Monday Week 1 aug. 22, 2016

Mod n and equivalence Relations

Def: Let S be a nonempty set. A rleation $\sim$ on S is an equivalence relation if

(1) reflexive, $\exists x \in S$ we have $x \sim x$.

(2) symmetric, $\exists x, y \in S$, if $x \sim y$, then $y \sim x$.

(3) transitive, $\exists x, y, z \in S$ if $x \sim y$ and $y \sim z$ then $x \sim z$

Recall: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ is the set of integers

Def: Let $a, b, n \in \mathbb{Z}$, s.t $n \geq 2$ if we say a and b are congruent modulo n (n divides the distance between a & b) n divides $a-b$

written as $n \mid a-b$, and we write $a \equiv b \pmod{n}$ Otherwise we write $a \not\equiv b \pmod{n}$ notation

example: $n = 3$

$\left.\begin{array}{l} a = 5 \\ b = 7 \end{array}\right\}$ $5 - 7 = -2$ which is not divisible by 3.

$5 \not\equiv 7 \pmod{3}$

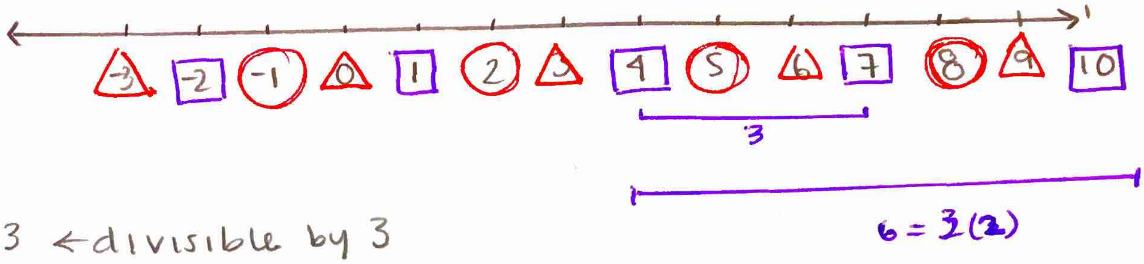
Recall

def: Let $\alpha, \beta \in \mathbb{Z}$ we say that α divides β if $\exists\, k \in \mathbb{Z}$ s.t. $\alpha k = \beta$ and we write $\alpha \mid \beta$

ex: $3 \mid 15$ since $\underset{\alpha}{3}\underset{k}{(5)} = \underset{\beta}{15}$

example $(n=3)$

$\mathbb{Z}$



- $7-4=3$ ← divisible by 3

  $7 \equiv 4 \pmod 3$

- $10-4=6$ ← is divisible by 3

  $10 \equiv 4 \pmod 3$

- $-6-(9) = -15 = 3(-5)$ ← multiple of 3

  $-6 \equiv 9 \pmod 3$

Theorem mod n is an equivalence relation on $\mathbb{Z}$.
and let $n \in \mathbb{Z}$ with $n \geq 2$

Proof

(reflexive) let $x \in \mathbb{Z}$
note that $x-x=0=n(0)$ so $n \mid x-x$
thus $x \equiv x \pmod n$

(symmetric) let $x, y \in \mathbb{Z}$, suppose $x \equiv y \pmod n$
then $n \mid x-y$, hence $nk = x-y$ for some $k \in \mathbb{Z}$
Ergo $n(-k) = y-x$ so $n \mid y-x$ therefore $y \equiv x \pmod n$

(transitive) let $x, y, z \in \mathbb{Z}$, suppose $x \equiv y \pmod n$ and
$y \equiv z \pmod n$
so $n \mid x-y$ and $n \mid y-z$, it follows that $nt = x-y$ and
$nl = y-z$ for some $t, l \in \mathbb{Z}$
adding gives $n(t+l) = x-z$ so $n \mid x-z$ $\therefore$ $x \equiv z \pmod n$

therefore since mod n is reflexive, symmetric
and transitive on $\mathbb{Z}$, mod n is an
equivalence relation on $\mathbb{Z}$.

8/24 P.1 Wednesday Week 1 aug 24, 2016

Last time

$\mathbb{Z} = \{0, 1, -1, 2, -2, \ldots\}$

$a \equiv b \pmod{n}$ means $n \mid (a-b)$

- Last we showed that this was an equivalence relation on $\mathbb{Z}$.

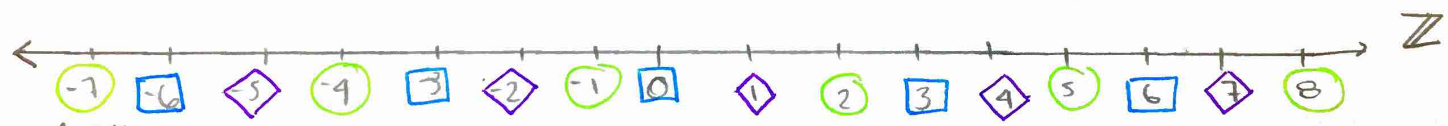
Def Let $\sim$ be an equivalence relation on a set S. Let $x \in S$. The equivalence class of x is

sometimes written $[x]$ $\rightarrow$ $\overline{x} = \{y \in S \mid x \sim y\}$

Fact If $\sim$ is an equivalence relation on a set S, then the equivalence classes of the elements of S partition S into disjoint pieces.

Example $(n=3)$ $\sim$ is mod 3.

