INSTITUTE OF INFORMATION TECHNOLOGY

Jahangirnagar University
জাহাঙ্গীরনগর বিশ্ববিদ্যালয়

IT-4259: Computer Network Security

for

4th Year 2nd Semester of B.Sc (Honors) in IT (5th Batch)

Lecture: 01

Mathematics for Network Security

Prepared by:

K M Akkas Ali
akkas_khan@yahoo.com, akkas@juniv.edu
Associate Professor
Institute of Information Technology (IIT)
Jahangirnagar University, Dhaka-1342

Objectives of this Lecture:

- ❖ To review integer arithmetic, concentrating on divisibility.
- ❖ To find the greatest common divisor using the Euclidean algorithm.
- ❖ To understand how the extended Euclidean algorithm can be used to solve linear Diophantine equations.
- ❖ To determine the multiplicative & additive inverse of an integer.
- ❖ To emphasize the importance of modular arithmetic and the modulo operator, because they are extensively used in cryptography.
- ❖ To review matrices and to determine the multiplicative inverse of a matrix.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Books Recommended

1. Cryptography & Network Security
   - Behrouz A Forouzan
2. Cryptography & Network Security
   - William Stallings

Why Need Mathematics in Cryptography?

- Modern cryptography is heavily based on some areas of mathematics, including number theory, linear algebra, and algebraic structures.
- Cryptographic algorithms are designed around computational hardness assumptions using mathematical functions and formula, making such algorithms hard to break in practice by any adversary.
- A list of mathematical fields used in cryptography is given below.
  - Number theory:
    It is used to understand why and how RSA works. Some algorithms use number theory for the difficulty of factoring large numbers as their basis.
  - Group theory:
    Group theory is used to understand why and how El Gamal works.
  - Probability theory:
    It is used in analyzing many kinds of ciphers to better understand what "statistical security" means.
  - Algebraic structure:
    The theory of finite fields is used in multiparty computation.
  - Linear Algebra:
    Lagrange interpolation is used in Shamir's Secret Sharing Scheme. Some linear operations are also used in AES.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Integer Arithmetic: The Set of Integers

- In integer arithmetic, we use a set and a few operations.
- We are already familiar with this set and the corresponding operations, but they are reviewed here to create a background for modular arithmetic.
- The set of integers, denoted by **Z**, contains all integral numbers (with no fraction) from negative infinity to positive infinity.
- Figure below shows the set of integers.

$$\mathbf{Z} = \{\, \ldots, -2, -1, 0, 1, 2, \ldots \,\}$$

Figure: The set of all integers

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Binary Operations

- A binary operation takes two inputs (e.g. ***a*** and ***b***) and creates one output (e.g. ***c***).
- In cryptography, we are interested in three binary operations applied to the set of integers: addition, subtraction and multiplication.

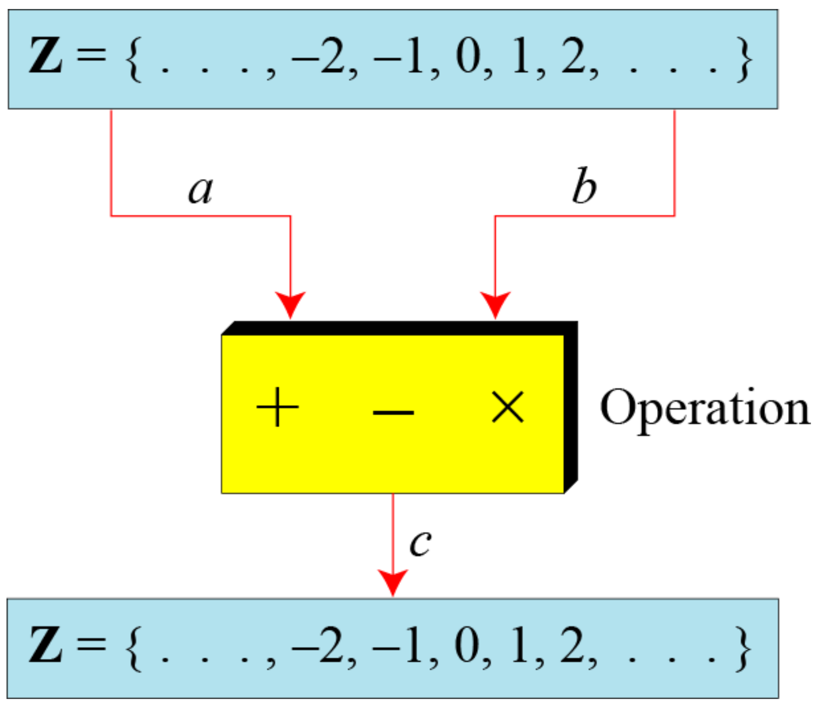


Figure: Three binary operations for the set of integers

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Binary Operations

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

- The following examples shows the results of the three binary operations on two integers.
- Because each input can be either positive or negative, we can have four cases for each operation.

Add:	$5 + 9 = 14$	$(-5) + 9 = 4$	$5 + (-9) = -4$	$(-5) + (-9) = -14$
Subtract:	$5 - 9 = -4$	$(-5) - 9 = -14$	$5 - (-9) = 14$	$(-5) - (-9) = +4$
Multiply:	$5 \times 9 = 45$	$(-5) \times 9 = -45$	$5 \times (-9) = -45$	$(-5) \times (-9) = 45$

Integer Division

- In integer arithmetic, if we divide *a* by *n*, we can get *q* and *r*. The relationship between these four integers can be shown as

$$a = q \times n + r$$

Where,

- a → dividend
- n → divisor
- q → quotient
- r → remainder

Note:

- Division is not a binary operation, because it produces two output instead of one (***q*** and ***r***). Instead, we can call it division relation.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Integer Division

Example:

- Assume that a = 255 and n = 11. We can find q = 23 and r = 2 using the division algorithm.

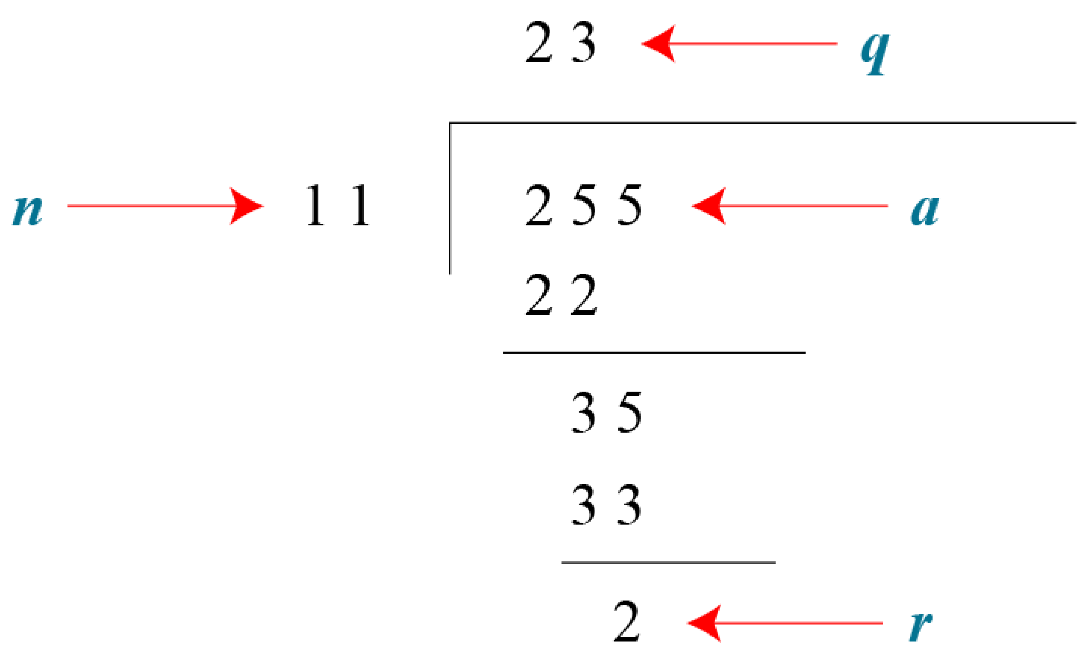


Figure: Finding the quotient and the remainder

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Integer Division

- When we use the above division relationship in cryptography, we impose two restrictions:
    1. The divisor be a positive integer (i.e. n>0)
    2. The remainder be a non-negative integer (i.e. r>=0)

