GAUSSIAN INTEGERS

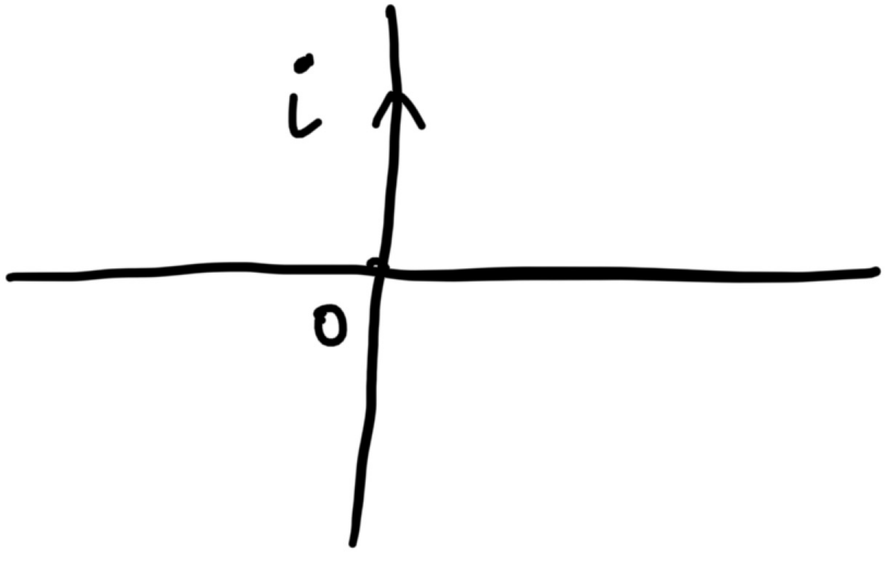
Named after

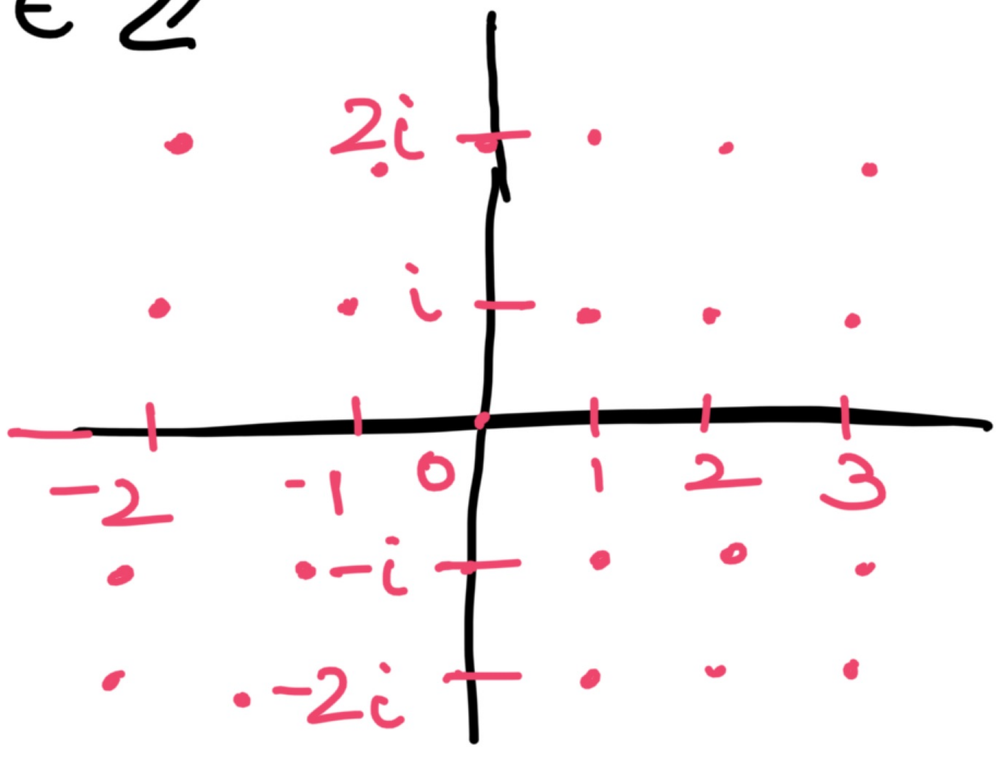
Carl Friedrich Gauss (1777 – 1855)

$= \mathbb{Z}[i]$

$a + bi$

$a, b \in \mathbb{Z}$





→ Addition

$$(a+bi) + (c+di)$$

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

→ Multiplication

$$(a+bi)(c+di) = (ac-bd) + (ad+bc)i$$

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

$= \frac{3+i}{2}$

$\text{Norm}(a+bi) = (a+bi)(a-bi) = a^2+b^2$

$\text{Norm}(\alpha\beta) = \text{Norm}(\alpha)\,\text{Norm}(\beta)$

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

Suppose $\alpha \mid \beta$ in $\mathbb{Z}[i]$ i.e.

