Topic 4 —
Integers modulo n

Integers modulo n (HW 4)

<u>Def:</u> Let $n \in \mathbb{Z}$ with $n \geq 2$.
Let $x, y \in \mathbb{Z}$.
We say that <u>x is congruent to y modulo n</u> if n divides $x-y$, and write $x \equiv y \pmod{n}$.
If n does not divide $x-y$ we write $x \not\equiv y \pmod{n}$.

<u>Ex:</u>

Is $1 \equiv 5 \pmod{4}$?

$1-5=-4=4(-1)$

$4 \mid (1-5)$

Yes

<u>Ex:</u>

Is $-3 \equiv 15 \pmod{6}$?

$-3-15=-18=6(-3)$

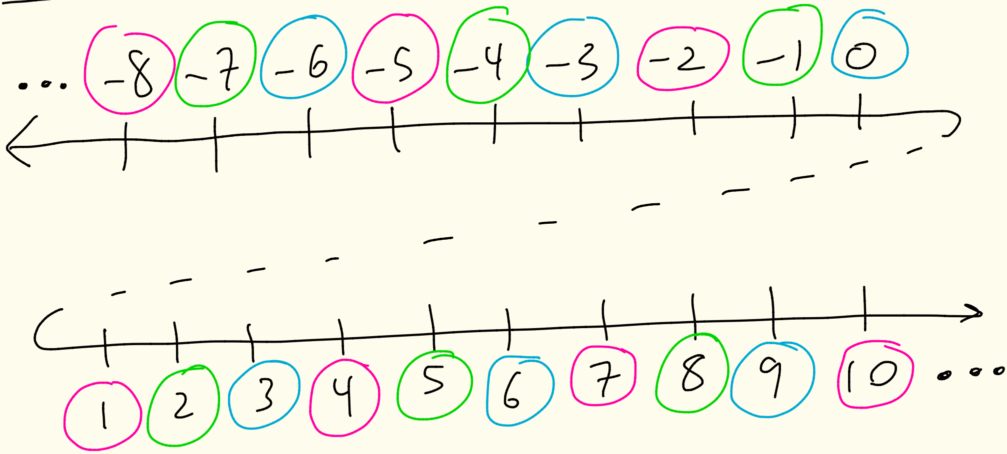
$6 \mid (-3-15)$

So, answer is yes

Ex: $15 \not\equiv 14 \pmod{6}$

because $6 \nmid \underbrace{(15-14)}_{1}$

Ex: $(n=3)$



$1 \equiv 4 \pmod{3}$

$1 \equiv 7 \pmod{3}$

$7 \equiv 10 \pmod{3}$

$-8 \equiv -2 \pmod{3}$

$0 \equiv -6 \pmod{3}$

$0 \equiv 3 \pmod{3}$

$-6 \equiv 6 \pmod{3}$

$-7 \equiv 8 \pmod{3}$

$5 \equiv -1 \pmod{3}$

<u>Theorem:</u> Let $n \in \mathbb{Z}$ with $n \geq 2$.

Let $w, x, y, z \in \mathbb{Z}$.

Then the following are true:

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 $x \equiv z \pmod{n}$

Equivalence relation
① reflexive
② symmetric
③ transitive

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 $x - x = 0 = n(0)$

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

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

② Suppose $x \equiv y \pmod{n}$.

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

So, $x - y = nq$ where $q \in \mathbb{Z}$

Thus, $y - x = n(-q)$

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

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

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

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

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

Adding both equations gives

$$(x-y) + (y-z) = nk + n\ell$$

Thus,

$$x - z = n(k+\ell)$$

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

Thus,

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

Another way:

$x = y + nk$

$z = y - n\ell$

So,

$$x - z = (y+nk) - (y-n\ell) = n(k-\ell)$$

④ Suppose $w \equiv x \pmod{n}$ and $y \equiv z \pmod{n}$.

