Proposition 0.1 *$f(x) = a_n x^n + ... + a_0 \in \mathbb{Z}[x]$ p = prime.*

Assume that $p|a_n, p|a_0, ...a_{n-1}$ and $p^2 \not| a_0$

Then $f(x)$ is irred over $\mathbb{Q}$

Proof: Suppose for a contradicition a˙nxˆn + .. a˙0 = (b˙rxˆr ˙ ... + b˙0)(c˙sxˆs+...+x˙0), with $r, s < n$.

By Gauss's lemma it is enough to assume that $b_i, c_i \in \mathbb{Z}$.

$a_0 = b_0 c_0$.

$\therefore p|b_0$ (say) and $p|c_0$.

$a_1 = b_1 c_1 + b_1 c_0$. pdiv .. pdiv pnot div c˙0

$\therefore p|b_1$

$\therefore a_{n-1} = b_{n-1} c_o + ... + b_o c_{n-1}$

$\therefore p|b_{n-1}$

But $r < s$

$\therefore p|b_r$

$\therefore p|b_r c_s = a_n$

Contradiction!. $\therefore f(x)$ irred. ■

Aside: $x^4 + 1$ is red over $\mathbb{F}_p$ for all p, but irred over $\mathbb{Q}$.

Proposition 0.2 *p prime, then $x^{p-1} + x^{p-2} + ... + x + 1$ is irreducible over $\mathbb{Q}$. More generally $\frac{x^{p^n}}{x^{p^{n-1}}} = x^{p^{n-1}(p-1)} + x^{p^{n-1}(p-2)} + ... + 1$ is irred over $\mathbb{Q}$.*

First, two tricks.

$\forall c \in F$

$f(x)$ is irreducible $\iff$ $f(x+c)$ is irreducible.

Eisenstein's property

$f(x) = \lambda x^n$ mod p $f(0) \ncong 0$ mod p^2

Translated version: $g(x) = f(x-c)$. $c \in Z$

$g(x) == \lambda(x-c)^n$ mod p.

$g(c) \neq= 0 mod p^2$

Proof technique: $f(x)$ is Eisenstein wrt p "at x=1"

i.e. $f(x+1)$ is Eisenstein w.r.t p.

Important facts:

1. p prime $\implies$ $p|\binom{p}{k}$, for $k = 1, ..., p-1$
2. $(x+y)^p = x^p + px^{p-1}y + \cdots + pxy^{p-1} + y^p = x^p + y^p$ mod p, as middle terms have p as a factor.

3. If R is a Ring of char p, then $F : R \to R, F(x) = x^p$ is a ring homomorphism (Frobenius homo)
4. $(x-y)^p == x^p - y^p$ mod p

Proof: $g(x)? = f(x+1)$ is Eisenstein wrt p.

$g(x)? = x^{p^{n-1}p-1}$ mod p.

$g(0)? \neq 0$ mod p

i.e. we need

$f(x+1)? = xp^{n-1}(p-1)$ mod p.

$f(1) = 0$, mod pˆ2

Recall $f(x) = \frac{x^{p^n}-1}{x^{p^{n-1}}-1} = 1 + x^{p^{n-1}} + ... + x^{p^{n-1}(p-1)}$

$\therefore f(1) = p \neq 0$ mod p^2

$x^{p^n} - 1 = (x^{p^{n-1}} - 1)f(x)$.

Working mod p,

$(x-1)^{p^n} == (x-1)^{p^{n-1}} f(x)$.

I.e. $\mathbb{F}_p[x]$, $(x-1)^{p^n} = (x-1)^{p^{n-1}} \bar{f}(x)$

We get $\therefore f(x) = x - 1$ i.e $f(x) = x - 1 mod p$ $\therefore f(x+1)$ is Eisenstein w.r.t p.

$\therefore f(x)$ is irred / $\mathbb{Q}$.

Ex: Prove $f(x+1)$ is Eisenstein directly.

Cor. $f(x)$ is the minimal polynomial over Q of $\zeta_p^n = e^{\frac{2\pi i}{p^n}}$

Cor. $[\mathbb{Q}(\zeta_p^n) : \mathbb{Q}] = p^{n-1}(p-1)$

$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$

Later : $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m)$ ■