

BCA: III SEM: VI

**CRYPTOGRAPHY & NETWORK
SECURITY**

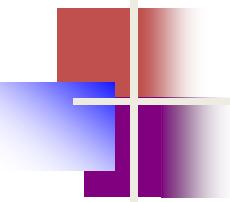
Dr.T.LOGESWARI

DEPT OF COMPUTER SCIENCE

UNIT - I

Introduction

Dr.T.Logeswari



Objectives

- To define three security goals
- To define security attacks that threaten security goals
- To define security services and how they are related to the three security goals
- To define security mechanisms to provide security services
- To introduce two techniques, cryptography and steganography, to implement security mechanisms.

INTRODUCTION

- Computer data often travels from one computer to another, leaving the safety of its protected physical surroundings.
- Once the data is out of hand, people with bad intention could modify or forge your data, either for amusement or for their own benefit.
- Cryptography can reformat and transform our data, making it safer on its trip between computers.

- The technology is based on the essentials of secret codes, augmented by modern mathematics that protects our data in powerful ways.
- Computer Security - generic name for the collection of tools designed to protect data and to frustrate hackers
- Network Security - measures to protect data during their transmission
- Internet Security - measures to protect data during their transmission over a collection of interconnected networks

Cryptography

- **Cryptography is the science of writing in secret code so that no other person except the intended recipient could read**

SECURITY GOALS

- Data Privacy(confidentiality)
- Data Authenticity(it came from where it claims)
- Data integrity(it has not been modified on the way) in the digital world

Figure 1.1 Taxonomy of security goals



- Confidentiality is probably the most common aspect of information security.
- An organization needs to guard against those malicious actions that endanger the confidentiality of its information.
- The meaning of a message is concealed by encoding it
- The sender encrypts the message using a cryptographic key
- The recipient decrypts the message using a cryptographic key that may or may not be the same as the one used by the sender

- Information needs to be changed constantly.
- Integrity means that changes need to be done only by authorized entities and through authorized mechanisms.
(Bank Transaction)

- The information created and stored by an organization needs to be available to authorized entities.
- Information needs to be constantly changed, which means it must be accessible to authorized entities.

Security Attacks, Services and Mechanisms

- To assess the security needs of an organization effectively, the manager responsible for security needs some systematic way of defining the requirements for security and characterization of approaches to satisfy those requirements.
- One approach is to consider three aspects of information security:

- Security attack – Any action that compromises the security of information owned by an organization.
- Security mechanism – A mechanism that is designed to detect, prevent or recover from a security attack.
- Security service – A service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks and they make use of one or more security mechanisms to provide the service.

Cryptographic Attacks

- They are broadly classified as
 - Cryptanalytic attacks
 - Non Cryptanalytic attacks

Types of Cryptanalytic Attacks

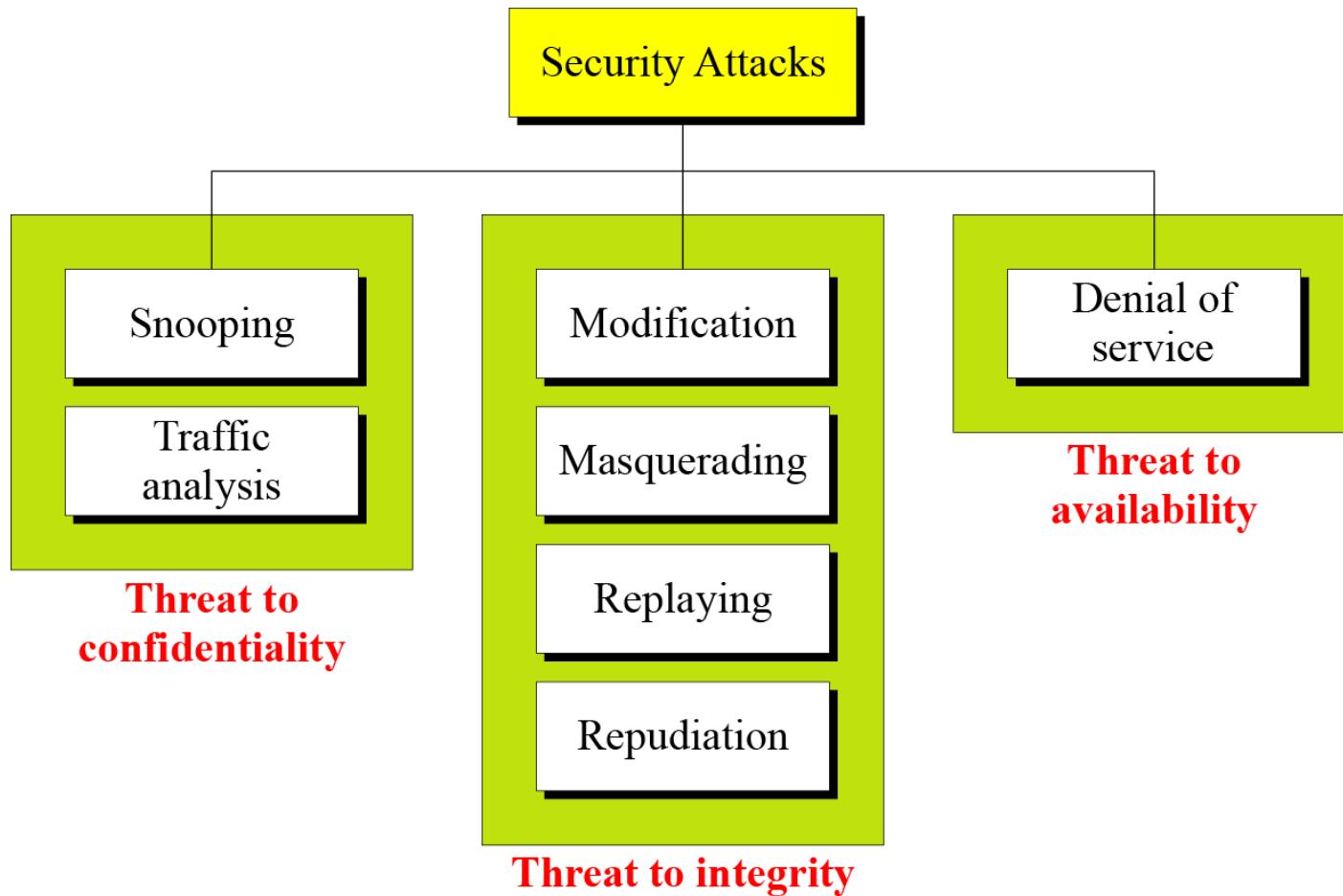
- **ciphertext only**
 - only know algorithm / ciphertext, statistical, can identify plaintext
- **known plaintext**
 - know/suspect plaintext & ciphertext to attack cipher
- **chosen plaintext**
 - select plaintext and obtain ciphertext to attack cipher
- **chosen ciphertext**
 - select ciphertext and obtain plaintext to attack cipher
- **chosen text**
 - select either plaintext or ciphertext to en/decrypt to attack cipher

Non Cryptanalytic Attacks

The three goals of security—confidentiality, integrity, and availability—can be threatened by security attacks.

- Attacks Threatening Confidentiality
- Attacks Threatening Integrity
- Attacks Threatening Availability
- Passive versus Active Attacks

Figure 1.2 Taxonomy of attacks with relation to security goals



Attacks Threatening Confidentiality

- Interception an unauthorized party gains access to an asset. This is an attack on confidentiality.
- Unauthorized party could be a person, a program or a computer .e.g., wire tapping to capture data in the network, illicit copying of files

Snooping refers to unauthorized access to or interception of data.

- Data transferred through internet may be intercepted by unauthorized entity and content may be used for self benefit

Traffic analysis refers to obtaining some other type of information by monitoring online traffic.

Attacks Threatening Integrity

- Modification by an unauthorized party not only gains access to but tampers with an asset.
- This is an attack on integrity. e.g., changing values in data file, altering a program, modifying the contents of messages being transmitted in a network

Modification means that the attacker intercepts the message and changes it.

Masquerading or **spoofing** happens when the attacker impersonates somebody else.

Replaying means the attacker obtains a copy of a message sent by a user and later tries to replay it.

Repudiation means that sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.

Attacks Threatening Availability

- Interruption an asset of the system is destroyed or becomes unavailable or unusable.
- This is an attack on availability
- e.g., destruction of piece of hardware, cutting of a communication line or Disabling of file management system.



Denial of service (DoS) is a very common attack. It may slow down or totally interrupt the service of a system.

Attacks Threatening Authenticity

- Fabrication an unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity. e.g., insertion of spurious message in a network or addition of records to a file.

Passive Attacks

- Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted.
- Passive attacks are of two types:
 - Release of message contents
 - Traffic analysis

- Release of message contents: A telephone conversation, an e-mail message and a transferred file may contain sensitive or confidential information.
- We would like to prevent the opponent from learning the contents of these transmissions.

- Traffic analysis: If we had encryption protection in place, an opponent might still be able to observe the pattern of the message.
- The opponent could determine the location and identity of communication hosts and could observe the frequency and length of messages being exchanged.
- This information might be useful in guessing the nature of communication that was taking place.

