# CHAPTER 8: THE MATHEMATICAL SYSTEM

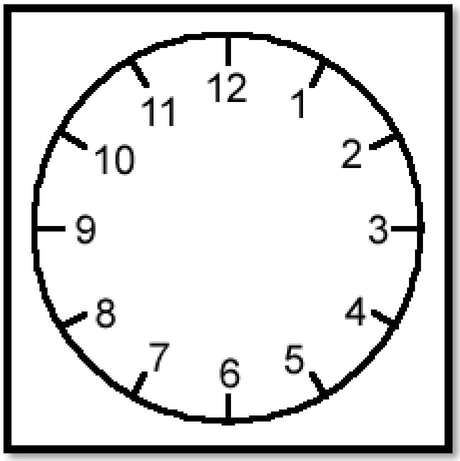
**Objectives:**
**a.** Identify the different mathematical system such as Modular Arithmetic and its application
**b.** Understand the Introduction of Group theory
**c.** Apply modular arithmetic in real life situation

## Lesson 1: Modular Arithmetic

### An Introduction to Modular Arithmetic

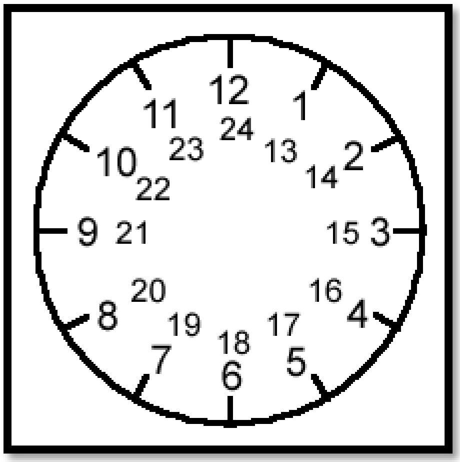
Many clocks have the familiar 12-hour design. We designate the time period with the abbreviation A.M and P.M. A reference for 10:00 A.M means 10 hours after 12:00 midnight, and a reference for 10 A.M. means 10 hours after 12:00 noon.

The best way to introduce modular arithmetic is by thinking about the face clock.



The numbers go from 1 to 12, but when you get to "13 o'clock", it actually becomes 1 o'clock again (think of how the 24 hour clock numbering works). So 13 becomes 1, 14 becomes 2, and so on.

This can keep going, so when you get to "25 o'clock", you are actually back round to where 1 o'clock is on the clock face (and also where 13 o'clock was too).



So in this clock world, you only care where you are in relation to the numbers 1 to 12. In this world, 1,13,25,37,… are all thought of as the same thing, as are 2,14,26,38,… and so on.

What we are saying is "13=1+ some multiple of 12", and "38=2+ some multiple of 12", or, alternatively, "the remainder when you divide 13 by 12 is 1" and "the remainder when you divide 38 by 12 is 2". The way we write this mathematically is 13≡1 mod 12, 38≡2 mod 12, and so on. This is read as "13 is congruent to 1 mod (or modulo) 12" and "38 is congruent to 2 mod 12".

**Modulus**

- The modulus is another name for remainder after division.
- This symbol "≡" means congruent to.

**Example:**

17 mod 5 = 2

**Solution:**

If we divide 17 by 5, we get 3 with the remainder of 2.

Sometimes we see, 17 ≡ 2 (mod 5) and that means that 17 and 2 are equivalent, after we consider the modulus of 5.

**Another Example:**

**a.** 15 mod 6 = 3
**b.** 35 mod 7 = 0
**c.** $3^4$ mod 4 = 1

**Solution:**

**a.** If we divide 15 by 6, we get 2 with the remainder of 3.
**b.** If we divide 35 by 7, we get 5 with no remainder that is why 35 mod 7 = 0.
**c.** First, find the $3^4$ which is equal to 81 then divide by 4, we get 20 with the remainder of 1.

**Modulus on a Standard Calculator**

To calculate *a* mod *n* on a standard calculator:

Step 1: Divide *a* by *n*.

Step 2: Subtract the whole part of the resulting quantity.

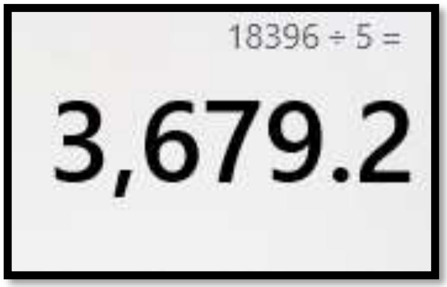
Step 3: Multiply by *n* to obtain the modulus.

**Example:**

**1.** 18396 mod 5

**Solution:**

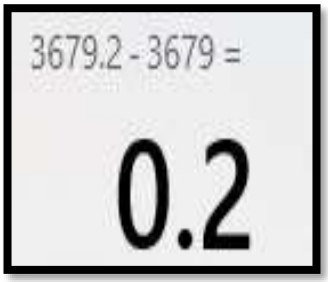
Step 1:



18396 ÷ 5 =

3,679.2

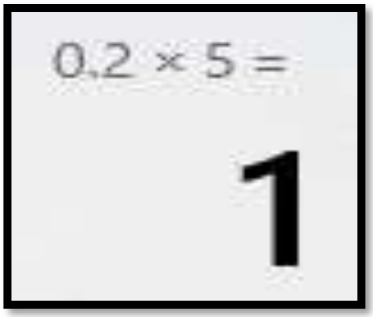
Step 2:



3679.2 - 3679 =

0.2

Step 3:



0.2 × 5 =

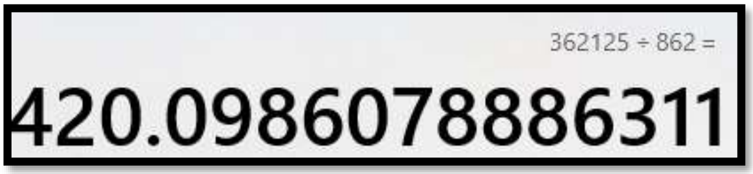
1

it means that 18396 mod 5= 1.

**2.** 362,125 mod 862

**Solution:**

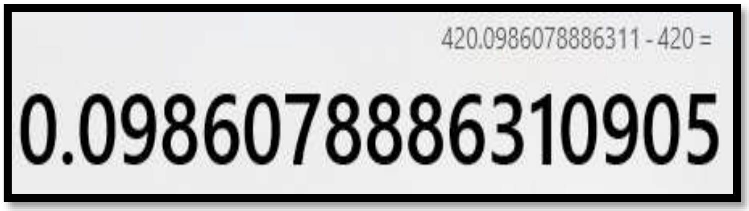
Step 1:



362125 ÷ 862 =

420.0986078886311

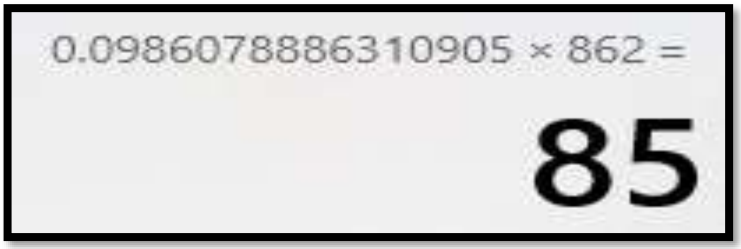
Step 2:



420.0986078886311 - 420 =

0.0986078886310905

Step 3:



0.0986078886310905 × 862 =

85

It means that 362,125 mod 862 = 85

**Modular Exponentiation Rule**

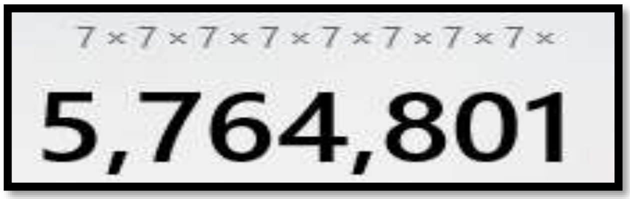
$(a^b \text{mod } n) = (a \bmod n)^b \text{ mod } n$

**Example:**

$7^8 \text{ mod } 5 = (7 \bmod 5)^8 \text{ mod } 5$

**Solution: a.** $7^8$ mod 5

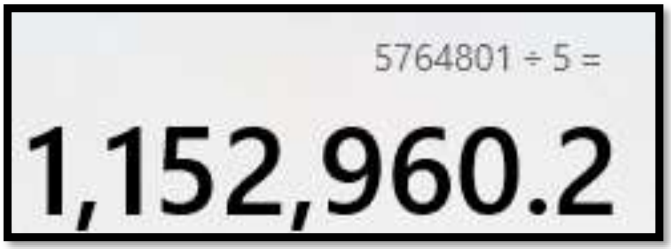
Find first 7 raise to 8.



