# Introduction to Cryptography
# CS 355

## Lecture 11

## Fermat & Euler Theorems

# 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
- E.g., $[1]_7=[8]_7=\{\ldots, -13,-6,1,8,15,22,\ldots\}$

# Modular Arithmetic in $\mathbf{Z}_n$

- Define $\mathbf{Z}_n$ as the set of residue classes modulo n
  - $\mathbf{Z}_7 = \{[0], [1], [2], \ldots, [6]\}$
- Define two binary operators + and $\times$ on $\mathbf{Z}_n$
- Given [x], [y] in $\mathbf{Z}_n$,
  $$[x] + [y] = [x+y],$$
  $$[x] \times [y] = [xy]$$
- 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. | $a \times b = b \times a$ | multiplication is commutative |
| 6. | $(a\times b)\times c = a\times(b\times c)$ | multiplication is associative |
| 7. | $a\times(b+c) = a\times b+ a\times c$ | mult. distributive over add. |
| 8. | $a\times[1] = [a]$ | 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.

# The Euler Phi Function

**Definition**

Given an integer n, $\Phi(n) = |Z_n^*|$ 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 $n = p_1^{e_1} p_2^{e2} \ldots p_k^{ek}$ then

$$\Phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_k})$$

# Fermat's Little Theorem

**Fermat's Little Theorem**

If *p* is a prime number and *a* i s 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*a mod p} 0< i < p is a permutation of the set {1, …, p-1}.(otherwise we have 0<n<m<p s.t. ma mod p = na mod p

p| (ma - na) ⇒ p | (m-n), where 0<m-n < p )

$a * 2a * \ldots *(p-1)a = (p-1)!\, a^{p-1} \equiv (p-1)! \pmod{p}$

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 $a^{\Phi(n)-1}$ mod n is a multiplicative inverse of a mod 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

**Basic Principle**

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

$a^e \equiv a^f \pmod{p}$

# Coming Attractions …

- The RC4 Stream Cipher

- Recommended reading for next lecture:
  - None