Topic 6 -
The Gaussian integers

Recall the set of complex numbers is

$$\mathbb{C} = \{ x + iy \mid x, y \in \mathbb{R} \}$$

and $i^2 = -1$.

Adding:

$$(a+bi) + (c+di) = (a+c) + (b+d)i$$

multiplying:

$$\begin{aligned}(a+bi)(c+di) &= ac + adi + bci + bdi^2 \\ &= ac + adi + bci - bd \\ &= (ac-bd) + (ad+bc)i\end{aligned}$$

Ex:

$$(1-2i)+\left(5+\tfrac{1}{2}i\right)=6-\tfrac{3}{2}i$$

$$(1+\pi i)(-1-i) = -1 - i - \pi i - \pi i^2$$

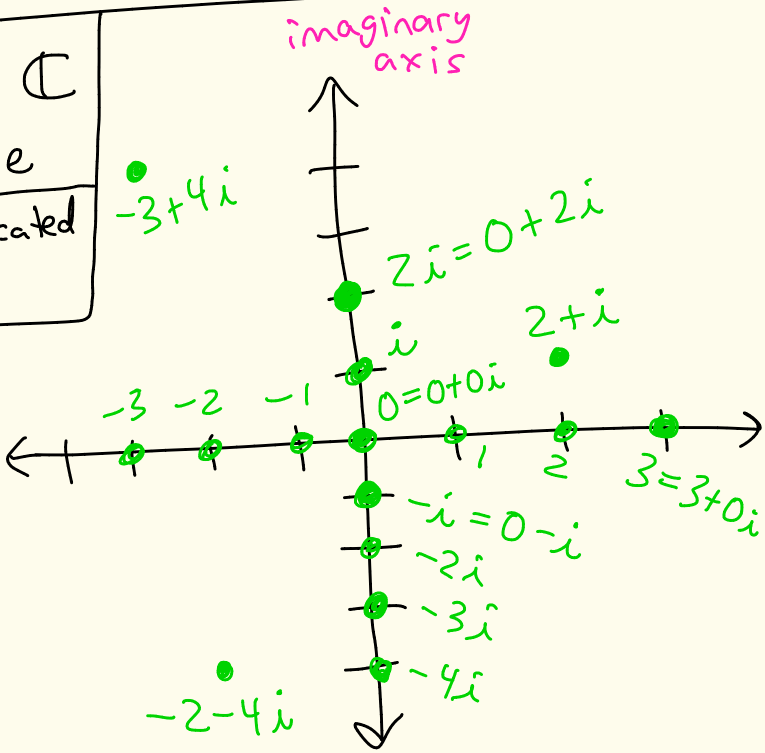
$$= -1 - i - \pi i + \pi$$

$i^2=-1$

$$= (-1+\pi)+(-1-\pi)i$$

We draw $\mathbb{C}$ as a plane

$x+iy$ is located at (x,y)



Def: Let $z = x + iy \in \mathbb{C}$.

The conjugate of z is

$$\overline{z} = x - iy$$

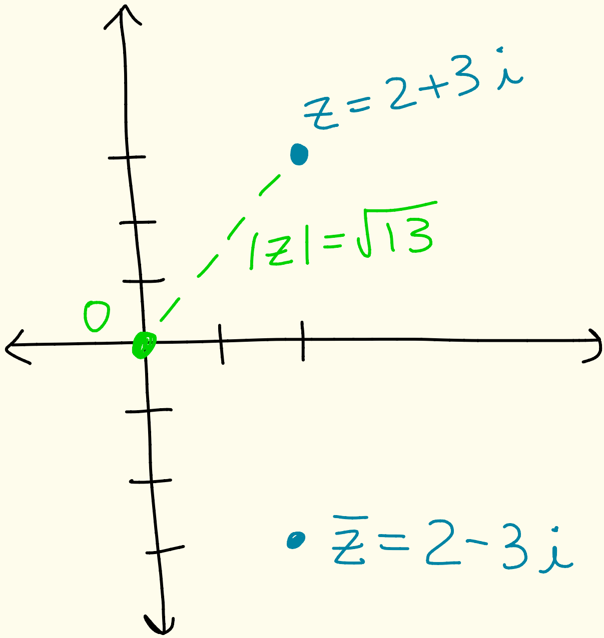
The absolute value of z is

$$|z| = \sqrt{x^2 + y^2}$$

Ex:

$z = 2 + 3i$

$$|z| = \sqrt{2^2 + 3^2}$$
$$= \sqrt{13}$$



Division in $\mathbb{C}$

$$\frac{a+bi}{c+di} = \frac{a+bi}{c+di} \cdot \frac{c-di}{c-di} = \text{simplify}$$

