Discrete Mathematics 2025 Spring

同济经管
TONGJI SEM

魏可佶 kejiwei@tongji.edu.cn

CAMEA 中国高质量MBA教育认证 AACSB ACCREDITED EQUIS ACCREDITED

- Fermat's Little Theorem
- Euler's Totient Function
- Euler's Theorem

- **Theorem 8.15 (Fermat's Little Theorem):**
  Let p be a prime number and a an integer such that **a** and p are coprime. Then: $a^{p-1} \equiv 1 \pmod{p}$.

- **Note:**
  - Furthermore, for any integer a, it holds that $a^p \equiv a \pmod{p}$.
  - P **is** prime ,a **and** p **coprime, then** a^{p-1} **- 1** is divisible by p.
  - $a^{p-1} \equiv 1 \pmod{p}$ is also $a * a^{p-2} \equiv 1 \pmod{p}$, $a^{p-2} \bmod p$ is the modular inverse of a.

- **Applications of Fermat's Little Theorem:**
  - *Solving congruences* $ax \equiv b \pmod{p}$, When p is a prime, the theorem helps simplify the computation of powers modulo p.
  - *Primality testing*: While not absolutely reliable, Fermat's Little Theorem is effective in many cases for checking whether a number is prime.
  - *Proving a number is composite*:
    If the theorem fails for a particular base a, it can be used to confirm that a number is not prime.
  - *To test whether a number p is prime*: If there exists any integer a ($1<a<p$ and a is coprime to p) such that $a^{p-1} \bmod p \neq 1$, then p can be definitively identified as a **composite number**.
- **Example:** $2^{9-1} \equiv 4 \pmod{9}$, so we can conclude that 9 is composite.

- *Euler's Totient Function* $\phi(n)$: It is the number of integers in the set $\{0,1,\ldots,n-1\}$ that are coprime to n.
- *Properties of* $\phi(n)$: If n is a prime number, then $\phi(n)=n-1$. If n is a composite number, then $\phi(n)<n-1$.
- *Formula for computing* $\phi(n)$: If the prime factorization of n is $n = p_1^{k1} \cdot p_2^{k2} \cdots \cdot p_r^{kr}$, where $p_1,p_2,\ldots,p_r$ are distinct prime numbers,

  then $\phi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \cdots \cdot \left(1 - \frac{1}{p_r}\right)$
- **Example 1:** *Direct Counting Method* to Find $\phi(4)$.

  $\{0, 1,\ldots, 3\}$, only 1 and 3 are coprime to 4, $\phi(4)=2$.
- **Example 2:** *Prime Factorization Method* to Find $\phi(12)$.

  The prime factorization of 12 is $2^2 \times 3$, $p_1=2$ *and* $p_2=3$,

  Therefore: $\phi(12) = 12 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 4$.

- **Theorem 8.16 (Euler's Theorem):**

  If a is coprime to n, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

- **Note:**
  - Since $\phi(n)$ when n is a prime, Euler's Theorem becomes **Fermat's Little Theorem** in that case.
  - Thus, **Euler's Theorem is a generalization of Fermat's Little Theorem**, and it can be applied to any positive integer n.
  - When n is a composite number, **Euler's Theorem provides a way to find the modular inverse of a modulo n**, because $a^{\phi(n)-1} \equiv a^{-1} \pmod{n}$.

Objective :

Key Concepts :