7 × 7 × 7 × 7 × 7 × 7 × 7 × 7 ×

5,764,801

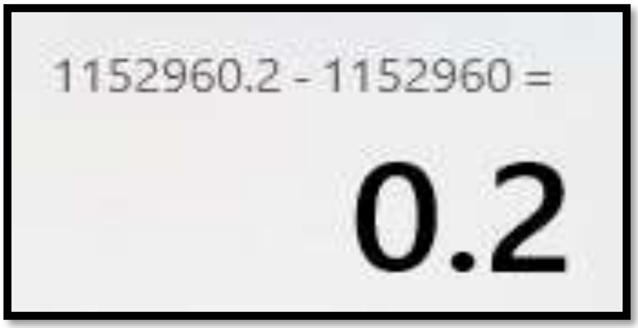
Divide by 5



5764801 ÷ 5 =

1,152,960.2

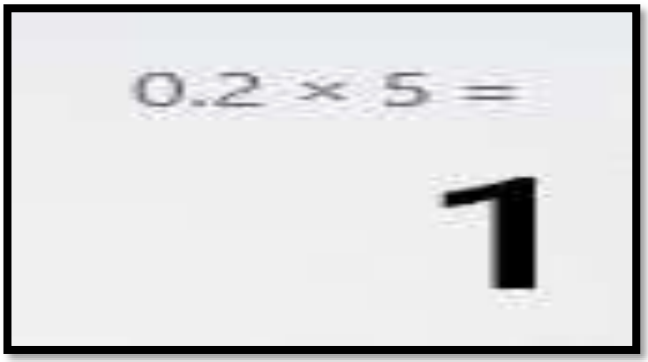
Subtract with the whole number.



1152960.2 - 1152960 =

0.2

Multiply by 5. We get 1.



0.2 × 5 =

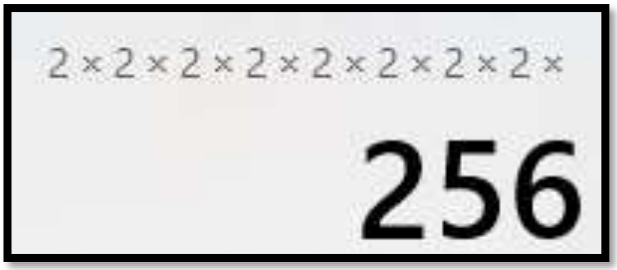
1

**b.** $(7 \bmod 5)^8$ mod *5*

First is to compute for 7 mod 5, dividing 7 by 5 we get 1 with a remainder of 2 it means 7 mod 5= 2.

$(7 \bmod 5)^8$ mod 5 can be write as $(2)^8$ mod 5

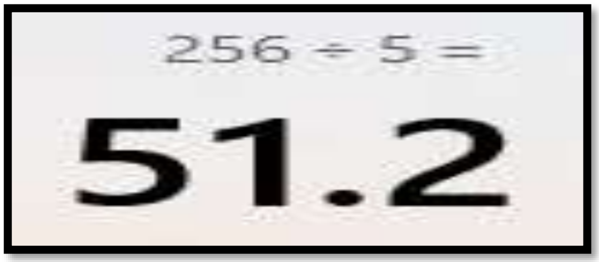
Step 1: Get 2 raise to 8 equals to 256



2×2×2×2×2×2×2×2×

256

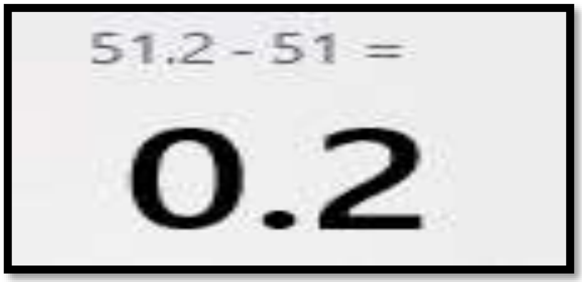
Step 2: Divide by 5.



256 ÷ 5 =

51.2

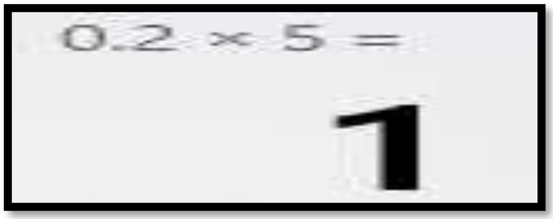
Step 3: Subtract the whole number.



51.2 - 51 =

0.2

Step 4: Multiply by 5.



0.2 × 5 =

1

With the complete solution using the standard calculator, we conclude that $7^8$ mod 5 = $(7 \bmod 5)^8$ mod *5* is congruent.

### Modular Exponent Power Rule

$(a^b \bmod n)\ ^c \bmod n = \ (a^{bc} \bmod n)$= $(a^c \bmod n)\ ^b \bmod n$

**Example:**

$(3^{2 \cdot 4} \bmod 7)$ = 6561 mod 7

Notice that a= 3, b=2, c= 4 and n=7

Verify using $(3^{2 \cdot 4} \bmod 7)$=2

$(3^2 \bmod 7)\ ^4 \bmod 7$ = $2^4$ mod 7

= 16 mod 7 = 2

$(3^4 \bmod 7)\ ^2 \bmod 7$= $(81 \bmod 7)\ ^2$ mod 7

= $4^2 \bmod 7$

= 16 mod 7 = 2

### Residue

We say that $a$ is the modulo-$m$ **residue** of $n$ when $n \equiv a \pmod{m}$, and $0 \le a < m$.

### Congruence

There is a mathematical way of saying that all of the integers are the same as one of the modulo 5 residues. For instance, we say that 7 and 2 are **congruent** modulo 5. We write this using the symbol $\equiv$: In other words, this means in base 5, these integers have the same residue modulo 5:

$2 \equiv 7 \equiv 12 \pmod{5}$.

The **(mod 5)** part just tells us that we are working with the integers modulo 5. In modulo 5, two integers are congruent when their difference is a multiple of 5. In general, two integers $a$ and $b$ are congruent modulo $n$ when $a - b$ is a multiple of $n$. In other words, $a \equiv b \pmod{n}$ when $\frac{a-b}{n}$ is an integer. Otherwise, $a \not\equiv b \pmod{n}$, which means that $a$ and $b$ are **not congruent** modulo $n$.

**Examples**

- $31 \equiv 1 \pmod{10}$ because $31 - 1 = 30$ is a multiple of $10$.
- $43 \equiv 22 \pmod{7}$ because $\frac{43-22}{7} = \frac{21}{7} = 3$, which is an integer.
- $8 \not\equiv -8 \pmod{3}$ because $8 - (-8) = 16$, which is not a multiple of $3$.
- $91 \not\equiv 18 \pmod{6}$ because $\frac{91-18}{6} = \frac{73}{6}$, which is not an integer.

**Sample Problem**

Find the modulo $4$ residue of $311$.

***Solution:***

Since $311 \div 4 = 77$ R $3$, we know that

$$311 \equiv 3 \pmod{4}$$

and $3$ is the modulo $4$ residue of $311$.

