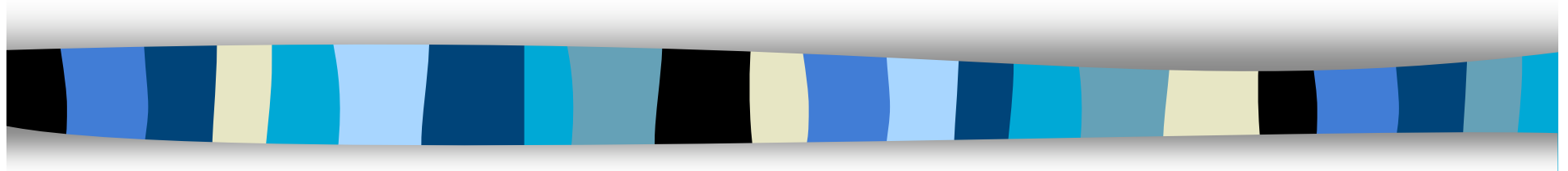


Introduction to Cryptography

CS 355



Congruence, Euler Phi function, Fermat
and Euler's Theorems

Congruence Relation

Definition: Let a, b, n be integers with $n > 0$, we say that a and b are congruent modulo n , denoted by $a \equiv b \pmod{n}$, if and only if $n \mid (a - b)$

Properties: $a \equiv b \pmod{n}$
if and only if $n \mid (a - b)$
if and only if $n \mid (b - a)$
if and only if $a = b + k \cdot n$ for some integer k
if and only if $b = a + k \cdot n$ for some integer k

E.g., $32 \equiv 7 \pmod{5}$, because $5 \mid (32 - 7) = 25$
 $-12 \equiv 37 \pmod{7}$, because $7 \mid (-12 - 37) = -49$
 $17 \equiv 17 \pmod{13}$, because $13 \mid (17 - 17) = 0$

Properties of the Congruence Relation

Proposition: Let a, b, c, n be integers with $n > 0$

1. $a \equiv a \pmod{n}$
2. $a \equiv b \pmod{n}$ if and only if $b \equiv a \pmod{n}$
3. if $a \equiv b$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$

Corollary: Congruence modulo n is an equivalence relation.

Every integer is congruent to exactly one number in $\{0, 1, 2, \dots, n-1\}$ modulo n

More Properties of the Congruence Relation

Proposition: Let a, b, c, n be integers with $n > 0$

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then:

$$a + c \equiv b + d \pmod{n},$$

$$a - c \equiv b - d \pmod{n},$$

$$a \cdot c \equiv b \cdot d \pmod{n}$$

E.g., $5 \equiv 12 \pmod{7}$ and $3 \equiv -4 \pmod{7}$, then,

$$5 + 3 \equiv 12 + (-4) \pmod{7}$$

$$5 \cdot 3 \equiv 12 \cdot (-4) \pmod{7}$$

Multiplicative Inverse

Definition: Given integers $n > 0$, a , b , we say that b is a **multiplicative inverse of a modulo n** if $ab \equiv 1 \pmod{n}$.

Proposition: Given integers $n > 0$ and a , then a has a multiplicative inverse modulo n if and only if a and n are relatively prime.

Solving Linear Congruences

Theorem:

- Let a, n, z, z' be integers with $n > 0$. If $\gcd(a, n) = 1$, then $az \equiv az' \pmod{n}$ if and only if $z \equiv z' \pmod{n}$.
- More generally, if $d := \gcd(a, n)$, then $az \equiv az' \pmod{n}$ if and only if $z \equiv z' \pmod{n/d}$.

Example:

- $5 \cdot 2 \equiv 5 \cdot -4 \pmod{6}$
- $3 \cdot 5 \equiv 3 \cdot 3 \pmod{6}$

Examples

Example 1:

- Observe that $3 \cdot 5 \equiv 1 \pmod{7}$.
- Let us try to solve $3 \cdot x + 4 \equiv 3 \pmod{7}$.
- Subtract 4 from both side, $3 \cdot x \equiv -1 \pmod{7}$.
- We know that $-1 \equiv 6 \pmod{7}$.
- Thus $3 \cdot x \equiv 6 \pmod{7}$.
- Multiply both side by 5, $3 \cdot 5 \cdot x \equiv 5 \cdot 6 \pmod{7}$.
- Thus, $x \equiv 1 \cdot x \equiv 3 \cdot 5 \cdot x \equiv 5 \cdot 6 \equiv 30 \equiv 2 \pmod{7}$.
- Thus, any x that satisfies $3 \cdot x + 4 \equiv 3 \pmod{7}$ must satisfy $x \equiv 2 \pmod{7}$ and vice versa.

Question: To solve that $2x \equiv 2 \pmod{4}$.
Is the solution $x \equiv 1 \pmod{4}$?

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:

$$\gcd(m, n) = 1, \Phi(mn) = \Phi(m) \Phi(n)$$

If

Proof using the Chinese Remainder Theorem.

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

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