Recall that a Euclidean domain is a domain with Euclidean algorithm.

That is, $\exists$ norm function N on domain $\mathcal{O} \setminus \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$

s.t.

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

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

Using $N(\alpha) := \alpha \cdot \bar{\alpha}$ on $\mathbb{Z}[i]$, then (i) is clear from multiplicativity and fact that $N(\alpha) = 0 \Rightarrow \alpha = 0$.

(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 $N(\alpha) = |\alpha|^2$)

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 $\mathcal{O}$ 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)

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

$\Rightarrow$ factorization exists

$\Rightarrow$ factorization unique

(A) follows b/c given $(a_1) \subsetneq (a_2) \subsetneq \cdots$ then $\bigcup_i (a_i)$ is ideal (d) so $d \in (a_n)$ for some n

so $(a_m) \supset (a_n) \supset d \supset (a_m) \quad \forall\ m \geq n$. chain stabilizes!

If p irreducible and $p \mid ab$ but $p \nmid a$, show $p \mid b$.

p irreducible means $\nexists$ ideal I s.t. $\mathcal{O} \setminus \{0\} \supsetneq I \supsetneq (p)$.

Now $p \nmid a$ means $a \notin (p)$ so $(p, a) \supsetneq (p) \Rightarrow (p, a) = (1)$.

then we can find $u, v \in \mathcal{O}$ s.t. $up + va = 1$.

$\Rightarrow upb + vab = b$ but since $p \mid ab$, p must divide b. //

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

and key step was understanding that $p \equiv 1 \ (4)$, 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 s.t. a^2 or $b^2 = 1$ other $= 0$.

Quickly check that units are
$\{\pm 1, \pm i\}$

—

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

Won't always require such a specific characterization...

Theorem : The primes π of $\mathbb{Z}[i]$ are :

(1) $\pi = 1+i$

(2) $\pi = a+bi$ with $a^2+b^2 = p$, $p \equiv 1 \ (4)$, " $\ni a > |b| > 0$.

(3) $\pi = p$, rational prime $\equiv 3 \ (4)$.

—

pf : First show all these are indeed primes of $\mathbb{Z}[i]$. Later show this exhausts all primes.

Recall that to 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 α or β must be unit, i.e. π prime.

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

↯ if $p \equiv 3 \ (4)$ so can't have $\pi = p = \alpha \cdot \beta$ in this case

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

$N(\pi) = p_1 \cdots p_r$ from unique fact. in $\mathbb{Z}$
p_i primes, not nec. distinct.

$N(\pi) = \pi \cdot \bar{\pi}$ so π divides some p_i, call it p. $\Rightarrow$ $N(\pi) \mid N(p) = p^2$

i.e. $N(\pi) = p$ 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 p/π is Gaussian integer with norm 1.

and $p \equiv 3 \ (4)$ in this case since if $p=2$ or $p \equiv 1 \ (4)$

then $p = a^2+b^2$ for some $a,b \in \mathbb{Z}$ by Fermat's thm.
$= (a+bi)(a-bi)$ $\Rightarrow$ p not prime ↯.

The theorem makes clear how primes $p \in \mathbb{Z}$ decompose in $\mathbb{Z}[i]$.

if $p \equiv 1 \ (4)$ then $p = \underset{\pi}{\underset{\shortparallel}{(a+bi)}}\underset{\bar{\pi}}{\underset{\shortparallel}{(a-bi)}}$ "p splits" into two conjugate prime factors

if $p \equiv 3 \ (4)$ then p remains prime ("inert")

if $p = 2$, then $p = (1+i)(1-i) = \underbrace{-i}_{\text{a unit}} (1+i)^2$

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: $\alpha = c + di$, $c, d \in \mathbb{Q}$

then α 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 $\equiv 0,1 \ (4)$, must have $(2c)^2 \equiv (2d)^2 \equiv 0 \ (4)$

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

Make this same 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 $a \cdot b$ is root)

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

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

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

$A^* = (a^*_{ij})$ "adjoint matrix" with $\underbrace{a^*_{ji}}_{\text{taking transpose!}} = (-1)^{i+j} \det(A^{(i,j)})$ ← matrix with i^{th} row, j^{th} column deleted

Then $AA^* = A^*A = \det(A) \cdot I_r$

(Cor: $A \cdot x = 0 \Rightarrow \det(A) \cdot x = 0$)
for any vector $x = (x_1, \dots, x_r)$

Now we can prove: if $A \subseteq B$ is an extension of rings then $b_1, \dots, b_n$ integral over A (satisfy monic poly. with coeffs in A)
$\Leftrightarrow A[b_1, \dots, b_n]$ is a finitely generated A-module. (Prop. 2.2 in Neukirch)

Cor: if $b_1, \dots, b_n \in B$ are integral over A, so is any elt in $A[b_1, \dots, b_n]$.

pf of cor: If $b \in A[b_1, \dots, b_n]$, then $A[b_1, \dots, b_n] = A[b, b_1, \dots, b_n]$ is a fin. gen. A-module. //

Proof of Proposition 2.2: Let $b \in B$ be integral over A and

f: ~~the~~ a monic polynomial in $A[x]$ with $f(b) = 0$. Show $A[b]$ is finitely generated.

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

$$g(x) = q(x) \cdot f(x) + r(x) \quad \text{with } \deg(r) < n.$$

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

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

the case ($b_1, \ldots, b_n$ integral over $A \Rightarrow A[b_1, \ldots, b_n]$ f.gen.)

now follows by induction.

For converse, let $w_1, \ldots, w_r$ be generators for $A[b_1, \ldots, b_n] / A$

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

$$b w_i = \sum_{j=1}^{n} a_{ij} w_j \qquad a_{ij} \in A \qquad (*)$$

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

Then ~~det~~ $M \cdot \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = 0$ by construction so

$\det(b \cdot I_n - (a_{ij})) \cdot w_i = 0 \quad \forall i.$ Since w_i's generators, then $1 = c_1 w_1 + \cdots + c_r w_r$

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

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