Euclidean algorithm

Lemma

For $f, g, h \in F[x]$ where F is a field

1. $deg(f + g) \leq \max(deg(f), deg(g))$.
2. If $f, g \neq 0$ then $deg(fg) = deg(f) + deg(g)$.
3. If $fg = 0$ then $f = 0$ or $g = 0$.
4. If $fh = gh$ and $h \neq 0$ then $f = g$.
5. If $f \neq 0$ then there exists g with $fg = 1$ iff $deg(f) = 0$.

Theorem (Euclidean algorithm)

For a field F, $f, g \in F[x]$ with $deg(g) \neq 0$ there exist unique $q, r \in F[x]$ where $deg(r) < deg(g)$ and

$$f = qg + r.$$

Irreducible polynomials

- For polynomials $f, g \in F[x]$, we say that g divides f if there is some $h \in F[x]$, $f = gh$.
- We say that $f \in F[x]$ is irreducible over F if whenever $g \in F[x]$ divides f then either $deg(g) = deg(f)$ or $deg(g) = 0$.
- Notice that $a_1x + a_0$ is irreducible for any $a_1 \neq 0$.
- Polynomials can also be thought of as functions on the underlying field but you must be careful. If $f \in F[x]$ for some field F then for any $c \in F$, $f(c)$ makes sense by direct substitution.
- On the other hand, it is possible for two polynomials to agree on all $c \in F$ but not to be equal as polynomials.

Irreducible polynomials, cont'd

Lemma

Suppose $f \in F[x]$.

1. *If $f(c) = 0$ for some $c \in F$ then $x - c$ divides f.*
2. *If f has degree n then f has at most n roots.*
3. *If $deg(f) = 2, 3$ then f is irreducible iff f has no root in F.*

Cut to the chase

- Where do the finite fields come from? From $Z_p[x]$ itself.
- Fix $f \in Z_p[x]$ and write
$$g \equiv h \bmod f$$
if f divides $g - h$.
- This is an equivalence relation just like conguences mod n was for integers.
- Notice that every $g \in Z_p[x]$ is equivalent to one with degree $< deg(f)$; in fact, if
$$g = qf + r$$
then $g \equiv r \bmod f$.
- It follows that there are only finitely many equivalence classes of $Z_p[x]$ mod f.
- In fact, no two polynomials of degree $< deg(f)$ are equivalent and so there are p^n many equivalence classes of polynomials in $Z_p[x]$ mod f where $n = deg(f)$.

The object $Z_p[x]/(f)$

- Write $Z_p[x]/(f)$ for the equivalence classes of $Z_p[x]$ modulo f.
- As with the integers, addition and multiplication of equivalence classes of $Z_p[x]$ mod f is well-defined. That is,

  $$g \equiv g' \bmod f \text{ and } h \equiv h' \bmod f$$

  then

  $$g + h \equiv g' + h' \bmod f \text{ and } gh \equiv g'h' \bmod f.$$

- All basic rules of arithmetic now apply. In particular, the class of 0 is the additive identity and the class of 1 is the multiplicative identity.
- The rest of the properties of $Z_p[x]$ depend on the properties of f.

The object $Z_p[x]/(f)$ cont'd

- If f is reducible over Z_p, say $f = gh$ then $Z_p[x]/(f)$ is not a field since $gh = 0 \bmod f$ but neither g nor h is 0 mod f.
- We want to show that if f is irreducible over Z_p then $Z_p[x]/(f)$ is a field. For this we need to develop the notion of gcd's of polynomials.

Definition

If $f, g \in Z_p[x]$ then $f = \mathrm{gcd}(g, h)$ if f is monic (has lead coefficient 1), divides g and h and if any other f' divides g and h then f' divides f.

- Claim: $\mathrm{gcd}(g, h)$ exists and is unique.