Math 4460

4/5/23

<u>Theorem (from Monday)</u> 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
in $\mathbb{Z}_n$, then that inverse is unique.

<u>proof:</u>

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

Then there exist integers x_0 and y_0
where $ax_0 + ny_0 = 1$.

Thus in $\mathbb{Z}_n$ we have $\overline{ax_0 + ny_0} = \bar{1}$.

Hence in $\mathbb{Z}_n$ we have $\overline{ax_0} + \overline{ny_0} = \bar{1}$.

So in $\mathbb{Z}_n$ we have $\bar{a}\,\bar{x}_0 + \underbrace{\bar{n}\,\bar{y}_0}_{\bar{0}} = \bar{1}$.

We know $\bar{n} = \bar{0}$ in $\mathbb{Z}_n$,
thus we have $\bar{a}\,\bar{x}_0 = \bar{1}$.

So, $\bar{x}_0$ is a multiplicative inverse
for $\bar{a}$ in $\mathbb{Z}_n$.

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

Then there exists $b \in \mathbb{Z}$ where
$$\bar{a} \cdot \bar{b} = \bar{1} \quad \text{in } \mathbb{Z}_n.$$

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

Our goal is to show that $d = 1$.

Suppose instead that $d > 1$.

Let's show that this leads to a contradiction.

Let $c = \frac{n}{d}$.

$c \in \mathbb{Z}$ because $d \mid n$

Since $d > 1$ we know $\boxed{c = \frac{n}{d} < n.}$

Since n, d are both positive and $d \mid n$ we know $d \leq n$.

So, $\boxed{1 \leq \frac{n}{d} = c.}$

Thus, $\boxed{1 \leq c < n}$

Hence, ergo, thus $\boxed{\bar{c} \neq \bar{0}}$ in $\mathbb{Z}_n$.

But on the other hand

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

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

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

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

$\boxed{\bar{n} = \bar{0} \text{ in } \mathbb{Z}_n}$

So, $\boxed{\bar{c} = \bar{0}.}$

Thus, $\bar{c} \neq \bar{0}$ and $\bar{c} = \bar{0}$.

Contradiction.

So, $d = 1$.

《moreover part》

Suppose $\overline{a}$ has a multiplicative inverse. Let's show the inverse is unique.

Suppose $\overline{g}_1$ and $\overline{g}_2$ are both multiplicative inverses for $\overline{a}$.

Then, $\boxed{\overline{a} \cdot \overline{g}_1 = \overline{1}}$ and $\boxed{\overline{a} \cdot \overline{g}_2 = \overline{1}.}$

Let's show $\overline{g}_1 = \overline{g}_2$.

We have

$$\overline{g}_1 = \overline{g}_1 \cdot \overline{1} = \overline{g}_1 \cdot (\overline{a} \cdot \overline{g}_2)$$

$$= (\overline{g}_1 \cdot \overline{a}) \cdot \overline{g}_2$$

$$= (\overline{a} \cdot \overline{g_1}) \cdot \overline{g_2}$$

$$= \overline{1} \cdot g_2$$

$$= \overline{g_2}$$

$\blacksquare$

<u>Notation:</u> If $\overline{a} \in \mathbb{Z}_n$ has a multiplicative inverse then we denote it's unique inverse by $\overline{a}^{-1}$.

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

Define

$$\mathbb{Z}_n^{\times} = \{ \bar{a} \in \mathbb{Z}_n \mid \bar{a} \text{ has a multiplicative inverse} \}$$
$$= \{ \bar{a} \in \mathbb{Z}_n \mid \gcd(a,n) = 1 \}$$

MATH 4550

- $\mathbb{Z}_n$ is a group under $+$
- $\mathbb{Z}_n^{\times}$ is a group under $\cdot$

Ex: Let's calculate $\mathbb{Z}_{10}^{\times}$.

We have

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

$\gcd(0,10) = 10 \neq 1$

$\gcd(1,10) = 1$

$\gcd(2,10) = 2 \neq 1$

$\gcd(3,10) = 1$

$\gcd(4,10) = 2 \neq 1$

$\gcd(5,10) = 5 \neq 1$

$\gcd(6,10) = 2 \neq 1$

$\gcd(7,10) = 1$

$\gcd(8,10) = 2 \neq 1$

$\gcd(9,10) = 1$

So, $\boxed{\mathbb{Z}_{10}^{\times} = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}}$

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

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

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

$\longrightarrow$

So, $\overline{1}^{-1} = \overline{1}$

$\overline{3}^{-1} = \overline{7}$

$\overline{7}^{-1} = \overline{3}$

$\overline{9}^{-1} = \overline{9}$

Ex: Let's calculate $\mathbb{Z}_{15}^{\times}$ and every elements multiplicative inverse.

$$\mathbb{Z}_{15} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \overline{10}, \overline{11}, \overline{12}, \overline{13}, \overline{14}\}$$

$\gcd(0,15) = 15 \neq 1$

$\gcd(1,15) = 1$

$\gcd(2,15) = 1$

$\gcd(3,15) = 3 \neq 1$

$\gcd(4,15) = 1$

$\gcd(5,15) = 5 \neq 1$

$\gcd(6,15) = 3 \neq 1$

$\gcd(7,15) = 1$

$\gcd(8,15) = 1$

$\gcd(9,15) = 3 \neq 1$

$\gcd(10,15) = 5 \neq 1$

$\gcd(11,15) = 1$

$\gcd(12,15) = 3 \neq 1$

$\gcd(13,15) = 1$

$\gcd(14,15) = 1$

Thus,

$$\boxed{\mathbb{Z}_{15}^{\times} = \{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \overline{11}, \overline{13}, \overline{14}\}}$$

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

$\overline{2}\cdot\overline{8}=\overline{16}=\overline{1}$

$\overline{4}\cdot\overline{4}=\overline{16}=\overline{1}$

$\overline{7}\cdot\overline{13}=\overline{91}=\overline{1}$

$\overline{11}\cdot\overline{11}=\overline{121}=\overline{1}$

$\overline{14}\cdot\overline{14}=\overline{196}=\overline{1}$

$$\begin{array}{r} 6 \\ 15\overline{)\,91} \\ -90 \\ \hline 1 \end{array}$$

$$\begin{array}{r} 8 \\ 15\overline{)\,121} \\ -120 \\ \hline 1 \end{array}$$

$$\begin{array}{r} 13 \\ 15\overline{)\,196} \\ -15 \\ \hline 46 \\ -45 \\ \hline 1 \end{array}$$

15
30
45
60
75
90
105
120
⋮

Thus,

$\overline{1}^{-1}=\overline{1}$

$\overline{2}^{-1}=\overline{8}$

$\overline{4}^{-1}=\overline{4}$

$\overline{7}^{-1}=\overline{13}$

$\overline{8}^{-1}=\overline{2}$

$\overline{11}^{-1}=\overline{11}$

$\overline{13}^{-1}=\overline{7}$

$\overline{14}^{-1}=\overline{14}$

Ex: If p is a prime, then

$$\mathbb{Z}_p = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{p-1}\}$$

and

$$\mathbb{Z}_p^{\times} = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$$

because $\gcd(0,p) = p \neq 1$
but if $1 \leq x \leq p-1$, then $\gcd(x,p) = 1$

Ex: 7 is prime so

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

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

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

Then, $\mathbb{Z}_n^\times$ is closed under multiplication.

That is, if $\bar{a}, \bar{b} \in \mathbb{Z}_n^\times$,

then $\bar{a} \cdot \bar{b} \in \mathbb{Z}_n^\times$

proof: Let $\bar{a}, \bar{b} \in \mathbb{Z}_n^\times$.

Then, $\bar{a}$ and $\bar{b}$ have multiplicative inverses $\bar{a}^{-1}$ and $\bar{b}^{-1}$.

So, $\boxed{\bar{a} \cdot \bar{a}^{-1} = \bar{1}}$ and $\boxed{\bar{b} \cdot \bar{b}^{-1} = \bar{1}}$.

Our goal is to show $\overline{a} \cdot \overline{b}$ has a multiplicative inverse and hence is also in $\mathbb{Z}_n^\times$.

Claim: $(\bar{a} \cdot \bar{b})^{-1} = \bar{b}^{-1} \cdot \bar{a}^{-1}$.

We see this is true since

$$(\overline{a}\cdot\overline{b})\cdot(\overline{b}^{-1}\cdot\overline{a}^{-1})$$

$$= \overline{a}\cdot\underbrace{(\overline{b}\cdot\overline{b}^{-1})}_{\overline{1}}\cdot\overline{a}^{-1}$$

$$= \overline{a}\cdot\overline{a}^{-1}$$

$$= \overline{1}$$

So, $\overline{a}\cdot\overline{b}$ has a multiplicate inverse and hence $\overline{a}\cdot\overline{b}\in\mathbb{Z}_n^{\times}$ $\blacksquare$