

CS355: Cryptography

Lecture 16: Fermat and Euler's Theorems.

The Euler Phi Function

Definition

Given an integer n , $\phi(n)$ is the number of all numbers a such that $0 < a < n$ and a is relatively prime to n (i.e., $\gcd(a, n) = 1$).

Theorem:

If $\gcd(m, n) = 1$, $\phi(mn) = \phi(m) \phi(n)$

The Euler Phi Function

Theorem: Formula for $\phi(n)$

Let p be prime, e, m, n be positive integers

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

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

3) If $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ then

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

Fermat's Little Theorem

Fermat's Little Theorem

If p is a prime number and a is a natural number that is not a multiple of p , then

$$a^{p-1} \equiv 1 \pmod{p}$$

Proof idea:

- $\gcd(a, p) = 1$, then the set $\{i \cdot a \pmod{p} \mid 0 < i < p\}$ is a permutation of the set $\{1, \dots, p-1\}$.
 - otherwise we have $0 < n < m < p$ s.t. $ma \pmod{p} = na \pmod{p}$, and thus $p \mid (ma - na) \implies p \mid (m-n)$, where $0 < m-n < p$
- $a \prod_{i=1}^{p-1} i = (p-1)! \equiv \prod_{i=1}^{p-1} (i \cdot a) \pmod{p}$
Since $\gcd((p-1)!, p) = 1$, we obtain $a^{p-1} \equiv 1 \pmod{p}$

Euler's Theorem

Euler's Theorem

Given integer $n > 1$, such that $\gcd(a, n) = 1$ then
$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Corollary

Given integer $n > 1$, such that $\gcd(a, n) = 1$ then
 $a^{\phi(n)-1} \pmod{n}$ is a multiplicative inverse of $a \pmod{n}$.

Corollary

Given integer $n > 1$, x , y , and a positive integers with
 $\gcd(a, n) = 1$. If $x \equiv y \pmod{\phi(n)}$, then
$$a^x \equiv a^y \pmod{n}.$$

Consequence of Euler's Theorem

Principle of Modular Exponentiation

Given a, n, x, y with $n \geq 1$ and $\gcd(a, n) = 1$, if $x \equiv y \pmod{\phi(n)}$, then

$$a^x \equiv a^y \pmod{n}$$

Proof idea:

$$a^x = a^{k\phi(n) + y} = a^y (a^{\phi(n)})^k$$

by applying Euler's theorem we obtain

$$a^x \equiv a^y \pmod{n}$$

Residue Classes

- Given positive integer n , congruence modulo n is an equivalence relation.
- This relation partition all integers into equivalent classes; we denote the equivalence class containing the number x to be $[x]_n$, or $[x]$ when n is clear from the context
- These classes are called residue classes modulo n

Modular Arithmetic in \mathbf{Z}_n

- Define \mathbf{Z}_n as the set of residue classes modulo n
 - $\mathbf{Z}_7 = \{[0], [1], [2], \dots, [6]\}$
- Define two binary operators $+$ and \square on \mathbf{Z}_n
- Given $[x], [y]$ in \mathbf{Z}_n ,
 $[x] + [y] = [x+y]$,
 $[x] \square [y] = [xy]$
- E.g., in \mathbf{Z}_7 : $[3]+[4] = [0]$, $[0]+[2] = [2]+[0] = [2]$,
 $[5]+[6] = [4]$
- Compute the table for \mathbf{Z}_4

Properties of Modular Addition and Multiplication

Let n be a positive integer and \mathbf{Z}_n be the set of residue classes modulo n . For all $a, b, c \in \mathbf{Z}_n$

1. $a + b = b + a$ addition is commutative
2. $(a+b)+c = a+(b+c)$ addition is associative
3. $a + [0] = a$ exists addition identity
4. $[x] + [-x] = [0]$ exists additive inverse
5. $a \cdot b = b \cdot a$ multiplication is commutative
6. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ multiplication is associative
7. $a \cdot (b+c) = a \cdot b + a \cdot c$ mult. distributive over add.
8. $a \cdot [1] = a$ exists multiplicative identity

Multiplicative Inverse

- Theorem: $[x]_n$ has a multiplicative inverse if and only if $\gcd(x, n) = 1$
- We use \mathbf{Z}_n^* to denote the set of all residue classes that have a multiplicative inverse.
- \mathbf{Z}_n^* is closed under multiplication.

Primitive roots

Definition: When p is a prime, a primitive root mod p is a residue whose powers yield every nonzero residue class mod p .

Example: Consider powers of 3 (mod 7)

$$3^1 \equiv 3, 3^2 \equiv 2, 3^3 \equiv 6, 3^4 \equiv 4, 3^5 \equiv 5, 3^6 \equiv 1$$

There are $\phi(p-1)$ primitive roots mod p .