AM 106/206: Applied Algebra **Prof. Salil Vadhan**

Lecture Notes 21

November 30, 2010

1 Finite Fields

- **Reading:** Gallian Ch. 22
- Recall (ps7): only possible sizes for finite fields are prime powers p^n.
- **Thm 22.1 (all the finite fields):** For every prime p and $n \in \mathbb{N}$,
  1. (Existence) There exists a finite field of order p^n, denoted $\mathbb{F}_{p^n}$ or $\mathrm{GF}(p^n)$ (for "Galois field").
  2. (Uniqueness) Every two finite fields of order p^n are isomorphic.

  Proof: Let F be splitting field of $f(x) = x^{p^n} - x$ over $\mathbb{Z}_p$, $F' =$ roots of $f(x)$ in F.
  - Claim 1: F' is a subfield of F (and hence $F' = F$ by def of splitting field).
  - Claim 2: the roots of $f(x)$ are all distinct in F.
  - Claim 3: every finite field of order p^n is a splitting field of $f(x)$.

- **Thm 22.2 (group structure):**
  1. The additive group of $\mathbb{F}_{p^n}$ is isomorphic to $\mathbb{Z}_p^n$.
  2. The multiplicative group $\mathbb{F}_{p^n}^*$ is cyclic. (A generator of the multiplicative group is called a *primitive element* of $\mathbb{F}_{p^n}$.)

  Proof:

1.

2.

- **Corollaries:**

  1. For every n, there is an element of $\mathbb{F}_{p^n}$ of degree n over $\mathbb{Z}_p$.
  2. For every n, there is an irreducible polynomial of degree n in $\mathbb{Z}_p[x]$.

  Proof:

  Thus, instead of constructing $\mathbb{F}_{p^n}$ as a splitting field by adjoining several roots, we can take a *single* irreducible polynomial $f(x)$ of degree n and $\mathbb{Z}_p[x]/\langle f(x)\rangle \cong \mathbb{F}_{p^n}$.

- **Examples:**

  1. $\mathbb{F}_{7^3} \cong \mathbb{Z}_7[x]/\langle x^3+2\rangle$.
  2. $\mathbb{F}_{7^3} \cong \mathbb{Z}_7[x]/\langle x^3+x^2+1\rangle$.
  3. Adding and multiplying x^2+5 and $3x+2$ in above representations of $\mathbb{F}_{7^3}$:

- **Computational Issues:**

  – Computations in the finite field $\mathbb{F}_{p^n}$ can be done efficiently given the prime p and an irreducible polynomial $f(x)$ over $\mathbb{Z}_p$ of degree n.
  Addition:

  Multiplication:

Inverses:

– How to find p and $f(x)$?
  1. Choose randomly and test for primality/irreducibility (which can be done in polynomial time). Primes and irreducible polynomials have noticeable density (PS10), so this doesn't take too many trials.
  2. Use a small value of p (e.g. $p = 2$) and known explicit irreducible polynomials, e.g. $f(x) = x^{2 \cdot 3^\ell} + x^{3^\ell} + 1$.