Works because

$$(c+di)(c-di) = c^2 - \cancel{cdi} + \cancel{cdi} \underbrace{- d^2 i^2}_{d^2}$$

$$= c^2 + d^2$$

which is a positive real number

Technique removes i from denominator

Ex:

$$\frac{1-2i}{2+3i} = \frac{1-2i}{2+3i} \cdot \frac{2-3i}{2-3i}$$

$$= \frac{2-3i-4i+6i^2}{4-\cancel{6i}+\cancel{6i}-9i^2}$$

$6i^2 \leftarrow -6$

$-9i^2 \leftarrow 9$

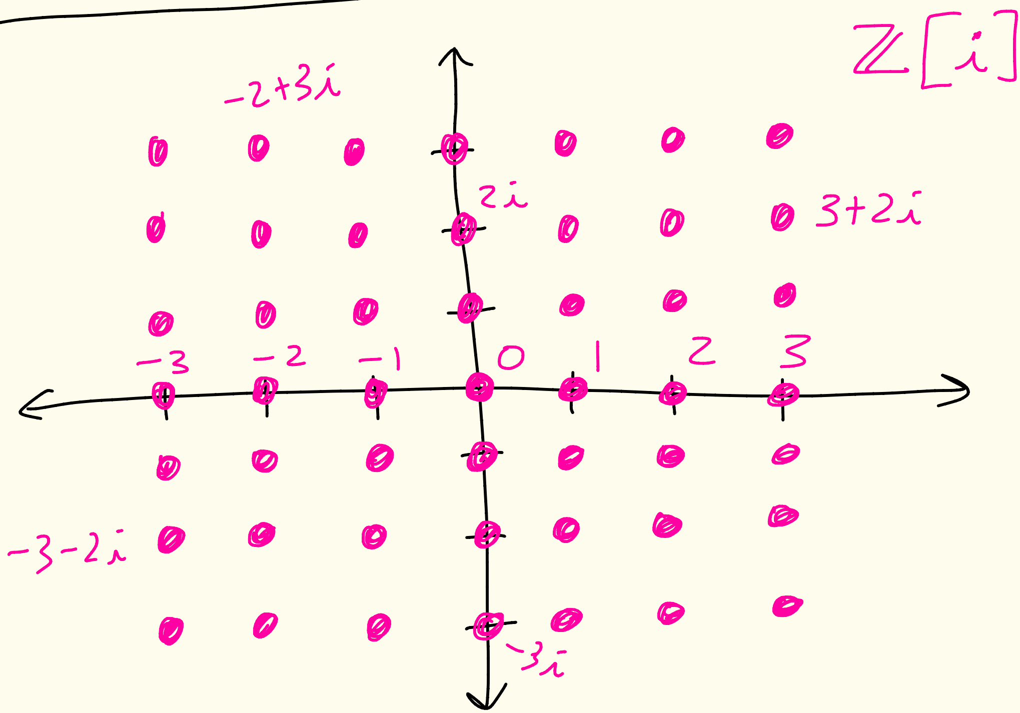
$\boxed{i^2=-1}$

$$= \frac{-4-7i}{13} = \boxed{\frac{-4}{13} - \frac{7}{13}i}$$

Def: The set

$$\mathbb{Z}[i] = \{ a + bi \mid a, b \in \mathbb{Z} \}$$

is called the <u>Gaussian integers</u>



Note: $\mathbb{Z} \subseteq \mathbb{Z}[i]$

Note: If $z, w \in \mathbb{Z}[i]$, then

$$\left.\begin{array}{l} z+w \in \mathbb{Z}[i] \\ z\cdot w \in \mathbb{Z}[i] \end{array}\right\}$$

$\mathbb{Z}[i]$ is closed under addition and multiplication

proof:
See formulas on pg 4 of the notes ▨

Note: $\mathbb{Z}[i]$ is not closed under division.
For example, $1-2i, 2+3i \in \mathbb{Z}[i]$
but

$$\frac{1-2i}{2+3i} = \frac{-4}{13} - \frac{7}{13}i \notin \mathbb{Z}[i]$$

<u>Def:</u> Let

$z = a+bi \in \mathbb{Z}[i]$.

The <u>norm</u> of z is

$$N(z) = z\bar{z} = a^2+b^2$$

<u>Note:</u> $N(z) = |z|^2$

<u>Ex:</u>

$$N(1+i) = (1+i)(1-i)$$
$$= 1 - \cancel{i} + \cancel{i} - i^2$$
$$= 1-(-1) = 2$$

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

Then,

① $N(z)$ is an integer and $N(z) \geq 0$

② $N(z) = 0$ iff $z = 0$

③ $N(zw) = N(z)\, N(w)$

proof:

Let $z = a+bi$, $w = c+di$ where $a, b, c, d \in \mathbb{Z}$

① $N(z) = a^2 + b^2$ is a non-negative integer.

