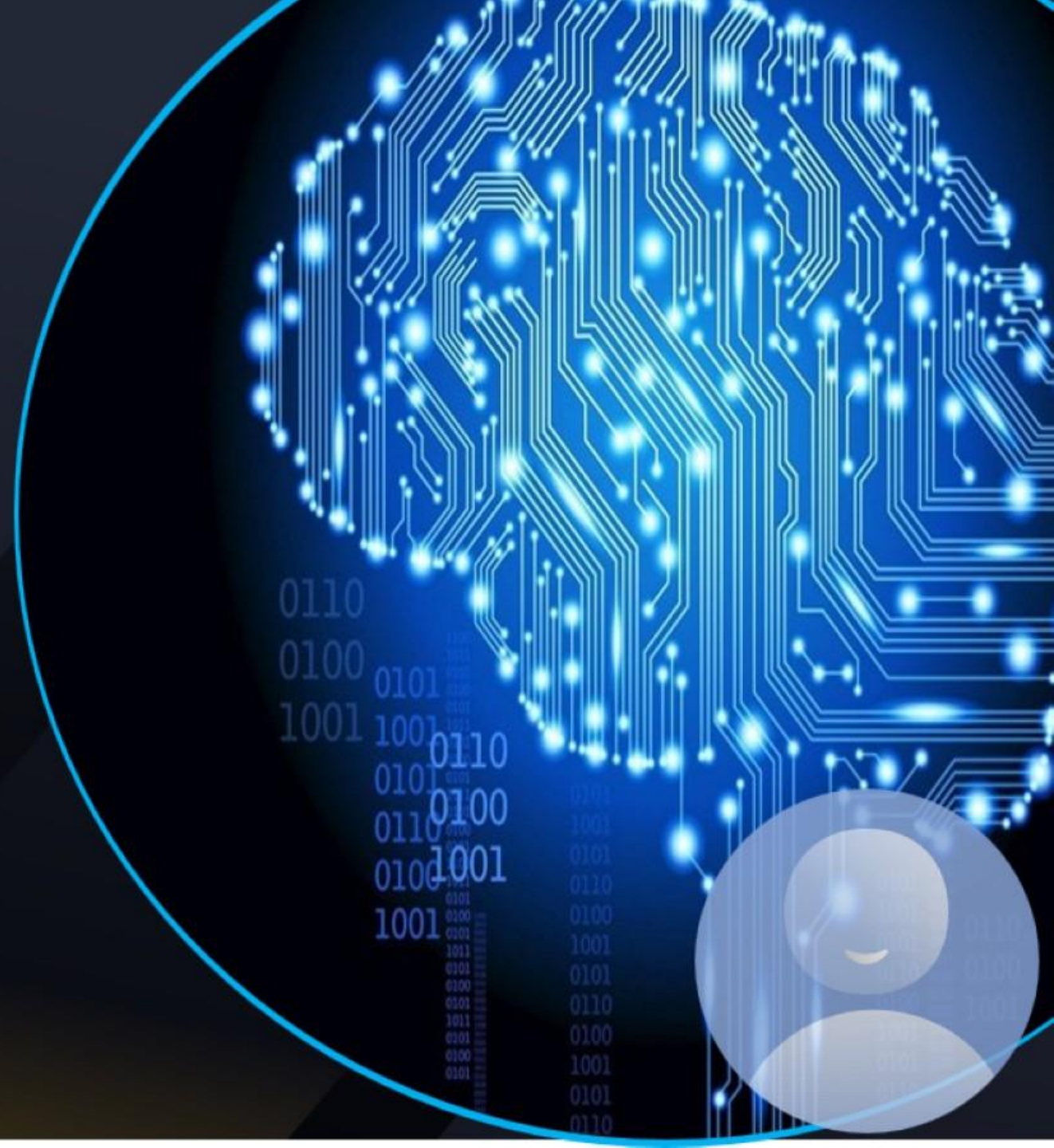


Discrete Mathematics

Dr. Shahira Ahmed

IT241

Lecture 8





Discrete Mathematics

Lecture 8

Number Theory and Cryptography

Dr. Shahira Ahmed



LEARNING OUTCOMES

- ◉ Understand the fundamental concepts of number theory.
- ◉ Recognize the importance and applications of number theory in various fields.
- ◉ Analyze and solve simple number theory s.



