Math Anthology

Author: Shivani AC

Index:

Preface

1. The Equability Factor
2. The Marble Proposition
3. Interpretation of *i* Using the Argand Plane
4. Construction of Ellipses Using the Foci Method
5. Addition and Multiplication in Integer Modulo Integer Number Systems
6. Scalar and Vector Triple Products and their Geometrical Interpretation

Preface

Throughout my journey in mathematics, I've had the privilege of exploring diverse mathematical concepts and theories, both within the structured environment of classrooms and through independent study. This anthology comprises a collection of 6 research papers, each delving into different branches of mathematics, ranging from algebra and complex numbers to geometry, number theory.

Writing these articles has been instrumental in deepening my understanding of the intricacies of various mathematical principles. It has not only honed my analytical skills but also reignited my passion for the beauty and elegance inherent in mathematical structures and proofs. Each article in this anthology is a testament to my fascination with the world of mathematics and my commitment to sharing its wonders with fellow enthusiasts.

To everyone reading this anthology, I hope you have as much fun as I had writing each feature article in here!

The Equability Factor

Abstract:

This project is our take on equable shapes and on the question: An eccentric artist says that the best paintings have the same area as their perimeter numerically. Let us not argue whether such sizes increase the viewer's appreciation, but only try to find what sides - in integers only - a rectangle must have if its area and perimeter are to be equal.

Introduction:

Ever heard of perfect shapes? Never?

Contrary to several people's beliefs, perfect shapes do exist. Perfect shapes or equable shapes refer to two dimensional shapes that have the same numerical perimeter and area. While in three dimensions, a shape is called equable when its surface area is numerically equal to its volume.

For any given shape (all dimensions), there is always a similar equable shape!

For example, a circle with a radius of r = 2, has both a perimeter and area of 4π and a cube with side length six has equal surface area and volume of 216.

$$\begin{aligned}\text{Circumference} &= 2.\pi.r\\ &= 2.\pi.2\\ &= \mathbf{4\pi}\end{aligned}$$

$$\text{Area} = \pi.r^2 = \pi.2^2 = \mathbf{4\pi}$$

$$\begin{aligned}\text{Surface area} &= 6.a^2\\ &= 6.6^2\\ &= \mathbf{216}\end{aligned}$$

$$\text{Volume} = a^3 = 6^3 = \mathbf{216}$$

While talking about areas and perimeters, it is important to consider the scaling and units. An area of a shape cannot be equal to the perimeter except in a particular relative unit of measurement. For example, if the shape has equal areas and perimeters while using yards, they might not maintain the same equality when the unit is converted to meters or feet.

Moreover, this difference also tends to be contrary to what the name "equable" implies. Changing the size while leaving the shape intact changes an 'equable shape' into a 'non-equable shape'. To check this difference, the use of integer dimensions becomes necessary.

While combining the restriction on integer dimensions to a shape being equable, the probability of equable shapes becomes significantly more limited than either of the conditions on their own.

For instance, there are infinitely many Pythagorean triples that describe integer-sided right triangles, and there are infinitely many equable right triangles having non-integer sides. However, there are only two equable right triangles with integer dimensions.

In this project, we have set out to find equable rectangles while combining the restriction of exclusively using integer dimensions. And here begins our quest to find out the 2 equable integer rectangles that ever exist in the entire universe of shapes!

The Experiment - A Quadrilogue:

(An - Anicham; Ak - Akshitha; Ad - Adhvighaa; Sh - Shivani)

Ad - Let's start by finding at least one that works.

Ak - Okay, let's start with squares then.

An - What? Squares? All the sides are the same in squares. How do they become rectangles?

Sh - All squares have the properties of a rectangle! The opposite sides are parallel and equal to each other, each interior angle is equal to 90 degrees, the sum of all the interior angles is equal to 360 degrees, the diagonals bisect each other, both the diagonals have the same length and so on. So, all squares are rectangles! However, remember that all rectangles are not squares because unlike squares rectangles don't have all the sides equal to each other and don't have diagonals that bisect each other perpendicularly...

An - Ohh! I get it now. In that case, we can start with squares and see if they work.

Sh - Okay. Let's make a table then.

[draws the following table]

Length of Side of Square = a	**Area = a^2**	**Perimeter = 4a**

1	1	4
2	4	8
3	9	12
4	16	16
5	25	20
6	36	24

An - We've got a winner! 4 works. Can any other squares work?

Ad - That may be the only one. The area is quickly getting larger than the perimeter as we increase the length of the square...

Ak - Yes, once we pass the side length of 4, it does not seem possible for the perimeter to catch up with the area.

Sh - Area's definitely winning that race! So, what's next?

An - A table is more complicated for non-squares because of the two different measurements of length and breadth.

Ak - Yeah... How are we going to make that work?

Ad - Well, let's start with testing a few with trial and error? We'll get some ideas after that for sure...

Sh - Yes, that makes sense. What about 2 and 3?

(2x3 rectangle drawing)

Ak - Nope! Perimeter of 10 and area of 6. Doesn't work.

An - So, then what about 2 1/2 and 3? That's a perimeter of 11 and area of 7 1/2 . That's closer.

Ad - Let's try using whole numbers first and see what happens.

An - Sure, let’s stick with those because our main goal is to use integer dimensions and make sure there isn't an anomaly with respect to units.

Ak - Okay, let’s try 4 and 3… 4 times 3 is 12. 4 + 3 is 7, double that and we get 14.

(4x3 rectangle drawing)

An - Close!

Sh - 5 times 3 is 15. 5 + 3 is 8, double that is 16.

(5x3 rectangle drawing)

Ad - Even closer!

Ak - I don’t think it will ever work if the area is odd, because the perimeter has to be even.

Sh - You’re right. After all, to find the perimeter, we add the two numbers and double the sum. It HAS to be even.

An - Well, that’s odd!

[laughing at the joke made]

Ad - Okay, so we were close with 5 and 3, but we need an even product. How about 6 and 3 then?

Sh - 6 times 3 is 18. 6 + 3 is 9 and double 9 is 18.

(6x3 rectangle drawing)

Ak - Hooray! Another winner! We found one more! Is that all of them?

[There is a long pause during which everyone thinks about the problem.]

An - I don’t know, but I don’t think so. What are we doing each time we try an example?

(axb rectangle drawing)

Sh - If we call the side lengths a and b , then area is a times b . *[writes* Area = ab *]* To find perimeter, we've been adding a and b and then doubling that sum. *[writes* Perimeter = $2(a + b)$*]* Then we want the area and perimeter to be equal, so...

An - Oh, I see. We need to find rectangles with sides lengths a and b that make the area ab equal to the perimeter, which is... *[pauses to write* $ab = 2(a + b)$ *]*...twice the sum of a and b . Now we can solve for a . We'll multiply first. *[mumbles about the distributive property while writing the following]*

$$\mathit{Area} = ab$$

$$\mathit{Perimeter} = 2(a+b)$$

If area and perimeter are equal then,

$$ab = 2(a + b)$$

$$ab = 2a + 2b$$

Ad - Then we can subtract $2a$ from both sides. And that will be...*[writes the following]*

$$ab - 2a = 2b$$

An - Right! And ab minus $2a$ is the same as a times the quantity b minus 2. *[writes the following]*

$$a(b - 2) = 2b$$

Sh - Then you can divide both sides by b minus 2 such that you have only a on one side. *[writes the following]*

$$a(b - 2) = 2b$$

$$a = (2b)/b-2$$

Ak - Oh, so there are lots of rectangles!! We can plug in whatever side length we choose for b and we'll always get the length of side a.

Ad - Let's try the two we've found so far. If you put 6 in for b you get $12/4 = 3$, and that was our other side length.

Sh - And if you put 4 in for b you get $8/2 = 4$ as our other side length. Yup, it checks!

Ak - So, how many more rectangles are there that work? Can we really put any number in for *b* and it will give us the *a* that works for it?

An - *[after a brief pause]* Sure. Like if you put in 10 as side length *b* , that gives us 20/8 for *a* . So for a 2.5 × 10 rectangle, the area is 25 square units and the perimeter is 25 units.

Ad - Guess they are not all going to be our "whole" numbers are they?

Sh - Yeah, but not every number will work...

An - Exactly! For example, in case we had a side length of 1, we'll get a negative value.

Ak - So basically, since *a = (2b)/b-2* and *a* and *b* are measurement that are always greater than 0... *[writes the following]*

$$b > 0$$

$$b-2 > 0$$

$$b > 2$$

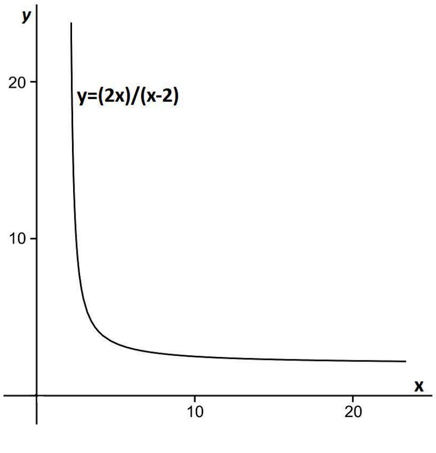
...*b* is always greater than 2.

Ad - So, there are an infinite number of these rectangles but yet limited to certain restrictions?

An - Yes! You got that right!

Sh - Wait, if I am presuming this right, it might be possible to draw a graph for this.

Ak - Really? Let's give it a try then. *[draws the following graph]*



An - So, according to this graph, if you continue halving the difference in lengths and subtracting this and doubling the breadth and adding it on you can find many more rectangles with equal perimeter and area.

Sh, Ak, Ad - Wait, what? You might want to walk us through this...

An - So ultimately, there is a pattern linking the length of the sides of successive equable rectangles.

Starting at the square with sides 4 by 4 and then the rectangle with side length of 3 and breadth of 6...

The difference between the lengths 3 and 4 is 1, the difference between the breadths 4 and 6 is 2.

To get from 3 to the next length you halve the difference between 4 and 3 and subtract this from 3, to get 2.5.

To get from 6 to the next breadth you double the difference between 4 and 6 and add this to 6, to get 10.

So, if you continue using this method you can find many more rectangles with equal perimeter and area.

Ak - So, what you're trying to say is:

$$L_3 = L_2 - (L_1 - L_2)/2$$

$$B_3 = B_2 + 2(B_2 - B_1)$$

An - Yes!

Sh - So, we'll get 4 by 4, 3 by 6, 2.5 by 10, 2.25 by 18, 2.125 by 34 and so on?

An - YES!!

Ad - That's amazing! I think we have reached our goal on solving this problem.

Ak - Yes, we have, haven't we?

An, Sh - WE GUESS SO!!

Result:

According to the above conducted experiment, it has been found, through a trial and error process, that there are only two rectangles which are both equable and have integral values for their lengths and breadths.

The relationship between the length and the breadth has been found to be $a = (2b)/b-2$ where a is the length and b is the breadth and the two equable rectangles have been found to have the dimensions 4 by 4 and 3 by 6 respectively.

In addition, a graph on the dimensions of equable rectangles has also been plotted. Thus, the relationship between the dimensions of various equable rectangles have been determined to be $L_3 = L_2 - (L_1 - L_2)/2$ and $B_3 = B_2 + 2(B_2 - B_1)$ where L is the length and B is the breadth.

Conclusion:

With this ends our quest to find out the 2 equable integer rectangles - the rectangles having the dimensions of 4 by 4 and 3 by 6 respectively - that exist. However, there are plenty other equable shapes that exist with integer sides, including one circle, five triangles, three rectangular pentagons, 2 other quadrilaterals and many more trapezoids, irregular quadrilaterals and irregular pentagons.

In addition, there are also over 200 equable integer solids including bicones, bicylinders, quadrilateral prisms, triangular prisms, trirectangular tetrahedrons, dipyramids and so on. But all of these shapes are still waiting to be explored by us and will remain on our bucket list until the next time!