② $N(z) = a^2 + b^2 = 0$ iff $a = b = 0$ iff $z = a+bi = 0$

(3) We have that

$$N(zw) = N[(a+bi)(c+di)]$$

pg 4

$$= N[(ac-bd)+(ad+bc)i]$$

$$= (ac-bd)^2 + (ad+bc)^2$$

$$= a^2c^2 - \cancel{2abcd} + b^2d^2 + a^2d^2 + \cancel{2abcd} + b^2c^2$$

$$= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2$$

$$= (a^2+b^2)(c^2+d^2)$$

$$= N(a+bi) \cdot N(c+di)$$

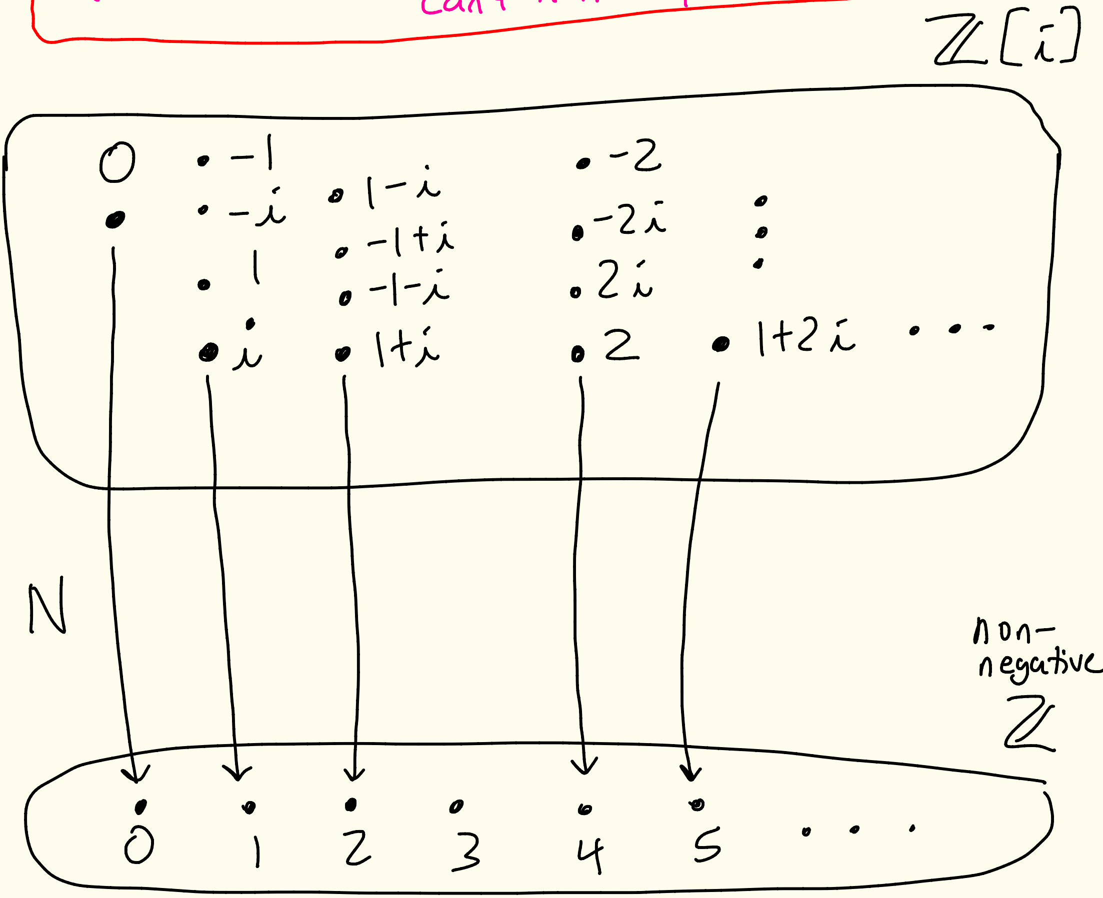
$$= N(z)\,N(w) \qquad \blacksquare$$

I think about the norm function as a way to move equations from $\mathbb{Z}[i]$ down to $\mathbb{Z}$.

$N(i) = N(0 + 1 \cdot i) = 0^2 + 1^2 = 1$

$N(1+i) = 1^2 + 1^2 = 2$

$N(a+ib) = 3 \iff a^2 + b^2 = 3$ can't happen



In $\mathbb{Z}$, we say that $u \in \mathbb{Z}$ is a <u>unit</u> if $\frac{1}{u} \in \mathbb{Z}$.
The units of $\mathbb{Z}$ are $1, -1$.

<u>Def:</u> Let $u \in \mathbb{Z}[i]$.
We say that u is a <u>unit</u> in $\mathbb{Z}[i]$ if $\frac{1}{u}$ is also in $\mathbb{Z}[i]$

<u>Ex:</u> $\frac{1}{1} = 1 \leftarrow$ 1 is a unit

$\frac{1}{-1} = -1 \leftarrow$ -1 is a unit

$\frac{1}{i} = \frac{1}{i} \cdot \frac{-i}{-i} = \frac{-i}{1} = -i \in \mathbb{Z}[i] \leftarrow$ i is a unit

$\frac{1}{-i} = -\frac{1}{i} = -(-i) = i \in \mathbb{Z}[i] \leftarrow$ $-i$ is a unit

Theorem: Let $z \in \mathbb{Z}[i]$.
Then, z is a unit iff $N(z)=1$.
Thus, the only units of $\mathbb{Z}[i]$ are $1, -1, i, -i$.

proof:

($\Longrightarrow$) Suppose $z \in \mathbb{Z}[i]$ is a unit.
Then, $w = \frac{1}{z}$ is in $\mathbb{Z}[i]$ and $zw = 1$

Apply the norm function we get that $\underbrace{N(zw)}_{N(z)N(w)} = \underbrace{N(1)}_{1}$.

So, $N(z)N(w) = 1$ where $N(z)$ and $N(w)$ are non-negative integers (ie in $\mathbb{Z}$ and not negative)

Thus, $N(z)=N(w)=1$. So, $N(z)=1$.

$(\Leftarrow)$ Suppose $z \in \mathbb{Z}[i]$ and $N(z) = 1$.

Then, $z = a + bi$ where $a, b \in \mathbb{Z}$ and $a^2 + b^2 = 1$.

