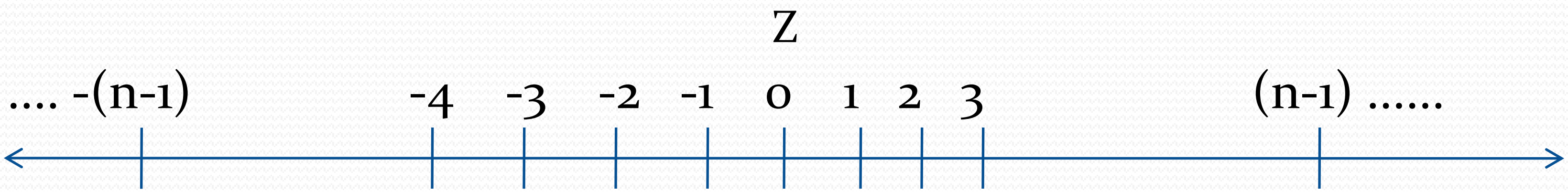
# Network and Information Security
# Lecture 4

B.Tech. Computer Engineering
Sem. VI.

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

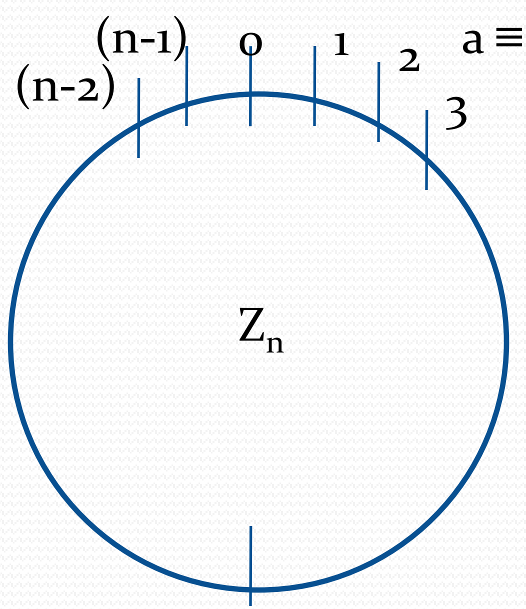
# Mathematical Notations

- The distribution of integers in Z




- $Z_n = \{ 0,1,2,\ldots\ldots,(n-1)\}$

The integers 0 to (n-1) are spaced evenly around a Circle.




$a \equiv 2 \pmod{n}$

All congruent integers modulo n occupy the same point on the circle.

- The result of modulo operation with modulus n is always an integer between 0 and (n-1).
- a mod n is always less than n and non-negative integer.
- $Z_n = \{ 0,1,2,......,(n-1)\}$
- $Z_2 = \{0,1\}$
- $Z_6 = \{ 0,1,2,3,4,5\}$
- $Z_n$ => set of least residues modulo n
- We have infinite instances of the set of residues ($Z_n$),
- $Z_2$, $Z_{10}$, $Z_{11}$,......

- Mapping from Z to $Z_n$ is not one-to-one
- 2 mod 10 = 2
- 12 mod 10 = 2
- 22 mod 10 = 2
- Congruent mod 10

