Math 4460

4/21/23

Topic 6 – Gaussian Integers

<u>Def:</u> The set

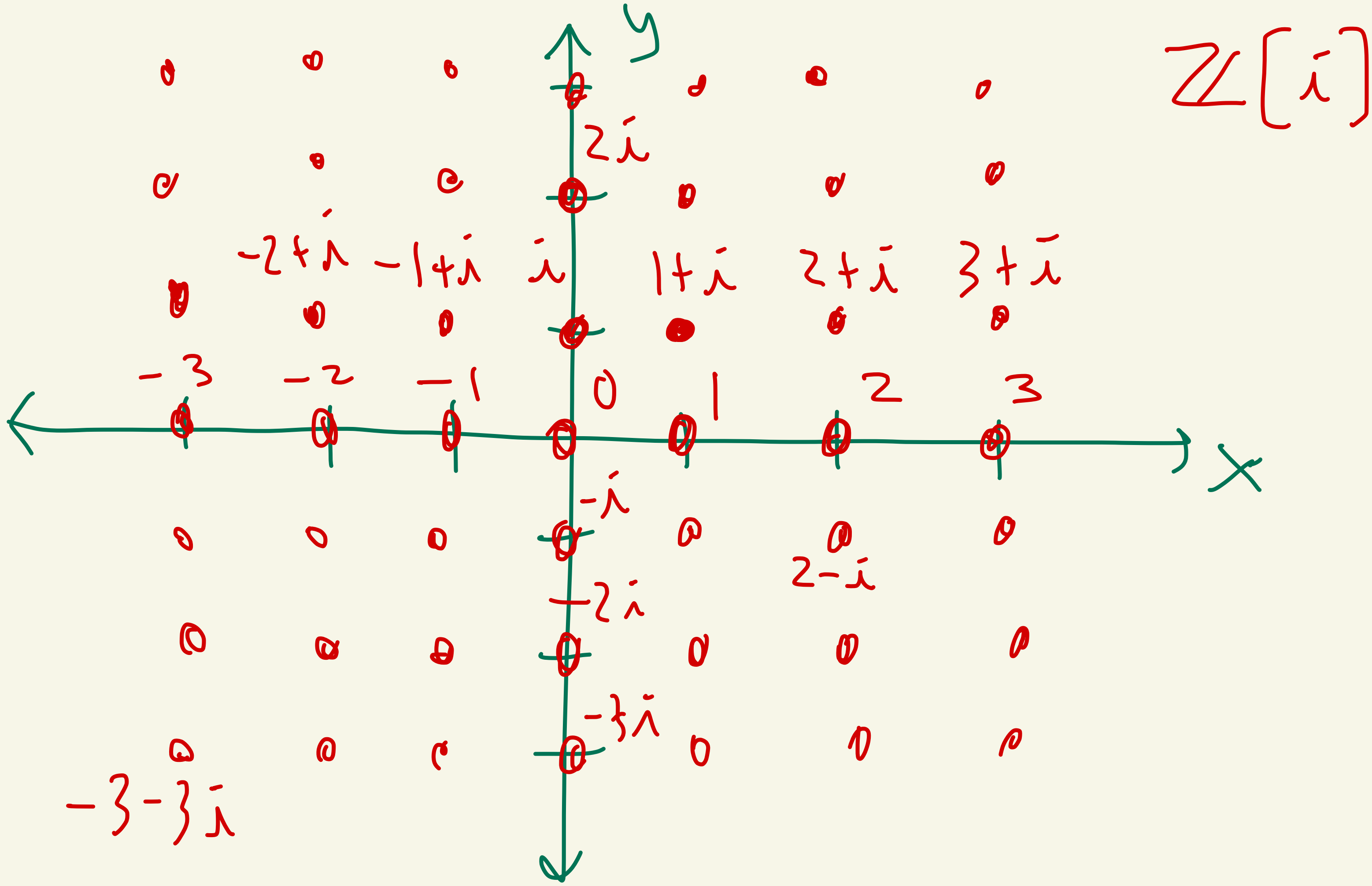
$$\mathbb{Z}[i] = \{ a + bi \mid a, b \in \mathbb{Z} \}$$

$$= \{ 0 + 3i, 1 + i, -10 + 0i, \ldots \}$$

is called the set of <u>Gaussian integers</u>.