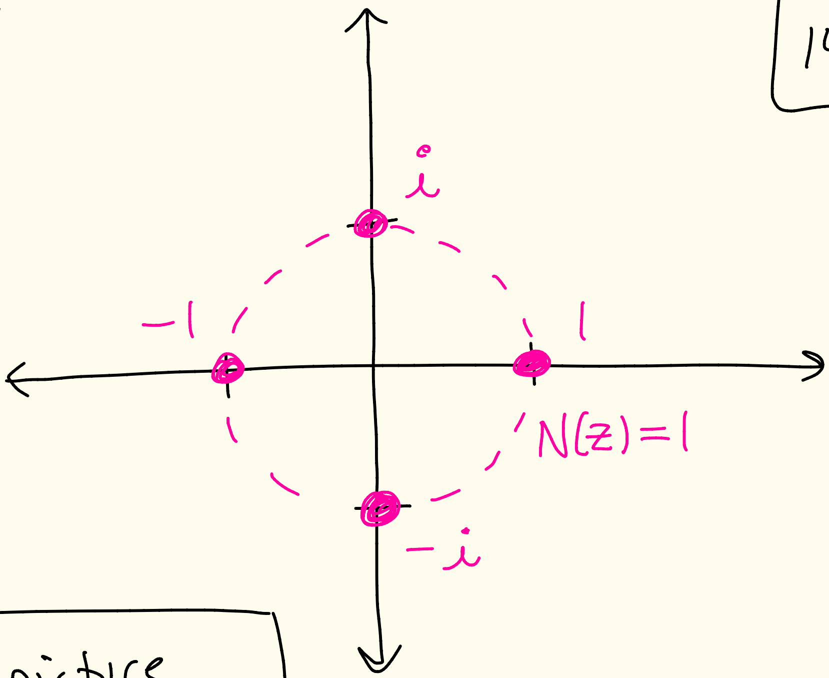
The only solutions to this equation are $(a,b) = (1,0), (-1,0), (0,1), (0,-1)$

These solutions correspond to $z = 1, -1, i, -i$.

These are all units as we saw earlier.

So, z is a unit. $\blacksquare$

picture of units

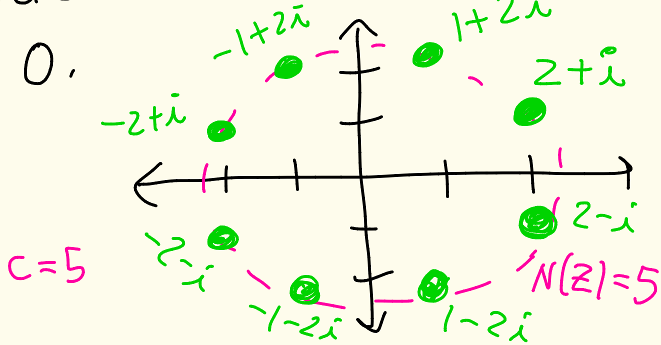


General picture of $N(z)=c$

$z = x+iy$, $c \in \mathbb{Z}$, $c \geq 0$

$N(z)=c$ is $x^2+y^2=c$

This is a circle of radius $\sqrt{c}$ centered at 0.



<u>Def:</u> Let $z, w \in \mathbb{Z}[i]$.
We say that z <u>divides</u> w if there exists $k \in \mathbb{Z}[i]$ where $w = zk$.
If z divides w, we say that z is a <u>divisor</u> of w and write $z \mid w$.

<u>Ex:</u> $2 \mid 6$ because $6 = (2)\underbrace{(3)}_{\text{in } \mathbb{Z}[i]}$

$(1+i) \mid 2$ because $2 \underset{\boxed{i^2=-1}}{=} (1+i)(1-i)$

Ex: Let's find all the divisors of 3 in $\mathbb{Z}[i]$.

We know

$$3 = (1)(3)$$
$$3 = (-1)(-3)$$
$$3 = (i)(-3i)$$
$$3 = (-i)(3i)$$

So, $\boxed{1, -1, i, -i, 3, -3, 3i, -3i}$ are all divisors of 3.

Are there any more divisors of 3? 17

Suppose $3 = zw$ where $z, w \in \mathbb{Z}[i]$.

Apply the norm function to get

$$\underbrace{N(3)}_{3^2+0^2=9} = \underbrace{N(zw)}_{N(z)N(w)}$$

So, $9 = \underbrace{\underbrace{N(z)}\,\underbrace{N(w)}}_{\text{non-negative integers dividing } 9}$.

Let's see what z can be

same answer will apply to w

We know $N(z)$ is a non-negative integer that divides 9.

So, $N(z) = 1, 3,$ or 9.

If $N(z)=1$, then $z = 1, -1, i,$ or $-i$ which are all divisors of 3 from earlier.

There are no solutions to $N(z)=3$ because if $z=a+ib$ then $\underbrace{a^2+b^2}_{N(z)}=3$ cannot be solved for $a,b\in\mathbb{Z}$.

a	b	a^2+b^2
0	0	0
±1	0	1
0	±1	1
±2	0	$4>3$
$\vdots$	$\vdots$	$\vdots$

all bigger than 3

What about $N(z)=9$?

If $z=a+ib$ the solutions to $\underbrace{a^2+b^2}_{N(z)}=9$ are $(a,b)=(3,0),(-3,0),(0,3),(0,-3)$ which correspond to $z=3,-3,3i,-3i,$ which are all divisors of 3 we saw earlier.

We have covered all the cases.

