Introduction to Cryptography CS 355

Lecture 8

Congruence Revisited

Announcements & Activities

- Homework 1 due on Wednesday September 14
- Join the class mailing list CS355_Fall2005@cs.purdue.edu
- Index of coincidence
- Demo Vigenère cipher
- Mathematical terminologies

Congruence Relation

Definition: Let a, b, n be integers with n>0, we say that $a \equiv b \pmod{n}$,

if a – b is a multiple of n.

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., $32 \equiv 7 \pmod{5}$, $-12 \equiv 37 \pmod{7}$,

$17 \equiv 17 \pmod{13}$

Properties of the Congruence Relation

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

1. $a \equiv 0 \pmod{n}$ if and only if $n \mid a$
2. $a \equiv a \pmod{n}$
3. $a \equiv b \pmod{n}$ if and only if $b \equiv a \pmod{n}$
4. 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 $\{0, 1, 2, \ldots, n-1\}$

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, …

Examples

Example 1:

- Observe that $3 \cdot 5 \equiv 1 \pmod 7$.
- Let us try to solve $3 \cdot x + 4 \equiv 3 \pmod 7$.
- Subtracts 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 $x \equiv 1 \pmod 4$?

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 if 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:

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

Coming Attractions …

- One-time Pad, Pseudo Random Number Generator
- Recommended reading for next lecture:
  - Trappe & Washington: 2.9, 2.10