4460
3/12/25

Let's do some calculations in $\mathbb{Z}_n$.

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

Method 1:

$43 - 27 = 16 = 4 \cdot 4$

$4 \mid (43 - 27)$

$43 \equiv 27 \pmod 4$

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

Method 2:

$\overline{43} = \overline{3}$

$\overline{27} = \overline{3}$

equal

$$\begin{array}{r} 6 \\ 4 \overline{)\,27} \\ -24 \\ \hline 3 \end{array} \qquad \begin{array}{r} 10 \\ 4 \overline{)\,43} \\ -40 \\ \hline 3 \end{array}$$

Ex: Consider $\mathbb{Z}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

Reduce the following in $\mathbb{Z}_7$:

$$\bar{4}^3 + \overline{-2} \cdot \overline{10}^2 + \overline{421}$$

$$= \overline{64} + \overline{-200} + \overline{421}$$

$$= \overline{285}$$

$$= \boxed{\bar{5}}$$

$$\begin{array}{r|l} & \;\;40 \\ \hline 7 & 285 \\ & -28 \\ \hline & \;\;05 \\ & -\;\;0 \\ \hline & \;\;\;\;5 \end{array}$$

Topic 5 - The multiplicative structure of $\mathbb{Z}_n$

Def: Let $n \in \mathbb{Z}$, $n \geq 2$.
Let $\overline{x}, \overline{y} \in \mathbb{Z}_n$.
We say that $\overline{x}$ and $\overline{y}$ are <u>multiplicative inverses</u> in $\mathbb{Z}_n$
if $\overline{x} \cdot \overline{y} = \overline{1}$

Ex: Consider

$$\mathbb{Z}_{10} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}\}$$

$\overline{0} \cdot \overline{y} = \overline{0}$ ← you can never get $\overline{1}$

$\boxed{\overline{0} \text{ has no mult. inverse}}$

$\overline{1} \cdot \overline{1} = \overline{1}$ ← $\boxed{\overline{1} \text{ is its own mult. inverse}}$

Does $\overline{2}$ have a mult. inverse?

$\overline{2} \cdot \overline{0} = \overline{0}$
$\overline{2} \cdot \overline{1} = \overline{2}$
$\overline{2} \cdot \overline{2} = \overline{4}$
$\overline{2} \cdot \overline{3} = \overline{6}$
$\overline{2} \cdot \overline{4} = \overline{8}$
$\overline{2} \cdot \overline{5} = \overline{10} = \overline{0}$
$\overline{2} \cdot \overline{6} = \overline{12} = \overline{2}$
$\overline{2} \cdot \overline{7} = \overline{14} = \overline{4}$
$\overline{2} \cdot \overline{8} = \overline{16} = \overline{6}$
$\overline{2} \cdot \overline{9} = \overline{18} = \overline{8}$

you never get $\overline{1}$

So, $\overline{2}$ has no mult. inverse

$\overline{3} \cdot \overline{7} = \overline{21} = \overline{1}$ ← $\boxed{\overline{3} \text{ and } \overline{7} \text{ are mult. inverses}}$

$\overline{9} \cdot \overline{9} = \overline{81} = \overline{1}$ ← $\boxed{\overline{9} \text{ is it's own inverse}}$

$$\begin{array}{r} 8 \\ 10 \overline{)81} \\ -80 \\ \hline 1 \end{array}$$

$\overline{x}$	inverse in $\mathbb{Z}_{10}$?
$\overline{0}$	no inverse
$\overline{1}$	$\overline{1}$
$\overline{2}$	no inverse
$\overline{3}$	$\overline{7}$
$\overline{4}$	no inverse
$\overline{5}$	no inverse

$\overline{6}$	no inverse
$\overline{7}$	$\overline{3}$
$\overline{8}$	no inverse
$\overline{9}$	$\overline{9}$

We need the next lemma to make our next theorem make sense.

LEMMA: Let $n \in \mathbb{Z}$, $n \geq 2$.
Let $a, b \in \mathbb{Z}$.

If $a \equiv b \pmod{n}$, then $\gcd(a,n) = \gcd(b,n)$

$\boxed{\text{Equivalently, if } \bar{a} = \bar{b}, \text{ then } \gcd(a,n) = \gcd(b,n)}$

<u>Theorem:</u> Let $a, n \in \mathbb{Z}$, $n \geq 2$. Then, $\bar{a}$ has a multiplicative inverse in $\mathbb{Z}_n$ iff $\gcd(a,n) = 1$

Moreover, if $\bar{a}$ has a multiplicative inverse, then that inverse is unique.

Ex: Does $\overline{3}$ have a multiplicative inverse in $\mathbb{Z}_{26}$?

We have $\gcd(3,26)=1$

Yes, $\overline{3}$ does have a mult. inverse.

It's $\overline{9}$ because $\overline{3}\cdot\overline{9}=\overline{27}=\overline{1}$

$$\begin{array}{r} 1 \\ 26\,\overline{)\,27} \\ -26 \\ \hline 1 \end{array}$$

$\overline{2}$ doesn't have a mult. inverse in $\mathbb{Z}_{26}$

because $\gcd(2,26)=2\neq 1$.

proof of theorem:

($\Rightarrow$) Suppose $\overline{a}$ has a multiplicative inverse in $\mathbb{Z}_n$

We must show that $\gcd(a,n)=1$

Since $\overline{a}$ has a mult. inverse there exists $\overline{b} \in \mathbb{Z}_n$ where $\boxed{\overline{a} \cdot \overline{b} = \overline{1}.}$

Let $d = \gcd(a,n)$.