$\beta = \alpha\gamma$ for some $\gamma \in \mathbb{Z}[i]$

> $\text{Norm}(\beta) \geq \text{Norm}(\alpha)$

More specifically $\text{Norm}(\alpha) \mid \text{Norm}(\beta)$.

Thm: For any $\alpha, \beta \in \mathbb{Z}[i]$ $\beta \neq 0$

there exists $q, r \in \mathbb{Z}[i]$ such that

$$\alpha = \beta q + r \quad \text{and} \quad 0 \leq \text{Norm}(r) < \text{Norm}(\beta)$$

Pf:

$\alpha = a + bi$ $\beta = c + di$

$\frac{\alpha}{\beta} = x + iy$

Choose $m, n \in \mathbb{Z}$

$|x - m| \leq 1/2$

$|y - n| \leq 1/2$

$$\frac{\alpha}{\beta} = x + iy \qquad |x - m| \leq 1/2 \qquad |y - m| \leq 1/2$$

$$q = m + ni$$

$$r = \alpha - \beta q = \beta\left((x-m) + (y-m)i\right)$$

$$\text{Norm}(r) \leq \frac{\text{Norm}(\beta)}{2} < \text{Norm}(\beta)$$

You can define GCD of two Gaussian integers similarly as before.

→ Find GCD $(10, 4+3i)$

① $\frac{10}{4+3i}\frac{(4-3i)}{(4-3i)} = \frac{40-30i}{25} = \frac{8-6i}{5}$

$10 = (4+3i)(2-i) + (-1-2i)$ $(m=2,\ n=-1)$

② $\frac{4+3i}{-1-2i}\frac{(-1+2i)}{(-1+2i)} = \frac{-4+8i-3i-6}{1-2i+2i+4} = \frac{-10+5i}{5}$

$= -2+i$

$$4+3i = (-1-2i)(-2+i)$$

$-1-2i$ is a GCD of $4+3i$ & 10.

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

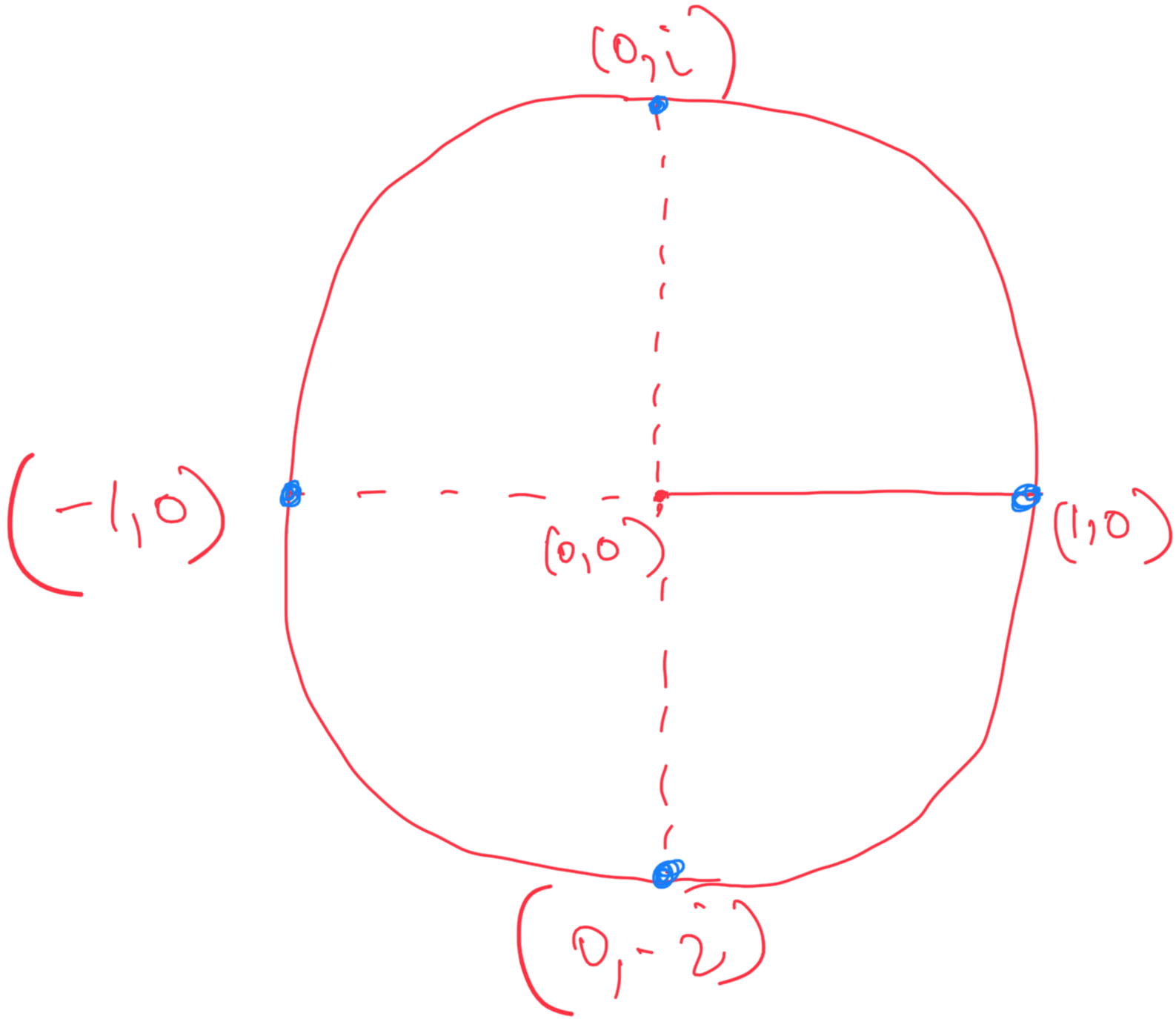
Units in $\mathbb{Z}[i]$ are those elements whose norm is 1.

