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

Lecture 16 — March 21, 2020

*Instructor: Saravanan Vijayakumaran* *Scribe: Saravanan Vijayakumaran*

# 1 Lecture Plan

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

# 2 The Group $\mathbb{Z}_N^*$

- For any integer $N > 1$, we define $\mathbb{Z}_N^* = \{b \in \{1, 2, \ldots, N-1\} \mid \gcd(b, N) = 1\}$.
- By the definition of the Euler phi function, the cardinality or order of $\mathbb{Z}_N^*$ is $\phi(N)$.
- **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 an integer $e \geq 1$ and prime $p$, $\phi(p^e) = p^e \left(1 - \frac{1}{p}\right)$.
- For distinct primes $p, q$, we have $\phi(pq) = (p-1)(q-1)$.
- For positive integers $m, n$ such that $\gcd(m, n) = 1$, we have $\phi(mn) = \phi(m)\phi(n)$.
  - Proof will follow from the Chinese Remainder Theorem
- **Theorem:** If $N$ is a prime, $\mathbb{Z}_N^*$ is a cyclic group.
  - Proof does not follow from Lagrange's theorem as $\phi(N)$ is composite.
  - Since proof requires results which we have not discussed, we will omit it.

# 3 Chinese Remainder Theorem

- **Definition:** Groups $G$ and $H$ are isomorphic if there exists a bijection $\phi : G \to H$ 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 $H$. 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

$$f(x) = (x \text{ mod } p, x \text{ mod } q)$$

  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 $\mathbb{Z}_3^* \times \mathbb{Z}_5^*$.

## 4 References and Additional Reading

- Sections 8.1.4, 8.1.5 from Katz/Lindell