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

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

Then,

$$
\begin{aligned}
(w+y)-(x+z) &= w-x+y-z \\
&= nk+nl \\
&= n(k+l)
\end{aligned}
$$

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

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

Also,

$$
\begin{aligned}
wy - xz &= \overbrace{(x+nk)}^{w}y - x\overbrace{(y-nl)}^{z} \\
&= xy + nky - xy + xnl \\
&= n[ky + xl]
\end{aligned}
$$

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

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

5 We have that

$$x \equiv y \pmod{n}$$

iff $n \mid (x-y)$

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

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

iff

$\blacksquare$

<u>Def:</u> Let $n \in \mathbb{Z}$ with $n \geq 2$.
Let $x \in \mathbb{Z}$.
The <u>equivalence class of x modulo n</u> is

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

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

part ⑤ of last thm

Ex: Let $n=3$.

The Land of mod 3

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

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

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

$$\bar{3} = \{ \ldots, -6, -3, 0, 3, 6, 9, 12, \ldots \}$$

Note $\bar{3} = \bar{0}$. Also note $3 \equiv 0 \pmod{3}$

$$\bar{4} = \{ \ldots, -5, -2, 1, 4, 7, 10, 13, \ldots \}$$

Note $\bar{4} = \bar{1}$. Also note $4 \equiv 1 \pmod{3}$.

<u>Theorem:</u> Let $n \in \mathbb{Z}$ with $n \geq 2$.
Let $x, y \in \mathbb{Z}$.

① Either $\overline{x} = \overline{y}$
or $\overline{x} \cap \overline{y} = \emptyset$

② $\overline{x} = \overline{y}$
iff $x \equiv y \pmod{n}$
iff $x \in \overline{y}$

③ A complete set of distinct equivalence classes modulo n is given by $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$.
That is, if $z \in \mathbb{Z}$ then $\overline{z} = \overline{r}$ for a unique integer r with $0 \leq r \leq n-1$.
Moreover, r is the remainder when you divide n into z.

Proof:

1 & 2 are HW. Or you can get these results because $\equiv$ mod n is an equivalence relation.

Let's prove 3.

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

By the division algorithm

$$z = qn + r$$

where $q, r \in \mathbb{Z}$ and $0 \le \underbrace{r \le n-1}_{r<n}$.

Then, $z - r = nq$.

So, $z \equiv r \pmod{n}$.

By part 2, $\overline{z} = \overline{r}$.

In summary, $\overline{z} \in \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$

Can any of the equivalence classes $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$ be equal?

No, they are all distinct.

Let's show this.

Suppose $0 \leq a \leq b \leq n-1$ with $\overline{a} = \overline{b}$.

We will show that $a = b$.

Since $\boxed{a \leq b \leq n-1}$ we have

$$\boxed{0 \leq b-a \leq n-1-a} \leq n-1.$$

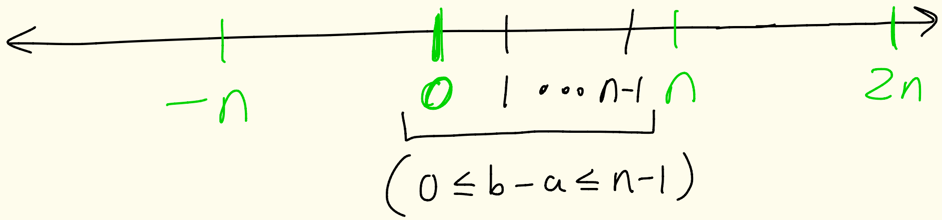
sub-tract a

Thus, $0 \leq b-a \leq n-1$ and $\overline{a} = \overline{b}$.

By part 2, since $\overline{a} = \overline{b}$ we know $a \equiv b \pmod{n}$.

Then, $b-a$ is a multiple of n and $0 \leq b-a \leq n-1$.

Multiples of n in green



Thus, $b-a=0$.

So, $b=a$.

Thus, $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$ form a complete set of distinct equivalence classes modulo n.

<u>Def:</u> Let $n \in \mathbb{Z}$ with $n \geq 2$.