LECTURE OUTLINE

- ◉ Why Number theory?
- ◉ Congruence
- ◉ Greatest common divisor
- ◉ Least Common Multiple
- ◉ Some Examples on using number theory in cryptography

Why?

- Number theory is about **integers** and their properties.
- Modern cryptography is based on *Number Theory*.
- In order to understand how modern cryptographic techniques work, and to estimate the extent to which they are secure, it is important to understand the basics of number theory.

Definition: If a and b are integers with $a \neq 0$, then

a divides b if there exists an integer c such that $b = ac$.

$$b \div a = c$$

Definition: If a and b are integers with $a \neq 0$, then

a divides b if there exists an integer c such that $b = ac$.

$$b \div a = c$$

- When a divides b we say that a is a **factor or divisor** of b and that b is a **multiple** of a .
- The notation $a \mid b$ denotes that a divides b .
- If a does not divide b , we write $a \nmid b$.

$$b \div a = c$$

True or False

➤ $4 \mid 12$

➤ $8 \mid 56$

➤ $3 \mid 7$

Solution

➤ True, since $12 = 4(3)$.

➤ True, since $56 = 8(7)$.

➤ False, $3 \nmid 7$, because $7/3$ is not an integer.

- If b is an integer and d a positive integer, then there are unique integers q and r , with $0 \leq r < d$, such that $b = dq + r$.
 - d is called the *divisor*.
 - b is called the *dividend*.
 - q is called the *quotient*.
 - r is called the *remainder*.

- If b is an integer and d a positive integer, then there are unique integers q and r , with $0 \leq r < d$, such that $b = dq + r$.
 - d is called the *divisor*.
 - b is called the *dividend*.
 - q is called the *quotient*.
 - r is called the *remainder*.

- What are the quotient and remainder when 10 is divided by 3?
- What are the quotient and remainder when 12 is divided by 5?
- What are the quotient and remainder when 10 is divided by 5?
- What are the quotient and remainder when 101 is divided by 11?
 - quotient =3 , remainder =1
 - quotient =2 , remainder =2
 - quotient =2 , remainder =0
 - quotient =9 , remainder =2.

What are the quotient and remainder when 10 is divided by 3?

-

- quotient = 3 , remainder = 1
- Quotient $\times$ Divisor + Remainder = Dividend
- $3 \times 3 + 1 = 10$

What are the quotient and remainder when 12 is divided by 5?

quotient = 2 , remainder = 2

- Quotient $\times$ Divisor + Remainder = Dividend
- $2 \times 5 + 2 = 12$

- What are the quotient and remainder when 0 is divided by 3?
- What are the quotient and remainder when 2 is divided by 3?
- - $q=0, r=0$
 - $q=0, r=2$

Divisibility Theorems

- For integers a , b , and c it is true that
 - if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$
 - **Example:** $3 \mid 6$ and $3 \mid 9$, so $3 \mid 15$.
- if $a \mid b$, then $a \mid bc$ for all integers c
- **Example:** $5 \mid 10$, so $5 \mid 20$, $5 \mid 30$, $5 \mid 40$, ...
- if $a \mid b$ and $b \mid c$, then $a \mid c$
- **Example:** $4 \mid 8$ and $8 \mid 24$, so $4 \mid 24$.

A positive integer p greater than 1 is called prime if the only positive factors of p are 1 and p .

A positive integer that is greater than 1 and is not prime is called **composite**.

Example:

The integer 7 is prime because its only positive factors are 1 and 7.

The integer 9 is composite because it is divisible by 3.

Examples:

- [illegible]

$$15 = 3 \cdot 5$$

$$48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^4 \cdot 3$$

$$17 = 17$$

$$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$$

$$512 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^9$$

$$515 = 5 \cdot 103$$

$$28 = 2 \cdot 2 \cdot 7$$

Greatest Common Divisors

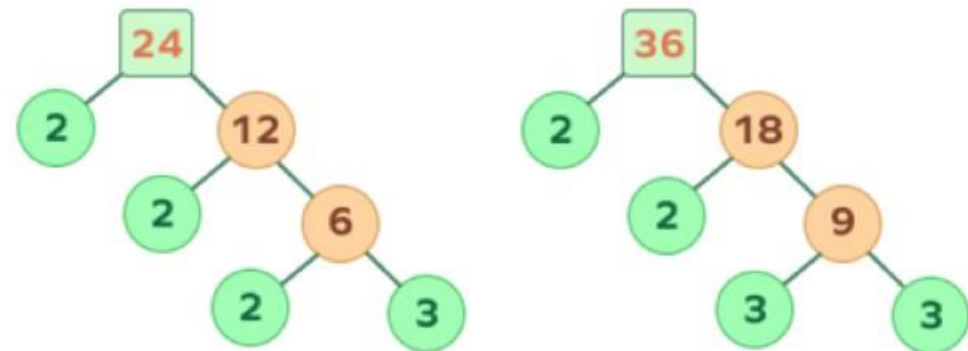
Let a and b be integers, **not both zero**.