Qn: What are all the units of $\mathbb{Z}[i]$?

$a^2+b^2=1$ So, $a^2=1$ & $b^2=0 \Rightarrow a=\pm 1, b=0$

or $a^2=0$ & $b^2=1 \Rightarrow a=0, b=\pm 1$

$\{1, -1, i, -i\}$ are the units



Units lie on this circle.

We will think of elements in $\mathbb{Z}[i]$ as a Set.

Primes in $\mathbb{Z}$

A number p is called a <u>prime number</u> if and only if

i) $p \neq \pm 1$

ii) If $p = xy$ for some integers x, y then x or y is ± 1.

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

A Gaussian integer p is called a Gaussian prime if and only if:

i) p is not a unit

ii) If $p = xy$ for some $x, y \in \mathbb{Z}[i]$ then x or y is a unit.

Qn: Show that if $p \mid \alpha\beta$, then $p \mid \alpha$ or $p \mid \beta$. (Solution on next page)

Thm: Every Gaussian integer can be uniquely factorized into product of primes.

(Unique here means upto units and reordering.) (Proof is same as integers.)

Soln: Suppose $p \nmid a$, then there exists q_1 & q_2 such that

$$a q_1 + p q_2 = 1$$

$$\beta a q_1 + p \beta q_2 = \beta$$

Since $p \mid a\beta$ & $p \mid p\beta \Rightarrow p \mid \beta$.

Factorize 10 in $\mathbb{Z}[i]$.

$10 = 2 \cdot 5$

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

this is prime because $N(1+i) = 2$

this is prime b/c $N(2+i) = 5$

$\mathbb{Z}$	$\mathbb{Z}[i]$
Absolute value $\lvert\ \rvert$	Norm $(a+bi) = a^2+b^2$
Division property	Division property
Primes, GCD	Primes, GCD
Unique factorization	Unique factorization

Eisenstein Integers

(named after Gotthold Eisenstein 1823 – 1852)

$$\mathbb{Z}[\omega] = \{ a + b\omega \mid a, b \in \mathbb{Z}, \ \omega = e^{2\pi i/3} \}$$

$$\omega = \frac{-1}{2} + \frac{\sqrt{3}\,i}{2}$$

Addition $(a+b\omega) + (c+d\omega) = (a+c) + (b+d)\omega$

Multiplication

$$(a+b\omega)(c+d\omega) = ac + ad\omega + bc\omega + bd\omega^2$$

$$= ac + ad\omega + bc\omega + bd(\omega - 1)$$

$$= (ac - bd) + (ad + bc - bd)\omega$$

$$\text{Norm}(a+b\omega) = (a+b\omega)(a+b\omega^2)$$

$$= a^2 + b^2 + ab\omega^2 + ab\omega$$

$$= a^2 + b^2 - ab$$

What are the units in $\mathbb{Z}[\omega]$?