Active attacks

- Masquerade – One entity pretends to be a different entity.
- Replay – involves passive capture of a data unit and its subsequent transmission to produce an unauthorized effect.
- Modification of messages – Some portion of message is altered or the messages are delayed or recorded, to produce an unauthorized effect.

- Denial of service – Prevents or inhibits the normal use or management of communication facilities.
- Another form of service denial is the disruption of an entire network, either by disabling the network or overloading it with messages so as to degrade performance.

Table 1.1 Categorization of passive and active attacks

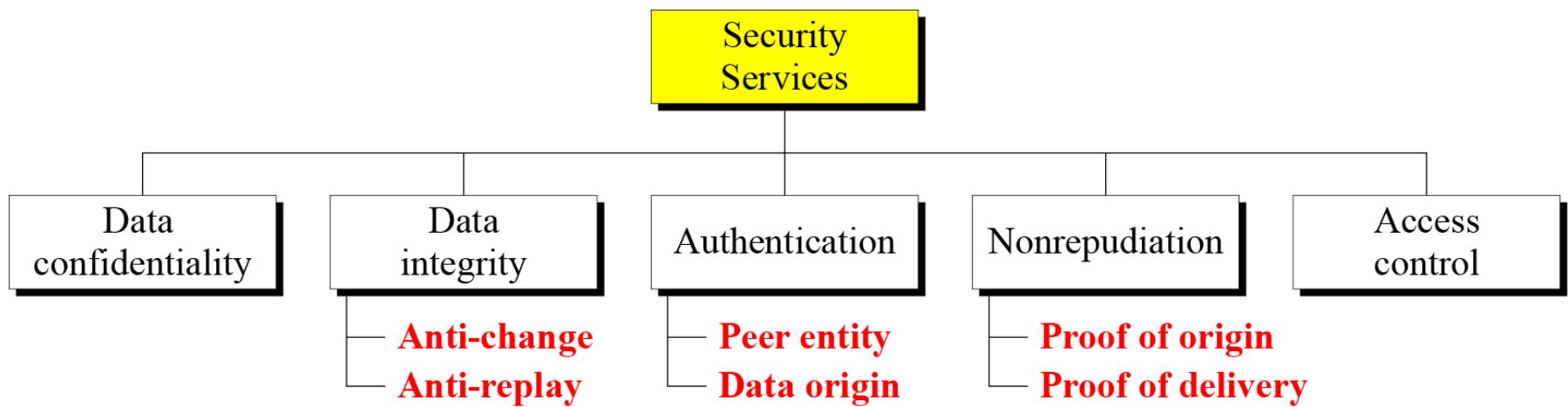
<i>Attacks</i>	<i>Passive/Active</i>	<i>Threatening</i>
Snooping Traffic analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability

SERVICES AND MECHANISMS

ITU-T provides some security services and some mechanisms to implement those services. Security services and mechanisms are closely related because a mechanism or combination of mechanisms are used to provide a service..

- Security Services
- Security Mechanism
- Relation between Services and Mechanisms

Figure 1.3 Security services

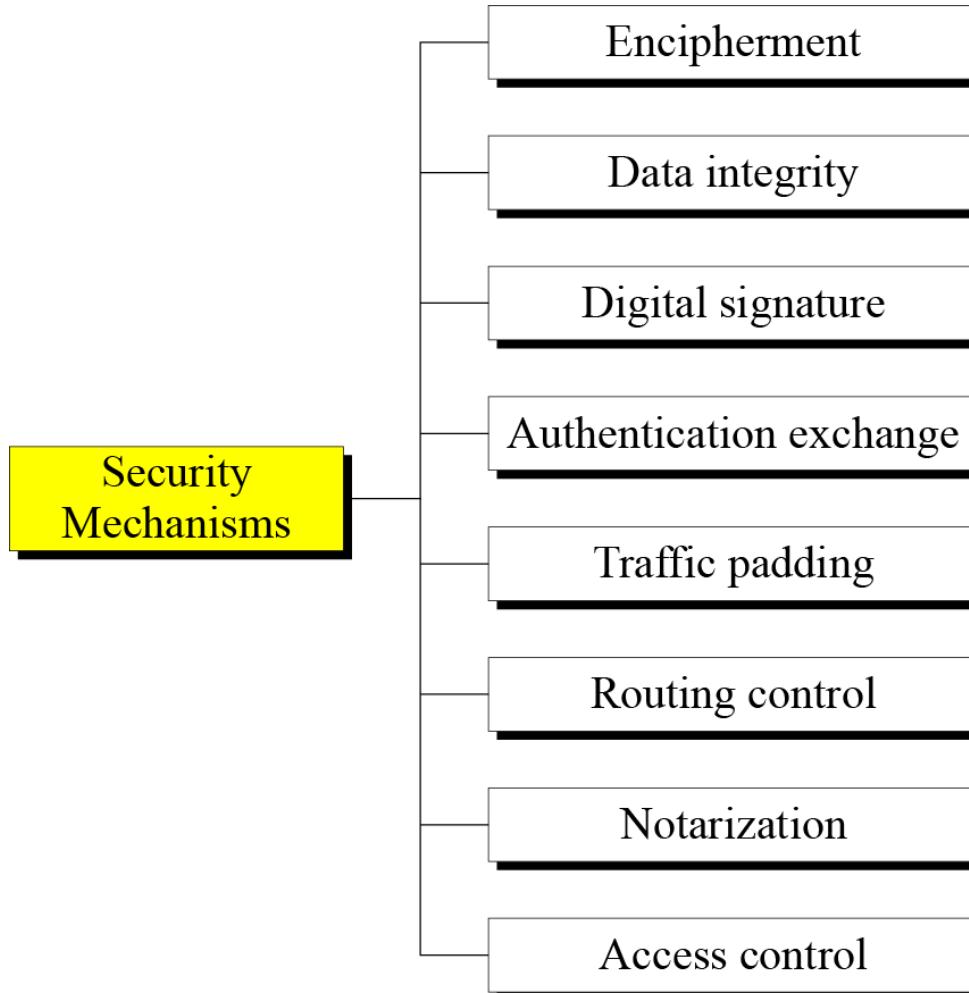


- The classification of security services are as follows:
- Confidentiality: Ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties. E.g. Printing, displaying and other forms of disclosure.
- Authentication: Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.

- Integrity: Ensures that only authorized parties are able to modify computer system assets and transmitted information.
 - Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages.
- Non repudiation: Requires that neither the sender nor the receiver of a message be able to deny the transmission.

- Access control: Requires that access to information resources may be controlled by or the target system.
- Availability: Requires that computer system assets be available to authorized parties when needed.

Figure 1.4 Security mechanisms



- Encipherment
 - It is hiding or covering of data (crypto and steganography)
- Data Integrity
 - This mechanism append to the data a short check value that has been created by a specific process from data itself
- Digital signature
 - The sender electronically sign the data and receiver can electronically verify the signature

- Authentication Exchange
 - Two entities exchange some message to prove their identify to each other
 - Something the user knows(unique secret)
 - Something the user has(security card)
 - Something the user is(fingerprint, retina voice)
- Traffic padding
 - It means inserting some bogus data into a data traffic to thwart the adversary attempt to use the traffic analysis

- Routing Control
 - It means selecting and continuously changing different available routes between the sender and the receiver to prevent eavesdropping
- Notarization
 - It means selecting third trusted party to control the communication between two parties. This can be done to prevent repudiation
- Access Control
 - It uses method to prove that user has right to the data or resources owned by a system

Relation between Services and Mechanisms

Table 1.2 Relation between security services and mechanisms

<i>Security Service</i>	<i>Security Mechanism</i>
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

TECHNIQUES

Mechanisms discussed in the previous sections are only theoretical recipes to implement security. The actual implementation of security goals needs some techniques. Two techniques are prevalent today: cryptography and steganography.

- Cryptography
- Steganography

Cryptography, a word with Greek origins, means “secret writing.”

However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks.

Cryptography

- can be characterized by:
 - type of encryption operations used
 - substitution / transposition / product
 - number of keys used
 - single-key or secret-key vs two-key or public-key
 - way in which plaintext is processed
 - block / stream

Cryptography

- Cryptographic systems are generally classified along 3 independent dimensions:
 - Type of operations used for transforming plain text to cipher text
 - All the encryption algorithms are based on two general principles:
 - substitution, in which each element in the plaintext is mapped into another element.
 - transposition, in which elements in the plaintext are rearranged.

- The number of keys used
 - If the sender and receiver uses same key then it is said to be symmetric key (or) single key (or) conventional encryption.
 - If the sender and receiver use different keys then it is said to be asymmetric key or public key encryption.

- The way in which the plain text is processed
 - A block cipher processes the input and block of elements at a time, producing output block for each input block.
 - A stream cipher processes the input elements continuously, producing output element one at a time, as it goes along.

The word steganography, with origin in Greek, means “covered writing,” in contrast with cryptography, which means “secret writing.”

Example: covering data with text

This book is mostly about cryptography, not steganography.