Bibliography:

1. https://nrich.maths.org/6398/solution
2. http://mathpractices.edc.org/pdf/Rectangles_with_the_Same_Numerical_Area_and_Perimeter.pdf
3. https://en.wikipedia.org/wiki/Equable_shape
4. http://lostmathlessons.blogspot.com/2017/09/equable-shapes-with-integer-dimensions.html
5. http://www.balmoralsoftware.com/equability/list.htm
6. https://miro.com/app/board/o9J_lDYMdBo=/

The Marble Proposition

Abstract:

This project is our take on the question: A board has some holes to hold marbles, red on one side and blue on the other. Interchange the positions by making one move at a time. A marble can jump over another to fill the hole behind. Start with one pair, then 2 and more. Find the relationship between the number of pairs of marbles and the number of moves while doing so.

Introduction:

A marble is a small spherical object often made from glass, clay, steel, plastic, or agate. Marbles date back to around 2500 BCE and this was confirmed when small marbles made of stone were found by archeologists at excavation near Mohenjo-daro, a site associated with the Indus Valley Civilization. They were also found in excavations of sites associated with Chaldeans of Mesopotamia and ancient Egypt.

Marbles vary in size but they're commonly about 13 mm in diameter. However, they may range from less than 1 mm to over 8 cm, while some art glass marbles for display purposes are over 30 cm wide. There are various types of marbles, and names vary from locality to locality. They are made using many techniques which can be categorized into two general types: hand-made and machine-made.

Marbles are often collected, both for nostalgia and for their aesthetic colors. They are also used for a variety of games and one such game is chinese checkers!

Chinese Checkers is a game that is based on an earlier Victorian game called Halma which is played on a square 16 x 16 checkerboard with the same rules. Chinese Checkers has been a beautiful experience which we all have enjoyed throughout our childhood and are enjoying even today.
It is a simple game where each player races all of one's pieces into the star corner on the opposite side of the board before the opponents do the same. But what does this have to do with the experiment conducted?

Well, this experiment is basically a linear version of Chinese Checkers. The setup and operation technique of this experiment coincides with that of Chinese Checkers.

Just like Chinese Checkers, in this experiment, we will be setting a board that has some holes to hold marbles, red on one side and blue on the other. We then will be interchanging the positions of the marbles by making one move at a time such that a marble can also jump over another to fill the hole behind.

However, we will additionally find the mathematical relationship between the number of pairs of marbles and the number of moves while doing so with increasing numbers of pairs of marbles. And here starts our pursuit to find out that arithmetic relationship with the help of a contained marble experiment setup.

Experiment:

Our experiment starts with one pair of marbles and then increases arithmetically upto 5 pairs of marbles. Each set has been given enough attention to make sure we have made the least possible number of moves to interchange the position of the marbles. After a couple of failures and wrong moves, we found a conclusive move technique that works with the least possible moves. Here's the move technique showing the number of moves required(m) for the respective number of marble pairs(n):

If n = 1 then,

m					🔵		🔴				
1						🔵	🔴				
2					🔴	🔵					
3					🔴		🔵				

If n = 2 then,

m				🔵	🔵		🔴	🔴			

1				🔵		🔵	🔴	🔴			
2				🔵	🔴	🔵		🔴			0
3				🔵	🔴	🔵	🔴				
4				🔵	🔴		🔴	🔵			
5					🔴	🔵	🔴	🔵			
6				🔴		🔵	🔴	🔵			
7				🔴	🔴	🔵		🔵			
8				🔴	🔴		🔵	🔵			

If n = 3 then,

m			🔵	🔵	🔵		🔴	🔴	🔴		
1			🔵	🔵		🔵	🔴	🔴	🔴		
2			🔵	🔵	🔴	🔵		🔴	🔴		
3			🔵	🔵	🔴	🔵	🔴		🔴		
4			🔵	🔵	🔴		🔴	🔵	🔴		
5			🔵		🔴	🔵	🔴	🔵	🔴		

6				🔵	🔴	🔵	🔴	🔵	🔴		
7			🔴	🔵		🔵	🔴	🔵	🔴		
8			🔴	🔵	🔴	🔵		🔵	🔴		
9			🔴	🔵	🔴	🔵	🔴	🔵			
10			🔴	🔵	🔴	🔵	🔴		🔵		
11			🔴	🔵	🔴		🔴	🔵	🔵		
12			🔴		🔴	🔵	🔴	🔵	🔵		
13			🔴	🔴		🔵	🔴	🔵	🔵		
14			🔴	🔴	🔴	🔵		🔵	🔵		
15			🔴	🔴	🔴		🔵	🔵	🔵		

If n = 4 then

m		🔵	🔵	🔵	🔵		🔴	🔴	🔴	🔴	
1		🔵	🔵	🔵		🔵	🔴	🔴	🔴	🔴	
2		🔵	🔵	🔵	🔴	🔵		🔴	🔴	🔴	
3		🔵	🔵	🔵	🔴	🔵	🔴		🔴	🔴	

4		🔵	🔵	🔵	🔴		🔴	🔵	🔴	🔴	
5		🔵	🔵		🔴	🔵	🔴	🔵	🔴	🔴	
6		🔵		🔵	🔴	🔵	🔴	🔵	🔴	🔴	
7		🔵	🔴	🔵		🔵	🔴	🔵	🔴	🔴	
8		🔵	🔴	🔵	🔴	🔵		🔵	🔴	🔴	
9		🔵	🔴	🔵	🔴	🔵	🔴	🔵		🔴	
10		🔵	🔴	🔵	🔴	🔵	🔴	🔵	🔴		
11		🔵	🔴	🔵	🔴	🔵	🔴		🔴	🔵	
12		🔵	🔴	🔵	🔴		🔴	🔵	🔴	🔵	
13		🔵	🔴		🔴	🔵	🔴	🔵	🔴	🔵	
14			🔴	🔵	🔴	🔵	🔴	🔵	🔴	🔵	
15		🔴		🔵	🔴	🔵	🔴	🔵	🔴	🔵	
16		🔴	🔴	🔵		🔵	🔴	🔵	🔴	🔵	
17		🔴	🔴	🔵	🔴	🔵		🔵	🔴	🔵	
18		🔴	🔴	🔵	🔴	🔵	🔴	🔵		🔵	

19		🔴	🔴	🔵	🔴	🔵	🔴		🔵	🔵	
20		🔴	🔴	🔵	🔴		🔴	🔵	🔵	🔵	
21		🔴	🔴		🔴	🔵	🔴	🔵	🔵	🔵	
22		🔴	🔴	🔴		🔵	🔴	🔵	🔵	🔵	
23		🔴	🔴	🔴	🔴	🔵		🔵	🔵	🔵	
24		🔴	🔴	🔴	🔴		🔵	🔵	🔵	🔵	

If n = 5 then

m	🔵	🔵	🔵	🔵	🔵		🔴	🔴	🔴	🔴	🔴
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	🔴		🔴	🔵	🔴	🔵	🔴	🔵	🔴	🔵	🔵
26	🔴	🔴		🔵	🔴	🔵	🔴	🔵	🔴	🔵	🔵
27	🔴	🔴	🔴	🔵		🔵	🔴	🔵	🔴	🔵	🔵
28	🔴	🔴	🔴	🔵	🔴	🔵		🔵	🔴	🔵	🔵
29	🔴	🔴	🔴	🔵	🔴	🔵	🔴	🔵		🔵	🔵
30	🔴	🔴	🔴	🔵	🔴	🔵	🔴		🔵	🔵	🔵
31	🔴	🔴	🔴	🔵	🔴		🔴	🔵	🔵	🔵	🔵
32	🔴	🔴	🔴		🔴	🔵	🔴	🔵	🔵	🔵	🔵
33	🔴	🔴	🔴	🔴		🔵	🔴	🔵	🔵	🔵	🔵
34	🔴	🔴	🔴	🔴	🔴	🔵		🔵	🔵	🔵	🔵
35	🔴	🔴	🔴	🔴	🔴		🔵	🔵	🔵	🔵	🔵

Result:

According to the experiment conducted, the equations relating the number of pairs of marbles(n) used and the number of moves(m) required to exchange their positions are:

If n=1, then m=3.

If n=2, then m=8.

If n=3, then m=15.

If n=4, then m=24.

If n=5, then m=35.

From these equations, we can derive one common general equation that shows the relationship and that is:

$$m = n(n+2) \text{ (or) } m = n^2+2n$$
$$\text{where } n > 0$$

Proof:

To prove and ensure that $m = n(n+2)$ truly does show the relationship between the number of pairs of marbles(n) used and the number of moves(m) required to exchange their positions, we carried out the following calculations:

If n=1 then,

$m = n(n+2)$

$m = 1(1+2)$

$m = 1 \text{ x } 3$

$m = 3$

If n=2 then,

$m = n(n+2)$

$m = 2(2+2)$

$m = 2 \text{ x } 4$

$m = 8$

If n=3 then,

$m = n(n+2)$

$m = 3(3+2)$

$m = 3 \text{ x } 5$

$m = 15$

If n=4 then,

$m = n(n+2)$

$m = 4(4+2)$

$m = 4 \text{ x } 6$

$m = 24$

If n=5 then,

$m = n(n+2)$

$m = 5(5+2)$

$m = 5 \text{ x } 7$

$m = 35$

The initial experiment supports the above values of m from when n=1 till when n=5.

If n=6 then,

$m = n(n+2)$

$m = 6(6+2)$

$m = 6 \text{ x } 8$

$m = 48$

The below table supports the above value of m when n=6:

Table showing the moving of marbles when the pairs of marbles used are 6

If n=7 then,

$m = n(n+2)$

$m = 7(7+2)$

$m = 7 \text{ x } 9$

$m = 63$

The below table supports the above value of m when n=7:

Table showing the moving of marbles when the pairs of marbles used are 7

THUS, PROVED.

<u>Note:</u> *We have practically verified the equation from considering n as 1 till n as 12. However, in this project we have only shown the proof till n as 6 due to highly increasing numeric values.*

If n=6 then,

$m = n(n+2)$

$m = 6(6+2)$

$m = 6 \text{ x } 8$

$m = 48$

If n=8 then,

$m = n(n+2)$

$m = 8(8+2)$

$m = 8 \text{ x } 10$

$m = 80$

If n=9 then,

$m = n(n+2)$

$m = 9(9+2)$

$m = 9 \text{ x } 11$

$m = 99$

If n=10 then,

$m = n(n+2)$

$m = 10(10+2)$

$m = 10 \text{ x } 12$

$m = 120$

If n=11 then,

$m = n(n+2)$

$m = 11(11+2)$

$m = 11 \text{ x } 13$

$m = 143$

If n=12 then,

$m = n(n+2)$

$m = 12(12+2)$

$m = 12 \text{ x } 14$

$m = 168$

Conclusion:

Chinese Checkers, just like chess, stimulates both the left and right hemispheres of the brain by recognizing the different colors and using logic to make the best move. Thanks to the visual stimuli and patterns one's required to keep track of while playing, the game also improves memory.

Chinese Checkers stimulates the brain and encourages innovative thinking to figure out which marbles to move and where to unclog the path for other of their marbles, thereby, improving their problem-solving skills.

Similarly, this project has also made us think, keep track, and solve the problem at hand logically and mathematically. As avid players of Chinese Checkers, we have navigated through one of our favourite experiences mathematically with the help of our problem-solving skills in this project.

We have discovered the mathematical side of acing a linear version of Chinese Checkers by the identification of the relationship between the number of pairs of marbles(n) used and the number of moves(m) required to exchange their positions: $m = n(n+2)$ *(or)* $m = n^2+2n$.

However, we are still in pursuit to find the formula to ace a game of normal Chinese Checkers. We know it's already out there but finding it mathematically on our own makes it a lot more enjoyable, doesn't it?

Bibliography:

1. https://en.wikipedia.org/wiki/Marble_(toy)
2. https://en.wikipedia.org/wiki/Chinese_checkers
3. https://miro.com/app/board/o9J_lDYMdBo=/

Interpretation of *i* Using the Argand Plane

Abstract:

This project is my take on the question: Using the argand plane, interpret geometrically, the meaning of $i = \sqrt{-1}$ and its integral powers.