So, the only divisors of 3 are

$$1, -1, i, -i \quad \longleftarrow \text{units}$$

$$3, -3, 3i, -3i \quad \longleftarrow \text{associates of } 3$$

<u>Def:</u> Let $z \in \mathbb{Z}[i]$.
The elements

$$z, \ -z, \ iz, \ -iz$$

are called the <u>associates</u>
<u>of z</u>.

z times each unit

<u>Note:</u> If $z \in \mathbb{Z}[i]$ then

$$z = (1)(z)$$
$$z = (-1)\cdot(-z)$$
$$z = (i)(-iz)$$
$$z = (-i)(iz)$$

every Gaussian integer z is divisible by the units $1, -1, i, -i$ and its associates $z, -z, iz, -iz$

Def: Let $z \in \mathbb{Z}[i]$.
We say that z is <u>prime</u> in $\mathbb{Z}[i]$ if

1. z is not a unit

units are $1, -1$ $i, -i$

and 2. the only divisors of z are the units $(1, -1, i, -i)$ and the associates of z $(z, -z, iz, -iz)$

Ex: we showed that the only divisors of $z = 3$ are $\underbrace{1, -1, i, -i}_{\text{units}}$, $\underbrace{3, -3, 3i, -3i}_{\text{associates of } z=3}$

Also, $z = 3$ is not a unit. So, 3 is prime in $\mathbb{Z}[i]$.

<u>Ex:</u> Let $z = 2$.

Then,

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

in $\mathbb{Z}[i]$.

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

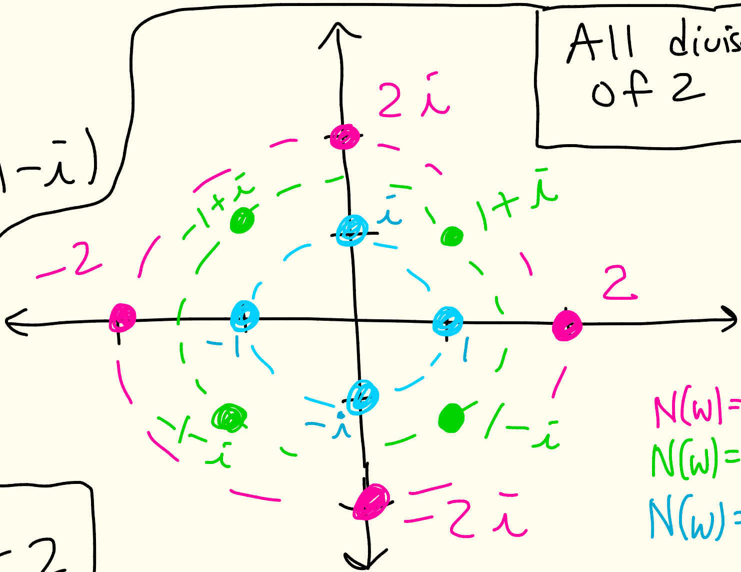
So, $1+i$ and $1-i$ are divisors of 2 and they aren't units or associates of 2.

Also,

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

In HW 6 you show these → are all the divisors of 2

All divisors of 2



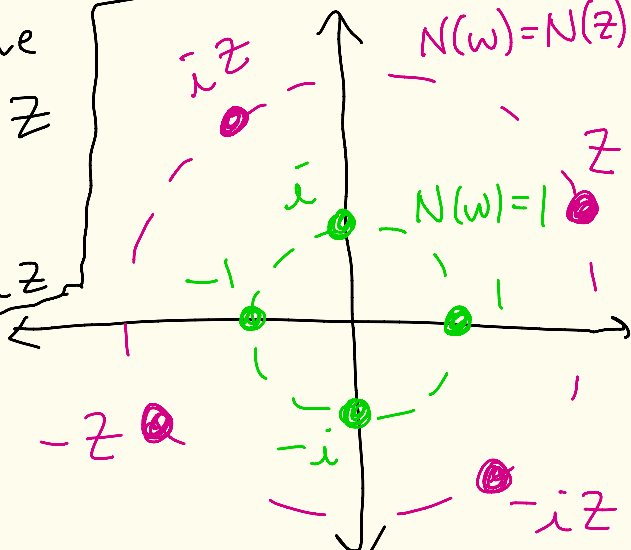
$N(w)=4$
$N(w)=2$
$N(w)=1$

Ex: $z = 5$

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

$2+i$ is a divisor of 5.
$2+i$ is not a unit and not an associate of z.
Thus, 5 is not prime.

Ex: Let z be prime in $\mathbb{Z}[i]$. The only divisors of z are $1, -1, i, -i$ and $z, -z, iz, -iz$



picture of divisors of a prime

HW 6 - 18

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

Ex: $z = 1+i$

$N(1+i) = 1^2 + 1^2 = 2$ ← prime in $\mathbb{Z}$

Thus, by HW 6 - #18,
$1+i$ is prime in $\mathbb{Z}[i]$

Note: The converse of HW 6 #18 is not true. That is, HW 6 #18 is not if and only if. For example, $z=3$ is prime in $\mathbb{Z}[i]$ but $N(3) = N(3+0i) = 3^2+0^2 = 9$ which is not prime in $\mathbb{Z}$.

<u>Thm:</u> (Division algorithm for $\mathbb{Z}[i]$)
Let $z, w \in \mathbb{Z}[i]$ with $w \neq 0$.
Then there exist $q, r \in \mathbb{Z}[i]$
where

$$z = qw + r$$

and $0 \leq N(r) < N(w)$.

<u>proof:</u> Let $z = a + ib$
and $w = c + id$ where $a, b, c, d \in \mathbb{Z}$
and $w = c + id \neq 0$.