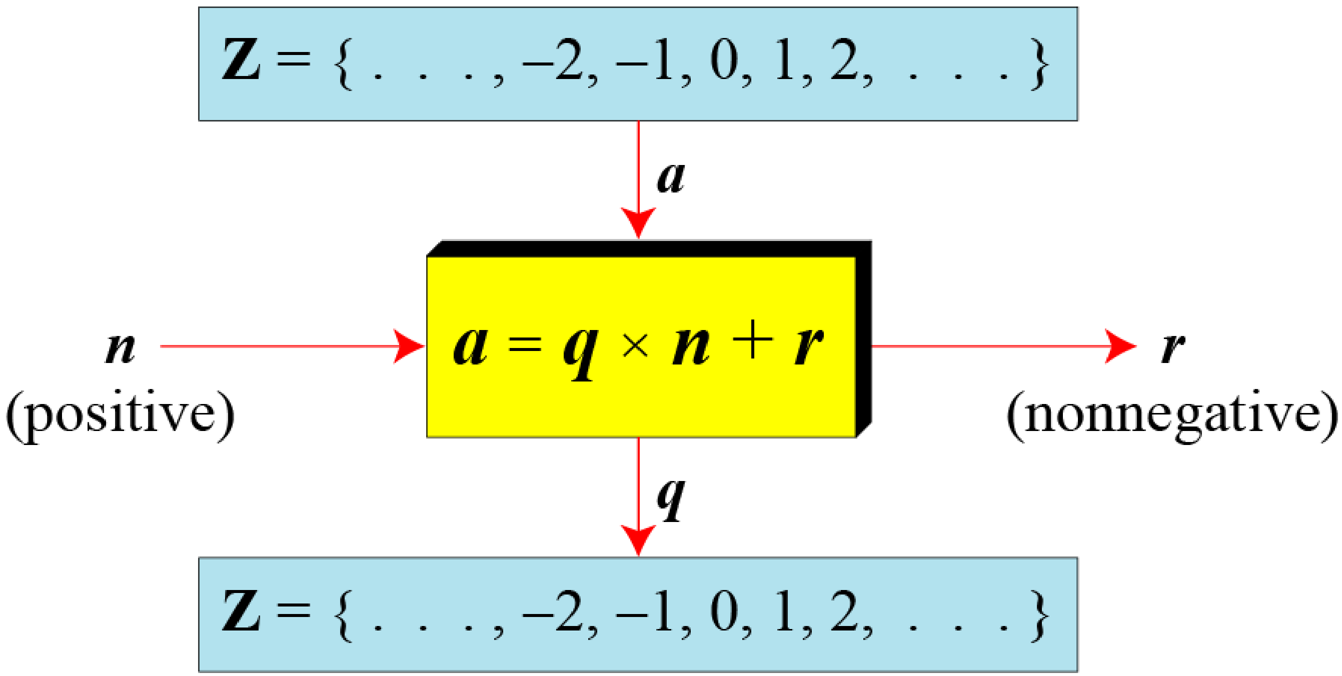


Figure: Division algorithm for integers

Integer Division

Example:

- When we use a computer or a calculator, r and q are negative when a is negative.
- How can we apply the restriction that r needs to be positive?
- The solution is simple, we decrement the value of q by 1 and we add the value of n to r to make it positive.

$$-255 = (\underbrace{-\mathbf{23}}_{q} \times \overbrace{11}^{n}) + \overbrace{(-\mathbf{2})}^{r} \quad \leftrightarrow \quad -255 = (\underbrace{-\mathbf{24}}_{q = q-1} \times 11) + \overbrace{\mathbf{9}}^{r = n + r}$$

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Divisibility

Division relation is: $a = q \times n + r$

Where
- a → dividend
- n → divisor
- q → quotient
- r → remainder

If a is not zero and we let $r = 0$ in the division relation, we get:

$a = q \times n$

We then say that
- n divides a
- or, n is a divisor of a
- or, a is divisible by n

Therefore, when a is divisible by n and we are not interested in the value of q, we can write the above relation as $a|n$

If a is not divisible by n (i.e. if r is not zero), then we can write the above relation as $a \nmid n$

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Example :

a. The integer 4 divides the integer 32 because 32 = 8 × 4. We show this as

$$4 \mid 32$$

b. The number 8 does not divide the number 42 because 42 = 5 × 8 + 2. There is a remainder, the number 2, in the equation. We show this as

$$8 \nmid 42$$

Example:

a. We have $13 \mid 78$, $7 \mid 98$, $-6 \mid 24$, $4 \mid 44$, and $11 \mid (-33)$.

b. We have $13 \nmid 27$, $7 \nmid 50$, $-6 \nmid 23$, $4 \nmid 41$, and $11 \nmid (-32)$.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Properties of Divisibility

***Property 1**:* if $a|1$, then $a = \pm 1$.

***Property 2**:* if $a|b$ and $b|a$, then $a = \pm b$.

Property 3: if $a|b$ and $b|c$, then $a|c$.
Example:
Since $3|15$ and $15|45$, then according to this property, $3|45$

***Property 4**:* if $a|b$ and $a|c$, then
$a|(m \times b + n \times c)$, where m
and n are arbitrary integers
Example:
Since $3|15$ and $3|9$, then according to this property,
$3|(15x2+9x4)$, which means $3|66$

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

GCD: Greatest Common Divisor

- A positive integer can have more than one divisor. For example, the integer 32 has six divisors: 1, 2, 4, 8, 16, 32.
- We can mention two interesting facts about divisors of positive integers:

Fact 1:

- The integer 1 has only one divisor, itself.

Fact 2:

- Any positive integer has at least two divisors, 1 and itself (but it can have more).

- The greatest common divisor (GCD) of two positive integers is the largest integer that can divide both integers.
- GCD is often needed in cryptography.
- Two positive integers may have many common divisors, but only one is the greatest of them.
- For example, the common divisors of 12 and 140 are: 1, 2, and 4. However, the greatest common divisor is 4.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

GCD: Greatest Common Divisor

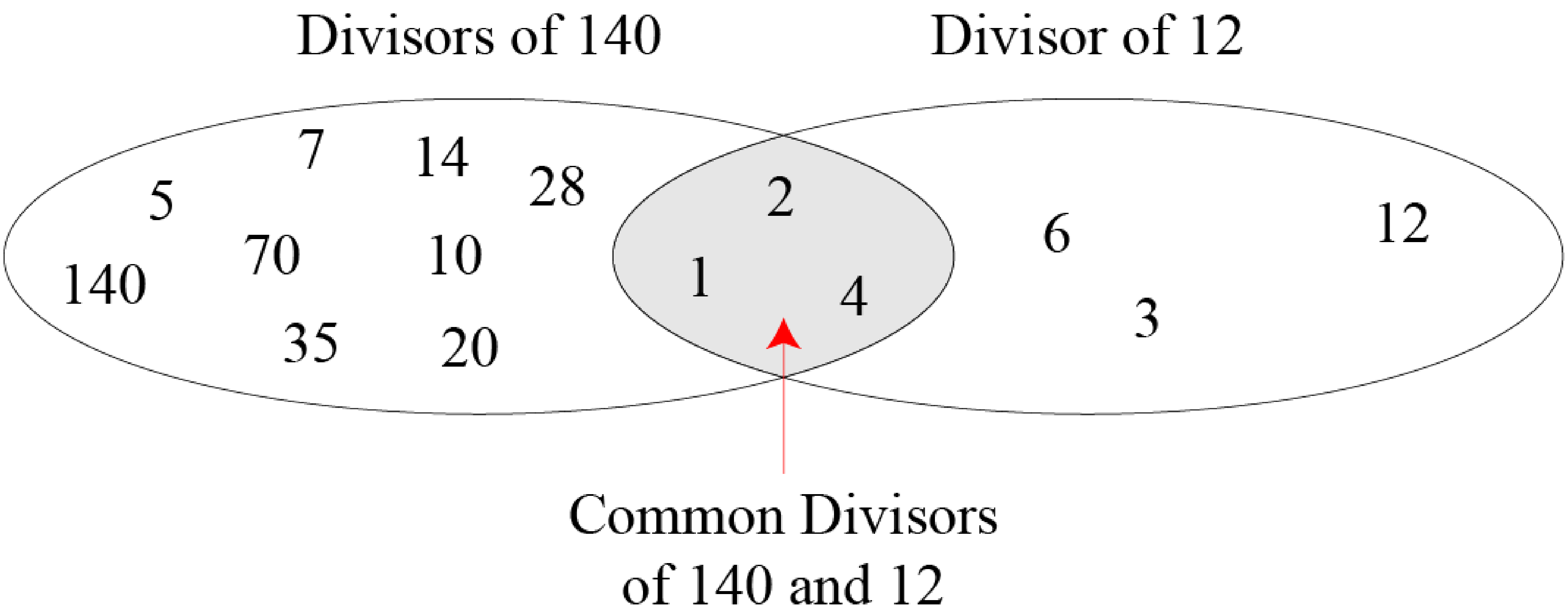


Figure: **Common divisors of two integers**

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

GCD Using Euclidean Algorithm

- Finding the GCD of two positive integers by listing all common divisors is not practical when the two integers are large.

