Eisenstein's criterion over $\mathbb{Z}$: Suppose $f \in \mathbb{Z}[x]$,

$$f(x) = \sum_{i=0}^{n} a_i x^i, \quad \gcd(a_0, \dots, a_n) = 1,$$

that p is a prime number, $p \mid a_i$, $0 \le i < n$, $p \nmid a_n$, and $p^2 \nmid a_0$. Then f is irred. over $\mathbb{Z}$ (and therefore over $\mathbb{Q}$ by Gauss's lemma).

Pf: Suppose f satisfies the hypotheses and, by way of contradiction, $\exists\, g, h \in \mathbb{Z}[x]$ with $f(x) = g(x)h(x)$.

Let $\tilde{f}$, $\tilde{g}$, and $\tilde{h}$ are the images of f, g, and h in $(\mathbb{Z}/p\mathbb{Z})[x]$, and $\deg g, h \ge 1$. Then:

- W.L.O.G., can assume that the leading coeffs of g and h are not $0 \bmod p$.
- $\tilde{f}(x) = a_n x^n = \tilde{g}(x)\tilde{h}(x)$. Since $(\mathbb{Z}/p\mathbb{Z})[x]$ is a UFD, the constant coeffs of g and h are $0 \bmod p$.

  $\Rightarrow$ const. coeff. of $f(x)$ is $0 \bmod p^2$.

  Contradiction $\Rightarrow$ f is irreducible over $\mathbb{Z}[x]$. $\blacksquare$

Exs: Are the following polys. irred. in $\mathbb{Z}[x]$?

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

Degree 2 poly. w/ no roots in $\mathbb{Z}/2\mathbb{Z}$

$\Rightarrow$ irred. over $\mathbb{Z}/2\mathbb{Z}$ $\Rightarrow$ irred. over $\mathbb{Z}$

2) $f(x)=x^4+10x^3+6x+2$

Irreducible by Eisenstein @ 2.

3) $f(x)=x^4+1$

$f(x+1)=(x+1)^4+1=x^4+4x^3+6x^2+4x+2$

is irred. by Eis. @ 2 $\Rightarrow f(x)$ irred.

4) $f(x)=x^{p-1}+x^{p-2}+\dots+x+1$, p a prime.

$$f(x)=\frac{x^p-1}{x-1}$$

$$\Rightarrow f(x+1)=\frac{(x+1)^p-1}{x}=x^{p-1}+\binom{p}{1}x^{p-2}+\binom{p}{2}x^{p-3}+\dots+\binom{p}{p-2}x+\binom{p}{p-1}$$

$p\mid\binom{p}{i}$, $1\le i\le p-1$, and $p^2\nmid\binom{p}{p-1}$,

so this is Eis. @ p $\Rightarrow$ f is irred.

Finite fields

Thm: If F is a finite field then $|F| = p^n$ for some prime p and $n \in \mathbb{N}$.

Pf: The prime subfield of F is finite, so it is $\mathbb{F}_p$ for some prime p. Therefore F is a vector space (of finite dimension) over $\mathbb{F}_p$, and the result follows. $\square$

Thm: For p prime and $n \in \mathbb{N}$, there exactly one finite field of order p^n (denoted $\mathbb{F}_{p^n}$), up to isomorphism.

(pf next semester)

Thm: Suppose F is a field. Any finite subgroup of $F^\times$ is cyclic.

Pf: Suppose G is a finite subgroup of $F^\times$.

By FTFGAC,

$$G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}, \quad n_i \mid n_{i+1}, \ 1 \le i < k.$$

Then every element of G is a root of the poly $f(x) = x^{n_k} - 1 \in F[x]$.

Since F is a field, f has at most n_k roots, so $k = 1$. $\square$