Introduction:

Imaginary Numbers

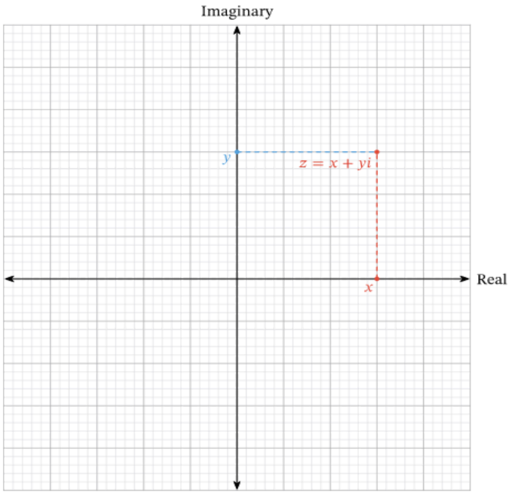
Imaginary numbers are an important mathematical concept; they extend the real number system $\mathbb{R}$ to the complex number system $\mathbb{C}$, in which at least one root for every nonconstant polynomial exists. An imaginary number is a real number multiplied by the imaginary unit *i*, where *i* is a solution to the quadratic equation $x^2 + 1 = 0$. The imaginary number *i* is defined solely by the property that its square is -1: $i^2 = -1$. With *i* defined this way, it follows directly from algebra that *i* and $-i$ are both square roots of -1. It is this property of *i* that we are going to interpret geometrically in this project.

Complex Numbers

An imaginary number *bi* can be added to a real number a to form a complex number of the form *a* + *bi*, where the real numbers a and b are called, respectively, the real part and the imaginary part of the complex number.

Argand Planes

The complex numbers can be represented geometrically on a two-dimensional plane with two perpendicular axes representing the real and imaginary parts of the number respectively. Such a plane is referred to as the complex plane, the Argand plane, or the Argand diagram.



An Argand diagram is a plot of complex numbers:

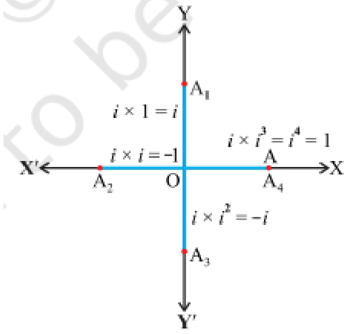
$$z = x + iy$$

represented by points (x,y) in Cartesian coordinates in the complex plane using the x-axis as the real axis and y-axis as the imaginary axis.

Interpretation of $i = \sqrt{-1}$ and its Integral Powers:

Construction

1. Draw two mutually perpendicular lines X X’ and Y Y’ interesting at the point O.
2. Using a compass with width 1 unit length, mark A on the OX with O as center.
3. Now, using the same width and center O, rotate the compass through angles of 90º, 180º, 270º and 360º and mark points A_1, A_2, A_3 and A4 respectively, on OY, OX’, OY’ and OX.



Interpretation

1. The plane marked by XX’ and YY’ is a complex plane or argand plane and OA, OA_1, OA_2, OA_3, and OA_4 denote complex numbers of the form z = x + iy.
2. Since OA, OA_1, OA_2, OA_3, and OA_4 are complex numbers:

   $OA = x + iy = 1 + i(0) = 1$

   $OA_1 = x + iy = 0 + i(1) = i$

   $OA_2 = x + iy = -1 + i(0) = -1$

   $OA_3 = x + iy = 0 + i(-1) = -i$

   $OA_4 = x + iy = 1 + i(0) = 1$
3. Since $i = \sqrt{-1}$,

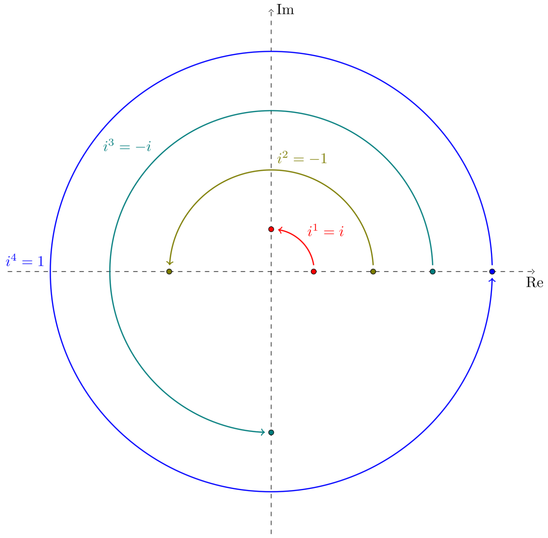
   $OA = 1 = i^0$

   $OA_1 = i = i * 1 = i^1$

   $OA_2 = -1 = i * i = i^2$

   $OA_3 = -i = i * -1 = i * i^2 = i^3$

   $OA_4 = 1 = (-1)^2 = (i^2)^2 = i^4$



Note that each time we rotate OA by 90º, it is equivalent to multiplying OA by i. i is, therefore, referred to as the multiplying factor for a rotation of 90º: $OA_n = i^n$.

For any complex number z, rotation through n-right angles will be: $z_n = z * i^n$. Therefore, through the converse of this statement, we can say that multiplying a complex number by *i* or any of its integral powers $i^{\,n}$, is equivalent to rotation through n-right angles.

Conclusion:

Geometrically, *i* (= $\sqrt{-1}$) is referred to as the multiplying factor for a rotation of 90º. Every time we multiply a complex number by *i*, it is equivalent to rotation by 90º. Therefore, multiplying a complex number z by any of *i*'s integral powers i^n, is equivalent to the rotation through n-right angles: $z * i^n = z^n$. This is the geometric meaning of $i = \sqrt{-1}$ and its integral powers.

Bibliography

1. https://ncert.nic.in/pdf/publication/sciencelaboratorymanuals/classXI/mathematics/kelm402.pdf
2. https://www.mathsisfun.com/numbers/imaginary-numbers.html
3. https://en.wikipedia.org/wiki/Imaginary_unit
4. https://en.wikipedia.org/wiki/Imaginary_number
5. https://www.nagwa.com/en/explainers/280109891548/
6. https://math.stackexchange.com/questions/1549816/complex-multiplication-as-rotation
7. https://mathworld.wolfram.com/ArgandDiagram.html

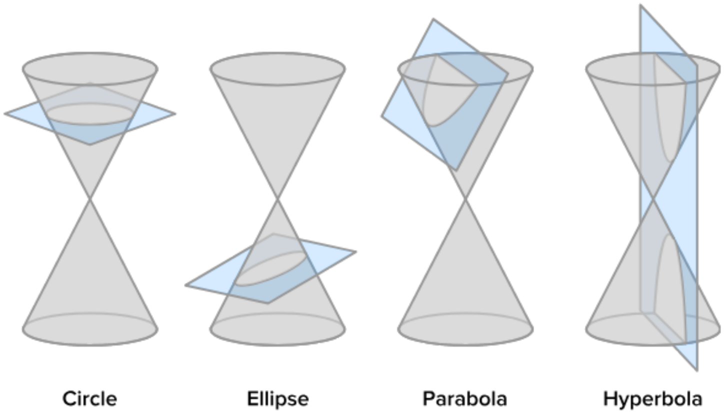
Construction of Ellipses Using the Foci Method

Abstract:

This project is my take on the question: Use the foci property of an ellipse to construct an ellipse.

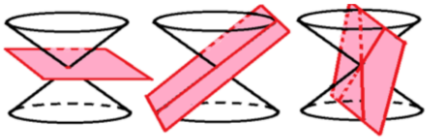
Introduction to Conics:

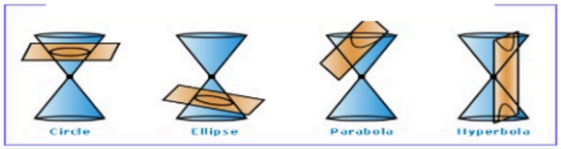
Conic sections have been studied for thousands of years and have provided a rich source of interesting and beautiful results in Euclidean geometry. Conic sections are the shapes or curves that can be created when a plane intersects a double-napped cone. In other words, conics are the cross sections of double-napped cones. Depending on the angle of the plane with respect to the cone, a conic section may be a circle, an ellipse, a parabola, or a hyperbola.



Types of Conics:

1. **Ellipses:** They are conic sections that look like elongated circles. They arise when the intersection of the cone and plane is a closed curve.
2. **Circles:** They are special kinds of ellipses which are obtained when the cutting plane is parallel to the plane of the generating circle of the cone; for a right cone, this means the cutting plane is perpendicular to the axis.
3. **Parabola:** If the cutting plane is parallel to exactly one generating line of the cone, then the conic is unbounded and is called a parabola.
4. **Hyperbola:** In the remaining case, the figure is a hyperbola: the plane intersects both halves of the cone, producing two separate unbounded U-shaped curves.
5. **Degenerate Conics:** There also exists a special category of conics called degenerate conics. They are conics that do not have the usual properties of a conic. They are formed by planes that pass through the vertex of the cone and are of three types: A singular point, a line, and a degenerate hyperbola.

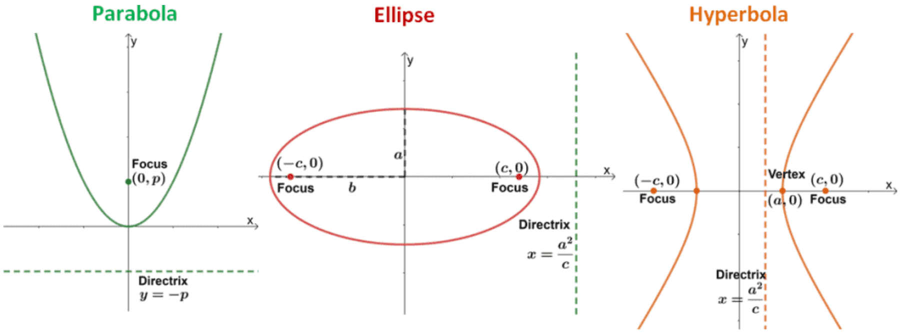




	Conic	Vertex	Generator	Axis
1	Point	Cuts	outside	
2	Line	Cuts	touches	
3	Line Pair	Cuts	inside	
4	Circle	Misses		Right angle
5	Ellipse	Misses		Not right angle
6	Parabola	Misses	Parallel to	
7	Hyperbola	Misses	Not Parallel to	

Focus, Directrix and Eccentricity:

Focuses or foci are special points with reference to which any of a variety of curves is constructed. Directrix is a straight line that, together with the point known as the focus, serves to define a conic section. The distance to the directrix from any point of a conic section is in fixed ratio to the distance from the same point to a focus.



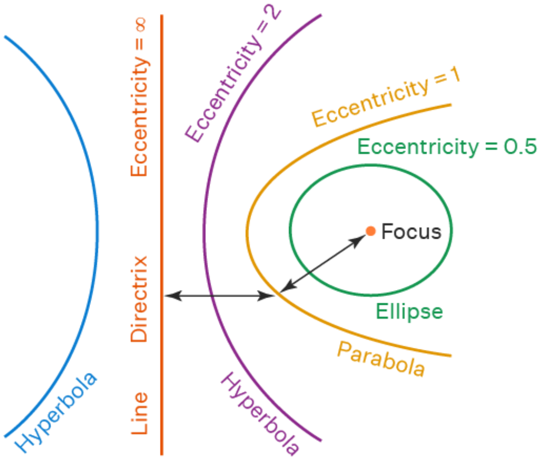
It is also possible to describe all conic sections in terms of a single focus and a single directrix. A conic is defined as the locus of points P for each of which the distance to the focus F divided by the distance to the directrix(the distance from P to a fixed line L) is a fixed positive constant, called the eccentricity e.

The eccentricity of the conic section is defined as the distance from any point to its focus, divided by the perpendicular distance from that point to its nearest directrix:

$$\text{Eccentricity} = \frac{Distance\ to\ the\ focus\ from\ any\ point\ on\ the\ conic\ section}{Distance\ to\ the\ directrix\ from\ the\ point}$$

$$e = \frac{c}{a}$$

The eccentricity value is constant for any conics. If 0 < e < 1 the conic is an ellipse, if e = 1 the conic is a parabola, and if e > 1 the conic is a hyperbola. If the distance to the focus is fixed and the directrix is a line at infinity, the eccentricity is zero and the conic is a circle. If the eccentricity is infinity, then it is of a line.



Ellipse:

An ellipse as mentioned earlier is a closed curve that can be described as the locus of points for which the sum of the distances to two given points or foci is constant. There are two types of ellipses: horizontal and vertical.

