Discrete Mathematics
Lecture 3

Liangfeng Zhang
School of Information Science and Technology
ShanghaiTech University

$\mathbb{Z}_n^*$

DEFINITION: Let $n \in \mathbb{Z}^+$ and $[b]_n \in \mathbb{Z}_n$. $[s]_n \in \mathbb{Z}_n$ is called an **inverse** of $[b]_n$ if $[b]_n[s]_n = [1]_n$.

- **division**: If $[b]_n\,[s]_n = [1]_n$, define $\frac{[a]_n}{[b]_n} = [a]_n \cdot [s]_n$

THEOREM: Let $n \in \mathbb{Z}^+$. $[b]_n \in \mathbb{Z}_n$ has an inverse iff $\gcd(b, n) = 1$

- Only if: $\exists\ s$ s.t. $[b]_n[s]_n \equiv [1]_n$; $\exists\ t, bs - 1 = nt$; $\gcd(b, n) = 1$
- If: $\exists\ s, t$ s.t. $bs + nt = 1$; $bs \equiv 1 \pmod{n}$

DEFINITION: Let $n \in \mathbb{Z}^+$. Define $\mathbb{Z}_n^* = \{[b]_n \in \mathbb{Z}_n\colon\ \gcd(b, n) = 1\}$

- If n is prime, then $\mathbb{Z}_n^* = \{1,2, \dots, n - 1\}$
- If n is composite, then $\mathbb{Z}_n^* \subset \mathbb{Z}_n$

EXAMPLE: $\mathbb{Z}_5^* = \{1,2,3,4\}$; $\mathbb{Z}_6^* = \{1,5\}$; $\mathbb{Z}_8^* = \{1,3,5,7\}$

Euler's Phi Function

QUESTION: How many elements are there in $\mathbb{Z}_n^*$?

- $|\mathbb{Z}_n^*|$ is the number of integers $b \in [n]$ ($[n] = \{1,2,\dots,n\}$) s.t. $\gcd(b,n) = 1$

DEFINITION: (Euler's Phi Function) $\phi(n) = |\mathbb{Z}_n^*|, \forall n \in \mathbb{Z}^+$.

- $\phi(n)$ is the number of integers $b \in [n]$ such that $\gcd(b,n) = 1$
- Gauss chose the symbol ϕ for Euler's Phi function

THEOREM: Let p be a prime. Then $\forall e \in \mathbb{Z}^+, \phi(p^e) = p^{e-1}(p-1)$.

- Let $x \in \{1,2,\dots,p^e\}$.
- $\gcd(x,p^e) \neq 1$ iff $p|x$

  iff $x = p, 2p, \dots, p^{e-1} \cdot p$

  - $\phi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$

EXAMPLE: $\phi(3^2) = 3(3-1) = 6$

- $\mathbb{Z}_9^* = \{1,2,\cancel{3},4,5,\cancel{6},7,8,\cancel{9}\}$

EXAMPLE: $\phi(p) = p - 1$

- $\mathbb{Z}_p^* = \{1,2,\dots,p-1\}$

Euler's Phi Function

QUESTION: Formula of $\phi(n)$ for general integer n?

THEOREM: If $n = p_1^{e_1} \cdots p_r^{e_r}$ for distinct primes $p_1, \dots, p_r$ and integers $e_1, \dots, e_r \geq 1$, then $\phi(n) = \phi\left(p_1^{e_1}\right) \cdots \phi\left(p_r^{e_r}\right)$.

Hence, $\phi(n) = n(1 - p_1^{-1}) \cdots (1 - p_r^{-1})$.

- There are many proofs. We will see in the future.
  - Principle of inclusion-exclusion; Chinese remainder theorem

COROLLARY: If $n = pq$ for two different primes p and q, then $\phi(n) = (p-1)(q-1)$.

EXAMPLE: $\phi(10) = (2-1)(5-1) = 4; n = 10; p = 2, q = 5$

- $\mathbb{Z}_{10}^* = \{1, \cancel{2}, 3, \cancel{4}, \cancel{5}, \cancel{6}, 7, \cancel{8}, 9, \cancel{10}\}$

Euler's Theorem

THEOREM (Euler, 1760) Let $n \geq 1$ and $\alpha \in \mathbb{Z}_n^*$. Then $\alpha^{\phi(n)} = 1$.