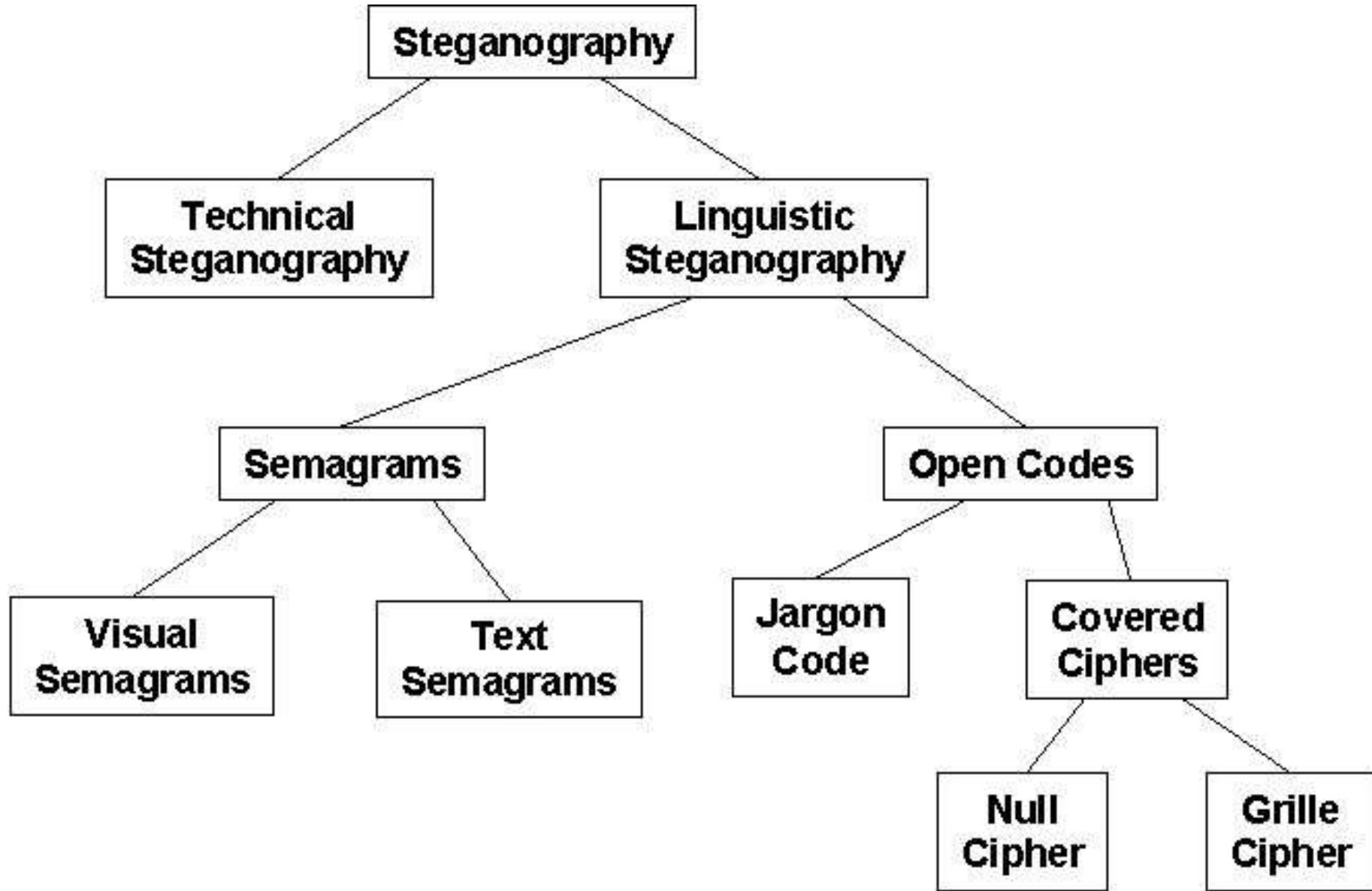
<input type="checkbox"/>							
0	1	0	0	0	0	1	

- .e.g., (i) the sequence of first letters of each word of the overall message spells out the real (Hidden) message.
- (ii) Subset of the words of the overall message is used to convey the hidden message.

Various other techniques

- Character marking – selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held to an angle to bright light.
- Invisible ink – a number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.

- Pin punctures – small pin punctures on selected letters are ordinarily not visible unless the paper is held in front of the light.
- Typewritten correction ribbon – used between the lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light.



Types of steganography

- Technical steganography uses scientific methods to hide a message, such as the use of invisible ink or microdots and other size-reduction methods.
- Linguistic steganography hides the message in the carrier in some nonobvious ways and is further categorized as semagrams or open codes.

- Semagrams hide information by the use of symbols or signs.
- A visual semagram uses innocent-looking or everyday physical objects to convey a message, such as doodles or the positioning of items on a desk or Website.
- A text semagram hides a message by modifying the appearance of the carrier text, such as subtle changes in font size or type, adding extra spaces, or different flourishes in letters or handwritten text.

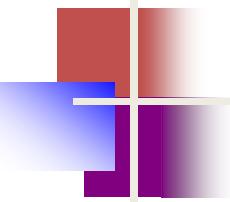
- Open codes hide a message in a legitimate carrier message in ways that are not obvious to an unsuspecting observer.
- The carrier message is sometimes called the overt communication whereas the hidden message is the covert communication.
- This category is subdivided into jargon codes and covered ciphers.

- Jargon code, as the name suggests, uses language that is understood by a group of people but is meaningless to others.
- A subset of jargon codes is cue codes, where certain prearranged phrases convey meaning.

- Covered or concealment ciphers hide a message openly in the carrier medium so that it can be recovered by anyone who knows the secret for how it was concealed.
- A grille cipher employs a template that is used to cover the carrier message. The words that appear in the openings of the template are the hidden message.
- A null cipher hides the message according to some prearranged set of rules, such as "read every fifth word" or "look at the third character in every word."

Mathematics of Cryptography

Part I: Modular Arithmetic, Congruence,
and Matrices



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 solve linear congruent equations, and to find the multiplicative inverses
- To emphasize the importance of modular arithmetic and the modulo operator, because they are extensively used in cryptography
- 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

2-1 INTEGER ARITHMETIC

In integer arithmetic, we use a set and a few operations. You are familiar with this set and the corresponding operations, but they are reviewed here to create a background for modular arithmetic.

Topics discussed in this section:

- 2.1.1 Set of Integers
- 2.1.2 Binary Operations
- 2.1.3 Integer Division
- 2.1.4 Divisibility
- 2.1.5 Linear Diophantine Equations

2.1.1 Set of Integers

The set of integers, denoted by \mathbb{Z} , contains all integral numbers (with no fraction) from negative infinity to positive infinity (Figure 2.1).

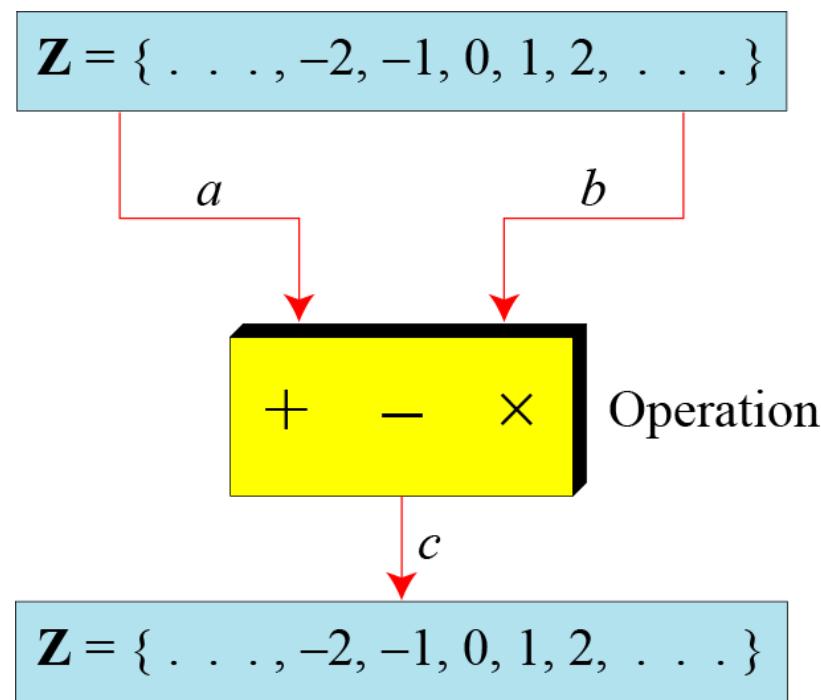
Figure 2.1 The set of integers

$$\mathbb{Z} = \{ \dots, -2, -1, 0, 1, 2, \dots \}$$

2.1.2 Binary Operations

In cryptography, we are interested in three binary operations applied to the set of integers. A binary operation takes two inputs and creates one output.

