MATHEMATICAL BACKGROUND FOR CRYPTOGRAPHY.

2.1 Modulo Arithmetic

→ Let a be an integer, a dividend.
m be a positive integer.
q be a quotient
r be a remainder.

→ The Relationship between a, m, q and r is

$$a = m*q + r, \quad \text{where } 0 \le r < m$$

→ $$r \equiv a \pmod m$$

→ Let $m=10$ and $r=3$,
Then 13, 23, 33 etc all satisfy with quotients 1, 2, 3 etc.

$$\{\ldots -17, -7, 3, 13, 23, 33, 43, \ldots\}$$

→ Any two numbers in the above set are said to be congruent modulo 10.

→ Set itself is referred to as Congruence class.

FACT: If two integers are Congruent modulo n, then they differ by an integral multiple of n.

$a \bmod n = r \rightarrow (1)$ $b \bmod n = r$,

then

$a = n * q_1 + r$ and

$b = n * q_2 + r$

→ q_1 and q_2 are integers

→ By Subtracting,

$a - b = n(q_1 - q_2)$

Since q_1 and q_2 are integers, a and b differ by an integral multiple of n.

Modulo arithmetic properties:

1. $(a+b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$
2. $(a-b) \bmod n = ((a \bmod n) - (b \bmod n)) \bmod n$
3. $(a*b) \bmod n = ((a \bmod n) * (b \bmod n)) \bmod n$

Example:

Given $n=8$, $a=27$ and $b=34$.

LHS of property 1 from above:

$\Rightarrow (a+b) \bmod n$

$\Rightarrow (27+34) \bmod 8$

$\Rightarrow 61 \bmod 8$

$\Rightarrow \boxed{5}$

RHS of property 1:

$\Rightarrow ((27 \bmod 8) + (34 \bmod 8)) \bmod 8$

$= (3+2) \bmod 8$

$= \underline{5}$

2.2. THE GREATEST COMMON DIVISOR.

→ Given two integers, a and b, we say a divides b, denoted by $\underline{a|b}$

Definition: If $a|b$ and $a|c$, there exists no $a' > a$, such that $a'|b$ and $a'|c$, then a is referred to as the greatest common divisor of b and c, denoted $a = \gcd(b, c)$.

Example: $\gcd(24, 78) = 6$.

Definition: If $\boxed{\gcd(b, c) = 1}$ we say b and c are relatively prime or co-prime.

EUCLID'S ALGORITHM

→ Euclid's algorithm is used to find the gcd of two integers b and c.

→ $b > c$

→ divide b by c explicitly, showing the quotient q and remainder r.

→ $\boxed{b = c * q + r}$

→ Assign c to b.

$b = c$.

→ Assign r to c

$c = r$

Compute gcd (161, 112)

Soln: b = 161
c = 112

$$b = c * q + r$$

Step 1: $161 = 112 * 1 + 49$

step 2: $112 = 49 * 2 + 14$

Step 3: $49 = 14 * 3 + 7$

step 4: $14 = 7 * 2 + 0$

→ Sequence of division continues until a remainder 0(zero) is encountered.

→ Observations about the above procedure:

(a) gcd(b,c) divides each nonzero remainder above.

↳ gcd(b,c)|b [∵ gcd(b,c) divides b]

↳ gcd(b,c)|c [∵ gcd(b,c) divides c]

↳ Ex→ gcd(161, 112) = 7

7 divides 49, 14.

(b) The remainder just above the zero, in step 4, is the gcd(b,c).

GCD Theorem: Given two integers b and c, there exist two integers x and y such that

$$b*x + c*y = \gcd(b,c).$$

Corollary 1: If b and c are relatively prime, then there exist integers x and y such that

$$b*x + c*y = 1$$

→ In Cryptography, it is often needed to compute multiplicative inverses modulo a prime number.

→ The formal procedure to obtain the inverse of c modulo b is called the Extended Euclids algorithm.

