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

$43 - 27 = 16 = 4 \cdot 4$ ← a multiple of 4

So, $43 \equiv 27 \pmod 4$

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

Method 2

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

$43 = 4 \cdot 10 + 3$

$43 - 3 = 4 \cdot 10$

$43 \equiv 3 \pmod 4$

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

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

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

$$\boxed{\text{So, } \overline{43} = \overline{3} = \overline{27} \qquad \mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}}$$

<u>Ex:</u> 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 $0 \leq x \leq 6$

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

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

$12 \equiv -2 \pmod 7$

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

$-12 \equiv 2 \pmod 7$

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

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

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

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

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

$$\boxed{-5 \equiv 2 \pmod 7} \qquad \boxed{8 \equiv 1 \pmod 7}$$

So,

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

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

$$= \overline{4}$$

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

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

$$-4311 = 7(-615) + (-6)$$

$$\overline{-4311} = \overline{-6}$$

$$= \overline{1}$$

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

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

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

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

<u>Ex:</u> Consider

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

Note that

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

$21-1=20=2\cdot 10$

$21\equiv 1 \pmod{10}$

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

Also note that

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

$81\equiv 1 \pmod{10}$

$81-1=80=8\cdot 10$

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

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

$\boxed{\text{So, } \overline{1} \text{ is it's own multiplicative inverse in } \mathbb{Z}_{10}.}$

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

$$\left.\begin{aligned}
\overline{2} \cdot \overline{0} &= \overline{0} \\
\overline{2} \cdot \overline{1} &= \overline{2} \\
\overline{2} \cdot \overline{2} &= \overline{4} \\
\overline{2} \cdot \overline{3} &= \overline{6} \\
\overline{2} \cdot \overline{4} &= \overline{8} \\
\overline{2} \cdot \overline{5} &= \overline{10} = \overline{0} \\
\overline{2} \cdot \overline{6} &= \overline{12} = \overline{2} \\
\overline{2} \cdot \overline{7} &= \overline{14} = \overline{4} \\
\overline{2} \cdot \overline{8} &= \overline{16} = \overline{6} \\
\overline{2} \cdot \overline{9} &= \overline{18} = \overline{8}
\end{aligned}\right\} \text{you never get } \overline{1}$$

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

element in $\mathbb{Z}_{10}$	multiplicative inverse
$\overline{0}$	none
$\overline{1}$	$\overline{1}$
$\overline{2}$	none
$\overline{3}$	$\overline{7}$
$\overline{4}$	none
$\overline{5}$	none
$\overline{6}$	none
$\overline{7}$	$\overline{3}$
$\overline{8}$	none
$\overline{9}$	$\overline{9}$

<u>Lemma:</u> 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 $\overline{a} = \overline{b}$ in $\mathbb{Z}_n$
then $\gcd(a,n) = \gcd(b,n)$

<u>proof:</u> HW 5 #15. $\blacksquare$

<u>Ex:</u> 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. Ie 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 $\overline{9}$!

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

$\boxed{27 \equiv 1 \pmod{26}}$

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

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