Then,

$$\frac{z}{w} = \frac{a+ib}{c+id} \cdot \frac{c-id}{c-id}$$

$$= \underbrace{\left(\frac{ac+bd}{c^2+d^2}\right)}_{A} + i \underbrace{\left(\frac{bc-ad}{c^2+d^2}\right)}_{B} = A + iB$$

here $A, B \in \mathbb{Q}$

Note that A and B are rational numbers.

Choose integers α and β that are as close to A and B as possible.

That is, let $\alpha, \beta \in \mathbb{Z}$ where

$$\boxed{\begin{aligned} |A-\alpha| &\leq \tfrac{1}{2} \\ \text{and} \quad |B-\beta| &\leq \tfrac{1}{2}. \end{aligned}} \quad (*)$$

Ex:
$A + iB = \frac{1}{8} + i\frac{7}{8}$

$\alpha = 0$

$\beta = 1$

Let $q = \alpha + i\beta$

and $r = z - wq.$

r must satisfy $z = wq + r$ so we define it this way

Then, $z = wq + r.$

And,

$$|r| = |z - wq| = |z - w\underbrace{(\alpha + i\beta)}_{q}| = |w|\left|\frac{z}{w} - (\alpha+i\beta)\right|$$

$$= |w|\,|(A+iB) - (\alpha + i\beta)|$$

$$= |w|\,|(A-\alpha) + i(B-\beta)| = |w|\sqrt{(A-\alpha)^2 + (B-\beta)^2}$$

By (*)

$$\leq |w|\sqrt{\left(\tfrac{1}{2}\right)^2 + \left(\tfrac{1}{2}\right)^2} = \frac{|w|}{\sqrt{2}} < |w|.$$

Thus, $0 \leq N(r) = |r|^2 < |w|^2 = N(w).$ ∎

Ex: Let $z = 10+2i$ and $w = 2-3i$.
Let's apply the division algorithm to get $z = qw + r$ with $0 \leq N(r) < N(w)$.

$$\frac{z}{w} = \frac{10+2i}{2-3i} \cdot \frac{2+3i}{2+3i}$$

$i^2 = -1$

$$= \frac{20 + 30i + 4i + 6i^2}{2^2 + \cancel{6i} - \cancel{6i} - 3^2 i^2}$$

$$= \frac{14 + 34i}{13} = \underbrace{\frac{14}{13}}_{\approx 1.077} + \underbrace{\frac{34}{13}}_{\approx 2.615} i$$

$$= A + Bi$$

Set
$$q = \alpha + \beta i = 1 + 3i$$

Set

$$
\begin{aligned}
r &= z - q w \\
&= (10+2i) - (1+3i)(2-3i) \\
&= 10 + 2i - [2 - 3i + 6i - 9i^2] \\
&= 10 + 2i - 2 + 3i - 6i - 9 \\
&= -1 - i
\end{aligned}
$$

Then,

$$N(w) = N(2-3i) = 2^2 + (-3)^2 = 13$$

and

$$0 \le N(r) = N(-1-i) = (-1)^2 + (-1)^2$$
$$= 2 < 13 = N(w)$$

So, $\underbrace{(10+2i)}_{z} = \underbrace{(1+3i)}_{q}\underbrace{(2-3i)}_{w} + \underbrace{(-1-i)}_{r}$

and $0 \le N(r) < N(w)$. $\square$

<u>Theorem:</u> 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 $z \mid w$.

<u>proof:</u> Suppose z is prime and $z \mid vw$.

<u>case 1: Suppose $z \mid v$.</u>
If this is the case, we are done.

<u>case 2: Suppose $z \nmid v$.</u>
We must show that $z \mid w$.
By the division algorithm there exist q, r in $\mathbb{Z}[i]$ with

$$v = qz + r$$

and $0 \leq N(r) < N(z)$.

Since $z \nmid v$ we know $r \neq 0$.
Thus, $N(r) \neq 0$.
Therefore, $0 < N(r) < N(z)$.

Let

$$S = \{ az + bv \mid a, b \in \mathbb{Z}[i] \}$$
$$= \{ 1 \cdot z + 0 \cdot v,\ i \cdot z + (1-i) \cdot v, \dots \}$$

$v = qz + r$

Note that

$$r = (-q) \cdot z + 1 \cdot v \in S.$$

Thus, since $N(r) > 0$, we know that S contains an element with positive norm.

Let d be an element of S of minimal positive norm.

That is, ① $d \in S$
② $N(d) > 0$
③ If $d' \in S$ and $0 < N(d')$, then $N(d) \le N(d')$

Since $d \in S$ we may write

$$d = a_0 z + b_0 v$$

where $a_0, b_0 \in \mathbb{Z}[i]$.

Then,

$$N(d) \le N(r) < N(z)$$

$r \in S$, so by ③ on previous page $N(d) \le N(r)$

division algorithm pg. 1

<u>Claim: $d \mid z$</u>

By the division algorithm there exists $q', r' \in \mathbb{Z}[i]$ where

$$z = q'd + r'$$

and $0 \le N(r') < N(d)$.

Note that

$$
\begin{aligned}
r' &= z - q'd \\
&= z - q'\underbrace{[a_0 z + b_0 v]}_{d} \\
&= z - q'a_0 z - q'b_0 v \\
&= \underbrace{(1-q'a_0)}_{\text{in } \mathbb{Z}[i]} z + \underbrace{(-q'b_0)}_{\text{in } \mathbb{Z}[i]} v \in S
\end{aligned}
$$

Thus, $r' \in S$ and $0 \leq N(r') < N(d)$.

