Proposition: $\mathbb{Z}[\omega]$ is a Euclidean domain. $\omega = (-1+\sqrt{-3})/2$.

pf: $\alpha = a + b\omega \in \mathbb{Z}[\omega]$, we need a function $\lambda : \mathbb{Z}[\omega] \to \mathbb{Z}_{\geq 0}$

$\lambda = |\alpha| = \alpha\bar{\alpha} = a^2 - ab + b^2$ (why ≥ 0?)
compare $a^2-2ab+b^2$.

Given $\alpha, \beta \in \mathbb{Z}[\omega]$, $\beta \neq 0$, then $\alpha/\beta = \alpha\bar{\beta}/\beta\bar{\beta} = r + s\omega$
some $r, s \in \mathbb{Q}$

(since $\beta\bar{\beta} \in \mathbb{Z}$, $\alpha\bar{\beta} \in \mathbb{Z}[\omega]$)

Find integers m, n s.t.

$|r-m| \leq 1/2$; $|s-n| \leq 1/2$

set $\gamma = m + n\omega$ ← this is our desired quotient.

i.e. pick two elts. consider what happens upon division.

want:
Consider $\rho = \alpha - \gamma\beta$. Either $\rho = 0$

or $\lambda(\rho) = \lambda(\alpha - \gamma\beta) < \lambda(\beta)$.

$$\lambda(\alpha - \gamma\beta) = \lambda(\alpha/\beta - \gamma)\cdot\lambda(\beta)$$

But $\lambda(\alpha/\beta - \gamma)$ should be small

check: $\lambda(\alpha/\beta - \gamma) = (r-m)^2 - (r-m)(s-n) + (s-n)^2$

$\leq 1/4 + 1/4 + 1/4 < 1$. ✓.

so we can indeed do modular arithmetic in $\mathbb{Z}[\omega]$.

Issue 1

Need to determine elements α with $\lambda(\alpha) = 1$. More typically denoted $N(\alpha)$.

(units: invertible elements of $\mathbb{Z}[\omega]$.

if invertible then $\exists\ \beta$ $\alpha\beta = 1$, $N(\alpha)N(\beta) = N(1) = 1$.
so $N(\alpha) = 1$.
since non-neg. ints.)

if $\alpha\bar{\alpha} = 1$, then clearly unit since $\bar{\alpha} \in \mathbb{Z}[\omega]$ as well

Solve : $1 = a^2 - ab + b^2$ want to factor this.

Trick : $4 = \underbrace{4a^2 - 4ab + b^2}_{(2a-b)^2} + 3b^2$

$(2a-b)^2 + 3b^2$

so can have $b = 0, \quad 2a - b = \pm 2$
$b = \pm 1, \quad 2a - b = \pm 1$ } six total:

$1, -1, \omega, -\omega,$
$\underbrace{-1-\omega}_{\omega^2}, \underbrace{1+\omega}_{-\omega^2}.$

since $\omega^2 + \omega + 1 = 0$.

Issue 2 : What are the primes in $\mathbb{Z}[\omega]$?

$7 = (3+\omega)(2-\omega)$ so no longer prime.

Need to be careful - don't want to mistake mult. by units for divisibility.

Investigate using norm again.

$\wp$ prime in $\mathbb{Z}[\omega]$. What can $N(\wp)$ be?

$N(\wp) = n$, some int. And we then have, since n product of primes, ~~[illegible]~~.

$\Rightarrow$ $\wp \mid p$ for some rational prime p. $\quad (\wp\bar{\wp} = n = p_1^{l_1} \cdots p_r^{l_r})$

i.e. $p_1^{l_1} \cdots p_r^{l_r} \equiv 0 \pmod{\wp}$, so $\wp \mid p_i$ some i.

Write ~~$\wp \neq p_i / q$~~, $q \in \mathbb{Z}[\omega]$.
$p_i = \wp \cdot q$

~~[illegible]~~

$\underbrace{N(p_i)}_{p_i^2} = N(\wp \cdot q) = \underline{N(\wp) \cdot N(q)}$

this is a map to $\mathbb{Z}_{\geq 0}$.

so only possibilities are $N(\wp) = p_i^2, \quad N(q) = 1$
$N(\wp) = p_i, \quad N(q) = p_i$

(Know $N(\wp) \neq 1$, since $\wp$ is not a unit.)

Notice that if $N(\wp) = p^2$, then q is unit. so $\wp$ is an "associate" of the rational prime p_i.

Note if $N(\wp) = p_i$, then can't have $\wp = u \cdot p$, some prime p.

(Get $p_i = N(\wp) = N(up) = p^2$. $\not\!\!\!\!\quad$)

Also converse is true. Given elt $z \in \mathbb{Z}[\omega]$ with $N(z) = p$, rat'l prime, then z is a prime in $\mathbb{Z}[\omega]$.