The **largest integer** d such that $d \mid a$ and $d \mid b$ is called **the greatest common divisor** of a and b .

The greatest common divisor of a and b is denoted by $\gcd(a, b)$.

Example 1: What is $\gcd(24, 36)$?

12



Greatest Common Divisors

Using prime factorizations:

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}, \quad b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n},$$

where $p_1 < p_2 < \dots < p_n$ and $a_i, b_i \in \mathbf{N}$ for $1 \leq i \leq n$

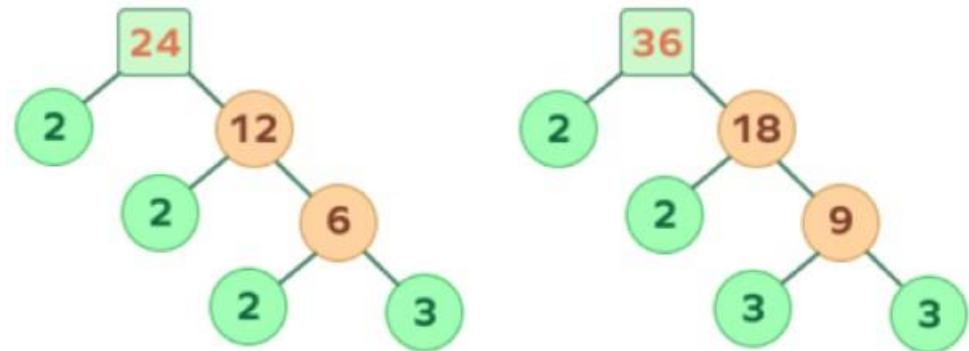
$$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \dots p_n^{\min(a_n, b_n)}$$

Example:

$$a = 60 = 2^2 3^1 5^1$$

$$b = 54 = 2^1 3^3 5^0$$

$$\gcd(a, b) = 2^1 3^1 5^0 = 6$$



Relatively Prime Integers

Two integers a and b are **relatively prime** if $\gcd(a, b) = 1$.

Examples:

Are 15 and 28 relatively prime?

Yes, $\gcd(15, 28) = 1$.

Are 55 and 28 relatively prime?

Yes, $\gcd(55, 28) = 1$.

Are 35 and 28 relatively prime?

No, $\gcd(35, 28) = 7$.

Least Common Multiples

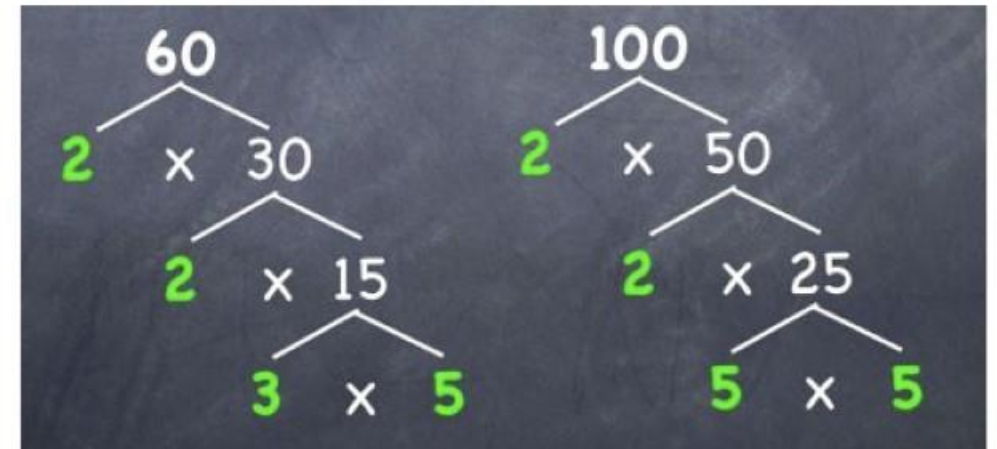
The **least common multiple** of the positive integers a and b is the smallest positive integer that is divisible by both a and b .

