Cryptography & Network Security

Lec#3

Maths for Symmetric key Cryptography…*cont'd*

Objectives

- To review integer arithmetic, concentrating on divisibility and finding the greatest common divisor using the Euclidean algorithm
- To understand how the extended Euclidean algorithm can be used to solve linear Diophantine equations.
- To emphasize the importance of modular arithmetic and the modulo operator
- To find the multiplicative inverses & solve linear congruent equations
- To emphasize and review matrices and operations on residue matrices that are extensively used in cryptography
- To solve a set of congruent equations using residue matrices

Additive & Multiplicative Inverse

Additive & Multiplicative Inverse in Integer (Z) arithmetic

- **Additive Inverse**
  - **a + b = 0 [a & b in Z]**
  - **a + (-a) = 0 ➔**
  - **(-a) is addInv of a in Z**

- **Multiplicative Inverse**
  - **a * b = 1 [a & b in Z]**
  - **a * (1/a) = 1 ➔ a * a^{-1} = 1 ➔**
  - **(1/a) is mult Inv of a in Z**

Additive Inverse in Zn

In modular arithmetic, each integer has an additive inverse. The sum of an integer & its additive inverse is congruent to 0 modulo n.

In Z_n, two numbers *a* & *b* are additive inverses of each other if

$$a + b \equiv 0 \pmod{n} \longrightarrow$$ ***a + b (mod n)= 0***

additive Inverse of a is (n-a) in Zn

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

The six pairs of additive inverses are:-
(0, 0), (1, 9), (2, 8), (3, 7), (4, 6), and (5, 5).

Multiplicative Inverse in Zn

In modular arithmetic, an integer may or may not have a multiplicative inverse. When it does, product of the integer & its multiplicative inverse is congruent to 1 modulo n.

In Z_n, two numbers *a* and *b* are the multiplicative inverse of each other if

$$a \times b \equiv 1 \pmod{n}$$

$$a \times a^{-1} \equiv 1 \pmod{n}$$

<u>note:</u> The number of multiplicative inverses of an element 'a' in the set Zn = gcd (n, a) i.e. if a is relative prime to n

Examples: Multiplicative Inverse in Zn

Ex1: Find the multiplicative inverse of 8 in Z_{10}.

There is no multiplicative inverse because gcd (10, 8) = 2 ≠ 1. In other words, we cannot find any number between 0 and 9 such that when multiplied by 8, the result is congruent to 1.

Ex2: Find all multiplicative inverses in Z_{10}.

Mod when Divisor is greater then dividen

modulus = dividend - (quotient * divisor)

There are only three pairs: (1, 1), (3, 7) and (9, 9). The numbers 0, 2, 4, 5, 6, and 8 do not have a multiplicative inverse.

Ex3: Find all multiplicative inverse pairs in Z_{11}.

We have seven pairs:-

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

X,Y=|11|

Finding Multiplicative Inverse using Extended Euclidean algorithm

$$a \times s + b \times t = \gcd(a, b)$$

[if a= n]

