EE 720: An Introduction to Number Theory and Cryptography (Spring 2020)

Lecture 15 — March 12, 2020

Instructor: Saravanan Vijayakumaran *Scribe: Saravanan Vijayakumaran*

1 Lecture Plan

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

2 Cyclic Groups

- **Proposition:** Let G be a finite group. Assume multiplicative notation for the group operation. For $g \in G$, the set $\langle g \rangle = \{g, g^2, g^3, \dots\}$ is a subgroup of G.
- $\langle g \rangle$ is called the *subgroup generated by* g. If the order of the subgroup is i, then i is called the *order of* g.
- **Definition:** Let G be a finite group and $g \in G$. The *order of* g is the smallest positive integer k with $g^k = 1$ where 1 is the identity of G.
- **Proposition:** Let G be a finite group of order m and let $g \in G$ have order k. Then $k \mid m$.
- **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 $\psi : G \to H$ such that

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

  for all $\alpha, \beta \in G$. Here $\star$ is the binary operation in G and $\otimes$ is the binary operation in H.
- Example of group isomorphism
  - $\mathbb{Z}_2 = \{0, 1\}$ is a group under modulo 2 addition
  - $R = \{1, -1\}$ is a group under multiplication

$\mathbb{Z}_2$	R
$0 \oplus 0 = 0$	$1 \times 1 = 1$
$1 \oplus 0 = 1$	$-1 \times 1 = -1$
$0 \oplus 1 = 1$	$1 \times -1 = -1$
$1 \oplus 1 = 0$	$-1 \times -1 = 1$

3 Some Properties of Cyclic Groups

- **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.
- **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, $\mathrm{lcm}(i, n) = in$. This implies that $\gcd(i, n) = 1$.

4 References and Additional Reading

- Section 8.3.1 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