We denote the least common multiple of a and b by $\text{lcm}(a, b)$.

Examples:

$\text{lcm}(60, 100)$

$$\text{lcm of } 60 \text{ and } 100 = 2 * 2 * 3 * 5 * 5 = 300.$$



Least Common Multiples

Using prime factorizations:

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}, \quad b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n},$$

where $p_1 < p_2 < \dots < p_n$ and $a_i, b_i \in \mathbf{N}$ for $1 \leq i \leq n$

$$\text{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \dots p_n^{\max(a_n, b_n)}$$

Example:

$$a = 60 = 2^2 3^1 5^1$$

$$b = 54 = 2^1 3^3 5^0$$

$$\text{lcm}(a, b) = 2^2 3^3 5^1 = 4 * 27 * 5 = 540$$

GCD and LCM

$$a = 60 = 2^2 \cdot 3^1 \cdot 5^1$$

$$b = 54 = 2^1 \cdot 3^3 \cdot 5^0$$

$$\gcd(a, b) = 2^1 \cdot 3^1 \cdot 5^0 = 6$$

$$\text{lcm}(a, b) = 2^2 \cdot 3^3 \cdot 5^1 = 540$$

Theorem: $a \cdot b = \gcd(a, b) \cdot \text{lcm}(a, b)$

- The Euclidian algorithm is an **efficient** method for computing the greatest common divisor of two integers.
- It is based on the idea that $\gcd(a,b)$ is equal to $\gcd(a,c)$ when c is the remainder when a is divided by b .

Example: Find $\gcd(91, 287)$:

- $287 = 91 \cdot 3 + 14$
- $91 = 14 \cdot 6 + 7$
- $14 = 7 \cdot 2 + 0$

$$\gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7) = 7$$

Let a and b be integers and m be a positive integer. We say that **a is congruent to b modulo m** if m divides $a - b$.

We use the notation **$a \equiv b \pmod{m}$** to indicate that a is congruent to b modulo m .

In other words: $a \equiv b \pmod{m}$ if and only if **$a \bmod m = b \bmod m$** .

True or False

$46 \equiv 68 \pmod{11}$?

Yes, because $11 \mid (46 - 68)$.

True or False

$46 \equiv 68 \pmod{11}$?

Yes, because $11 \mid (46 - 68)$.

$46 \equiv 68 \pmod{22}$?

Yes, because $22 \mid (46 - 68)$.

For which integers z is it true that $z \equiv 12 \pmod{10}$?

It is true for any $z \in \{\dots, -28, -18, -8, 2, 12, 22, 32, \dots\}$

Julius Caesar created secret messages by shifting each letter three letters forward in the alphabet (sending the last three letters to the first three letters.)

For example, the letter B is replaced by E and the letter X is replaced by A. This process of making a message secret is an example of *encryption*.

Caesar Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
13	14	15	16	17	18	19	20	21	22	23	24	25

Here is how the encryption process works:

- **Replace each letter by an integer** from $\mathbf{Z}_{26}$, that is an integer from 0 to 25 representing one less than its position in the alphabet.
- The **encryption function** is $f(p) = (p + 3) \bmod 26$. It replaces each integer p in the set $\{0,1,2,\dots,25\}$ by $f(p)$ in the set $\{0,1,2,\dots,25\}$.
- **Replace each integer p** by the letter with the position p in the alphabet.

Example: Encrypt the message “MEET YOU IN THE PARK” using the Caesar cipher.

12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10.

Now replace ea

15 7

A	B	C	D	E	F	G	H	I	J	K	L	M
↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
13	14	15	16	17	18	19	20	21	22	23	24	25

Translating the message back to reverse produces the encrypted message

“PHHW BRX LQ WKH SDUN.”

Example: Encrypt the message “MEET YOU IN THE PARK” using the Caesar cipher.

12 4 4 19

Now replac

A	B	C	D	E	F	G	H	I	J	K	L	M
↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
13	14	15	16	17	18	19	20	21	22	23	24	25

Translating the numbers back to letters produces the encrypted message

“PHHW BRX LQ WKH SDUN.”

- To recover the original message, use $f^{-1}(p) = (p-3) \bmod 26$. This process of recovering the original message from the encrypted message is called *decryption*.

Example: decrypt the message ““PHHW BRX LQ WKH SDUN.””
using the Caesar cipher.