$$n \times s + b \times t = \gcd(n, b)$$

multInv of b exists only if gcd(n,b)=1

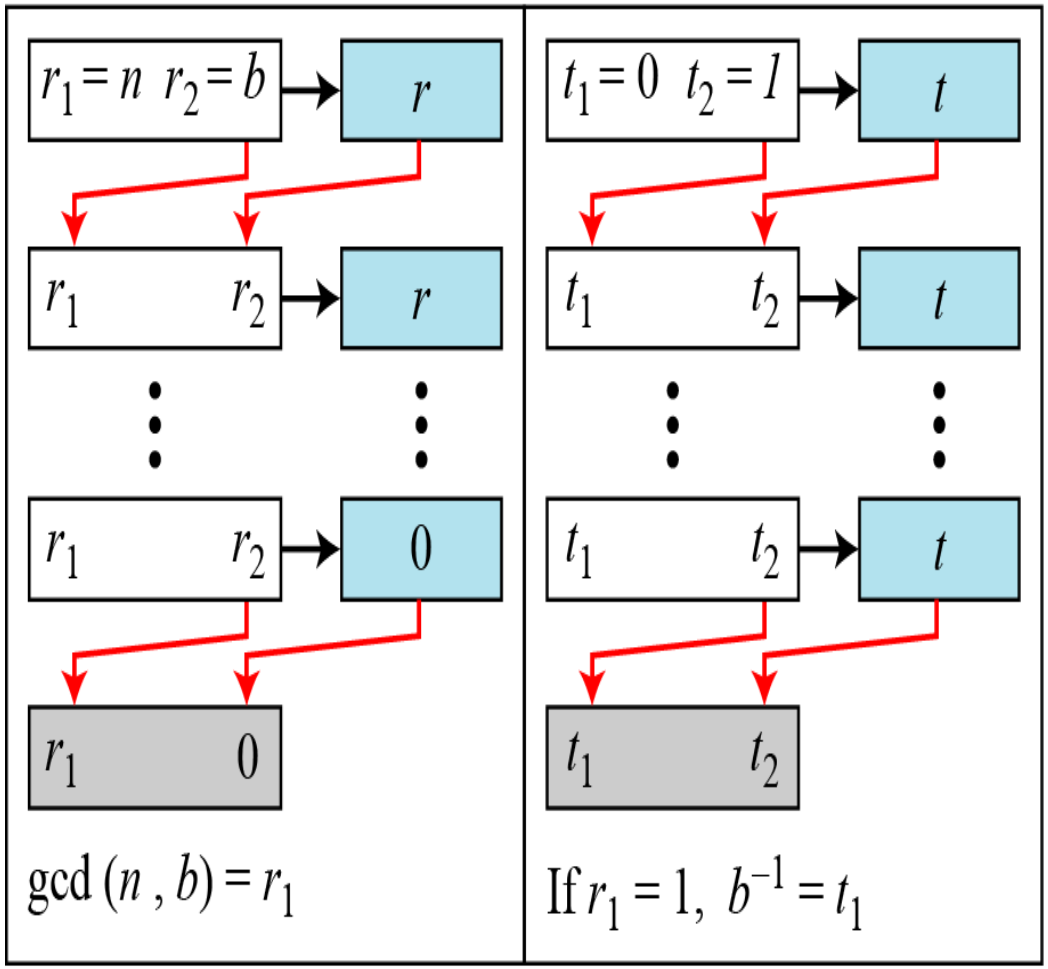
$$n \times s + b \times t = 1$$

Taking (mod n) on both sides of eqn

$$0 \times s + (b \times t) \equiv 1 \pmod{n}$$

Use extended Euclidean algorithm to compute the gcd (n, b) if it is 1 then the multiplicative inverse of b is the value of t in the above EEA after being mapped to Z_n.

Finding Multiplicative Inverse using Extended Euclidean algorithm.....*contd*



a. Process

$r_1 \leftarrow n; \quad r_2 \leftarrow b;$

$t_1 \leftarrow 0; \quad t_2 \leftarrow 1;$

while $(r_2 > 0)$

{

$q \leftarrow r_1 / r_2;$

$r \leftarrow r_1 - q \times r_2;$

$r_1 \leftarrow r_2; \quad r_2 \leftarrow r;$

$t \leftarrow t_1 - q \times t_2;$

$t_1 \leftarrow t_2; \quad t_2 \leftarrow t;$

}

if $(r_1 = 1)$ then $b^{-1} \leftarrow t_1$

b. Algorithm

Examples: Finding Multiplicative Inverse using EEA

Ex1: Find the multiplicative inverse of 11 in Z_{26}.

The gcd (26, 11) is 1; so the mult inverse of 11 in Z_{26} is –7 or 19.

Ex2: Find mult inv of 12 in Z_{26}

q	r_1	r_2	r	t_1	t_2	t
2	26	12	2	0	1	–2
6	12	2	0	1	–2	13
	2	0		–2	13	

The gcd (26, 12) is 2≠1; so mult inverse of 12 in Z_{26} does not exist.

