Mathematicians are brilliant people. Especially before they have so many fancy tools, all they have is brilliance.

— Micheal Zieve

Lemma. *If R is Noetherian (i.e. an integral domain in which every ideal is finitely generated) then every non-zero non-unit in R is product of irreducible elements.*

In general, it is easier for elements to be irreducible than prime.

Proof. Suppose otherwise. Then $\exists x \in R$ non-zero non-unit, not a product of irreducible elements $\implies$ x is reducible, say $x = yz$. At least on of y or z is neither a unit nor a product of irreducibles.

Hence $x = x_1 y_1$, where x_1 is not unit or product of irreducibles, y_1 is not a unit. Likewise $x_1 = x_2 y_2$ where x_2 is a not unit or product of irreducibles with y_2 is not a unit. $x_n = x_{n+1} y_{n+1}$.

$$(x) \subsetneq (x_1) \subsetneq (x_2) \subsetneq \dots$$

$\bigcup_{n \geq 1} (x_n)$ is an ideal of R which doesn't contain 1. It is finitely generated $\implies$ all generator is in x_n for some finite $n \implies (x_n) = (x_{n+1})$, a contradiction. ■

Last time: $R =$ PID $\implies$ all irreducible elements in R are prime $\implies$ every element or R has ≤ 1 factorization into irreducible elements (up to permutation).

On the other hand, $R =$ PID $\implies$ R is Noetherian $\implies$ every nonzero element of R has a factorization into irreducible elements.

These two together shows that R is UFD.

Lemma. *If R is a Euclidean integral domain (i.e. $\exists \phi : R \to \{-\infty\} \cup \mathbb{Z}_{\geq 0}$ s.t. $\forall a, b \in R$ with $b \neq 0$, $\exists q, r \in R$ s.t. $a = bq + r$ where $\phi(R) < \phi(b)$) then R is PID.*

Proof. If I is a nonzero ideal of R, then $\phi(I) \subset \{-\infty\} \cup \mathbb{Z}_{\geq 0}$. So $\phi(I \setminus \{0\})$ has a smallest element $\phi(b), b \in I, b \neq 0$. Then $I = (b)$, since $(b) \subseteq I$ and also $I \subseteq (b)$ because $a \in I \implies a = bq + r, q, r \in R, \phi(r) < \phi(b)$.

But $a, b \in I, a = bq + r \implies r \in I$. So the minimalist of b of $\phi(b)$ implies $r = 0$, so $b \mid a \implies a \in (b)$. ■

Example. $\mathbb{Z}[i]$ Euclidean $\implies$ PID $\implies$ UFD.

$\phi(a + b\sqrt{3}) := a^2 + 3b^2$ is NOT a Euclidean function on $\mathbb{Z}[\sqrt{-3}]$, since you can't divide $1 + \sqrt{-3}$ by 2 to get a smaller remainder.

Moreover, $\mathbb{Z}[\sqrt{-3}]$ is not Euclidean, since it is not a UFD: $(1+\sqrt{-3})(1-\sqrt{-3}) = 4 = 2\cdot 2$, all irreducible and they are not unit multiples of each other.

But $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ is Euclidean with ϕ as Euclidean function.

$\mathbb{Z}[i]$ Euclidean $\implies$ PID $\implies$ UFD. What are the primes in $\mathbb{Z}[i]$?

Define the "norm" $N : \mathbb{Z}[i] \to \mathbb{Z}, a+bi \mapsto a^2+b^2 = |a+bi|^2$. Then $N(xy) = N(x)N(y)$ and $N(x) = x\bar{x}$ where $\overline{a+bi} = a-bi$.

Lemma. *$N(x) \geq 0$, $N(x) = 0 \iff x = 0$, $N(x) = 1 \iff x = \pm 1$ or $\pm i$, $N(x) = 1 \iff$ x is a unit in $\mathbb{Z}[i]$.*

Proof. The first 3 statements are easy. If $N(x) = 1$ then $x\bar{x} = 1 \implies x =$ unit. If $x =$ unit then $xy = 1, y \in \mathbb{Z}[i] \implies N(xy) = N(x)N(y) = N(1) = 1 \implies N(x) = 1$. ■

Corollary. *If $x \in \mathbb{Z}[i]$ and $N(x)$ is prime in $\mathbb{Z}$ then x is irreducible in $\mathbb{Z}[i]$.*

But there are other irreducibles in $\mathbb{Z}[i]$ too. Given $x \in R$ non-zero non-unit, then $N(x) \in \mathbb{Z}_{\geq 2}$. If x is irreducible then $\bar{x}$ is also irreducible (since complex conjugation is a homomorphism) so $N(x)$ is a product of two irreducibles in $\mathbb{Z}[i]$. But we can write $N(x) = p_1 p_2 \ldots p_k$ where p_i is prime numbers in $\mathbb{Z}$ and then write each p_i as product of irreducibles in $\mathbb{Z}[i]$, so either $k = 1$ and $p_1 =$ product of two irreducibles in $\mathbb{Z}[i]$ or $k = 2$ and p_1, p_2 are two irreducibles in $\mathbb{Z}[i]$ where $x = up_1, \bar{x} = p_2 v$, u, v units $\implies p_1 = p_2$.

Remains to show for $p \in \mathbb{Z}$ prime, p is irreducible in $\mathbb{Z}[i] \iff p \equiv 3 \pmod 4$.