We can't have $0 < N(r')$ because this would contradict property ③ of d from page 2.

Thus, $N(r') = 0$.

Therefore, $r' = 0$.

Hence, $z = q'd + \underbrace{r'}_{0} = q'd$.

Hence, $d \mid z$. $\boxed{\text{claim}}$

Claim: d is a unit

Since d is a divisor of z and z is prime, either d is a unit $(1, -1, i, -i)$ or d is an associate of z $(z, -z, iz, -iz)$.

Let's rule out d being an associate of z.

Suppose $d = uz$ where u is a unit.

Then,

$$N(z) = N(q'd) = N(q'uz)$$
$$= N(q')\underbrace{N(u)}_{1}N(z)$$
$$= N(q')N(z).$$

Dividing by $N(z)$ we get $1 = N(q')$.

So, q' is a unit.

Thus,

$$N(z) = N(q'd) = \underbrace{N(q')}_{1} N(d)$$

$$= N(d)$$

But we can't have $N(z) = N(d)$ because we know from earlier that $N(d) \leq N(r) < N(z)$.

Contradiction.

Hence d is not an associate of z, it is a unit. $\boxed{\text{claim}}$

Now for the finale!

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

Multiplying $d = a_0 z + b_0 v$ by wd^{-1} we get that

$$(wd^{-1})d = (wd^{-1})\left[a_0 z + b_0 v\right].$$

Which gives

$$w = (wd^{-1}a_0)z + (wd^{-1}b_0)v$$

We know that $z \mid vw$, thus $vw = zk$ where $k \in \mathbb{Z}[i]$.

So,

$$\begin{aligned} w &= (wd^{-1}a_0)z + (d^{-1}b_0)vw \\ &= (wd^{-1}a_0)z + (d^{-1}b_0)zk \\ &= \underbrace{\left[wd^{-1}a_0 + d^{-1}b_0 k\right]}_{\text{in } \mathbb{Z}[i]} z. \end{aligned}$$

Therefore $z \mid w$. $\blacksquare$

(11) Find all the divisors of 2 in $\mathbb{Z}[i]$.

Suppose $w \in \mathbb{Z}[i]$ is a divisor of 2.

Then, $2 = wz$ where $z \in \mathbb{Z}[i]$.

So, $N(2) = N(wz)$.

$2 = 2 + 0i$

$N(2) = 2^2 + 0^2 = 4$

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

non-negative integers that divide 4

Thus, $\boxed{N(w) = 1, 2, \text{ or } 4.}$

Case 1: $N(w) = 1$

In this case, w is a unit.

So, $\boxed{w = 1, -1, i, \text{ or } -i}$

These are all divisors of 2.

case 2: $N(w)=4$

Suppose $w=a+bi$, where $a,b\in\mathbb{Z}$.

Then, $\underbrace{a^2+b^2}_{N(w)}=4$

The solutions are

$$(a,b)=\underbrace{(2,0)}_{2^2+0^2=4},\ \underbrace{(0,2)}_{0^2+2^2=4},\ \underbrace{(-2,0)}_{(-2)^2+0^2=4},\ \overbrace{(0,-2)}^{4=0^2+(-2)^2}$$

These correspond to

$$w=2+0i,\ 0+2i,\ -2+0i,\ 0-2i$$
$$=\boxed{2,\ 2i,\ -2,\ -2i}$$

These are the associates of 2 and we know these are divisors of 2.

Every Gaussian integer is divisible by its associates

Case 3: $N(w) = 2$

Let $w = a+bi$.

Then, $\underbrace{a^2+b^2}_{N(w)} = 2$

The solutions are

$$(a,b) = \underbrace{(1,1)}_{2=1^2+1^2}, \underbrace{(-1,1)}_{2=(-1)^2+1^2}, \overbrace{(1,-1)}^{2=1^2+(-1)^2}, \underbrace{(-1,-1)}_{2=(-1)^2+(-1)^2}$$

Thus,

$$w = 1+i, \ -1+i, \ 1-i, \ -1-i$$

Now we must verify which of these are actually divisors of 2.

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

$$= \frac{2-2i}{2} = 1-i \in \mathbb{Z}[i]$$

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

Thus, $1+i$ and $1-i$ are divisors of 2.

You can verify that

$$\frac{2}{-1+i} = -1-i.$$

So, $2 = (-1-i)(-1+i)$.

So, $-1-i$ and $-1+i$ are divisors of 2.

The divisors of 2 are

$$\boxed{\begin{array}{l} 1, -1, i, -i \\ 2, -2, 2i, -2i \\ 1+i, 1-i, -1+i, -1-i \end{array}}$$

$\blacksquare$

Our goal now is to figure out what odd primes $p \in \mathbb{Z}$ can be written in the form $p = x^2 + y^2$.

We need one more thm and then we will be ready to do this

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

<u>Ex:</u> $p = 13 \equiv 1 \pmod 4$

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

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

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

$$= \overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \overline{4} \cdot \overline{5} \cdot \overline{6} \cdot \underbrace{\overline{-1} \cdot \overline{-2} \cdot \overline{-3} \cdot \overline{-4} \cdot \overline{-5} \cdot \overline{-6}}_{6\ -1\text{'s cancel}}$$

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

$$= \overline{(13-1)!} = \overline{-1}$$

Wilson's thm

Proof of theorem:

Since $p \equiv 1 \pmod 4$ we know that
$p-1 = 4n$ for some positive integer n.

