Recall that a Euclidean domain is a domain with Euclidean algorithm. That is, a norm function $N$ on domain $\mathcal{O} \setminus \{0\} \to \mathbb{N}_0$

s.t.

(i) $N(b) \leq N(ab) \forall a,b \in \mathcal{O} \setminus \{0\}$

(ii) $a = qb + r$ for some $q,r \in \mathcal{O}$, with $N(r) < N(b)$ or $r = 0$.

Using $N(a) := a \overline{a}$ on $\mathbb{Z}[i]$, then (i) is clear from multiplicative
and fact that $N(w) = 0 \Rightarrow w = 0$.

(ii) follows b/c $\mathbb{Z}[i]$ is square lattice in $\mathbb{C}$.

We must show $\exists q \in \mathbb{Z}[i]$ s.t.

$$\left| \frac{a}{b} - q \right| < 1$$

since $N(a) = |a|^2$.

But $\frac{a}{b} \in \mathbb{C}$ is always at most $\frac{\sqrt{2}}{2}$ from lattice point (i.e. $< 1$)

Finally recall that Euclidean domains are UFDs. (converse is false)

This is immediate from the existence of norm function.

Given ideal $\mathfrak{a}$, pick elt. $a \in \mathfrak{a}$ of minimal norm. This must be generator. Else $\exists b$ with $b = q \cdot a + r$ with $0 < N(r) < N(a)$ contradicting the minimality of $a$, so $\mathfrak{a}$ is a P.I.D.

But P.I.D.s are U.F.D.s:

show that P.I.D.s satisfy (A) divisor chain condition (no infinite sequence of proper divisibility of elts)

$\Rightarrow$ factorization exists

(B) every irreducible (no proper factors) is prime ($p | ab \Rightarrow p | a$ or $p | b$)

$\Rightarrow$ factorization unique

(A) follows b/c given $(a_1) \subseteq (a_2) \subseteq \ldots$ then $U(a_i)$ is ideal $(d) \Rightarrow d | (a_i)$ for some $d$

so $(am) \subseteq (an) \subseteq \ldots \subseteq (am)$ $\Rightarrow$ $m \geq n$. chain stabilizes!
If \( p \) is irreducible and \( p \mid ab \) but \( p \nmid a \), show \( p \mid b \).

\( p \) irreducible means \( \# \) ideal \( I \) s.t. \( \theta I = \mathbb{Z}[\frac{1}{p}] \).

Now \( p \nmid a \) means \( a \not\in (p) \) so \( (p,a) \not= (p) \Rightarrow (p,a) = (1) \).

Then we can find \( u,v \in \mathbb{Z} \) s.t. \( up + va = 1 \).

\[ \Rightarrow \] \( upb + vab = b \) but since \( p \mid ab \), \( p \) must divide \( b \). \( \square \)

---

So putting it all together, \( p \equiv 1 \pmod{4} \) \( \iff \) \( p = a^2 + b^2 \) for some \( a, b \in \mathbb{Z} \)

or \( p = 2 \)

and key step was understanding that \( p \equiv 1 \pmod{4} \) \( \Rightarrow \) then \( p \) not prime in \( \mathbb{Z}[i] \).

---

Let's collect what we've learned about \( \mathbb{Z}[i] \) so far:

- \( \alpha \in \mathbb{Z}[i] \) is unit \( \iff \) \( N(\alpha) = 1 \) i.e. \( \alpha = a + bi \) with one of \( a \) or \( b \) \( \iff \) \( a^2 + b^2 = 1 \) other \( = 0 \).

Quickly check that units are \( \xi, \bar{\xi}, -1, i, -i \).

- What are primes? Note: report everything up to units.

Won't always require such a specific characterization...
Theorem: The primes \( \pi \) of \( \mathbb{Z}[i] \) are:

1. \( \pi = 1+i \)
2. \( \pi = a+bi \) with \( a^2+b^2 \) squarefree, \( \rho \equiv (4), \quad \frac{a}{\pi} > |b| \geq 0 \).
3. \( \pi = p \), rational prime \( \equiv 3 \pmod{4} \).

- First show all these are indeed primes of \( \mathbb{Z}[i] \). Later show this exhausts all primes.

Recall that for any elt. \( \pi \in \mathbb{Z}[i] \), if \( \pi = \alpha \cdot \beta \), then \( N(\pi) = N(\alpha) \cdot N(\beta) \).

In cases (1) + (2), \( N(\pi) = p \) so \( \alpha \) or \( \beta \) must be unit, i.e. \( \pi \) prime.

In case (3) \( p^2 = N(\alpha) \cdot N(\beta) \) so \( p = N(\alpha) = N(\beta) = a^2+b^2 \) if \( d = a+bi \).

Now show all primes \( \pi \in \mathbb{Z}[i] \) are in the above list:

\[ N(\pi) = \pi \cdot \bar{\pi} \text{ from unique fact. in } \mathbb{Z} \]

\( \pi, \bar{\pi} \) prime, not nec. distinct.

\( \pi \cdot \bar{\pi} \) so \( \pi \) divides some \( \pi_i \), call it \( \rho \) so \( N(\pi) = p^2 \).

i.e. \( N(\rho) = p \) or \( p^2 \). Just use earlier analysis.

- If \( N(\pi) = p \) and \( \pi = a+bi \) then \( p = a^2+b^2 \), so in case 1 or 2.
- If \( N(\pi) = p^2 \) then \( \rho \) is Gaussian integer with norm 1 and \( \rho \equiv (4) \pmod{4} \) in this case since if \( p=2 \) or \( p \equiv 1 \pmod{4} \).

then \( p = a^2+b^2 \) for some \( a, b \in \mathbb{Z} \) by Fermat's theorem.

