Math 4460
3/1/23

Test 1 is
Weds 3/8

We can cover any
problems you want
to do on Monday

Theorem Let $n \in \mathbb{Z}$ with $n \geq 2$. Let $w, x, y, z \in \mathbb{Z}$. Then:

① $x \equiv x \pmod{n}$

② If $x \equiv y \pmod{n}$, then $y \equiv x \pmod{n}$.

③ If $x \equiv y \pmod{n}$ and $y \equiv z \pmod{n}$, then $x \equiv z \pmod{n}$.

① reflexive
② symmetric
③ transitive

$\equiv$ is an equivalence relation

④ If $w \equiv x \pmod{n}$ and $y \equiv z \pmod{n}$, then $w + y \equiv x + z \pmod{n}$ and $wy \equiv xz \pmod{n}$.
Also, $w - y \equiv x - z \pmod{n}$.

⑤ $x \equiv y \pmod{n}$ iff $x = y + nk$ where $k \in \mathbb{Z}$.

proof:

① $x - x = 0 = n(0)$

So, $n \mid (x-x)$.

Thus, $x \equiv x \pmod n$.

$a \equiv b \pmod n$

means

$n \mid (a-b)$

② Suppose $x \equiv y \pmod n$.

Then, $n \mid (x-y)$.

So, $x - y = n\ell$ where $\ell \in \mathbb{Z}$.

Thus, $y - x = n(-\ell)$.

Hence, $n \mid (y-x)$.

So, $y \equiv x \pmod n$.

③ Suppose $x \equiv y \pmod n$

and $y \equiv z \pmod n$.

Then, $n \mid (x-y)$ and $n \mid (y-z)$.

Hence, $\boxed{x-y=ns}$ and $\boxed{y-z=nt}$

where $s,t \in \mathbb{Z}$.

Adding gives

$$x-z = ns+nt$$

So, $x-z = n[s+t]$.

Ergo $n \mid (x-z)$.

It follows that $x \equiv z \pmod{n}$.

Alternative method

$x-z = (y+ns) - (y-nt)$

$= ns+nt$

$= n(s+t)$

---

(4) Suppose $w \equiv x \pmod{n}$

and $y \equiv z \pmod{n}$.

Then, $n \mid (w-x)$ and $n \mid (y-z)$.

Thus, $\boxed{w-x = n\alpha}$ and $\boxed{y-z = n\beta}$

where $\alpha, \beta \in \mathbb{Z}$.

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

$$= (w-x)+(y-z)$$
$$= n\alpha + n\beta$$
$$= n[\alpha+\beta]$$

So, $n \mid [(w+y)-(x+z)]$

Thus,

$$(w+y) \equiv (x+z) \pmod{n}$$

$$w - x = n\alpha$$
$$y - z = n\beta$$

Note that

$$wy - xz$$

$$= \underbrace{(x + n\alpha)}_{w} y - x \underbrace{(y - n\beta)}_{z}$$

$$= xy + n\alpha y - xy + xn\beta$$

$$= n[\alpha y + x\beta]$$

Hence, $n \mid [wy - xz]$.

So, $wy \equiv xz \pmod{n}$.

$w - x = n\alpha$
$y - z = n\beta$

Also,

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

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

$$= n\alpha - n\beta$$

$$= n[\alpha - \beta].$$

So, $n \mid [(w-y)-(x-z)]$

Thus, $(w-y) \equiv (x-z) \pmod{n}$.

(5) $x \equiv y \pmod{n}$

iff $n \mid (x-y)$

iff $x - y = nk$ for some $k \in \mathbb{Z}$

iff $x = y + nk$ for some $k \in \mathbb{Z}$.

$\blacksquare$

__Def:__ Let $n \in \mathbb{Z}$ with $n \geq 2$.

Let $x \in \mathbb{Z}$.

The __equivalence class of x modulo n__ is

$$\overline{x} = \{ y \in \mathbb{Z} \mid y \equiv x \pmod{n} \}$$

$$= \{ \ldots, x-3n, x-2n, x-n, x, x+n, x+2n, x+3n, \ldots \}$$

⑤ from theorem

Ex: $n=2$

$$\bar{0} = \{ y \in \mathbb{Z} \mid y \equiv 0 \pmod{2} \}$$

$$= \{ \ldots, -8, -6, -4, -2, 0, 2, 4, 6, 8, \ldots \}$$

$$\bar{1} = \{ y \in \mathbb{Z} \mid y \equiv 1 \pmod{2} \}$$

$$= \{ \ldots, -7, -5, -3, -1, 1, 3, 5, 7, \ldots \}$$

$$\bar{2} = \{ y \in \mathbb{Z} \mid y \equiv 2 \pmod{2} \}$$

$$= \{ \ldots, -6, -4, -2, 0, 2, 4, 6, 8, \ldots \}$$

$$= \bar{0}$$

$$\bar{3} = \{ \ldots, -5, -3, -1, 1, 3, 5, 7, 9, \ldots \}$$

$$= \bar{1}$$

Note $\overline{3} = \overline{1}$ and $3 \equiv 1 \pmod{2}$

$\overline{0} = \overline{2}$ and $0 \equiv 2 \pmod{2}$

Mod 2 partitions $\mathbb{Z}$ into two equivalence classes: $\overline{0}, \overline{1}$

$\mathbb{Z}$

$\overline{0}$	$\overline{1}$
$\ldots, -10, -8, -6, -4, -2, 0, 2, 4, 6, 8, 10, 12, \ldots$	$\ldots, -11, -9, -7, -5, -3, -1, 1, 3, 5, 7, 9, 11, 13, \ldots$
evens	odds

Ex: $n=3$

$$\bar{0} = \{ y \in \mathbb{Z} \mid y \equiv 0 \pmod 3 \}$$
$$= \{ \ldots, -9, -6, -3, 0, 3, 6, 9, \ldots \}$$

$$\bar{1} = \{ y \in \mathbb{Z} \mid y \equiv 1 \pmod 3 \}$$
$$= \{ \ldots, -8, -5, -2, 1, 4, 7, 10, 13, \ldots \}$$

$$\bar{2} = \{ y \in \mathbb{Z} \mid y \equiv 2 \pmod 3 \}$$
$$= \{ \ldots, -7, -4, -1, 2, 5, 8, 11, \ldots \}$$

$$\bar{3} = \{ y \in \mathbb{Z} \mid y \equiv 3 \pmod 3 \}$$
$$= \{ \ldots, -6, -3, 0, 3, 6, 9, 12, \ldots \}$$

$= \overline{0}$ and note $3 \equiv 0 \pmod 3$

Mod 3 partitions $\mathbb{Z}$ into 3 equivalence classes: $\overline{0}, \overline{1}, \overline{2}$

$\mathbb{Z}$

$\overline{0}$	$\overline{1}$	$\overline{2}$
$\vdots$	$\vdots$	$\vdots$
-9	-8	-7
-6	-5	-4
-3	-2	-1
0	1	2
3	4	5
6	7	8
9	10	11
$\vdots$	$\vdots$	$\vdots$