Chapter 12 Factorization

Studying solutions to Diophantine equations like $x^2+y^2=103$ (no solutions), $x^2+y^2=125$ ($(x,y)=(\pm 5,\pm 10)$, $(x,y)=(\pm 2,\pm 11)$), $x^2+5y^2=99$ with $x,y\in\mathbb{Z}$

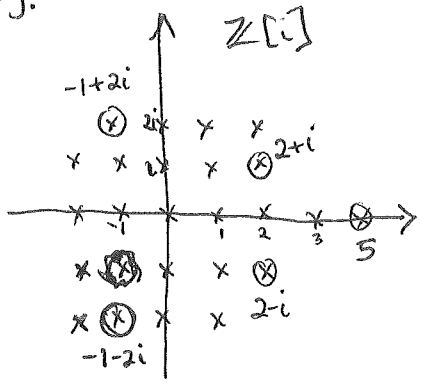
people (Fermat, Gauss, ...) realized it would be useful to

factor $(x+iy)(x-iy)=103$ or $(x+iy)(x-iy)=125$ } in $\mathbb{Z}[i]\subset\mathbb{C}$

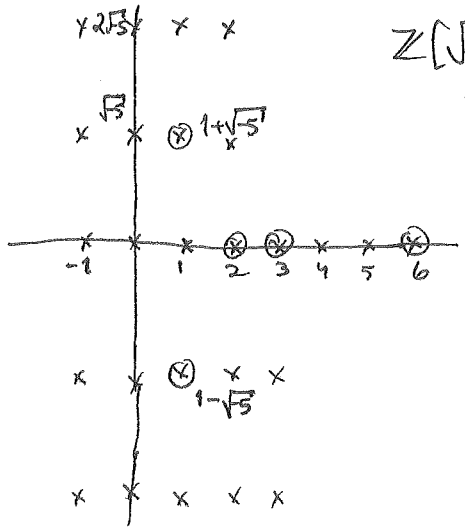
$(x+\sqrt{-5}y)(x-\sqrt{-5}y)=99$ in $\mathbb{Z}[\sqrt{-5}]\subset\mathbb{C}$

but factorizations in $\mathbb{Z}[i]$ have better uniqueness properties than in $\mathbb{Z}[\sqrt{-5}]$!

e.g.



versus



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

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

$=i(2+i)\cdot(-i)(2-i)$

units in $\mathbb{Z}^\times=\{\pm 1,\pm i\}$

Similar to in $\mathbb{Z}$,

$12=2\cdot 2\cdot 3$

$=(-2)(2)(-3)$

$=(-2)(-2)\cdot 3$

$=\cdots$

$6=2\cdot 3$

$=(1+\sqrt{-5})(1-\sqrt{-5})$

but none of $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ differ by units, as

$\mathbb{Z}[\sqrt{-5}]^\times=\{\pm 1\}$

What makes $\mathbb{Z}[i]$ behave better, more like $\mathbb{Z}$ and $\mathbb{F}[x]$?

It has an analogous division algorithm ...

DEFN: A domain R is called a Euclidean domain if it has a size function $\sigma: R \to \{0,1,2,\ldots\}$ with the following property:

given $a, b \in R$ with $a \neq 0$,

$\exists$ an expression $b = a \cdot q + r$ where $q, r \in R$ and either $r = 0$ or $\sigma(r) < \sigma(a)$.

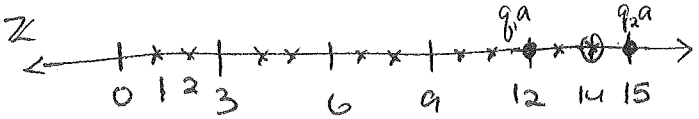
EXAMPLES:

① $R = \mathbb{Z}$ with $\sigma(r) = |r|$

Note the remainder as specified above is not unique,

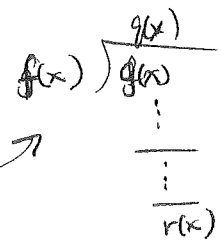
e.g. $b = 14$, $a = 3$ have $\underbrace{b}_{} = \underbrace{a \cdot q_1}_{} + \underbrace{r_1}_{}$, $14 = 3 \cdot 4 + 2$ with $|2| < |3|$

