 $\equiv$ is an equivalence relation on $\mathbb{Z}$.

Pf $\forall a \in \mathbb{Z}$

- $a \equiv a \pmod{n}$?

  Yes! because $a - a = 0$ is divisible by n.

- If $a \equiv b \pmod{n}$ (aRb) then $b \equiv a \pmod{n}$?

Yes! because

$a \equiv b \mod n$

$\Rightarrow \exists r \in \mathbb{Z}$ s.t. $b - a = r \cdot n$

$\Rightarrow a - b = (-r) \cdot n$

$\Rightarrow b \equiv a \mod n.$

$n = 7$

$2 \equiv 9 \mod 7$

$9 - 2 = 7$ is divisible by 7

$4 \equiv 18 \mod 7$

$18 - 4 = 14$ is divisible by 7.

- If $a \equiv b \mod n$ $(a \not\mathcal{R} b)$

  $b \equiv c \mod n$ $(b \not\mathcal{R} c)$

  Then

  $a \equiv c \mod n$? $(a \not\mathcal{R} c)$

Since $a \equiv b \mod n$, there exists $r \in \mathbb{Z}$ s.t. $b - a = r \cdot n$. ... (*)

Similarly, since $b \equiv c \mod n$,

there exists $s \in \mathbb{Z}$ s.t.

$$c - b = s \cdot n.$$

... (**)

$$c - a = c - b + b - a$$

$$= s \cdot n + r \cdot n \quad (*)\,(**)$$

$$= (r+s) \cdot n$$

Therefore, n divides $c - a$.

i.e. $c \equiv a \pmod{n}$. $\square$

Def Let n be a fixed positive integer

We will write

$$[a]_n \quad \text{or} \quad [a]$$

to mean the equivalence class represented by a, i.e.

$$[a]_n := \{b \in \mathbb{Z} \mid a \equiv b \bmod n\}.$$

$$(= \{b \in S \mid a R b\})$$

We'll write

$\mathbb{Z}_n$ to mean

the set of all equivalence classes

w.r.t.

the relation "$\equiv \bmod n$"

on $\mathbb{Z}$.

In particular, if n is a prime

number p,

we'll write $\mathbb{F}_p$ instead.

Prop 11 The cardinality of $\mathbb{Z}_n$ is n.

Equivalently, there are exactly n equivalence classes in $\mathbb{Z}_n$.

Rk $\{[a]\}_{a \in \mathbb{Z}}$

So lots of $[a]$'s are identified.

Example $n = 5$

$$
\begin{array}{ccccc}
\vdots & & & & \\
[-4]_5 & [-3]_5 & [-2]_5 & [-1]_5 & [0]_5 \\
\| & \| & \| & \| & \| \\
[1]_5 & [2]_5 & [3]_5 & [4]_5 & [5]_5 \\
\| & \| & \| & \| & \| \\
[6]_5 & [7]_5 & \cdots & &
\end{array}
$$

We saw in Week 2 that

$$a \not\equiv b \iff [a] = [b].$$

i.e.

$$a \equiv b \bmod n \iff [a]_n = [b]_n$$

The left-most column:

Since

$$1 \equiv -4 \mod 5,$$

(because $(-4) - 1$ is divisible by 5)

$$[1]_5 = [-4]_5$$

Similarly

$$1 \equiv 6 \mod 5,$$

$$[1]_5 = [6]_5$$

Example $n=6$

$\mathbb{Z}_6$ should have 6 equiv

$[-6]$ $[-5]$ ... classes

$\|$ $\|$

$[0]_6$, $[1]_6$, $[2]_6$, $[3]_6$, $[4]_6$, $[5]_6$

$\|$ $\|$

$[6]$ $[7]$ ...

Proof of Prop 11

* Every integer s belongs to exactly one of the

equivalence classes

$$\{ [0]_n, [1]_n, \cdots, [n-1]_n \}$$

* $[0], [1], \cdots, [n-1]$

are all distinct.

Let's check the first *.

From Week 1,

$\Rightarrow s = qn + r$

for some $q \in \mathbb{Z}$

$0 \leq r < n-1 <$

Mistake

This is $n!$

$s' \in [r] := \{ t \in \mathbb{Z} \mid r \equiv t \mod n \}$

Why? This is because

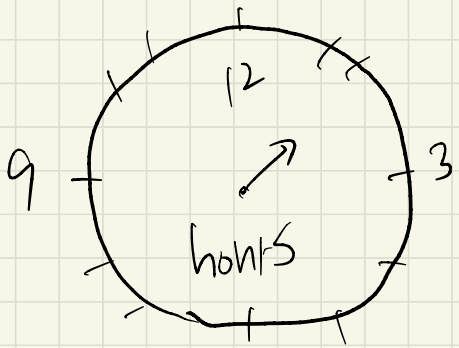
$$r - s' = (-q) \cdot n$$

is divisible by n.

