CM 1606 Computational Mathematics

Logarithm and Modular Arithmetic

Week 06| Ganesha Thondilege

ROBERT GORDON UNIVERSITY ABERDEEN
INFORMATICS INSTITUTE OF TECHNOLOGY

Learning Outcomes

- Covers LO1 for Module
- On completion of this lecture, students are expected to be able to:
  - Review the mathematical concept behind logarithm
  - Discuss some basic rules in logarithm
  - Locate the relevant rule appropriately in different examples
  - Review the concept and applications of modular arithmetic

CONTENT

- Definition
- Laws of logarithm
- Examples
- Natural logarithm
- Basics of Modular Arithmetic
- Applications of Modular arithmetic

Logarithm

Definition

If a number N can be expressed as a^x, then the index x is called the

Logarithm of N to the base a

denoted as

$$x = \log_a N$$

$$where \quad N = a^x$$

$$Then,$$

$$x = \log_a a^x$$

Example

$$1)8 = 2^3$$

$$\log_2 8 = \log_2 2^3 = 3$$

$$2)64 = \log_4 4^3 = 3$$

Base 10 is known as the common logarithm

$$If \quad \log_a x = \log_a y, \text{ then } x = y$$

Laws of Logarithm

- $\log_a 1 = 0$ for $a \neq 0$
- $\log_a xy = \log_a x + \log_a y$
- $\log_a \left(\dfrac{x}{y} \right) = \log_a x - \log_a y$
- $\log_a x^r = r \log_a x$

$$\log_a x^{\frac{1}{r}} = \frac{1}{r} \log_a x$$

Change of Base

- $\log_b x = \dfrac{\log_a x}{\log_a b}$ or
- $\log_a b \times \log_b x = \log_a x$

Example

Simplify the following

$$1)\ \log_2 \sqrt{256}$$

$$2)\ 6\log_a 3 + 4\log_a x - \log_a 9 = 2\log_a 25$$

$$3)\ \log_a x = \frac{1}{2}[\log_a 9 + \log_a 12 - \log_a 3]$$

Natural logarithm

- Logarithm to the base of the constant 'e'
- Denoted as

$$\log_e \text{ or } \ln$$

- 'e' is an irrational and $\simeq 2.718$
- Highly applicable for fitting a growth function for large set of data

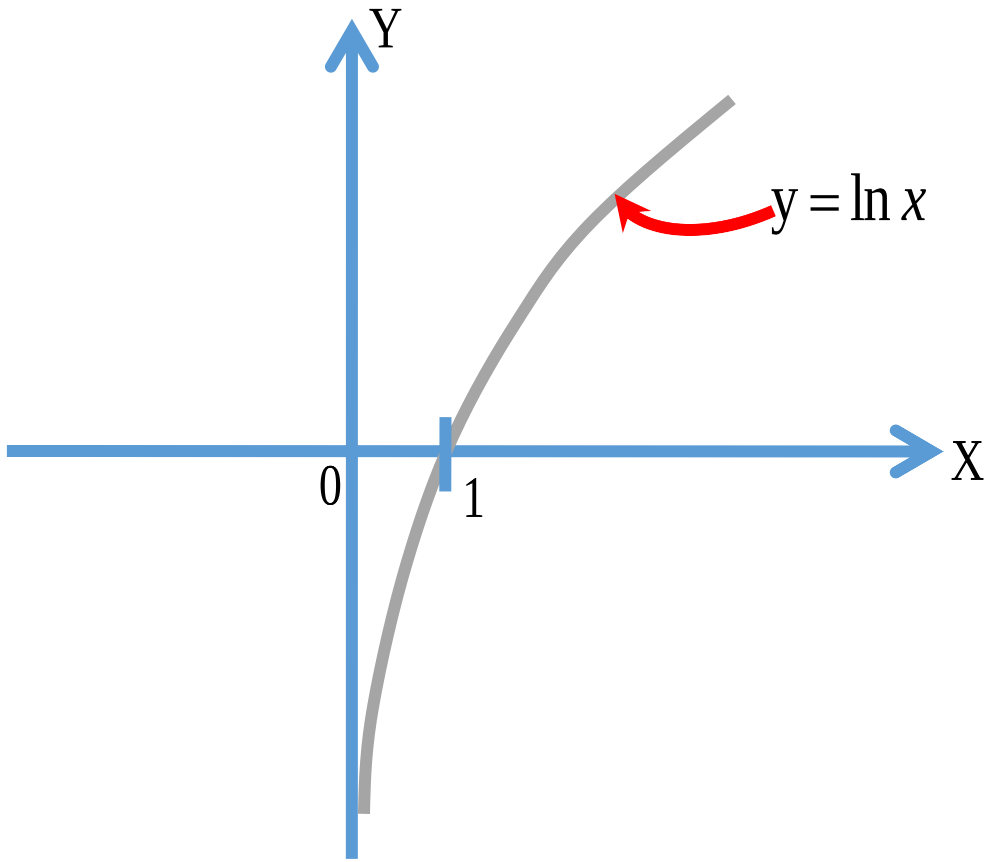
Example:

$$1) \ln e = 1$$

$$2) \text{simplify for } x$$

$$\ln(5x - 2) = 5$$

Graph of ln(x)



Modular Arithmetic

Modular Arithmetic

- Consider the division

Dividend

Quotient

$$\frac{A}{B} = Q \text{ remainder } R$$

Remainder

Divisor

- Sometimes we only consider the remainder of $\dfrac{A}{B}$
- For such cases, the operator ' modulo' is used.

abbreviated as 'mod'

Congruency modulo *m*

Definition

Let m be a fixed natural number greater than 1. The integer a is congruent to the integer b modulo m if and only if (a − b) is divisible by m.

Notation

$$a \equiv b \pmod{m}$$

The number m is called the modulus

Example

$$i)17 \equiv 5(\bmod 12)$$

since $(17-5)$ is divisible by 12

$$ii)-5 \equiv 11(\bmod 8)$$

since $(-5-11)$ is divisible by 8

$$iii)248 \equiv 113(\bmod 5)$$

since $(248-113)$ is divisible by 5

Many properties of modular arithmetic are very similar to properties of equalities and can be demonstrate by following theorems.

ROBERT GORDON UNIVERSITY ABERDEEN | INFORMATICS INSTITUTE OF TECHNOLOGY

Equivalence relation and congruent

- $a \equiv a \pmod{m}$ - Reflexive
- If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$ - Symmetric
- If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$ - Transitive

Theorem

Theorem 6.1 : congruence behaves nicely with respect to addition, subtraction, and multiplication

If

$$a \equiv b \pmod{m}$$
$$c \equiv d \pmod{m}$$

then,

$$a + c \equiv b + d \pmod{m} \text{ - Addition}$$
$$a - c \equiv b - d \pmod{m} \text{ - Subtraction}$$
$$a \times c \equiv b \times d \pmod{m} \text{ - Multiplication}$$

Addition

Let a ≡ b (mod m) and c ≡ d (mod m)

Then a − b and c − d are divisible by m (multiples of m)

So,

$$a-b = m*s \text{ and}$$

$$c-d = m*t \text{ for some integers } s \text{ and } t$$

Then

$$(a + c) - (b + d) = (a - b) + (c - d)$$

$$= ms + mt$$

$$= m(s + t)$$

So, a + c ≡ b + d (mod m),

since (a + c) − (b + d) is a multiple of m.

Subtraction

Let $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$

Then $a - b$ and $c - d$ are divisible by m (multiples of m)

So,

$$a-b = m*s \text{ and}$$

$$c-d = m*t \text{ for some integers s and t}$$

Then

$$(a - c) - (b - d) = (a - b) - (c - d)$$

$$= ms - mt$$

$$= m(s - t)$$

So, $a - c \equiv b - d \pmod{m}$,

since $(a - c) - (b - d)$ is a multiple of m.

Multiplication

Let $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$

Then $a - b$ and $c - d$ are divisible by of m (multiples of m)

So,

$a-b = m*s$ and ---------------------------->> $a = ms + b$

$c-d = m*t$ for some integers s and t------->> $c = mt + d$

Then

$ac - bd = (ms + b)(mt + d) - bd$

$= (m^2 st + dms + bmt + bd) - bd$

$= m(mst + ds + bt) + bd - bd$

$= m(mst + ds + bt),$

so $ac \equiv bd \pmod{m}$, since $ac - bd$ is a divisible by m.

