4460
3/10/25

We want to define $+$ and $\cdot$ on $\mathbb{Z}_n$. What if we just define it as:

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

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

Is this well-defined?

$\boxed{\text{Ex:}}$ $n=4$, $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$

$$\overline{1} + \overline{3} = \overline{1+3} = \overline{4} = \overline{0}$$

$\boxed{4 \equiv 0 \pmod 4}$

equal

equal

$$\overline{5} + \overline{7} = \overline{5+7} = \overline{12} = \overline{0}$$

$\boxed{12 \equiv 0 \pmod 4}$

Thm: (+ and $\cdot$ are well-defined on $\mathbb{Z}_n$)

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

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

$$\bar{a} = \bar{c} \text{ and } \bar{b} = \bar{d}$$

then

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

$$\overline{ab} = \overline{cd} \leftarrow \bar{a} \cdot \bar{b} = \bar{c} \cdot \bar{d}$$

---

proof:

Since $\bar{a} = \bar{c}$ we know $a \equiv c \pmod{n}$

Since $\bar{b} = \bar{d}$ we know $b \equiv d \pmod{n}$

Previously we saw this gives

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

and

$$ab \equiv cd \pmod{n}.$$

Thus,

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

and

$$\overline{ab} = \overline{cd}$$

$\blacksquare$

<u>Ex:</u>

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

$$(\overline{3}+\overline{5})\cdot\overline{6} = \overline{3+5}\cdot\overline{6}$$

$$= \overline{8}\cdot\overline{6}$$

$$= \overline{1}\cdot\overline{6} = \overline{6}$$

$$\begin{array}{r}
1 \\
7\,\overline{)\,8} \\
-7 \\
\hline
1
\end{array}$$

$$\overline{6}^{20} = \overline{-1}^{20} = \overline{(-1)^{20}} = \overline{1}$$

$$6 \equiv -1 \pmod{7}$$

$$\overline{1,000} = \overline{6}$$

$$\begin{array}{r}
142 \\
7\,\overline{)\,1,000} \\
-7 \\
\hline
30 \\
-28 \\
\hline
20 \\
-14 \\
\hline
6
\end{array}$$

$$\overline{1000} = \overline{7}\cdot\overline{142} + \overline{6}$$

$$\overline{1000} = \overline{0}\cdot\overline{142} + \overline{6}$$

$\overline{7} = \overline{0}$ in $\mathbb{Z}_7$

$\boxed{\overline{1000} = \overline{6}}$

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

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

In $\mathbb{Z}_n$ we have:

$$\left.\begin{array}{l} (1)\ \overline{a} + \overline{b} = \overline{b} + \overline{a} \\ (2)\ \overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a} \end{array}\right\} \text{commutative}$$

$$\left.\begin{array}{l} (3)\ \overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c} \\ (4)\ \overline{a} \cdot (\overline{b} \cdot \overline{c}) = (\overline{a} \cdot \overline{b}) \cdot \overline{c} \end{array}\right\} \text{associative}$$

$$\left.\begin{array}{l} (5)\ \overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c} \\ (6)\ (\overline{b} + \overline{c})\overline{a} = \overline{b} \cdot \overline{a} + \overline{c} \cdot \overline{a} \end{array}\right\} \text{distributive}$$

<u>proof:</u> In HW 4. Let's prove (5). We have

$$\overline{a}\cdot\left(\overline{b}+\overline{c}\right) = \overline{a}\cdot\left(\overline{b+c}\right)$$

def of + in $\mathbb{Z}_n$

$$= \overline{a\cdot(b+c)}$$

def of ·

Properties of $\mathbb{Z}$

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

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

def of +

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

def of ·

$\blacksquare$

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

$$\overline{0} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\} \leftarrow \text{evens}$$

$$\overline{1} = \{\ldots, -5, -3, -1, 0, 1, 3, 5, \ldots\} \leftarrow \text{odds}$$

Given $x \in \mathbb{Z}$, then

$\overline{x} = \overline{0}$ if x is even

$\overline{x} = \overline{1}$ if x is odd

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

$$\left.\begin{array}{l} \overline{0} = \{\ldots, -8, -4, 0, 4, 8, \ldots\} \\ \overline{2} = \{\ldots, -6, -2, 2, 6, 10, \ldots\} \end{array}\right\} \text{evens}$$

$$\left.\begin{array}{l} \overline{1} = \{\ldots, -7, -3, 1, 5, 9, \ldots\} \\ \overline{3} = \{\ldots, -5, -1, 3, 7, 11, \ldots\} \end{array}\right\} \text{odds}$$

$$\boxed{\begin{array}{l} x \text{ is even iff } \overline{x} = \overline{0} \text{ or } \overline{x} = \overline{2} \\ x \text{ is odd iff } \overline{x} = \overline{1} \text{ or } \overline{x} = \overline{3} \end{array}}$$

$$\boxed{x \text{ is odd iff } x \equiv 1 \pmod 4 \text{ or } x \equiv 3 \pmod 4}$$

<u>Side note</u> (Dirichlet's theorem)

If $\gcd(a,n)=1$, there exist an infinite # of primes that satisfy $\underbrace{p \equiv a \pmod n}_{p = a + nk}$

$\boxed{\text{HW 2}}$ $a, b \neq 0$

10 If $a|c$, $b|c$, $\gcd(a,b)=1$, then $ab|c$.

<u>pf:</u> Since $a|c$ we know $c = ak$ where $k \in \mathbb{Z}$.

Since $b|c$ we know $b|ak$.

Since $b|ak$ and $\gcd(a,b)=1$ we know $b|k$.

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

So, $c = ak = abl$.

Thus, $ab|c$. $\blacksquare$

Method 2:

Since $a|c$ we get $c = ak, k \in \mathbb{Z}$
Since $b|c$ we get $c = bl, l \in \mathbb{Z}$.

Since $\gcd(a,b) = 1$ we get

$$ax + by = 1 \text{ where } x, y \in \mathbb{Z}.$$

Multiply by c to get

$$cax + cby = c$$

So,

$$\underbrace{(bl)}_{c} ax + \underbrace{(ak)}_{c} by = c$$

Then,

$$ab[lx + ky] = c$$

So, $ab|c$. $\blacksquare$

Hw 2

(11) If $\gcd(a,b)=1$, $x \mid a$, $x \mid bc$, then $x \mid c$

Claim: $\gcd(x,b)=1$

Let $d=\gcd(x,b)$.

Then, $d \mid x$ and $d \mid b$ and $d \geq 1$.

Since $d \mid x$ and $x \mid a$ we know $d \mid a$. (HW 1)

So, $d \mid a$ and $d \mid b$.

But $\gcd(a,b)=1$.

So, $d=1$.

Since $x \mid bc$ and $\gcd(x,b)=1$ we know $x \mid c$. $\blacksquare$