An ellipse has two axes of symmetry:

1. **The major axis**, which is the line through (or line segment between) the two points most distant from the center (vertices).
2. **The minor axis**, which is the line through (or line segment between) the two points least distant from the center (co-vertices).

The line segments from the center to each vertex are called the semi-major axes, and the line segments from the center to each co-vertex are called the semi-minor axes. The foci of an ellipse, E and F, lie on the ellipse's major axis and are equidistant from the center.

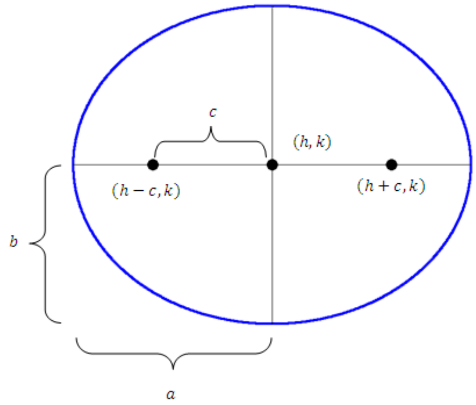
The general equation for a horizontal ellipse (a > b) is:

$$\frac{(x-h)^2}{a^2} + \frac{(y-k)^2}{b^2} = 1$$

while the general equation for a vertical ellipse (a < b) is:

$$\frac{(x-h)^2}{b^2} + \frac{(y-k)^2}{a^2} = 1$$

where (h, k) is the center, a is the length of the semi-major axis, and b is the length of the semi-minor axis.



Often the above equation is written as follows:

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$

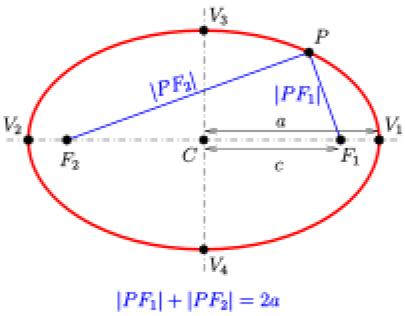
This is called the standard form of the equation of an ellipse, such that the ellipse is centered at the origin (0, 0). The distance from the center to a focus c of an ellipse can be found by using the formula $c^2 = a^2 - b^2$.

Construction of Ellipse:

There exists multiple ways to construct an ellipse including the concentric circles method, the rectangular method, the trammel method, the eccentricity method, etc. The one we are going to employ here is the **foci method**.

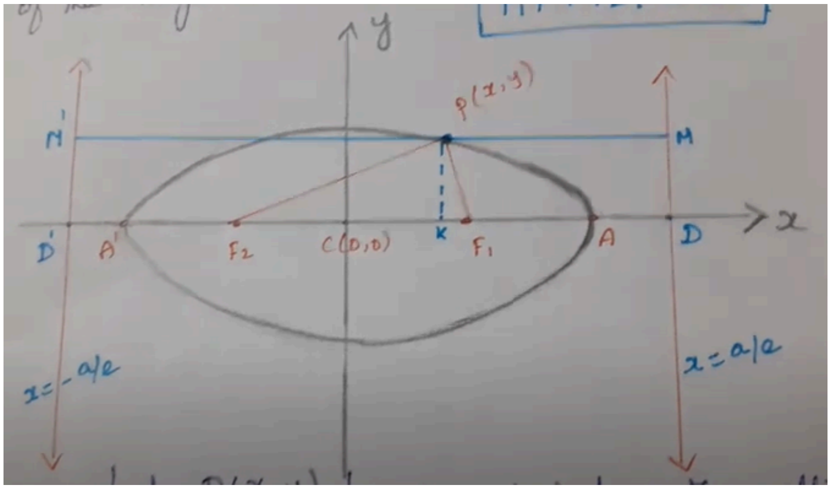
Principle:

The foci method of construction of an ellipse uses the focal property of the ellipse for its construction. According to this property, the sum of the distances from any point P on the ellipse to these two foci F_1 and F_2 is equal to the length of the major axis, ie. $F_1P + F_2P = 2a$.



To understand this property, let us consider an ellipse centered at C(0, 0) with an equation:

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$



Let P(x, y) be any point on the ellipse and let MPM' be the perpendicular through P on directrices MD and M'D'. Additionally, let there be a line PK which is perpendicular to the x-axis. Now, by the definition of the conics, we get:

$e = \frac{F_1P}{PM}$

$\Rightarrow F_1P = e \cdot PM$

$\Rightarrow F_1P = e \cdot KD$

$\Rightarrow F_1P = e\,(CD - CK)$

$\Rightarrow F_1P = e\,(\frac{a}{e} - x)$

$\Rightarrow F_1P = a - ex$ ......(i)

$e = \frac{F_2P}{PM'}$

$\Rightarrow F_2P = e \cdot PM'$

$\Rightarrow F_2P = e \cdot (KD')$

$\Rightarrow F_2P = e\,(CD' + CK)$

$\Rightarrow F_2P = e\,(\frac{a}{e} + x)$

$\Rightarrow F_2P = a + ex$ ......(ii)

[Since the distance from the center to the directrix in an ellipse can be found by using the formula $\frac{a}{e}$ *(where a is the distance to the directrix from the point P).]*

On adding (i) and (ii),

$$F_1P + F_2P = a - ex + a + ex$$

$$F_1P + F_2P = 2a$$

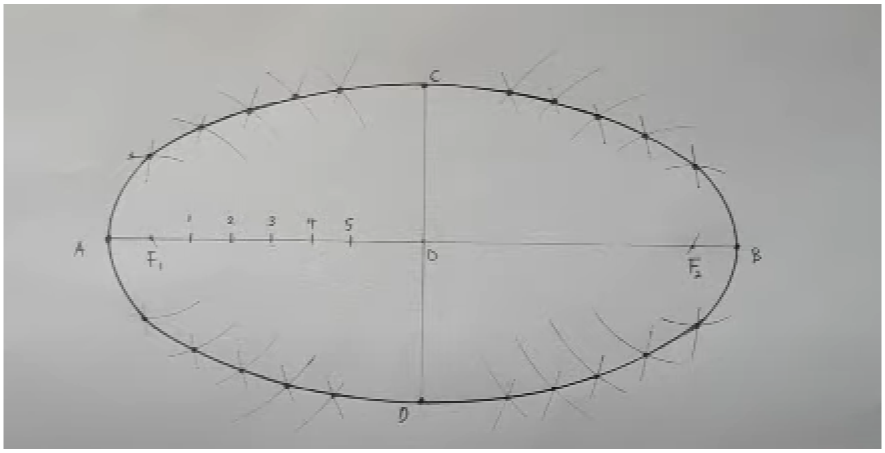
Therefore, the sum of the distances from any point P on the ellipse to these two foci F_1 and F_2 is equal to the length of the major axis. And we will use this property to construct the ellipse.

Process:

The foci method of ellipse construction involves plotting a series of points along the circumference of the ellipse by drawing a series of intersecting arcs using the foci on the major axis as centers. To construct an ellipse using the foci method, the following steps are followed:

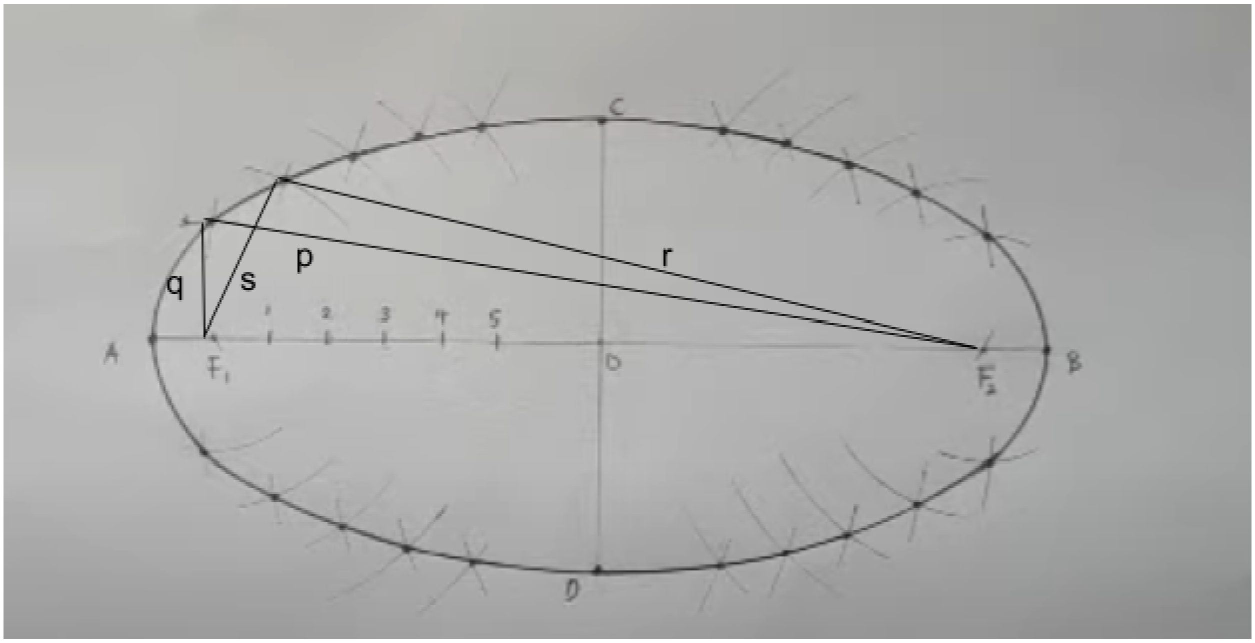
1. Lay out horizontal (AB) and vertical axes (CD) that intersect at right angles.
2. Locate the foci (F_1, F_2) by setting the compass to one half distance of the major axis AB and striking arcs along AB using C as the center.
3. Mark a minimum of ten equal distances between F_1 and F_2. The more distances marked, the more accurate the ellipse construction.
4. With F_1 as center, and radius A1, A2, A3, etc. draw arcs above and below line AB. And with F_2 as center, and radius B1, B2, B3, etc. draw arcs to intersect those struck from F_1.
5. Continue plotting points this way until all points form an ellipse circumference.
6. Once all points are plotted, connect the points using french curves to form an ellipse.

Construction:



Proof:

To prove and ensure that the above construction was indeed done using the focal property of an ellipse, let’s consider the following:



S.No.	Argument	Reason
1	F1, F2 are the foci of the ellipse	By construction ie. ● Since the compass width set from OB was used to draw CF_2 and CF_1, line segments CF_2 and OB and line segments CF_1 and OB are congruent. Thus, the line segments CF_2 and CF_1 are congruent. ● Since OB is half of AB, $CF_1 + CF_2 = AB$ ● Therefore, according to the **focal property of an ellipse**, F_1 and F_2 are the foci of the ellipse because from any point C on the ellipse, the sum of the distances from C to the two foci F_1 and F_2 is equal to the length of the major axis AB.

2	q = A1 and p = B1
	s = A2 and r = B2
		The compass width used to draw q was A1 and that for p was B1. Similarly, the compass width used to draw s was A2 and for r it was B2.

3	q + p = A1 + B1 and s + r = A2 + B2	According to 2.
4	q + p = AB s + r = AB	A1 + B1 = AB. A2 + B2 = AB

5	Length between any point P and F_1 + Length between any point P and F_2 = AB	All other plots of the ellipse pointed above and below the major axis were also plotted in the same manner as the ones involved in p & q and in r & s.
6	The figure is an ellipse	According to the **focal property of an ellipse**, the sum of the distances from any point P on the ellipse to the two foci F_1 and F_2 is equal to the length of the major axis AB.

(QED)

THUS, IT HAS BEEN PROVEN THAT THE ABOVE CONSTRUCTION IS MATHEMATICALLY ACCURATE ACCORDING TO THE FOCAL PROPERTY OF AN ELLIPSE AND THAT THE ENTIRETY OF THE CONSTRUCTION WAS BASED ON THE SAME PROPERTY.

Applications of Ellipse:

The shape of an ellipse is formed when a cone is cut at an angle. If you tilt a glass of water, the resulting shape of the surface of the water is also an ellipse. You can also see ellipses when a hula hoop or tire of a car looks askew. Though these are examples of optical ellipses, the ellipse also has practical uses in real life:

Rugby Ball:

Rotate an ellipse about its major axis, and you obtain a rugby ball which is easier to pass.