***Another Solution:***

Since $311 = 300 + 11$, we know that

$$311 \equiv 0 + 11 \pmod{4}$$

We can now solve it easily

$$11 \equiv 3 \pmod{4}$$

and $3$ is the modulo $4$ residue of $311$

***Another Solution:***

We know $308$ is a multiple of $4$ since $8$ is a multiple of $4$. Thus, $311 - 308 = 3$ and $3$ is the modulo $4$ residue of $311$.

Consider four integers $a, b, c, d$ and a positive integer $m$ such that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. In modular arithmetic, the following identities hold:

- Addition: $a + c \equiv b + d \pmod{m}$.
- Subtraction: $a - c \equiv b - d \pmod{m}$.

- Multiplication: $ac \equiv bd \pmod{m}$.
- Division: $\frac{a}{e} \equiv \frac{b}{e} \left(\bmod \frac{m}{\gcd(m,e)}\right)$, where $e$ is a positive integer that divides $a$ and $b$ .

For more knowledge about Modular Arithmetic, please check the link provided;
https://www.slideshare.net/SamBowne/modular-arithmetic-addition-and-subtraction
http://www.acm.ciens.ucv.ve/main/entrenamiento/material/ModularArithmetic-Presentation.pdf

## REMEMBER

- The modulus is another name for remainder after division.
- This symbol “≡” means congruent to.
- **Modular Exponentiation Rule**
  - $(a^b \bmod n) = (a \bmod n)^b \bmod n$
- **Modular Exponent Power Rule**

$-(a^b \bmod n)^c \bmod n = (a^{bc} \bmod n) = (a^c \bmod n)^b \bmod n$

**ACTIVITY: Count what hours**
Using modular arithmetic, answer the following. Show your solution.

**a.** It is currently 7:00 PM. What time (in AM or PM) will it be in 1000 hours for me to do my assignment?
**b.** It is currently 5:00 AM. What time (in AM or PM) will it be in 500 hours for me to go shopping?

## Lesson 2: Applications of Modular Arithmetic

ISBN and UPC is the most common application of Modular Arithmetic. When a book is published, it is assigned a number called the International Standard Book Number (ISBN). From 1970 until 2007, this number consisted of a 10-digit number, but it now consists of a 13-digit number. For example, the ISBN of UMAP Modules (1984) is 0-912843-07-1, but the ISBN of Dan Brown's The lost Symbol (2009) is 978-0-385-50422-5.

An International Standard Book Number consists of 4 parts (if it is a 10 digit ISBN) or 5 parts (for a 13 digit ISBN):

(1) for a 13-digit ISBN, a prefix element - so far 978 or 979 are the only ones available

(2) the registration group element, (language-sharing country group, individual country or territory)

(3) the registrant element,

(4) the publication element, and

(5) a checksum character or check digit.

In the 10-digit ISBN above, the first digit, 0, indicates that the book was published in an English-speaking country; the digits 912843 represent the publisher (COMAP, Inc.); 07 are the identifying numbers that COMAP has assigned to the book; **the final digit, 1, is called the check digit of the ISBN.**

**To obtain the ISBN check digit:**

I. Multiply the first nine digits of the ISBN by 10, 9, 8, 7, 6, 5, 4, 3, and 2, respectively, and then compute the sum of these nine products.

2. Find the remainder when this sum is divided by 11.

3. Subtract the remainder from 11 to determine the check digit.

[NOTE: So that each possible check digit is a single digit, a check digit of 10 is written as X and a check digit is assigned the value of 0 if there is a remainder of 0.]

Formally, using modular arithmetic, we can say:

$$(10x_1 + 9x_2 + 8x_3 + 7x_4 + 6x_5 + 5x_6 + 4x_7 + 3x_8 + 2x_9 + x_{10}) \equiv 0 \pmod{11}.$$

For the ISBN 0-912843-07-1 that is discussed above:

I. 10(0) + 9(9) + 8(1) + 7(2) + 6(8) + 5(4) + 4(3) + 3(0) + 2(7) = 197

2. 197 = 11(17) + a remainder of 10.

3. Check digit = 11 – 10 = 1. (It checks!)

- An **ISBN** is a 13-digit number used to identify a book. The 13th digit is a check digit. The formula for the ISBN check digit is given below.

**Formula for the ISBN Check Digit**

$$d_{13} = 10 - (d_1 + 3d_2 + d_3 + 3d_4 + d_5 + 3d_6 + d_7 + 3d_8 + d_9 + 3d_{10} + d_{11} + 3d_{12}) \bmod 10$$

If $d_{13} = 10$, then the check digit is 0.

**Example:**

Determine the ISBN check digit for the book "*The Equation that Couldn't Be Solved"* by Marko Livio. The first 12 digits of the ISBN are 978-07432-5820-?

**Solution:**

$d_{13} = 10 - (d_1 + 3d_2 + d_3 + 3d_4 + d_5 + 3d_6 + d_7 + 3d_8 + d_9 + 3d_{10} + d_{11} + 3d_{12}) \bmod 10$

$d_{13} = 10 - [9 + 3(7) + 8 + 3(0) + 7 + 3(4) + 3 + 3(2) + 5 + 3(8) + 2 + 3(0)] \bmod 10$

$d_{13} = 10 - 97 \bmod 10$

$d_{13} = 10 - 7$

$d_{13} = 3$

Therefore, the check digit is 3.

- **UPC CHECK DIGIT**

A **UPC** is a 12-digit number that is used to identify a product such as a DVD, game, or grocery item. which stands for "Universal Product Code"

If we label the twelve digits of the UPC as $d_1, d_2, \ldots d_{12}$, then the UPC check digit is given by:

**Formula for the UPC Check Digit**

$$d_{12} = 10 - (3d_1 + d_2 + 3d_3 + d_4 + 3d_5 + d_6 + 3d_7 + d_8 + 3d_9 + d_{10} + 3d_{11}) \bmod 10$$

If $d_{12} = 10$, then the check digit is 0.

**Example:**

Find the check digit for the UPC of the Blu-ray disc release of the fil Jurassic World. The first 11 digits are 0-25192-21221-?

**Solution:**

$$d_{12} = 10 - (3(0) + 2 + 3(5) + 1 + 3(9) + 2 + 3(2) + 1 + 3(2) + 2 + 3(1)) \bmod 10$$

$$d_{12} = 10 - 65 \bmod 10$$

$$d_{12} = 10 - 5$$

$$d_{12} = 5$$

### Credit Cards Number

There are companies that issues credit cards that also uses modular arithmetic to determine whether a credit card number is valid.

The primary coding method is based on the **Luhn Algorithm**, which uses mod 10 arithmetic.

Credit card numbers are normally 13 to 16 digits long. The first one to six digits are used to identify the card issuer. The table below shows name of the identification prefixes used by four popular card issuers.

| Card Issuer | Prefix | Number of Digits |
|---|---|---|
| MasterCard | 51 to 55 | 16 |
| Visa | 4 | 13 or 16 |
| American Express | 34 or 37 | 15 |
| Discover | 6011 | 16 |

### Luhn Algorithm

- The Luhn algorithm, also known as the **modulus 10** or **mod 10** algorithm, is a simple checksum formula used to validate a variety of identification numbers, such as credit card numbers, IMEI numbers, Canadian Social Insurance Numbers.

## Validation of Credit Card using Luhn Algortihm

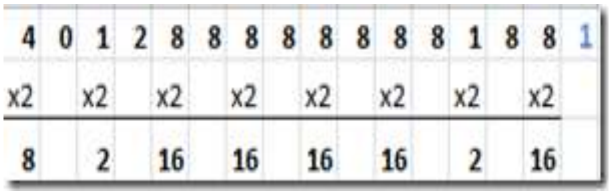
The last digit of the credit card number is a check digit. Beginning with the next-to-last digit and reading from right to left double every other digit. Treat any resulting two-digit number as two individual digits. Find the sum of the revised set of digits; the check digit is chosen such that the sum is congruent to 0 mod 10.