- More than 2000 years ago, a mathematician named Euclid developed an algorithm that can find the GCD of two large positive integers.

- The Euclidian algorithm is based on the two facts:

Fact 1: When 2nd integer is zero, then gcd (a, 0) = a
Example: gcd(5, 0) = 5

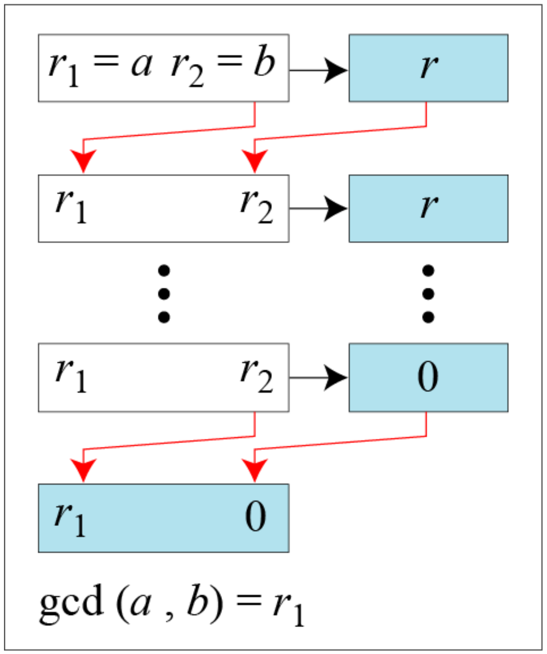
Fact 2: When both integer is positive, then gcd (a, b) = gcd (b, r), where r is the remainder of dividing a by b (here the value of first and second integer is changed until the second integer becomes zero.

Example:
Gcd(36, 10) = gcd(10, 6) = gcd(6, 4) = gcd(4,2) = gcd(2, 0) = 2

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

GCD Using Euclidean Algorithm

- Figure below shows how we use Fact 1 and Fact 2 to calculate gcd (a, b)



a. Process

$$
\begin{aligned}
&r_1 \leftarrow a; \qquad r_2 \leftarrow b; \qquad \text{(Initialization)}\\
&\text{while } (r_2 > 0)\\
&\quad \{\\
&\qquad q \leftarrow r_1 \,/\, r_2;\\
&\qquad r \leftarrow r_1 - q \times r_2;\\
&\qquad r_1 \leftarrow r_2; \quad r_2 \leftarrow r;\\
&\quad \}\\
&\text{gcd } (a, b) \leftarrow r_1
\end{aligned}
$$

b. Algorithm

Figure: Euclidean Algorithm

Note:

- When gcd (a, b) = 1, we say that a and b are relatively prime or they are coprime.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

GCD Using Euclidean Algorithm

Example:

Find the greatest common divisor of 2740 and 1760.

Solution:

We have gcd (2740, 1760) = 20.

q	r_1	r_2	r
1	2740	1760	980
1	1760	980	780
1	980	780	200
3	780	200	180
1	200	180	20
9	180	20	0
	20	0	

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

GCD Using Euclidean Algorithm

Example:

Find the greatest common divisor of 25 and 60.

Solution:

We have gcd (25, 60) = 5.

q	r_1	r_2	r
0	25	60	25
2	60	25	10
2	25	10	5
2	10	5	0
	5	0	

Note:

- The above example shows that it does not matter if the first number is smaller than the second number. We immediately get our correct ordering gcd(60, 25).

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Extended Euclidean Algorithm

- Given two integers *a* and *b*, we often need to find other two integers, *s* and *t*, such that

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

- The extended Euclidean algorithm can calculate the gcd (*a*, *b*) and at the same time calculate the value of *s* and *t*.

- Using extended Euclidean algorithm, we also can find the solutions to the linear Diophantine equations of two variables, an equation of type $ax + by = c$.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Extended Euclidean Algorithm

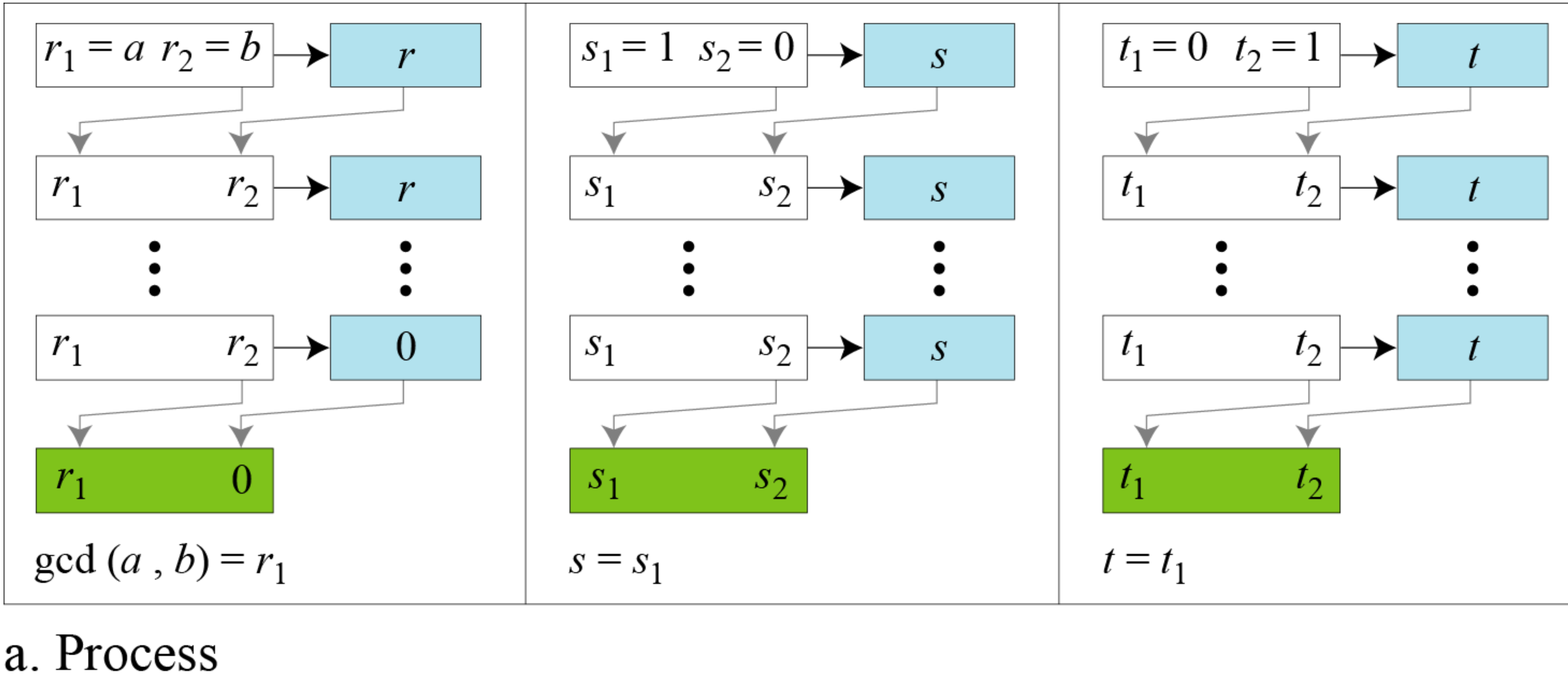


Figure: Extended Euclidean algorithm, part a: Process

Note:

- Figure shows that the extended Euclidean algorithm uses the same number of steps as the Euclidean algorithm, however, in each step, we use three sets of calculations and exchanges instead of one.
- Here, three sets of variables are used: r's, s's and t's.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Extended Euclidean Algorithm

$$r_1 \leftarrow a; \quad r_2 \leftarrow b;$$
$$s_1 \leftarrow 1; \quad s_2 \leftarrow 0;$$
$$t_1 \leftarrow 0; \quad t_2 \leftarrow 1;$$

(Initialization)

while ($r_2 > 0$)

{

$q \leftarrow r_1 / r_2;$

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

(Updating r's)

$$s \leftarrow s_1 - q \times s_2;$$
$$s_1 \leftarrow s_2; \; s_2 \leftarrow s;$$

(Updating s's)

$$t \leftarrow t_1 - q \times t_2;$$
$$t_1 \leftarrow t_2; \; t_2 \leftarrow \text{t};$$

(Updating t's)

}

gcd $(a, b) \leftarrow r_1; \; s \leftarrow s_1; \; t \leftarrow t_1$

b. Algorithm

Figure: Extended Euclidean algorithm, part b: Algorithm

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Extended Euclidean Algorithm

Example:

Given a = 161 and b = 28, find gcd (a, b) and the values of s and t such that gcd(a, b) = s × a + t × b.

Solution: $r = r_1 - q \times r_2 \quad s = s_1 - q \times s_2 \quad t = t_1 - q \times t_2$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
5	161	28	21	1	0	1	0	1	−5
1	28	21	7	0	1	−1	1	−5	6
3	21	7	0	1	−1	4	−5	6	−23
	7	0		**−1**	4		**6**	−23	

We get gcd (161, 28) = 7, *s* = −1 and *t* = 6.

The result can be tested, because (-1) × 161 + 6 × 28 = 7

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Extended Euclidean Algorithm

Example:

Given a = 17 and b = 0, find gcd (a, b) and the values of s and t.

Solution:

We get gcd (17, 0) = 17, s = 1, and t = 0.

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
	17	0		**1**	**0**		**0**	**1**	

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Extended Euclidean Algorithm

Example:

Given $a = 0$ and $b = 45$, find gcd (a, b) and the values of s and t.

Solution:

We get gcd (0, 45) = 45, $s = 0$, and $t = 1$.

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
0	0	45	0	1	0	1	0	1	0
	45	0		0	1		**1**	0	

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Modular Arithmetic

- Given any positive integer ***n*** and any nonnegative integer ***a***, if we divide ***a*** by ***n***, we get an integer quotient ***q*** and an integer remainder ***r*** such that $a = q \times n + r$.

- This division relation has two inputs (*a* and *n*) and two outputs (*q* and *r*).

- In modular arithmetic, we are interested in only one of the outputs, the remainder *r*. In other words, we want to know what is the value of *r* when we divide *a* by *n*. This implies that, using modular arithmetic, we can change the division relation into a binary operator (called modulo operator) with two inputs *a* and *n* and one output r.

- Several important cryptosystems make use of modular arithmetic.

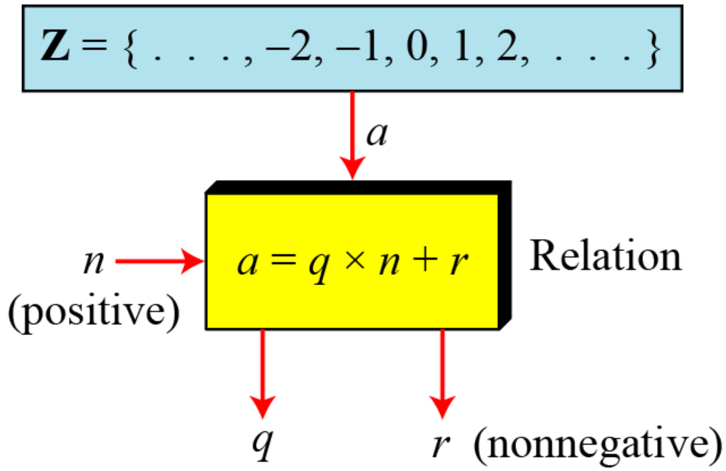
Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Modular Arithmetic

- The modulo operator is shown as mod. The second input (n) is called the modulus. The output r is called the residue.

- Figure below shows the division relation compared with the modulo operator.

Figure: Division relation Vs. modulo operator



- In the figure we see that the modulo operator (mod) takes an integer (a) from the set of integers ($\mathbf{Z}$) and a positive modulus (n). The operator creates a non-negative residue (r) where $0 <= r <= n-1$. We can say that:

$$a \bmod n = r$$

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Modular Arithmetic

Calculation of a mod n:

There are three cases:

Case-1: When both of *a* and *n* is positive integer where *a*<*n*:

In this case, we add as many multiples of ***n*** with ***a*** as necessary to get ***a*** greater than ***n***. Then divide ***a*** by ***n*** to get the remainder ***r***. The result will be in the range ***0*** to ***n-1***.
For example, *2 mod 7 = 9 mod 7 = 2.*

Case-2: When both of *a* and *n* is positive integer where *a*>=*n*:

In this case, just divide ***a*** by ***n*** to get the remainder ***r***. The result will be in the range ***0*** to ***n-1***.
For example, *9 mod 7 = 2.*

Case-3: When *a* is negative and *n* is positive integer:

In this case, we add as many multiples of ***n*** with ***a*** as necessary to get ***a*** positive and greater than ***n.*** Then divide ***a*** by ***n*** to get the remainder ***r***. The result will be in the range ***0*** to ***n-1***. The process is known as modulo reduction.
For example, *-12 mod 7 = -5 mod 7 = 2 mod 7 = 9 mod 7*

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Modular Arithmetic

Example:

Find the result of the following operations:

a. 27 mod 5

b. 36 mod 12

c. −18 mod 14

d. −7 mod 10

Solution:

a. Dividing 27 by 5 results in r = 2. Therefore 27 mod 5 = 2

b. Dividing 36 by 12 results in r = 0. Therefore 36 mod 12 = 0

c. Dividing −18 by 14 results in r = −4. After adding the modulus (14) with the result to make it non-negative, we have r = -4 + 14 = 10. Therefore -18 mod 14 = 10

d. Dividing −7 by 10 results in r = −7. After adding the modulus (10) with the result to make it non-negative, we have r = -7 + 10 = 3. Therefore −7 mod 10 = 3

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Z_n: Set of Residues

- The result of a mod n is always an integer between 0 and n-1.

- Therefore, the modulo operation creates a set, which in modular arithmetic is referred to as the set of least residues modulo n, or Z_n.

- Figure below shows the set of residues Z_n and three instances of the set of residues Z_2, Z_6, Z_{11}.

$$\mathbf{Z}_n = \{ 0, 1, 2, 3, \ldots, (n-1) \}$$

$$\mathbf{Z}_2 = \{ 0, 1 \} \qquad \mathbf{Z}_6 = \{ 0, 1, 2, 3, 4, 5 \} \qquad \mathbf{Z}_{11} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \}$$

Figure: Some Z_n sets

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Congruence

- The result of 2 mod 10 = 2, 12 mod 10 = 2, 22 mod 10 = 2, 32 mod 10 = 2 and so on.
- In modular arithmetic, integers like 2, 12, 22 and 32 are called congruent mod 10.
- To show that two integers are congruent, we use the congruence operator (≡). For example, we write:

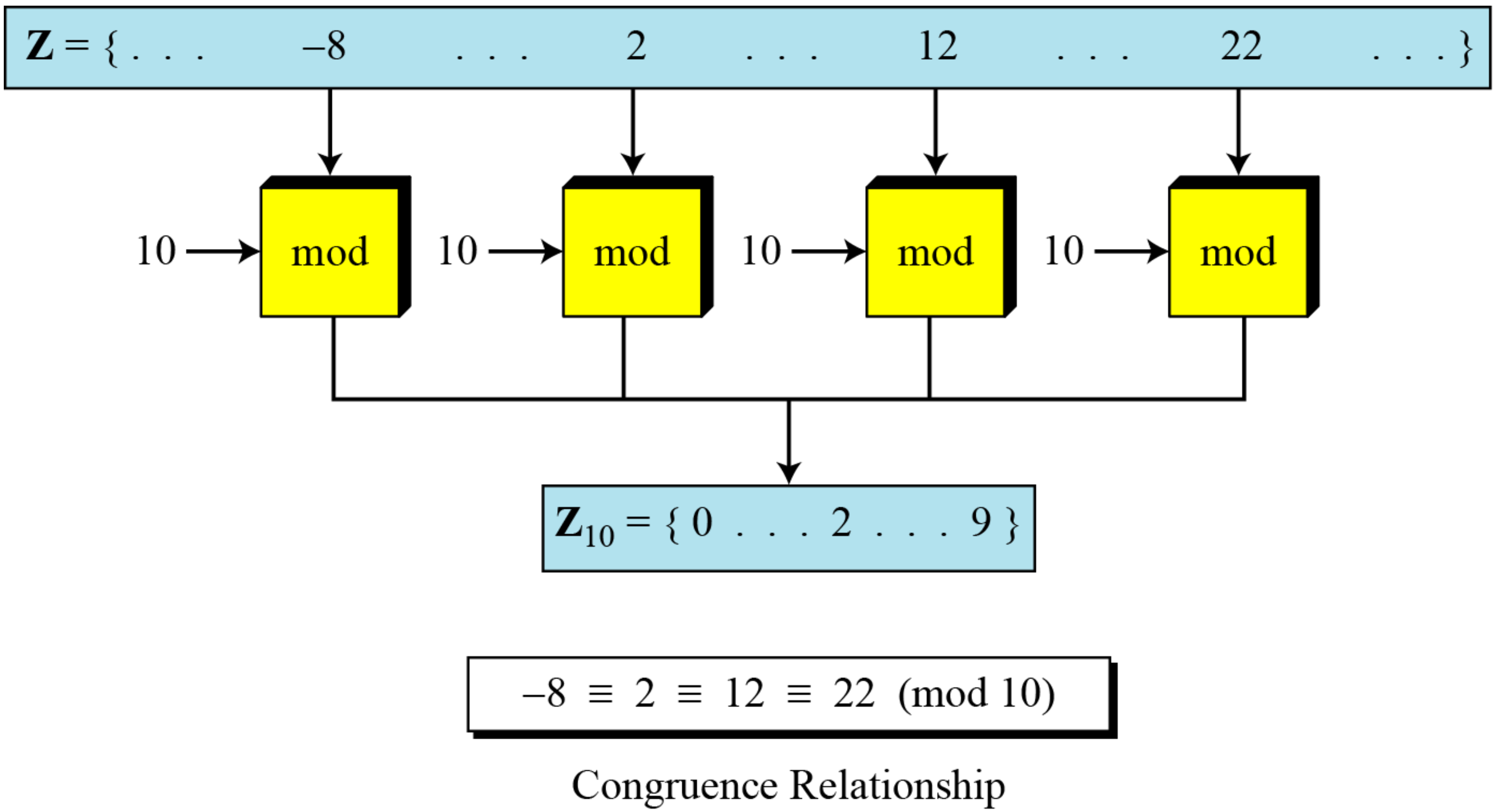
$$2 \equiv 12 \pmod{10} \qquad 13 \equiv 23 \pmod{10}$$
$$3 \equiv 8 \pmod{5} \qquad 8 \equiv 13 \pmod{5}$$

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Congruence

Figure below shows the idea of congruence.

Figure 2.11 ***Concept of congruence***



Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Modular Arithmetic

Residue Sets or Classes:

A residue class *[a]* or $[a]_n$ is the set of integers congruent modulo *n*. That is, a residue class is the set of all integers such that $x = a \pmod{n}$. For example, if $n = 5$, we have five sets of residue classes [0], [1], [2], [3] and [4] as shown below:

$$
\begin{aligned}
[0] &= \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\} \\
[1] &= \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\} \\
[2] &= \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\} \\
[3] &= \{\ldots, -12, -7, -5, 3, 8, 13, 18, \ldots\} \\
[4] &= \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\}
\end{aligned}
$$

Note:

- All the integers in the residue class [0] are reduced to 0 when we apply the modulo 5 operation on them.
- Similarly, all the integers in the residue class [1] are reduced to 1 when we apply the modulo 5 operation on them, and so on.

In each residue set or class, there is one element called the least residue. For example, in set [0], [1], [2], [3] and [4], this element (least residue) is 1, 2, 3, and 4 respectively. The set of all of these least residues is written as $Z_5 = \{0, 1, 2, 3, 4\}$. In other words, the set Z_n is the set of all least residue modulo n.

Modular Arithmetic: Inverse

- In cryptography, we often need to find the inverse of a number relative to an operation e.g., encryption/decryption.
- For example, if the sender uses an integer as the encryption key, the receiver uses the inverse of that integer as the decryption key.
- We are normally looking for two kinds of inverse:
  - **Additive Inverse**
    - If the operation is addition, we are normally looking for additive inverse.
    - The set of additive inverse is expressed as Z_n
  - **Multiplicative Inverse**
    - If the operation is multiplication, we are normally looking for multiplicative inverse.
    - The set of multiplicative inverse is expressed as Z_{n*}

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Modular Arithmetic: Additive Inverse

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

$$a + b \equiv 0 \pmod{n}$$

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

Example:

Find all additive inverse pairs in Z_{10}.

Solution:

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

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Modular Arithmetic: Multiplicative Inverse

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

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

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

Example:

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

Solution:

- There is no multiplicative inverse of 8 in Z_{10} 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.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Modular Arithmetic: Multiplicative Inverse

Example:

Find all multiplicative inverses in Z_{10}.

Solution:

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.

Example:

Find all multiplicative inverse pairs in Z_{11}.

Solution:

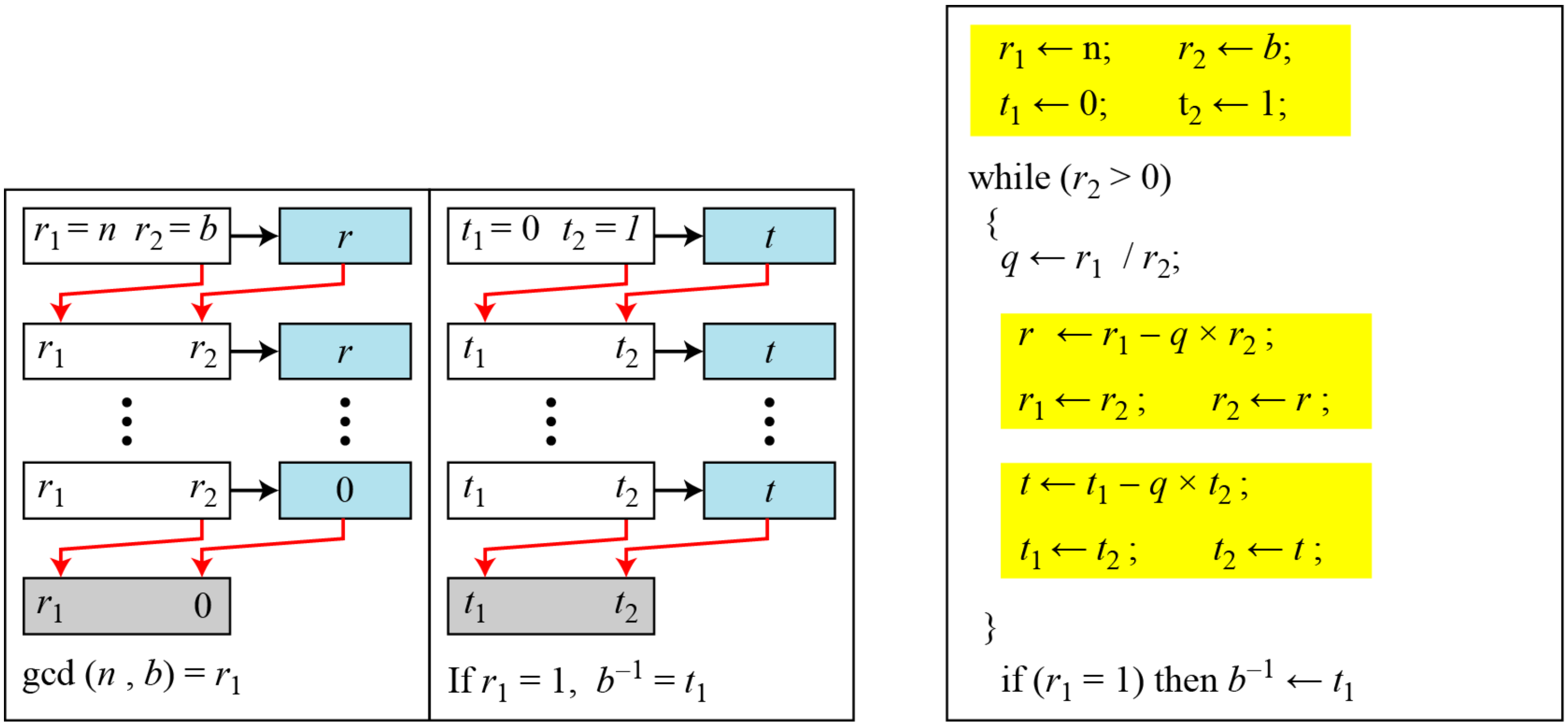
We have seven pairs: (1, 1), (2, 6), (3, 4), (5, 9), (7, 8), (9, 5), and (10, 10).