→ It assumes b and c are relatively prime, which means gcd(b,c) = 1

Example:

Q: Compute the Inverse of 12 modulo 79.
(Inverse of c " b)

Soln: Given: $b = 79$
$c = 12$.

Assumptions: $x_1 = 1$, $y_1 = 0$, $x_2 = 0$, $y_2 = 1$.

Compute
$x = x_1 - (x_2 * q)$, $b' = b$
$y = y_1 - (y_2 * q)$, $c' = c$

q	b ↓	c ↓	r	x1	x2	x	y1	y2	y	$(x*b') + (y*c') = r$
6	79	12	7	[1]	[0]	1	[0]	[1]	-6	$(1*79)+(-6*12)=7$
1	12	7	5	0	1	-1	1	-6	7	$(-1*79)+(7*12)=5$
1	7	5	2	1	-1	2	-6	7	-13	$(2*79)+(-13*12)=2$
2	5	2	[1]	-1	2	[-5]	7	-13	[33]	$(-5*79)+(33*12)=1$

At the end of last iteration,
$r = 1$, and $(-5*79)+(33*12) = \underline{1}$.

$$33*12 = 1 + 5*79 \equiv 1 \pmod{79}$$
$$396 = 1 + 395$$
$$396 = 396.$$

Thus the inverse of 12 modulo 79 is 33//

Algorithm

```
ComputeInverse(b,c)    // Compute the inverse of c mod b
{
    b'=b               // Copy b and c to b' & c'
    c'=c
    x1=1 , y1=0        // Assumptions
    x2=0 , y2=1
    r=2
    while(r>1)
    {
        q=b/c          // Compute quotient
        r=b%c          // Compute Remainder.
        x = x1-x2*q    // Compute x.
        x1=x2          // update x1 and x2
        x2=x
        y = y1-y2*q    // Compute y
        y1=y2          // update y1 and y2
        y2=y
        b=c            // Copy c to b
        c=r            // Copy r to c.
    }
    return y.          // last iteration y value.
}
```

2.3 ALGEBRAIC STRUCTURES.

2.3.1 GROUPS

→ A group is the most basic algebraic structure used in Cryptography.

→ Definition: A group is a pair $\langle G, * \rangle$, where G is a set and $*$ is a binary operation such that the following hold:

i) Closure: If a and b are elements of G, then $a * b$.

ii) Associativity: If a, b, and c are elements of G then $a * (b * c) = (a * b) * c$.

iii) Identity element: There exist an element I in G, such that for all b in G, $I * b = b = b * I$.

iv) Inverse: For each element b in G, there exist exactly one element C in G such that $b * C = C * b = I$

[C is referred as Inverse of b].

Notation:

Let Z_n^* denote the set

$\{i \mid 0 < i \leq n \text{ and } \gcd(i, n) = 1\}$

ie, Z_n^* is the set of all integers modulo n that are relatively prime.

Ex:- $Z_5^* = \{1, 2, 3, 4\}$

$\gcd(i, n) = 1$.

$\gcd(1, 5) = 1$

$\gcd(2, 5) = 1$

$\gcd(3, 5) = 1$

$\gcd(4, 5) = 1$.

Ex:- $Z_6^* = \{1, 5\}$.

$\gcd(i, n) = 1$

$\gcd(1, 6) = 1$

$\gcd(2, 6) \neq 1$

$\gcd(3, 6) \neq 1$

$\gcd(4, 6) \neq 1$

$\gcd(5, 6) = 1$

ϕ : $i < n$

$5 < 6$.

Definitions:

1. The order of a group, $\langle G, * \rangle$ is the number of elements in G.
2. The Euler totient function, denoted by $\phi(n)$, is the order of $\langle Z_n^*, *_n \rangle$.

Ex: $\phi(5) = 4$

$Z_5^* = \{1, 2, 3, 4\}$

Number of elements to, in Z_5.

3. Lagrange's theorem: The order of any subgroup, divides the order of the parent group.

→ Consider $\langle Z_5^*, *_5 \rangle$, Its order is 4, no subgroup of it can have order = 3.