Figure 2.2 Three binary operations for the set of integers



2.1.2 Continued

Example 2.1

The following 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:	$5 \times 9 = 45$	$(-5) \times 9 = -45$	$5 \times (-9) = -45$	$(-5) \times (-9) = 45$

2.1.3 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

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

2.1.3 Continued

Example 2.2

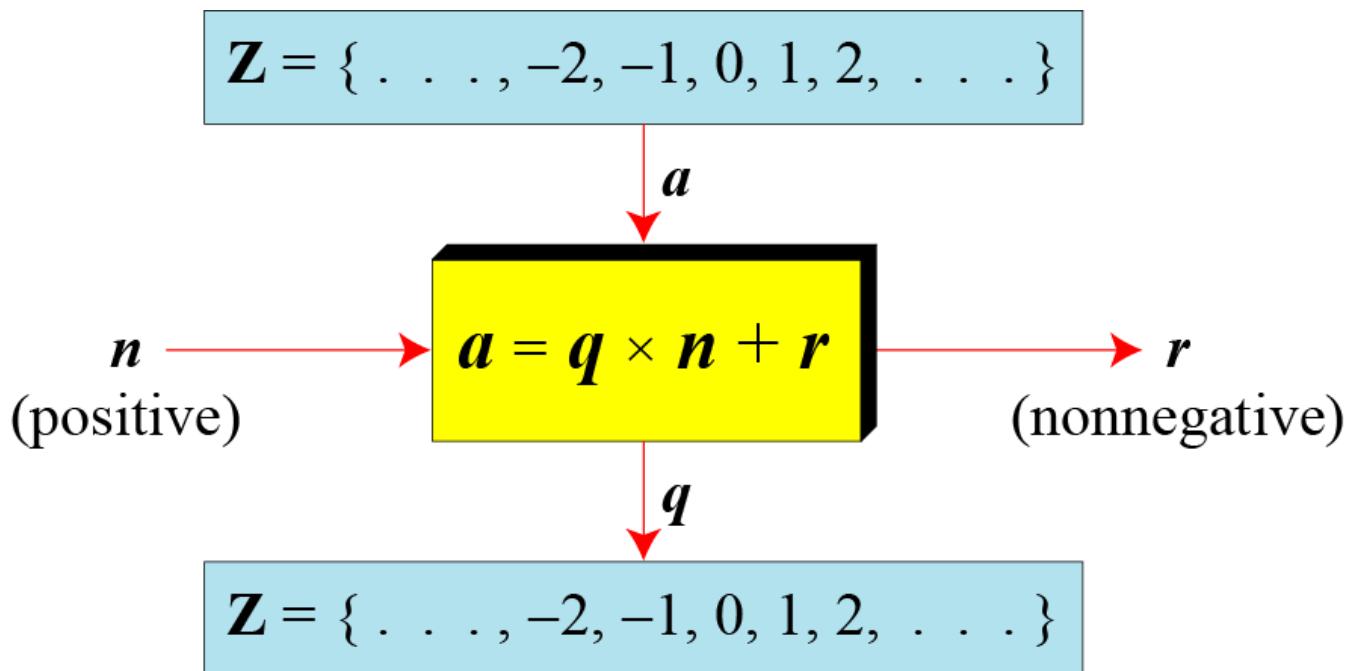
Assume that $a = 255$ and $n = 11$. We can find $q = 23$ and $R = 2$ using the division algorithm.

Figure 2.3 Example 2.2, finding the quotient and the remainder

$$\begin{array}{r} 23 \xleftarrow{q} \\[-1ex] \overline{)255 \xleftarrow{a} \quad 22} \\[-1ex] 35 \\[-1ex] 33 \\[-1ex] \hline 2 \xleftarrow{r} \end{array}$$

Restriction on integer division relation

Figure 2.4 Division algorithm for integers



2.1.3 Continued

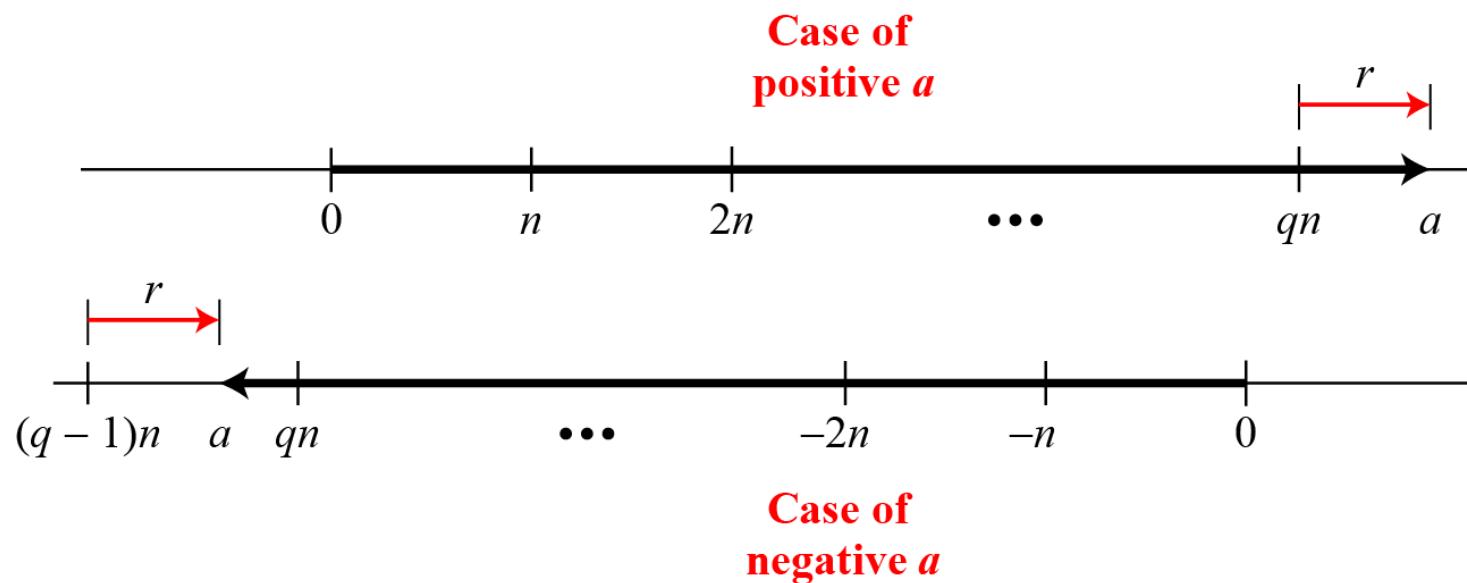
Example 2.3

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.

$$-255 = (-23 \times 11) + (-2) \leftrightarrow -255 = (-24 \times 11) + 9$$

2.1.3 Continued

Figure 2.5 Graph of division algorithm



2.1.4 Divisibility

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

$$a = q \times n$$

If the remainder is zero, $a | n$

If the remainder is not zero, $a \nmid n$

2.1.4 Continued

Example 2.4

- a. The integer 4 divides the integer 32 because $32 = 8 \times 4$. We show this as

$$4|32$$

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

$$8\nmid42$$

2.1.4 Continued

Properties

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 $a|c$.

Property 4: if $a|b$ and $a|c$, then
 $a|(m \times b + n \times c)$, where m
and n are arbitrary integers

2.1.4 Continued

Example 2.5

- a. We have $13|78$, $7|98$, $-6|24$, $4|44$, and $11|-33$.

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

2.1.4 Continued

Example 2.6

- a. Since $3|15$ and $15|45$,
according to the third property, $3|45$.

- b. Since $3|15$ and $3|9$,
according to the fourth property,
 $3|(15 \times 2 + 9 \times 4)$, which means $3|66$.

2.1.4 Continued

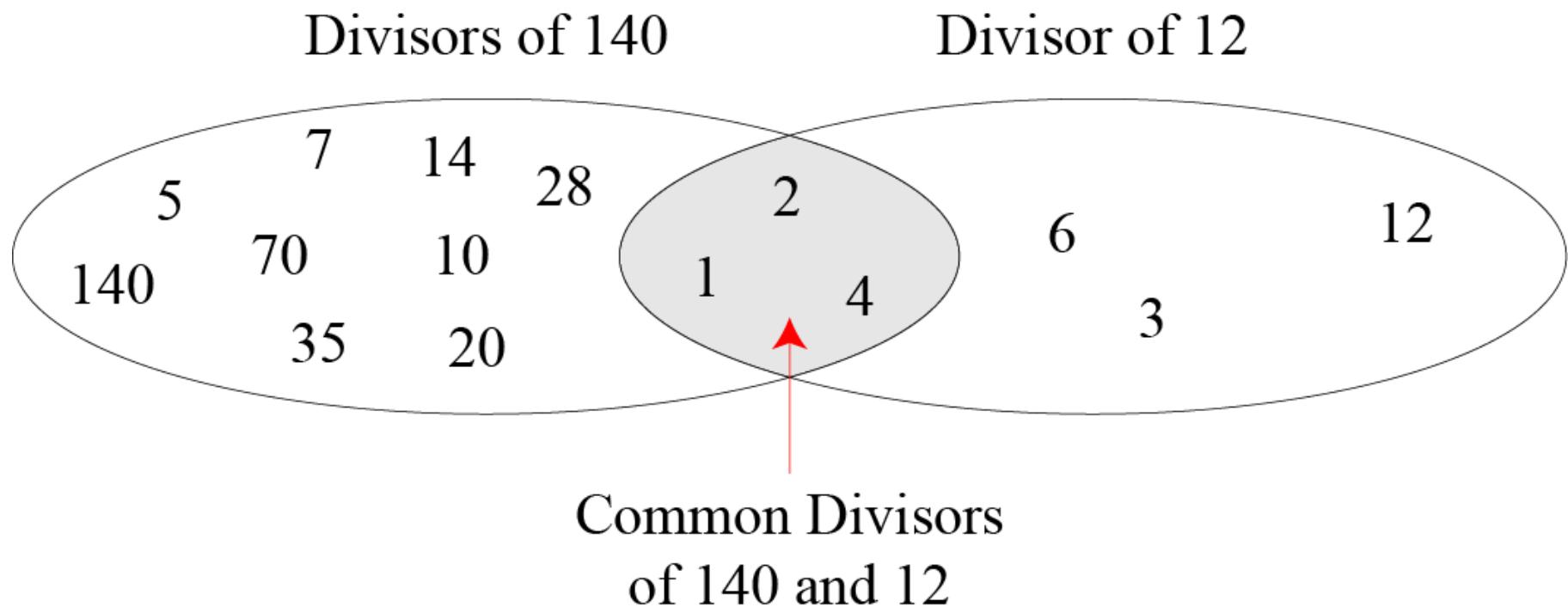
Note

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).