6. Addition & Multiplication Tables for Z_{10}

+	0	1	2	3	4	5	6	7	8	9
0	**0**	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	**0**
2	2	3	4	5	6	7	8	9	**0**	1
3	3	4	5	6	7	8	9	**0**	1	2
4	4	5	6	7	8	9	**0**	1	2	3
5	5	6	7	8	9	**0**	1	2	3	4
6	6	7	8	9	**0**	1	2	3	4	5
7	7	8	9	**0**	1	2	3	4	5	6
8	8	9	**0**	1	2	3	4	5	6	7
9	9	**0**	1	2	3	4	5	6	7	8

Addition Table in $\mathbf{Z}_{10}$

×	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	**1**	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	**1**	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	**1**	8	0	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	**1**

Multiplication Table in $\mathbf{Z}_{10}$

Examples: Z_n, Z_n^*, Z_p, Z_p^* sets

We need to use Zn when additive inverses are needed; we need to use Zn* when multiplicative inverses are needed. *(Definitions)*

$\mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

Relative Primes

$\mathbf{Z}_6^* = \{1, 5\}$

$\mathbf{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$

$\mathbf{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

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

$\mathbf{Z}_{10}^* = \{1, 3, 7, 9\}$

Cryptography often uses two more sets: Z_p and Z_p^*. The modulus in these two sets is a prime number.

Cryptographic Keys & Additive & Multiplicative Inverses

- If the operation (Encryption/ Decriyption Algorithm) is Addition, use additive inverse pairs in Zn as Encryption/ Decryption keys.
- If the operation (Encryption/ Decryption Algorithm) is Multiplication use Multiplicative inverse pairs in Zn* as Encryption/ Decryption keys.
- Zp* can provide Encryption/ Decryption key pairs for both addition & multiplication algorithms.

RESIDUE MATRICES

In cryptography we need to handle residue matrices. Residue matrices use many properties from integer matrices operations. Although this topic belongs to a special branch of algebra called linear algebra, the following brief review of integer matrices is necessary preparation for the study of residue matrices for cryptography.

Topics discussed in this section:

1 **Definitions**
2 **Operations and Relations**
3 **Determinants**
4 **Residue Matrices**

Matrices Definitions & Operations

- Row, column, square & Identity matrix
- Operations & Relations
  - Equality
  - Addition/ Subtraction
  - Determinant
  - Multiplication
  - Additive Inverse of a Matrix
  - Multiplicative Inverse of a Matrix

1 Definition

A matrix of size $l \times m$

Matrix A:

$$\begin{matrix} & \overbrace{\quad\quad\quad\quad} \\ & m \text{ columns} \end{matrix}$$

$$\left.\begin{matrix} \\ \\ \\ \\ \end{matrix}\right\} l \text{ rows}$$

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & & \vdots \\ a_{l1} & a_{l2} & \cdots & a_{lm} \end{bmatrix}$$

Examples of matrices

$$\begin{bmatrix} 2 & 1 & 5 & 11 \end{bmatrix}$$

Row matrix

$$\begin{bmatrix} 2 \\ 4 \\ 12 \end{bmatrix}$$

Column matrix

$$\begin{bmatrix} 23 & 14 & 56 \\ 12 & 21 & 18 \\ 10 & 8 & 31 \end{bmatrix}$$

Square matrix

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$$

0

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

I

2 Operations & Relations

Ex1: Addition and subtraction of matrices

$$\begin{bmatrix} 12 & 4 & 4 \\ 11 & 12 & 30 \end{bmatrix} = \begin{bmatrix} 5 & 2 & 1 \\ 3 & 2 & 10 \end{bmatrix} + \begin{bmatrix} 7 & 2 & 3 \\ 8 & 10 & 20 \end{bmatrix}$$

$$\mathbf{C = A + B}$$

$$\begin{bmatrix} -2 & 0 & -2 \\ -5 & -8 & 10 \end{bmatrix} = \begin{bmatrix} 5 & 2 & 1 \\ 3 & 2 & 10 \end{bmatrix} - \begin{bmatrix} 7 & 2 & 3 \\ 8 & 10 & 20 \end{bmatrix}$$