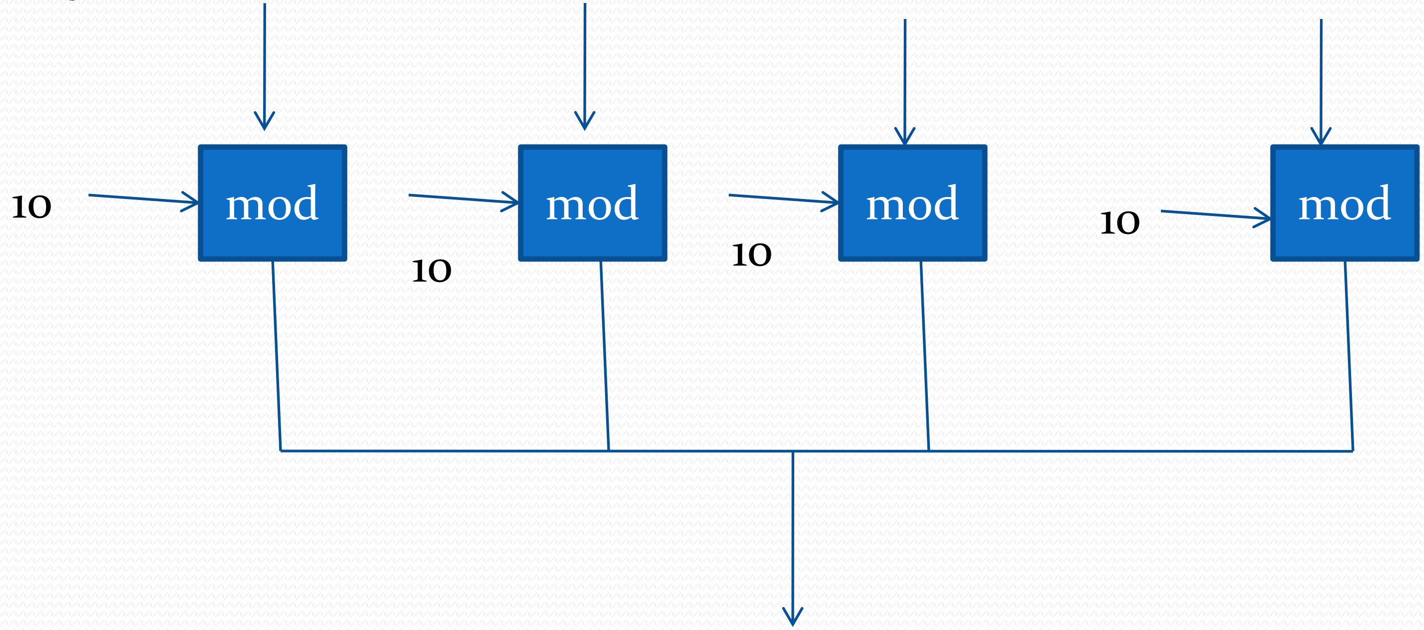
# Concept of Congruence

- Difference between equality operator and congruence operator
- An equality operator maps a member of Z to itself.

  The congruence operator maps a member from Z to a member of $Z_n$.
- The equality operator is one-to-one.

  The congruence operator is many-to-one.

- Z = { ......,-8,..      ....,2,.      .....12,      ....      22..... }




$$Z_{10} = \{ 0,1,2,3,4,5,6,7,8,9\}$$

$-8 \equiv 2 \equiv 12 \equiv 22 \pmod{10}$ The destination set is Z10.

- Residue Classes
- A residue class [a] or $[a]_n$ is the set of integers congruent modulo n.
- A set of all integers such that x = a (mod n)
- If n=5, five sets, [0], [1], [2],[3],[4],[5]

- [0] = { ..-15,-10,-5,0,5,10,15,.......}
- [1] = { ....-14,-9,-4, 1, 6,11,16,......}
- [2] = { ....,-13,-8, -3, 2, 7,12,....}

- Properties
- (a + b ) mod n = [ (a mod n) + (b mod n) ] mod n
- (a – b) mod n = [ (a mod n) – (b mod n) ] mod n
- (a x b) mod n = [ (a mod n) x (b mod n)] mod n

- Example 1:

(1,723,345 + 2,124,945 ) mod 11
=[(1,723,345  mod 11) + (2,124,945 mod 11)] mod 11
=( 8 + 9 ) mod 11
=6

- (1,723,345 - 2,124,945 ) mod 11

=( 8 - 9 ) mod 11
= -1 mod 11
= 10

- (1,723,345 x 2,124,945 ) mod 11

= (8 x 9) mod 11
= 72 mod 11
= 6

- Example 2
- We need to find 10 mod 3, $10^2$ mod 3, $10^3$ mod 3, and so on.
- $10^n$ mod x = ( 10 mod x)$^n$ mod x

= (10 x 10 x 10 x ……x 10) mod x

= [(10 mod x) x (10 mod x) x …….x(10 mod x) ] mod x

= (10 mod x)$^n$ mod x

e.g. 10 mod 3 = 1 => $10^n$ mod 3 = (10 mod 3)$^n$ = (1)$^n$ =1

10 mod 9 =1 => $10^n$ mod 9 = (10 mod 9)$^n$ = (1)$^n$ =1

$10^n$ mod 7 = (10 mod 7)$^n$ = $3^n$ = $3^n$ mod 7

- Example 3
- The remainder of an integer divided by 3 is the same as the remainder of the sum of its decimal digits.
- The remainder of dividing 6371 by 3 is the same as dividing 17 by 3 because 6+3+7+1 = 17.
- $a = a_n \times 10^n + a_{n-1} \times 10^{n-1} + \ldots. + a_0 \times 10^0$
- $a \bmod 3 = (a_n \times 10^n + a_{n-1} \times 10^{n-1} + \ldots. + a_0 \times 10^0) \bmod 3$

$= (a_n \times 10^n) \bmod 3 + (a_{n-1} \times 10^{n-1}) \bmod 3 + \ldots. + (a_0 \times 10^0) \bmod 3$

$= (a_n \bmod 3) \times (10^n \bmod 3) + (a_{n-1} \bmod 3) \times (10^{n-1} \bmod 3) + \ldots\ldots. + (a_0 \bmod 3) \times (10^0 \bmod 3)$

$= a_n \bmod 3 + a_{n-1} \bmod 3 + \ldots\ldots. + a_0 \bmod 3$

$= (a_n + a_{n-1} + \ldots.. + a_0) \bmod 3$