Main theorem of finite fields

Theorem

- *Every finite field is isomorphic to* $Z_p[x]/(f)$ *for some irreducible polynomial* f*.*
- *Up to isomorphism, there is exactly one field of size* p^n *for every prime* p *and* $n > 0$*.*
- *If* F *is a finite field of size* p^n *then there is some* $a \in F$ *such that the order of* a *is* $p^n - 1$ *i.e. the least* m *such that* $a^m = 1$ *is* $p^n - 1$*.*
- *In fact, for a field* F *of size* p^n *there is are* $\phi(p^n - 1)$ *many* $a \in F$ *of order* $p^n - 1$*.*

Proofs of the main facts

- We proved in the last class that every finite field F of size p^n has an element of multiplicative order $p^n - 1$ and that every element of F satisfies the polynomial $x^{p^n} - x$.
- In fact, if F is a finite field, the order of any non-zero element divides $p^n - 1$.
- Last fact from last time: if F is a finite field of characteristic p then
$$K = \{a \in F : a^{p^n} = a\}$$
is a field.
- Unfortunately, although K is always a field, depending on F, it doesn't have to have p^n many elements.

Proofs of the main facts, cont'd

- To find the unicorn called "a finite field of size p^n" we need to learn a little something about fields in general.
- Claim: if F is a field and $f \in F[x]$ then there is a larger field K, $F \subseteq K$ such that f has a root in K.
- To see this, first we note that we may assume that f is irreducible over F. Then we let $K = F[x]/(f)$. x is the solution of f in K!
- It follows that if F is any field and $f \in F[x]$ then there is a field K, $F \subseteq K$, in which f factors into linear factors completely. That is, all roots of f are already in K. Moreover, if F is finite then K is finite as well.
- We are almost there: Start with $F = Z_p$ and let K be a field like the one above in which all solutions of $x^{p^n} - x$ occur. It would seem that this field must contain our long sought field of size p^n.

Proofs of the main facts, cont'd

- The only issue is whether $x^{p^n} - x$ has multiple roots. If it did then the set of realizations would not be of size p^n.
- First, notice that 0 is a root of $x^{p^n} - x$ of multiplicity 1. Now suppose that $c \in K$ is a non-zero root of $x^{p^n} - x$ and look at the following factorization which is obtained by long division:

$$x^{p^n} - x = x(x - c)\underbrace{\left(x^{p^n-2} + cx^{p^n-3} + c^2x^{p^n-4} + \ldots + c^{p^n-2}\right)}_{g(x)}.$$

- If c is a multiple root then it should be a root of $g(x)$ so we evaluate $g(c)$ which is $(p^n - 1)c^{p^n-2} = -c^{-1} \neq 0$.
- So K **is** a field of p^n many elements!

Proofs of the main facts, cont'd

- Finally, suppose that F is of size p^n and a is a multiplicative generator i.e. order of a is $p^n - 1$.
- Choose $f \in Z_p[x]$ of least degree such that $f(a) = 0$. Notice that f divides $x^{p^n-1} - 1$.
- In fact, if you think of the map sending $Z_p[x]$ to F by $g \mapsto g(a)$ then this map is onto and every element of F has the unique form $g(a)$ for some polynomial g of degree less than the degree of f.
- The conclusion then is that $deg(f) = n$ and F is isomorphic to $Z_p[x]/(f)$
- But every field of size p^n has a solution of f and is similarly isomorphic to $Z_p[x]$ so F is unique and of the form $Z_p[x]/(f)$.