$$\mathbf{D = A - B}$$

Ex2: Scalar multiplication **B = k x A**

$$\underbrace{\begin{bmatrix} 15 & 6 & 3 \\ 9 & 6 & 12 \end{bmatrix}}_{\mathbf{B}} = 3 \times \underbrace{\begin{bmatrix} 5 & 2 & 1 \\ 3 & 2 & 4 \end{bmatrix}}_{\mathbf{A}}$$

2 Operations & Relations….cont'd

Ex3:Multiplication of a row matrix (1 × 3) by a column matrix (3 × 1) The result is a matrix of size 1 × 1.

$$\underset{C}{[53]} = \underset{A}{[5 \quad 2 \quad 1]} \times \underset{B}{\begin{bmatrix} 7 \\ 8 \\ 2 \end{bmatrix}}$$

In which: $53 = 5 \times 7 + 2 \times 8 + 1 \times 2$

Ex4: Multiplication of 2×3 matrix by 3×4 matrix results in 2×4 matrix

$$\underset{C}{\begin{bmatrix} 52 & 18 & 14 & 9 \\ 41 & 21 & 22 & 7 \end{bmatrix}} = \underset{A}{\begin{bmatrix} 5 & 2 & 1 \\ 3 & 2 & 4 \end{bmatrix}} \times \underset{B}{\begin{bmatrix} 7 & 3 & 2 & 1 \\ 8 & 0 & 0 & 2 \\ 1 & 3 & 4 & 0 \end{bmatrix}}$$

3 Determinant

The determinant of a square matrix A of size m × m denoted as det (A) is a scalar calculated recursively as shown below:

1. If $m = 1$, $\det(\mathbf{A}) = a_{11}$

2. If $m > 1$, $\det(\mathbf{A}) = \sum_{\substack{i=1\ldots m \\ j=1\ldots..m}} (-1)^{i+j} \times a_{ij} \times \det(\mathbf{A}_{ij})$

by deleting the ith row and jth column.

The determinant is defined only for a square matrix.

Examples: Determinant of a matrix

Ex1: we can calculate the determinant of a 2 × 2 matrix based on the determinant of a 1 × 1 matrix.

$$\det\begin{bmatrix} 5 & 2 \\ 3 & 4 \end{bmatrix} = (-1)^{1+1} \times 5 \times \det[\,4\,] + (-1)^{1+2} \times 2 \times \det[\,3\,] \longrightarrow 5 \times 4 - 2 \times 3 = 14$$

or

$$\det\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = a_{11} \times a_{22} - a_{12} \times a_{21}$$

Ex2: calculation of the determinant of a 3 × 3 matrix.

$$\det\begin{bmatrix} 5 & 2 & 1 \\ 3 & 0 & -4 \\ 2 & 1 & 6 \end{bmatrix} = (-1)^{1+1} \times 5 \times \det\begin{bmatrix} 0 & -4 \\ 1 & 6 \end{bmatrix} + (-1)^{1+2} \times 2 \times \det\begin{bmatrix} 3 & -4 \\ 2 & 6 \end{bmatrix} + (-1)^{1+3} \times 1 \times \det\begin{bmatrix} 3 & 0 \\ 2 & 1 \end{bmatrix}$$

$$= (+1) \times 5 \times (+4) \quad + \quad (-1) \times 2 \times (24) \quad + \quad (+1) \times 1 \times (3) = -25$$

4 Multiplicative Inverse of a Matrix

Multiplicative inverses are only defined for square matrices.

if A x B = I ➔ A x A^{-1} =I ➔ B is MI of A

$$A^{-1} = (1/\det A)\ [(-1)^{i+j} Aij]^T$$

5 Residue Matrices

Cryptography uses residue matrices: matrices where all elements are in Z_n. A residue matrix has a multiplicative inverse if gcd (n, det(A)) = 1.