(here $i = \sqrt{-1}$ or $i^2 = -1$)

To draw $x + iy$ just plot it at the point (x, y).



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

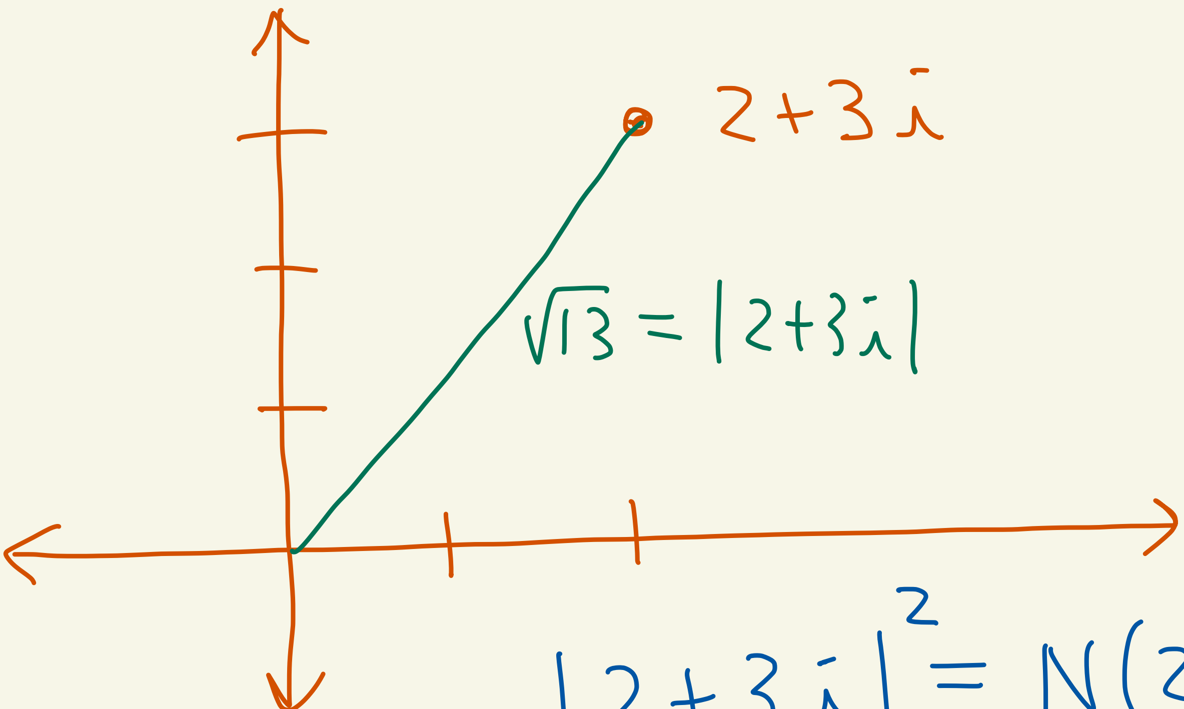
<u>Def:</u> Let $z = x + iy$ be a Gaussian integer. Define the <u>norm</u> of z to be

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

The <u>absolute value</u> of z is

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

<u>Ex:</u> $N(2+3i) = 2^2+3^2 = 13$



$$|2+3i|^2 = N(2+3i)$$

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

Then:

① $z+w \in \mathbb{Z}[i]$

$\mathbb{Z}[i]$ is <u>closed</u> under adding and

② $zw \in \mathbb{Z}[i]$ } multiplying

③ $N(z) \in \mathbb{Z}$ and $N(z) \geq 0$

④ $N(z) = 0$ iff $z = 0$

⑤ $N(zw) = N(z)N(w)$

<u>proof of ⑤:</u>

Let $z = a+bi$, $w = c+di$.

Then,

$$N(zw) = N\big((a+bi)(c+di)\big)$$

$$= N(ac + adi + bci + bdi^2)$$

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

$i^2 = -1$

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

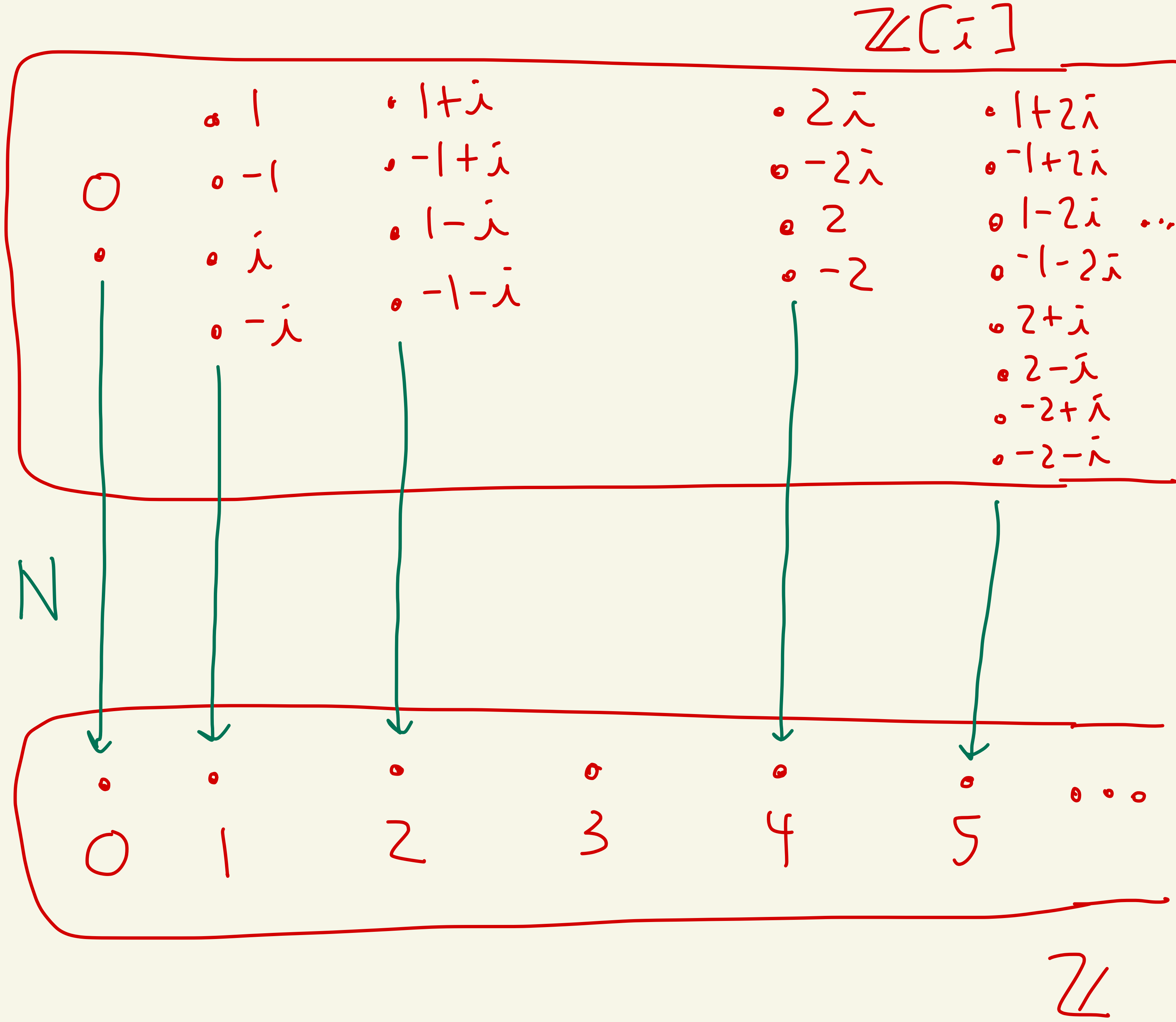
$\boxed{N(x+iy) = x^2+y^2}$

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

$$
\begin{aligned}
&= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \\
&= a^2(c^2+d^2) + b^2(c^2+d^2) \\
&= (a^2+b^2)(c^2+d^2) \\
&= N(a+bi)\,N(c+di) \\
&= N(z)\,N(w)
\end{aligned}
$$

$\blacksquare$

You can think of $N(z)$ as a way to turn a Gaussian integer into a non-negative integer.



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

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

Def: An element $u \in \mathbb{Z}[i]$ is called a **unit** iff
$$u^{-1} = \frac{1}{u} \in \mathbb{Z}[i]$$

Ex:

$\frac{1}{1} = 1 \in \mathbb{Z}[i]$. So, 1 is a unit.

$\frac{1}{-1} = -1 \in \mathbb{Z}[i]$. So, -1 is a unit.

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

So,
$$\left.\begin{aligned} \frac{1}{i} &= -i \in \mathbb{Z}[i]. \\ \frac{1}{-i} &= i \in \mathbb{Z}[i]. \end{aligned}\right\} \text{So } i \text{ and } -i \text{ are units}$$

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

---

proof:

($\Rightarrow$) Suppose z is a unit.

Let $w = \frac{1}{z}$.

Then $w \in \mathbb{Z}[i]$ since z is a unit.

So, $zw = 1$

Then, $N(zw) = N(1)$

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

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

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

So, $N(z)=1$

($\Leftarrow$) Suppose $N(z)=1$ where $z=x+iy$ and $x,y\in\mathbb{Z}$.

Then, $x^2+y^2=1$.

So, $\underbrace{(x+iy)}_{z}(x-iy)=1$.

Thus,

$$\frac{1}{z}=x-iy\in\mathbb{Z}[i]$$

So, z is a unit.

Now for the moreover part!