→ The Subgroups have order 1, 2 and 4.

4. Euler's theorem: If m and n are relatively prime, $m^{\phi(n)} \bmod n = 1$.

5. Fermat's Little theorem: Let p be prime, and m be a non-zero integer that is not a multiple of P, the $\boxed{m^{P-1} \bmod p = 1}$

6. A group $\langle G, * \rangle$ is cyclic if there is atleast one element g in it such that $\langle g \rangle$ is $\langle G, * \rangle$. We refer to such an element of $\langle G, * \rangle$ as a generator of G.

Example:

Check if 2 is a generator of Z_{13}^*.

$Z_{13}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

$\uparrow i < n$

$12 < 13.$

→ generator $g = 2$.

→ $g^i \bmod n$

→ $2^1 \bmod 13 = 2$

$2^2 \bmod 13 = 4$

$2^3 \bmod 13 = 8$

$2^4 \bmod 13 = 3$

$2^5 \bmod 13 = 6$

$2^6 \bmod 13 = 12$

$2^7 \bmod 13 = 11$

$2^8 \bmod 13 = 9$

$2^9 \bmod 13 = 5$

$2^{10} \bmod 13 = 10$

$2^{11} \bmod 13 = 7$

$2^{12} \bmod 13 = 1.$

→ $\langle Z_{13}^*, *_{13} \rangle$ is a cyclic group, which has a generator 2, generates all elements of Z_{13}^*.

→ Hence it is cyclic.

Fact: The group $\langle Z_p^*, *_p \rangle$ is cyclic, iff p is prime.

Fact: Let P be prime, and let $P_1, P_2 \ldots P_K$ be distinct prime factors of $P-1$. Then g is a generator of $\langle Z_p^*, *_p \rangle$ iff,

$$g^{(P-1)/P_i} \neq 1 \bmod P \text{ for all } P_i,$$

$$\boxed{g^{(P-1)/P_i} \bmod p \neq 1} \qquad 1 \leq i \leq K.$$

The generators of Z_{13}^* are 2, 6, 11, 7.

Q. Check whether 7 and 3 are generators of $\langle Z_{13}^*, *_{13} \rangle$

→ $P = 13$.

→ $P-1 = 12$

2	12
2	6
3	3
	1

Prime factors of 12 are 2 and 3

Given $\Rightarrow$ $g = 7$, $P = 13$.

$P - 1 = 12$

$P_i^\circ = 2$ and 3

$\Rightarrow g^{(P-1)/P_i} \neq 1 \bmod P$.

$7^{(12)/2} \neq 1 \bmod P$

$\Rightarrow 7^6 \bmod P$.

$\equiv -1$.

$\Rightarrow g^{(P-1)/P_i^\circ} \bmod P$.

$7^{12/3} \bmod 13$

$7^4 \bmod 13$

$\equiv 9$.

Hence 7 is a generator of Z_{13}^*.

$\Rightarrow g = 3$, $P = 13$.

$g^{(P-1)/P_i^\circ} \bmod P$

$3^{(12)/2} \bmod 13$

$\equiv 1$ $\longrightarrow$ hence $g = 3$ is not a generator of Z_{13}^*

RINGS

→ A ring is a triplet $\langle R, +, * \rangle$, where + and * are Binary operations and R is a set satisfying the following properties.

→ $\langle R, + \rangle$ is a Commutative group.

→ The additive identity is designated as 0.

→ $\langle R, + \rangle$ is a Commutative group.

→ for all x, y, z in R.

1) $x * y$ is also in R

2) $x * (y * z) = (x * y) * z$ (Associative)

3) $(x) * (y + z) = x * y + x * z = (y + z) * x$.
(Distributive)

→ while each element x, has an additive inverse $-x$,

→ An element need not have multiplicative inverse (x^{-1}).

Polynomial ring

→ Let $Z_p[x]$ be the set of all polynomials in x with coefficient belonging to Z_p.

