EE 720: An Introduction to Number Theory and Cryptography (Spring 2019)

Lecture 17 — March 14, 2019

Instructor: Saravanan Vijayakumaran *Scribe: Saravanan Vijayakumaran*

1 Lecture Plan

- Some more results on cyclic groups
- Properties of $\mathbb{Z}_N^*$
- Chinese Remainder Theorem

2 Recap

- **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.
- **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.

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

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

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

5 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 $18^{25} \bmod 35$

- How to go from $(x_p, x_q) = (x \bmod p, x \bmod q)$ to $x \bmod N$ where $\gcd(p, q) = 1$?
  - Compute X, Y such that $Xp + Yq = 1$.
  - Set $1_p := Yq \bmod N$ and $1_q := Xp \bmod N$.
  - Compute $x := x_p \cdot 1_p + x_q \cdot 1_q \bmod N$.

- Example: $p = 5, q = 7$ and $N = 35$. What does $(4, 3)$ correspond to?

- Let $m_1, m_2, \ldots, m_l$ be pairwise relatively prime positive integers. Then the unique solution modulo $M = m_1 m_2 \cdots m_l$ of the system of congruences

$$\begin{aligned} x &= a_1 \bmod m_1 \\ x &= a_2 \bmod m_2 \\ &\vdots \\ x &= a_l \bmod m_l \end{aligned}$$

  is given by

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_l M_l y_l$$

  where $M_i = \frac{M}{m_i}$ and $M_i y_i = 1 \bmod m_i$.

- Example: Solve for x modulo 105 which satisfied the following congruences.

$$\begin{aligned} x &= 1 \bmod 3 \\ x &= 2 \bmod 5 \\ x &= 3 \bmod 7 \end{aligned}$$

6 References and Additional Reading

- Section 8.3.1 from Katz/Lindell
- Sections 8.1.4, 8.1.5 from Katz/Lindell