Furniture and Carpentry:

Elliptical tables, book-cases, vent pipes, etc. look elegant and hence the shape is used often in carpentry.

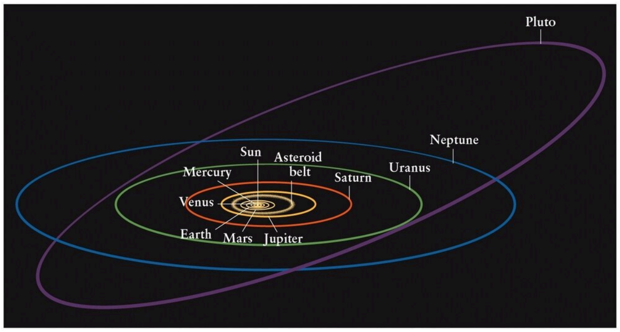
© Isabel Trun

Food:

Foods are cut to form ellipses, offering a refined touch to simple foods. Cutting a carrot, cucumber or sausage at an angle to its main axis results in an elliptical slice. Wraps – tortillas wrapped around a filling – are also often cut into two elliptical wedges. The sharp focus of the ellipse gives these everyday food items a more elegant look.

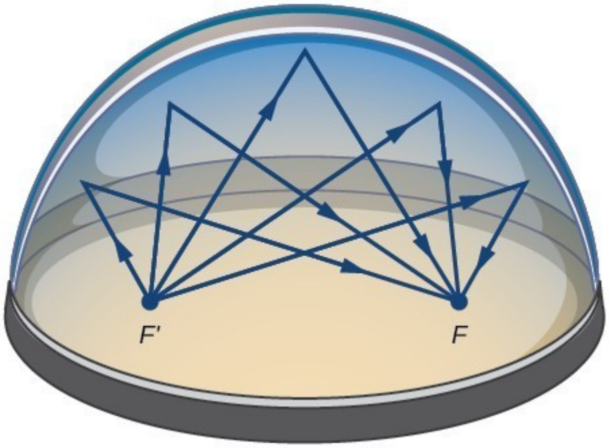
Orbits of Planets and Satellites:

The path of each planet is an ellipse with the Sun at one focus. In physics, this is known as Kepler's first law of planetary motion. The orbits of planets, satellites, moons, and comets, are also elliptical.



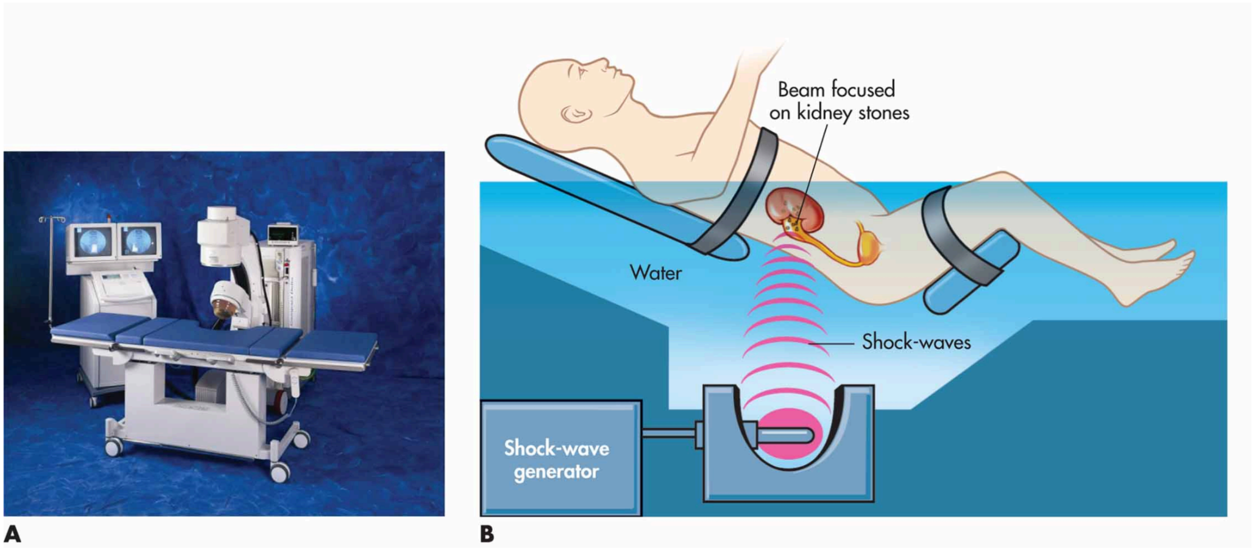
Whispering Gallery:

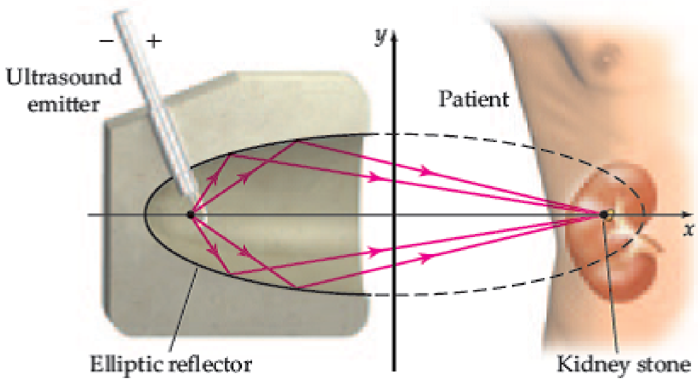
A focus is one of two points that defines the shape and size of the ellipse; they're located on the major axis of the ellipse, at equidistant points from the center of that axis. If light or a sound wave emanates from one focus of a real-life ellipse, it will be reflected to the other focus. This property is used to create whispering galleries, which are structures that allow someone who is whispering in one area to be heard clearly by someone in another area but not by anyone else. Famous examples of whispering galleries include the United States Statuary Capitol Hall, Museum of Science and Industry in Chicago, London's St. Paul's Cathedral and India’s Gol Gumbaz.



Lithotripsy:

Lithotripsy is a surgery-free method of destroying a kidney stone that uses the properties of the ellipse's two foci. For a lithotripsy treatment the patient lies in an elliptical tub, with the kidney stone aligned to one of the foci of the ellipse. Shockwaves emanating from the other focus concentrate on the kidney stone, reducing it to debris as small as sand that can pass through the body without discomfort.





Elliptical Pool Table:

The reflection property of the ellipse is useful in an elliptical pool table — if you hit the ball so that it goes through one focus, it will reflect off the ellipse and go into the hole which is located at the other focus.

Elliptical Trainers:

An elliptical training machine simulates the motion of running or walking, offering a low-impact cardio workout. When you walk or run in an elliptical trainer, your foot describes an elliptical path. An elliptical machine can be motor-driven or user-driven, and some elliptical trainers also feature handlebars that one can push or pull on to help move the foot pedals through their elliptical path.

Others:

The shapes of boat keels, rudders, and some aviation wings, can all be represented by ellipses.

Conclusion:

We have, in this project, constructed an ellipse using the focal property of ellipses. However, an ellipse is not simply about mathematics or how we plot it. Ellipse has its own significance; a significance that can produce something extraordinary; a significance that can delight others with its beauty and uniqueness. We have seen its immense uses in the real world, which led to this significant role in the mathematical world.

Bibliography:

1. https://k12.libretexts.org/Bookshelves/Mathematics/Analysis/06%3A_Conic_Sections
2. https://www.ck12.org/c/calculus/conic-sections/
3. https://www.ck12.org/c/calculus/ellipses/
4. https://www.maplesoft.com/support/help/maple/view.aspx?path=MathApps%2FFocalPropertyOfAnEllipse
5. www.youtube.com/watch?v=pleDRxPUnj4
6. www.youtube.com/watch?v=hyue0hnGRV0
7. www.youtube.com/watch?v=TBK6TFucgWI

Addition and Multiplication in Integer Modulo Integer Number Systems

Abstract:

This project explores addition and multiplication in the integer modulo integer number systems. It includes verification of whether addition and multiplication are binary operations in ℤ modulo *n* number systems using composition tables as well as the verification of the existence of the properties of binary operations in them.

A.1 Introduction

A.1.1. Some Definitions

Here are some of the definitions of terms used ahead in the paper:

a. **Sets:**

Sets are a collection of well-defined objects or elements. A set is represented by a capital letter symbol and elements are written within a curly bracket {...} each separated from one another by a comma ‘ , ’.

b. **Relations:**

A relation is a set of ordered pairs that establishes a connection or association between elements of two sets. Relations can be represented using tables, graphs, or formulas. For example, a relation R between sets A and B can be represented as R = {(a, b) | a ∈ A, b ∈ B}.

c. **Functions:**

A function is a relation between two sets where each input element from the first set is associated with exactly one output element from the second set. It assigns a unique output for every input. Functions are denoted by lowercase letters and can be represented using equations or mappings. For example, *f* : A → B denotes a function *f* that maps elements from set A to set B.

d. **Operation:**

An operation is a mathematical procedure that combines one or more elements to produce a result. An operation can be a relation, function or combination of both.

e. **Binary Operation:**

A binary operation is an operation that takes two elements from a set and combines them to produce a single element from the same set.

f. **Diophantine Equation:**

A Diophantine equation is an equation, typically a polynomial equation in two or more unknowns with integer coefficients, such that the only solutions of interest are the integer ones. A linear Diophantine equation equates a constant to the sum of two or more monomials, each of degree one. It is of the form:

$$ax + by = c$$

where a, b, c are integers. A linear Diophantine of the above form is said to have solutions iff $gcd(a, b)|\ c$.

A.1.2. Integers and their Axioms

The integers (ℤ) are a set of numbers with two operations, addition '+' and multiplication '·'. There exists a set of fundamental properties that define the behavior of the integers under addition and multiplication called axioms of integers.

The axioms of integers, also known as the axioms of arithmetic, include:

I1. **Closure:** ℤ is closed under addition and multiplication, ie.

$$\forall a, b \in \mathbb{Z}\,,\ a + b \in \mathbb{Z}$$

and: $$\forall a, b \in \mathbb{Z}\,,\ a \cdot b \in \mathbb{Z}\,.$$

I2. **Associativity:** $\forall a, b, c \in \mathbb{Z}\,, (a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$.

I3. **Commutativity:** $\forall a, b \in \mathbb{Z}\,, a + b = b + a$ and $ab = ba$.

I4. **Distributivity:** $\forall a, b, c \in \mathbb{Z}\,, (a + b)c = ac + bc$ and $c(a + b) = ca + cb$.

I5. **Existence of additive identity (0):** The re is a unique element $0 \in \mathbb{Z}$ such that $\forall a \in \mathbb{Z}\,, a + 0 = 0 + a = a.$

I6. **Existence of multiplicative identity (1):** There is a unique element $1 \in \mathbb{Z}$ such that $\forall a \in \mathbb{Z}\,, a \cdot 1 = 1 \cdot a = a.$

I7. **Existence of additive inverse:** $\forall a \in \mathbb{Z}\,, \exists!\,(-\ a) \in \mathbb{Z}$ such that $a + (-\ a) = (-\ a) + a = 0.$

I8. **Existence of natural numbers:** There is a unique non-empty subset $\mathbb{N} \subseteq \mathbb{Z}$ such that:

a. $\forall a, b \in \mathbb{N}\,, a + b \in \mathbb{N}$ and $ab \in \mathbb{N}$.

b. $\forall a \in \mathbb{N}$, exactly one of the following is true: $a \in \mathbb{N}\,, (-\ a) \in \mathbb{N},\ a = 0.$

I9. **Well-ordering principle:** Any non-empty subset $S \subseteq \mathbb{Z}$ has a least element.

From axiom 8, we can say that $\mathbb{Z}$ is a set of numbers formed by the union of natural numbers $\{1, 2, 3, 4, \dots, \infty\}$, zero $\{0\}$ and additive inverses of the natural numbers $\{-1, -2, -3, \dots, -\infty\}$ ie.

$$\mathbb{Z} = \{-\infty, \dots, -3, -2, -1, 0, 1, 2, 3, \dots, \infty\}.$$

A.1.3. Binary Operations and their Properties

Binary Operations as defined earlier (in Section A.1.1), is an operation that takes two elements from a set and combines them to produce a single element from the same set.