$a \sim b$ is $a \equiv b \pmod 3$ on $S = \mathbb{Z}$



equivalence class of $\mathbb{Z}$ under mod 3 $\rightarrow$ $\overline{2} = \{y \in \mathbb{Z} \mid \underbrace{2 \equiv y \pmod 3}_{\text{means: } 3 \mid (2-y)}\} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$

$\overline{1} = \{y \in \mathbb{Z} \mid \underbrace{1 \equiv y \pmod 3}\} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$

$\overline{0} = \{y \in \mathbb{Z} \mid \underbrace{0 \equiv y \pmod 3}\} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$

$\overline{4} = \{y \in \mathbb{Z} \mid 4 \equiv y \pmod 3\} = \{\ldots, -5, -2, 1, 4, 7, \ldots\} = \overline{1}$

$4 \equiv 1 \pmod 3$ $\quad \overline{1} = \overline{4}$

Facts Let $\sim$ be an equivalence relation on a set S. Let $x, y \in S$. Let $\overline{x}$ and $\overline{y}$ be the equivalence classes of x and y then:

(1) $\overline{x} = \overline{y}$ iff $x \sim y$

(2) $\overline{x} \cap \overline{y} = \emptyset$ iff $x \not\sim y$

(3) $\overline{x} = \overline{y}$ iff $y \in \overline{x}$

ex $4 \equiv 1 \pmod 3$

$\overline{4} = \overline{1}$

$1 \in \overline{4}$

Def Let $n \geq 2$ be an integer
Let $\mathbb{Z}_n$ be the set of equivalence classes modulo n
$\mathbb{Z}_n$ is called the set of integers modulo n.

Ex $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

Theorem Let $n \geq 2$ be an integer, then
$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$ and $\underbrace{\bar{x} \neq \bar{y} \text{ when } 0 \leq x \leq y \leq n-1}$

• none of these guys are equal to eachother.

notation

$$\boxed{\begin{array}{l} \bar{x} = \bar{y} \\ x \equiv y \pmod{n} \end{array}}$$

Example $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$

$\bar{0} = \bar{2} = \bar{4} = \bar{6} = \overline{-2} = \overline{-4} = \cdots$

$\bar{1} = \bar{3} = \overline{-3} = \bar{5} = \overline{-5} = \cdots$

Notice in $\mathbb{Z}_2$ $\bar{0} = \{\ldots, \overline{-4}, \overline{-2}, \bar{0}, \bar{2}, \bar{4}, \ldots\}$

in $\mathbb{Z}_3$ $\bar{0} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$

Example $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

$\bar{2} = \bar{6} = \overline{10} = \overline{-2} = \cdots$

Is $\bar{3} = \overline{10278}$?

check
$10278 - 3 = 10275$

$$3 \overline{)10275} \quad 2568.75$$

no 4 does not divide $10278 - 3$

• what if we define $+$ and $\cdot$ in $\mathbb{Z}_n$ as follows?

$\bar{a} + \bar{b} = \overline{a+b}$

$\bar{a} \cdot \bar{b} = \overline{a \cdot b}$

• does this make sense?

Is it well defined?

8/24 p.2

For example consider $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

$$\left.\begin{array}{l} \bar{2} + \bar{3} = \overline{2+3} = \bar{5} = \bar{1} \\ \;\| \qquad \| \\ \bar{6} + \bar{7} = \overline{6+7} = \overline{13} = \bar{1} \end{array}\right\} \text{equal in } \mathbb{Z}_4$$

lets do multiplication

$$\left.\begin{array}{l} \bar{2} \cdot \bar{3} = \overline{2 \cdot 3} = \bar{6} = \bar{2} \\ \;\| \\ \overline{-2} \cdot \overline{-1} = \overline{-2 \cdot -1} = \bar{2} \end{array}\right\} \text{equal in } \mathbb{Z}_4$$

Proposition Let $n \geq 2$ be an integer

Let $a, b, c, d \in \mathbb{Z}$

If $\bar{a} = \bar{b}$ and $\bar{c} = \bar{d}$ in $\mathbb{Z}_n$

then $\overline{a+c} = \overline{b+d}$ and $\overline{a \cdot c} = \overline{b \cdot d}$ in $\mathbb{Z}_n$

proof Suppose $\bar{a} = \bar{b}$ and $\bar{c} = \bar{d}$ in $\mathbb{Z}_n$

So $\bar{a} = \bar{b}$ means $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$

Thus $n \mid a-b$ and $n \mid c-d$

So $\exists\, l, k \in \mathbb{Z}$ s.t. $a-b = nk$ and $c-d = nl$

Scratchwork

$\overline{a+c} = \overline{b+d}$

$a+c \equiv b+d \pmod{n}$

$n \mid [(a+c) - (b+d)]$

Hence,
$$\begin{aligned} (a+c)-(b+d) &= (a-b)+(c-d) \\ &= nk + nl \\ &= n(k+l) \end{aligned}$$

Thus $n \mid [(a+c)-(b+d)]$

So $(a+c) \equiv (b+d) \pmod{n}$

Therefore, $\overline{a+c} = \overline{b+d}$ ☒

The $\overline{a \cdot c} = \overline{b \cdot d}$ proof is similar. $\Rightarrow$

and $ac - bd = a[d + n\ell] - [a - nk]d$

$= ad + an\ell - ad + nkd$

$= n[a\ell + kd]$

so $n \mid ac - bd$

thus, $ac \equiv bd \pmod{n}$

so $\overline{ac} = \overline{bd}$ ▨

Ex: Define $+$ and $\cdot$ in $\mathbb{Z}_n$ to be:

$\bar{a} + \bar{b} = \overline{a+b}$

$\bar{a} \cdot \bar{b} = \overline{ab}$

Ex: $(n = 3)$

$\mathbb{Z}_4, +$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\mathbb{Z}_4, \cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$