4460
3/3/25

Topic 4 – Integers modulo n

Def: Let $n \in \mathbb{Z}$, $n \geq 2$.
We say that integers x and y are **congruent modulo n** if $n \mid (x-y)$,
and we write $x \equiv y \pmod{n}$.

If $n \nmid (x-y)$, then
we write $x \not\equiv y \pmod{n}$.

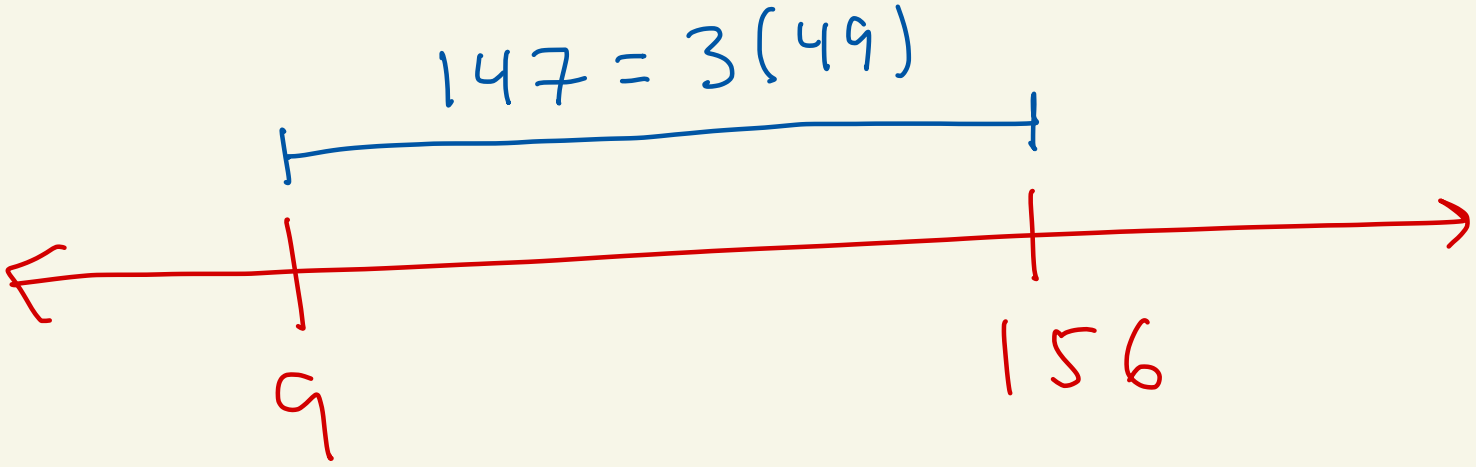
Ex: $n = 3$, $x = 156$, $y = 9$

$x - y = 156 - 9 = 147 = 3 \cdot 49$

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

$3 \mid (156-9)$

Thus, $156 \equiv 9 \pmod 3$



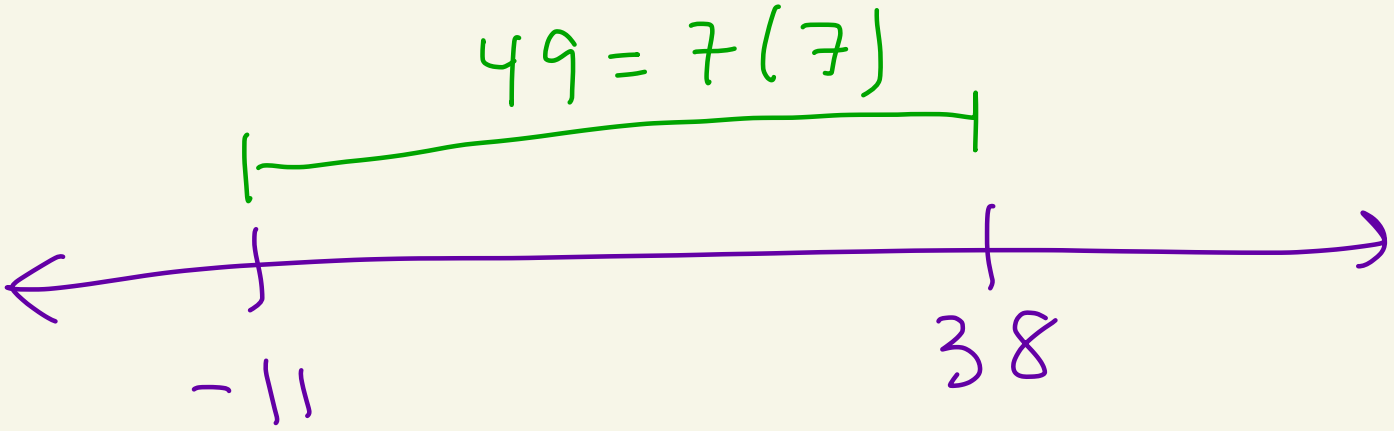
Ex: $n = 7,\ x = -11,\ y = 38$

$x - y = -11 - 38 = -49 = 7(-7)$

$7 \mid (-11 - 38)$

$n \mid (x - y)$

So, $-11 \equiv 38 \pmod 7$



Is $38 \equiv -11 \pmod 7$? Yes!

