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

Lecture Notes 9

October 19, 2009

1 Orbits and Stabilizers

- Reading: Gallian Chapter 7
- Defs of $\text{stab}_G(s)$, $\text{orb}_G(s)$ for $G \leq Sym(S)$ and $s \in S$.
- Orbit-Stabilizer Theorem (Thm. 7.3)
  Proof:
  - For $\varphi, \psi \in G$, $\varphi(s) = \psi(s)$ iff $\varphi\text{stab}_G(s) = \psi\text{stab}_G(s)$.
  - Thus $|\text{orb}_G(s)| = [G : \text{stab}_G(s)]$.
- Example: Symmetries (a.k.a. automorphisms) of graph with edges $\{1,3\}$, $\{2,4\}$, $\{3,4\}$, $\{3,5\}$, $\{4,6\}$.

2 External Direct Products

- Reading: Gallian Ch. 8
- Definition. More common to write $G_1 \times G_2$ instead of Gallian's $G_1 \oplus G_2$.
- Examples:
  - $\mathbb{R}^n$
  - $\mathbb{C}$
  - $\mathbb{Z}_3 \times \mathbb{Z}_5$
  - $\mathbb{R}^*$
  - $\mathbb{C}^*$ vs. $\mathbb{R}^* \times \mathbb{R}^*$
  - $\mathbb{Z}_2^n$ vs. $\mathbb{Z}_{2^n}$

- Chinese Remainder Theorems: Let m, n be integers such that $\gcd(m, n) = 1$.
  1. The map $x \mapsto (x \bmod m, x \bmod n)$ is a bijection from $\mathbb{Z}_{mn}$ to $\mathbb{Z}_m \times \mathbb{Z}_n$. ("Numbers smaller than mn are uniquely determined by their residues modulo m and n.")
  2. $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.
  3. $\mathbb{Z}_{mn}^* \cong \mathbb{Z}_m^* \times \mathbb{Z}_n^*$.
- Proof:
  1. Inverse: $(y, z) \mapsto ay + bz \bmod mn$ for integers a, b such that $a \equiv 1 \bmod m$, $b \equiv 0 \bmod m$, $a \equiv 0 \bmod n$, $b \equiv 1 \bmod n$. How to find a, b?
  2. $((x + y) \bmod mn) \bmod m = (x + y) \bmod m = x \bmod m + y \bmod m$, and similarly $((x + y) \bmod mn) \bmod n = x \bmod n + y \bmod n$.
  3. Similar.
- Examples: $\mathbb{Z}_{15}$ and $\mathbb{Z}_{15}^*$.

- Can understand $\mathbb{Z}_N$ and $\mathbb{Z}_N^*$ well given the prime factorization of $N = p_1^{e_1} \cdots p_k^{e_k}$.
  - $\mathbb{Z}_N \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}$.
  - $\mathbb{Z}_N^* \cong \mathbb{Z}_{p_1^{e_1}}^* \times \cdots \times \mathbb{Z}_{p_k^{e_k}}^*$
  - Fact: For odd prime p, $\mathbb{Z}_{p^e}$ is always cyclic. $\mathbb{Z}_{2^e}$ is cyclic if $e = 1, 2$ and is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_{2^{e-2}}$ otherwise.
  - Example: $\mathbb{Z}_{56}^*$.
- But factorization seems difficult (no fast algorithms known)!
  - Many cryptographic algorithms (e.g. RSA) capitalize on the fact it seems difficult to take advantage of the structure of $\mathbb{Z}_N^*$ without knowing the factorization of N.
- Classification of Abelian Groups (Gallian Ch. 11): Every finite abelian group is an external direct product of cyclic groups.