Define

$$\mathbb{Z}_n = \{ \bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1} \}$$

$\mathbb{Z}_n$ is called the <u>set of integers modulo n</u>

<u>Ex:</u>

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

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

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

$$\mathbb{Z}_5 = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4} \}$$

and so on.

We want to define $+$ and $\cdot$ on $\mathbb{Z}_n$. What if we just defined it as $\overline{a}+\overline{b}=\overline{a+b}$ and $\overline{a}\cdot\overline{b}=\overline{ab}$?

$\boxed{\text{Is this well-defined?}}$

For example, consider

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

We would have

$$\overline{2}+\overline{3}=\overline{2+3}=\overline{5}=\overline{1}$$

$5 \equiv 1 \pmod 4$

$\boxed{\text{or}}$

$$\begin{array}{r} 1 \\ 4\,\overline{)\,5} \\ -4 \\ \hline 1 \end{array}$$

remainder

so, $\overline{5}=\overline{1}$

There are an infinite # of ways to represent $\overline{2}$ and $\overline{3}$. We want to make sure we get the same answer no matter how we represent them. For example in $\mathbb{Z}_4$, $\overline{2}=\overline{6}$ and $\overline{3}=\overline{11}$.

And, $\underset{\overline{2}}{\overline{6}}+\underset{\overline{3}}{\overline{11}}=\overline{17}=\overline{1}$

because $17 \equiv 1 \pmod 4$
$4 \mid (17-1)$

same answer in this example

Theorem (Addition and Multiplication in $\mathbb{Z}_n$ is well-defined)

Let $n \in \mathbb{Z}$ with $n \geq 2$.
Given $x, y \in \mathbb{Z}$, the operations

$$\overline{x} + \overline{y} = \overline{x+y}$$

and $\overline{x} \cdot \overline{y} = \overline{xy}$

are well-defined operations on $\mathbb{Z}_n$.

proof: Let $a, b, c, d \in \mathbb{Z}$.
Suppose that $\overline{a} = \overline{b}$ and $\overline{c} = \overline{d}$ in $\mathbb{Z}_n$
We need to show that

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

and $\overline{a} \cdot \overline{c} = \overline{ac} = \overline{bd} = \overline{b}\,\overline{d}$

Since $\overline{a} = \overline{b}$ and $\overline{c} = \overline{d}$ we know

$$a \equiv b \pmod{n} \text{ and } c \equiv d \pmod{n}.$$

By monday's theorem, $(a+c) \equiv (b+d) \pmod{n}$ and $ac \equiv bd \pmod{n}$. Thus, $\overline{a+c} = \overline{b+d}$ and $\overline{ac} = \overline{bd}$. $\blacksquare$

Ex: Let's work in

$$\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$$

Some calculations:

$9 \equiv 3 \pmod{6}$

$$\bar{4} + \bar{5} = \overline{4+5} = \bar{9} = \bar{3}$$

$$\bar{2} \cdot \bar{3} + \bar{4}^2 + \overline{-10} = \bar{6} + \overline{16} + \overline{-10} = \overline{22} + \overline{-10} = \overline{12} = \bar{0}$$

$12 \equiv 0 \pmod{6}$

$$\begin{array}{r|l} & \;\;40 \\ \hline 6 & 243 \\ & -24 \\ \hline & \;\;\;03 \\ & \;-00 \\ \hline & \;\;\;\;\;3 \end{array}$$

$$\bar{3}^5 = \overline{243} = \bar{3}$$

or

$$\bar{3}^5 = \overline{243} = \bar{6} \cdot \overline{40} + \bar{3} = \bar{0} \cdot \overline{40} + \bar{3} = \bar{3}$$

$\bar{9} = \bar{3}$

or

$$\bar{3}^5 = \bar{3}\,\bar{3}\,\bar{3}\,\bar{3}\,\bar{3} = \bar{9} \cdot \bar{9} \cdot \bar{3} = \bar{3} \cdot \bar{3} \cdot \bar{3} = \bar{9} \cdot \bar{3} = \bar{3} \cdot \bar{3} = \bar{9} = \bar{3}$$

