Abstract II Spring 2010
Finite Fields-Section 33

Goal: Determine the structure of all finite fields. **Ultimate Goal:** Show that up to isomorphism there is exactly one finite field of order p^n, where p is a prime.

The Structure of a Finite Field

Fact to be proved below: All finite fields must have prime-power order.

Theorem 0.1. *Let E be a finite extension of degree n over a finite field F. If F has q elements, then E has q^n elements.*

Proof:

Corollary 0.2. *If E is a finite field of characteristic p, then E contains exactly p^n elements for some positive integer n.*

Proof:

Theorem 0.3. *Let E be a field of p^n elements contained in an algebraic closure $\bar{\mathbb{Z}}_p$ of $\mathbb{Z}_p$. The elements of E are precisely the zeros in $\mathbb{Z}_p$ of the polynomial $x^{p^n} - x$ in $\mathbb{Z}[x]$.*

Proof:

Definition 0.4. *An element α of a field is an nth root of unity if $\alpha^n = 1$. It is a primitive nth root of unity if $\alpha^n = 1$ and $\alpha^m \neq 1$ for $0 < m < n$.*

Theorem 0.5. *The multiplicative group $< F^*, \cdot >$ of nonzero elements of a finite field is cyclic.*

Corollary 0.6. *A finite extension E of a finite field F is a simple extension of F.*

Proof:

Examples: