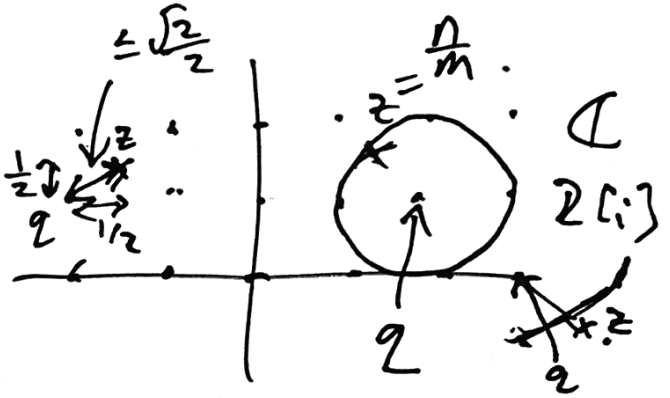
Recall: Euclidean algorithm in $\mathbb{Z}[i]$.

Lemma: $\forall n, m \neq 0 \ \exists q, r$:
$n = q \cdot m + r$ & $0 \leq N(r) < N(m)$

where $N(x+iy) = x^2 + y^2 := |x+iy|^2$.



Pf: Consider $\frac{n}{m} = z = \frac{n \cdot \bar{m}}{|m|^2}$, with $N(m) \to |m|^2$

$\exists$ "nearby" / a closest $q \in \mathbb{Z}[i]$ s.t. $\left|q - \frac{n}{m}\right| \leq \frac{\sqrt{2}}{2} = \frac{1}{\sqrt{2}} < 1$.

$$\Rightarrow \underbrace{|mq - n|}_{=r} \leq \frac{1}{\sqrt{2}}|m| \Rightarrow N(r) = |r|^2 \leq \frac{1}{2}|m|^2 = \frac{1}{2}N(m) < N(m).$$

Recall: $\mathbb{Z}$ is a PID. ie any ideal $(n_1, n_2, \ldots) = (d)$.
& $d = \gcd(n_1, n_2, \ldots)$.

Prop: If $a \mid b \cdot c$ & $\gcd(a,b)=1 \Rightarrow a \mid c$.

pf: Look at ideal $(a,b) = \{ax+by \mid x,y \in \mathbb{Z}\} = \mathbb{Z}$.

i.e. Euclidean alg gives solution to $ax+by=1$. Mult by c:

$acx + bcy = c \Rightarrow a \mid c$. ✓

$a \mid acx$, $a \mid bcy$

Corollary: If p = prime & $p \mid b \cdot c \Rightarrow p \mid b$ or $p \mid c$.

pf: Assume p = prime & $p \mid b \cdot c$ & $p \nmid b$. $\Rightarrow \gcd(p,b) = \begin{cases} p \\ 1 \end{cases}$

Use Prop with $a=p$. $\Rightarrow p \mid c$.

Cor: If p = prime & $a,b \in \mathbb{Z}$, $\Rightarrow \text{ord}_p(a \cdot b) = \text{ord}_p(a) + \text{ord}_p(b)$.

Def: $\text{ord}_p(a)$ = "order of p in a" $= \max\{k \mid p^k \mid a\}$.

pf(Cor): Let $\text{ord}_p(a) = \alpha$, i.e. $p^\alpha \| a$.

i.e. $a = p^\alpha \cdot a_1$, $\gcd(a_1, p) = 1$. $p \nmid a_1$ ✓

$p^k \| a$ ← "exactly divides"

Ex: $\text{ord}_3(18) = 2$. (since $3^2 \| 18$)

$\text{ord}_5(18) = 0$.

Similarly, let $\beta = ord_p(b)$, so $b = p^\beta \cdot b_1$, and ~~$\gcd(b_1, p) = 1$~~ $p \nmid b_1$.

So: look at $a \cdot b = p^\alpha \cdot a_1 \cdot p^\beta \cdot b_1 = p^{\alpha+\beta} \cdot a_1 b_1$.

Aside: $ord_6(18) = 1$. $ord_6(12) = 1$. $ord_6(18 \cdot 12) = ord_6(216) = 3$. $\neq 1+1$.

$18 = 6^1 \cdot 3$ $\quad 6 \nmid 3$. If p was not prime, then ord_p would not necessarily be additive.

If $ord_p(a \cdot b) > \alpha+\beta \Rightarrow p \mid a_1 \cdot b_1 \Rightarrow p \mid a_1$ or $p \mid b_1$ ↯.

$\Rightarrow \leq ord_p(a \cdot b) \leq \alpha+\beta \Rightarrow ord_p(a \cdot b) = ord_p(a) + ord_p(b)$.

Fundamental Thm of Arithmetic: If $n \neq 0$, $n \in \mathbb{Z}$, then $\exists\, \varepsilon(n) = \begin{cases} 0 \\ 1 \end{cases}$.

$n = (-1)^{\varepsilon(n)} \cdot \prod_p p^{ord_p(n)}$ & this decomposition is unique.

i.e. If $n = (-1)^{\varepsilon(n)} \cdot \prod_p p^{e_p} \Rightarrow e_p = ord_p(n)$.

Pf: Assume n has "second" factorization,

$n = (-1)^{\varepsilon(n)} \prod_p p^{e_p}$. Fix p. Apply ord_p to both sides.

$$\text{ord}_p(n) = \text{ord}_p\left((-1)^{\varepsilon(n)} \prod_q q^{e_q}\right) \overset{((or)}{=} \text{ord}_p\left((-1)^{\varepsilon(n)}\right) + \sum_q \text{ord}_p(q^{e_q}).$$

$2^{e_2} \cdot 3^{e_3} \cdot 5^{e_5} \cdot 7^{e_7} \cdots$ So what is $\text{ord}_p\left((-1)^{\varepsilon(n)}\right) = 0$. $\text{ord}_p(2^{e_2}) + \text{ord}_p(3^{e_3}) + \cdots$

For $q \neq p$, $\text{ord}_p(q^{e_q}) = 0$, $\text{ord}_p(p^{e_p}) = e_p$.