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

Lecture 17 — March 16, 2018

Instructor: Saravanan Vijayakumaran *Scribe: Saravanan Vijayakumaran*

1 Lecture Plan

- Subgroups of Cyclic Groups
- Properties of $\mathbb{Z}_N^*$

2 Recap of Cyclic Groups

- **Definition:** A cyclic group is a finite group G such that there exists a $g \in G$ with $\langle g \rangle = G$. We say that g is a *generator of* G.
- **Proposition:** If G is a group of prime order p, then G is cyclic. Furthermore, all elements of G except the identity are generators of G.
- **Definition:** Groups G and H are isomorphic if there exists a bijection $\phi : G \to H$ such that

$$\phi(\alpha \star \beta) = \phi(\alpha) \otimes \phi(\beta)$$

  for all $\alpha, \beta \in G$. Here $\star$ is the binary operation in G and $\otimes$ is the binary operation in H.
- **Theorem:** Every cyclic group G of order n is isomorphic to $\mathbb{Z}_n$ with addition modulo n as the operation.
- **Corollary:** Every cyclic group is abelian.

3 Subgroups of Cyclic Groups

- **Theorem:** Every subgroup of a cyclic group is cyclic.
  - Example: $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ has subgroups $\{0\}$, $\{0, 3\}$, $\{0, 2, 4\}$, $\{0, 1, 2, 3, 4, 5\}$
  - Proof
    - ∗ If h is a generator of a cyclic group G of order n, then

$$G = \left\{h, h^2, h^3, \dots, h^n = 1\right\}$$

    - ∗ Every element in a subgroup S of G is of the form h^i where $1 \leq i \leq n$
    - ∗ Let h^m be the smallest power of h in S
    - ∗ Every element in S is a power of h^m

- **Theorem:** If G is a cyclic group of order n, then G has a unique subgroup of order d for every divisor d of n.
  - Proof
    * If $G = \langle h \rangle$ and d divides n, then $\langle h^{n/d} \rangle$ has order d
    * Every subgroup of G is of the form $\langle h^k \rangle$ where k divides n
    * If k divides n, $\langle h^k \rangle$ has order $\frac{n}{k}$
    * So if two subgroups have the same order d, then they are both equal to $\langle h^{n/d} \rangle$

- **Definition:** The *Euler phi function* $\phi(n)$ is defined on the positive integers as follows. We define $\phi(1) = 1$. For $n > 1$, the value of $\phi(n)$ is the number of integers in $\{1, 2, \ldots, n-1\}$ which are relatively prime to n, i.e. which satisfy $\gcd(i, n) = 1$.

- **Theorem:** A cyclic group of order n has $\phi(n)$ generators.
  - Examples
    * $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ has four generators $1, 2, 3, 4$
    * $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ has two generators $1, 5$
    * $\mathbb{Z}_{10} = \{0, 1, 2, \ldots, 9\}$ has four generators $1, 3, 7, 9$
  - Proof
    * Let $G = \langle g \rangle$.
    * If g^i is also a generator of G, then $(g^i)^n = e$ and $\left(g^i\right)^k \neq e$ for all positive integers $k < n$.
    * Since $g^n = e$, ik cannot be a multiple of n unless $k = n$. In other words, $\text{lcm}(i, n) = in$. This implies that $\gcd(i, n) = 1$.
    * We have shown that G has at least $\phi(n)$ generators.
    * Can it have more? No. We cannot have g^i as a generator with $\gcd(i, n) \neq 1$.

- **Theorem**: $n = \sum_{d:d|n} \phi(d)$

4 The Group $\mathbb{Z}_N^*$

- For any integer $N > 1$, we define $\mathbb{Z}_N^* = \{b \in \{1, 2, \ldots, N-1\} \mid \gcd(b, N) = 1\}$.

- **Theorem:** For $N > 1$, $\mathbb{Z}_N^*$ is a group under multiplication modulo N.

5 References and Additional Reading

- Section 8.3 from Katz/Lindell

- Section 7.3 of lecture notes of MIT's Principles of Digital Communication II, Spring 2005. `https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-451-principles-readings-and-lecture-notes/MIT6_451S05_FullLecNotes.pdf`

- Section 2.4 of *Topics in Algebra*, I. N. Herstein, 2nd edition

- Section 8.1.4 from Katz/Lindell