Math 4460
5/5/25

On test 2 I wrote
GSF = your grade so far
This is your grade if you don't take the final

Final = test 1 + test 2
Use those tests and study guides to study.
The final can replace one or both tests

Final = Mon, 5/12, 2:30-4:30

Weds - I'll be here for any questions if you have any

Gaussian integers continued...

<u>Theorem:</u> Let z, v, w be Gaussian integers. If z is prime in the Gaussian integers and $z \mid vw$, then $z \mid v$ or $z \mid w$.

<u>proof:</u> online notes

<u>Application:</u>

Let p be an odd prime in $\mathbb{Z}$. When does $p = x^2 + y^2$ where $x, y \in \mathbb{Z}$?

Ex: $5 = 2^2 + 1^2$

$3 = x^2 + y^2$ ← no integer solutions

Theorem: Let $p \equiv 3 \pmod 4$ be an odd prime. Then $p = x^2 + y^2$ has no integer solutions x, y.

proof:

Suppose $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$. Then in $\mathbb{Z}_4$ we would have

$$\overline{p} = \overline{x}^2 + \overline{y}^2.$$

Note that if $\overline{a} \in \mathbb{Z}_4$

then $\bar{a}^2 = \bar{0}$ or $\bar{a}^2 = \bar{1}$

by the following table →

$\bar{a}$	$\bar{a}^2$
$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$
$\bar{2}$	$\bar{4} = \bar{0}$
$\bar{3}$	$\bar{9} = \bar{1}$

This implies that

$$\bar{x}^2 + \bar{y}^2 = \bar{0}$$

or
$$\bar{x}^2 + \bar{y}^2 = \bar{1}$$

or
$$\bar{x}^2 + \bar{y}^2 = \bar{2}$$

But $p \equiv 3 \pmod 4$, so $\bar{p} = \bar{3}$ in $\mathbb{Z}_4$

So, $\bar{p} = \bar{x}^2 + \bar{y}^2$ is impossible.

$\blacksquare$

Theorem: Let $p \in \mathbb{Z}$ be an odd prime with $p \equiv 1 \pmod 4$. Then $p = x^2 + y^2$ has integer solutions.

---

proof:

From Topic 5, since $p \equiv 1 \pmod 4$ there exists $\bar{x} \in \mathbb{Z}_p^\times$ where $\bar{x}^2 = \overline{-1}$ in $\mathbb{Z}_p^\times$.

So, $x^2 \equiv -1 \pmod p$.

Thus, $\boxed{x^2 + 1 = pk}$ where $k \in \mathbb{Z}$.

Then, $(x+i)(x-i) = pk$ in $\mathbb{Z}[i]$.

Thus, $p \mid (x+i)(x-i)$ in $\mathbb{Z}[i]$.

<u>Claim:</u> p is not prime in $\mathbb{Z}[i]$.

<u>pf of claim:</u> If p was prime in $\mathbb{Z}[i]$ then either $p \mid (x+i)$ or $p \mid (x-i)$ in $\mathbb{Z}[i]$.

But then either

$$\frac{x+i}{p} \quad \text{or} \quad \frac{x-i}{p} \quad \text{is in } \mathbb{Z}[i].$$

So either

$$\frac{x}{p} + \frac{1}{p} i \quad \text{or} \quad \frac{x}{p} - \frac{1}{p} i \quad \text{is in } \mathbb{Z}[i].$$

But $\frac{1}{p} \notin \mathbb{Z}$, so the above is not true.

$\boxed{\text{claim}}$ —

Since p is not prime in $\mathbb{Z}[i]$ we know that p has a divisor $z \in \mathbb{Z}[i]$ where z is not a unit and not an associate of p.

$$\boxed{z \neq \underbrace{1, -1, -i, i}_{\text{unit}}, \underbrace{p, -p, -ip, ip}_{\text{associates of } p}}$$

Then $p = zk$ where $k \in \mathbb{Z}[i]$.

Thus, $\underbrace{N(p)} = N(zk)$.

