**Tutorial 1**

**Name**:Bhavin Patil

**Roll No:** 66

**TY-CS-D**

# Mathematical Background for Cryptography

**Mathematical Background for Cryptography:**

**Modular arithmetic and gcd**  
Network Security Design

FundamentalsET-IDA-082

**Mathematical Background In Discrete Mathematics, number theory**  
Outlines

Euclidean Algorithm

Remainder

Greatest Common Divisor (gcd)

Group Theory, Rings, Finite Fields

Element’s Order, Euler Theorem

Prime Numbers

Prime Number Generation

Extension Fields

**Mathematical background: number theory**  
Number sets of interest in cryptography:

Natural numbers N =

Integers set Z =

For any n  N and n >1 :=> pi prime numbers r is the number of prime factors of n.

**Euclidean Division theorem for integers**  
For any Integers n and d with d  0 there is q and r, such that:

n / d = q r / d

n = q d + r where  r < d

We say: Rd (n) = r , r is Remainder of n modulo d

Example: /5 = /5or =

In remainder algebra R5 (13) = 3

**Rd (a + b ) = Rd [ Rd (a) + Rd (b) ]**  
Remainder arithmetic

Rd (a + b ) = Rd [ Rd (a) + Rd (b) ]

Rd (a . b ) = Rd [ Rd (a) . Rd (b) ]

Examples:R5 ( ) = R5 [ R5 (7) + R5 (14) ]= R5 [ ] = R5 (6) = 1R5 ( ) = R5 [ R5 (9) . R5 (22) ]= R5 [ ] = R5 (8) = 3

**Equivalence: Integer remainder system modulo d**  
Rd (n) = Rd (n + i d ) where n, i are any integers

Example: Remainder modulo 5:

R5 (7) = R5 [ x 5 ] = R5 [22 ] = 2

R5 (7) = R5 [ x 5 ] = R5 [-3 ] = 2

In this remainder algebra: 22 = -3 = 2

Integers having the same remainder can be tabulated in the so called Slepian Array (or Standard Array) for d=5, all Z elements are ordered in a table of 5 cosets:

r...

- 10 5 15....

Remainder Class (coset)

1 9 4 6 11 16 2 8 3 7 12 17 13 18 14 19

Example this coset is equivalent to 3

We have a total of 5 cosets modulo 5Coset leader

**gcd: greatest common divisor**  
gcd (m1 , m mt ) is the greatest positive integer

which divides m1 , m mt without remainder.

Example: gcd (15,5) = 5

If gcd (n1 , n2) = 1, then n1 , n2 are called relatively prime integers

Example: gcd (15,28) = 1 => 15, 28 are relatively prime

**Properties of gcd: Fundamental property of gcd:**  
gcd (n, 0) = n (for n  0)

gcd (n, 0) = ? , undefined (if n = 0)

gcd (n1 , n2) = gcd (n2 , n1)

gcd (n1 , n2) = gcd ( + n1 , + n2)

Fundamental property of gcd:

gcd (n1 , n2) = gcd ( n1 + i n2 , n2 )

or gcd (n1 , n2) = gcd ( Rn2 ( n1) , n2 )

Examples: gcd (15, 10) = gcd ( , 10 ) = gcd ( , 10 )

= gcd ( 15 – 2x10 , 10 ) = gcd (-5,10)

Or gcd (15, 10) = gcd ( R10(15) , 10 ) = gcd ( 5 , 10 ) = gcd ( 5 , R5 (10) ) = gcd (5 , 0 ) = 5

**Euclidean gcd Algorithm**  
Example:

Gcd

Complexity < log2 n operations

n = Max [n1, n2]

**Stein`s improvement for the Euclidean gcd Algorithm**  
n1 and n2 even: gcd (n1 , n2) = gcd ( n1 / 2 , n2 / 2 )

n1 even, n2 odd: gcd (n1 , n2) = gcd ( n1 / 2 , n2 )

n1 and n2 odd: gcd (n1 , n2) = gcd [ (n1-n2) / 2 , n2 ]

**Stein`s improvement for Euclidean gcd Algorithm**  
Complexity < log2 n + 1

n= Max [n1, n2]

gcd

gcd

**Extended Euclidean gcd Algorithm**  
gcd (n1 , n2) = a . n b . n2

**Special gcd Properties**  
gcd (tn-1, tm-1) = t gcd (n, m) -1

Example:

gcd(215-1, 220-1) = 2 gcd(15,20) - 1 = 25-1 = 31

gcd[ (x + y)15-1, (x + y)20-1 ] = (x + y)5-1

**Extended “gcd” and Multiplicative Modular Inversion**  
If an integer is invertible under multiplication, then it is called a unit

Example: 3 x 2 = 6 = 1 (mod 5)

says that : is the multiplicative inverse of 2 modulo 5 (2-1=3)

or 2 is the multiplicative inverse of 3 modulo 5 (3-1=2)

Fundamental Theorem of units:

An integer u is a unit modulo m (or has a multiplicative inverse modulo m) iff (if and only if):

gcd (m, u) = 1

Computation: If gcd (m, u) = 1 then a.m + b.u = 1

Rm (a m + b u) = Rm (1)

Rm (b . u) = => u-1 = Rm (b)

Example: gcd (7, 3) = 1 =R7 ( – ) = 1R7 (-2 . 3) = => R7 (3-1) = -2 =>

thus = Test: = 15 = 1 (mod 7)