EE 720: An Introduction to Number Theory and Cryptography (Spring 2018)

Lecture 15 — March 9, 2018

Instructor: Saravanan Vijayakumaran *Scribe: Saravanan Vijayakumaran*

1 Lecture Plan

- Groups
- Subgroups

2 Groups

- Let G be a set. A binary operation $\circ$ on G is simply a function with domain $G \times G$.
- For $g, h \in G$, we write $g \circ h$ to represent $\circ(g, h)$.
- A *group* is a set G along with a binary operation which satisfies:
  - **Closure:** For all $g, h \in G$, $g \circ h \in G$.
  - **Existence of identity:** There exists an identity $e \in G$ such that for all $g \in G$, $e \circ g = g \circ e = g$.
  - **Existence of inverses:** For all $g \in G$ there exists an element $h \in G$ such that $g \circ h = h \circ g = e$. Such an h is called the inverse of g.
  - **Associativity:** For all $g_1, g_2, g_3 \in G$, $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$.
- If G has a finite number of elements, we say G is a finite group and use $|G|$ to denote the *order* of the group (the number of group elements).
- A group is *abelian* if for all $g, h \in G$, $g \circ h = h \circ g$.
- The identity in a group G is *unique*.
- Each element g in a group has a *unique* inverse.

3 Subgroups

- If G is a group, a set $H \subseteq G$ is a *subgroup* of G if H itself forms a group under the same operation associated with G.
- Example: Consider the subgroups of $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$.
- Every group G has the trivial subgroups G and $\{e\}$ where e is the identity of G.

- **Notation**: It is covenient to use *additive* or *multiplicative* notation to denote the group operation, i.e. $g+h$ or gh instead of $g \circ h$. This does not mean that the group operation is addition or multiplication of numbers.
- In additive notation, the inverse of g is denoted by $-g$. When we write $h-g$, we mean $h+(-g)$. In multiplicative notation, the inverse of g is denoted by g^{-1}.
- **Proposition:** A nonempty subset H of a group G is called a subgroup of G if
  (i) $g+h \in H$ for all $g, h \in H$.
  (ii) $-g \in H$ for all $g \in H$.
- **Lagrange's Theorem:** If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.
  - Example: Consider the subgroups of $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$ again.
  - **Definition:** Let H be a subgroup of a group G. For any $g \in G$, the set $H+g = \{h+g \mid h \in H\}$ is called a *right coset* of H.
  - **Example:** $H = \{0,3\}$ is a subgroup of $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$. It has right cosets
    $H+0=\{0,3\}\,,\quad H+1=\{1,4\}\,,\quad H+2=\{2,5\}\,,$
    $H+3=\{0,3\}\,,\quad H+4=\{1,4\}\,,\quad H+5=\{2,5\}\,.$
  - **Lemma:** Two right cosets of a subgroup are either equal or disjoint.
  - **Lemma:** If H is a finite subgroup, then all its right cosets have the same cardinality.
  - The proof of Lagrange's theorem follows from these two lemmas.

4 References and Additional Reading

- Section 8.1 from Katz/Lindell