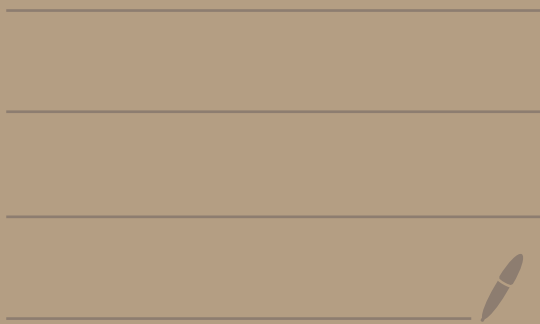


Math 4460
4/3/23



Before we start topic 5
let's do some practice calculations
in \mathbb{Z}_n

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

Method 1

$$43 - 27 = 16 = 4 \cdot 4 \leftarrow \text{a multiple of 4}$$

$$\text{So, } 43 \equiv 27 \pmod{4}$$

$$\text{Thus, } \overline{27} = \overline{43} \text{ in } \mathbb{Z}_4.$$

Method 2

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

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

$$\begin{array}{r} 10 \\ 4 \overline{) 43} \\ -40 \\ \hline 3 \end{array}$$

$$\begin{array}{r} 6 \\ 4 \overline{) 27} \\ -24 \\ \hline 3 \end{array}$$

$$43 = 4 \cdot 10 + 3$$

$$43 - 3 = 4 \cdot 10$$

$$43 \equiv 3 \pmod{4}$$

$$\text{So, } \overline{43} = \overline{3} = \overline{27}$$

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

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

$$0 \leq x \leq 6$$

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

$$\overline{12}^2 \cdot (\overline{-3}) = \overline{-2}^2 \cdot (\overline{-3}) = \overline{-12} = \overline{2}$$

$$12 \equiv -2 \pmod{7}$$

$$\overline{12} = \overline{-2}$$

$$-12 \equiv 2 \pmod{7}$$

$$\begin{aligned} \overline{-12} &= \overline{-12} + \overline{0} \\ &= \overline{-12} + \overline{2 \cdot 7} \end{aligned}$$

$$\overline{7} = \overline{0}$$

$$= \overline{2}$$

$$\overline{4201} = \bar{1}$$

$$\begin{array}{r} 600 \\ 7 \overline{) 4201} \\ \underline{-42} \\ 1 \end{array}$$

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

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

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

So,

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

$$= \overline{2} + \bar{1} + \bar{1}$$

$$= \boxed{4}$$

What is $\overline{-4311}$ equal to modulo 7?

$$\begin{array}{r} -615 \\ 7 \overline{) -4311} \\ \underline{-(-42)} \\ -11 \\ \underline{-(-7)} \\ -41 \\ \underline{-(-35)} \\ -6 \end{array}$$



$$\begin{aligned} -4311 &= \\ &7(-615) + (-6) \end{aligned}$$



$$\begin{aligned} \overline{-4311} &= \overline{-6} \\ &= \overline{1} \end{aligned}$$

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

Def: Let $n \in \mathbb{Z}$ with $n \geq 2$.

Let $\bar{x}, \bar{y} \in \mathbb{Z}_n$.

We say that \bar{x} and \bar{y} are multiplicative inverses in \mathbb{Z}_n if

$$\bar{x} \cdot \bar{y} = \bar{1}$$

← this implies also $\bar{y} \cdot \bar{x} = \bar{1}$

Ex: Consider

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

Note that

$$\overline{3} \cdot \overline{7} = \overline{21} = \overline{1}$$

$$\begin{aligned} 21 - 1 &= 20 = 2 \cdot 10 \\ 21 &\equiv 1 \pmod{10} \end{aligned}$$

So, $\overline{3}$ and $\overline{7}$ are multiplicative inverses in \mathbb{Z}_{10} .

Also note that

$$\overline{9} \cdot \overline{9} = \overline{81} = \overline{1}$$

$$\begin{aligned} 81 &\equiv 1 \pmod{10} \\ 81 - 1 &= 80 = 8 \cdot 10 \end{aligned}$$

So, $\overline{9}$ is its own multiplicative inverse in \mathbb{Z}_{10} .

$$\text{Also, } \overline{1} \cdot \overline{1} = \overline{1}$$

So, $\overline{1}$ is its own multiplicative inverse in \mathbb{Z}_{10} .

Let's see if $\overline{2}$ has a multiplicative inverse in \mathbb{Z}_{10} .

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

you never get $\overline{1}$

So, $\overline{2}$ does not have a multiplicative inverse in \mathbb{Z}_{10}

element in \mathbb{Z}_{10}	<u>multiplicative inverse</u>
$\bar{0}$	none
$\bar{1}$	$\bar{1}$
$\bar{2}$	none
$\bar{3}$	$\bar{7}$
$\bar{4}$	none
$\bar{5}$	none
$\bar{6}$	none
$\bar{7}$	$\bar{3}$
$\bar{8}$	none
$\bar{9}$	$\bar{9}$

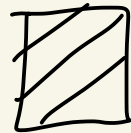
Lemma: Let $n \in \mathbb{Z}$ with $n \geq 2$.

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

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

Equivalently, if $\bar{a} = \bar{b}$ in \mathbb{Z}_n
then $\gcd(a, n) = \gcd(b, n)$

proof: HW 5 #15.



Ex: In \mathbb{Z}_6 , we have $\overline{22} = \overline{4}$

And $\gcd(22, 6) = 2$

$\gcd(4, 6) = 2$

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

Then, \bar{a} has a multiplicative inverse in \mathbb{Z}_n if and only if $\gcd(a, n) = 1$.

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

This theorem is well-defined because of the lemma. I.e. if $\bar{a} = \bar{b}$, then $\gcd(a, n) = \gcd(b, n)$

Ex: $n = 26$

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

Well, $\gcd(3, 26) = 1$

Yes, $\overline{3}$ has a multiplicative inverse.

It is $\overline{9}$!

$$\overline{3} \cdot \overline{9} = \overline{27} = \overline{1}$$

↑

$27 \equiv 1 \pmod{26}$

Note $\gcd(4, 26) = 2 \neq 1$

So, $\overline{4}$ does not have a multiplicative inverse in \mathbb{Z}_{26} .