

Math 4460

3/24/25

---



# (Topic 5 continued...)

---

Notation: If  $\bar{a} \in \mathbb{Z}_n$

has a multiplicative inverse,

then its unique inverse

will be denoted by  $\bar{a}^{-1}$ .

---

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

Define

$$\mathbb{Z}_n^{\times} = \left\{ \bar{a} \in \mathbb{Z}_n \mid \bar{a} \text{ has a multiplicative inverse} \right\}$$

theorem  $\Rightarrow \left\{ \bar{a} \in \mathbb{Z}_n \mid \gcd(a, n) = 1 \right\}$

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

We have

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

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

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

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

$$\gcd(3, 10) = 1$$

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

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

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

$$\gcd(7, 10) = 1$$

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

$$\gcd(9, 10) = 1$$

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

$$\bar{1}^{-1} = \bar{1} \quad \text{because} \quad \bar{1} \cdot \bar{1} = \bar{1}$$

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

$$\overline{7}^{-1} = \overline{3} \quad \text{because } \nearrow$$

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

MATH 4550 / 4560

$\mathbb{Z}_n$  is a group under  $+$

$\mathbb{Z}_n^*$  is a group under  $\cdot$

$\mathbb{Z}_n$  is a ring  $(+, \cdot)$

# TEST 1

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

Prove:  $x \leq y$

proof: Since  $x = \gcd(a, b)$

we get  $x \mid a$  and  $x \mid b$ .

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

Thus,  $a+b = x(l+m)$

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,  $x \leq y$



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

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

---

proof: Since  $\gcd(a, b) = 1$

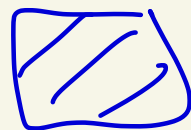
we get  $ax + by = 1$  where  $x, y \in \mathbb{Z}$

Since  $c|a$  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.

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



HW  
2  
#12

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

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

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

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

$$\gcd(2, 15) = 1$$

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

$$\gcd(4, 15) = 1$$

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

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

$$\gcd(7, 15) = 1$$

$$\gcd(8, 15) = 1$$

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

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

$$\gcd(11, 15) = 1$$

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

$$\gcd(13, 15) = 1$$

$$\gcd(14, 15) = 1$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$\begin{array}{r} 13 \\ 15 \overline{) 196} \end{array}$$



Multiples of 15:

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

$\frac{-195}{1}$

For  $\overline{14}$ :

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

↑  
mod 15

Fact: If  $p$  is prime, then

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

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

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

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

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

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

---

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

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

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

We have

$$\begin{aligned} & (\bar{a} \cdot \bar{b}) \cdot (\bar{b}^{-1} \cdot \bar{a}^{-1}) \\ &= \bar{a} \cdot \underbrace{\bar{b} \cdot \bar{b}^{-1}}_{\bar{1}} \cdot \bar{a}^{-1} = \bar{a} \cdot \bar{1} \cdot \bar{a}^{-1} \\ &= \bar{a} \cdot \bar{a}^{-1} = \bar{1} \end{aligned}$$

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

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

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



Theorem: Let  $p$  be prime.

Then the only elements of  $\mathbb{Z}_p^{\times}$  that are their own inverse are  $\bar{1}$  and  $\overline{p-1} = \bar{-1}$ .

proof:

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

$\overline{-1} \cdot \overline{-1} = \bar{1}$ . So,  $\bar{1}$  and  $\overline{p-1} = \bar{-1}$

$$\underbrace{\overline{-1}}_{\overline{p-1}} \cdot \underbrace{\overline{-1}}_{\overline{p-1}}$$

are their own inverse.

Why are these the only ones?

Suppose  $\bar{x} \in \mathbb{Z}_p^*$  is its own inverse.

$$\text{Then, } \bar{x} \cdot \bar{x} = \bar{1}.$$

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

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

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

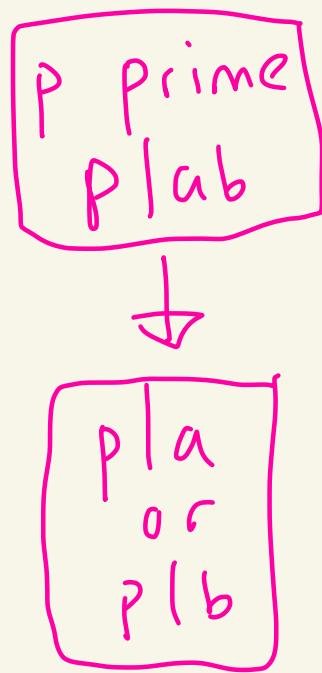
$$\text{So, } p \mid (x+1)(x-1).$$

Since  $p$  is prime we get

$$p \mid (x+1) \text{ or } p \mid (x-1)$$

So,

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



So either

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

So,  $\bar{1}$  and  $\overline{p^{-1}} = \bar{-1}$

are the only elements  
with their own inverse.

