MATH 2301

# * Modular arithmetic

## ** Recap

Consider $\{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid x-y \text{ is even}\}$

We have two equivalence classes:

① the set of even integers $= [0] = [-28] = [40]$

② the set of odd integers $= [1] = [-143] = [57]$

## ** Representatives of equivalence classes

If $[a]$ is an equivalence class for some equivalence relation, then $a$ is called a representative of this class.

- Equiv. classes can have many representatives; in fact any $b \in [a]$ is a representative.

## ** Back to our example

Note that:

① & ② cover $\mathbb{Z}$: $[0] \cup [1] = \mathbb{Z}$, and

① & ② have no overlap: $[0] \cap [1] = \emptyset$.

This shows we have found all possibilities of equivalence classes for this relation.

## ** Extending arithmetic

For modular arithmetic, we will no longer operate on integers. Instead we operate on equivalence classes of integers

modulus $=2$

Let $\sim$ be as before: $x \sim y$ if $x-y$ is even.

Set    definition

new operation   $[a] +_2 [b] := [a+b]$

$$[a] -_2 [b] := [a-b]$$

$$[a] \times_2 [b] := [ab]$$

### *** Examples

$[42] +_2 [-7] = [42 + (-7)] = [35] = [1]$

even + odd = odd

$[30] +_2 [4] = [34] = [0]$

even + even = even

$[7] \times_2 [11] = [77] = [1]$

odd × odd = odd

$[8] -_2 [15] = [-7] = [1]$

even − odd = odd

** <u>Well-defined-ness</u>

Whenever we define or state something about equivalence classes, we have to check that our statement is <u>well-defined</u>.

This means that if $[a] = [b]$, then we get the same answer whether we work with $a$ or $b$ as our representative.

** <u>Modular arithmetic in general</u>.

Fix a positive integer $d > 1$. ← modulus

Consider the equivalence relation:

$x \sim y$ if $x - y$ is an integer multiple of $d$.

*** <u>Definition</u>. Let $[a]$ and $[b]$ be equivalence classes under the relation above.

Set $[a] +_d [b] := [a+b]$

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

$[a] \times_d [b] := [ab]$

*** <u>Well-definedness</u>

Check for $+_d$: Let $[s] = [a]$ & $[t] = [b]$

So $s, t$ are new (arbitrary) representatives.

We have to show that

$$[a+b] = [s+t]$$

We know: $s - a$ is an integer multiple of $d$

$t - b$ is an integer multiple of $d$

$\Rightarrow (s-a) = kd$ for some $k \in \mathbb{Z}$

$(t-b) = ld$ for some $l \in \mathbb{Z}$

<u>Add</u>: $(s+t) - (a+b) = (k+l)\,d \Rightarrow (s+t) \sim (a+b)$

$\Rightarrow [s+t] = [a+b]$

$\blacksquare$ ← Done!

Check for $\times_d$:

We have to show: $[ab] = [st]$

We know: $s - a$ is an integer multiple of $d$

$t - b$ is an integer multiple of $d$

$\Rightarrow (s-a) = kd$ for some $k \in \mathbb{Z}$

$(t-b) = ld$ for some $l \in \mathbb{Z}$

$s = (a+kd)$, $t = (b+ld)$

Compute $st - ab = (a+kd)(b+ld) - ab$

$$st - ab = \cancel{ab} + kdb + ald + kld^2 - \cancel{ab}$$

$$= d\,(\underbrace{kb + al + kld}_{\text{integer}}).$$

$$\Rightarrow \quad st \sim ab \underset{\substack{\text{"implies"} \\ \text{"if ... then ..."}}}{\Rightarrow} [st] = [ab]$$

$\blacksquare$

*** Example

Choose $d = 12$

$$[1] -_d [5] = [-4] = [12-4] = [8]$$

$$[4] \times_d [20] = [80] = [8]$$

A conventional system of representatives is often $0, 1, 2, \dots d-1$

$[0], [1], \dots, [d-1]$ are all the equivalence classes

** Alternate notation

If $d =$ modulus, then saying that $a \equiv b \pmod{d}$ is the same as "a is congruent to b modulo d"

saying $[a] = [b]$ under our relation,

which is the same as saying
$a - b$ is an integer multiple of $d$.

** Bonus: division?

Sometimes we can divide integers, but not always.

When can you divide in modular arithmetic?

Example: $d = 6$

$[a]$, $[b]$ two classes.

$[24]/[12]$ ? should this make sense?

(Probably not: $[12] = [0]$, $[24] = [0]$ !! )

$[5]/[1]$ ? should this make sense?