and $14 = 3 \cdot 5 + (-1)$ with $|(-1)| < |3|$, $b = a \cdot q_2 + r_2$



② $R = \mathbb{F}[x]$ with $\sigma(f(x)) = \deg(f)$

via usual division algorithm →



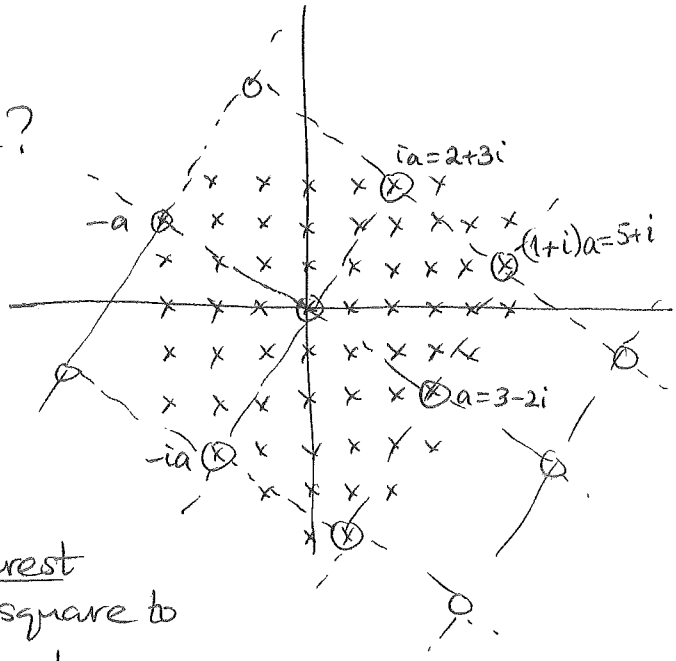
③ $R = \mathbb{Z}[i]$ = Gaussian integers and $\sigma(x+iy) = \|z\|^2 = x^2 + y^2$

Given $b, a \in \mathbb{Z}[i]$ with $a \neq 0$, how to find q, r with $b = a \cdot q + r$, and $\|r\|^2 < \|a\|^2$?

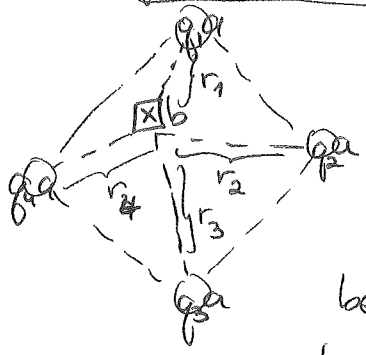
e.g. $b = 1000 - 713i$

$a = 3 - 2i$

What do $q \cdot a \in \mathbb{Z}[i]$ look like?



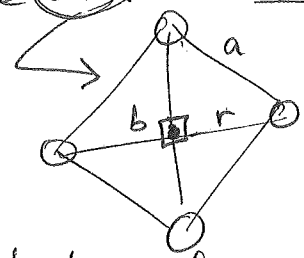
So wherever b is, it lies in one of these squares of sidelength $\|a\|$:



Pick the nearest corner of the square to be qa, and then $b = qa + r$

has $\|r\|$ = distance to nearest corner from b

$\leq \dfrac{\|a\|}{\sqrt{2}}$ because this is the worst case:



$\|a\| = \sqrt{2}\,\|r\|$

so $\|r\|^2 \leq \dfrac{\|a\|^2}{2} < \|a\|^2$

$\sigma(r)$ $\qquad$ $\sigma(a)$

REMARKS: ① Note how there is no canonical choice for q, r here, but we won't need that

② This geometry can still work for $\mathbb{Z}[\sqrt{2}] = \mathbb{Z}[\sqrt{2}i]$ (on HOMEWORK 2)

but fails for $\mathbb{Z}[\sqrt{5}]$.

PROPOSITION (12.2.7): Every Euclidean domain R is a principal ideal domain (P.I.D.)

(i.e. all ideals $I \overset{CR}{} $ are principal $I = (r)$.

Proof: Given an ideal $I \subset R$, if $I = \{0\} = (0)$ we're done.

Else pick any $a \neq 0$ in I with smallest $\sigma(a)$ (Why does such an a exist?)

Certainly $(a) \subseteq I$, but we claim $(a) = I$ since any $b \in I$ has $b = q \cdot a + r$ with $\sigma(r) < \sigma(a)$ or $r = 0$, and since $r = b - q \cdot a \Rightarrow r \in I$ we know $\sigma(r) < \sigma(a)$ can't happen. ∎