


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?

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

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

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

equal

↑ equal
↓

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

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

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

then

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

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

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

$$\bar{a} \cdot \bar{b} = \bar{c} \cdot \bar{d}$$

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

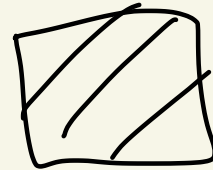
$$ab \equiv cd \pmod{n}.$$

Thus,

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

and

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



Ex:

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

$$\begin{aligned} (\overline{3} + \overline{5}) \cdot \overline{6} &= \overline{3+5} \cdot \overline{6} \\ &= \overline{8} \cdot \overline{6} \\ &= \overline{1} \cdot \overline{6} = \overline{6} \end{aligned}$$

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

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

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

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

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

$$\begin{aligned} \overline{1000} &= \overline{7} \cdot \overline{142} + \overline{6} \\ \overline{1000} &= \overline{0} \cdot \overline{142} + \overline{6} \end{aligned}$$

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

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

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

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

In \mathbb{Z}_n we have:

$$\textcircled{1} \quad \overline{a} + \overline{b} = \overline{b} + \overline{a}$$

$$\textcircled{2} \quad \overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$$

commutative

$$\textcircled{3} \quad \overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c}$$

$$\textcircled{4} \quad \overline{a} \cdot (\overline{b} \cdot \overline{c}) = (\overline{a} \cdot \overline{b}) \cdot \overline{c}$$

associative

$$\textcircled{5} \quad \overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$$

$$\textcircled{6} \quad (\overline{b} + \overline{c}) \cdot \overline{a} = \overline{b} \cdot \overline{a} + \overline{c} \cdot \overline{a}$$

distributive

proof: In HW 4, Let's

prove $\textcircled{5}$. We have

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

↑
def of + in \mathbb{Z}_n

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

↑
def of \cdot

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

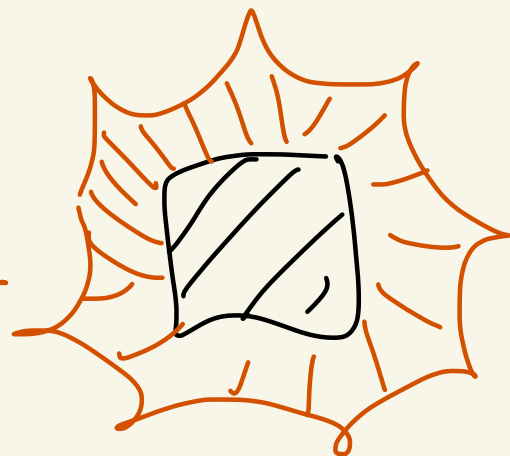
$$= \overline{a \cdot b} + \overline{a \cdot c}$$

↑
def of +

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

↑
def of \cdot

properties
of \mathbb{Z}



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

$\bar{0} = \{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\} \leftarrow \text{evens}$

$\bar{1} = \{\dots, -5, -3, -1, 1, 3, 5, \dots\} \leftarrow \text{odds}$

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

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

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

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

$\bar{0} = \{\dots, -8, -4, 0, 4, 8, \dots\}$

$\bar{2} = \{\dots, -6, -2, 2, 6, 10, \dots\}$

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

$\bar{3} = \{\dots, -5, -1, 3, 7, 11, \dots\}$

evens

odds

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

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

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

Side note (Dirichlet's theorem)

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

$$p = a + nk$$

HW 2 $a, b \neq 0$

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

Pf: 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, $ab|c$.



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, $ab|c$.



HW 2

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

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

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

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

Since $d|x$ and $x|a$ we know $d|a$. (HW)

So, $d|a$ and $d|b$.

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

So, $d = 1$.

Since $x|bc$ and $\gcd(x, b) = 1$

we know $x|c$.