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Modular Arithmetic: Multiplicative Inverse

Multiplicative Inverse Using Extended Euclidean Algorithm:

- The extended Euclidean algorithm finds the multiplicative inverses of ***b*** in Z_n when ***n*** and ***b*** are given and **gcd (n, b) = 1**.
- The multiplicative inverse of ***b*** is the value of ***t*** after being mapped to Z_n.



a. Process b. Algorithm

Figure: To find multiplicative inverse using extended Euclidean algorithm

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Modular Arithmetic: Multiplicative Inverse

Example-1:

Find the multiplicative inverse of 11 in Z_{26} using extended Euclidean algorithm.

Solution:

q	r_1	r_2	r	t_1	t_2	t
2	26	11	4	0	1	−2
2	11	4	3	1	−2	5
1	4	3	1	−2	5	−7
3	3	1	0	5	−7	26
	1	0		−7	26	

The gcd (26, 11) is 1; the inverse of 11 is -7 or 19.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Modular Arithmetic: Multiplicative Inverse

Example-2:

Find the multiplicative inverse of 23 in Z_{100} using extended Euclidean algorithm

Solution:

q	r_1	r_2	r	t_1	t_2	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	100	

The gcd (100, 23) is 1; the inverse of 23 is -13 or 87.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Modular Arithmetic: Multiplicative Inverse

Example-3:

Find the inverse of 12 in Z_{26} using extended Euclidean algorithm.

Solution:

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; the inverse does not exist.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Modular Arithmetic: Multiplicative Inverse

Multiplicative Inverse Using Fermat's Little Theorem:

- If the modulus is a prime, then multiplicative inverse of an integer can be found quickly without using the Extended Euclidean's algorithm:
  - If ***p*** is a prime and ***a*** is an integer such that ***p*** does not divide ***a*** ($p \nmid a$), then

$$\mathbf{a^{-1} \bmod p = a^{p-2} \bmod p}$$

Example:

Find the multiplicative inverse of 8 in Z_{17} using Fermat's Little Theorem.

Solution:

Since, the modulus 17 is a prime, so according to Fermat's Little theorem,

$$8^{-1} \bmod 17 = 8^{17-2} \bmod 17 = 8^{15} \bmod 17 = 15$$

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Set of Additive and Multiplicative Inverse

Set of Additive Inverse Z_n :

- Z_n is a set that contains all integers from 0 to n-1.
- In Z_n , each integer has an additive inverse. Therefore Z_n can also be used as the set of additive inverse.
- Each member of Z_n has an additive inverse.

Set of Multiplicative Inverse Z_{n*} :

- In Z_n, an integer may or may not have a multiplicative inverse. Only some members of Z_n have a multiplicative inverse.
- Therefore, for multiplication operation, we need another set Z_n* which is a subset of Z_n that includes only those integers from Z_n that have a unique multiplicative inverse.

Note:

- Each member of Z_n has an additive inverse, but only some members of Z_n have a multiplicative inverse.
- On the other hand, Each member of Z_n* has a multiplicative inverse, but only some members of Z_n* have an additive inverse.

Set of Additive and Multiplicative Inverse

Finding the number of elements in Z_n :

- Z_n is a set that contains all integers from 0 to n-1.

Finding the number of elements in Z_{n*} :

- We can determine the number of elements in the set Zn* using Euler's Phi-Function (sometimes called the Euler's Totient function), Φ(n) that finds the number of integers that are both smaller than n and relatively prime to n.
- The following rules helps to find the value of Φ(n):

1. $\phi(1) = 0$.
2. $\phi(p) = p - 1$ if p is a prime.
3. $\phi(m \times n) = \phi(m) \times \phi(n)$ if m and n are relatively prime.
4. $\phi(p^e) = p^e - p^{e-1}$ if p is a prime.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Set of Additive and Multiplicative Inverse

Example-1:

Find the number of elements in Z_{13}* using Euler's Phi-Function.

Solution:

Since 13 is a prime, so according to the second rule,

$$\Phi(13)=(13-1)=12$$

Example-2:

Find the number of elements in Z_{10}* using Euler's Phi-Function.

Solution:

Since 10 is not a prime, so according to the third rule,

$$\Phi(10)= \Phi(5x2)= \Phi(2) \text{ x } \Phi(5)=(2-1) \text{ x } (5-1)= 1 \text{ x } 4 =4$$

Example-3:

Find the number of elements in Z_{49}* using Euler's Phi-Function.

Solution:

Since 49 is not a prime and it can not be factored as the product of two relatively primes, so according to the fourth rule,

$$\Phi(49)= \Phi(7^2)= 7^2 - 7^{2-1}= 49 - 7 = 42$$

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Additive and Multiplicative Inverse Using Multiplication Tables

- Z_n and Z_n* can be made from addition and multiplication tables respectively.
- We need to use Z_n when additive inverses are needed; we need to use Z_n* when multiplicative inverses are needed.

	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 $\mathbf{Z}_{10}$

Figure: ***Addition and multiplication table for Z_{10}***

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Set of Additive and Multiplicative Inverse

Some Instances of Z_n and Z_{n^*}

$Z_6 = \{0, 1, 2, 3, 4, 5\}$

$Z_6^* = \{1, 5\}$

$Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$

$Z_7^* = \{1, 2, 3, 4, 5, 6\}$

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

$Z_{10}^* = \{1, 3, 7, 9\}$

Figure: Some Z_n and Z_{n^*} sets

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Set of Additive and Multiplicative Inverse

Two More Sets: Z_p and Z_{p*} :

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

- The set Z_p is the same as Z_n except that n is a prime.
- Z_p contains all integers from 0 to p-1.
- Each member in Z_p has an additive inverse; each member except 0 has a multiplicative inverse.

- The set Z_{p*} is the same as Z_{n*} except that n is a prime.
- Z_{p*} contains all integers from 1 to p-1.
- Each member in Z_{p*} has an additive and a multiplicative inverse.
- Z_p* is a very good candidate when we need a set that supports both additive and multiplicative inverse.

$$Z_{13} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$
$$Z_{13}* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

Figure: The set Z_p and Z_{p*} when p=13

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Matrices

In cryptography we need to handle matrices. Although this topic belongs to a special branch of algebra called linear algebra, the following brief review of matrices is necessary preparation for the study of cryptography.

Topics discussed in this section:

Definitions
Operations and Relations
Determinants
Residue Matrices

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Matrices

- A matrix is a rectangular array of $l \times m$ elements, in which l is the number of rows and m is the number of columns.
- It is normally denoted with a boldface uppercase letter such as **A**.
- The element a_{ij} is located in the ith row and jth column.

$$\text{Matrix } \mathbf{A}: \quad \begin{array}{cc} & m \text{ columns} \\ l \text{ rows} & \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & & \vdots \\ a_{l1} & a_{l2} & \cdots & a_{lm} \end{bmatrix} \end{array}$$

Figure: ***A matrix of size $l \times m$***

Example of Matrices:

- **Row matrix:**
  If a matrix has only one row (l), then it is called a row matrix.

- **Column matrix:**
  If a matrix has only one column (m), then it is called a column matrix.

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

Row matrix

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

Column matrix

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Example of Matrices:

- **Square matrix:**
  If a matrix has same number of rows and columns ($l = m$), then it is called a square matrix. In a square matrix, the elements a_{11}, a_{22}, ….. ,a_{mm} make the main diagonal.