Theorem: Let $n \in \mathbb{Z}$, $n \geq 2$.
Let $a, b, c \in \mathbb{Z}$.
In $\mathbb{Z}_n$ we have that

① $\bar{a} + \bar{b} = \bar{b} + \bar{a}$

② $\bar{a}\,\bar{b} = \bar{b}\,\bar{a}$

③ $\bar{a}(\bar{b}\,\bar{c}) = (\bar{a}\,\bar{b})\bar{c}$

④ $\bar{a} + (\bar{b} + \bar{c}) = (\bar{a} + \bar{b}) + \bar{c}$

⑤ $\bar{a}(\bar{b} + \bar{c}) = \bar{a}\,\bar{b} + \bar{a}\,\bar{c}$

⑥ $(\bar{b} + \bar{c})\bar{a} = \bar{b}\,\bar{a} + \bar{c}\,\bar{a}$

proof: This is a HW problem.
For example for ① we have that

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

$a + b = b + a$ since $a, b \in \mathbb{Z}$

$\blacksquare$

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

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

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

Given $x \in \mathbb{Z}$, then in $\mathbb{Z}_2$ we have

$\bar{x} = \bar{0}$ iff x is even

$\bar{x} = \bar{1}$ iff x is odd

So, $\mathbb{Z}_2$ "detects" even or odd-ness of an integer.

Ex: $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$

In $\mathbb{Z}_4$,

$\overline{0} = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$

$\overline{2} = \{\ldots, -6, -2, 2, 6, 10, \ldots\}$

even integers

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

$\overline{3} = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$

odd integers

Given $x \in \mathbb{Z}$, then in $\mathbb{Z}_4$ we have

x is even iff $\overline{x} = \overline{0}$ or $\overline{x} = \overline{2}$

x is odd iff $\overline{x} = \overline{1}$ or $\overline{x} = \overline{3}$

Common useful fact:

x is odd iff $x \equiv 1 \pmod 4$

or $x \equiv 3 \pmod 4$

Some
More
examples
follow
if
needed

Ex: Is

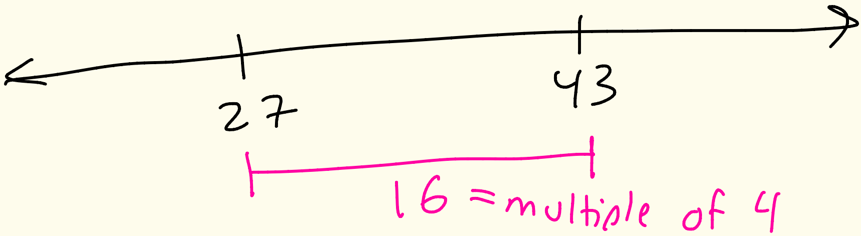
$\overline{27} = \overline{43}$ in $\mathbb{Z}_4$?

Method 1:

$27 - 43 = -16 = 4(-4)$
which is a multiple of 4

Thus, $27 \equiv 43 \pmod{4}$.

So, $\overline{27} = \overline{43}$



Note: You can subtract in either order because

$x \equiv y \pmod{n}$ iff $y \equiv x \pmod{n}$

$\boxed{\text{Method 2}}$:

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

$$\overline{27} = \overline{27} + \underbrace{\overline{-6} \cdot \bar{4}}_{\bar{0}} = \overline{27-24} = \bar{3}$$

because $\bar{0} = \bar{4}$

$$\begin{array}{r} 10 \\ 4\,\overline{)\,43} \\ -4 \\ \hline 03 \\ -\ 0 \\ \hline 3 \end{array}$$

$$43 = (10)(4) + 3$$

$$\overline{43} = \overline{(10)(4)+3}$$
$$= \overline{10 \cdot 4} + \bar{3}$$
$$= \overline{10} \cdot \bar{4} + \bar{3}$$
$$= \overline{10} \cdot \bar{0} + \bar{3} = \bar{3}$$

$\bar{4} = \bar{0}$ in $\mathbb{Z}_4$

Thus, $\overline{27} = \bar{3} = \overline{43}$

HW 4

5 (c) Is $\overline{-51} = \overline{-109}$ in $\mathbb{Z}_8$?