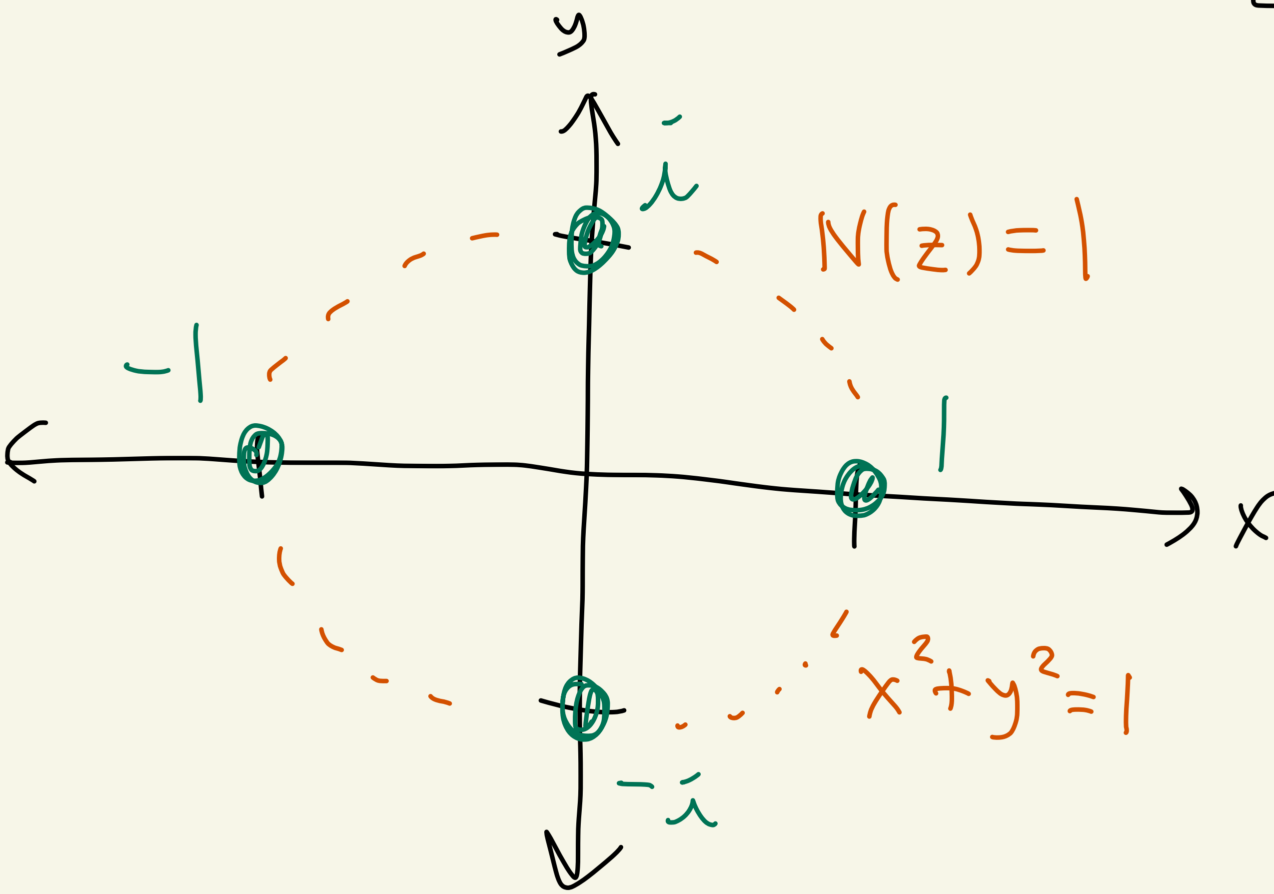
$z = x + iy$ is a unit

iff $x^2 + y^2 = 1 \longleftarrow \boxed{N(z) = 1}$

iff $(x, y) = (1, 0), (-1, 0), (0, 1), (0, -1)$

iff $z = 1, -1, i, -i$

$\blacksquare$



Def: Let $z, w \in \mathbb{Z}[i]$ with $z \neq 0$. We say that z **divides** w, and write $z \mid w$, if there exists $k \in \mathbb{Z}[i]$ where $w = zk$.

If this is the case then we call z a **divisor** of w.

Ex: $z = \underbrace{(1+i)(1-i)}$

$$1 - i + i - i^2$$

$$1 - i^2$$

$$1 - (-1)$$

$$2$$

$(1+i) \mid 2$ and $(1-i) \mid 2$

Ex: $3 = \underbrace{(3i)(-i)}_{-i^2 = 1}$

$3i \mid 3$ and $-i \mid 3$

Note: Every non-zero Gaussian integer has several divisors

Why? Let z be a Gaussian integer. Then,

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

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

Thus, z has these divisors always:

$$\underbrace{1, -1, i, -i}_{\text{units}}, \underbrace{z, -z, iz, -iz}_{\text{associates of } z}$$

[The <u>associates</u> of z are of the form uz where u is a unit]

<u>Def:</u> 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
2. the only divisors of z are

$$\underbrace{1, -1, i, -i}_{\text{units}}, \underbrace{z, -z, iz, -iz}_{\text{associates of } z}$$

Ex: See in notes that 3 is prime in $\mathbb{Z}[i]$.

Ex:

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

So, 2 and 5 are not prime in $\mathbb{Z}[i]$