- **Additive Identity matrix:**
  It is a kind of matrix with all rows and columns set to 0's. It is denoted as **O**.

- **Identity matrix:**
  It is a kind of square matrix with 1's on the main diagonal and 0's elsewhere. It is denoted as **I.**

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

Square matrix

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

0

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

I

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Operations and Relations in Matrices:

In linear algebra, one relation (equality) and four operations (addition, subtraction, multiplication and scalar multiplication) are defined for matrices.

Equality:

Two matrices are equal if they have the same number of rows and columns and the corresponding elements are equal. In other words, **A = B** if we have aij = B_{ij} for all i's and j's.

$$A = \begin{bmatrix} 3 & 5 & 7 \\ 2 & 2 & 1 \\ 1 & 4 & 3 \end{bmatrix} \qquad B = \begin{bmatrix} 3 & 5 & 7 \\ 2 & 2 & 1 \\ 1 & 4 & 3 \end{bmatrix}$$

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Addition and Subtraction:

Two matrices can be added if they have the same number of rows and columns. The resulting matrix has also the same number of rows and columns, e.g. **A + B = C**.

Example:

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

C = A + B

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

D = A − B

Figure: ***Addition and subtraction of matrices***

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Multiplication:

Two matrices can be multiplied if the number of columns of the first matrix is the same as the number of rows of the second matrix. If **A** is an $l \times m$ matrix and **B** is an $m \times p$ matrix, then their product is a matrix **C** of size $l \times p$.

Example: Figure 2.21 shows the product of a row matrix (1 × 3) by a column matrix (3 × 1). The result is a matrix of size 1 × 1.

$$\overset{\mathbf{A}}{\begin{bmatrix} 5 & 2 & 1 \end{bmatrix}} \times \overset{\mathbf{B}}{\begin{bmatrix} 7 \\ 8 \\ 2 \end{bmatrix}} = \overset{\mathbf{C}}{\begin{bmatrix} 53 \end{bmatrix}}$$

$$\boxed{53 = 5 \times 7 + 2 \times 8 + 1 \times 2}$$

Figure: ***Multiplication of a row matrix by a column matrix***

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Example:

Figure 2.22 shows the product of a 2×3 matrix by a 3×4 matrix. The result is a 2×4 matrix.

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

Figure: ***Multiplication of a 2 × 3 matrix by a 3 × 4 matrix***

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Scalar Multiplication:

We can multiply a matrix by a number (called a scalar). If **A** is an $l \times m$ matrix and x is a scalar, then **C = xA** is a matrix of size $l \times m$.

Example:

Figure below shows an example of scalar multiplication.

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

Figure: ***Scalar multiplication***

Transpose of a Matrix:

A matrix which is formed by turning all the rows of a given matrix into columns and vice-versa is called the transpose of the original matrix. The transpose of matrix A is written A^T.

Example:

Suppose, the given matrix is $A = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 1 & 0 & 6 \end{bmatrix}$.

Find the transpose of A.

Solution:

The transpose of matrix A is:

$$A^T = \begin{bmatrix} 1 & 0 & 1 \\ 2 & 4 & 0 \\ 3 & 5 & 6 \end{bmatrix}$$

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Determinant

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

1. If $m = 1$, $\det(\mathbf{A}) = a_{11}$
2. If $m > 1$, $\det(\mathbf{A}) = \sum (-1)^{i+j} \times a_{ij} \times \det(\mathbf{A}_{ij})$

Where $\mathbf{A}_{ij}$ is a matrix obtained from $\mathbf{A}$ by deleting the ith row and jth column.

The determinant is defined only for a square matrix.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Matrices

Example:

Figure below shows how 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

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

Figure: ***Calculating the determinant of a 2 × 2 matrix***

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Example:

Figure below shows the calculation of the determinant of a 3 × 3 matrix.

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

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

Figure: ***Calculating the determinant of a 3 × 3 matrix***

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

More Example

Calculate the determinant of the following matrix.

$$\begin{bmatrix} 2 & -2 & 0 \\ 0 & -2 & -4 \\ 1 & 1 & -1 \end{bmatrix}$$

$$\det\begin{bmatrix} 2 & -2 & 0 \\ 0 & -2 & -4 \\ 1 & 1 & -1 \end{bmatrix}$$

$$= 2\{[(-2)\times(-1)] - [(-4)\times(1)]\} - (-2)\{[(0)\times(-1)] - [(-4)\times(1)]\} + (0)\{[(0)\times(1)] - [(-2)\times(1)]\}$$

$$= 2\{[2] - [-4]\} - (-2)\{[0] - [-4]\} + (0)\{[0] - [-2]\}$$

$$= 2\{2+4\} - (-2)\{0+4\} + (0)\{0+2\}$$

$$= 2\times 6 - (-2\times 4) + 0\times 2$$

$$= 12 + 8 + 0 \quad = 20$$

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Matrices

Cofactor Matrix of a Given Matrix

Example:

Suppose, the given matrix is $A = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 1 & 0 & 6 \end{bmatrix}$. Determine the cofactor matrix of A.

Solution:

First, find the cofactor of each element of matrix A.

$$A_{11} = \begin{vmatrix} 4 & 5 \\ 0 & 6 \end{vmatrix} = 24 \qquad A_{12} = -\begin{vmatrix} 0 & 5 \\ 1 & 6 \end{vmatrix} = 5 \qquad A_{13} = \begin{vmatrix} 0 & 4 \\ 1 & 0 \end{vmatrix} = -4$$

$$A_{21} = -\begin{vmatrix} 2 & 3 \\ 0 & 6 \end{vmatrix} = -12 \qquad A_{22} = \begin{vmatrix} 1 & 3 \\ 1 & 6 \end{vmatrix} = 3 \qquad A_{23} = -\begin{vmatrix} 1 & 2 \\ 1 & 0 \end{vmatrix} = 2$$

$$A_{31} = \begin{vmatrix} 2 & 3 \\ 4 & 5 \end{vmatrix} = -2 \qquad A_{32} = -\begin{vmatrix} 1 & 3 \\ 0 & 5 \end{vmatrix} = -5 \qquad A_{33} = \begin{vmatrix} 1 & 2 \\ 0 & 4 \end{vmatrix} = 4$$

Therefore, the cofactor matrix of A is

$$\boxed{Cofac(A) = \begin{bmatrix} 24 & 5 & -4 \\ -12 & 3 & 2 \\ -2 & -5 & 4 \end{bmatrix}}$$

F..., Associate Professor, IIT, Jahangirnagar University, Dhaka

Adjoint of a Given Matrix

The matrix formed by taking the transpose of the cofactor matrix of a given original matrix is called the adjoint of the given matrix. The adjoint of matrix *A* is often written *adj A*.

Example:

Suppose, the given matrix is $A = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 1 & 0 & 6 \end{bmatrix}$.

Find the adjoint of the above matrix.

Solution:
First, find the cofactor matrix of the given matrix.

In the previous example, we see that the cofactor matrix of A is

$$Cofac(A) = \begin{bmatrix} 24 & 5 & -4 \\ -12 & 3 & 2 \\ -2 & -5 & 4 \end{bmatrix}$$

Finally the adjoint of A is the transpose of the cofactor matrix:

$$Adj\ A = \begin{bmatrix} 24 & -12 & -2 \\ 5 & 3 & -5 \\ -4 & 2 & 4 \end{bmatrix}$$

Prepa… ociate Professor, IIT, Jahangirnagar University, Dhaka

Inverse of Matrix

For an $n \times n$ square matrix A, the inverse of A (written as A^{-1}) is another $n \times n$ square matrix such that when A is multiplied by A^{-1} the result is an $n \times n$ identity matrix I. Not all $n \times n$ matrices are invertible. Non-square matrices do not have inverses.

$$AA^{-1} = A^{-1}A = I$$

- A matrix which is not invertible is sometimes called a singular matrix.
- An invertible matrix is called a nonsingular matrix.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Examples:

For matrix $A = \begin{bmatrix} 4 & 3 \\ 3 & 2 \end{bmatrix}$, its inverse is $A^{-1} = \begin{bmatrix} -2 & 3 \\ 3 & -4 \end{bmatrix}$ since

$$AA^{-1} = \begin{bmatrix} 4 & 3 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} -2 & 3 \\ 3 & -4 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

and $A^{-1}A = \begin{bmatrix} -2 & 3 \\ 3 & -4 \end{bmatrix} \begin{bmatrix} 4 & 3 \\ 3 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

For matrix $A = \begin{bmatrix} 4 & 2 & 1 \\ -2 & -1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$, its inverse is $A^{-1} = \begin{bmatrix} -1 & -2 & 1 \\ -2 & 3 & -2 \\ 1 & 2 & 0 \end{bmatrix}$

because, $\begin{bmatrix} 4 & 2 & 1 \\ -2 & -1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & -2 & 1 \\ -2 & 3 & -2 \\ 1 & 2 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

and $\begin{bmatrix} -1 & -2 & 1 \\ -2 & 3 & -2 \\ 1 & 2 & 0 \end{bmatrix} \begin{bmatrix} 4 & 2 & 1 \\ -2 & -1 & 0 \\ 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Determining the Inverse of Matrix

When A is a 2×2 Matrix:

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. If $ad - bc \neq 0$, then A is invertible and

$$A^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \frac{1}{\det(A)}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

If $ad - bc = 0$, then A is not invertible.