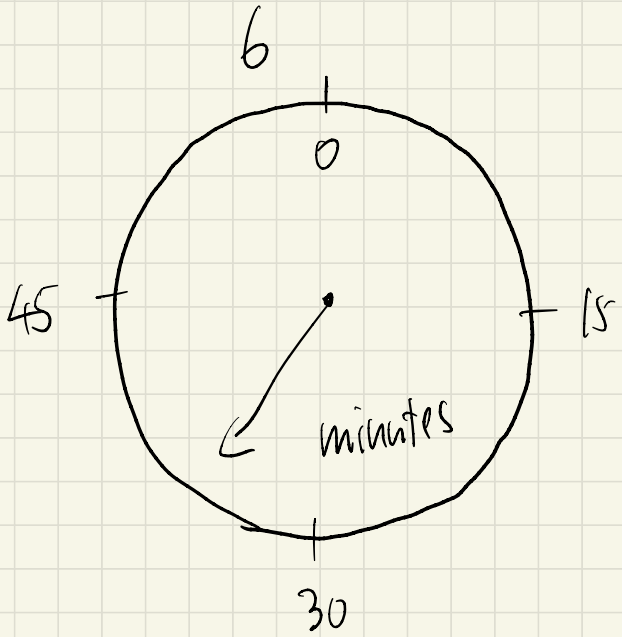
See the notes for the second $*$.

□.

In real life, we see lots of $\mathbb{Z}_n$.



$\mathbb{Z}_{12}$



$\mathbb{Z}_{60}$

Theorem 9 says we have a partition of $\mathbb{Z}$.

Indeed, $\{[0]_n, [1]_n, \ldots, [n-1]_n\}$

is the partition Theorem 9 gives us.

$[a] = [a]_R = \{b \in S \mid aRb\}$

$\Rightarrow S = \mathbb{Z}$, $R = "\equiv \pmod n"$

$\{b \in \mathbb{Z} \mid a \equiv b \pmod n\}$

3.3 Arithmetic with congruence classes

$\mathbb{Z}_n :=$ the set of equiv. classes w.r.t. "$\equiv \bmod n$"

Elements are

$$[a]_n = \{ b \in \mathbb{Z} \mid a \equiv b \bmod n \}$$

$$\Updownarrow$$

$$n \mid (b-a)$$

We want to add

subtract

multiply

elements in $\mathbb{Z}_n$, i.e.

want to define "+"

"−"

& "×" in $\mathbb{Z}_n$.

addition

$\mathbb{Z}_n$

$$[a]_n + [b]_n \overset{\text{def}}{=} [a+b]_n$$

$\mathbb{Z}_n$

Subtraction

$$[a]_n - [b]_n \overset{\text{def}}{=} [a-b]_n$$

$\uparrow$

$\mathbb{Z}_n$

multiplication

$$[a]_n \cdot [b]_n \overset{\text{def}}{=} [ab]_n$$

No division!

It does NOT make sense to define $\left[\frac{a}{b}\right]$ when

"$[a]$ divides $[b]$"

$$\frac{[a]}{[b]} = \left[\frac{a}{b}\right]$$

Example $n=3$

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

$$[1] + [2] = [1+2] = [3]$$

$$= [0]$$

$[5] = [2]$ because $5 \equiv 2 \pmod 3$

$$[2] + [5] = [2] + [2]$$

$$\overset{\text{def}}{=} [2+2]$$

$$= [4]$$

$$= [1]$$

$[4] = [1]$ because $4 \equiv 1 \bmod 3$

$$[2] \cdot [2] = [2 \cdot 2]$$

$$= [4] = [1].$$

$n=6$ Let's work out addition table:

Addition table

$+_{\mathbb{Z}_6}$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$

Multiplication table

$\mathbb{Z}_6$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[10] = [4]
[3]	[0]	[3]	[0]	[3]	[12] = [0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

We do know that

2 divides 6

so $\frac{6}{2} = 3$

but can we define

$$\frac{[6]_6}{[2]_6} = [3]_6 \; ??$$

In the first place: $[6]_6 = [0]_6$

$$\frac{[0]}{[2]} \stackrel{?}{=} \left[\frac{0}{2}\right] = [0] \neq [3]$$

If we want to make sense of "dividing", we'll do the following.

$[a]$ divides $[b]$

if $\exists\, c \in \mathbb{Z}$

s.t. $[b] = [a][c]$

so $[c]$ plays the role of "$\frac{[b]}{[a]}$"

If $[2]$ divides $[5]$,

then there should be $[c]$

s.t. $[5] = [2] \cdot [c] = [2c]$.

For example,

in $\mathbb{Z}_3$, $[1]_3 + [2]_3 = [3]_3 = [0]_3$

but I could have used

$[4]_3$ instead of $[1]_3$

to "define" +

$$[4]_3 + [2]_3 = [6] = [0]$$

This example tells you that our definition of addition does NOT depend on our choice of representatives.

More rigorously:

let $a, a', b \in \mathbb{Z}$

&

suppose $a \equiv a' \pmod{n}$.

Then $[a] + [b]$

should be the same as

$[a'] + [b]$.

This amounts to checking

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

but

$$(a'+b)-(a+b)$$

$$= a'-a \quad \text{is divisible by } n$$

Therefore

$$(a'+b) \equiv (a+b).$$

Similarly, we can check that

$$[a]-[b] = [a']-[b]$$

$$[a][b] = [a'b].$$

$\mathbb{Z}_5$.

Can I find a

s.t. $[3]_5[a]_5 = [1]_5$

$a = 2$?

$[3][2] = [6]_5 = [1]_5$

$\mathbb{Z}_6$ Can I find a

s.t. $[3]_6[a]_6 = [1]_6$?

There is No such a.