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

Lecture Notes 11

October 18, 2010

1 Direct Products

- Reading: Gallian Ch. 8, 11.
- **Def:** For groups G_1, G_2, their *(external) direct product* is the group

$$G_1 \times G_2 = \{(g_1, g_2) : g_1 \in G_1, g_2 \in G_2\},$$

  under componentwise multiplication.

  - Gallian writes $G_1 \oplus G_2$ instead of $G_1 \times G_2$.
  - Generalizes naturally to define $G_1 \times G_2 \times \cdots G_n$.

- **Examples:**
  - $\mathbb{R}^n$
  - $\mathbb{C}$
  - $\mathbb{Z}_3 \times \mathbb{Z}_5$
  - $\mathbb{R}^*$
  - $\mathbb{Z}_2^n$ vs. $\mathbb{Z}_{2^n}$

2 Classifying Finite Abelian Groups

- **Theorem 11.1 (Classification of Finite Abelian Groups):** Every finite abelian group G is isomorphic to a product of cyclic groups of prime power order. That is,

$$G \cong \mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}},$$

  where $k \in \mathbb{N}$, $p_1, \ldots, p_k$ are primes (not necessarily distinct!), and $e_1, \ldots, e_k$ are positive integers.

Moreover, this factorization is unique up to the order of the factors. That is, if $\mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}} \cong \mathbb{Z}_{q_1^{f_1}} \times \cdots \times \mathbb{Z}_{q_\ell^{f_\ell}}$, then there is a bijection $\sigma : [k] \to [\ell]$ such that $p_i = q_{\sigma(i)}$ and $e_i = f_{\sigma(i)}$ for all i.

- **Example:** every finite abelian group of order 36 is isomorphic to exactly one of the following four groups:

- We won't have time to prove the classification theorem, but you can find the proof in Gallian (Ch. 11), and some AM206 students might want to cover it for the their essay. We will see, however, to obtain the factorization for the groups $\mathbb{Z}_n$ and $\mathbb{Z}_n^*$, using the following important theorem.

- **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. $((x + y) \bmod mn) \bmod m = (x + y) \bmod m = (x \bmod m + y \bmod m) \bmod m$, and similarly $((x + y) \bmod mn) \bmod n = (x \bmod n + y \bmod n) \bmod n$.
  3. Similar.

- **Examples:** $\mathbb{Z}_{15}$ and $\mathbb{Z}_{15}^*$.

- **Consequence:** Can decompose the groups $\mathbb{Z}_N$ and $\mathbb{Z}_N^*$ using the factorization of N. If $N = p_1^{e_1} \cdots p_k^{e_k}$, then

$$\begin{aligned} \mathbb{Z}_N &\cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}. \\ \mathbb{Z}_N^* &\cong \mathbb{Z}_{p_1^{e_1}}^* \times \cdots \times \mathbb{Z}_{p_k^{e_k}}^*. \end{aligned}$$

- Note that for the case of $G = \mathbb{Z}_N$, this immediately provides the factorization claimed in the Classification of Finite Abelian Groups.

  - **Example:** $\mathbb{Z}_{24} \cong$

  - **Q:** Why are we not done for $\mathbb{Z}_N^*$?

- For $\mathbb{Z}_N^*$, we need to use the following theorem (which you may assume without proof).

- **Theorem:**

  1. If p is an odd prime and e is a positive integer, then $\mathbb{Z}_{p^e}^*$ is cyclic of order $\phi(p^e) = (p-1) \cdot p^{e-1}$. That is, $\mathbb{Z}_{p^e}^* \cong \mathbb{Z}_{(p-1)\cdot p^{e-1}}$.
  2. $\mathbb{Z}_2^* \cong$
  3. $\mathbb{Z}_4^* \cong$
  4. For $e \geq 3$, $\mathbb{Z}_{2^e}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{e-2}}$.

- **Example:** $\mathbb{Z}_{72}^* \cong$

- **Message:** If we know the factorization of N, we can understand the group $\mathbb{Z}_N^*$ very well. But if we are given just N, factorization seems difficult in general (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.