MATH 2301 — 04 Aug 2022

* 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:

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

(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

$x \equiv y$ (modulo d)

(is congruent to)

E.g. $2 \equiv 5$ (modulo 3)

is the same as saying:

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

* 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. $d = 3$, $r = 2$, $s = 7$

$[2] + [7] = [2+7] = [9] = [0]$ ✓

But $[7] = [1]$

What is $[2] + [1] = [3] = [0]$ ✓

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

$(a-b) = k \cdot d$ 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 $m, n \in \mathbb{Z}$

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

$r + s = r' + md + s' + nd$

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

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

$[r+s] = [\underline{r'+s'}]$

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

Result: We have a binary operation

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

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

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

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

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

* Modular subtraction

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

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

Eg. $d = 5$

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

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

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

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

set $[r] \times_d [s] := [r s]$

Well-definedness?

Let $r = r' + md$

$s = s' + nd$

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

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

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

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

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 $\mathbb{Z}_d$.

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

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

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