Last time: $\mathbb{Z}[i] \to$ Euc ring ($\Rightarrow$ PID $\Rightarrow$ UFD)

For $x \in \mathbb{Z}[i]$ put $N(x) = x\bar{x}$

Note $N(xy) = N(x) \cdot N(y)$

Obs 1 $x \in \mathbb{Z}[i]$ is a unit iff $N(x) = 1$

Pf If x is a unit

$xy = 1 \to N(x)N(y) = 1 \Rightarrow N(x) = 1$

If $N(x) = 1 \Rightarrow x\bar{x} = 1 \Rightarrow x$ unit

Cor 1 units of $\mathbb{Z}[i]$ $\{\pm 1, \pm i\}$

Obs 2 If π is a Gaussian prime $\to \pi$ divides ordinary prime!

Pf π divides $N(\pi) = \pi\bar{\pi}$

As $N(\pi)$ is an int it factors $p_1 \cdots p_r$ for primes p_i

Since π prime, π divides some p_i

Strat: to understand Gauss primes: factor ordinary primes in $\mathbb{Z}[i]$

E.g. 1) $2 = 1^2 + 1^2$ ← if can rep 2 as sum of sq int $\Rightarrow$ Norm of some elt $\mathbb{Z}[i]$

$= N(1+i)$ ← not prime

$= (1+i)(1-i) = -i(i+1)^2$ ↪ 2 is the only prime # that has a sq factor

Obs 1 If $\pi \in \mathbb{Z}[i]$ has a prime norm $\Rightarrow \pi$ is a gauss prime

Pf If $\pi = xy$ then $N(\pi) = N(x) \cdot N(y)$

$\to N(x) = 1$ or $N(y) = 1$ (irred in prime)

$\Rightarrow x$ or y unit

E.g. 2) 3 is prime

Reason if $3 = \overbrace{xy}^{\text{not unit}} \Rightarrow 9 = N(x)N(y)$

$\Rightarrow N(x) = 3 \Rightarrow 3 = a^2 + b^2$ impossible

e.g. 3) $5 = 4^2 + 1^2$

$= (2+i)(2-i)$

So, 3 is prime $\iff$ (3) is maximal

$\iff$ no ideal above (3) (except (1))

5 not prime $\iff$ (5) contained in $(2+i)$, $(2-i)$

Strat: given a prime $\#p$ try to find ideals of $\mathbb{Z}[i]$ containing (p). By ideal corr thm, these corr to ideals of $\mathbb{Z}[i]/(p)$

What is $\mathbb{Z}[i]/p\mathbb{Z}[i]$

Well $\mathbb{Z}[i] = \frac{\mathbb{Z}[x]}{(x^2+1)}$

So, $\mathbb{Z}[i]/p\mathbb{Z}[i] \cong \frac{\mathbb{Z}[x]}{(p, x^2+1)} \overset{\text{Can}}{\cong} \frac{\mathbb{F}_p[x]}{x^2+1} = \mathbb{F}_p[i]$!

Goal: understand ideals in $\mathbb{F}_p[i] = \frac{\mathbb{F}[x]}{(x^2+1)}$

$p=2 \Rightarrow x^2+1 = (x+1)^2$

↳ $x+1$ is nilpotent in for $p=2$

$\frac{\mathbb{F}_2[y]}{y^2} \overset{\text{Can}}{\cong} \frac{\mathbb{F}_2[x]}{(x+1)^2} \cong \frac{\mathbb{F}_2[x]}{(x^2+1)}$

↳ Structure Thm

↳ why this is weird

Key point: If x^2+1 has root in $\mathbb{F}_p$

↳ **No root** $\Rightarrow$ x^2+1 is an irreducible of $\mathbb{F}_p$ coef

$\Rightarrow$ gens maximal ideal.

$\Rightarrow$ $\frac{\mathbb{F}_p[x]}{x^2+1}$ a field

$\Rightarrow$ (p) is maximal $\Rightarrow$ p is prime

2) x^2+1 has a root in $\mathbb{F}_p$, say α ($\alpha = \sqrt{-1}$)

$\Rightarrow -\alpha$ also a root, and $\alpha \neq -\alpha$ as p is odd

$\Rightarrow x^2+1 = (x+\alpha)(x-\alpha)$

$$\frac{\mathbb{F}_p[x]}{(x^2+1)} \underset{\text{CRT}}{\simeq} \frac{\mathbb{F}_p[x]}{(x-\alpha)} \times \frac{\mathbb{F}_p[x]}{(x+\alpha)} \simeq \mathbb{F}_p \times \mathbb{F}_p$$

$\Rightarrow$ in $\mathbb{Z}[i]$ $\exists$ 2 ideals between (p) & (1).

$(p) \subset (p, 1+\alpha)$

To determine which case we are in, need to know if x^2+1 has a root in $\mathbb{F}_p$ i.e. if -1 is a sqr in $\mathbb{F}_p$.

Prop p - odd prime

-1 is a sqr iff $p \equiv 1 \pmod 4$

Pf Recall $\mathbb{F}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ (cyclic of ord $p-1$)

If $p \equiv 3 \pmod 4$ then $\mathbb{F}_p$ has ord $p-1 \equiv 2 \pmod 4$

$\Rightarrow$ no elts of order 4

If $p \equiv 1 \pmod 4$ & $4 \mid p-1$

$\Rightarrow \mathbb{F}_p^\times$ has elt of order 4

$\Rightarrow$ root of -1 !

Summary

If p prime

a) $p=2$ $\quad 2 = -i(i+1)^2$

b) $p \equiv 1 \bmod 4$ $\quad p = \pi_1 \pi_2$ in $\mathbb{Z}[i]$

In fact, $\pi_2 = \overline{\pi_1}$ (conjugate) $\Big\}$ $p = \pi\overline{\pi}$, $\pi = a+bi$, $p = a^2+b^2$

c) $p \equiv 3 \bmod 4$ $\Rightarrow$ p is a prime!