15 7 7 22 1 17 22 11 16 22 10 7 18 2 20 12

Now replace ea

12 4 4

Translating the

A	B	C	D	E	F	G	H	I	J	K	L	M
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
13	14	15	16	17	18	19	20	21	22	23	24	25

ssage

“MEET YOU IN THE PARK.”

Encrypt the message “**STOP GLOBAL WARMING**” using the shift cipher with $k = 11$.

Replace each letter with the corresponding element of $\mathbf{Z}_{26}$.

18 19 14 15 6

Apply the shift $f(x)$

3 4 25 0 17 22

A	B	C	D	E	F	G	H	I	J	K	L	M
↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
13	14	15	16	17	18	19	20	21	22	23	24	25

Translating the numbers back to letters produces the ciphertext

“DEZA RWZMLW HLCXTYR.”

Decrypt the message “**LEWLYPLUJL PZ H NYLHA ALHJOLY**” that was encrypted using the shift cipher with $k = 7$.

Replace each letter with the corresponding element of **Z**

11 4 22 11 2

Shift each of the

4 23 15 4

Translating the

“EXPERIENCE IS A GREAT TEACHER.”

A	B	C	D	E	F	G	H	I	J	K	L	M
↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
13	14	15	16	17	18	19	20	21	22	23	24	25

24.

7.

isage

- Shift ciphers are a special case of *affine ciphers* which use functions of the form

$$f(p) = (ap + b) \bmod 26,$$

where a and b are integers, chosen so that f is a bijection.

The function is a bijection if and only if $\gcd(a, 26) = 1$.

- **Example:** What letter replaces the letter K when the function

$f(p) = (7p + 3) \bmod 26$ is used for encryption.

Since 10 represents
replaced by V.

A	B	C	D	E	F	G	H	I	J	K	L	M
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
13	14	15	16	17	18	19	20	21	22	23	24	25

en

- The process of **recovering plaintext from ciphertext** without **knowledge both of the encryption method and the key** is known as *cryptanalysis* or *breaking codes*.
- An important tool for cryptanalyzing ciphertext produced with a affine ciphers is the relative **frequencies of letters**.
- The nine most common letters in the English texts are E 13%, T 9%, A 8%, O 8%, I 7%, N 7%, S 7%, H 6%, and R 6%.

- analyze ciphertext:
 - **Find** the frequency of the letters in the ciphertext.
 - **Hypothesize** that the most frequent letter is produced by encrypting **E**.
 - If the value of the shift from E to the most frequent letter is k , shift the ciphertext by $-k$ and see if it makes sense.
 - If not, try T as a hypothesis and continue.

- **Example:** We intercepted the message
“ZNK KGXRE HOXJ MKZY ZNK CUXS” that we know was produced
by a shift cipher. Let’s try to cryptanalyze.jkm
- The most common letter in the ciphertext is K. So perhaps the letters
were shifted by 6 since this would then map E to K. Shifting the entire
message by -6 gives us “THE EARLY BIRD GETS THE WORM.”

- A group is a mathematical structure consisting of a set of elements and an associated binary operation that satisfies four fundamental properties: closure, associativity, identity, and inverse.
- Let G be a set, and let $*$ be a binary operation defined on G . G is called a group if it satisfies the following properties:
 - **Closure:** For any two elements a and b in G , the result of the operation $a * b$ is also in G .
 - **Associativity:** For any three elements a , b , and c in G , the operation is associative, i.e., $(a * b) * c = a * (b * c)$.
 - **Identity:** There exists an element e in G , called the identity element, such that for any element a in G , $a * e = e * a = a$.
 - **Inverse:** For every element a in G , there exists an element b in G , called the inverse of a , such that $a * b = b * a = e$.

- $(\mathbb{N}, +)$ Form a group?
- No, there is no inverse

- $(\mathbb{Z}, +)$ Form a group?
- Yes
- $(\mathbb{Z}, *)$ Form a group?
- No, There is no inverse

	Addition	Multiplication
Closure	$a+b$ is an integer	$a*b$ is an integer
Associativity	$a+(b+c) = (a+b)+c$	$a*(b*c) = (a*b)*c$
Existence of an identity element	$a+0 = a$	$a*1 = a$
Existence of inverse elements	$a+(-a) = 0$	Only 1 and -1 have inverses: $1*1 = 1, -1*(-1) = 1$
Commutativity	$a+b = b+a$	$a*b = b*a$