**Example 1:**

Check if the credit card number is valid or not valid. **4 0 1 2 8 8 8 8 8 8 8 8 1 8 8 1**

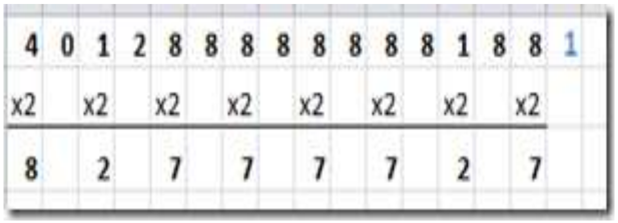
**Solution:**

**Step 1** - Starting with the check digit double the value of every other digit (right to left every 2nd digit)



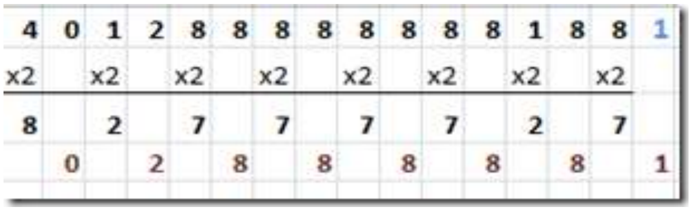
| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 0 | 1 | 2 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 1 | 8 | 8 | 1 |
| x2 | | x2 | | x2 | | x2 | | x2 | | x2 | | x2 | | x2 | |
| 8 | | 2 | | 16 | | 16 | | 16 | | 16 | | 2 | | 16 | |

**Step 2** - If doubling of a number results in a two digits number, add up the digits to get a single digit number. This will results in eight single digit numbers.



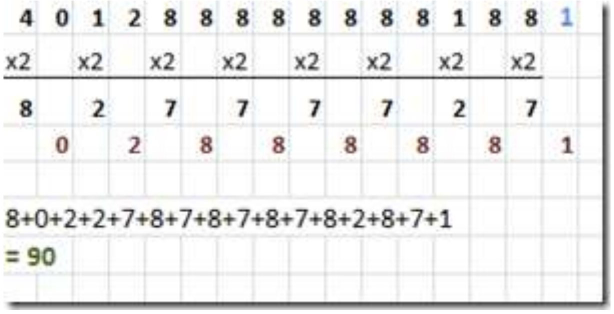
| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 0 | 1 | 2 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 1 | 8 | 8 | 1 |
| x2 | | x2 | | x2 | | x2 | | x2 | | x2 | | x2 | | x2 | |
| 8 | | 2 | | 7 | | 7 | | 7 | | 7 | | 2 | | 7 | |

**Step 3** - Now add the un-doubled digits to the odd places



| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 0 | 1 | 2 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 1 | 8 | 8 | 1 |
| x2 | | x2 | | x2 | | x2 | | x2 | | x2 | | x2 | | x2 | |
| 8 | | 2 | | 7 | | 7 | | 7 | | 7 | | 2 | | 7 | |
| | 0 | | 2 | | 8 | | 8 | | 8 | | 8 | | 8 | | 1 |

**Step 4** - Add up all the digits in this number



| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 0 | 1 | 2 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 1 | 8 | 8 | 1 |
| x2 | | x2 | | x2 | | x2 | | x2 | | x2 | | x2 | | x2 | |
| 8 | | 2 | | 7 | | 7 | | 7 | | 7 | | 2 | | 7 | |
| | 0 | | 2 | | 8 | | 8 | | 8 | | 8 | | 8 | | 1 |

8+0+2+2+7+8+7+8+7+8+7+8+2+8+7+1
= 90

***NOTE:*** *If the final sum is divisible by 10, then the credit card number is valid. If it is not divisible by 10, the number is invalid.*

**Example 2: 4 0 9 3 4 4 2 1 3 0 7 3 4 2 1 7**

**Step 1** - Starting with the check digit double the value of every other digit (right to left every 2nd digit)

| **4** | **0** | **9** | **3** | **4** | **4** | **2** | **1** | **3** | **0** | **7** | **3** | **4** | **2** | **1** | **7** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| X2 | | X2 | | X2 | | X2 | | X2 | | X2 | | X2 | | X2 | |
| 8 | | 18 | | 8 | | 4 | | 6 | | 14 | | 8 | | 2 | |

**Step 2** - If doubling of a number results in a two digits number, add up the digits to get a single digit number. This will results in eight single digit numbers.

| **4** | **0** | **9** | **3** | **4** | **4** | **2** | **1** | **3** | **0** | **7** | **3** | **4** | **2** | **1** | **7** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| X2 | | X2 | | X2 | | X2 | | X2 | | X2 | | X2 | | X2 | |
| 8 | | 18 | | 8 | | 4 | | 6 | | 14 | | 8 | | 2 | |
| **8** | | **1+8=9** | | **8** | | **4** | | **6** | | **1+4=5** | | **8** | | **2** | |

**Step 3** - Now add the un-doubled digits to the odd places

| **4** | **0** | **9** | **3** | **4** | **4** | **2** | **1** | **3** | **0** | **7** | **3** | **4** | **2** | **1** | **7** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| X2 | | X2 | | X2 | | X2 | | X2 | | X2 | | X2 | | X2 | |
| 8 | | 18 | | 8 | | 4 | | 6 | | 14 | | 8 | | 2 | |
| **8** | **0** | **1+8=9** | **3** | **8** | **4** | **4** | **1** | **6** | **0** | **1+4=5** | **3** | **8** | **2** | **2** | **7** |

**Step 4** - Add up all the digits in this number

| 4 | 0 | 9 | 3 | 4 | 4 | 2 | 1 | 3 | 0 | 7 | 3 | 4 | 2 | 1 | 7 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| X2 | | X2 | | X2 | | X2 | | X2 | | X2 | | X2 | | X2 | |
| 8 | | 18 | | 8 | | 4 | | 6 | | 14 | | 8 | | 2 | |
| **8** | **0** | **1+8=9** | **3** | **8** | **4** | **4** | **1** | **6** | **0** | **1+4=5** | **3** | **8** | **2** | **2** | **7** |

$$\mathbf{8+0+9+3+8+4+4+1+6+0+5+3+8+2+2+7=70}$$

Therefore, the credit card number **4 0 9 3 4 4 2 1 3 0 7 3 4 2 1 7** is valid since the sum 70 is divisible by 10.

## Cryptology

- Cryptology is the study of making and breaking secret codes.

These codes are used to send messages between people, companies or nations. It is hope that by devising a code that is difficult to break, the sender can prevent the communication from being read if it is interpreted by an unauthorized person.

Before we discuss how messages are coded, we need to define few terms:

- **Plaintext**- is a message before it is coded.

  SHE WALKS IN BEAUTY LIKE THE NIGHT

- **Ciphertext**- is encrypted text transformed from plaintext using an encryption algorithm.

  ODA SWHGO EJ XAWQPU HEGA PDA JECDP

- **Encryption**- the method of changing from plaintext to ciphertext.

The line from the poem was encrypted by substituting each letter in plaintext with the letter that is 22 letters after the letter in the alphabet.

This is called the ***cyclical coding theme*** because each letter of the alphabet is shifted the same number of position, the original alphabet and the shifted alphabet is shown below.

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ |

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |

- **Decrypt-** to decrypt means to take the ciphertext messages and write it in a plaintext.

  If a cryptologist think a message has been encrypted using a cyclical substitution code like the shown above, the key can be found by taking a word from the message (usually one of the longer words) and continuing the alphabet for each letter of the word.
  This method is shown below

| | | | | | |
|---|---|---|---|---|---|
| X | A | W | Q | P | U |
| Y | B | X | R | Q | V |
| Z | C | Y | S | R | W |
| A | D | Z | T | S | X |
| B | E | A | U | T | Y |

SHIFT
FOUR
POSITION

Cyclical encrypting using the alphabet is related to modular arithmetic.