$$a^2+b^2-ab=1 \qquad a,b\in\mathbb{Z}$$

$$\left(a-\frac{b}{2}\right)^2+\frac{3}{4}b^2=1$$

If $|b|\geq 2$, then we cannot get one

So, $|b|\leq 1$

$b=-1, 1$ or 0

$b=0 \longrightarrow a=\pm 1$

$b=1 \longrightarrow a^2+1-a=1 \Rightarrow a^2=a$

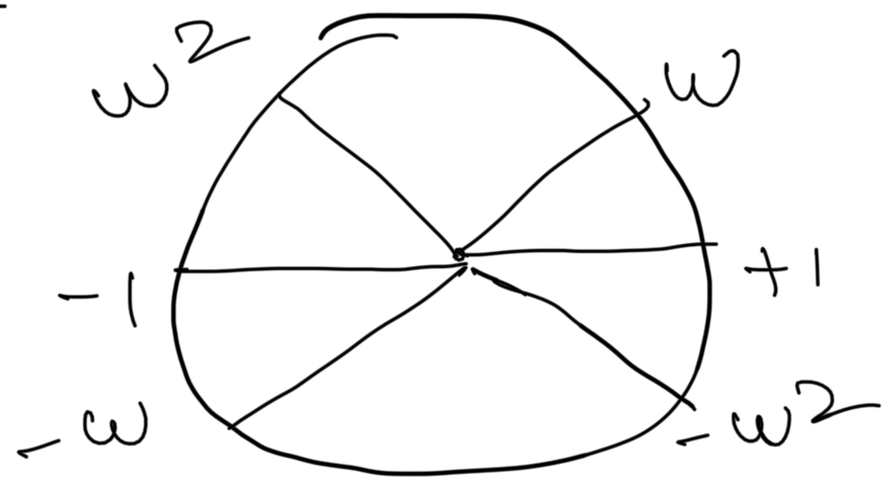
$\Downarrow$

$a=0$ or 1

$b=-1 \longrightarrow a^2+1+a=1 \Rightarrow a^2=-a$

$\Rightarrow a=0$ or -1

Units $\{\pm 1, \omega, 1+\omega, -\omega, -1-\omega\}$



Division algorithm

(Same as $\mathbb{Z}[i]$)

$\alpha, \beta \in \mathbb{Z}[\omega]$

$\frac{\alpha}{\beta} = x + yi \qquad x, y \in \mathbb{Q}$

Choose $m, n \in \mathbb{Z}$ s.t $|x - m| \leq 1/2$

$|y - n| \leq 1/2$

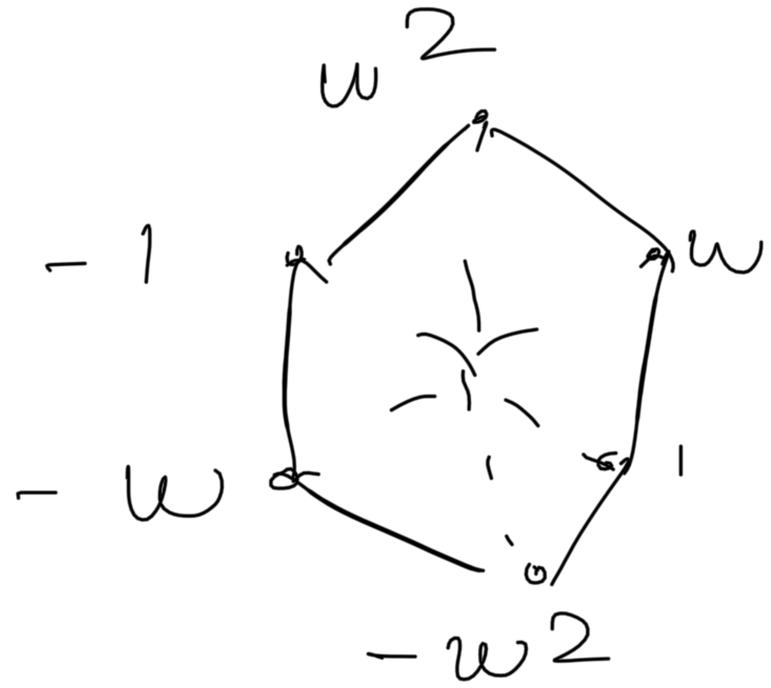
$q = m + ni \in \mathbb{Z}[\omega]$

$[r = \alpha - \beta q]$ (Show that $N(r) < N(\beta)$)

Division algorithm

⇓

GCD



How should we define primes in $\mathbb{Z}[w]$? (Same as $\mathbb{Z}[i]$)

Factorize 13 in $\mathbb{Z}[\omega]$

$13 = (4+3\omega)(4+3\omega^2)$

this is because $(4+3\omega)$ is prime

$N(4+3\omega) = 13$ is a prime

$\mathbb{Z}$	$\mathbb{Z}[i]$	$\mathbb{Z}[\omega]$
Absolute value	Norm $(a+bi) = a^2+b^2$	Norm $(a+b\omega) = a^2+b^2-ab$
Division algorithm	Division algorithm	Division algorithm
Unique Factorization	Unique Factorization	Unique Factorization