To determine if an operation is binary or not, we need to ensure that it satisfies certain criteria:

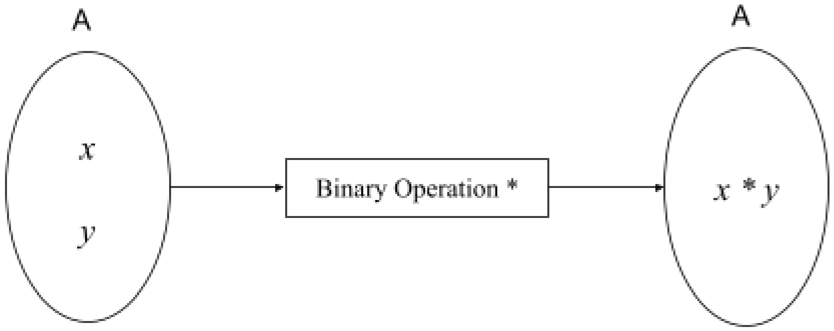
R1. The operation must take exactly two elements from a set as input/operands.

R2. The operation must produce a single, well-defined, unique output.

R3. The operation must exhibit closure ie. the \/;/\;;’result of the operation should belong to the same set from which the input elements are taken.

A binary operation ‘*’ on a non-empty set A can therefore also be defined as a function from A × A to A, ie.:

$$* : A \times A \rightarrow A.$$



Such binary operations exhibit some properties that describe specific characteristics or behaviors exhibited by the operation when applied to elements of a set. They include:

P1) Closure: A binary operation ‘*’ on a set S is said to exhibit closure if for any elements a and b in S, the result of the operation $a * b$ is also an element of S.

P2) Associativity: A binary operation ‘*’ on a set S is said to be associative if $\forall\ a, b, c \in S$, $(a * b) * c = a * (b * c)$.

P3) Commutativity: A binary operation '*' on a set S is said to be commutative (or exhibit commutativity) if $\forall\ a, b \in\ S,\ a * b = b * a$.

P4) Distributivity: A binary operation '*' is distributive over another binary operation '#' if it means that (a # b) * c = (a * c) # (b * c), $\forall\ a, b, c \in\ S$.

P5) Identity Element: An element $e \in\ S$ is called an identity element for a binary operation '*' iff $\forall$ $a \in\ S, a * e = e * a = a$.

P6) Inverse Elements: If there exists an element $b \in\ S$ such that $a * b = b * a = e$ (identity element), then b is called the inverse element of a with respect to the binary operation '*'.

P7) Idempotency: An operation is idempotent if applying the operation multiple times to an element does not change its value after the first application. In other words, $a\ *\ a\ =\ a,\ \forall a\ \in\ S$. An element $a\ \in\ S$ is called idempotent under * if $a\ *\ a\ =\ a$.

P8) Cancellation: A binary operation * in a non-empty set S has the cancellation property if $\forall a, b, c\ \in\ S$, we have:

$$a * b = a * c \Rightarrow b = c \qquad \text{[Left Cancellation]}$$

$$b * a = c * a \Rightarrow b = c \qquad \text{[Right Cancellation]}$$

From the axioms of integers (see section A.1.2), we know that addition and multiplication are binary operations in ℤ. Addition in ℤ follows all the properties listed above except (P7) or idempotency. However, it is to be noted that 0 is idempotent over addition in ℤ. On the other hand, multiplication follows all the properties listed above except (P6) and (P7). However, it is to be noted that 0, 1 are idempotent over multiplication in ℤ and (P8) is true iff a $\neq$ 0.

A.1.4. Modular Arithmetics and their Properties

Modular arithmetic is a system of arithmetic that deals with integers and their remainders when divided by a fixed positive integer called the modulus. For any $n \in \mathbb{Z}$ **,** the integers modulo n are the set of least positive residues of the set of residue classes modulo n, ie.

$$\mathbb{Z}/n\mathbb{Z}\ =\ \{0, 1, 2,\ .\ .\ .\ ,\ (n\ -\ 1)\}$$

It has some important properties and definitions with respect to modular arithmetics:

M1. **Congruence:** In modular arithmetic, we use the symbol "≡" (congruent) to denote equivalence modulo the modulus. For all $a,\ b\ \in\ \mathbb{Z}$, a ≡ b (mod n) means that a and b have the same remainder when divided by n. And for all $a,\ b,\ n\ \in\ \mathbb{Z}$ such that $n \neq 0$, we write a ≡ b (mod n) iff n | (a – b).

M2. **Modular Addition:** For any integers a, b $\in \mathbb{Z}/n\mathbb{Z}$ (for some $n \in \mathbb{Z}$), then a + b ≡ (a + b) (mod n). In other words, if two numbers *a, b* belong to the set of integers modulo $n \in \mathbb{Z}$, then addition of *a* and *b* gives the remainder produced by the sum of *a* and *b* modulo n.

Proof:

Let *a, b* $\in \mathbb{Z}$ such that $a \equiv x(mod\, n)$ and $b \equiv y(mod\, n)$ where $n \in \mathbb{Z}$ and $n > 1$.
Then:

$x, y \in \mathbb{Z}/n\mathbb{Z}$ (by M1)

n | $a - x$ => $a - x = nk$ for some $k \in \mathbb{Z}$ (by M1)

=> $a = x + nk$ ...*(i)*

n | $b - y$ => $b - y = nl$ for some $l \in \mathbb{Z}$ (by M1)

=> $b = y + nl$ ...*(ii)*

Adding *(i)* and *(ii)*, we get:

$a + b = (x + nk) + (y + nl)$ ` (by I1)

=> $a + b = (x + y) + (nk + nl)$ (by I2 and I3)

=> $a + b = (x + y) + n(k + l)$ (by I4)

=> $a + b - (x + y) = [(x + y) + n(k + l)] - (x + y)$ (by I1)

=> $a + b - (x + y) = n(k + l)$ (by I2, I3, I7)

Since $k, l \in \mathbb{Z},\ k + l \in \mathbb{Z}$ by I1. Then:

=> $n|a + b - (x + y)$ (by divisibility)

=> $a + b \equiv (x + y)$ (mod *n*) (by M1)

=> $x(mod\, n) + y(mod\, n) \equiv (x + y)\ (mod\, n)$ □

M3. **Modular Multiplication:** For any integers a, b $\in \mathbb{Z}/n\mathbb{Z}$ (for some $n \in \mathbb{Z}$), then a · b ≡ (a · b) (mod n). In other words, if two numbers *a, b* belong to the set of integers modulo $n \in \mathbb{Z}$, then multiplication of *a* and *b* gives the remainder produced by the product of *a* and *b* modulo n.

Proof:

Let *a, b* $\in \mathbb{Z}$ such that $a \equiv x(mod\, n)$ and $b \equiv y(mod\, n)$ where $n \in \mathbb{Z}$ and $n > 1$.
Then:

$x, y \in \mathbb{Z}/n\mathbb{Z}$ (by M1)

n | $a - x$ => $a - x = nk$ for some $k \in \mathbb{Z}$ (by M1)

=> $a = x + nk$ ...*(i)*

n | $b - x$ => $b - y = nl$ for some $l \in \mathbb{Z}$ (by M1)

$=> b = y + nl$ ...*(ii)*

Since $k, n \in \mathbb{Z}$, $nk \in \mathbb{Z}$ by I1 and since $nk \in \mathbb{Z}$, $(-nk) \in \mathbb{Z}$. by I7. Now, since:

$a, (-nk) \in \mathbb{Z} => a + (-nk) \in \mathbb{Z}$ (by I1)
$=> a - nk \in \mathbb{Z}$ (by I1)
$=> x \in \mathbb{Z}$ (from eq.*(i)*)

Similarly, WLOG, from the given and eq.*(ii)*, we can say that $y \in \mathbb{Z}$.

Now, Multiplying *(i)* and *(ii)*, we get:

$ab = (x + nk)(y + nl)$ (by I1)
=> $ab = (xy + xnl) + (ynk + n^2kl)$ (by I4)
=> $ab = (xy) + n(xl + yk + nkl)$ (by I3, I4)
=> $ab - (xy) = [(xy) + n(xl + yk + nkl)] - (xy)$ (by I1)
=> $ab - (xy) = n(xl + yk + nkl)$ (by I2, I3, I7)

Since $x, y, k, l \in \mathbb{Z}$, $xl, yk, nkl \in \mathbb{Z}$ by I1. Then:

=> $n | ab - (xy)$ (by divisibility)
=> $ab \equiv (xy)\ (\mathrm{mod}\ n)$ (by M1)
=> $x(mod\, n) \cdot y(mod\, n) \equiv (xy)\ (mod\, n)$ □

A.1.5. Cayley Table

A Cayley table, also known as composition table, is a technique of visual representation used to describe an algebraic structure (usually a finite group) by representing the results of a binary operation on a set in the form of a square array. It provides a systematic way of showing the outcomes of combining elements from a set using a specific operation.

This table can be formed as follows:
i. Write the elements of the set (which are finite in number) in the column and row headers.
ii. Write the element associated with the ordered pair (a_i, a_j) at the intersection of the row headed by a_i and the column headed by a_j. Thus, (ith entry on the left) (binary operator) (jth entry on the top) = entry where the ith row and jth column intersect.

For example, let's consider a set {a, b, c, d} and a binary operation 'α' defined on this set. The Cayley table for this operation would have four rows and four columns. Each cell in the table would contain the result of applying the operation ‘α’ to the corresponding row and column elements. The table might look as follows:

α	a	b	c	d
a	a α a	b α a	c α a	d α a
b	a α b	b α b	c α b	d α b
c	a α c	b α c	c α c	d α c
d	a α d	b α d	c α d	d α d

A.2. Binary Operations in $\mathbb{Z}/n\mathbb{Z}$

We already know that addition and multiplication are binary operations in $\mathbb{Z}$. But are they binary operations in $\mathbb{Z}$ modulo 2? In $\mathbb{Z}$ modulo 3? In $\mathbb{Z}$ modulo 4? In $\mathbb{Z}$ modulo 5?
In $\mathbb{Z}$ modulo any other integer $n > 1$? Let’s explore and verify these using Cayley tables.

A.2.1. Addition in $\mathbb{Z}/n\mathbb{Z}$

Let’s first verify if addition is a binary operation in $\mathbb{Z}$ modulo *n* systems.

In $\mathbb{Z}$ modulo 2 ($\mathbb{Z}/2\mathbb{Z}$):

For $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$, the Cayley table for addition is:

+	0	1
0	0	1
1	1	0

Is addition a binary operation in $\mathbb{Z}/2\mathbb{Z}$?

A.1.2	R1	R2	R3
Yes/No	Yes	Yes	Yes

Therefore, yes, addition is a binary operation in $\mathbb{Z}/2\mathbb{Z}$.

What properties of binary operations does addition exhibit in $\mathbb{Z}/2\mathbb{Z}$?9

A.1.2	P1	P2	P3	P4	P5	P6	00P7	P8

Yes/No	Yes	Yes	Yes	No	Yes (0)	Yes	No (but 0 is idempotent)	Yes

In $\mathbb{Z}$ modulo 3 ($\mathbb{Z}/3\mathbb{Z}$):

For $\mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$, the Cayley table for addition is:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Is addition a binary operation in $\mathbb{Z}/3\mathbb{Z}$?

A.1.2	R1	R2	R3
Yes/No	Yes	Yes	Yes

Therefore, yes, addition is a binary operation in $\mathbb{Z}/3\mathbb{Z}$.

What properties of binary operations does addition exhibit in $\mathbb{Z}/3\mathbb{Z}$?

A.1.2	P1	P2	P3	P4	P5	P6	P7	P8
Yes/No	Yes	Yes	Yes	No	Yes (0)	Yes	No (but 0 is idempotent)	Yes

In $\mathbb{Z}$ modulo 4 ($\mathbb{Z}/4\mathbb{Z}$):

For $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$, the Cayley table for addition is:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Is addition a binary operation in $\mathbb{Z}/4\mathbb{Z}$?

A.1.2	R1	R2	R3
Yes/No	Yes	Yes	Yes

Therefore, yes, addition is a binary operation in $\mathbb{Z}/4\mathbb{Z}$.