Theorem

Theorem 6.2:

If $a \equiv b \pmod{m}$ then for every natural number n, then

$$a^n \equiv b^n \pmod{m}$$

Addition of a constant

If $a \equiv b \pmod{m}$, then $a + c \equiv b + c \pmod{m}$ for any c.

Eg:

$7 \equiv 1 \pmod{3}$, So $1+7 \equiv 1+1 \pmod{3}$

Examples

1) $23 \equiv 3 \pmod 4$ and $18 \equiv 2 \pmod 4$, So

   i) $(23 + 18) \equiv (3 + 2) \pmod 4 \equiv 1 \pmod 4$

   ii) $(23 - 18) \equiv (3 - 2) \pmod 4 \equiv 1 \pmod 4$

   iii) $23 \cdot 18 \equiv 3 \cdot 2 \pmod 4 \equiv 2 \pmod 4$

2) $13 \equiv 1 \pmod{12}$, so

   $4{,}826{,}809 = 13^6 \equiv 1^6 \pmod{12} \equiv 1 \pmod{12}$

Examples

3) What is the remainder of

I. 13+9+27+31+18 when divided by 4

II. 25+19+31+17 when divided by 3

III. 42+17+38+14 when divided by 5

Example

4) What is the remainder when $8 + 5^{301563}$ divide by 31?

$$5^{301563} = (5^3)^{100521} - - - (1)$$

$$5^3 = 125 \equiv 1 (\bmod 31)$$

So by (1)

$$5^{301563} = (5^3)^{100521} \equiv 1^{100521} (\bmod 31) \equiv 1 (\bmod 31)$$

$$8 + 5^{301563} = 8 + (5^3)^{100521} \equiv 8 + 1 (\bmod 31)$$

$$8 + 5^{301563} \equiv 9 (\bmod 31)$$

Example

5) Find a solution in the set $\{0, 1, 2, \ldots, 16\}$ to the congruence

i) $7x \equiv 11 \pmod{17}$

ii) $6x \equiv 6 \pmod{15}$

Applications

1) Check whether the decimal numbers 6347 and 6345 are divisible by 3 or not.

- Can you explain an easy way to check this?

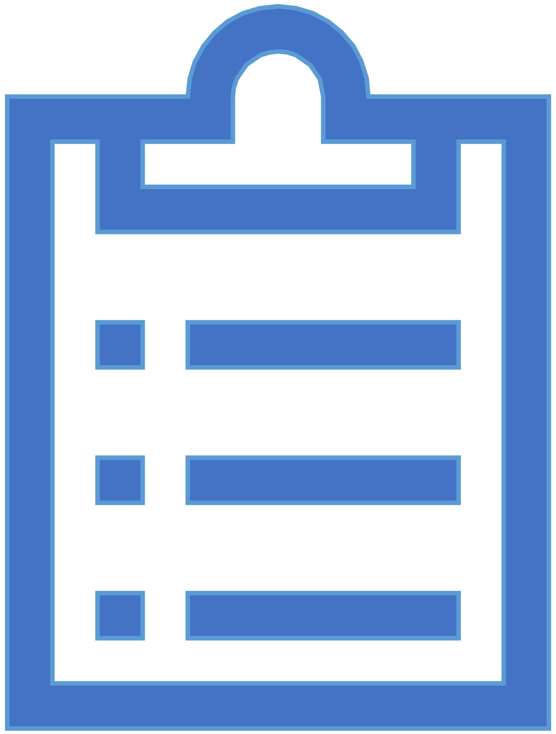
Applications

1) What is the remainder of $13\times(17\times22+8)-19$ when divided by 3?

- Do we need to evaluate this to answer?
- Any easy way?

Applications

3) What are the last two digits of the number 99^{99} ?



Task

Identify at least three situations that we can use the function mod in Excel and discuss how you use the function mod in each case by giving a proper example.