$$\mathbf{A} = \begin{bmatrix} 3 & 5 & 7 & 2 \\ 1 & 4 & 7 & 2 \\ 6 & 3 & 9 & 17 \\ 13 & 5 & 4 & 16 \end{bmatrix} \qquad \mathbf{A}^{-1} = \begin{bmatrix} 15 & 21 & 0 & 15 \\ 23 & 9 & 0 & 22 \\ 15 & 16 & 18 & 3 \\ 24 & 7 & 15 & 3 \end{bmatrix}$$

$$\det(\mathbf{A}) = 21 \qquad \det(\mathbf{A}^{-1}) = 5$$

LINEAR CONGRUENCE

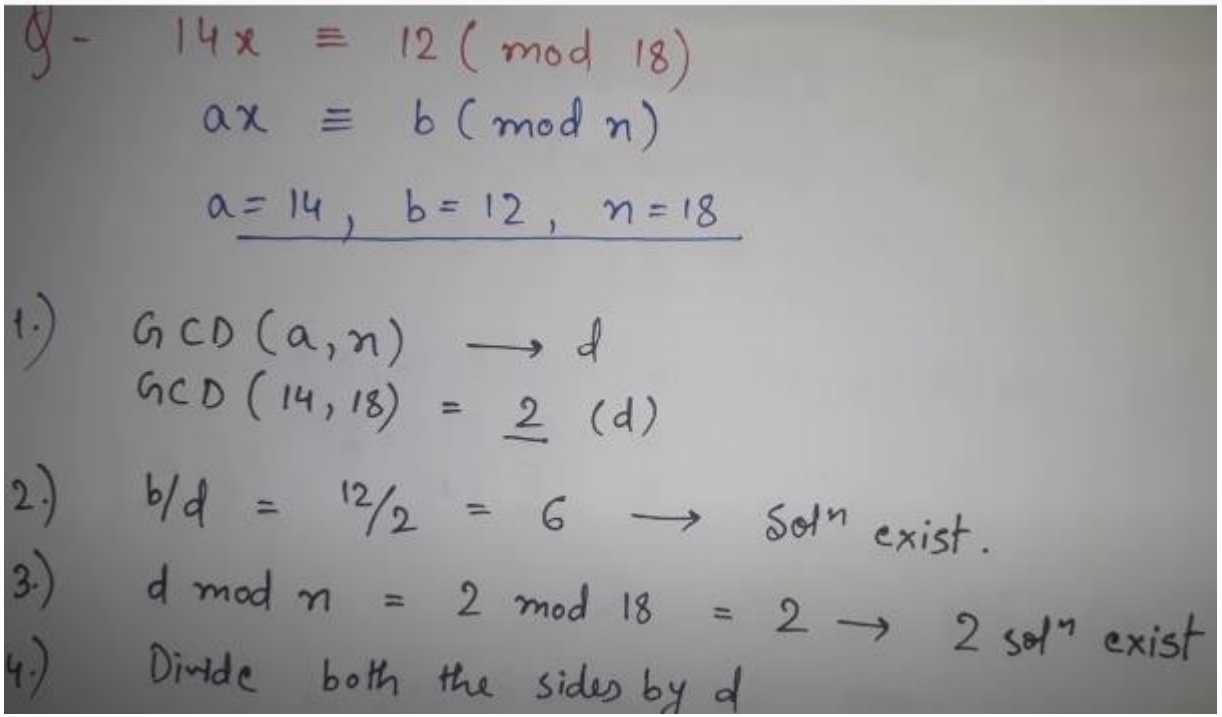
Cryptography often involves solving an equation or a set of equations of one or more variables with coefficient in Z_n. This section shows how to solve equations when the power of each variable is 1 (linear equation).

