

* Assignment 1 due tomorrow-

* Modular arithmetic

R_d an equivalence relation on \mathbb{Z} ,
where d is a fixed positive integer.

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

Equivalence classes are:

$$\{[0], [1], \dots, [d-1]\} := \mathbb{Z}_d$$

(Each equivalence class contains all integers that have a fixed remainder w.r.t. division by d).

Notation:

If $x \sim y$ w.r.t. R_d , we also write

$$x \equiv y \pmod{d}$$

(\uparrow is congruent to)

E.g. $2 \equiv 5 \pmod{3}$

is the same as saying:

- $(2, 5) \in R_3$
- $2 \sim 5$ under R_3
- $[2]_3 = [5]_3$

(2)

* An addition operation on \mathbb{Z}_d
(modular addition w.r.t. d)

Def: If $[r]$ and $[s]$ are in \mathbb{Z}_d

set $[r] +_d [s] := [r + s]$
↑
definition

Note: We need to check that this is well-defined. That is, if we change the representatives of the same eqv. class, we get the same output.

E.g. $d=3$, $r=2$, $s=7$

$$[2] + [7] = [2+7] = [9] = [0] \checkmark$$

But $[7] = [1]$

What is $[2] + [1] = [3] = [0] \checkmark$

Rmk: If $a \equiv b \pmod{d}$, then $(a-b)$ is divisible by d , so

$$(a-b) = k \cdot d \text{ for some integer } k.$$

* Proving that the definition makes sense

Suppose that $[r] = [r']$ for $r, r' \in \mathbb{Z}$
 $[s] = [s']$ for $s, s' \in \mathbb{Z}$

i.e. $r \equiv r' \pmod{d}$
 $s \equiv s' \pmod{d}$

So we see: $(r-r') = m \cdot d$
 $(s-s') = n \cdot d$ for $m, n \in \mathbb{Z}$

$r = r' + md, \quad s = s' + nd.$

~~$r+s$~~ $r+s = r' + md + s' + nd$
 $r+s = r' + s' + (m+n)d.$

$\Rightarrow [r+s] = [r' + s' + (m+n)d]$

$[r+s] = [r' + s']$

(because $r' + s' + (m+n)d \equiv r' + s' \pmod{d}$).

Result: We have a binary operation

$+_d : \mathbb{Z}_d \times \mathbb{Z}_d \rightarrow \mathbb{Z}_d$

E.g. $d = 3, \quad \mathbb{Z}_d = \{[0], [1], [2]\}$

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

$[1] + [2] = [0]$

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

* Modular subtraction

(4)

Def: Let $[r]$ and $[s]$ be elements of \mathbb{Z}_d .

Define $[r] -_d [s] = [r - s]$

Ex. $d = 5$

$$[2] - [1] = [1]$$

$$[2] - [6] = [-4]$$

Well-definedness:

If $r' \equiv r \pmod{d}$, $s' \equiv s \pmod{d}$

then $r = r' + md$, $s = s' + nd$ for $m, n \in \mathbb{Z}$

$$r - s = r' - s' + (m - n)d.$$

$$\Rightarrow [r - s] = [r' - s'].$$

E.g. $d = 3$

$$[1] - [2] = [-1] = [2]$$

$$[2] - [1] = [1]$$

* Modular multiplication

(5)

Def: If $[r], [s] \in \mathbb{Z}_d$

$$\text{set } [r] \times_d [s] := [rs]$$

Well-definedness?

$$\text{Let } r = r' + md \\ s = s' + nd$$

$$rs = (r' + md)(s' + nd)$$

$$rs = \underline{r's'} + \underline{ms'd + nr'd + mnd^2}$$

$$rs = r's' + (ms' + nr' + mnd) \cdot d$$

$$\Rightarrow \text{~~66d~~ ~~66~~ } [rs] = [r's']$$

Eg: $d = 5$

$$[1] \cdot [1] = [1]$$

$$[2] \cdot [2] = [4]$$

$$[2] \cdot [3] = [1]$$

$$[3] \cdot [3] = [4]$$

Together, we get 3 binary operations on \mathbb{Z}_d .

$(+_d, -_d, \times_d)$

$$\mathbb{Z}_d \times \mathbb{Z}_d \rightarrow \mathbb{Z}_d$$

Q: Can you define modular division?
(Excluding division by zero...)

(6)