Math 2301 02 Aug 2023

* Admin : Quiz 1 on Friday (syllabus: until end of last week)

HW 1 due on Friday → check extn policy

Gradescope enrolments have been processed.

RC 2 will open on Friday & close on Sunday.

* Last time : Equivalence classes & the R_d relation:

$R_d = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid (x-y) \text{ is divisible by } d\}$. (d positive integer)

$x \sim_d y$ if x and y have the same remainder when divided by d.

→ there are d equivalence classes, usually labelled as

$[0]_d, [1]_d, \ldots, [d-1]_d$. (often, if $x \sim_d y$, we also say $x \equiv y \pmod d$)

Set $\mathbb{Z}_d :=$ set of equiv. classes of $R_d = \{[0]_d, [1]_d, \cdots, [d-1]_d\}$

* Today : Modular addition / arithmetic

[Example : $d = 7$.] → $\mathbb{Z}_7 = \{[0]_7, [1]_7, [2]_7, \ldots, [6]_7\}$

Define : An operation $+_d$ on $\mathbb{Z}_d$ as follows:
if $[a]_d, [b]_d$ are in $\mathbb{Z}_d$,

set $[a]_d +_d [b]_d = [a+b]_d$

trial. ↓ need to check if well-defined.

E.g. $[6]_7 + \underset{\substack{\| \\ [1]_7}}{[8]_7} = [14]_7 = [0]_7$

* Well-definedness

Recall that equivalence classes can have different representatives. That is, we can have $[x] = [y]$ with $x \neq y$.

E.g. For $d=7$, we have $[0]_7 = [14]_7$

So, 0 and 14 are both representatives of the equiv. class $[0]_7 = [14]_7 = [21]_7$.

For $+_d$, we should check that if we have ~~a, b, c, d ∈ ℤ such~~

x, y, z, w such that $[x]_d = [z]_d$, and

$$[y]_d = [w]_d$$

$[x]_d +_d [y]_d = [x+y]_d$ (trial def)

$[z]_d +_d [w]_d = [z+w]_d$ (trial def)

We have to check that ~~[x+y]~~ $[x+y]_d \stackrel{?}{=} [z+w]_d$

This means, we must check that $(x+y)-(z+w)$ is divisible by d.

$$(x+y)-(z+w) = (x-z)+(y-w)$$

$(x-z)+(y-w) \longrightarrow$ is divisible by d, because $[x]_d = [z]_d$ and $[y]_d = [w]_d$.

$\Rightarrow$ $+_d$ is well defined.

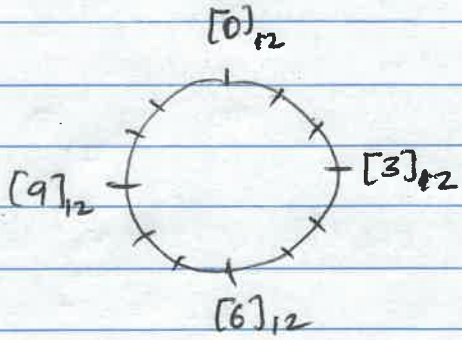
Examples : $(d = 7)$

$$[-72]_d + [10]_d = [-62]_d$$

$$\| \qquad\qquad \| \qquad\qquad \|$$

$$[5]_d + [3]_d = [1]_d$$

$(d = 12) \longrightarrow$ visualise clock



Other modular operations

Def: The operation $-_d$ on $\mathbb{Z}_d$ is defined as

$$[a]_d -_d [b]_d = [a-b]_d .$$

* Again, we need to check that this is well-defined.

That is, if $[x] = [z]$, $[y] = [w]$, then we need to show that $[x-y] = [z-w] \longrightarrow$ exercise

Def: The operation $\times_d$ on $\mathbb{Z}_d$:

$$[a]_d \times_d [b]_d = [ab]_d .$$

* Need to check it is well-defined.

That is, if $[x] = [z]$ and $[y] = [w]$, then $[xy] = [zw]$. (i.e. that $(xy - zw)$ is divisible by d)

Since $[x] = [z]$, we can say that

$$(x - z) = d \cdot k \quad \text{for some integer } k.$$

Similarly $(y - w) = d \cdot l$ for some integer l.

Then $(xy - zw) = (z + dk)(w + dl) - zw$

$= \cancel{zw} + dkw + zdl + d^2kl - \cancel{zw}$

$= d(kw + zl + dkl) \longrightarrow$ hence divisible by d.
(which is what we wanted!)

Question: Is there a notion of modular division?

Eg. $d = 6$; does it make sense to say

$$[2]_6 / [4]_6 \ ?$$

↳ Food for thought...

Summary:

We have $\mathbb{Z}_d$ & operations $+_d, -_d, \times_d$.

Key: $[x]_d = [y]_d$ is the same as saying

$(x - y)$ divisible by d, ie. there is some $k \in \mathbb{Z}$ such that $\boxed{(x-y) = dk}$.

Preview for Friday $\longrightarrow$ Directed graphs