Math 4460

5/3/23

Ex: Find all the divisors of 2 in $\mathbb{Z}[i]$.

Suppose $z \in \mathbb{Z}[i]$ and $z \mid 2$.

Then $2 = zw$ where $w \in \mathbb{Z}[i]$.

So, $N(2) = N(zw)$

$N(a+bi) = a^2 + b^2$

Thus, $4 = \underbrace{N(z)}\underbrace{N(w)}$

non-negative integers

So, $N(z) = 1, 2,$ or 4.

Case 1: Suppose $N(z) = 1$

Then, $\boxed{z = 1, -1, i, \text{ or } -i}$

These all divide 2.

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

Case 2: Suppose $N(z) = 4$

Let $z = a + bi$.

Then $a^2 + b^2 = 4$. $\leftarrow$ $\boxed{\begin{array}{c} a = \pm 2, b = 0 \\ \hline a = 0, b = \pm 2 \end{array}}$

So, $\boxed{z = 2, -2, 2i, \text{ or } -2i.}$

These are the associates of 2 and so divide 2.

Case 3: Suppose $N(z) = 2$

Let $z = a + bi$.

Then $a^2 + b^2 = 2$.

Then $z = 1+i, 1-i, -1+i$, or $-1-i$.

This gives possible divisors of 2, but need to check if they are.

Let's see.

$$\frac{2}{1+i} = \frac{2}{1+i} \cdot \frac{1-i}{1-i} = \frac{2-2i}{1-i+i-i^2} = \frac{2-2i}{2}$$

$$= 1 - i$$

So, $\boxed{2 = (1+i)(1-i)}$

Similarly, $\frac{2}{-1+i} = -1-i$ and

$$\boxed{2=(-1+i)(-1-i)}$$

The divisors of 2 are

$\underbrace{1, -1, i, -i}_{\text{units}}, \underbrace{2, -2, 2i, -2i}_{\text{associates}}, \underbrace{1+i, 1-i, -1+i, -1-i}_{\text{extra ones}}$

So 2 is <u>not</u> prime in $\mathbb{Z}[i]$ $\blacksquare$

<u>Theorem:</u> Let $z \in \mathbb{Z}[i]$.
If $N(z)$ is prime in $\mathbb{Z}$,
then z is prime in $\mathbb{Z}[i]$.

<u>proof:</u> HW 6 #18 $\square$

<u>Ex:</u> $N(1+i) = 1^2 + 1^2 = 2$

Since 2 is prime in $\mathbb{Z}$ by the theorem $1+i$ is prime in $\mathbb{Z}[i]$.

The converse

"If z is prime in $\mathbb{Z}[i]$, then $N(z)$ is prime in $\mathbb{Z}$"

is not always true.

For example, let $z = 3$ is prime in $\mathbb{Z}[i]$ (we saw that on monday), but $N(3) = 3^2 = 9$

which is not prime in $\mathbb{Z}$.

Theorem: Let $z, v, w \in \mathbb{Z}[i]$

Suppose z is prime in $\mathbb{Z}[i]$.

If $z \mid vw$, then $z \mid v$ or $z \mid w$.

proof: Look at online notes. $\blacksquare$

Application of $\mathbb{Z}[i]$

Let p be an odd prime in $\mathbb{Z}$.

What are conditions on p

so that $p = x^2 + y^2$

has integer solutions x, y ?

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

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

We need a theorem to help us.

Theorem: Let p be an odd prime in $\mathbb{Z}$ where $p \equiv 1 \pmod 4$. Then there exists $\overline{x} \in \mathbb{Z}_p^\times$ where $\overline{x}^2 = \overline{-1}$. $\leftarrow$ [$x^2 \equiv -1 \pmod p$]

Ex: $p = 13 \equiv 1 \pmod 4$

$$\mathbb{Z}_{13}^{\times} = \{\underbrace{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}}_{\text{first half}}, \underbrace{\overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{12}}_{\text{2nd half}}\}$$

Let $\overline{x} = \overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \overline{4} \cdot \overline{5} \cdot \overline{6}$

$$\boxed{6 = \frac{13-1}{2} = \frac{p-1}{2}}$$

Then

$$\overline{x}^2 = \overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \overline{4} \cdot \overline{5} \cdot \overline{6} \cdot \overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \overline{4} \cdot \overline{5} \cdot \overline{6}$$

$$= \overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \overline{4} \cdot \overline{5} \cdot \overline{6} \cdot \underbrace{\overline{-1} \cdot \overline{-2} \cdot \overline{-3} \cdot \overline{-4} \cdot \overline{-5} \cdot \overline{-6}}_{\text{even \# of terms}}$$

$$= \overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \overline{4} \cdot \overline{5} \cdot \overline{6} \cdot \overline{12} \cdot \overline{11} \cdot \overline{10} \cdot \overline{9} \cdot \overline{8} \cdot \overline{7}$$

$$= \overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \overline{4} \cdot \overline{5} \cdot \overline{6} \cdot \overline{7} \cdot \overline{8} \cdot \overline{9} \cdot \overline{10} \cdot \overline{11} \cdot \overline{12}$$

$$= \overline{12!} = \overline{-1} \text{ by } \text{Wilson's thm.}$$

$\blacksquare$

If there exists $x, y \in \mathbb{Z}$ where $p = x^2 + y^2$ then we say that p is the <u>sum of two squares.</u>

<u>Ex:</u> $5 = 1^2 + 2^2$ is the sum of two squares

3 is not the sum of two squares.

<u>Q:</u> What odd primes are the sum of two squares?

If p is an odd prime then either $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$.

<u>Theorem</u>: Let p be an odd prime in $\mathbb{Z}$ with $p \equiv 3 \pmod 4$. Then p is <u>not</u> the sum of two squares.

<u>Proof</u>: Note that if $\overline{a} \in \mathbb{Z}_4$, then by Table 1 we have $\overline{a}^2 = \overline{0}$ or $\overline{a}^2 = \overline{1}$.

Table 1

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

(In $\mathbb{Z}_4$)

By Table 2, if

$\overline{x}, \overline{y} \in \mathbb{Z}_4$

then

$\overline{x}^2 + \overline{y}^2 \neq \overline{3}$

Table 2

$\overline{x}^2$	$\overline{y}^2$	$\overline{x}^2 + \overline{y}^2$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{0}$	$\overline{1}$	$\overline{1}$
$\overline{1}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{2}$

(In $\mathbb{Z}_4$)

Let p be an odd prime with $p \equiv 3 \pmod 4$. If $p = x^2 + y^2$ with $x, y \in \mathbb{Z}$, then $\overline{3} = \overline{p} = \overline{x}^2 + \overline{y}^2$ in $\mathbb{Z}_4$ which isn't possible. So, p is not the sum of two squares. $\blacksquare$