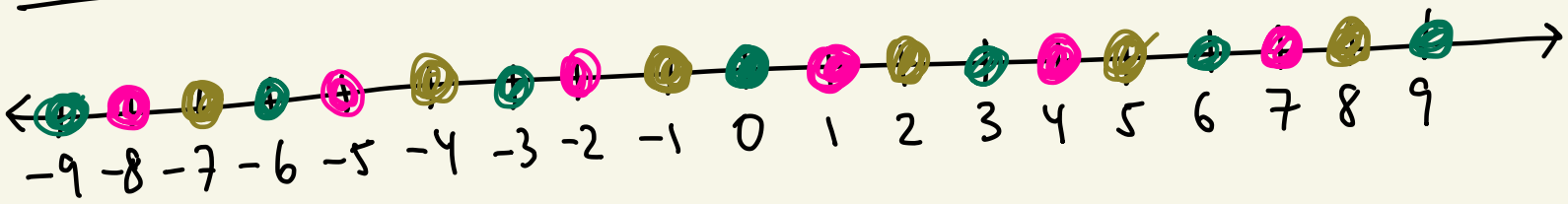
$38 - (-11) = 49 = 7(7)$ ← multiple of 7

Ex: $n = 3, x = 1, y = -3$

$x - y = 1 - (-3) = 4$ ← not a multiple of 3

So, $1 \not\equiv -3 \pmod 3$

Ex: $n = 3$



$3 \equiv 0 \pmod 3$

$-6 \equiv 3 \pmod 3$

$-3 \equiv 3 \pmod 3$

⋮

$4 \equiv 1 \pmod 3$

$7 \equiv -2 \pmod 3$

$-8 \equiv -5 \pmod 3$

⋮

$2 \equiv -1 \pmod 3$

$8 \equiv -7 \pmod 3$

$5 \equiv -4 \pmod 3$

⋮

Theorem: Let $n \in \mathbb{Z}$, $n \geq 2$.

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 $x \equiv z \pmod{n}$.

2450/3450
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 $wy \equiv xz \pmod{n}$.

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

Proof:

① $x - x = 0 = n \cdot 0$

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

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

---

② Assume $x \equiv y \pmod{n}$.

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

So, $x - y = nk$ where $k \in \mathbb{Z}$.

Then, $y - x = n(-k)$.

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

Ergo, $y \equiv x \pmod{n}$.

---

③ Assume $x \equiv y \pmod{n}$ and $y \equiv z \pmod{n}$.

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

Thus, $x - y = nk$ and $y - z = nl$

where $k, l \in \mathbb{Z}$.

Then,

$$x - z = (nk + y) - (y - nl)$$
$$= nk + nl$$
$$= n(k + l)$$

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

Thus, $x \equiv z \pmod{n}$.

---

(4) Assume $w \equiv x \pmod{n}$
and $y \equiv z \pmod{n}$.

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

So, $\boxed{w - x = nk}$ and $\boxed{y - z = nl}$
where $k, l \in \mathbb{Z}$.

Then,

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

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

$$= nk + nl$$

$$= n(k+l).$$

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

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

Also,

$$wy - xz$$

$$= \underbrace{(nk+x)}_{w} y - x \underbrace{(y-nl)}_{z}$$

$$= nky + xy - xy + xnl$$

$$= n(ky + xl)$$

Thus,

$$n \mid (wy - xz).$$

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

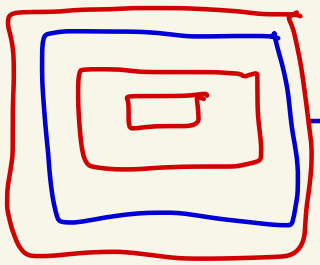
---

(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 $k \in \mathbb{Z}$.



Corollary: If $x \equiv y \pmod{n}$ and $w \equiv z \pmod{n}$, then $(x-w) \equiv (y-z) \pmod{n}$.

proof:

Assume $x \equiv y \pmod{n}$, $w \equiv z \pmod{n}$.

Note $-1 \equiv -1 \pmod{n}$ by part (1).

Since $w \equiv z \pmod{n}$ and $-1 \equiv -1 \pmod{n}$,

by (4) we get $-w \equiv -z \pmod{n}$.

Since $x \equiv y \pmod{n}$ and $-w \equiv -z \pmod{n}$,

by part (4) we get $x-w \equiv y-z \pmod{n}$.