- $(\mathbb{Z}, -)$ Form a group?
- No
- $(\mathbb{Z}, /)$ Form a group?
- No, $\mathbb{Z}$ is not closed under division

- An **Abelian or Commutative Group** is a Group with the additional condition
5. **Commutativity.** For all $a, b \in G$, $a*b=b*a$

- A **Field** is a set of elements F with binary operators $*$ and $+$ such that
 1. $(F, +)$ is an **abelian group**
 2. $(F \setminus I_+, *)$ is an **abelian group**
the “multiplicative group”
 3. **Distribution**: $a*(b+c) = a*b + a*c$
 4. **Cancellation**: $a*I_+ = I_+$
- The **order** of a field is the number of elements.
- A field of finite order is a **finite field**.

- Error Correction Codes: Finite fields are extensively used in coding theory and error correction codes. They form the foundation for constructing error correction codes such as Reed-Solomon codes, BCH codes, and LDPC codes. These codes are widely used in communication systems, storage devices, and data transmission to detect and correct errors.
- Cryptography: Finite fields play a crucial role in modern cryptography. They are used in the design and implementation of symmetric key algorithms such as the Advanced Encryption Standard (AES) and block ciphers. Finite fields also form the basis for elliptic curve cryptography (ECC), which is widely used in public-key cryptography systems.
- Combinatorics and Design Theory: Finite fields are used in combinatorics and design theory to construct combinatorial structures such as finite projective planes, block designs, and error-correcting codes. These structures have applications in coding theory, information theory, and experimental design.
- Finite Field Arithmetic in Hardware: Finite field arithmetic is implemented in hardware for various applications. It is used in digital signal processors (DSPs), field-programmable gate arrays (FPGAs), and cryptographic hardware modules to perform efficient computations involving finite fields.

Recap

- Does 2 divide 68?
- Does 15 divide 68?
- Does 5 divide 25?
- Does 5 divide 2?

- Solution
 - True , False , True , False

Determine whether each of these integers is prime.

- a) 21
- b) 29
- c) 71
- d) 97
- e) 111
- f) 143

- Solution
 - 29, 71, 97 prime; 21, 111, 143 not prime

Determine whether the integers in each of these sets are relatively prime.

- a) 11, 15
- b) 11, 19
- c) 14, 15
- d) 14, 21
- e) 12, 18
- f) 11, 22

- Solution

a) Yes b) Yes c) Yes d) No e) No f) No

- Encrypt the message DO NOT PASS GO by translating the letters into numbers, applying the given encryption function
 - a) $f(p) = (p + 3) \bmod 26$ (the Caesar cipher)
 - b) $f(p) = (p + 13) \bmod 26$
 - c) $f(p) = (3p + 7) \bmod 26$

Solutions

- a) GR QRW SDVV JR
- b) QB ABG CNFF TB
- c) QX UXM AHJJ ZX

Decrypt these messages encrypted using the shift cipher

$$f(p) = (p + 10) \bmod 26.$$

- a) CEBBOXNOB XYG
- b) LO WI PBSOXN
- c) DSWO PYB PEX

Solution

- a) SURRENDER NOW
- b) BE MY FRIEND
- c) TIME FOR FUN

- a) Find the GCD of 36 and 48.
- b) Determine the positive integer that divides 72 and 120 with the greatest Common divisor.
- c) Compute the GCD of 105 and 140.
- d) What is the GCD of 54 and 81?
- e) Find the common divisor of 63 and 105 with the greatest value.

- Solution

- a) The GCD of 36 and 48 is 12.
- b) The GCD of 72 and 120 is 24.
- c) The GCD of 105 and 140 is 35.
- d) The GCD of 54 and 81 is 27.
- e) The GCD of 63 and 105 is 21.

1. Determine the LCM of 15 and 20.
2. Find the LCM of 8 and 12.
3. Compute the LCM of 18 and 24
4. What is the LCM of 30 and 45?
5. Determine the LCM of 36 and 48

- Solution:

- 60
- 24
- 72
- 90
- 144



LECTURE SUMMARY

- Number theory is a branch of mathematics that focuses on the properties and relationships of integers.
- Prime numbers are integers greater than 1 that are divisible only by 1 and themselves, and they play a fundamental role in number theory. Prime factorization is the process of expressing a composite number as a product of prime factors.
- Number theory has practical applications in cryptography

*Thank
you*