What properties of binary operations does addition exhibit in $\mathbb{Z}/4\mathbb{Z}$?

A.1.2	P1	P2	P3	P4	P5	P6	P7	P8
Yes/No	Yes	Yes	Yes	No	Yes (0)	Yes	No (but 0 is idempotent)	Yes

In $\mathbb{Z}$ modulo 5 ($\mathbb{Z}/5\mathbb{Z}$):

For $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$, the Cayley table for addition is:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Is addition a binary operation in $\mathbb{Z}/5\mathbb{Z}$?

A.1.2	R1	R2	R3
Yes/No	Yes	Yes	Yes

Therefore, yes, addition is a binary operation in $\mathbb{Z}/5\mathbb{Z}$.

What properties of binary operations does addition exhibit in $\mathbb{Z}/5\mathbb{Z}$?

A.1.2	P1	P2	P3	P4	P5	P6	P7	P8
Yes/No	Yes	Yes	Yes	No	Yes (0)	Yes	No (but 0 is idempotent)	Yes

In $\mathbb{Z}$ modulo n ($\mathbb{Z}/n\mathbb{Z}$):

For $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, 3, . . ., (n - 1)\}$, the Cayley table for addition is:

+	0	1	2	3	...	$n - 1$
0	0	1	2	3	...	$n - 1$
1	1	2	3	4	...	n
2	2	3	4	5	...	$n + 1$
3	3	4	5	6	...	$n + 2$
. . .	. . .	. . .	. . .	. . .	... ...	. . .
$n - 1$	$n - 1$	n	$n + 1$	$n + 2$	...	$2n - 2$

<u>Proposition 1.</u> Addition is a binary operation in $\mathbb{Z}/n\mathbb{Z}$ for any integer $n > 0$.

Proof:

In order to prove the above proposition we need to prove that addition in $\mathbb{Z}/n\mathbb{Z}$ adheres to the below principles:

i. It must take exactly two elements from $\mathbb{Z}/n\mathbb{Z}$ as input.
ii. When applied to the two input elements, it must yield a single, unique output.
iii. It must exhibit closure.

By def^{n} of addition in modular arithmetics (see M2 in section A.1.4.):

$$x(mod\ n) + y(mod\ n) \equiv (x + y)\ (mod\ n)$$

From this it can be observed that addition in $\mathbb{Z}/n\mathbb{Z}$ has exactly two inputs from the set. Therefore, (i) is true.

Now, by division algorithm, we can write:

$$x + y = nq + r \qquad \text{where } 0 \le r < q$$

Taking *mod n* on both sides:

$$(x + y)(mod\ n) \equiv r\ (mod\ n) \qquad \text{(by M1)}$$

Then:

$$x(mod\ n) + y(mod\ n) \equiv r\ (mod\ n)$$

This shows that if $x, y \in \mathbb{Z}/n\mathbb{Z}$ then $x + y \in \mathbb{Z}/n\mathbb{Z}$ and thus, addition in $\mathbb{Z}/n\mathbb{Z}$ is closed. This shows that *(iii)* is true.

Additionally, since the division algorithm states that r is unique for every $(x{+}y)$, n and q, $r\ (mod\ n)$ and in turn $x(mod\ n) + y(mod\ n)$ is also unique for every x, y. Therefore, showing that *(ii)* is true as well.

Altogether, we can say addition is a binary operation in $\mathbb{Z}/n\mathbb{Z}$ □

<u>Proposition 2.</u> Addition adheres to the following properties of binary operations in $\mathbb{Z}/n\mathbb{Z}$ (for any integer $n > 1$):

i. Closure: $\forall a, b \in \mathbb{Z}/n\mathbb{Z}\ ,\ a + b \in \mathbb{Z}/n\mathbb{Z}$

ii. Associativity: $\forall a, b, c \in \mathbb{Z}/n\mathbb{Z}\ , (a + b) + c \equiv a + (b + c)$.

iii. Commutativity: $\forall a, b \in \mathbb{Z}/n\mathbb{Z}\ , a + b \equiv b + a$.

iv. Existence of additive identity: There is a unique element $0 \in \mathbb{Z}/n\mathbb{Z}$ such that $\forall a \in \mathbb{Z}/n\mathbb{Z}\ , a + 0 \equiv 0 + a \equiv a$.

v. Existence of additive inverse: $\forall a \in \mathbb{Z}/n\mathbb{Z}\ , \exists!\ (-\ a) \in \mathbb{Z}/n\mathbb{Z}$ such that $a + (-\ a) \equiv (-\ a) + a \equiv 0$.

vi. Cancellation: If $\forall a, b, c \in \mathbb{Z}/n\mathbb{Z}$, we have:

$$a + b \equiv a + c \Rightarrow b \equiv c \text{ and } b + a \equiv c + a \Rightarrow b \equiv c$$

Proof:

i. <u>To prove:</u> $\forall a, b \in \mathbb{Z}/n\mathbb{Z}\ ,\ a + b \in \mathbb{Z}/n\mathbb{Z}$.
See proof of proposition 1.

ii. <u>To prove:</u> $\forall a, b, c \in \mathbb{Z}/n\mathbb{Z}\ , (a + b) + c \equiv a + (b + c)$.
This can alternatively be written as: $(a + b) + c \equiv a + (b + c)(mod\ n)$.
or: $[a(mod\ n) + b(mod\ n)] + c(mod\ n) \equiv a(mod\ n) + [b(mod\ n) + c(mod\ n)]$.

Let $a, b, c \in \mathbb{Z}$. Then:

$$\begin{aligned}[a(mod\ n) + b(mod\ n)] + c(mod\ n) &\equiv [(a + b)(mod\ n)] + c(mod\ n) \quad \text{(by M2)}\\ &\equiv [(a + b) + c](mod\ n) \quad \text{(by M2)}\\ &\equiv [a + (b + c)](mod\ n) \quad \text{(by I2)}\end{aligned}$$

$$\equiv a(mod\,n) + [(b + c)(mod\,n)] \quad \text{(by M2)}$$
$$\equiv a(mod\,n) + [b(mod\,n) + c(mod\,n)] \quad \text{(by M2)}$$

iii. To prove: $\forall a, b \in \mathbb{Z}/n\mathbb{Z}, a + b \equiv b + a$.

This can alternatively be written as: $a + b \equiv b + a(mod\,n)$.

or: $a(mod\,n) + b(mod\,n) \equiv b(mod\,n) + a(mod\,n)$.

Let $a, b \in \mathbb{Z}$. Then:

$$a(mod\,n) + b(mod\,n) \equiv [a + b](mod\,n) \quad \text{(by M2)}$$
$$\equiv [b + a](mod\,n) \quad \text{(by I3)}$$
$$\equiv b(mod\,n) + a(mod\,n) \quad \text{(by M2)}$$

iv. To prove: There is a unique element $0 \in \mathbb{Z}/n\mathbb{Z}$ such that$\forall a \in \mathbb{Z}/n\mathbb{Z}$, $a + 0 \equiv 0 + a \equiv a$.

This can alternatively be written as: $a + 0 \equiv 0 + a \equiv a\ (mod\,n)$.

or: $a(mod\,n) + 0 \equiv 0 + a(mod\,n) \equiv a(mod\,n)$.

Let $a \in \mathbb{Z}$. Then:

$$a(mod\,n) + 0 \equiv 0 + a(mod\,n) \quad \text{(from part } \textit{iii}\text{)}$$
and: $$a(mod\,n) + 0 \equiv [a + 0](mod\,n) \quad \text{(by M2)}$$
$$\equiv [a](mod\,n) \quad \text{(by I5)}$$

Combining both: $a(mod\,n) + 0 \equiv 0 + a(mod\,n) \equiv a(mod\,n)$

Let's assume for contradiction that $\exists$ more than one additive identity in $\mathbb{Z}/n\mathbb{Z}$ and let them be $e_1$and e_2. Then for all a $\in \mathbb{Z}/n\mathbb{Z}$:

$$a\ (\text{mod } n) + e_1 \equiv a\ (\text{mod } n)$$

Since $e_2 \in \mathbb{Z}/n\mathbb{Z}$, substituting a = e_2, we get:

$$e_2 + e_1 \equiv e_2\ (\text{mod } n)$$

But since e_2 is also an additive identity,

$$e_2 + e_1 \equiv e_1\ (\text{mod } n)$$

is also true.

Equating both of the above equations we get:

$$e_1 \equiv e_2\ (\text{mod } n)$$

which is a contradiction. Therefore, additive identity in $\mathbb{Z}/n\mathbb{Z}$ is unique and since $a(mod\, n) + 0 \equiv 0 + a(mod\, n) \equiv a(mod\, n)$ is true, the additive identity must be only 0.

v. To prove: $\forall a \in \mathbb{Z}/n\mathbb{Z}, \exists! (-a) \in \mathbb{Z}/n\mathbb{Z}$ such that $a + (-a) \equiv (-a) + a \equiv 0.$
This can alternatively be written as: $a + (-a) \equiv (-a) + a \equiv 0 \ (mod\, n).$
or: $a(mod\, n) + (-a)(mod\, n) \equiv (-a)(mod\, n) + a(mod\, n) \equiv 0(mod\, n).$

Let $a \in \mathbb{Z}$. Then:

$$a(mod\, n) + (-a)(mod\, n) \equiv (-a)(mod\, n) + a(mod\, n) \qquad \text{(from part } iii\text{)}$$

and:

$$\begin{aligned} a(mod\, n) + (-a)(mod\, n) &\equiv [a + (-a)](mod\, n) && \text{(by M2)} \\ &\equiv [0](mod\, n) && \text{(by I7)} \end{aligned}$$

Combining both:

$$a(mod\, n) + (-a)(mod\, n) \equiv (-a)(mod\, n) + a(mod\, n) \equiv 0(mod\, n)$$

Let's assume for contradiction that $\exists$ more than one additive inverse for $a \in \mathbb{Z}/n\mathbb{Z}$ and let them be a_1 and a_2. Then:

$$a + a_1 \equiv 0 \text{ (mod n) and } a + a_2 \equiv 0 \text{ (mod n)} \qquad ...(i)$$

We know that:

$$\begin{aligned} a_1 &\equiv a_1 + 0 \text{ (mod n)} && \text{(from part } iv\text{)} \\ a_1 &\equiv a_1 + (a + a_2) \text{ (mod n)} && \text{(from eq. } (i)\text{)} \\ a_1 &\equiv (a + a_1) + a_2 \text{ (mod n)} && \text{(by part } ii \text{ and } iii\text{)} \\ a_1 &\equiv 0 + a_2 \text{ (mod n)} && \text{(from eq. } (i)\text{)} \\ a_1 &\equiv a_2 \text{ (mod n)} && \text{(from part } iv\text{)} \end{aligned}$$

which is a contradiction. Therefore, additive inverse for *a* in $\mathbb{Z}/n\mathbb{Z}$ is unique and since $a(mod\, n) + (-a)(mod\, n) \equiv (-a)(mod\, n) + a(mod\, n) \equiv 0(mod\, n)$ is true, there must exist a unique additive inverse $(-a)$ for all *a* in $\mathbb{Z}/n\mathbb{Z}$.

vi. To prove: If $\forall a, b, c \in \mathbb{Z}/n\mathbb{Z}$, then: a + b ≡ a + c ⇒ b ≡ c and b + a ≡ c + a ⇒ b ≡ c.
This can alternatively be written as: a + b ≡ a + c (mod n) ⇒ b ≡ c (mod n) and b + a ≡ c + a ⇒ b ≡ c (mod n).

$$\begin{aligned} & a + b \equiv a + c \text{ (mod n)} && \text{(given)} \\ \Rightarrow\ & n \mid (a + b) - (a + c) && \text{(by M1)} \\ \Rightarrow\ & (a + b) - (a + c) = nk \text{ for some } k \in \mathbb{Z} && \text{(by divisibility)} \end{aligned}$$

=> (a + b) + (– a – c) = nk (by I4)
=> (a + –a) + (b – c) = nk (by I2, I3)
=> (0) + (b – c) = nk (by I7)
=> (b – c) = nk (by I5)
=> n | (b – c) (by divisibility)
=> b ≡ c (mod n) (by M1)

and: b + a ≡ c + a (mod n) (given)
=> n | (b + a) – (c + a) (by M1)
=> (b + a) – (c + a) = nk for some k ∈ ℤ (by divisibility)
=> (b + a) + (– c – a) = nk (by I4)
=> (b + – c) + (a – a) = nk (by I2, I3)
=> (b – c) + (0) = nk (by I7)
=> (b – c) = nk (by I5)
=> n | (b – c) (by divisibility)
=> b ≡ c (mod n) (by M1)

Altogether, the six properties (i) through (vi) are true, proving proposition 2. □

A.2.2. Multiplication in $\mathbb{Z}/n\mathbb{Z}$

Let's now verify if multiplication is a binary operation in ℤ modulo *n* systems.