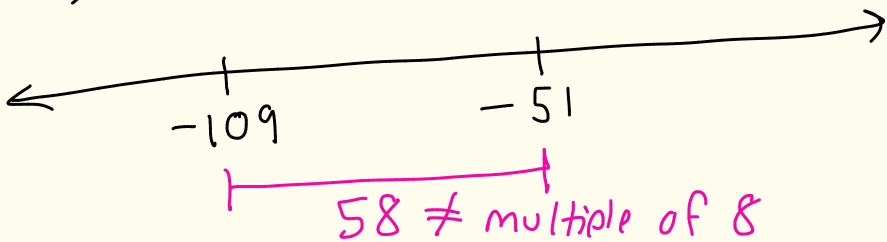
Method 1

$(-51)-(-109) = -51+109 = 58$

Is 58 a multiple of 8? No

Thus, $-51 \not\equiv -109 \pmod 8$

So, $\overline{-51} \neq \overline{-109}$



$\boxed{\text{Method 2}}$:

$\mathbb{Z}_8 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}\}$

$$\overline{-51} = \overline{-51 + \underbrace{8 \cdot 7}_{\overline{0}}} = \overline{-51+56} = \overline{5}$$

because $\overline{8} = \overline{0}$ in $\mathbb{Z}_8$

$$\begin{array}{r} -14 \\ 8 \overline{\smash{)}-109} \\ -(-112) \\ \hline 3 \end{array} \quad -109 = \underbrace{(-14)(8)}_{112} + 3$$

So, $\overline{-109} = \overline{(-14)(8) + 3}$

$= \overline{(-14)(8)} + \overline{3}$

$= \overline{(-14)} \cdot \overline{8} + \overline{3}$

$= \overline{(-14)} \cdot \overline{0} + \overline{3} = \overline{3}$

$\overline{8} = \overline{0}$ in $\mathbb{Z}_8$

Thus,
$\overline{-51} = \overline{5}$
$\overline{-109} = \overline{3}$
and $\overline{3} \neq \overline{5}$
So,
$\overline{-51} \neq \overline{-109}$

Ex: Consider

$$\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$$

Reduce the following expression into the form $\overline{x}$ where $0 \leq x \leq 6$.

$$\boxed{\overline{12}^{\,2} \cdot (\overline{-3}) + \overline{4201} + \overline{-5}^{\,3}}$$

$$\overline{12}^{\,2} = \overline{5}^{\,2} = \overline{25} = \overline{4}$$

$\overline{12} = \overline{5}$ in $\mathbb{Z}_7$

$12 - 5 = 7$

$25 - 4 = 21 = \underbrace{(7)(3)}_{\text{multiple of } 7}$

or

$$\begin{array}{r} 3 \\ 7\overline{)25} \\ -21 \\ \hline 4 \end{array}$$

remainder of 4

Notation:

$\overline{25} = \overline{4}$

$25 \equiv 4 \pmod 7$

$$\begin{array}{r} 600 \\ 7\overline{)4201} \\ -4200 \\ \hline 1 \end{array}$$

$4201 = (600)(7) + 1$

Thus,

$4201 - 1 = (600)(7)$

So,

$4201 \equiv 1 \pmod 7$

Thus,

$\overline{4201} = \overline{1}$ in $\mathbb{Z}_7$

$\overline{-5}^3 = \overline{2}^3 = \overline{8} = \overline{1}$

$\boxed{-5 \equiv 2 \pmod 7}$

$\boxed{8 \equiv 1 \pmod 7}$

Thus,

$(\overline{12}^2)(\overline{-3}) + \overline{4201} + (\overline{-5})^3$

$= (\overline{4})(\overline{-3}) + \overline{1} + \overline{1} = \overline{-12} + \overline{2}$

$= \overline{-10} = \overline{4}$

$\overline{14} = \overline{2 \cdot 7} = \overline{0}$

I added 14