<u>pf</u>: if z not prime, then $z = \alpha\beta$, $N(\alpha), N(\beta) > 1$. (i.e. non-units)

then have $p = N(z) = N(\alpha)N(\beta)$. $\not\!\!\!\!\quad$

Classification of primes. $p \equiv 1 \ (3)$ (p: rat'l prime) then $p = \wp \cdot \bar{\wp}$ with $\wp$: prime in $\mathbb{Z}[\omega]$

if $q \equiv 2 \ (3)$ (q: rat'l prime), then q prime in $\mathbb{Z}[\omega]$ as well.

Lastly, $3 = \underbrace{-\omega^2}_{\text{unit}} (1-\omega)^2$ and $(1-\omega)$ is prime in $\mathbb{Z}[\omega]$.

<u>pf</u>: Given any rat'l prime p, not prime in $\mathbb{Z}[\omega]$, then

$p = \alpha\beta$ with $N(\alpha), N(\beta) > 1$. $p^2 = N(\alpha)N(\beta)$. $\Rightarrow N(\alpha) = N(\beta) = p$.

Write $\alpha = a + b\omega$, $p = N(\alpha) = a^2 - ab + b^2$, i.e. $4p = (2a-b)^2 + 3b^2$

$\Rightarrow p \equiv (2a-b)^2 \pmod 3$. if $3 \nmid p$, then $p \equiv 1 \ (3)$ (only square mod 3)

i.e. $q \equiv 2 \ (3) \Rightarrow q$ prime.

For $p \equiv 1 \ (3)$, use clever trick:

<u>QR</u>: $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{p-1/2} \cdot \left(\frac{p}{3}\right) (-1)^{(p-1/2)(3-1/2)}$

$= \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1.$

$\Rightarrow \quad \exists\ a \pmod p$ s.t. $a^2 \equiv -3 \pmod p$. i.e.

$$p \cdot c = a^2 + 3 = \underbrace{(a + \sqrt{-3})}_{(a+1+2w)}\underbrace{(a - \sqrt{-3})}_{(a-1-2w)} \Rightarrow p \mid \text{one of these}$$

if it were prime.

not possible since then $p \mid 2$. ↯.

so $p^2 = N(\alpha)N(\beta) \Rightarrow N(\alpha) = p = \alpha \cdot \bar{\alpha}$.

Finally last case easy to check. $N(1-\omega) = 3$. ✓.

Now know primes $\wp$ in $\mathbb{Z}[\omega]$. In fact, a lot like $\mathbb{Z}/p\mathbb{Z}$.

Show $\mathbb{Z}[\omega] / \wp\,\mathbb{Z}[\omega]$ is a field.

(easy: if $z \in \mathbb{Z}[\omega]$, $z \not\equiv 0 \ (\wp)$, then using Euclidean alg.

find α, β s.t. $\alpha z + \beta \wp = 1$. i.e. α is a mult. inv. (mod $\wp$).)

Work a bit harder, you can show $\mathbb{Z}[\omega] / \wp\,\mathbb{Z}[\omega]$ has $N(\wp)$

distinct residue classes mod $\wp$.

Conclusion: have an analog of FLT: $\alpha^{N(\wp)-1} \equiv 1 \ (\wp)$.

If $N(\wp) \neq 3$, claim residue classes $\{1, \omega, \omega^2\}$ are distinct in

$\mathbb{Z}[\omega] / \wp\,\mathbb{Z}[\omega]$.

Started this to show:

$$a^{\frac{p-1}{3}} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Know if $p \equiv 1 \ (3)$, then $p = \wp \cdot \bar{\wp}$, $\wp$: prime.

Have $a^{N(\pi)-1} \equiv 1 \pmod{\pi}$

AND : $a^{N(\pi)-1/3} \pmod{\pi}$ must be ~~a~~ number whose cube is $\equiv 1 \ (\pi)$.

Now : $N(\pi) = p$. giving $a^{p-1/3} \equiv$ either $1, \omega, \omega^2 \pmod{\pi}$

---

if $\alpha \in \mathbb{Z}[\omega]$, show $\alpha \equiv$ one of $0, 1, -1$ mod $1-\omega$.

Show that if $N(\wp) \neq 3$,

then $1, \omega, \omega^2$ distinct in $\mathbb{Z}[\omega] / \wp\,\mathbb{Z}[\omega]$.

Conclude that $3 \mid N(\wp) - 1$.

Show that 13 is not a prime in $\mathbb{Z}[\omega]$ by giving an explicit factorization

---

Prove that $\mathbb{Z}[i]$ is a Euclidean domain by finding function $\lambda : \mathbb{Z}[i] \longrightarrow \mathbb{Z}_{\geq 0}$ and mimicking pf. for $\mathbb{Z}[\omega]$.

Factor 2 into irreducible elements in $\mathbb{Z}[i]$.

What are units of $\mathbb{Z}[i]$? Prove your answer is correct.