**Numerical Equivalence for the Letters of the Alphabet**

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

If the encrypting code is to shift each letter of the plaintext message to ciphertext. Then the corresponding letter in the ciphertext message is given by

$$C = (p + m) \bmod 26$$

Where

p= the numerical equivalent of the plaintext letter

c= the numerical equivalent of the ciphertext letter

m= position through the alphabet

**Example:**

Code the plaintext letter S in the word SHE, we use the congruence

***C* = *(p* + *m)* mod 26**

Looking at the numerical equivalent of the Alphabet letter, S is in 19 so that p= 19, m=22 (the number of position the letter shifted)

$C = (19 + 22) \text{ mod } 26$

$C = 41 \text{ mod } 26$

$C = 15$

The 15th letter is O. So the code for S is O.

For more knowledge about Application of Modular Arithmetic, please check the link provided;
https://www.irishtimes.com/news/science/modular-arithmetic-you-may-not-know-it-but-you-use-it-every-day-1.3268649
http://www.personal.psu.edu/jxs23/courses/math035/fa11/handouts/27_check_digits_isbn_upc_codes.pdf
https://www.luther.edu/bergerr/assets/Math_260_Check_digits.pdf

## REMEMBER

- An **ISBN** is a 13-digit number used to identify a book. The 13th digit is a check digit. The formula for the ISBN check digit is given below.
- A **UPC** is a 12-digit number that is used to identify a product such as a DVD, game, or grocery item. which stands for “Universal Product Code”
- The Luhn algorithm, also known as the **modulus 10** or **mod 10** algorithm, is a simple checksum formula used to validate a variety of identification numbers, such as credit card numbers
- Cryptology is the study of making and breaking secret codes.

APPLICATION

## ACTIVITY: Check my Value

**Direction:** Use the application of Modular Arithmetic to solve for the following problem.

1. The Library Publishing house want to know the ISBN check digit of Math Power book with the ISBN: 978-971-0499-31-?

2. Jay’s restaurant wants to know if the credit card use by the costumer is valid. The credit card number is 4000 0012 3456 7899.

# Lesson 3: Introduction to Group theory

## Introduction to Group

- **Algebraic System**
  - Is a set of elements with one or more operations combining the elements. The real numbers with the operations of addition and multiplication are example of the algebraic system.

Mathematicians classify this particular algebraic system term as ***field.***

In previous lesson, we discussed the modulo *n*. Consider the set {0, 1, 2, 3, 4, 5} and addition modulo 6. The set of elements is {0, 1, 2, 3, 4, 5} and the operation addition modulo 6. In this case there is only one operation. This is an example of an algebraic system called ***group.***

## Group

- Is a set of elements, with one operation, that satisfies the four properties.

### Properties of Group

1. The set is closed with respect to the operation.
2. The operation satisfies the associative property.
3. There is an identity element.
4. Each element has an inverse.

Note from the present definition that a group is an algebraic system with one operation and that the operation must have a certain characteristic. The first of these are the characteristics that a set is formed with respect to the operation.

1. **Closure** means that if any two elements are combined using the operation, the result must be an element of the set.

   **Example:**

   - The set (0, 1, 2, 3, 4, 5) with addition modulo 6 as the operation is closed. If we add the numbers of this and modulo 6, the result is always a member of the set. For instance, (3 + 5) mod 6 = 2 and (1 + 3) mod 6 = 4.

   - Consider the whole number (0, 1, 2, 3, 4,…) with multiplication as the operation. If we multiply two whole numbers, the result is a whole number. For instance, 5 x 9 = 45 and 12 x 15 = 180. Thus, the set of whole numbers is closed using multiplication as the operation. However, the set of whole numbers is not closed when the operation is division. For example, even though 36 ÷ 9 = 4 (a whole number), 6 ÷ 4 = 1.5 (not a whole number). Therefore, the set of whole numbers is not closed with respect to division.

2. The second requirement of a group is that the operation must satisfy the **associative property**. Recall that the associative property of addition states that; $a + (b + c) = (a + b) + c$. **Addition modulo 6 is an associative operation.** For instance, if we use the symbol ∇ to represent addition modulo 6, then

$$2 \nabla (5 \nabla 3) = 2\nabla (8 \bmod 6) = 2 \nabla 2 = 4$$

And

$$(2 \nabla 5) \nabla 3 = (7 \bmod 6) \nabla 3 = 1 \nabla 3 = 4$$

Thus $2 \nabla (5 \nabla 3) = (2 \nabla 5)\nabla 3$

3. **Identity element** is an element that, when combined with second element using the group's operation, always returns the second element. As an illustration, if zero was added to a number, there is no change. Example:

$6 + 0 = 6$ and $0 + 10 = 10$.

- The number zero is called an ***additive identity.***

Similarly, if we multiply any number by 1, there is no change. Example:

$\frac{2}{3} \cdot 1 = \frac{2}{3}$ and $1 \cdot 3 = 3$

- The number 1 is called the ***multiplicative identity***.

For the set (0,1, 2, 3, 4, 5) with addition modulo 6 as the operation, the identity element is 0. But take note that identity element does not always have to be zero or one.

- The number 3 and -3 are called ***additive inverses***.

Adding these two numbers result in the additive identity 3 +(-3) = 0.

- The numbers $\frac{2}{3}$ and $\frac{3}{2}$ are called the ***reciprocals*** or ***multiplicative inverses***.

Multiply these two numbers results in the multiplicative identity.

$$\frac{2}{3} \cdot \frac{3}{2} = 1$$

4. The last requirement of a group is that each element must have an ***inverse***. This is a little difficult to see for the set (0, 1, 2, 3, 4, 5) with addition modulo 6 as the operation. However, using addition modulo 6, we have

$(0 + 0) \bmod 6 = 0$ $\quad\quad$ $(2 + 4) \bmod 6 = 0$

$(1 + 5) \bmod 6 = 0$ $\quad\quad$ $(3 + 3) \bmod 6 = 0$

The above equations show that 0 is its own inverse, 1 and 5 are inverses, 2 and 4 are inverses, and 3 is its own inverse. Therefore, every element of this set is inverse.

**Commutative Property** for an operation states that the order in which two elements are combined does not affect the result. For each of the groups discussed thus far, the operation has satisfied the commutative property. For example, the group (0, 1, 2, 3, 4, 5) with addition modulo 6 satisfies the commutative property, since for instance, $2 + 5 = 5 + 2$.

**Commutative groups** or **abelian groups**

- Groups in which the operation satisfies the commutative property. Named after Niels Abel.

**Nonabelian group**

- Is a group whose operation does not satisfy the commutative property.

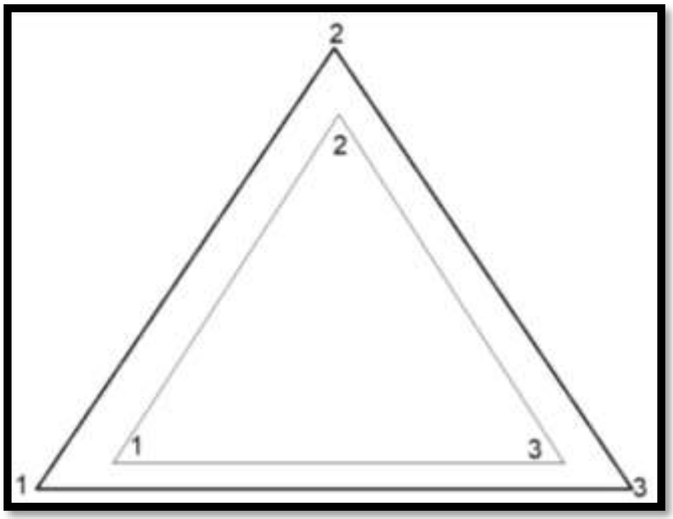
**Symmetry Group**

- An extension of group which plays an important role in the study of atomic reactions.
- It is based on regular polygons.