$p = p + 0i$

$N(p) = p^2 + 0^2 = p^2$

So, $p^2 = \underbrace{N(z)}\underbrace{N(k)}$

equation in $\mathbb{Z}$

these are non-negative integers in $\mathbb{Z}$

Since p is prime in $\mathbb{Z}$ the above gives three possibilities:

(i) $N(z)=1$, $N(k)=p^2$

(ii) $N(z)=p$, $N(k)=p$

(iii) $N(z)=p^2$, $N(k)=1$

But (i) can't hold because z is not a unit so $N(z)\neq 1$.

If (iii) was true then $N(k)=1$ gives k is a unit and then $p=zk$ would give $z=k^{-1}p$ which gives z is an associate of p which isn't true.

Thus, (ii) is true.

So, $N(z) = p$.

Suppose $z = x + iy$.

Then $\underbrace{x^2 + y^2}_{N(z)} = p$.

$\blacksquare$

<u>Note:</u> Let p be an odd prime in $\mathbb{Z}$.

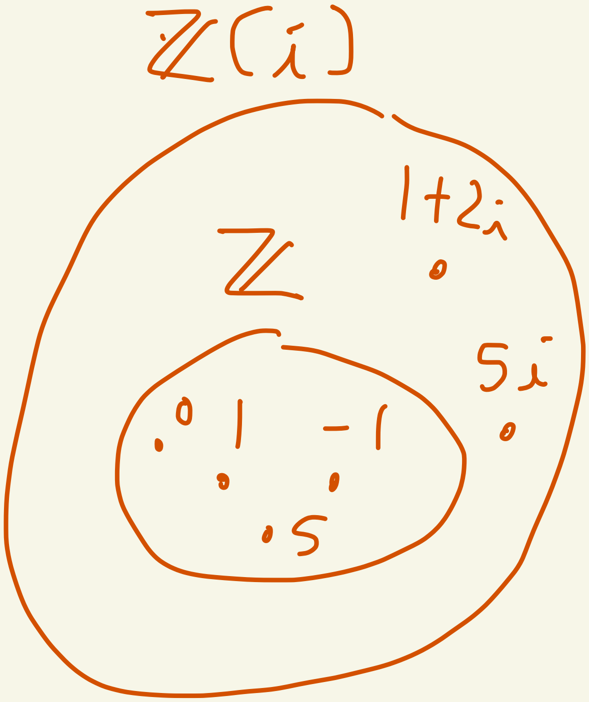
If $p \equiv 1 \pmod 4$, then p is not prime in $\mathbb{Z}[i]$

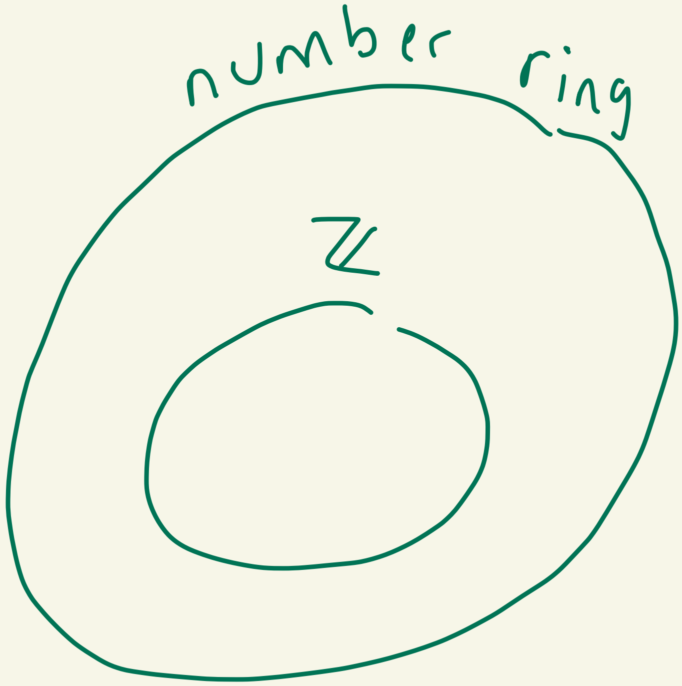
If $p \equiv 3 \pmod 4$, then p is prime in $\mathbb{Z}[i]$.

Also, 2 is not prime in $\mathbb{Z}[i]$

Ex: $2 = (1+i)(1-i)$

$5 = (2-i)(2+i)$





Algebraic number theory