We want $d=1$.

Suppose $d>1$.

Let $c = \frac{n}{d}$. $\leftarrow$ $\boxed{c \in \mathbb{Z} \text{ because } d \mid n}$

Since $\underbrace{d>1}$ and $\underbrace{d \leq n}$ we know

$$1 \le \frac{n}{d} < n.$$

So, $1 \le c < n$.

Thus, $\overline{c} \neq \overline{0}$ in $\mathbb{Z}_n$.

But also

$$\overline{c} = \overline{\left(\frac{n}{d}\right)} = \overline{\left(\frac{n}{d}\right)} \cdot \overline{1} = \overline{\left(\frac{n}{d}\right)} \cdot \overline{a} \cdot \overline{b}$$

$\boxed{\overline{a} \cdot \overline{b} = \overline{1}}$

$$= \overline{\left(\frac{nab}{d}\right)} = \overline{n\left(\frac{a}{d}\right)b} = \overline{n} \cdot \underbrace{\overline{\left(\frac{a}{d}\right)}} \cdot \overline{b}$$

$\frac{a}{d} \in \mathbb{Z}$ since $d \mid a$, $d = \gcd(a, n)$

$$= \overline{0} \cdot \overline{\left(\frac{a}{d}\right)} \cdot \overline{b} = \overline{0}$$

$\overline{n} = \overline{0}$ in $\mathbb{Z}_n$

So if $d>1$ then $c=\frac{n}{d}$ would satisfy $\overline{c}=\overline{0}$ and $\overline{c}\neq\overline{0}$, which is a contradiction.

So, $d=\gcd(a,n)=1$.

($\Leftarrow$) Suppose $\gcd(a,n)=1$

We must show $\overline{a}$ has a mult. inverse.

Since $\gcd(a,n)=1$ we know

$$ax_0+ny_0=1 \text{ for some } x,y\in\mathbb{Z}.$$

Then in $\mathbb{Z}_n$ we get $\overline{ax_0+ny_0}=\overline{1}$

So, $\overline{ax_0}+\overline{ny_0}=\overline{1}$.

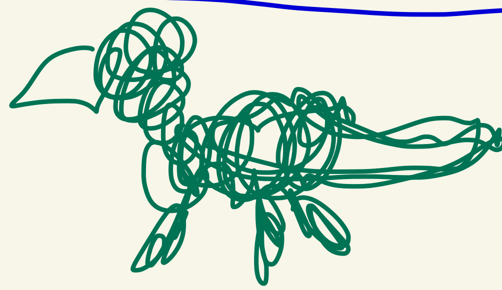
So, $\overline{a}\cdot\overline{x_0}+\underbrace{\overline{n}}_{\overline{n}=\overline{0} \text{ in } \mathbb{Z}_n}\cdot\overline{y_0}=\overline{1}$.

Thus, $\overline{a}\cdot\overline{x_0}=\overline{1}$ in $\mathbb{Z}_n$.

So, $\overline{a}$ has a mult. inverse in $\mathbb{Z}_n$

$\boxed{\text{Iff}}$

(Moreover part)



Suppose $\overline{a}$ has a multiplicative inverse in $\mathbb{Z}_n$.

Let's show the inverse is unique.

Suppose $\overline{b_1}$ and $\overline{b_2}$ are both multiplicative inverses of $\overline{a}$.

Then, $\overline{a} \cdot \overline{b_1} = \overline{1}$ and $\overline{a} \cdot \overline{b_2} = \overline{1}$.

So, $\overline{a} \cdot \overline{b_1} = \overline{a} \cdot \overline{b_2}$.

Multiply by $\overline{b_2}$ to get

$$\underbrace{\overline{b_2} \cdot \overline{a}} \cdot \overline{b_1} = \underbrace{\overline{b_2} \cdot \overline{a}} \cdot \overline{b_2}$$

So, $\underbrace{\bar{a}\cdot\bar{b}_2}\cdot\bar{b}_1 = \underbrace{\bar{a}\cdot\bar{b}_2}\cdot\bar{b}_2$

$\bar{a}\cdot\bar{b}_2=\bar{1}$

Then, $\bar{1}\cdot\bar{b}_1 = \bar{1}\cdot\bar{b}_2$

So, $\bar{b}_1 = \bar{b}_2$.

The inverse is unique!

Side commentary from class question

In $\mathbb{Z}_{10}$ suppose you have

$$\bar{2}\,\bar{x} = \bar{2}\,\bar{y}.$$

Then, $\bar{x}=\bar{0}$, $\bar{y}=\bar{5}$ solve this

but $\bar{x}\neq\bar{y}$.

Be careful, can't divide off $\bar{2}$
to get $\bar{x}=\bar{y}$. Not true

What about $\bar{3}\bar{x} = \bar{3}\bar{y}$ in $\mathbb{Z}_{10}$?

Multiply by $\bar{7}$ to get

$$\bar{7} \cdot \bar{3}\,\bar{x} = \bar{7} \cdot \bar{3}\,\bar{y}$$

So, $\overline{21}\,\bar{x} = \overline{21}\,\bar{y}$

$\overline{21} = \bar{1}$ in $\mathbb{Z}_{10}$

Then, $\bar{x} = \bar{y}$