2.1.4 Continued

Figure 2.6 Common divisors of two integers



2.1.4 Continued

Note Greatest Common Divisor

The greatest common divisor of two positive integers is the largest integer that can divide both integers.

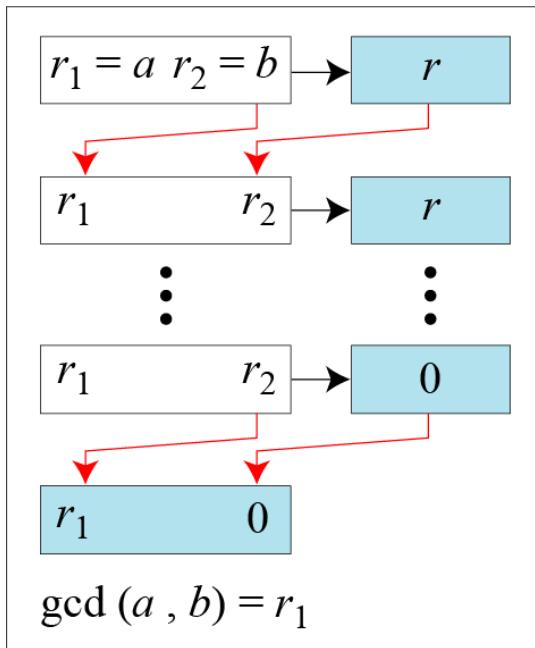
Note Euclidean Algorithm

Fact 1: $\gcd(a, 0) = a$

Fact 2: $\gcd(a, b) = \gcd(b, r)$, where r is the remainder of dividing a by b

2.1.4 Continued

Figure 2.7 Euclidean Algorithm



a. Process

```
 $r_1 \leftarrow a; \quad r_2 \leftarrow b;$  (Initialization)  
while ( $r_2 > 0$ )  
{  
     $q \leftarrow r_1 / r_2;$   
     $r \leftarrow r_1 - q \times r_2;$   
     $r_1 \leftarrow r_2; \quad r_2 \leftarrow r;$   
}  
 $\gcd(a, b) \leftarrow r_1$ 
```

b. Algorithm

Note

When $\gcd(a, b) = 1$, we say that a and b are relatively prime.

2.1.4 Continued

Note

When $\gcd(a, b) = 1$, we say that a and b are relatively prime.

2.1.4 Continued

Example 2.7

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	

2.1.4 Continued

Example 2.8

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	

2.1.4 Continued

Extended Euclidean Algorithm

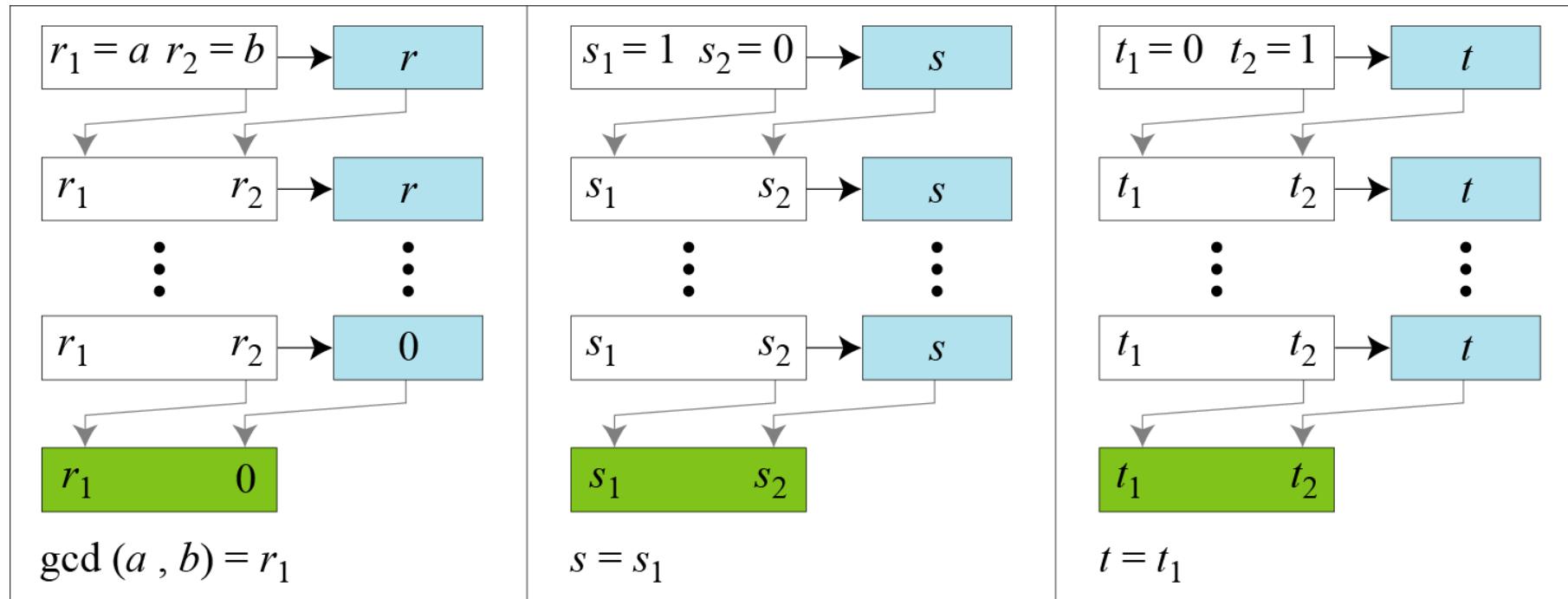
Given two integers a and b , we often need to find other two integers, s and t , such that

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

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

2.1.4 Continued

Figure 2.8.a Extended Euclidean algorithm, part a



a. Process

2.1.4 Continued

Figure 2.8.b Extended Euclidean algorithm, part b

```
r1 ← a;      r2 ← b;  
s1 ← 1;      s2 ← 0;  
t1 ← 0;      t2 ← 1;
```

(Initialization)

while ($r_2 > 0$)

{

$q \leftarrow r_1 / r_2;$

```
  r ← r1 − q × r2;  
  r1 ← r2; r2 ← r;
```

(Updating r 's)

```
  s ← s1 − q × s2;  
  s1 ← s2; s2 ← s;
```

(Updating s 's)

```
  t ← t1 − q × t2;  
  t1 ← t2; t2 ← t;
```

(Updating t 's)

}

gcd(a, b) ← r₁; s ← s₁; t ← t₁

b. Algorithm

2.1.4 Continued

Example 2.9

Given $a = 161$ and $b = 28$, find $\gcd(a, b)$ and the values of s and t .

Solution

We get $\gcd(161, 28) = 7$, $s = -1$ and $t = 6$.

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	

2.1.4 Continued

Example 2.10

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	

2.1.4 Continued

Example 2.11

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	

2.1.4 Continued

Linear Diophantine Equation

Note

A linear Diophantine equation of two variables is $ax + by = c$.

2.1.4 Continued

Linear Diophantine Equation

Note

Particular solution:

$$x_0 = (c/d)s \text{ and } y_0 = (c/d)t$$

Note

General solutions:

$$x = x_0 + k(b/d) \text{ and } y = y_0 - k(a/d)$$

where k is an integer

2.1.4 Continued

Example 2.12

Find the particular and general solutions to the equation
 $21x + 14y = 35$.

Solution

Particular: $x_0 = 5 \times 1 = 5$ and $y_0 = 5 \times (-1) = -5$

General: $x = 5 + k \times 2$ and $y = -5 - k \times 3$

2.1.4 Continued

Example 2.13

For example, imagine we want to cash a \$100 check and get some \$20 and some \$5 bills. We have many choices, which we can find by solving the corresponding Diophantine equation $20x + 5y = 100$. Since $d = \gcd(20, 5) = 5$ and $5 \mid 100$, the equation has an infinite number of solutions, but only a few of them are acceptable in this case. The general solutions with x and y nonnegative are

$$(0, 20), (1, 16), (2, 12), (3, 8), (4, 4), (5, 0).$$

2-2 MODULAR ARITHMETIC

The division relationship ($a = q \times n + r$) discussed in the previous section 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 .

