Math 4460 4/5/23

Theorem (from Monday) Let
$$a, n \in \mathbb{Z}$$
 with $n \ge 2$.
Then, \overline{a} has a multiplicative inverse in $\mathbb{Z}n$
if and only if $gcd(a,n) = 1$.
Moreover, if \overline{a} has a multiplicative inverse
in $\mathbb{Z}n$, then that inverse is unique.
proof:
(()) Suppose that $gcd(a,n) = 1$.
Then there exist integers x_0 and y_0
Then there exist integers x_0 and y_0 .
Then there $ax_0 + ny_0 = 1$.
Thus in $\mathbb{Z}n$ we have $\overline{ax_0 + ny_0} = \overline{1}$.
Hence in $\mathbb{Z}n$ we have $\overline{ax_0 + ny_0} = \overline{1}$.
So in $\mathbb{Z}n$ we have $\overline{ax_0 + ny_0} = \overline{1}$.
We know $\overline{n} = \overline{0}$ in $\mathbb{Z}n$,
thus we have $\overline{ax_0} = \overline{1}$.
So, \overline{x}_0 is a multiplicative inverse
for \overline{a} in $\mathbb{Z}n$.

(D) Suppose a has a multiplicative
inverse in Zn.
Then there exists
$$b \in \mathbb{Z}$$
 where
 $a \cdot b = 1$ in Zn.
Let $d = \gcd(a,n)$ 4
Our goal is to show that $d = 1$.
Suppose instead that $d > 1$.
Let's show that this leads to
a contradiction.
Let $c = \frac{n}{d}$. $f = \frac{c \in \mathbb{Z}}{d \ln d}$
Since $d > 1$ we know $c = \frac{n}{d} < n$.
Since n/d are both positive and $d \ln d$
we know $d \leq n$.
So, $1 \leq \frac{n}{d} = c$.

Hence, ergo, thus
$$\overline{c} \neq \overline{o}$$
 in \mathbb{Z}_n .
But on the other hand
 $\overline{c} = \left(\frac{\overline{n}}{d}\right) = \left(\frac{\overline{n}}{d}\right) \cdot \overline{1} = \left(\frac{\overline{n}}{d}\right) \cdot \overline{a} \cdot \overline{b}$
 $= \left(\frac{\overline{n}}{d} \cdot \overline{a}\right) \cdot \overline{b} = \left(\overline{n} \cdot \frac{\overline{a}}{d}\right) \cdot \overline{b}$
 $= \left(\frac{\overline{n}}{d} \cdot \overline{a}\right) \cdot \overline{b} = \overline{o} \cdot \left(\frac{\overline{a}}{d}\right) \cdot \overline{b} = \overline{o}$
 $d \mid a$
 $because$
 $d = gcd(a_n)$

$$S_{0}, \overline{c} = \overline{0}.$$

Thus,
$$\overline{c} \neq \overline{0}$$
 and $\overline{c} = 0$.
Contradiction.
So, $d = l$.

Suppose g, and g2 are both multiplicative inverses for a. Then, $\overline{\alpha} \cdot \overline{g} = \overline{1}$ and $\overline{\alpha} \cdot \overline{g}_2 = \overline{1}$. $\int ef's$ show $\overline{g}_1 = \overline{g}_2$. We have $\overline{g}_1 = \overline{g}_1 \cdot \overline{I} = \overline{g}_1 \cdot (\overline{\alpha} \cdot \overline{g}_2)$ $= (\overline{g}, \overline{\alpha}), \overline{g}_2$

$$= (\overline{a} \cdot \overline{g}_{1}) \cdot \overline{g}_{2}$$

$$= \overline{f}_{2}$$

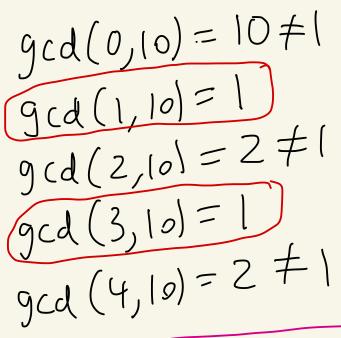
$$= \overline{g}_{2}$$
Notation: If $\overline{a} \in \mathbb{Z}_{n}$
has a multiplicative inverse
then we denote it's unique
inverse by \overline{a}^{-1} .

