Network and Information Security
Lecture 5

B.Tech. Computer Engineering
Sem. VI.

M. T. Mehta
Associate Professor
Computer Engineering Department
Faculty of Technology,
Dharmsinh Desai University, Nadiad

Examples : Modular Arithmetic

Example 1

Perform the following operations (inputs come from Z_n)

a. Add 7 to 14 in Z_{15}

b. Subtract 11 from 7 in Z_{13}

c. Multiply 11 by 7 in Z_{20}

Example 2

Perform the following operations (inputs come from Z or Z_n)

a. Add 17 to 27 in Z_{14}

b. Subtract 43 from 12 in Z_{13}

c. Multiply 123 by -10 in Z_{19}

Additive Inverse

- In Zn, two numbers a and b are additive inverse of each other if
- $a + b \equiv 0 \pmod{n}$

- In Zn, additive inverse of a can be calculated as $b = n - a$
- Additive inverse of 4 in Z_{10} is 6
- The sum of an integer and its additive inverse is congruent to 0 modulo n.

- Example Find all additive inverse pairs in Z_{10}.

(0,0)

(1,9)

(2,8)

(3,7)

(4,6)

(5,5)

Multiplicative Inverse

- In Zn, two numbers a and b are the multiplicative inverse of each other if
- a x b ≡ 1 (mod n)
- The multiplicative inverse of 3 is 7, if the modulus is 10.
- 3 x 7 mod 10 = 1
- In modular arithmetic, an integer may or may not have a multiplicative inverse. When it does the product of the integer and its multiplicative integer is congruent to 1 modulo n.

Example

(a) Find the multiplicative inverse of 8 in Z_{10}.

(b) Find all multiplicative inverses in Z_{10}.

(c) Find all multiplicative inverse pairs in Z_{11}.

(b) (1,1), (3,7), (9,9)

(c) (1,1), (2,6), (3,4), (5,9), (7,8), (9,9), (10,10)

- The integer a in Z_n has a multiplicative inverse if and only if gcd (n,a) ≡ 1 (mod n)

Numbers a and b are called relatively prime or co-prime if gcd(a,b)=1

We know that according to extended Euclidean algorithm,

a x s + b x t = gcd (a,b)

Let us put n in place of a, a in place of b

n x s + a x t = gcd (n,a)

$(n \times s + a \times t) \bmod n = [\gcd(n,a)] \bmod n$

$[(n \times s) \bmod n + (a \times t) \bmod n] \bmod n = [\gcd(n,a)] \bmod n$

$[0 + (a \times t) \bmod n] \bmod n = 1 \bmod n = 1$

$(axt) \bmod n = 1$

The numbers a and t are multiplicative inverse of each other.

$a^{-1} \bmod n = t$, $t^{-1} \bmod n = a$

If a and n are co-prime then it is possible to find $a^{-1} \bmod n$ (multiplicative inverse of a with respect to n) using extended euclidean algorithm.

Example

Find the multiplicative inverse of 11 in Z_{26}.

Find the multiplicative inverse of 23 in Z_{100}.

Find the inverse of 12 in Z_{26}.

Apply extended Euclidian algorithm

Multiplicative inverse of 23 in Z_{100}

q	r1	r2	r	t1	t2	t
4	100	23	8	0	1	-4
2	23	8	7	1	-4	19
1	8	7	1	-4	9	-13
7	7	1	0	9	-13	100
	1	0		-13		

-13 mod 100
=87

23 and 87 are multiplicative inverse.

(23 x 87) mod 100 = 2001 mod 100 = 1

- Find the inverse of 12 in Z_{26}.

q	r1	r2	r	t1	t2	t
2	26	12	2	0	1	-2
6	12	2	0	1	-2	13
	2	0		-2	13	

gcd (26,12) is 2 ≠ 1.
Hence, multiplicative inverse of 12 in Z_{26} is not possible.