Math 4460

5/8/23

Theorem: Let $p \in \mathbb{Z}$ be an odd prime with $p \equiv 1 \pmod{4}$. Then p is the sum of two squares.

Proof:

By a theorem from last week since p is an odd prime with $p \equiv 1 \pmod{4}$ there exists $\bar{x} \in \mathbb{Z}_p^\times$ where

$\bar{x}^2 = \overline{-1}$ in $\mathbb{Z}_p^\times$.

Then, $x^2 \equiv -1 \pmod{p}$.

So, $x^2 - (-1) = pk$ where $k \in \mathbb{Z}$.

That is, $\boxed{x^2+1 = pk}$.

Then, $(x-i)(x+i) = pk$

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

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

Why?

If p was prime in $\mathbb{Z}[i]$,

since $p \mid (x+i)(x-i)$ we

would have $p \mid (x+i)$ or $p \mid (x-i)$

But

$$\frac{x+i}{p} = \frac{x}{p} + \frac{1}{p} i \notin \mathbb{Z}[i]$$

not an integer

and

$$\frac{x-i}{p} = \frac{x}{p} - \frac{1}{p} i \notin \mathbb{Z}[i]$$

So $p \nmid (x+i)$ and $p \nmid (x-i)$.

Thus, p is not prime in $\mathbb{Z}[i]$

$\boxed{\text{Claim}}$

So, p has a divisor $z \in \mathbb{Z}[i]$ where z is not a unit and not an associate of p.

<u>Ex:</u> 2 is not prime

<u>units</u>	<u>associates</u>	<u>other factors</u>
$1, -1, i, -i$	$2, -2, 2i, -2i$	$1+i, -1+i, -1-i, 1-i$

Thus, $p = zk$ where $k \in \mathbb{Z}[i]$

Then, $N(p) = N(zk)$

$$\boxed{\begin{array}{l} p = p + i0 \\ N(p) = p^2 \end{array}}$$

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

non-negative integers

So, $N(z) = 1$, p, or p^2

Can $N(z) = 1$?

No, because z is not a unit!

Can $N(z) = p^2$?

If $N(z) = p^2$, then $N(k) = 1$.

Then k is a unit and $k^{-1} \in \mathbb{Z}[i]$
and k^{-1} is a unit.

Multiply $p = zk$ by k^{-1} to get

$$z = k^{-1} p.$$

But then z would
be an associate of p which
it isn't.

Thus, therefore, ergo, we must
have $N(z) = p$.

Suppose $z = x + iy$ where $x, y \in \mathbb{Z}$.

Then, $x^2 + y^2 = p$ and p
is the sum of squares $\blacksquare$

<u>Corollary:</u> If $p \in \mathbb{Z}$ is an odd prime with $p \equiv 1 \pmod 4$ then p is not prime in the Gaussian integers $\mathbb{Z}[i]$.

<u>proof:</u> We saw this in the above proof. $\blacksquare$

<u>Ex:</u> $p = 5 \equiv 1 \pmod 4$

$5 = (1+2i)(1-2i)$

<u>Theorem</u> (HW 6 #15)

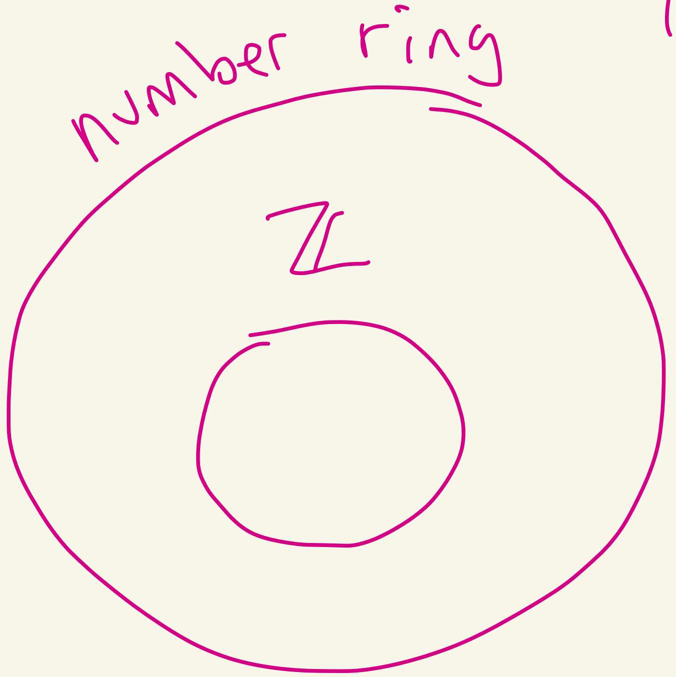
Let $p \in \mathbb{Z}$ be an odd prime with $p \equiv 3 \pmod 4$