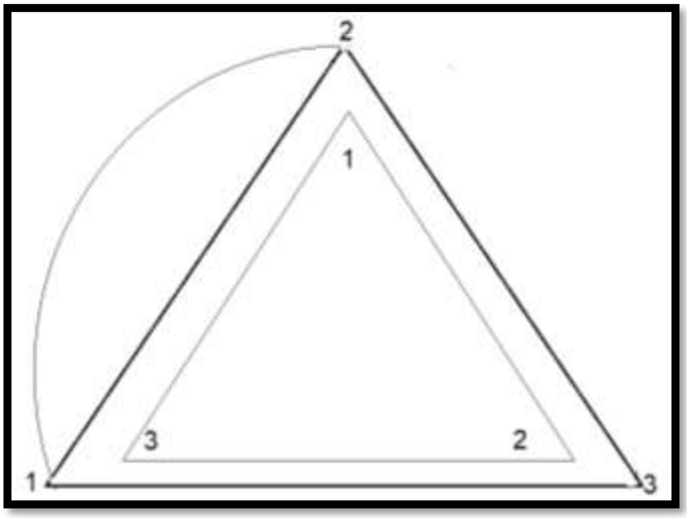
**Regular polygons –** is a polygon all of whose sides have the same length and all of whose angles have the same measure.

Consider the two equilateral triangles, one placed inside the other, with their vertices membered clockwise from 1 to 3. The larger triangle is ***reference triangle***. If we pick up the smaller triangle, there are several different ways in which we can set it back in its place. Each possible positioning of the inner triangle will be an element of the group. For instance, we can pick up the triangle and replace it exactly as we found it. We will this position *I*, it will represent no change in position.

Now pick up the smaller triangle, rotate it 120° clockwise, and let it down again in top of the reference triangle. The result is shown below:



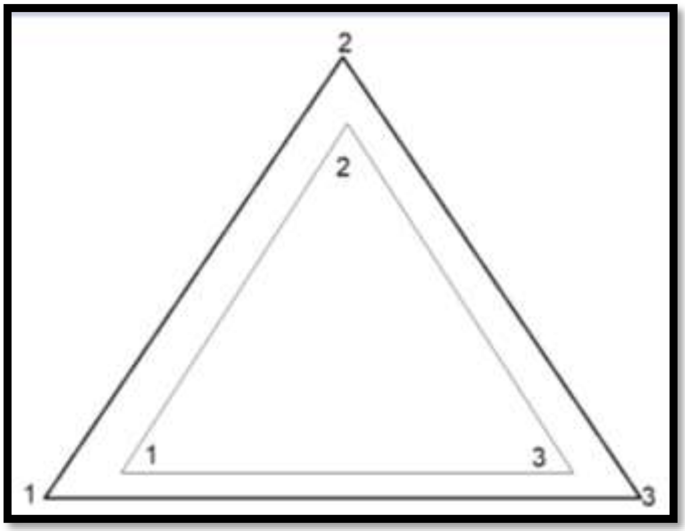
I



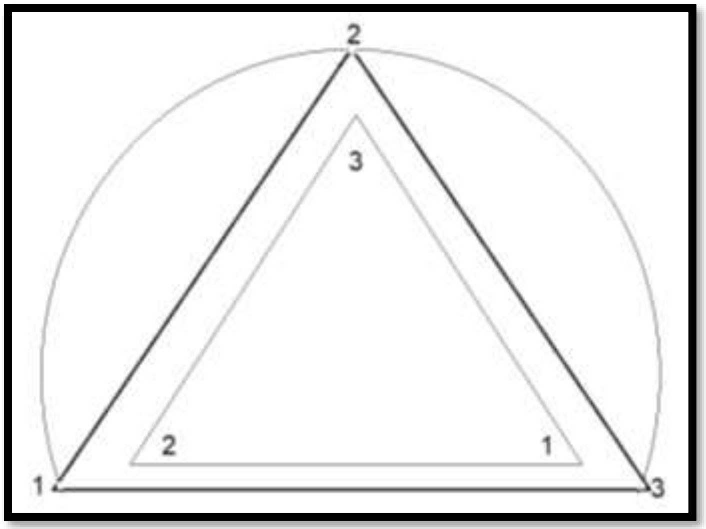
$R_{120}$

Note that the vertex originally at vertex 1 of the reference triangle is not at vertex 2, 2 is now at 3, and 3 is now at 1. We call the rotation of the triangle 120° clockwise $R_{120}$.

Now return the smaller triangle to its original position, where the numbers on the vertices of the triangles coincide. Consider a 240° clockwise rotation of the smaller triangle. The result of the rotation is shown below.



I



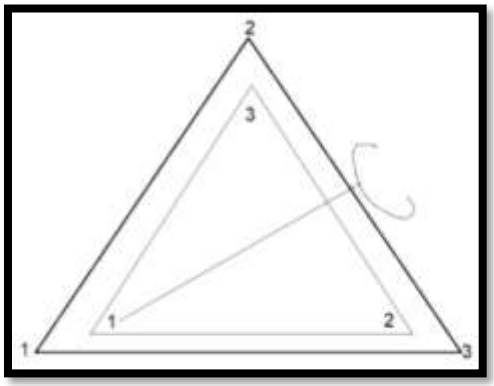
$R_{240}$

Note that the vertex originally at vertex 1 of the reference triangle is now at vertex 3, 2 is now at 1 and 3 is now at 2. We call the rotation of the triangle 240° clockwise $R_{240}$.

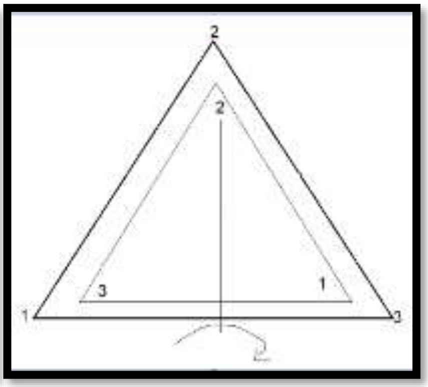
If the original triangle were rotated 360°, there would be no apparent of change. The vertex at 1 would return to 1, the vertex 2 would return to 2, and the vertex at 3 would return to 3. Because this rotation does not produce a new arrangement of the vertices, we consider it the same as the element we named *I*.

If we rotate the inner triangle *counterclockwise* 120°, the effect is the same as rotating it 240° clockwise. The rotation does not produce a different arrangement of the vertices. Similarly, a counterclockwise rotation of 240° is the same as rotation of 120°.

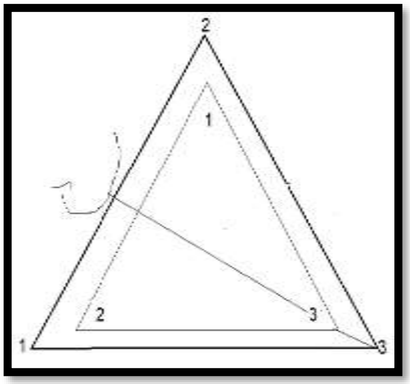
In addition of rotating the triangle clockwise 120° and 240° as we did above, we could rotate the triangle about a line of symmetry that goes through a vertex before setting the triangle back down, because there are three vertices, there are three possible results. These are shown below:



$R_1$



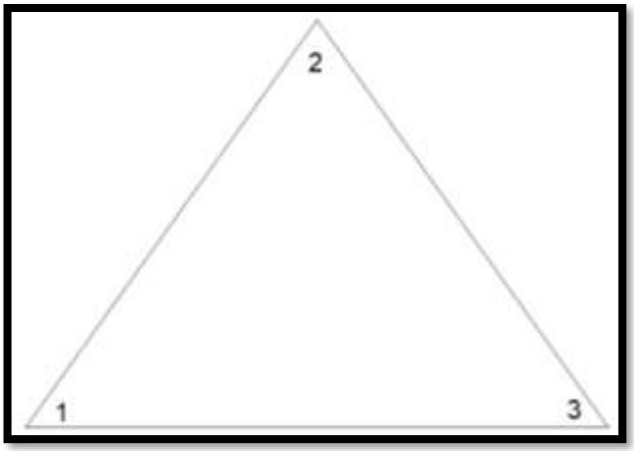
$R_2$



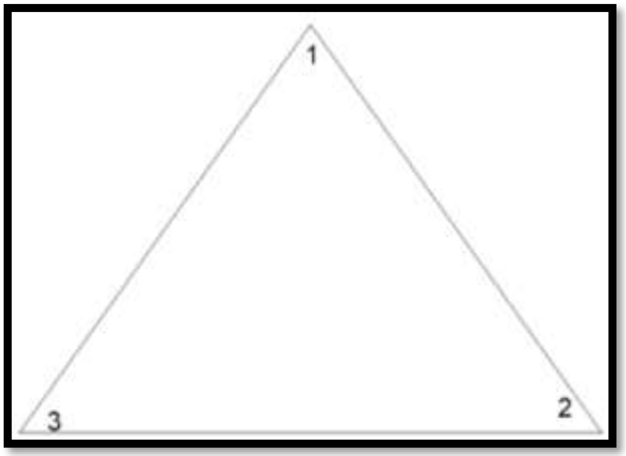
$R_3$

For notation $R_1$ The bottom left vertex does not change but vertices 2 and 3 are interchanged. If we rotate the triangle about the line of symmetry through the top vertex, rotation $R_2$ vertex 2 does not change but vertices 1 and 3 interchanged. For rotation $R_3$, the bottom right vertex does not change, but vertices 1 and 2 are interchanged.

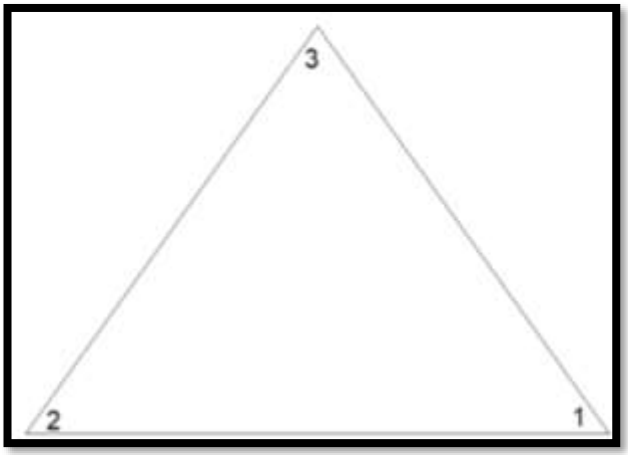
The six propositions of the vertices we have seen, thus far are only possibilities. *I* (the triangle that without any rotation) $R_{120}$ , $R_{240}$, $R_{1,}$ $R_{2,}$ $R_3$. These propositions are shown below without reference triangle).



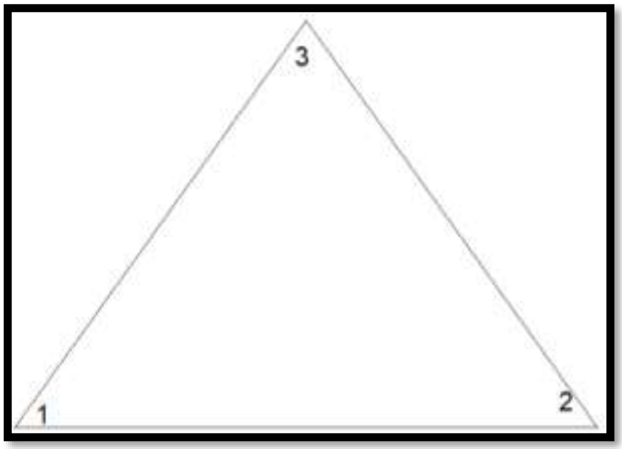
$I$



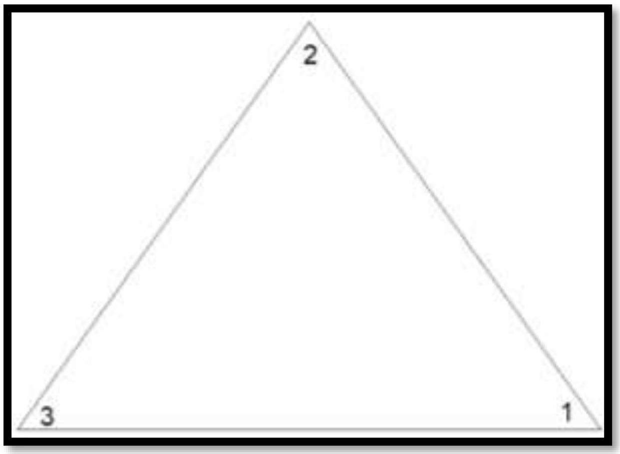
$R_{120}$



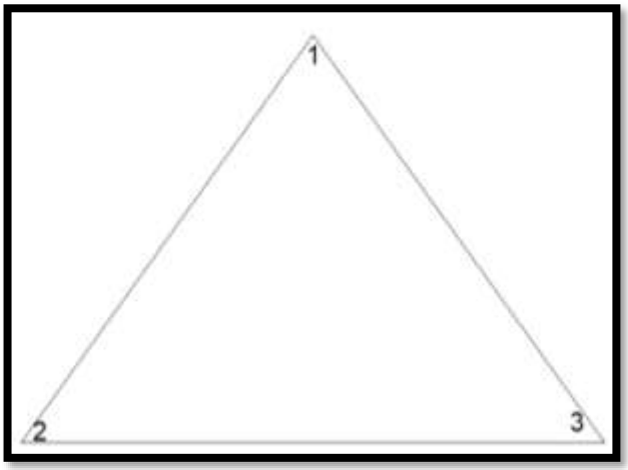
$R_{240}$.