- $\alpha^{\phi(n)}, 1$ are both residue classes modulo n
- Suppose that $\alpha = [a]_n$ for $a \in \mathbb{Z}$. Then $\alpha^{\phi(n)} = 1$ is $([a]_n)^{\phi(n)} = [1]_n$
- How to prove?
  - Consider the map $f\colon \mathbb{Z}_n^* \to \mathbb{Z}_n^* \quad [x]_n \mapsto [a]_n \cdot [x]_n$
  - We show that f is injective
    - $f([x]_n) = f([y]_n)$
    - $[a]_n \cdot [x]_n = [a]_n \cdot [y]_n$
    - $[ax]_n = [ay]_n$
    - $n|a(x-y)$
    - $n|(x-y)$, this is because $\gcd(n,a) = 1$
      - $[x]_n = [y]_n$

Euler's Theorem

THEOREM (Euler, 1760) Let $n \geq 1$ and $\alpha \in \mathbb{Z}_n^*$. Then $\alpha^{\phi(n)} = 1$.

- $\alpha^{\phi(n)}, 1$ are both residue classes modulo n
- Suppose that $\alpha = [a]_n$ for $a \in \mathbb{Z}$. Then $\alpha^{\phi(n)} = 1$ is $([a]_n)^{\phi(n)} = [1]_n$
- How to prove?
    - Consider the map $f: \mathbb{Z}_n^* \to \mathbb{Z}_n^* \quad [x]_n \mapsto [a]_n \cdot [x]_n$
    - Suppose that $\mathbb{Z}_n^* = \left\{[x_1]_n, \ldots, \left[x_{\phi(n)}\right]_n\right\}$.
        - $f([x_1]_n) \cdots f\left(\left[x_{\phi(n)}\right]_n\right) = [x_1]_n \cdots \left[x_{\phi(n)}\right]_n$
        - $[ax_1]_n \cdots \left[ax_{\phi(n)}\right]_n = [x_1]_n \cdots \left[x_{\phi(n)}\right]_n$
        - $\left[a^{\phi(n)} x_1 \cdots x_{\phi(n)}\right]_n = \left[x_1 \cdots x_{\phi(n)}\right]_n$
            - $n \mid (a^{\phi(n)} - 1) x_1 \cdots x_{\phi(n)}$
                - $n \mid (a^{\phi(n)} - 1)$, this is because $\gcd\left(n, x_1 \cdots x_{\phi(n)}\right) = 1$
                    - $\left[a^{\phi(n)}\right]_n = [1]_n$, i. e., $([a]_n)^{\phi(n)} = [1]_n$

Fermat's Little Theorem

EXAMPLE: Understand Euler's theorem with $\mathbb{Z}_{10}^* = \{1,3,7,9\}$.

- $n = 10, \phi(n) = 4,$
- $1^4 \equiv 1 \pmod{10} \Rightarrow ([1]_{10})^4 = [1]_{10}$
- $3^4 = 81 \equiv 1 \pmod{10} \Rightarrow ([3]_{10})^4 = [1]_{10}$
- $7^4 = 2401 \equiv 1 \pmod{10} \Rightarrow ([7]_{10})^4 = [1]_{10}$
- $9^4 = 6561 \equiv 1 \pmod{10} \Rightarrow ([9]_{10})^4 = [1]_{10}$
  - Consider the map $f\colon \mathbb{Z}_{10}^* \to \mathbb{Z}_{10}^* \quad [x]_n \mapsto [9]_n \cdot [x]_n$
  - $f([1]_{10}) = [9]_{10} \cdot [1]_{10} = [9]_{10}; f([3]_{10}) = [7]_{10}; f([7]_{10}) = [3]_{10}, f([9]_{10}) = [1]_{10}$
  - f is injective
  - $f([1]_{10})f([3]_{10})f([7]_{10})f([9]_{10}) = [9]_{10}[7]_{10}[3]_{10}[1]_{10}$

Fermat's Little Theorem (Euler, 1736) If p is a prime and $\alpha \in \mathbb{Z}_p$. Then $\alpha^p = \alpha$.

- This is a corollary of Euler's theorem for $n = p$
- By Euler's theorem, $\alpha^{p-1} = 1$ $(\forall \alpha \neq [0]_p)$
  - $\alpha^p = \alpha$