then p is prime in the Gaussian integers $\mathbb{Z}[i]$

Ex: $p = 3$

$p = 11$

etc



Algebraic Number Theory

Review time

HW 5

(13) Prove that 19 is not a divisor of $4n^2+4$ for any integer n.

<u>proof:</u> Suppose it is!

Then, $4n^2+4 = 19k$ where $k \in \mathbb{Z}$.

multiples of 19

19
38
57
76
⋮

Then in $\mathbb{Z}_{19}$ we have

$$\overline{4}\,\overline{n}^2 + \overline{4} = \overline{0}.$$

So, $\overline{4}\,\overline{n}^2 = \overline{15}$.

Thus, $\boxed{\overline{5}\cdot\overline{4}\,\overline{n}^2 = \overline{5}\cdot\overline{15}}$

Since $\overline{20} = \overline{1}$ and $\overline{75} = \overline{18}$ in $\mathbb{Z}_{19}$ we get that

$$\boxed{\overline{n}^2 = \overline{18}.}$$

multiples of 19

19
38
57
76
95
114
133
⋮

But in $\mathbb{Z}_{19}$ we have

$\overline{0}^2 = \overline{0}$

$\overline{1}^2 = \overline{1}$

$\overline{2}^2 = \overline{4}$

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

$\overline{4}^2 = \overline{16}$

$\overline{5}^2 = \overline{25} = \overline{6}$

$\overline{6}^2 = \overline{36} = \overline{17}$

$\overline{7}^2 = \overline{49} = \overline{11}$

$\overline{8}^2 = \overline{64} = \overline{7}$

$\overline{9}^2 = \overline{81} = \overline{5}$

$\overline{10}^2 = \overline{100} = \overline{5}$

$\overline{11}^2 = \overline{(-8)}^2 = \overline{8}^2 = \overline{7}$

$\overline{12}^2 = \left(\overline{-7}\right)^2 = \overline{7}^2 = \overline{11}$

$\overline{13}^2 = \overline{17}$

$\overline{14}^2 = \overline{6}$

$\overline{15}^2 = \overline{16}$

$\overline{16}^2 = \overline{9}$

$\overline{17}^2 = \overline{4}$

$\overline{18}^2 = \overline{1}$

There is no $\bar{n} \in \mathbb{Z}_{19}$ with $\bar{n}^2 = \overline{18}$. Contradiction.

Thus, $19 \nmid (4n^2+4)$ when $n \in \mathbb{Z}$ $\blacksquare$

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

19 Let $w, y, z \in \mathbb{Z}[i]$.

Prove: If w is a unit and $z \mid wy$, then $z \mid y$.

<u>proof:</u> Let w be a unit and $z \mid wy$.

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

Since w is a unit, we know $w^{-1} \in \mathbb{Z}[i]$.

Multiplying by w^{-1} we get

$$\cancel{w^{-1}} w y = w^{-1} z k.$$

Thus, $y = z(w^{-1}k)$.

Since $w^{-1}, k \in \mathbb{Z}[i]$ we know $w^{-1}k \in \mathbb{Z}[i]$

Thus, $z \mid y$. ∎