Example-1:

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}^{-1} = \frac{1}{-2}\begin{bmatrix} 4 & -2 \\ -3 & 1 \end{bmatrix} = \begin{bmatrix} -2 & 1 \\ 3/2 & -1/2 \end{bmatrix}$$

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

When A is a 2×2 Matrix:

Example-2:

The inverse of

$$A = \begin{pmatrix} -3 & -1 \\ 0 & -7 \end{pmatrix}$$

is

$$A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} -7 & 1 \\ 0 & -3 \end{pmatrix} = \frac{1}{21} \begin{pmatrix} -7 & 1 \\ 0 & -3 \end{pmatrix} = \begin{pmatrix} -0.33333 & 0.04762 \\ 0 & -0.14286 \end{pmatrix}$$

Check:

$$AA^{-1} = \begin{pmatrix} -3 & -1 \\ 0 & -7 \end{pmatrix} \begin{pmatrix} -0.33333 & 0.04762 \\ 0 & -0.14286 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

When A is an m×m Matrix:

$$A^{-1} = \frac{1}{\det A}(\text{adjoint of } A) \quad \text{or} \quad A^{-1} = \frac{1}{\det A}(\underline{\text{cofactor matrix}} \text{ of } A)^T$$

To find the inverse of an m×m matrix, follow the steps given below:

1. Find the adjoint of the given matrix.

2. Find the determinant of the given matrix.

3. Now, determine the inverse using the above formula.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Example:

Suppose, the given matrix is $A = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 1 & 0 & 6 \end{bmatrix}$.

Find the inverse of A.

Solution:

The adjoint of A is :

$$Adj\ \ A = \begin{bmatrix} 24 & -12 & -2 \\ 5 & 3 & -5 \\ -4 & 2 & 4 \end{bmatrix}$$

The determinant of A is : $Det\ \ A = Det \begin{bmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 1 & 0 & 6 \end{bmatrix} = 22$

The inverse of A is :

$$A^{-1} = \frac{1}{22} \begin{bmatrix} 24 & -12 & -2 \\ 5 & 3 & -5 \\ -4 & 2 & 4 \end{bmatrix} = \begin{bmatrix} 12/11 & -6/11 & -1/11 \\ 5/22 & 3/22 & -5/22 \\ -2/11 & 1/11 & 2/11 \end{bmatrix}.$$

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Additive & Multiplicative Inverse of Matrix

Matrices have both additive and multiplicative inverses.

Additive Inverse of a Matrix:

The additive inverse of a matrix **A** is another matrix **B** such that **A + B = 0**. In other words, we have $a_{ij} = - b_{ij}$ for all values of i and j. Normally the additive inverse of **A** is denoted by **–A**.

Prepared by: ***K M Akkas Ali****, Associate Professor, IIT, Jahangirnagar University, Dhaka*

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Multiplicative Inverse of a Matrix:

The multiplicative inverse of a square matrix **A** is another square matrix **B** such that $\mathbf{A} \times \mathbf{B} = \mathbf{B} \times \mathbf{A} = \mathbf{I}$. Normally the multiplicative inverse of **A** is denoted by $\mathbf{A}^{-1}$.
The multiplicative inverse exists only if the det(A) has a multiplicative inverse in the corresponding set.

Multiplicative inverses are only defined for square matrices.

Residue Matrices

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

Example:

Figure: ***A residue matrix and its multiplicative inverse***

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

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

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

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:

- **Single-Variable Linear Equations**
- **Set of Linear Equations**

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Single-Variable Linear Equations

Equations of the form $ax \equiv b \pmod{n}$ is a single variable linear equation. This type of equation might have no solution or a limited number of solutions.

$\boxed{\text{Assume that the gcd } (a, n) = d.}$

If $d \nmid b$, there is no solution.

If $d \mid b$, there are d solutions.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Linear Congruence

If d|b, we use the following strategy to find the solution to a single-variable linear equation:

1. Reduce the equation by dividing both sides of the equation (including the modulus) by ***d*** where d = gcd (a, n).

2. Multiply both sides of the reduced equation by the multiplicative inverse of ***a*** to find the particular solution x_0.

3. The general solutions are $x = x_0 + k(n/d)$ for $k = 0, 1, \ldots..(d-1)$.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Linear Congruence

Example:

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

Solution

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

Example:

Solve the equation 14 $x \equiv$ 12 (mod 18).

Solution

First we find the gcd (14 and 18) = 2. Since 2 divides 12, we have exactly two solutions.

$$14x \equiv 12 \pmod{18} \rightarrow \quad 7x \equiv 6 \pmod 9 \quad \rightarrow \quad x \equiv 6\ (7^{-1}) \pmod 9$$
$$x_0 = (6 \times 7^{-1}) \bmod 9 = (6 \times 4) \pmod 9 = 6$$
$$x_1 = x_0 + 1 \times (18/2) = 15$$

- Here 4 is the multiplicative inverse of 7 in Z_9. That is, if we multiply 4 and 7 and then divide the result by 9, we get 1 as the remainder.
- Both solutions 6 and 15 satisfy the congruence relation, because (14×6) mod 18 = 12 and also (14×15) mod 18 = 12.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Example:

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

Solution

- 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 give $3x \equiv 2 \pmod{13}$.

- Because gcd (3, 13) = 1, the equation has only one solution, which is:
 $x_0 = (2 \times 3^{-1}) \bmod 13 = (2{\times}9) \bmod 13 = 18 \bmod 13 = 5.$

  Here 9 is the multiplicative inverse of 3 in Z_{13}. We can see that the answer satisfies the original equation:

$$3 \times 5 + 4 \equiv 6 \pmod{13}.$$

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Linear Congruence

Set of Multiple-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.

To solve, we make three matrices:

- The first is the square matrix made from the coefficients of the variables.
- The second is a column matrix made from the variables.
- The third is a column matrix made from the values at the right-hand side of the congruence operator.

Figure : ***Set of linear equations***

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

a. Equations

1st matrix 2nd matrix 3rd matrix

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

b. Interpretation

Multiplicative inverse of the first matrix

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

c. Solution

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Linear Congruence

Example:

Solve the set of following three equations:

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

$$\begin{bmatrix} 3 & 5 & 7 \\ 1 & 4 & 13 \\ 2 & 7 & 3 \end{bmatrix} \qquad \begin{bmatrix} 3 & 5 & 7 \\ 1 & 4 & 13 \\ 2 & 7 & 3 \end{bmatrix}^{-1}$$

Solution

At first, we form a matrix from the coefficients of variables of the equations. The matrix is invertible.
Now, we determine the multiplicative inverse of the matrix.

$$\begin{bmatrix} 3 & 5 & 7 \\ 1 & 4 & 13 \\ 2 & 7 & 3 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} \equiv \begin{bmatrix} 3 \\ 5 \\ 4 \end{bmatrix} \qquad \begin{bmatrix} x \\ y \\ z \end{bmatrix} \equiv \begin{bmatrix} 3 & 5 & 7 \\ 1 & 4 & 13 \\ 2 & 7 & 3 \end{bmatrix}^{-1} \begin{bmatrix} 3 \\ 5 \\ 4 \end{bmatrix}$$

Linear Congruence

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.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka