Irreducibles in $\mathbb{Z}_p[x]$

Look first in $\mathbb{Z}_2[x]$.

degree 2: four polynomials:

~~x^2~~

~~$x^2+\bar{1} = (x+\bar{1})^2$~~

~~$x^2+x = x(x+1)$~~

$x^2+x+\bar{1}$ $\rightsquigarrow$ $f(\bar{0}) = \bar{1}$ $f(\bar{1}) = \bar{1}$

no roots, deg = 2, so irred.

degree 3: eight polynomials

~~x^3~~

~~$x^3+\bar{1}$~~

~~x^3+x~~

$x^3+x+\bar{1}$

~~x^3+x^2~~

$x^3+x^2+\bar{1}$

~~x^3+x^2+x~~

~~$x^3+x^2+x+\bar{1}$~~

no roots, deg = 3, so irred.

0 is a root of these

1 is a root of these

degree 4: let's only list ones w/o roots

$\bar{0}$ not a root $\Rightarrow$ const term is $\bar{1}$

$\bar{1}$ not a root $\Rightarrow$ odd # of terms.

$f(\bar{1}) = \begin{cases} 0 & \text{if even \# of non-zero terms} \\ 1 & \text{if odd \# of non-zero terms} \end{cases}$

x^4+x+1

~~x^4+x^2+1~~

x^4+x^3+1

$x^4+x^3+x^2+x+1$

but a quartic could also factor as quadratic · quadratic

$(x^2+x+\bar{1})(x^2+x+\bar{1}) = x^4+x^2+\bar{1}$

3 irreducibles.

degree 5: on worksheet. 6 irreducible quintics.

You could do a similar process of elimination to get irreducibles in $\mathbb{Z}_p[x]$ for any p.

(Probably write a computer program...)

Page 112: list for $\mathbb{Z}_3[x]$ deg ≤ 4

Why do we care?

Let $f \in \mathbb{Q}[x]$ $\quad x^4 + \frac{3}{5}x + \frac{1}{5}$

clear denominators to get in $\mathbb{Z}[x]$ $\quad 5x^4 + 3x + 1$

if it factors in $\mathbb{Z}[x]$ ws it also factors in $\mathbb{Q}[x]$

Gauss's lemma: converse is true too.

Proof: next time.

Proposition: given $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$

let $p \nmid a_n$, and consider

$$\bar{f} = \bar{a}_n x^n + \cdots + \bar{a}_1 x + \bar{a}_0 \in \mathbb{Z}_p[x].$$

If f is reducible in $\mathbb{Z}[x]$ then $\bar{f}$ is reducible in $\mathbb{Z}_p[x]$. | prove this

Equivalently: if $\bar{f}$ is irreducible in $\mathbb{Z}_p[x]$ then f is irreducible in $\mathbb{Z}[x]$. | use this

Proof: if $f = gh$ then $\bar{f} = \bar{g}\bar{h}$
because $+$ and $\cdot$ of coeffs is compat w/ reducing mod p.

if g and h are not const in $\mathbb{Z}[x]$
write $g = b_m x^m + \cdots \qquad h = c_k x^k + \cdots$

then $gh = b_m c_k x^{m+k} + \cdots$
so $b_m c_k = a_n$

assumed $p \nmid a_n$, so $p \nmid b_m$ and $p \nmid c_k$
so $\bar{g}$ and $\bar{h}$ are not const in $\mathbb{Z}_p[x]$ ∎

Example: $f = 5x^4 + 3x + 1$ in $\mathbb{Z}[x]$
reduce mod 2:
$\bar{f} = \bar{5}x^4 + \bar{3}x + \bar{1} = x^4 + x + \bar{1}$ in $\mathbb{Z}_2[x]$
this is irred, so f was irred.

Notice: rat'l root thm tells us that
f has no roots in $\mathbb{Q}$
but can't tell us that $f \neq$ quadratic · quadratic

WARNING: Don't use it backwards.

if I reduce mod 3, then
$\bar{f} = \bar{2}x^4 + \bar{1} \in \mathbb{Z}_3[x]$

factors as $(\bar{2}x + \bar{1})(x + \bar{1})(x^2 + \bar{1})$