Thus, $\frac{p-1}{2} = 2n$ is an even integer.

Let

$$\overline{x} = \underbrace{\overline{1} \cdot \overline{2} \cdot \overline{3} \cdots \overline{\left(\frac{p-1}{2}\right)}}_{\frac{p-1}{2} \text{ terms}} \qquad (*)$$

in $\mathbb{Z}_p^\times$.

Also, since there are an even number of terms in $(*)$ we know

$$\overline{x} = \overline{-1} \cdot \overline{-2} \cdot \overline{-3} \cdots \overline{\left[-\left(\frac{p-1}{2}\right)\right]}$$

Also note that

$$\overline{p-k} = \overline{p} + \overline{-k} = \overline{-k}$$

in $\mathbb{Z}_p^\times$.

Thus,

$$
\begin{aligned}
\overline{x}^2 &= \overline{x} \cdot \overline{x} \\
&= \left[\overline{1} \cdot \overline{2} \cdot \overline{3} \cdots \overline{\tfrac{p-1}{2}}\right]\left[\overline{-1} \cdot \overline{-2} \cdot \overline{-3} \cdots \overline{-\left(\tfrac{p-1}{2}\right)}\right] \\
&= \left[\overline{1} \cdot \overline{2} \cdot \overline{3} \cdots \overline{\tfrac{p-1}{2}}\right]\left[\overline{p-1} \cdot \overline{p-2} \cdot \overline{p-3} \cdots \underbrace{\overline{p-\left(\tfrac{p-1}{2}\right)}}_{\frac{p+1}{2}}\right] \\
&= \overline{1} \cdot \overline{2} \cdot \overline{3} \cdots \overline{\tfrac{p-1}{2}} \cdot \overline{\tfrac{p+1}{2}} \cdots \overline{p-3} \cdot \overline{p-2} \cdot \overline{p-1} \\
&= \overline{(p-1)!} = \overline{-1}
\end{aligned}
$$

Wilson's Thm

So, $\overline{x} \in \mathbb{Z}_p^\times$ with $\overline{x}^2 = \overline{-1}$. ▨

Def: We say that an integer n is the <u>sum of two squares</u> if there exist integers x and y with
$n = x^2 + y^2$.

Ex:

$2 = 1^2 + 1^2$ ← 2 is the sum of two squares

$3 = x^2 + y^2$ ← has no integer solutions. So 3 is not the sum of two squares

$4 = 2^2 + 0^2$ ← 4 is the sum of two squares

- $p=2$ is the sum of two squares since $2=1^2+1^2$. This takes care of the even prime.

The odd primes fall into two cases: $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$

Theorem: Let p be an odd prime with $p \equiv 3 \pmod 4$. Then p is not the sum of two squares.

proof: Let $a \in \mathbb{Z}$. Then by table 1 $\bar{a}^2 = \bar{0}$ or $\bar{a}^2 = \bar{1}$ in $\mathbb{Z}_4$.

table 1

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

(In $\mathbb{Z}_4$)

Let $x, y \in \mathbb{Z}$.

Then by Table 2 $\overline{x}^2 + \overline{y}^2 \neq \overline{3}$ in $\mathbb{Z}_4$.

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 $\mathbb{Z}_4$)

Thus if p is an odd prime with $p \equiv 3 \pmod 4$ then since $\overline{p} = \overline{3}$ in $\mathbb{Z}_4$ we know $\overline{p} = \overline{x}^2 + \overline{y}^2$ has no solutions in $\mathbb{Z}_4$.

Thus, $p = x^2 + y^2$ has no solutions in $\mathbb{Z}$. ∎

<u>Theorem:</u> Let p be an odd prime with $p \equiv 1 \pmod 4$. Then p is the sum of two squares.

<u>proof:</u>

By our first theorem today, there exists an integer x where

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

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

Thus, $\underbrace{x^2+1}_{x^2-(-1)} = pk$ for some $k \in \mathbb{Z}$.

Hence,

$$pk = x^2+1 = (x+i)(x-i)$$

Thus, p divides $(x+i)(x-i)$ in the Gaussian integers.

If p was prime in the Gaussian integers, then $p \mid (x+i)$ or $p \mid (x-i)$ in the Gaussian integers.

But

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

$\pm\frac{1}{p} \notin \mathbb{Z}$

and

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

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

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

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

Also, $p = zw$ where $w \in \mathbb{Z}[i]$.

Thus, $\underbrace{N(p)}_{N(p+0i)=p^2+0^2=p^2} = N(zw)$.

So, $\boxed{p^2 = N(z)N(w)}$

Hence, $N(z)$ is a non-negative integer that divides p^2.

Since p is prime, we know
$$N(z) = 1, p, \text{ or } p^2.$$

We can't have $N(z)=1$ because then z would be a unit, which it isn't.

Why can't $N(z)=p^2$.
Suppose $N(z)=p^2$.
Then $N(w) = 1$.
So, then w would be a unit.
Then, $z = w^{-1}p$ which is an associate of p, which can't happen.

Therefore, $N(z) = p$.

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

Then $N(z) = x^2 + y^2$.

So, $p = x^2 + y^2$. $\blacksquare$

If you look at the proof above we also proved the following.

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

<u>proof:</u> See pg. 47 $\blacksquare$

Theorem: (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 $\mathbb{Z}[i]$.