Gaussian and Eisenstein integers

integers $\mathbb{Z} \subset \mathbb{Q}$ rationals

$\overline{\mathbb{Z}} \subset \overline{\mathbb{Q}}$

$\overline{\mathbb{Z}}$ — alg. integers — roots of monic polys over $\mathbb{Z}$

$\overline{\mathbb{Q}}$ — alg. numbers — roots of monic polys over $\mathbb{Q}$

Gaussian integers / rationals

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

$$\mathbb{Q}(i) = \{a+bi \in \mathbb{C} \mid a, b \in \mathbb{Q}\}$$

ring

field

$$\frac{1}{a+bi} = \frac{a-bi}{a^2+b^2}$$

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

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

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

$\Rightarrow$ The set of rational integers which are sums of two squares is closed under multiplication

Prop $\mathbb{Z}[i]$ is a Euclidean domain,

like $\mathbb{Z}$ and $K[x]$ for K a field.

i.e. for $a, b \in \mathbb{Z}[i]$ with $b \neq 0$

we can write

$$a = qb + r \quad \text{where } |r| < |b|,$$

r in $\mathbb{Z}[i]$ should have abs. value < 1

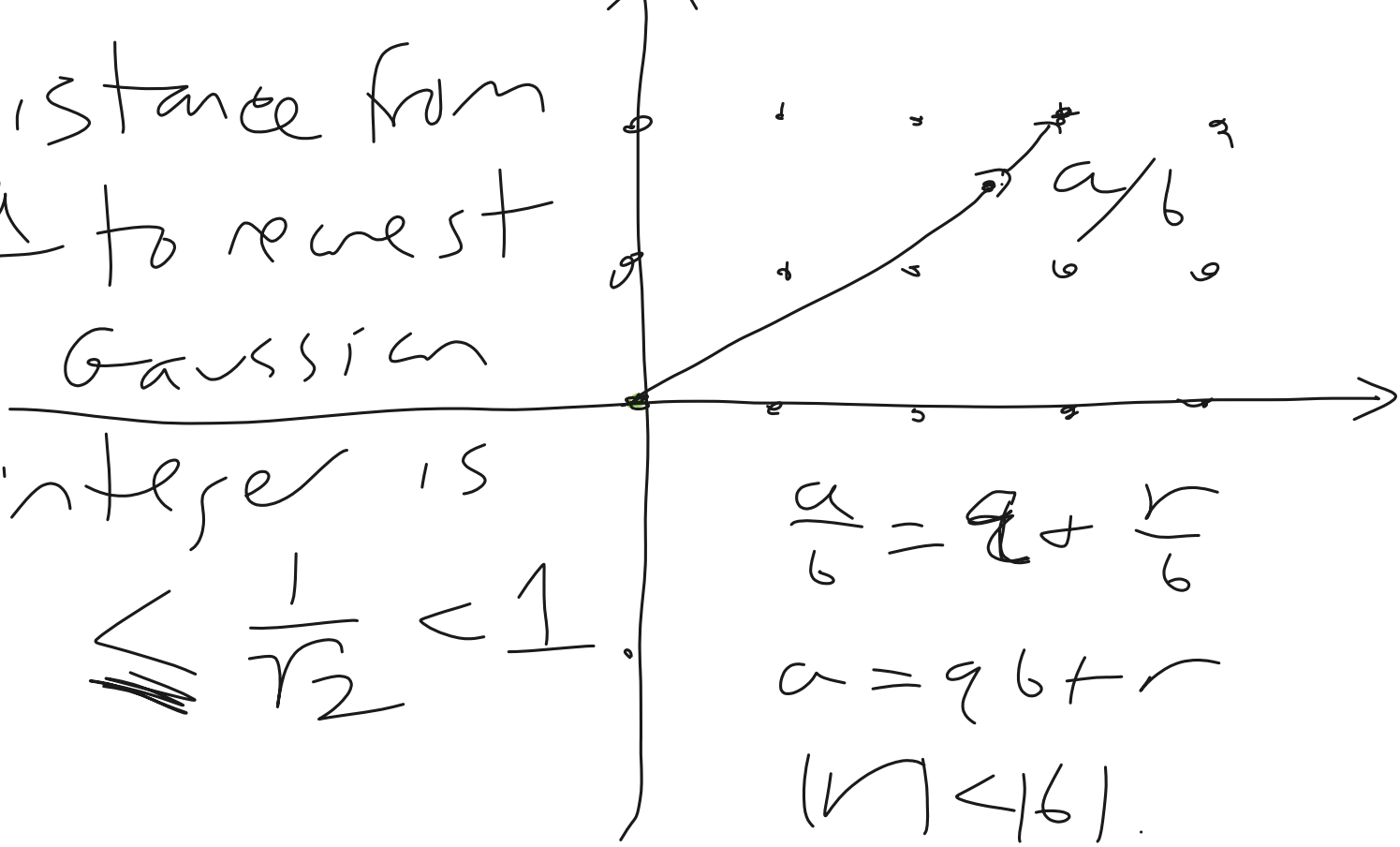
Complex abs. value

Pf Take $\frac{a}{b}$, round to nearest Gaussian integer

$\frac{a}{b}$ in $\mathbb{Q}(i)$ $\rightarrow$ $\frac{a}{b} = q + \frac{r}{b}$

Distance from $\frac{a}{b}$ to nearest Gaussian integer is

$$\leq \frac{1}{\sqrt{2}} < 1.$$



$$\frac{a}{b} = q + \frac{r}{b}$$

$$a = qb + r$$

$$|r| < |b|.$$

The key point: for any C, there are finitely many possible absolute values of Gaussian integers less than C.

$\rightsquigarrow$ Euclidean algorithm:

to compute $\gcd(a, b)$,

do repeated Euclidean division

$r_0 = a$

$r_1 = b$

$r_2 =$ remainder of r_0 divided by r_1

$r_3 =$ remainder of r_1 divided by r_2

$\vdots$

$r_{k-1} = \cdots$

$r_k = 0$

$$\gcd(a, b) = \gcd(r_0, r_1)$$
$$= \gcd(r_1, r_2)$$
$$\vdots$$
