Recap: Looked at Ring, $+, -, 0, \times, 1$. No $\div$.

Def: Set $R^\times$ = set of units $= \{u \in R : \exists v \in R \cdot uv = 1\}$.

Def: $r \in R$ is irreducible if: $s \mid r \Rightarrow \begin{cases} s \sim r \\ s \in R^\times \end{cases}$ OR

Def: $p \in R$ is prime if: $p \mid ab \Rightarrow \begin{cases} p \mid a \\ p \mid b \end{cases}$ OR (or both)

Def: $r \sim s$ "associates" $\Leftrightarrow \exists u \in R^\times : r = s \cdot u$.

"Irreducible: Who divides me; Prime: Who do I divide".

Lemma: prime $\Rightarrow$ irreducible (For R an Integral Domain).

pf: Let $p \in R$ be prime. Suppose $s \mid p$. Want: $\begin{cases} s \in R^\times \\ s \sim p \end{cases}$.

$\Rightarrow \exists k$ s.t. $s \cdot k = p \Rightarrow p \mid s \cdot k \Rightarrow$

$\begin{cases} p \mid s \Rightarrow p \cdot \ell = s \Rightarrow p = s \cdot k = p \cdot \ell \cdot k. \\ p \mid k \text{ same argument} \Rightarrow s \in R^\times. \end{cases} \Rightarrow p^1(\ell k - 1) = 0.$

Def: A ring R is an Integral Domain if: $x \cdot y = 0 \Rightarrow \begin{cases} x = 0 \\ y = 0 \end{cases}$ OR (or both)

$\Rightarrow \ell \cdot k - 1 = 0.$
$\Rightarrow \ell \cdot k = 1$
$\Rightarrow k \in R^\times$
$\Rightarrow s \sim p$ ✓
$\Rightarrow p$ irred ∎

(Non) Ex: $R = \mathbb{Z}/6\mathbb{Z}$. $2 \cdot 3 \equiv 0$.
Not Integral Domain.

Converse lemma: Assume R is a PID. Then irreducible $\Rightarrow$ prime.

Pf: Let $r \in R$ be irreducible. Assume $r \mid a \cdot b$

Assume $r \nmid a$ (Need: $r \mid b$). Look at $(r, a) = (d)$ (PID).

But $d \mid r \Rightarrow \begin{cases} d \sim r \Rightarrow d = r \cdot u \mid a. \Rightarrow r \mid a \\ d \in R^\times \end{cases}$ ← CAN'T happen.

$a \in (d)$.

$\Rightarrow (d) = R$.

In summary: $r \nmid a$ & r irred $\Rightarrow (r, a) = R$.

$\Rightarrow (r \cdot b, a \cdot b) = (b) \subset (r) \Rightarrow r \mid b$ ✓

But $(r \cdot b) \subset (r)$

$(a \cdot b) \subset (r)$ ⇉

Proved: Euclidean Domain (division alg) $\Rightarrow$ PID $\Rightarrow$ Noetherian $\Rightarrow$ ord_p has good properties $\Rightarrow$ UFD.

Def: R is Noetherian iff: $I_1 \subseteq I_2 \subseteq \cdots \Rightarrow \exists N$ ← $I_N = I_{N+1} = \cdots$

"ascending chain of ideals" condition.

Examples: $\mathbb{Z}$, $\mathbb{Z}[i]$ $(\Rightarrow p = x^2 + y^2)$, $k[x]$ ← norm = degree. polynomial long division.

$\mathbb{Z}[\omega]$ $(\Rightarrow p = x^2 - xy + y^2)$ if $p \equiv 1 \pmod 3$. (2)

Review How to find $x, y \in \mathbb{Z}$ s.t.

$p \equiv 1 \pmod 3 \Rightarrow p = x^2 - xy + y^2$

Ex: $p = 3571$.

$p \pmod 3 = 3+5+7+1$

$\equiv 1 \ (3)$.

(Because $10 \equiv 1 \pmod 3$).

$\ell = 1190$.

Try a's until $a^\ell \neq 1$.

$a=2$? Efficiently: X^1.

$2^{1190} \pmod{3571} \equiv 3467$.

Now:

$z = 3467$.

$3467^3 \equiv 1 (3571)$.

Abstractly, given p.

Let $\ell = \frac{p-1}{3}$.

Then $(a^\ell)^3 = a^{p-1} \equiv 1$.

So any $z = a^\ell$ has

$z^3 \equiv 1 \ (p)$.

But don't want $z = 1$.

Claim: 2ℓ of the a's mod p have $a^\ell \neq 1$.

Why? Look at

$X^\ell - 1 \equiv 0$.

Claim: Any poly of deg ℓ has $\leq \ell$ roots.

proof: (by induction on ℓ.)

$\ell = 1$: $f(x)$ is a poly of deg 1.

$\Rightarrow ax + b = f(x) \Rightarrow x = -b \cdot \bar{a}$.

Induction: If $f(x)$ has root r,

Then $f(x) = (x-r)\, g(x)$.

& $g(x)$ has deg $\ell - 1$.

$\Rightarrow$ # a mod with $a^\ell - 1 \equiv 0$ is $\leq \ell$.

"Factor Thm"

pf: division alg:

$f(x) = q \cdot (x-r) + s$.

$\uparrow$ deg $s < 1$.

Eval at $x = r$.

$0 = f(r) = s$.

Concrete:

$z-w = 3467-w$ | $\bar{w} = w^2 = -1-w$

$\gcd(3467-w, 3571)$.

$3571 = (3467-w)\cdot q_1 + r_1$

$\frac{(3571)(3467+1+w)}{(3467-w)(3467-\bar{w})}$

$= \frac{(3571)(3468+w)}{3467^2+3467+1} \to 12023557$

$= \frac{12\text{mill} \quad +w}{12\text{mill}} \approx 1 = q_1$

$r_1 = 104+w$.

Look at: $\frac{(3467-w)}{(104+w)}\frac{(104+\bar{w})}{(104+\bar{w})}$ (103, $-1-w$)

$= \frac{357101 - 3467w + w^2}{104^2 - 104\cdot 1 + 1^2}$ ($-103w$, $-1-w$)

$= \frac{357100 - 3571w}{10713} \approx 33 + 0w = q_2$

$3467-w = \underbrace{33\cdot(104+w)}_{3432+33w} + r_2 \Rightarrow r_2 = 35 - 34w$

$N(r_2) = 35^2 + 34\cdot 35 + 34^2 = 3571$.

$X=35, y=-34$

Abstractly:

$z^3 - 1 \equiv 0 \pmod{p}$.

$(z^3-1) = p\cdot k$.

$(z-1)(z^2+z+1)$

$(z-1, p) = 1$.

$\Rightarrow z^2+z+1 = p\cdot k'$.

$(\text{in } \mathbb{Z}[w]) \Rightarrow (z-w)(z-\bar{w})$

$\Rightarrow p$ factors

$\Rightarrow \gcd_{\mathbb{Z}[w]}(z-w, p) = x+yw$.

$\Rightarrow p = (x+yw)(x+y\bar{w}) = x^2 - xy + y^2$.

Next: $3467-w = q_2(104+w) + r_2$.