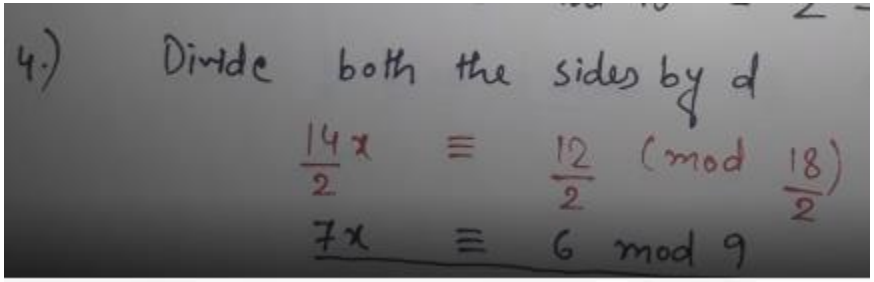
Topics discussed in this section:

1 **Single-variable Linear Equations**

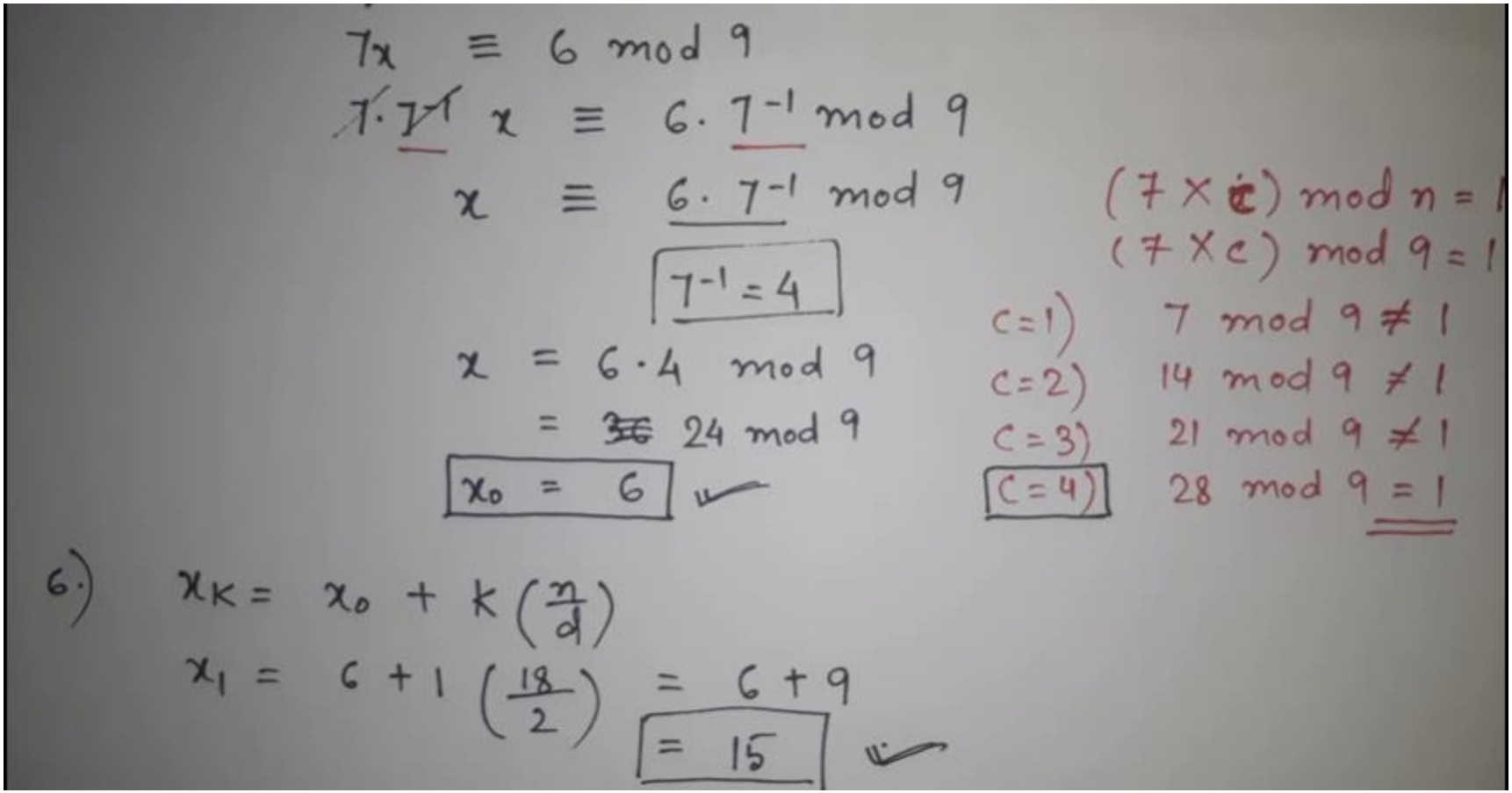
2 **Set of single-variable Linear Equations**

Linear Congruence Equation:





Linear Congruence Equation:



Linear Congruence Equation:

- A single variable linear cong equation with coeffs in Z_n:

$$ax \equiv b \pmod{n}$$

- Let gcd(a, n) =d ; if $d \nmid b$, no soln else d solns as follows:-

a' x $\underline{=}$ b' (modn')

$$x_0 = ((a')^{-1} \times b') \bmod n'$$

Examples: Single-Variable Linear Cong Equations

Ex1: Solve the equation $10x \equiv 2 \pmod{15}$.

First we find the gcd (10 and 15) = 5.
Since 5 does not divide 2, we have no solution.

Ex2: Solve the equation $14x \equiv 12 \pmod{18}$.

Ex3: Solve the equation $3x + 4 \equiv 6 \pmod{13}$.

First we change the equation to the form $ax \equiv b \pmod{n}$. We add -4 (the additive inverse of 4) to both sides, which gives $3x \equiv 2 \pmod{13}$ Because gcd (3, 13) = 1, equation has only one solution, which is $x_0 = (2 \times 3^{-1}) \bmod 13 = 18 \bmod 13 = 5$. We can see that the answer satisfies the original equation: $3 \times 5 + 4 \equiv 6 \pmod{13}$.

Residue Matrix

- Matrix with elements in Z_n ; Used in Cryptography
- All matrix operations same as in integer matrices, but using modular arithmetic
- A residue matrix (A) in Z_n has mult Inv, if the determinant of A has mult Inv in Z_n.
  - **Residue matrix A has mult Inv, if gcd (det(A), n) =1**
- Example: A residue matrix A in Z_{26} has det(A)= 21, as gcd (21, 26)=1, mult Inv of detA = 5 in Z_{26}, so we can find Inv **matrix** A^{-1} such that A x A^{-1} = I
- Example: Find MI of following matrix A:-

$$A = \begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix}$$

2. Set of Single-Variable Linear Equations

We can also solve a set of linear equations with the same modulus if the matrix formed from the coefficients of the variables is invertible.

$$
\begin{aligned}
a_{11}x_1 &+ a_{12}x_2 + \ldots + a_{1n}x_n \equiv b_1 \\
a_{21}x_1 &+ a_{22}x_2 + \ldots + a_{2n}x_n \equiv b_2 \\
&\vdots \qquad\quad \vdots \qquad\qquad\quad \vdots \qquad \vdots \\
a_{n1}x_1 &+ a_{n2}x_2 + \ldots + a_{nn}x_n \equiv b_n
\end{aligned}
$$

a. Equations

$$
\begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{bmatrix}
\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \equiv
\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}
$$

b. Interpretation

$$
\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \equiv
\begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{bmatrix}^{-1}
\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}
$$

c. Solution

Example: Set of Linear Equations (Single-Variable)

Ex: Solve the set of following three equations:

EXAMPLE Solve the set of following three equations:

$$3x + 5y + 7z \equiv 3 \pmod{16}$$
$$x + 4y + 13z \equiv 5 \pmod{16}$$
$$2x + 7y + 3z \equiv 4 \pmod{16}$$

Solution

The result is $x \equiv 15 \pmod{16}$,

$y \equiv 4 \pmod{16}$, &

$z \equiv 14 \pmod{16}$.

We can check the answer by inserting these values into the equations.