Main topics relevant to the second exam.

Thursday, November 20, 2014
6:45 PM

**Elementary Arithmetic:**

- Division algorithm.
  
  \[ a \mathbb{Z} + b \mathbb{Z} = \text{gcd}(a,b) \mathbb{Z} \]

- \( a \mid bc \) and \( \text{gcd}(a,b)=1 \) \( \implies \) \( a \mid c \)

- Unique factorization and \( \nu_p \).

- Congruences and \( \mathbb{Z}_n \).

- Group of units \( \mathbb{Z}_n^\times \).

- Chinese Remainder Theorem

  \[ \mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n, \ [a]_{mn} \mapsto ([a]_m, [a]_n) \]

  is a well-defined bijection. It is also a homomorphism.

- Euler \( \varphi \) function:
  
  \[ \varphi(mn) = \varphi(m) \varphi(n) \quad \text{if} \quad \text{gcd}(m,n)=1. \]

  \[ \varphi(p^k) = p^k - p^{k-1}. \]

**Group theory:**

- Definition, uniqueness of the identity and inverse of an element.
• Subgroup criteria.
  • Group generated by a set.
  • Cyclic groups:

* Any subgroup of \( \mathbb{Z} \) is of the form \( d \mathbb{Z} \) where
  either \( d = 0 \) or \( d \) is the smallest positive
  number of this subgroup.

  In particular any subgroup of \( \mathbb{Z} \) is cyclic.

* Let \( G = \langle g \rangle \).
  • \( I_0 = \{ n \in \mathbb{Z} \mid g^n = e \} \) is a subgroup of \( \mathbb{Z} \).
  • If \( |G| < \infty \), then \( I_0 = |G| \mathbb{Z} \).

* Order \( o(g) \) of \( g \).

* Important properties of order:
  • \( \mathbb{Z}_{o(g)} \rightarrow \langle g \rangle , [m]_{o(g)} \mapsto g^m \) is well-defined
    bijection. It is also a homomorphism
  • \( o(g) = |\langle g \rangle| \).
  • \( g^n = g^m \iff n \equiv m \pmod{o(g)} \).
  • \( o(g^m) = \frac{o(g)}{\gcd(o(g),m)} \).
\[ ab = ba \quad \Rightarrow \quad o(ab) = o(a) \cdot o(b) \]
\[ \gcd(o(a), o(b)) = 1 \]

- A finite group \( G \) is cyclic

\[ \exists g \in G, \quad o(g) = |G| \]

- Group Actions.

- Orbits: TFAE
  1. \( x_1 \in O(x_2) \)
  2. \( O(x_1) \cap O(x_2) \neq \emptyset \)
  3. \( O(x_1) = O(x_2) \)

- \( G/X := \{ O(x) \mid x \in X \} \) is a partition.

- Lagrange Theorem

\[ |G| = |H| \cdot |G/H| \quad \text{if} \quad H \leq G \]

and \( G \) is a finite group.

- Index of \( H \) in \( G \) = \( [G : H] = \frac{|G|}{|H|} \).

- \( G \smallsetminus x, x \in X \Rightarrow \)

  1. \( G_x := \{ g \in G \mid g \cdot x = x_g \leq G \} \)

  2. \( G/G_x \rightarrow O(x) \)

\[ H \rightarrow G/H, \quad Hg \mapsto g^{-1}H \quad \text{is a well-defined bijection.} \]
\[ gG_x \mapsto g \cdot x \]

is a well-defined bijection.

3. \( |O(x)| = [G : G_x] \).

- How to understand the action of a finite cyclic group via Schreier cycles.

The vertices in each cycle give us an orbit of \( \langle g \rangle \). So their size divide \( o(g) \).

- \( H \triangleleft G \) left multiplication: orbits are called right cosets.
- \( G \triangleleft G \) by conjugation: orbits are called conjugacy classes.

- Symmetric Group:

  - Any permutation can be uniquely written as a product of disjoint cycles.
  - Any permutation is a product of transpositions.
- Even and odd permutation.

- \( \text{Sgn}: S_n \rightarrow \{\pm 1\} \) and \( A_n \)

- Two important equations:

\[
(a_1, a_2, \ldots, a_n)(a_n, a_{n+1}, \ldots, a_{n+k}) = (a_1, a_2, \ldots, a_n, a_{n+1}, \ldots, a_{n+k})
\]

and \( \tau \cdot (a_1, a_2, \ldots, a_n) \cdot \tau^{-1} = (\tau(a_1), \ldots, \tau(a_n)) \)

- \( o(C_1 \cdot C_2 \cdot \ldots \cdot C_n) = \text{lcm}(k_1, k_2, \ldots, k_n) \)

where \( C_i \) are disjoint \( k_i \)-cycles.