$R_1$



$R_2$

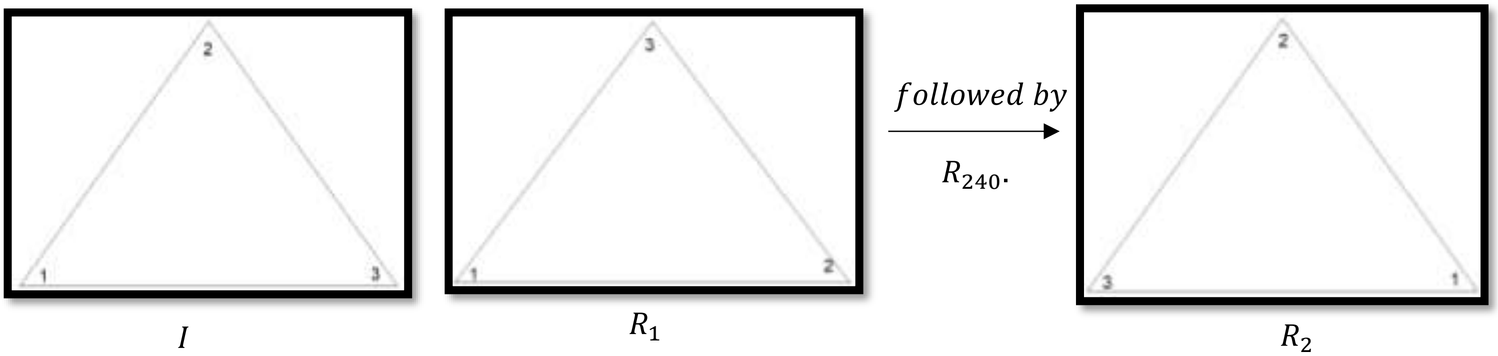


$R_3$

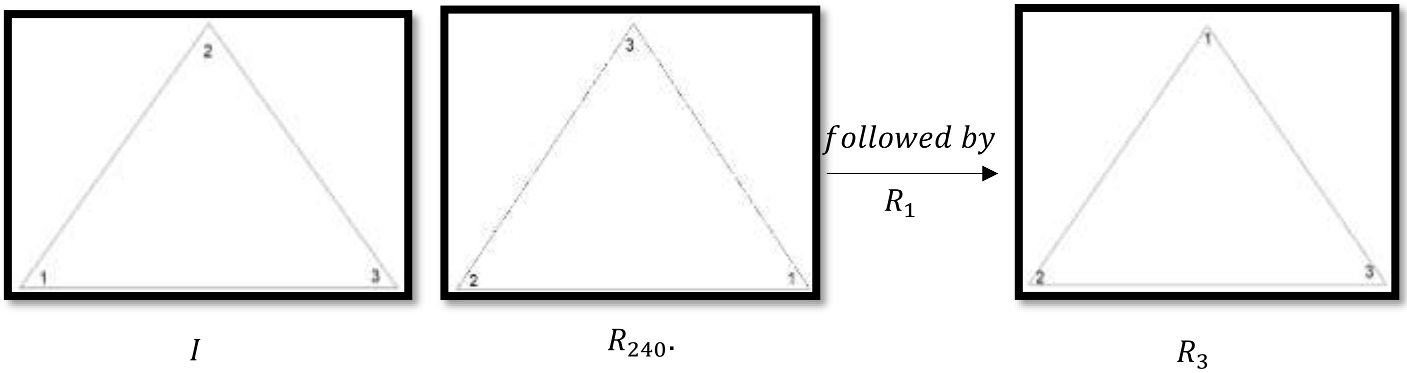
As we will see these rotations are elements that form a group.

A group must have an operation, a method by which two elements of the group can be combined to form a third element that must also be a member of the group. (Recall that a group operation must be closed) The operation we will used is called **"followed by"** and is symbolized by $\Delta$**.** Next we show an example of how the operation works.

Consider $R_1 \Delta R_{240}$. This means we rotate the original triangle, labeled as *I*, about the line of symmetry through vertex 1 "followed by" (without returning to the original position) a clockwise rotation of 240°. The result is one of the elements of the group, $R_1$. This operation is shown below.



Now try reversing the operation, and consider $R_{240} \Delta R_1$.This means we rotate the original triangle, *I*, clockwise 240° "followed by" (without returning to the original position) a rotation about the axis of symmetry through the bottom left vertex. Note that the result is an element of the group, namely $R_1$, as shown below.



From these two examples, $R_1 \Delta R_{240} = R_2$ and $R_{240} \Delta R_1 = R_3$. Therefore, $R_1 \Delta R_{240} \neq R_{240} \Delta R_1$, which means the operation "followed by" is not commutative.

We have stated that the elements $R_{120}$, $R_{240}$, $R_1$, $R_{2,}$ $R_3$ ,and *I,* with the operation "followed by", form a group. However, we have not demonstrated this fact, so we will do so now.

As we have seen, the set is closed with respect to the operation $\Delta$. To show that the operation $\Delta$ is associative, think about the meaning of $x\Delta(y\Delta z)$ and $(x\Delta y)\Delta z$, where $x, y$ and $z$ are elements of the group $x\Delta(y\Delta z)$ means $x$, followed by the result of $y$ followed $z$. $(x\Delta y)\Delta z$ means $x$ followed by $y$, followed by $z$. For instance,

$$R_1\Delta(R_I\Delta R_3) = R_1\Delta R_{120} = R_3 \text{ and } (R_1\Delta R_2)\Delta R_I = R_{120}\Delta R_1 = R_I$$

All the remaining combinations of elements can be verified similarly.

The identity element is *I* and can be thought as "no notation". To see each element has an inverse, verify the following

$$R_{120}\Delta R_{240} = I \qquad R_I\Delta R_1 = I \qquad R_1\Delta R_2 = I \qquad R_2\Delta R_3 = I$$

Your work should show that every element has an inverse. (The inverse of *I* is *1).* Thus, the four conditions of a group are satisfied.

To determine the outcome of the "followed by" operation on two elements of the group, we drew triangles and then rotated them as directed by the type of rotation. Form a mathematical point of view, it would be nice to have a symbolic (rather than geometric) way of determining the outcome. We can do this by creating a mathematical object that describe the geometric object.

Note that any rotation of the triangle changes the position of the vertices. For $R_{120}$ the vertex originally at position 1 moved to position 2, the vertex at 2 moved to 3 and the vertex 3 moved to 1. We can represent this as

$$R_{120} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Similarly, for $R_1$, the vertex originally at position 1 moved to position 3, the vertex at 2 remained at 2, and the vertex at 3 moved to 1. This can be represented as

$$R_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

The remaining four elements can be represented as

$$I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad R_{240} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad R_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad R_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

**Permutation Groups**

- The triangular symmetry group discovered previously is an example of group called ***permutation group.***

**Permutation**

- Is a rearrangement of objects.

For instance, if we start with the arrangement of objects (● ♥ ♣), then one permutation of these objects is the rearrangement (♥ ♣ ●). If we consider each permutation of these object as an element of a set, then the set of all possible permutations form a group. The elements of a group are not numbers or the objects themselves, but rather the different permutations of the objects that are possible.

If we start with the number 1, 2, 3 we can repeat permutation of the numbers using the same symbol method that we used for the triangular symmetry group. For example, the permutation that rearranges 123 to 231 can be written

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Which means that 1 is replaced by 2, 2 is replaced by 3, and 3 is replaced by 1.

There are only six distinct permutation of the numbers 123. We list and label these below. The identity element is named *I*.

$$I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$C = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, D = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, E = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

The operation for the group is “followed by”, which we call again denote by the symbol Δ. One can verify that the six elements along with this operation do indeed form a group.

For more knowledge about Introduction of Group theory, please check the link provided;
https://www.math.upenn.edu/~mlazar/math170/notes07.pdf
https://www.slideshare.net/DurgeshChahar/group-theory-68263207

## REMEMBER

- **Group**
- Is a set of elements, with one operation, that satisfies the four properties.

**Properties of Group**

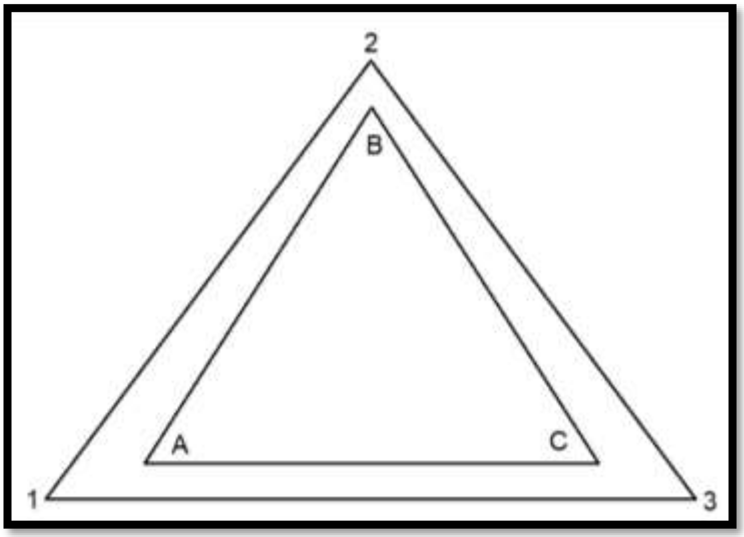
1. The set is closed with respect to the operation.
2. The operation satisfies the associative property.
3. There is an identity element.
4. Each element has an inverse.

- **Commutative groups** or **abelian groups**
- Groups in which the operation satisfies the commutative property. Named after Niels Abel.
- **Nonabelian group**
- Is a group whose operation does not satisfy the commutative property.
- **Permutation**
- Is a rearrangement of objects.

## APPLICATION

**ACTIVITY:**

**Direction:** Rotate the smaller triangle, 120°, 240° and 360° and find its vertex. After that show that 123 and ABC has six permutations.



## REFERENCES

https://brilliant.org/wiki/modular-arithmetic/

https://networlding.com/isbn-vs-upc/

https://www.maths.gla.ac.uk/~mwemyss/teaching/3alg1-7.pdf