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

Lecture 18 — March 21, 2018

Instructor: Saravanan Vijayakumaran *Scribe: Saravanan Vijayakumaran*

1 Lecture Plan

- Properties of $\mathbb{Z}_N^*$
- Chinese Remainder Theorem

2 Recap

- **Theorem:** Every subgroup of a cyclic group is cyclic.
- **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.
- **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 $\{1, 2, \dots, n-1\}$ 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.
- **Theorem**: $n = \sum_{d:d|n} \phi(d)$

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

- For any integer $N > 1$, we define $\mathbb{Z}_N^* = \{b \in \{1, 2, \dots, N-1\} \mid \gcd(b, N) = 1\}$.
- **Theorem:** For $N > 1$, $\mathbb{Z}_N^*$ is a group under multiplication modulo N.
- **Fermat's little theorem:** If p is a prime and a is any integer not divisible by p, then $a^{p-1} = 1 \bmod p$.
- **Euler's theorem:** For any integer $N > 1$ and $a \in \mathbb{Z}_N^*$, we have $a^{\phi(N)} = 1 \bmod N$.
- For distinct primes p, q, we have $\phi(pq) = (p-1)(q-1)$.
- **Theorem:** $\mathbb{Z}_N^*$ is a cyclic group.

4 Chinese Remainder Theorem

- **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. If G and H are isomorphic, we write $G \simeq H$.

- Given groups G and H with group operations $\star$ and $\otimes$ respectively, we can define a new group $G \times H$as follows. The elements of $G \times H$ are ordered pairs (g, h) with $g \in G$ and $h \in H$. The group operation $\circ$ of $G \times H$ is defined as
$$(g, h) \circ (g', h') = (g \star g', h \otimes h').$$

- **Chinese Remainder Theorem:** Let $N = pq$ where p, q are integers greater than 1 which are relatively prime, i.e. $\gcd(p, q) = 1$. Then
$$\mathbb{Z}_N \simeq \mathbb{Z}_p \times \mathbb{Z}_q \text{ and } \mathbb{Z}_N^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_q^*.$$
Moreover, the function $f : \mathbb{Z}_N \mapsto \mathbb{Z}_p \times \mathbb{Z}_q$ defined by
$$f(x) = (x \bmod p, x \bmod q)$$
is an isomorphism from $\mathbb{Z}_N$ to $\mathbb{Z}_p \times \mathbb{Z}_q$, and the restriction of f to $\mathbb{Z}_N^*$ is an isomorphism from $\mathbb{Z}_N^*$ to $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$.

- Example: $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$. This group is isomorphic to $\mathbb{Z}_3^* \times \mathbb{Z}_5^*$.

- An extension of the Chinese remainder theorem says that if $p_1, p_2 \ldots, p_l$ are pairwise relatively prime (i.e., $\gcd(p_i, p_j) = 1$ for all $i \neq j$) and $N = \Pi_{i=1}^l p_i$, then
$$\mathbb{Z}_N \simeq \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_l} \text{ and } \mathbb{Z}_N^* \simeq \mathbb{Z}_{p_1}^* \times \mathbb{Z}_{p_2}^* \times \cdots \times \mathbb{Z}_{p_l}^*.$$

- Usage
  - Compute $14 \cdot 13 \bmod 15$
  - Compute $11^{53} \bmod 15$
  - Compute $18^{25} \bmod 35$

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
- Sections 8.1.4, 8.1.5 from Katz/Lindell