$$= \gcd(r_{k-1}, r_k)$$
$$= r_{k-1}.$$

Similarly,

- Any ideal in $\mathbb{Z}[i]$ is principal.

- For any $a, b \in \mathbb{Z}[i]$, $\exists$ $x, y \in \mathbb{Z}[i]$ s.t.

$$ax + by = d$$

d = a gcd of a, b (i.e. a generator of ideal (a, b))

Since $\mathbb{Z}[i]$ is Euclidean, I can prove unique factorization into primes.

$\alpha \in \mathbb{Z}[i]$ is <u>prime</u> if

- α is not a unit $\{1, -1, i, -i\}$
- if α divides $\beta\gamma$, then α divides at least one of β or γ

Theorem

For every $\beta \in \mathbb{Z}[i]$ nonzero, there exists a factorization

$$\beta = u\,\alpha_1^{e_1} \cdots \alpha_n^{e_n}$$

$e_1, \dots, e_n \leftarrow$ positive integers.

u: unit; $\alpha_1, \dots, \alpha_n$: primes

which is unique up to permutation & shifting unit factors.

What are the primes in $\mathbb{Z}[i]$?

Claim: they are, up to units,

- $1+i$ $\quad (1+i)^2 = 2u$
- $a+bi$ $\quad |a+bi|^2 = p \equiv 1 \bmod 4$
- p $\quad p \equiv 3 \bmod 4$ rational primes $\quad |p|^2 = p^2$

Corollary: (Fermat)

rational

every prime $p \equiv 1 \bmod 4$

is sum of two squares!

Conversely, if $p = a^2 + b^2$ in $\mathbb{Z}$

with p prime, then $p = 2$ or

$p \equiv 1 \pmod 4$.

Key step of proof: e.g. $5 = (2+i)(2-i)$

Show that if p prime $p \equiv 1 \bmod 4$ then p factors non-trivially in $\mathbb{Z}[i]$

Lemma: $\exists\, x, y$ s.t. x, y not divis. by p and $x^2 + y^2 \equiv 0 \bmod p$.

e.g. $x = 1$ $y = \left(\frac{p-1}{2}\right)!$ (use Wilson's theorem)

Look at ideal $(p, x+yi)$

and pick a generator $a+bi$

now $a+bi$ divides p, so

a^2+b^2 divides p^2.

but can't have $a^2+b^2 = p^2$

in that case $\frac{p}{a+bi}$ would be a unit. ~~$\neq$~~

so $a^2+b^2 = p$.

Tensor: there exist other number fields that have a similar Euclidean property,

e.g. $\mathbb{Z}[\zeta_3] \subset \mathbb{Q}(\zeta_3)$

Eisenstein integers