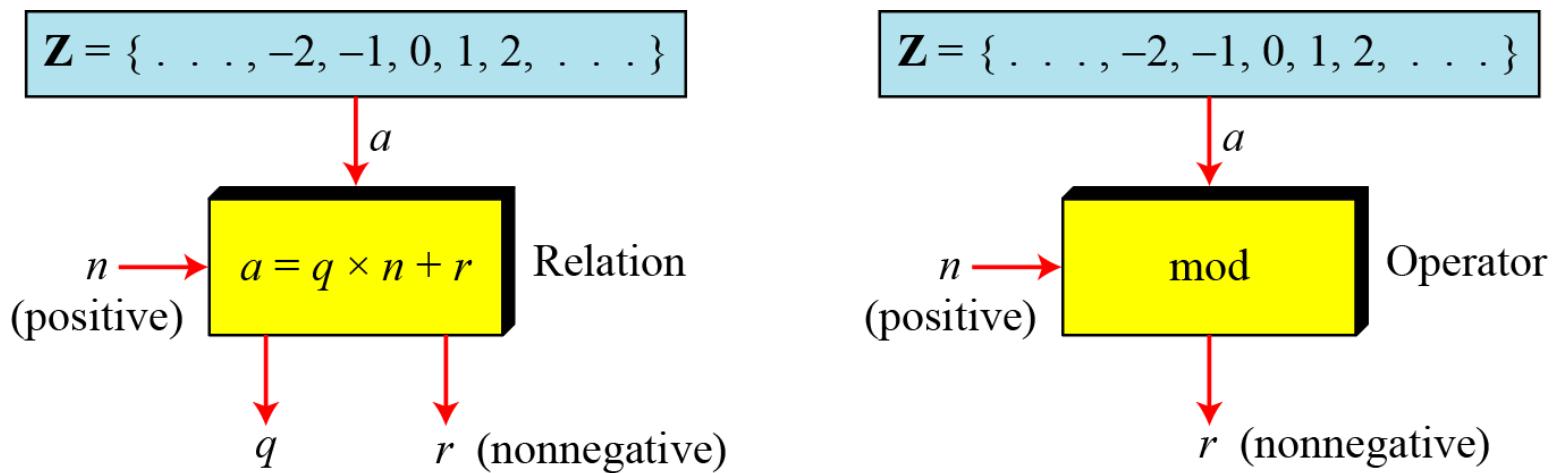
Topics discussed in this section:

- 2.2.1 Modular Operator
- 2.2.2 Set of Residues
- 2.2.3 Congruence
- 2.2.4 Operations in Z_n
- 2.2.5 Addition and Multiplication Tables
- 2.2.6 Different Sets

2.2.1 Modulo Operator

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

Figure 2.9 Division algorithm and modulo operator



2.1.4 Continued

Example 2.14

Find the result of the following operations:

- a. $27 \bmod 5$
- b. $36 \bmod 12$
- c. $-18 \bmod 14$
- d. $-7 \bmod 10$

Solution

- a. Dividing 27 by 5 results in $r = 2$
- b. Dividing 36 by 12 results in $r = 0$.
- c. Dividing -18 by 14 results in $r = -4$. After adding the modulus $r = 10$
- d. Dividing -7 by 10 results in $r = -7$. After adding the modulus to -7 , $r = 3$.

2.2.2 Set of Residues

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 2.10 Some Z_n sets

$$Z_n = \{ 0, 1, 2, 3, \dots, (n - 1) \}$$

$$Z_2 = \{ 0, 1 \}$$

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

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

2.2.3 Congruence

To show that two integers are congruent, we use the congruence operator (\equiv). For example, we write:

$$2 \equiv 12 \pmod{10}$$

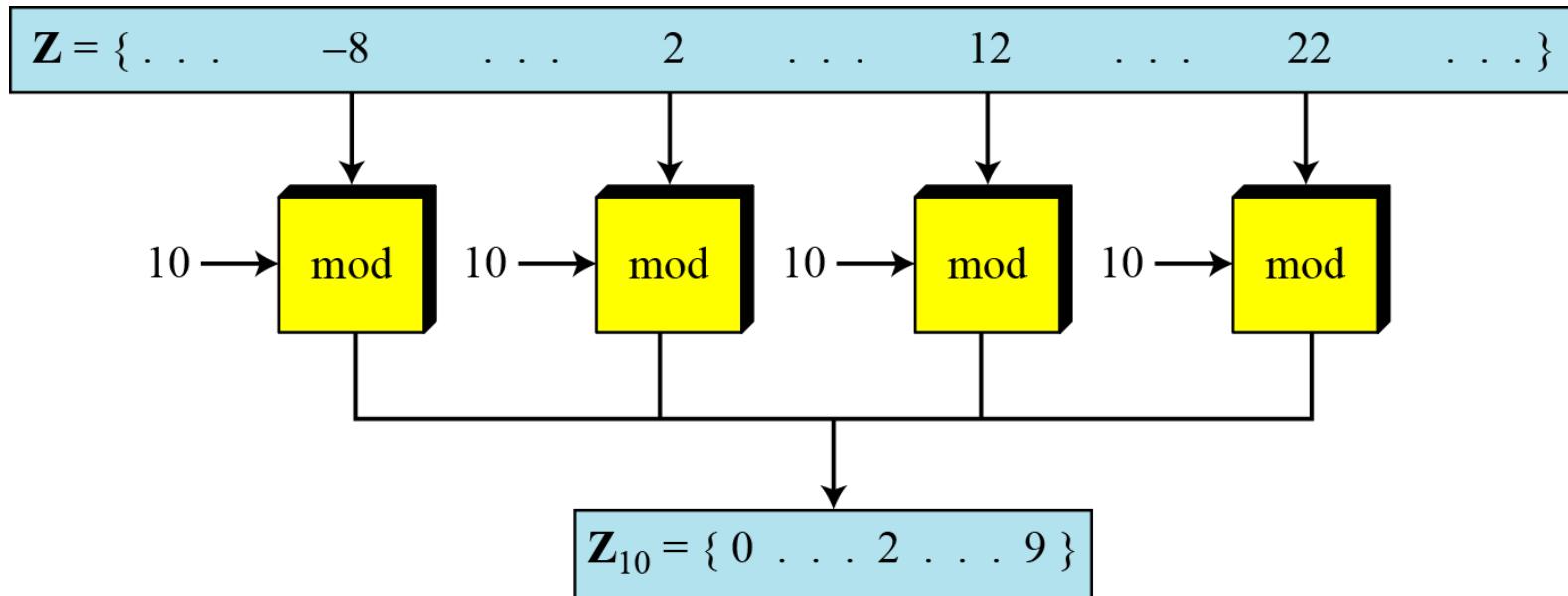
$$3 \equiv 8 \pmod{5}$$

$$13 \equiv 23 \pmod{10}$$

$$8 \equiv 13 \pmod{5}$$

2.2.3 Continued

Figure 2.11 Concept of congruence

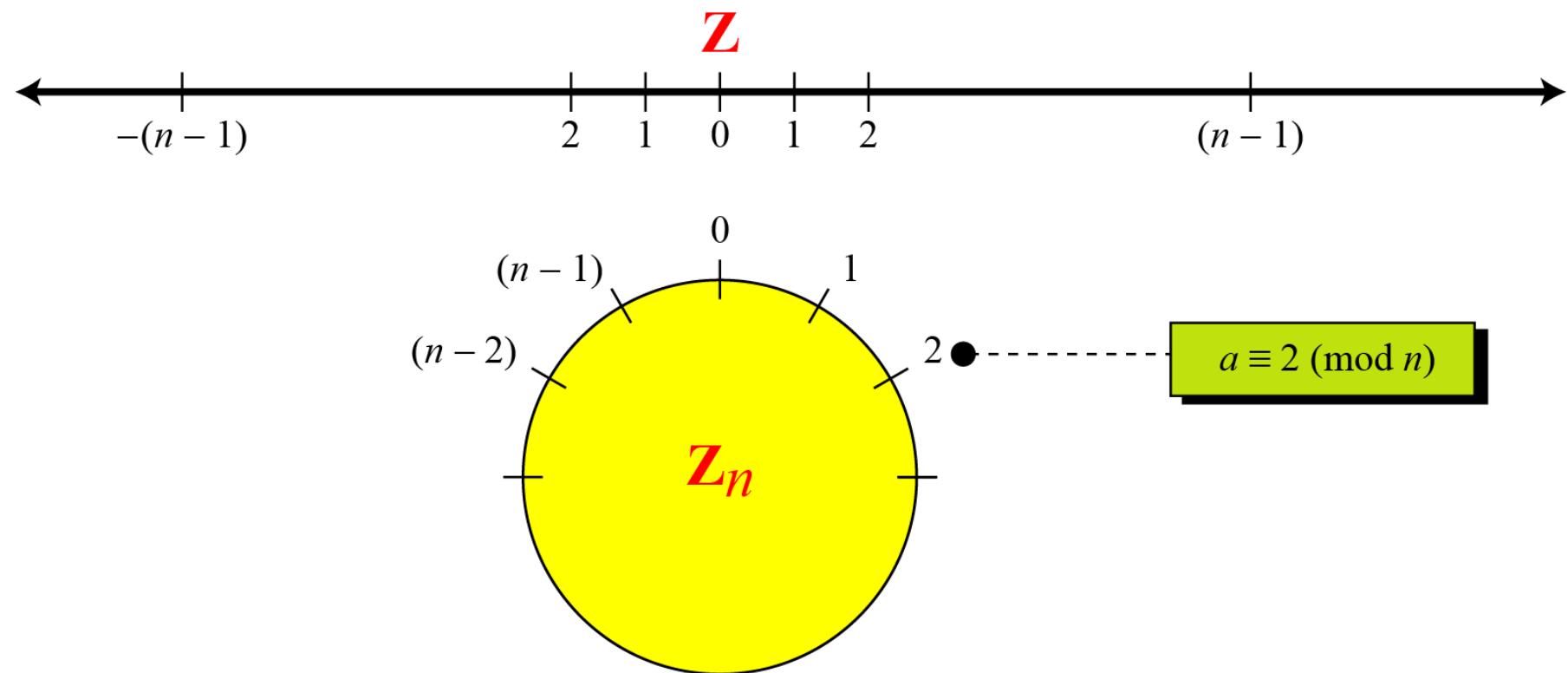


$$-8 \equiv 2 \equiv 12 \equiv 22 \pmod{10}$$

Congruence Relationship

2.2.3 Continued

Figure 2.12 Comparison of Z and Z_n using graphs



2.2.3 Continued

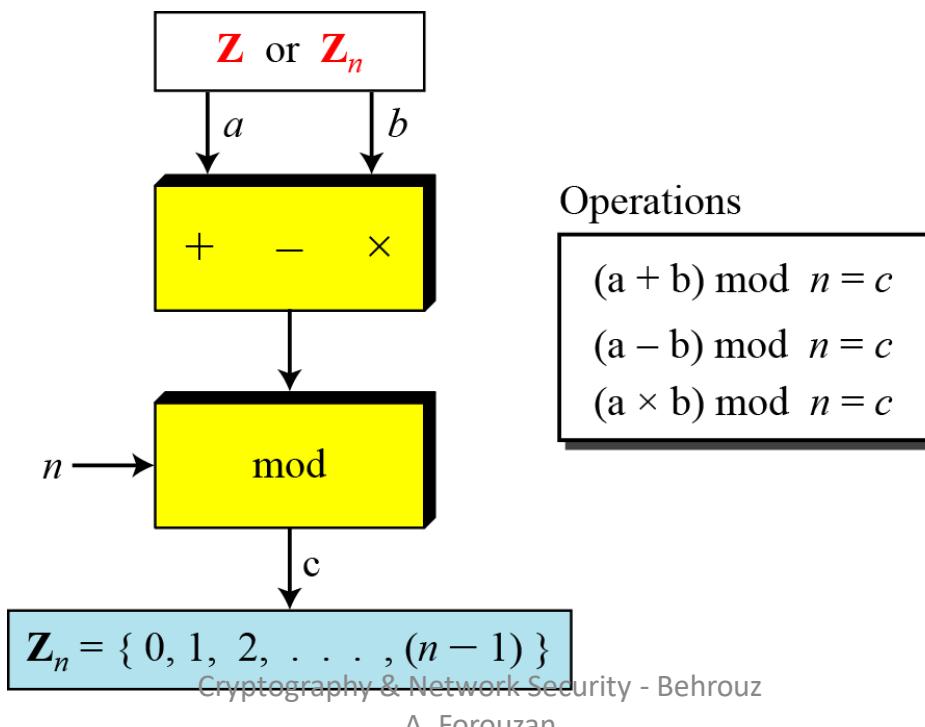
Example 2.15

We use modular arithmetic in our daily life; for example, we use a clock to measure time. Our clock system uses modulo 12 arithmetic. However, instead of a 0 we use the number 12.

2.2.4 Operation in Z_n

The three binary operations that we discussed for the set Z can also be defined for the set Z_n . The result may need to be mapped to Z_n using the mod operator.

Figure 2.13 Binary operations in Z_n



2.2.4 Continued

Example 2.16

Perform the following operations (the inputs come from Z_n):

- Add 7 to 14 in Z_{15} .
- Subtract 11 from 7 in Z_{13} .
- Multiply 11 by 7 in Z_{20} .

Solution

$$(14 + 7) \bmod 15 \rightarrow (21) \bmod 15 = 6$$

$$(7 - 11) \bmod 13 \rightarrow (-4) \bmod 13 = 9$$

$$(7 \times 11) \bmod 20 \rightarrow (77) \bmod 20 = 17$$

2.2.4 Continued

Properties

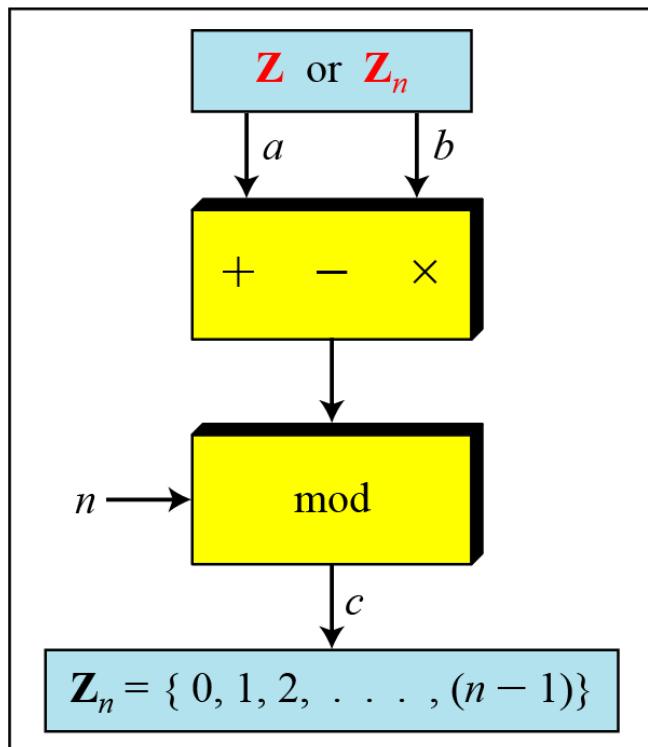
First Property: $(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$

Second Property: $(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$

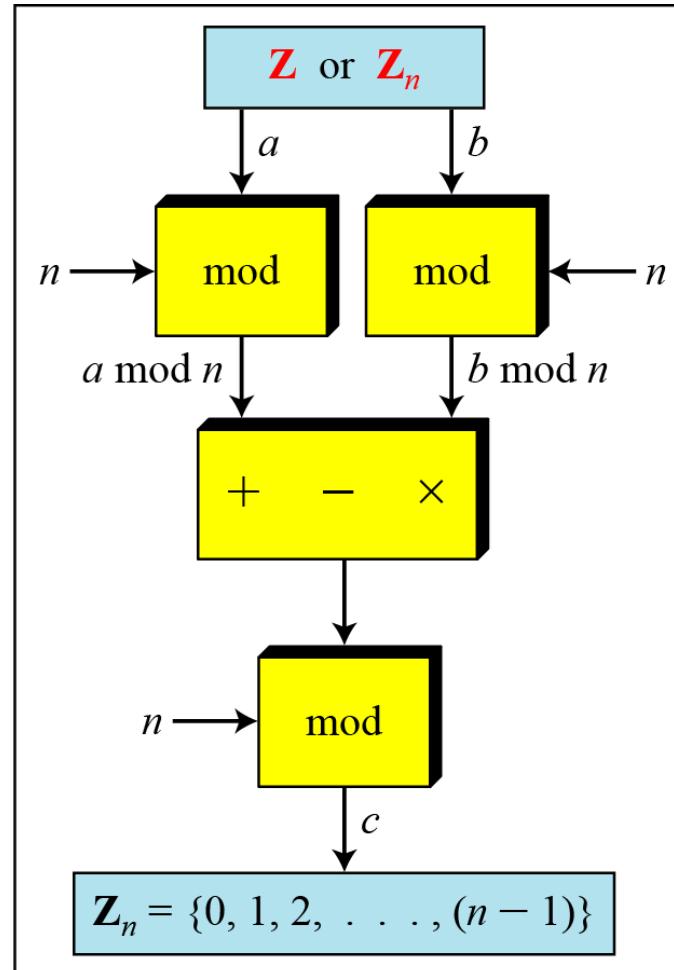
Third Property: $(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

2.2.4 Continued

Figure 2.14 Properties of mode operator



a. Original process



b. Applying properties

2.2.4 Continued

Example 2.18

The following shows the application of the above properties:

$$1. (1,723,345 + 2,124,945) \bmod 11 = (8 + 9) \bmod 11 = 6$$

$$2. (1,723,345 - 2,124,945) \bmod 16 = (8 - 9) \bmod 11 = 10$$

$$3. (1,723,345 \times 2,124,945) \bmod 16 = (8 \times 9) \bmod 11 = 6$$

Or

$$(200+301) \bmod 11 = (2+4)\bmod11 = 6$$

$$(200-301) \bmod 11 = (2-4)\bmod11 = 9$$

$$(200*301) \bmod 11 = (2*4)\bmod11 = 8$$

2.2.5 Inverses

When we are working in modular arithmetic, we often need to find the inverse of a number relative to an operation. We are normally looking for an additive inverse (relative to an addition operation) or a multiplicative inverse (relative to a multiplication operation).

2.2.5 Continue

Additive Inverse

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

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

Note

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

2.2.5 Continued

Example 2.21

Find all additive inverse pairs in \mathbb{Z}_{10} .

Solution

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

2.2.5 Continue

Multiplicative Inverse

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

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

Note

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.

2.2.5 Continued

Example 2.22

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

Solution

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

Example 2.23

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.

2.2.5 Continued

Example 2.24

Find all multiplicative inverse pairs in Z_{11} .

Solution

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

2.2.5 Continued

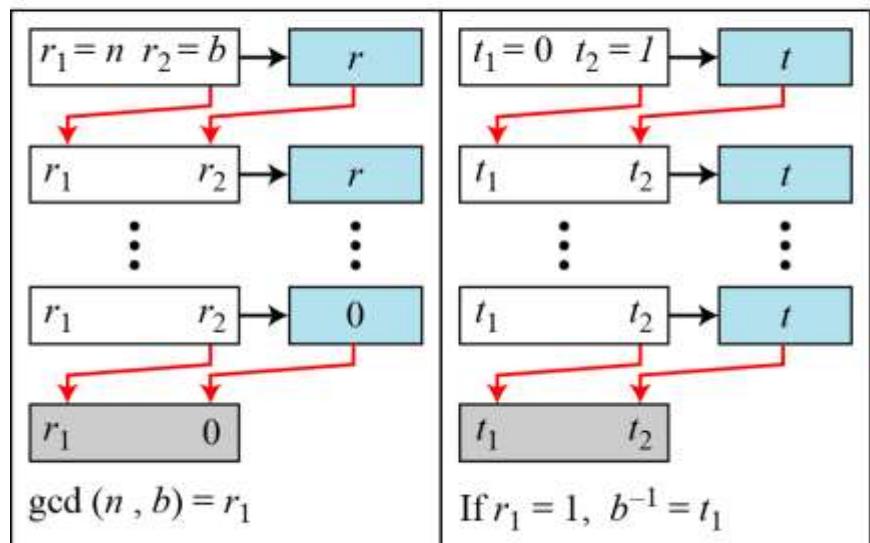
Note

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 .

2.2.5 Continued

Figure 2.15 Using extended Euclidean algorithm to find multiplicative inverse



a. Process

```
r1 ← n;      r2 ← b;  
t1 ← 0;      t2 ← 1;  
  
while (r2 > 0)  
{  
    q ← r1 / r2;  
  
    r ← r1 - q × r2;  
    r1 ← r2;      r2 ← r;  
  
    t ← t1 - q × t2;  
    t1 ← t2;      t2 ← t;  
}  
if (r1 = 1) then b-1 ← t1
```

b. Algorithm

2.2.5 Continued

Example 2.25

Find the multiplicative inverse of 11 in \mathbb{Z}_{26} .

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.

2.2.5 Continued

Example 2.26

Find the multiplicative inverse of 23 in \mathbb{Z}_{100} .

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.

2.2.5 Continued

Example 2.27

Find the inverse of 12 in \mathbb{Z}_{26} .

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.

2.2.6 Addition and Multiplication Tables

Figure 2.16 Addition and multiplication table for \mathbb{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 \mathbb{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 \mathbb{Z}_{10}

2.2.7 Different Sets

Figure 2.17 Some Z_n and Z_n^* sets

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

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

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

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

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

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

Note

We need to use Z_n when additive inverses are needed; we need to use Z_n^* when multiplicative inverses are needed.

2.2.8 Two More Sets

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

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

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

2-3 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:

- 2.3.1 Definitions
- 2.3.2 Operations and Relations
- 2.3.3 Determinants
- 2.3.4 Residue Matrices

2.3.1 Definition

Figure 2.18 A matrix of size $l \times m$

Matrix A:

m columns

$$\begin{matrix} & & & & \\ & & & & \\ & & & & \\ & & & & \\ l \text{ rows} & \left[\begin{array}{ccccc} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ a_{l1} & a_{l2} & \dots & a_{lm} \end{array} \right] & & & \\ & & & & \end{matrix}$$

2.3.1 Continued

Figure 2.19 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

2.3.2 Operations and Relations

Example 2.28

Figure 2.20 shows an example of addition and subtraction.

Figure 2.20 Addition and subtraction of matrices

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

C = A + B

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

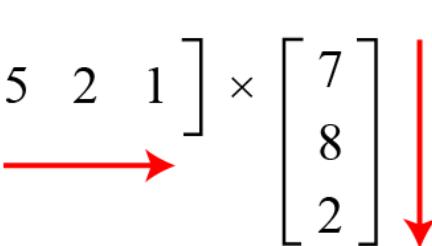
D = A - B

2.3.2 Continued

Example 2.29

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 .

Figure 2.21 Multiplication of a row matrix by a column matrix

$$\begin{matrix} \text{C} & \text{A} & \text{B} \\ \left[\begin{matrix} 5 & 3 \end{matrix} \right] & = & \left[\begin{matrix} 5 & 2 & 1 \end{matrix} \right] \times \left[\begin{matrix} 7 \\ 8 \\ 2 \end{matrix} \right] \end{matrix}$$


In which:

$$53 = 5 \times 7 + 2 \times 8 + 1 \times 2$$

2.3.2 Continued

Example 2. 30

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

Figure 2.22 Multiplication of a 2×3 matrix by a 3×4 matrix

$$\begin{matrix} \mathbf{C} \\ \left[\begin{array}{cccc} 52 & 18 & 14 & 9 \\ 41 & 21 & 22 & 7 \end{array} \right] \end{matrix} = \begin{matrix} \mathbf{A} \\ \left[\begin{array}{ccc} 5 & 2 & 1 \\ 3 & 2 & 4 \end{array} \right] \end{matrix} \times \begin{matrix} \mathbf{B} \\ \left[\begin{array}{cccc} 7 & 3 & 2 & 1 \\ 8 & 0 & 0 & 2 \\ 1 & 3 & 4 & 0 \end{array} \right] \end{matrix}$$

2.3.2 Continued

Example 2.31

Figure 2.23 shows an example of scalar multiplication.

Figure 2.23 Scalar multiplication

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

2.3.3 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 $m = 1$, $\det(A) = a_{11}$
2. If $m > 1$, $\det(A) = \sum_{i=1 \dots m} (-1)^{i+j} \times a_{ij} \times \det(A_{ij})$

Where A_{ij} is a matrix obtained from A by deleting the i th row and j th column.

Note

The determinant is defined only for a square matrix.

2.3.3 Continued

Example 2.32

Figure 2.24 shows how we can calculate the determinant of a 2×2 matrix based on the determinant of a 1×1 matrix.

Figure 2.24 Calculating the determinant of a 2×2 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
$$\det \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = a_{11} \times a_{22} - a_{12} \times a_{21}$$

2.3.3 Continued

Example 2.33

Figure 2.25 shows the calculation of the determinant of a 3×3 matrix.

Figure 2.25 Calculating the determinant of a 3×3 matrix

$$\det \begin{bmatrix} 5 & 2 & 1 \\ 3 & 0 & -4 \\ 2 & 1 & 6 \end{bmatrix} = (-1)^{1+1} \times 5 \times \det \begin{bmatrix} 0 & -4 \\ 1 & 6 \end{bmatrix} + (-1)^{1+2} \times 2 \times \det \begin{bmatrix} 3 & -4 \\ 2 & 6 \end{bmatrix} + (-1)^{1+3} \times 1 \times \det \begin{bmatrix} 3 & 0 \\ 2 & 1 \end{bmatrix}$$
$$= (+1) \times 5 \times (+4) \quad + \quad (-1) \times 2 \times (24) \quad + \quad (+1) \times 1 \times (3) = -25$$

2.3.4 Inverses

Note

Multiplicative inverses are only defined for square matrices.

2.3.5 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 2.34

Figure 2.26 A residue matrix and its multiplicative inverse

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

$$\det(\mathbf{A}) = 21$$

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

2-4 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:

- 2.4.1 Single-Variable Linear Equations
- 2.4.2 Set of Linear Equations

2.4.1 Single-Variable Linear Equations

Equations of the form $ax \equiv b \pmod{n}$ might have no solution or a limited number of solutions.

Assume that the $\gcd(a, n) = d$.

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

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

2.4.1 Continued

Example 2.35

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

Solution

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

Example 2.36

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

Solution

$$14x \equiv 12 \pmod{18} \rightarrow 7x \equiv 6 \pmod{9} \rightarrow x \equiv 6(7^{-1}) \pmod{9}$$

$$x_0 = (6 \times 7^{-1}) \pmod{9} = (6 \times 4) \pmod{9} = 6$$

$$x_1 = x_0 + 1 \times (18/2) = 15$$

2.4.1 Continued

Example 2.37

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 $x_0 = (2 \times 3^{-1}) \pmod{13} = 18 \pmod{13} = 5$. We can see that the answer satisfies the original equation: $3 \times 5 + 4 \equiv 6 \pmod{13}$.

2.4.2 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.

Figure 2.27 Set of linear equations

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

a. Equations

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

b. Interpretation

c. Solution

2.4.2 Continued

Example 2.38

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 $x \equiv 15 \pmod{16}$, $y \equiv 4 \pmod{16}$, and $z \equiv 14 \pmod{16}$. We can check the answer by inserting these values into the equations.