Factorisation & irreducibility of polynomials

Problem: Given $p(x) \in \mathbb{Q}[x]$

Determine if $p(x)$ is irreducible.

Idea:- (1) ~~Fo~~ Irred in

$$\mathbb{Z}[x] \xleftrightarrow[\text{almost equivalent}]{} \mathbb{Q}[x]$$

(2) For irred in $\mathbb{Z}[x]$ use 'mod p' techniques, cleverly.

<u>Ex:</u> $p(x) = x^3 + 2x + 20$ is irred in $\mathbb{Z}[x]$.

<u>Pf</u>: Suppose $p(x) = f(x) \cdot g(x)$ in $\mathbb{Z}[x]$

Homomorphism
$$\mathbb{Z}[x] \to \mathbb{Z}/3\mathbb{Z}[x]$$
$$h(x) \mapsto \bar{h}[x]$$

gives $\bar{p}(x) = \bar{f}(x) \cdot \bar{g}(x)$

$$x^3 + 2x + 2 = (\bar{f}(x)) \cdot (\bar{g}(x))$$

Let's rule out a <u>linear factor</u> $\leftrightarrow$ <u>root</u>.

$\uparrow$ Check $0, 1, 2$.

No root $\Rightarrow$ LHS is irred in $\mathbb{Z}/3\mathbb{Z}[x]$. $\Rightarrow$ $\bar{f}$ or $\bar{g}$ is a constant.

Then f is either a constant in $\mathbb{Z}[x]$

or its non-const terms are div. by 3. $\Big\}$ can't <u>happen</u>.

$\hookrightarrow$ leading term div by 3.

$$x^3+2x+20 = p(x) = \underbrace{f(x)}\cdot g(x)$$

$\bar{g}(x)$ has deg 3 $\Rightarrow$ $g(x)$ deg ≥ 3 $\Rightarrow$ $f(x)$ deg 0.

Lead term of $f(x)$ $\mid$ leading term of $p(x)$ $\Rightarrow$ 3 cannot divide leading term of $f(x)$.

The only constant dividing $x^3+2x+20$ in $\mathbb{Z}$

are ± 1 $\Rightarrow$ $f(x) = \pm 1$.

$\square$

Thm: Let $f(x) \in \mathbb{Z}[x]$ be such that leading coeff of $f(x)$ not divisible by prime p. If $\bar{f}(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ is irreducible then $f(x)$ is ~~irreducible~~ ~~can~~) ~~only~~ ~~be~~ does not factor as a product of poly of lower deg.

Pf (sketch) :– Consider $f(x) = h(x) \cdot g(x) \in \mathbb{Z}[x]$

Want $h(x)$ or $g(x)$ is a constant.

Get $\bar{f}(x) = \bar{h}(x) \cdot \bar{g}(x)$. $\in \mathbb{Z}/p\mathbb{Z}[x]$.

$\bar{f}(x)$ irred $\Rightarrow$ $\bar{h}(x)$ or $\bar{g}(x)$ is constant.

Then $\deg \bar{g}(x) = \deg \bar{f}(x) = \deg f(x)$.

$$\leq \deg g(x).$$

So $\deg f(x)$ must be $= \deg g(x) \Rightarrow h(x)$ constant.

$\square$

Ex. $x^4+2x+20$ mod 3

x^4+2x+2 — irred or red in $\mathbb{Z}/3\mathbb{Z}[x]$?

irred.

Quadr. Qudr.

Linear. Cubic

Check all roots

No roots

Eliminated!

✓(x) ✓$(x+1)$ ✓$(x+2)$

$\cancel{x^2}$ $\cancel{x^2+x}$ $\cancel{x^2+2x}$ x^2+1 $\cancel{x^2+2}$

$\cancel{x^2+x+1}$ x^2+x+2 $\cancel{x^2+2x+1}$ x^2+2x+2