Def: Let nEZ with n>2. Define Zn=SaEZn | āhas a ? Zn=SaEZn | multiplicative inverse] $= \{ \overline{a} \in \mathbb{Z} \mid | g(d(a,n)) = | \}$

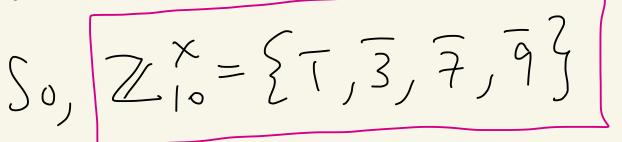
· Un is a group Under + · Za is a group under .

EX: Let's calculate ZIO.

We have $Z_{10} = \{\overline{2}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}\}$

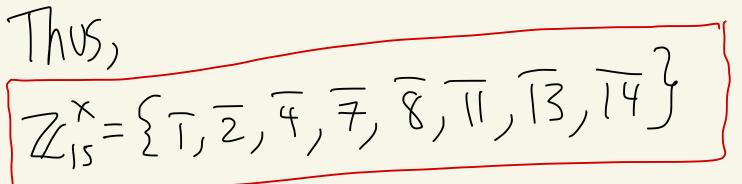


 $gcd(5,10) = 5 \neq 1$ $9cd(6,10) = 2 \neq 1$ 9cd(7,10) = 1gcd (8,10) = Z = 1 gcd(9,10) = 1



 $\sum_{i=1}^{n} \sum_{j=1}^{n} \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} \sum_{i=1}^{n-1} \sum$ $\overline{1}.\overline{1}=\overline{1}$ $\overline{3}, \overline{7} = \overline{21} = \overline{1}$ $\overline{9}, \overline{9} = \overline{81} = \overline{1}$ $\overline{G}^{-1} = \overline{G}$

EXi Let's calculate Zis and every elements multiplicative inverse. $\mathbb{Z}_{15} = \{\overline{2}, \overline{2}, \overline{2}, \overline{2}, \overline{3}, \overline{9}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{7}, \overline{10}, \overline{11}, \overline{12}, \overline{13}, \overline{14}\}$ gcd(8,15)=1 9cd (0,15)=15+1 $gcd(9, 15) = 3 \neq 1$ 9cd(1,15)=1gcd (10,15)=5 = 1 gcd(2,15)=1 gcd(11,15)=1 gcd(3,15)=3=1 $9cd(12,15) = 3 \neq 1$ 9cd(4,15) = 19cd(13,15) = 13gcd(5,15) = 5 = 1 gcd(14,15) = 1 $g_{Ld}(6, [5] = 3 \neq 1$ gcd(7,15) = 1



6 S $\overline{2.8} = \overline{16} = \overline{1}$ 90 30 45 $\overline{4.4} = \overline{16} = \overline{1}$ 60 $\overline{7}.\overline{13} = \overline{91} = \overline{14}$ 8 7S 121 90 $\overline{||\cdot||} = \overline{|2|} = \overline{|}$ _ \ 2 0 05 20 14.14 = 196 = 143 96 Thus, --1 <u>-</u> 8 = 2 45 $\hat{2}^{-1} = \hat{8}$ $\widehat{4} = \widehat{4}$ $[3^{-1} = 7$ $\frac{1}{7} = [3]$ $14^{-1} = 14$

Ex: If p is a prime, then $\mathbb{Z}_{P} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{P} - 1\}$ and $Z_p^{x} = \{\overline{z}, \overline{z}, \dots, p^{-1}\}$ $gcd(0,p)=p\neq 1$ because $|\leq X \leq P-I$, then gcd(X,P)=Jbutif EX: 7 is prime so $Z_{7} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$ $Z_{2}^{X} = \{1, 2, 3, 4, 5, 5\}$

Theorem: Let nEZ with n72. Then, Zn is closed under multiplication. That is, if a, b e Zn, then a.beZn proof: Let a, b E Zn. Then, a and b have multiplicative inverses a and b. So, $\overline{a} \cdot \overline{a}^{-1} = \overline{1}$ and $\overline{b} \cdot \overline{b}^{-1} = \overline{1}$. has Our goal is to show a.b and a multiplicative inverse hence is also in Zn. Claim: $(\overline{a} \cdot \overline{b})^{-1} = \overline{b} \cdot \overline{a}$.

