Math 4460
3/24/25

(Topic 5 continued...)

Notation: If $\bar{a} \in \mathbb{Z}_n$ has a multiplicative inverse, then it's unique inverse will be denoted by $\bar{a}^{-1}$.

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

Define

$$\mathbb{Z}_n^{\times} = \left\{ \bar{a} \in \mathbb{Z}_n \;\middle|\; \begin{array}{c}\bar{a} \text{ has a} \\ \text{multiplicative} \\ \text{inverse}\end{array} \right\}$$

theorem

$$= \left\{ \bar{a} \in \mathbb{Z}_n \;\middle|\; \gcd(a,n) = 1 \right\}$$

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

We have

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

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

$\gcd(1,10) = 1$

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

$\gcd(3,10) = 1$

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

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

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

$\gcd(7,10) = 1$

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

$\gcd(9,10) = 1$

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

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

$\overline{3}^{-1} = \overline{7}$ because $\overline{3} \cdot \overline{7} = \overline{21} = \overline{1}$

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

$\overline{9}^{-1} = \overline{9}$ because $\overline{9} \cdot \overline{9} = \overline{81} = \overline{1}$

$$\boxed{\begin{array}{l} \underline{\text{MATH } 4550/4560} \\ \mathbb{Z}_n \text{ is a group under } + \\ \mathbb{Z}_n^\times \text{ is a group under } \cdot \\ \mathbb{Z}_n \text{ is a ring } (+, \cdot) \end{array}}$$

TEST 1

5C $a, b > 0$, $x = \gcd(a,b)$
$y = \gcd(a, a+b)$

Prove: $x \le y$

proof: Since $x = \gcd(a,b)$ we get $x \mid a$ and $x \mid b$.

So, $a = x\ell$, $b = xm$ where $m, \ell \in \mathbb{Z}$.

Thus, $a+b = x(\ell+m)$

So, $x \mid (a+b)$.

Thus, $x \mid a$ and $x \mid (a+b)$,

So, x is a common divisor of a and $a+b$.

But $y = \gcd(a, a+b)$.

So, $x \le y$ $\blacksquare$

5D) $a, b, c > 0$

If $\gcd(a,b)=1$ and $c \mid a$ then $\gcd(b,c)=1$.

---

proof: Since $\gcd(a,b)=1$ we get $ax+by=1$ where $x, y \in \mathbb{Z}$

Since $c \mid a$ we get $a=ck$ where $k \in \mathbb{Z}$

Thus, $c(kx)+b(y)=1$.

Since $cx_0+by_0=1$ has an integer solution we get $\gcd(c,b)$ divides 1.

HW 2 #12

So, $\gcd(c,b)=1$ $\blacksquare$

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

$$\mathbb{Z}_{15} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \ldots, \overline{13}, \overline{14}\}$$

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

$\gcd(1,15) = 1$

$\gcd(2,15) = 1$

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

$\gcd(4,15) = 1$

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

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

$\gcd(7,15) = 1$

$\gcd(8,15) = 1$

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

$\gcd(10,15) = 5$

$\gcd(11,15) = 1$

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

$\gcd(13,15) = 1$

$\gcd(14,15) = 1$

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

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

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

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

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

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

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

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

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

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

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

$$\begin{array}{r|l} & \;\;6 \\ 15 & \overline{91} \\ & -90 \\ \hline & \;\;\;1 \end{array}$$

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

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

$$\begin{array}{r|l} & \;\;\;8 \\ 15 & \overline{121} \\ & -120 \\ \hline & \;\;\;\;1 \end{array}$$

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

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

$$\begin{array}{r|l} & \;13 \\ 15 & \overline{196} \end{array}$$

$$\begin{array}{r} -195 \\ \hline 1 \end{array}$$

Multiples of 15:

15, 30, 45, 60, 75, 90, 105, 120, 135, 150, 165, 180, 195, ...

For $\overline{14}$:

$$\overline{14} \cdot \overline{14} \underset{\text{mod } 15}{=} \overline{-1} \cdot \overline{-1} = \overline{1}$$

Fact: If p is prime, then

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

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

(because $\gcd(a,p)=1$ if $1 \le a \le p-1$)

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

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

because 7 is prime

MATH 4560 or 5401

$\mathbb{Z}_p$ is called a field when p is prime

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

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

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

---

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

Then $\overline{a}^{-1}$ and $\overline{b}^{-1}$ exist.

Let's show $\overline{a} \cdot \overline{b}$ has a multiplicative inverse.

We have

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

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

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

So, $(\bar{a}\cdot\bar{b})^{-1} = \bar{b}^{-1}\cdot\bar{a}^{-1}$

Thus, $\bar{a}\cdot\bar{b}$ has a multiplicative inverse.

And so, $\bar{a}\cdot\bar{b}\in\mathbb{Z}_n^{\times}$ $\blacksquare$

<u>Theorem:</u> Let p be prime.
Then the only elements of $\mathbb{Z}_p^{\times}$ that are their own inverse are $\bar{1}$ and $\overline{p-1}=\overline{-1}$.

<u>proof:</u>

We have $\bar{1}\cdot\bar{1}=\bar{1}$ and

$\underbrace{\overline{-1}}_{\overline{p-1}}\cdot\underbrace{\overline{-1}}_{\overline{p-1}}=\bar{1}$. So, $\bar{1}$ and $\overline{p-1}=\overline{-1}$ are their own inverse.

Why are these the only ones?

Suppose $\overline{x} \in \mathbb{Z}_p^\times$ is it's own inverse.

Then, $\overline{x} \cdot \overline{x} = \overline{1}$.

So, $\overline{x^2} = \overline{1}$.

Thus, $x^2 \equiv 1 \pmod{p}$.

So, $p \mid (x^2 - 1)$.

So, $p \mid (x+1)(x-1)$.

Since p is prime we get

$p \mid (x+1)$ or $p \mid (x-1)$

$\boxed{\begin{array}{c} p \text{ prime} \\ p \mid ab \end{array}} \Downarrow \boxed{\begin{array}{c} p \mid a \\ \text{or} \\ p \mid b \end{array}}$

So,

$x \equiv -1 \pmod{p}$ or $x \equiv 1 \pmod{p}$.

So either

$$\overline{x} = \overline{-1} \quad \text{or} \quad \overline{x} = \overline{1}.$$

So, $\overline{1}$ and $\overline{p-1} = \overline{-1}$ are the only elements with their own inverse.

$\blacksquare$