On Wednesday, you classified the set of primes in $\mathbb{Z}[\omega]$.

<u>Outline</u>: (1) if π : prime in $\mathbb{Z}[\omega]$, then $N(\pi) = \pi \cdot \bar{\pi} =$ either p or p^2.

here, not assoc.

you are an assoc. of a prime

(2) Conversely, any elt. $\eta \in \mathbb{Z}[\omega]$ with $N(\eta) = p$, prime is prime in $\mathbb{Z}[\omega]$.

(3) For $q \equiv 2 \ (3)$, q remains prime in $\mathbb{Z}[\omega]$.

$p \equiv 1 \ (3)$ $\quad p = \pi \cdot \bar{\pi}$ $\quad \pi, \bar{\pi}$ primes "p splits in $\mathbb{Z}[\omega]$"

$p = 3$ $\quad 3 = \underbrace{-\omega^2}_{\text{unit}} \underbrace{(1-\omega)^2}_{\text{prime}}$ "3 ramifies in $\mathbb{Z}[\omega]$".

$$\begin{array}{ccccc} \mathbb{Z}[\omega] & (1-\omega)^2 & \pi \quad \bar{\pi} & q \\ | & | & \backslash\,/ & | \\ \mathbb{Z} & 3 & p & q \\ & & (\equiv 1 \ (3)) & (q \equiv 2 \ (3)) \end{array}$$

Given prime $\pi \in \mathbb{Z}[\omega]$ (any prime) then

$\mathbb{Z}[\omega] / \pi\mathbb{Z}[\omega]$ behaves like $\mathbb{Z}/p\mathbb{Z}$

(in part., every elt. of this ring has mult. inverse (mod π) i.e. field.)

Know $\mathbb{Z}[\omega]$ is Euclidean,

so given $\alpha \not\equiv 0 \pmod{\pi}$ find β, γ s.t. $\alpha\beta + \pi\gamma = 1$

(Bezout's identity)

so β is the mult. inv.

Moreover $\mathbb{Z}[\omega] / \pi\mathbb{Z}[\omega]$ has $N(\pi)$ elts.

if $\pi = q \equiv 2 \ (3)$, q integer prime, then check that

$\{ a + b\omega \mid a, b \in [0, q) \}$ is complete residue system

q^2 elements $= N(q)$.

if $\pi \cdot \bar{\pi} = p \equiv 1 \ (3)$ need set of reps.

$\{0, 1, \ldots, p-1\}$ is set. $\quad \pi = a + b\omega$, $p = a^2 - ab + b^2$, $p \nmid b$.

Given $\eta = m + n\omega$ need to show $\eta \equiv r \pmod{\pi}$

But ~~a~~ m, n are integers (and if $\equiv 0$ (p), then $\equiv 0 \pmod{\pi}$)

$\eta = m + n\omega$ $\quad \pi = a + b\omega$. Find c s.t. $bc \equiv n \pmod p$

then $\eta - c\pi \equiv m - ca \pmod p$ (reduce $m-ca$, if nec., to least residue mod p)

then $\eta \equiv m - ca \pmod p$. ✓.

Just remains to check that if $r, r' \in [0,p)$ s.t. $r \equiv r'$ (π) then $r = r'$.

(Easy. take norms)

Now have Fermat's Little Thm. for $\mathbb{Z}[\omega]$: if $\pi \nmid \alpha$, then

$$\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}.$$

In <u>HW</u>: showed that $1, \omega, \omega^2$ distinct if $N(\pi) \neq 3$. (i.e. π not assoc. of $(1-\omega)$)

and $3 \mid N(\pi) - 1$.

$\Rightarrow$

$$\alpha^{N(\pi)-1} - 1 = \left(\alpha^{N(\pi)-1/3} - 1\right)\left(\alpha^{N(\pi)-1/3} - \omega\right)\left(\alpha^{N(\pi)-1/3} - \omega^2\right)$$

So, since $\alpha^{N(\pi)-1} \equiv 1$ (π) $\Rightarrow$ one of the 3 factors above must be divis. by π.

i.e. $\alpha^{N(\pi)-1/3} \equiv \begin{cases} 1 \\ \omega \\ \omega^2 \end{cases} \pmod{\pi}$.

In this spirit, define $\left(\frac{\alpha}{\pi}\right)_3 = \begin{cases} 1 \\ \omega \\ \omega^2 \end{cases}$ according to $\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{\frac{N(\pi)-1}{3}}$ (π)

(or $= 0$ if $\pi \mid \alpha$.)

✓ have to prove prim. elt. thm in $\mathbb{Z}[\omega]$.

<u>Note</u>: $\left(\frac{\alpha}{\pi}\right)_3 = 1$ iff $x^3 \equiv \alpha$ (π) has solution. (same pf. Need to consider $\alpha^{N(\pi)-1/3} \overset{?}{\equiv} 1$)

and that this "cubic residue symbol" has same nice properties as Legendre symbol.

$$\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3,$$

if $\alpha \equiv \alpha'$ (π), then $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\alpha'}{\pi}\right)_3$.

To formulate cubic reciprocity : better to pick a unique assoc.

Define : π prime in $\mathbb{Z}[\omega]$, then π "primary" if $\pi \equiv 2 \ (3)$.

(makes sense, since, if $q \equiv 2 \ (3)$, then q prime, and

CR is easy for primes of form $3k+2$.

$$\left(\frac{q_1}{q_2}\right) = \left(\frac{q_2}{q_1}\right) \quad)$$

if $\pi = a + b\omega$, then saying $a \equiv 2 \ (3)$, $b \equiv 0 \ (3)$.

Claim : if π prime, $N(\pi) = p \equiv 1 \ (3)$, there is a unique

assoc. π' s.t. π' primary.

e.g. $7 = (3+\omega)(2-\omega)$

$N(3+\omega) = 3^2 - 3 + 1^2 = 7.$ ✓.

$N(2-\omega) = 2^2 + 2 + 1^2 = 7.$

$(2-\omega)(-\omega) = -2\omega + \omega^2$

$= -3\omega + \underbrace{\omega + \omega^2}_{-1}$ ✓.

mult. by $-\omega^2$:

$-3\omega^2 - 1 \equiv 2 \ (3)$ ✓.

Law of Cubic Reciprocity : π_1, π_2 primary, $N(\pi_1), N(\pi_2) \neq 3$, $N(\pi_1) \neq N(\pi_2)$

then $\left(\frac{\pi_1}{\pi_2}\right)_3 = \left(\frac{\pi_2}{\pi_1}\right)_3$.

compare with Q.R.

we'll need supplementary laws to handle units.