\( = (a+bi)(a-bi) \Rightarrow p \text{ not prime } \).
The theorem makes clear how primes \( p \in \mathbb{Z} \) decompose in \( \mathbb{Z}[i] \).

- If \( p \equiv 1 (4) \) then \( p = (a+bi)(a-bi) \), "p splits" into two conjugate prime factors.

- If \( p \equiv 3 (4) \) then \( p \) remains prime ("inert") factors.

- If \( p = 2 \), then \( p = (1+i)(1-i) = -i(1+i)^2 \) so equal to the square of a prime (up to unit) \( p \) "ramifies" (infinitely many primes split, inert, finitely many primes ramify).

How to begin studying the problem in general?

Define analogue of Gaussian integers (subring of \( \mathbb{Q}(i) \)) for any number field. Naive guess: pick basis of \( \mathbb{Q}(i)/\mathbb{Q} \) and consider instead \( \mathbb{Z} \)-linear combinations.

**Better (basis-free) definition:**

View \( \mathbb{Z}[i] \) as \( \{ \alpha \in \mathbb{Q}(i) \mid \alpha \text{ is root of monic poly.} \} \) with coeffs. in \( \mathbb{Z} \).

[In this example, it is of form \( (x^2 + ax + b = 0) \) \( a, b \in \mathbb{Z} \).]

Check: \( \alpha = c + di \), \( c, d \in \mathbb{Z} \)

then \( \alpha \) is root of \( x^2 + ax + b \) with \( a = -2c \), \( b = c^2 + d^2 \)

if \( c, d \in \mathbb{Z} \) then \( a, b \in \mathbb{Z} \).

if \( a, b \in \mathbb{Z} \) then a priori, just \( 2c, 2d \in \mathbb{Z} \). But \( (2c)^2 + (2d)^2 = 4b \equiv 0 (4) \).
since squares are always $0,1$ (4), must have $(2c)^2 \equiv (2d)^2 \equiv 0$ (4)

$\Rightarrow c, d \in \mathbb{Z}$. //

Make this some definition over arbitrary field. Then differs in general from $\mathbb{Z}$-basis, of course, but gives satisfactory theory.

Note: not even immediately clear that these elts form subring.

Check this next -- using a bit of linear algebra. (i.e. need alternate characterization of integrality, rather than producing poly. for which $a, b$ is root)

In what follows, work in arbitrary ring (comm. with unit)

Row-Column Expansion: (Prop. 2.3 in Neukirch)

\[ A = (a_{ij}) \text{ be } r \times r \text{ matrix with entries } a_{ij} \text{ in arb. ring.} \]

\[ A^* = (a^*_{ij}) \text{ "adjoint matrix" with } a^*_{ij} = (-1)^{i+j} \det(A^{(ij)}) \]

\[ \text{Then } AA^* = A^*A = \det(A) \cdot I_r \]

\[ (\text{Cor: } A \cdot x = 0 \Rightarrow \det(A) \cdot x = 0) \]

for any vector \( x = (x_1, \ldots, x_r) \)

Now we can prove: if \( A \subseteq B \) is an extension of rings

then \( \mathcal{A} b_1, \ldots, b_n \) integral over \( A \) (satisfy monic poly. with coeef in \( A \))

\[ \langle \text{d} \rangle \quad A [b_1, \ldots, b_n] \text{ is a finitely generated } A \text{-module.} \quad (\text{Prop. 2.2 in Neukirch}) \]

Cor: if \( b_1, \ldots, b_n \in B \) are integral over \( A \), so is any elt in \aabbn

\[ A [b_1, \ldots, b_n] \]

If of cor: if \( b \in A [b_1, \ldots, b_n] \), then \( A [b_1, \ldots, b_n] = A [b, b_1, \ldots, b_n] \)

is a fin. gen. \( A \)-module. /
Proof of Proposition 2.2: Let $b \in B$ be integral over $A$ and $f$ a monic polynomial with $f(b) = 0$. Show $A[b]$ is finitely generated.

If $\deg(f) = n$, then any $g \in A[x]$ written as

$$g(x) = g(x) \cdot f(x) + r(x)$$

with $\deg(r) < n$.

Then $g(b) = r(b) = a_0 + a_1 b + \ldots + a_{n-1} b^{n-1}$ (poly of $\deg < n$ coefts in $A$)

i.e. any polynomial in $b$ expressible in terms of $b, b^2, \ldots, b^{n-1}$.

In the case $(b_1, \ldots, b_n \text{ integral over } A \Rightarrow A[b_1, \ldots, b_n]$ f-gen.)

now follows by induction.

For converse, let $\omega_1, \ldots, \omega_r$ be generators for $A[b_1, \ldots, b_n]/A$

Then for any $b \in A[b_1, \ldots, b_n]$,

$$b \omega_i = \sum_{j=1}^{n} a_{ij} \omega_j \quad a_{ij} \in A \quad (*)$$

Using row-column expansion prop: Let $M = \text{matrix } b \cdot I_n - (a_{ij})$

Then $M \cdot (\omega_1 \ldots \omega_n) = 0$ by construction.

$$\det (b \cdot I_n - (a_{ij})) \cdot \omega_i = 0 \quad \forall i.$$ 

Since $\omega_i$'s generators, then

$$1 = c_1 \omega_1 + \ldots + c_r \omega_r$$

$$\Rightarrow \det (b \cdot I_n - (a_{ij})) = 0$$

so $b$ is a root of the monic poly. $\det (x \cdot I_n - (a_{ij}))$. 