→ Addition of two polynomials is addition of coefficients value with modulo P.

→ Example Consider two polynomials a(x) and b(x) in $Z_3[x]$

$$a(x) = 2x^4 + x^3 + 2x + 1$$

$$b(x) = x^5 + x^4 + 2x$$

$$a(x)+b(x) = (x^5 + 3x^4 + x^3 + 4x + 1) \bmod 3$$

for coeff.

$$1x^5 \equiv 1 \bmod 3 = 1 = x^5$$

$$3x^4 = 3 \bmod 3 = 0 = 0$$

$$1x^3 = 1 \bmod 3 = 1 = x^3$$

$$4x = 4 \bmod 3 = 1 = x$$

$$1 = 1 \bmod 3 = 1 = 1.$$

$$\Rightarrow \boxed{x^5 + x^3 + x + 1}$$

Multiplication of two polynomials.

$a(x) * b(x)$.

$a(x) = 2x^4 + x^3 + 2x + 1$

$b(x) = x^5 + x^4 + 2x$.

$a(x) * b(x)$

$\Rightarrow (2x^4 + x^3 + 2x + 1) * (x^5 + x^4 + 2x)$

$\Rightarrow 2x^9 + 2x^8 + 4x^5 + x^8 + x^7 + 2x^4 + 2x^6 + 2x^5 + 4x^2 + x^5 + x^4 + 2x$.

$\Rightarrow (2x^9 + 3x^8 + x^7 + 2x^6 + 7x^5 + 3x^4 + 2x) \bmod 3$

$\Rightarrow 2x^9 + x^7 + 2x^6 + x^5 + 2x$

$\Rightarrow \boxed{2x^9 + x^7 + 2x^6 + x^5 + 2x}$

FIELDS

→ A field, $\langle R, +, * \rangle$ is a Commutative ring

→ R has multiplicative identity 1, additive identity 0.

Chinese Remainder Theorem.

→ The Chinese Remainder Theorem is used in proving a number of results in cryptography.

→ Consider the factorization of an integer, N.

$$N = n_1 * n_2 \ldots * n_K$$

→ where n_1 and n_2 are relatively prime ie $\gcd(n_i, n_j) = 1$.

→ $1 \leq i \leq K$ and $1 \leq j \leq K$, $i \neq j$.

→ Consider the mapping.

$f: Z_n \rightarrow Z_{n_1} \times Z_{n_2} \times Z_{n_3} \ldots Z_{n_K}$

$f(x) := (x \bmod n_1, x \bmod n_2 \ldots\ldots$

$x \bmod n_K)$, where $0 \leq x < N$.

Q. Solve using Chinese Remainder theorem, for $N=30$, Compute $f(x)$.

Soln: N=30

→ prime factors for 30 are 6 and 5 (6 * 5 = 30)

→ $n_1 = 6$, $n_2 = 5$

→ $f(x) \rightarrow 0 \leq x < 30$.

