Eisenstein's Criterion

Given $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$
where $a_i \in \mathbb{Z}$, if $\exists p$, prime such that
$p \nmid a_n$, $p \mid a_i$ for $0 \le i < n$, and $p^2 \nmid a_0$
then $f(x)$ is irreducible over $\mathbb{Z}$, hence $\mathbb{Q}$.

Pf: FSOC suppose $f(x)$ factors as
$g(x) \cdot h(x)$ where $1 \le \partial g, \partial h < n$.

Let $g(x) = b_r x^r + b_{r-1}x^{r-1} + \cdots b_1 x + b_0$
$h(x) = c_s x^s + c_{s-1}x^{s-1} + \cdots c_1 x + c_0$

Note $a_0 = b_0 c_0$. Implies $p \mid b_0$ but
$p \nmid c_0$.

Also $p \nmid a_n = b_r c_s$ so $b \nmid b_r$

Claim: $\exists t \in \mathbb{N}$ such that $p \nmid b_t$ and
t is minimal in this regard.

Consider $a_t = \overset{p\nmid}{b_t} c_0 + \overset{p\mid}{b_{t-1}} c_1 + \overset{p\mid}{b_{t-2}} c_2 + \cdots$
$\overset{p\mid}{b_0} c_t$. We have assumed that $p \mid a_t$

This shows $p \mid b_t$ $\Rightarrow\Leftarrow$

So $f(x)$ <u>not</u> reducible. ■

$2x^5 - 6x^3 + 9x^2 - 15$ $\quad p=3$

not reducible

$$\frac{x^p - 1}{x-1} = \underline{x^{p-1} + x^{p-2} + \cdots x + 1}$$

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots$$

Show $\phi_p(x)$ is irreducible over $\mathbb{Z}$:

Consider $\phi_p(y)$ where $y = x+1$

$$\phi_p(x+1) = \frac{(x+1)^p - 1}{(x+1)-1} \stackrel{?}{=}$$

$$(x+1)^p = \sum_{k=0}^{p} \binom{p}{k} x^k \underline{(1)^{p-k}}$$

$$\binom{p}{0} x^0 + \binom{p}{1} x^1 + \binom{p}{2} x^2 + \cdots \binom{p}{p} x^p$$

$$(x+1)^p - 1 = \binom{p}{1} x + \binom{p}{2} x^2 + \cdots \binom{p}{p} x^p$$

③

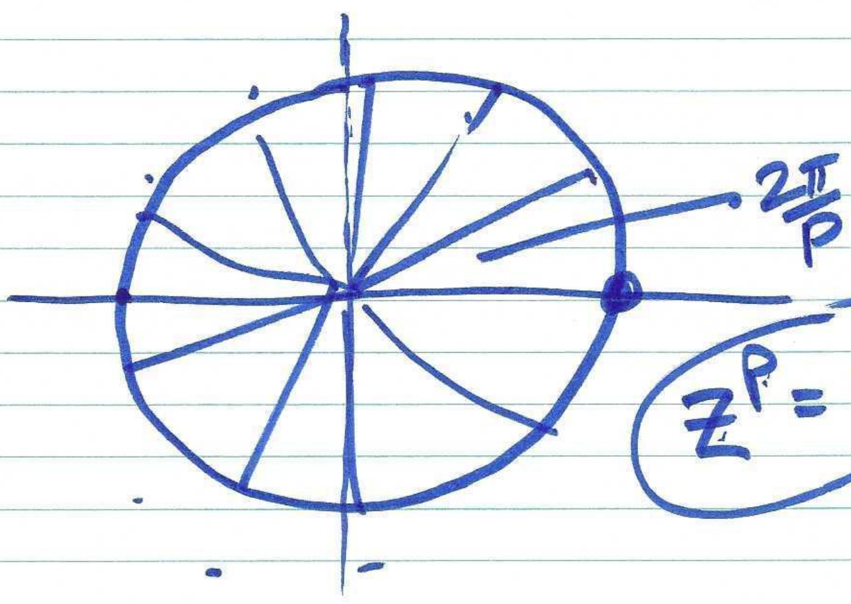
$$\frac{(x+1)^p-1}{x} = \binom{p}{1} + \binom{p}{2}x + \cdots \binom{p}{p}x^{p-1}$$

$$\downarrow$$

$$\frac{p!}{(p-1)!\,1!} \quad \frac{p!}{(p-2)!\,2!} + \cdots + x^{p-1}$$

$$\downarrow$$

$$p + \frac{p(p-1)}{2}x + \cdots x^{p-1}$$



$$z^p = 1$$

If $a_0, a_1, a_2, \cdots a_n \in \mathbb{F}$

$c_0, c_1, c_2, \cdots c_n \in \mathbb{F}$

f is unique poly $\ni f(a_i) = c_i$

Lagrange Interpolation $\quad (x - a_i)$

$$f(x) = \sum_{i=0}^{n} \frac{(x-a_0)\cdots(x-a_{i-1})(x-a_{i+1})\cdots(x-a_n)}{(a_i-a_0)\cdots(a_i-a_{i-1})(a_i-a_{i+1})\cdots(a_i-a_n)} c_i$$

Finite Fields all have order p^n, some n w/ p prime.

Field of order 8.

x^3+x+1 is irred. over $\mathbb{Z}_2$

$\mathbb{Z}_2 / \langle x^3+x+1 \rangle$

"zero"

$x^2+x+1+\langle x^3+x+1\rangle + x^2+1+\langle x^3+x+1\rangle$

$$x^3+x+1 \equiv 0$$
$$x^3 \equiv x+1$$

$$= \underline{x} + \langle x^3+x+1 \rangle$$

	1	x	$x+1$	x^2	x^2+1	$\cdots$
1	1	x	$x+1$	x^2	x^2+1	
x	x					
$x+1$	$x+1$					
x^2	x^2		x^2+x+1			
x^2+1	x^2+1		x^2		x^2+x+1	

$$x^2(x+1) = x^3+x^2 = x^2+x+1$$

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

$$x(\underbrace{x^3}_{x+1}) = x(x+1) = \underline{x^2+x}$$

$$(x^2+1)(x+1) = \underline{x^3} + x^2 + \underline{x+1}$$

$\mathbb{Z}_3$

ax^2+bx+c

x^2+x+1

$x=1$

$x^2+x+2 = 0_{(3)}$

x^2+x+2

$x^2 = -x-2$

$+2x+1$

$$\mathbb{Z}_3[x] \Big/ \langle x^2+x+2 \rangle \approx F_9$$

	1	x^2+2
1		
$x+1$		

$2(-x-2) =$

$-2x-4$

$x-1$

$2(x^3+1)$

$$x^3+\underbrace{x^2+2x+2}_{x}$$

x^3+x

$$x^3 = x(x^2) = x(+2x+1) = 2x^2+x$$

$$\mathbb{Z}_3[x]/\langle x^2+x+2\rangle = ax+b \qquad a,b \in 0,1,2$$

$$\begin{array}{cc|ccc}
 & & & a & \\
 & & 0 & 1 & 2 \\
\hline
 & 0 & 0 & x & 2x \\
b & 1 & 1 & x+1 & 2x+1 \\
 & 2 & 2 & x+2 & 2x+2
\end{array}$$

$$\mathbb{Z}_K[x]/\langle \underbrace{x^n + \cdots a_0}\rangle$$

$$a_1x^{n-1}+a_2x^{n-2}\cdots a_0$$

$$a_i \in \mathbb{Z}_K$$