Math 4460

5/10/23

# HW 5

(5) $\mathbb{Z}_{14}^{\times} = \{\overline{1}, \overline{3}, \overline{5}, \overline{9}, \overline{11}, \overline{13}\}$

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

$\overline{3}^2 = \overline{9}$

$\overline{3}^3 = \overline{27} = \overline{13}$

$\overline{3}^4 = \overline{39} = \overline{11}$

$\overline{3}^5 = \overline{33} = \overline{5}$

$\overline{3}^6 = \overline{15} = \overline{1}$

$\vdots \quad \vdots$ (now repeats)

Since the powers of $\overline{3}$ give us all of $\mathbb{Z}_{14}^{\times}$ we know $\overline{3}$ is a primitive root.

---

$\overline{3} \cdot \overline{5} = \overline{15} = \overline{1}$

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

Since $\overline{3}$ is a primitive root, so is $\overline{5}$.

$\boxed{\text{Thm: If } \overline{a} \in \mathbb{Z}_n^{\times} \text{ is a primitive root, then } \overline{a}^{-1} \text{ is also a primitive root}}$

$\overline{9}$ isn't a primitive root.

$$\overline{9}^1 = \overline{9} = \overline{3}^2$$
$$\overline{9}^2 = (\overline{3}^2)^2 = \overline{3}^4 = \overline{11}$$
$$\overline{9}^3 = (\overline{3}^2)^3 = \overline{3}^6 = \overline{1}$$
$$\vdots \qquad \vdots \quad \text{(now repeats)}$$

---

$$\begin{array}{r} 7 \\ {}^{2}14\overline{)99} \\ -98 \\ \hline 1 \end{array}$$

$$\overline{9} \cdot \overline{11} = \overline{99} = \overline{1}$$

Since $\overline{11} = \overline{9}^{-1}$

and $\overline{9}$ is not a primitive root, $\overline{11}$ won't be a primitive root too.

$\overline{13} = \overline{3}^3$

$\overline{13}^2 = (\overline{3}^3)^2 = \overline{3}^6 = \overline{1}$

$\vdots \quad \vdots$ (repeats)

$\overline{13}$ is not a primitive root.

# Hw 5

## 8/9 modified

Reduce $\overline{3}^{1562}$ in $\mathbb{Z}_{28}^{\times}$

Need $\varphi(28)$

$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$

$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$

$\varphi(28) = \varphi(2^2 \cdot 7^1)$

$= 2^2 \cdot 7\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{7}\right)$

$$= \cancel{2^2} \cdot \cancel{7}\left(\frac{1}{\cancel{2}}\right)\left(\frac{6}{\cancel{7}}\right) = 12$$

Thus, $|\mathbb{Z}_{28}^{\times}| = \varphi(28) = 12$

**Euler:** $\bar{a} \in \mathbb{Z}_n^{\times} \to \bar{a}^{\varphi(n)} = \bar{1}$

So, Euler says:

Since $\bar{3} \in \mathbb{Z}_{28}^{\times}$ we know

$\varphi(28) = 12$

$$\bar{3}^{12} = \bar{1}.$$

$$\begin{array}{r} 130 \\ 12\overline{)1562} \\ -12\phantom{00} \\ \hline 36\phantom{0} \\ -36\phantom{0} \\ \hline 02 \end{array}$$

So,

$$\bar{3}^{1562} = \bar{3}^{12(130)+2}$$

$$= \left(\overline{3}^{12}\right)^{130} \cdot \overline{3}^{2}$$

$$= \overline{1}^{130} \cdot \overline{3}^{2} = \overline{9}$$

---

HW 6

16 Let $z, w \in \mathbb{Z}[i]$. Prove: $w \mid z$ iff $\overline{w} \mid \overline{z}$.

proof:

($\Rightarrow$) Suppose $w \mid z$.

Then, $z = wk$ where $k \in \mathbb{Z}[i]$.

So, $\overline{z} = \overline{wk}$.

Thus, $\overline{z} = \overline{w} \cdot \overline{k}$

Since $\overline{k} \in \mathbb{Z}[i]$ and $\overline{z} = \overline{w} \cdot \overline{k}$

we know $\overline{w} \mid \overline{z}$.

($\Leftarrow$) Suppose $\overline{w} \mid \overline{z}$.

Then by ($\Rightarrow$) we know $\overline{\overline{w}} \mid \overline{\overline{z}}$

Thus, $w \mid z$. $\blacksquare$

---

$\boxed{\text{HW 6}}$

8) Is $2+i$ prime in $\mathbb{Z}[i]$? What are all its divisors?

$$N(2+i) = 2^2 + 1^2 = 5$$ prime

$\boxed{\text{Theorem: If } N(z)=p \text{ where } p \text{ is prime in } \mathbb{Z}, \text{ then}}$

$\mathbb{Z}$ is prime in $\mathbb{Z}[i]$

Using the theorem, $2+i$ is prime.

The divisors of $2+i$ are:

<u>units</u>: $1, -1, i, -i$

<u>associates</u>:

$1 \cdot (2+i) = 2+i$

$-1 \cdot (2+i) = -2-i$

$i \cdot (2+i) = 2i + i^2 = -1+2i$

$-i \cdot (2+i) = -(-1+2i)$

$= 1-2i$

(17) (c) $z \in \mathbb{Z}[i]$

Prove: $z$ is prime iff $\bar{z}$ is prime.

P iff Q $\longleftrightarrow$ $(\neg P)$ iff $(\neg Q)$

<u>We will prove:</u>

$z$ is not prime iff $\bar{z}$ is not prime.

<u>proof:</u>

$(\Rightarrow)$

Suppose $z$ is not prime.

Then $z$ has a divisor $w \in \mathbb{Z}[i]$

where $w$ is not a unit

and $w$ is not an associate of $z$.

$w \neq 1, -1, i, -i$

$w \neq uz$ where $u = 1, -1, i, -i$

Since $w \mid z$ we have

$z = wk$ where $k \in \mathbb{Z}[i]$.

Then, $\overline{z} = \overline{wk} = \overline{w} \cdot \overline{k}$.

So, $\overline{w} \mid \overline{z}$.

Note $\overline{w}$ is not a unit because $w$ is not a unit.

[Using 17(b): $u$ is a unit iff $\overline{u}$ is a unit]

Is $\overline{w}$ an associate of $\overline{z}$?

Suppose it is!

Then, $\overline{w} = u \cdot \overline{z}$ where $u$ is a unit.

This implies $\overline{\overline{w}} = \overline{u\overline{z}}$.

So, $w = \overline{u} \cdot \overline{\overline{z}}$.

$\overline{\overline{a}} = a$

$\overline{ab} = \overline{a}\,\overline{b}$

Then, $w = \overline{u} \cdot z$

Since $u$ is a unit, we know $\overline{u}$ is also a unit.

But then since $w = \overline{u} z$ we would get that $w$ is an associate of $z$.

Contradiction.

Summary: $\overline{w} \mid \overline{z}$ and $\overline{w}$ is not a unit and $\overline{w}$ is not an associate of $\overline{z}$. Thus, $\overline{z}$ is not prime.

($\Leftarrow$) Suppose $\overline{z}$ is not prime.

Then by $(\Rightarrow)$, we know

$\overline{\overline{z}}$ is not prime.

So, $z$ is not prime. $\blacksquare$

---

FINAL – MONDAY

2:30 – 4:30