$f(x) = (x \bmod n_1, x \bmod n_2)$

$f(0) = (0 \bmod 6, 0 \bmod 5) = (0,0)$

$f(1) = (1 \bmod 6, 1 \bmod 5) = (1,1)$

$f(2) = (2 \bmod 6, 2 \bmod 5) = (2,2)$

$f(3) = (3 \bmod 6, 3 \bmod 5) = (3,3)$

$f(4) = (4 \bmod 6, 4 \bmod 5) = (4,4)$

$f(5) = (5 \bmod 6, 5 \bmod 5) = (5,0)$

$f(6) = (6 \bmod 6, 6 \bmod 5) = (0,1)$

$f(7) = (7 \bmod 6, 7 \bmod 5) = (1,2)$

$f(8) = (8 \bmod 6, 8 \bmod 5) = (2,3)$

$f(9) = (9 \bmod 6, 9 \bmod 5) = (3,4)$

$f(10) = (10 \bmod 6, 10 \bmod 5) = (4,0)$

$f(11) = (11 \bmod 6, 11 \bmod 5) = (5,1)$

$f(12) = (12 \bmod 6, 12 \bmod 5) = (0,2)$

$f(13) = (13 \bmod 6, 13 \bmod 5) = (1,3)$

$f(14) = (14 \bmod 6, 14 \bmod 5) = (2,4)$

$f(15) = (15 \bmod 6, 15 \bmod 5) = (3,0)$

$f(16) = (16 \bmod 6, 16 \bmod 5) = (4,1)$

$f(17) = (17 \bmod 6, 17 \bmod 5) = (5,2)$

$f(18) = (18 \bmod 6, 18 \bmod 5) = (0,3)$

$f(19) = (19 \bmod 6, 19 \bmod 5) = (1,4)$

$f(20) = (20 \bmod 6, 20 \bmod 5) = (2,0)$

$f(21) = (21 \bmod 6, 21 \bmod 5) = (3,1)$

$f(22) = (22 \bmod 6, 22 \bmod 5) = (4,2)$

$f(23) = (23 \bmod 6, 23 \bmod 5) = (5,3)$

$f(24) = (24 \bmod 6, 24 \bmod 5) = (0,4)$

$f(25) = (25 \bmod 6, 25 \bmod 5) = (1,0)$

$f(26) = (26 \bmod 6, 26 \bmod 5) = (2,1)$

$f(27) = (27 \bmod 6, 27 \bmod 5) = (3,2)$

$f(28) = (28 \bmod 6, 28 \bmod 5) = (4,3)$

$f(29) = (29 \bmod 6, 29 \bmod 5) = (5,4)$

Nagashree. C
Asst Professor, Department of CSE,SVIT

→ It is straightforward to compute $f(x)$ given an x.

→ Given a tuple in:
$Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_K} \rightarrow Z_n$.

→ Given a tuple,
$(x_1, x_2, \cdots x_K) \in (Z_{n_1} \times Z_{n_2} \times Z_{n_3} \cdots Z_{n_K})$

→ $x \in Z_N$.

→ $a_i = \frac{N}{n_i}$, $1 \leq i \leq K$.

→ Let x_i denote the inverse of a_i in the modulo n_i,

→ $x_i \times a_i \equiv 1 \pmod{n_i}$

for $1 \leq i \leq K$

→ x can be computed as:
$(x_1 \times a_1 \times x_1 + x_2 \times a_2 \times x_2 \cdots x_K \times a_K \times x_K)$
$\bmod n_i = x_i$

Nagashree. C
Asst Professor, Department of CSE,SVIT

$(x_1 \times a_1 \times \alpha_1 + x_2 \times a_2 \times \alpha_2 \cdots + x_k \times a_k \times \alpha_k) \bmod n_i \equiv x_i$

Example: If $N = 210$, $n_1 = 5$, $n_2 = 6$, $n_3 = 7$, Compute $f^{-1}(3, 5, 2)$

Soln: $x_1 = 3$ $\quad n_1 = 5$

$x_2 = 5$ $\quad n_2 = 6$

$x_3 = 2$ $\quad n_3 = 7$

→ $a_1 = N/n_1 = 210/5 = 42$

$a_2 = N/n_2 = 210/6 = 35$

$a_3 = N/n_3 = 210/7 = 30$

→ $\alpha_1 = 42^{-1} \pmod 5 = 3$

$\alpha_2 = 35^{-1} \pmod 6 = 5$

$\alpha_3 = 30^{-1} \pmod 7 = 4.$

→ $x = (x_1 \times a_1 \times \alpha_1 + x_2 \times a_2 \times \alpha_2 + x_3 \times a_3 \times \alpha_3) \bmod N$

$= (3 \times 42 \times 3 + 5 \times 35 \times 5 + 2 \times 30 \times 4) \bmod 210$

Nagashree. C
Asst Professor, Department of CSE,SVIT

→ $1493 \pmod{210}$

→ $\boxed{23}$

Nagashree. C
Asst Professor, Department of CSE,SVIT