In ℤ modulo 2 ($\mathbb{Z}/2\mathbb{Z}$):

For $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$, the Cayley table for multiplication is:

·	0	1
0	0	0
1	0	1

Is multiplication a binary operation in $\mathbb{Z}/2\mathbb{Z}$?

A.1.2	R1	R2	R3
Yes/No	Yes	Yes	Yes

Therefore, yes, multiplication is a binary operation in $\mathbb{Z}/2\mathbb{Z}$.

What properties of binary operations does multiplication exhibit in $\mathbb{Z}/2\mathbb{Z}$?

A.1.2	P1	P2	P3	P4	P5	P6	P7	P8
Yes/No	Yes	Yes	Yes	Yes (over '+')	Yes (1)	Selectively (yes if a = 1)	No (but 0,1 are idempotent)	Selectively (yes if a = 1)

In $\mathbb{Z}$ modulo 3 ($\mathbb{Z}/3\mathbb{Z}$):

For $\mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$, the Cayley table for multiplication is:

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Is multiplication a binary operation in $\mathbb{Z}/3\mathbb{Z}$?

A.1.2	R1	R2	R3
Yes/No	Yes	Yes	Yes

Therefore, yes, multiplication is a binary operation in $\mathbb{Z}/3\mathbb{Z}$.

What properties of binary operations does multiplication exhibit in $\mathbb{Z}/3\mathbb{Z}$?

A.1.2	P1	P2	P3	P4	P5	P6	P7	P8
Yes/No	Yes	Yes	Yes	Yes (over '+')	Yes (1)	Selectively (yes if a = 1,2)	No (but 0,1 are idempotent)	Selectively (yes if a = 1,2)

In $\mathbb{Z}$ modulo 4 ($\mathbb{Z}/4\mathbb{Z}$):

For $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$, the Cayley table for multiplication is:

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3

$\cdot$	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Is multiplication a binary operation in $\mathbb{Z}/4\mathbb{Z}$?

A.1.2	R1	R2	R3
Yes/No	Yes	Yes	Yes

Therefore, yes, multiplication is a binary operation in $\mathbb{Z}/4\mathbb{Z}$.

What properties of binary operations does multiplication exhibit in $\mathbb{Z}/4\mathbb{Z}$?

A.1.2	P1	P2	P3	P4	P5	P6	P7	P8
Yes/No	Yes	Yes	Yes	Yes (over '+')	Yes (1)	Selectively (yes if a = 1,3)	No (but 0,1 are idempotent)	Selectively (yes if a = 1,3)

In $\mathbb{Z}$ modulo 5 ($\mathbb{Z}/5\mathbb{Z}$):

For $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$, the Cayley table for multiplication is:

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Is multiplication a binary operation in $\mathbb{Z}/5\mathbb{Z}$?

A.1.2	R1	R2	R3
Yes/No	Yes	Yes	Yes

Therefore, yes, multiplication is a binary operation in $\mathbb{Z}/5\mathbb{Z}$.

What properties of binary operations does multiplication exhibit in $\mathbb{Z}/5\mathbb{Z}$?

A.1.2	P1	P2	P3	P4	P5	P6	P7	P8
Yes/No	Yes	Yes	Yes	Yes (over '+')	Yes (1)	Selectively (yes if a = 1,2,3,4)	No (but 0,1 are idempotent)	Selectively (yes if a = 1,2,3,4)

In $\mathbb{Z}$ modulo n ($\mathbb{Z}/n\mathbb{Z}$):

For $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, 3, . . ., (n - 1)\}$, the Cayley table for multiplication is:

·	0	1	2	3	...	$n - 1$
0	0	0	0	0	...	0
1	0	1	2	3	...	$n - 1$
2	0	2	4	6	...	$2n - 2$
3	0	3	6	9	...	$3n - 3$
. . .	. . .	. . .	. . .	. . .	... ...	. . .
$n - 1$	0	$n - 1$	$2n - 2$	$3n - 3$	...	n^2-2n+1

<u>Proposition 3.</u> Multiplication is a binary operation in $\mathbb{Z}/n\mathbb{Z}$ for any integer $n > 0$.

Proof:

In order to prove the above proposition we need to prove that multiplication in $\mathbb{Z}/n\mathbb{Z}$ adheres to the below principles:

i. It must take exactly two elements from $\mathbb{Z}/n\mathbb{Z}$ as input.
ii. When applied to the two input elements, it must yield a single, unique output
iii. It must exhibit closure.

By def^n of multiplication in modular arithmetics (see M3 in section A.1.4.):

$$x(mod\ n) \cdot y(mod\ n) \equiv (xy)\ (mod\ n)$$

From this it can be observed that multiplication in $\mathbb{Z}/n\mathbb{Z}$ has exactly two inputs from the set. Therefore, (i) is true.

Now, by division algorithm, we can write:

$$xy = nq + r \qquad \text{where } 0 \leq r < q$$

Taking *mod n* on both sides:

$$(xy)(mod\, n) \equiv r\ (mod\, n) \qquad \text{(by M1)}$$

Then:

$$x(mod\, n) \cdot y(mod\, n) \equiv r\ (mod\, n)$$

This shows that if $x, y \in \mathbb{Z}/n\mathbb{Z}$ then $xy \in \mathbb{Z}/n\mathbb{Z}$ and thus, multiplication in $\mathbb{Z}/n\mathbb{Z}$ is closed. This shows that *(iii)* is true.

Additionally, since the division algorithm states that r is unique for every (xy), n and q, $r\ (mod\, n)$ and in turn $x(mod\, n) \cdot y(mod\, n)$ is also unique for every x, y. Therefore, showing that *(ii)* is true as well.

Altogether, we can say multiplication is a binary operation in $\mathbb{Z}/n\mathbb{Z}$. □

Proposition 4. Multiplication adheres to the following properties of binary operations in $\mathbb{Z}/n\mathbb{Z}$ (for any integer $n > 1$):

i. Closure: $\forall a, b \in \mathbb{Z}/n\mathbb{Z}\,,\ ab \in \mathbb{Z}/n\mathbb{Z}$
ii. Associativity: $\forall a, b, c \in \mathbb{Z}/n\mathbb{Z}\,, (ab)c \equiv a(bc)$.
iii. Commutativity: $\forall a, b \in \mathbb{Z}/n\mathbb{Z}\,, ab \equiv ba$.
iv. Distributivity over addition: $\forall a, b, c \in \mathbb{Z}/n\mathbb{Z}\,, (a + b)c \equiv ac + bc$ and $c(a + b) \equiv ca + cb$.
v. Existence of multiplicative identity: There is a unique element $1 \in \mathbb{Z}/n\mathbb{Z}$ such that $\forall a \in \mathbb{Z}/n\mathbb{Z}\,, a \cdot 1 \equiv 1 \cdot a \equiv a$.
vi. Selective existence of multiplicative inverse: $\forall a \in \mathbb{Z}/n\mathbb{Z}$ and $gcd\ (a, n) = 1, \exists!\, a' \in \mathbb{Z}/n\mathbb{Z}$ such that $a \cdot a' \equiv a' \cdot a \equiv 1$.
vii. Selective cancellation: If $\forall a, b, c \in \mathbb{Z}/n\mathbb{Z}$ and $gcd\ (a, n) = 1$, we have:

$$\text{ab} \equiv \text{ac} \Rightarrow \text{b} \equiv \text{c and ba} \equiv \text{ca} \Rightarrow \text{b} \equiv \text{c}$$

Proof:

i. <u>To prove:</u> $\forall a, b \in \mathbb{Z}/n\mathbb{Z}\,,\ a + b \in \mathbb{Z}/n\mathbb{Z}$.

See proof of proposition 3.

ii. To prove: $\forall a, b, c \in \mathbb{Z}/n\mathbb{Z}, (ab)c \equiv a(bc)$.

This can alternatively be written as: $(ab)c \equiv a(bc)(mod\, n)$.

or: $[a(mod\, n) \cdot b(mod\, n)] \cdot c(mod\, n) \equiv a(mod\, n) \cdot [b(mod\, n) \cdot c(mod\, n)]$.

Let $a, b, c \in \mathbb{Z}$. Then:

$$\begin{aligned} [a(mod\, n) \cdot b(mod\, n)] \cdot c(mod\, n) &\equiv [(ab)(mod\, n)] \cdot c(mod\, n) && \text{(by M3)} \\ &\equiv [(ab)c](mod\, n) && \text{(by M3)} \\ &\equiv [a(bc)](mod\, n) && \text{(by I2)} \\ &\equiv a(mod\, n) \cdot [(bc)(mod\, n)] && \text{(by M3)} \\ &\equiv a(mod\, n) \cdot [b(mod\, n) \cdot c(mod\, n)] && \text{(by M3)} \end{aligned}$$

iii. To prove: $\forall a, b \in \mathbb{Z}/n\mathbb{Z}, ab \equiv ba$.

This can alternatively be written as: $ab \equiv ba(mod\, n)$.

or: $a(mod\, n) \cdot b(mod\, n) \equiv b(mod\, n) \cdot a(mod\, n)$.

Let $a, b \in \mathbb{Z}$. Then:

$$\begin{aligned} a(mod\, n) \cdot b(mod\, n) &\equiv [a \cdot b](mod\, n) && \text{(by M3)} \\ &\equiv [b \cdot a](mod\, n) && \text{(by I3)} \\ &\equiv b(mod\, n) \cdot a(mod\, n) && \text{(by M3)} \end{aligned}$$

iv. To prove: $\forall a, b, c \in \mathbb{Z}/n\mathbb{Z}, (a + b)c \equiv ac + bc \text{ and } c(a + b) \equiv ca + cb$.

This can alternatively be written as: $(a + b)c \equiv ac + bc\ (mod\, n)$ and $c(a + b) \equiv ca + cb(mod\, n)$.

or: $[a(mod\, n) + b(mod\, n)] \cdot c(mod\, n) \equiv ac\ (mod\, n) + bc\ (mod\, n)$ and $c(mod\, n) \cdot [a(mod\, n) + b(mod\, n)] \equiv ca + cb(mod\, n)$.

Let $a, b, c \in \mathbb{Z}$. Then:

$$\begin{aligned} [a(mod\, n) + b(mod\, n)] \cdot c(mod\, n) &\equiv [(a + b)c](mod\, n) && \text{(by M3)} \\ &\equiv [ac + bc](mod\, n) && \text{(by I4)} \\ &\equiv ac(mod\, n) + bc(mod\, n) && \text{(by M3)} \end{aligned}$$

and:

$$\begin{aligned} c(mod\, n) \cdot [a(mod\, n) + b(mod\, n)] &\equiv [c(a + b)](mod\, n) && \text{(by M3)} \\ &\equiv [ca + cb](mod\, n) && \text{(by I4)} \\ &\equiv ca(mod\, n) + cb(mod\, n) && \text{(by M3)} \end{aligned}$$

v. <u>To prove:</u> There is a unique element $1 \in \mathbb{Z}/n\mathbb{Z}$ such that $\forall a \in \mathbb{Z}/n\mathbb{Z}, a \cdot 1 \equiv 1 \cdot a \equiv a$.

This can alternatively be written as: $a \cdot 1 \equiv 1 \cdot a \equiv a\ (mod\ n)$.
or: $a(mod\ n) \cdot 1 \equiv 1 \cdot a(mod\ n) \equiv a(mod\ n)$.

Let $a \in \mathbb{Z}$. Then:
$a(mod\ n) \cdot 1 \equiv 1 \cdot a(mod\ n)$ (from part *iii*)
and: $a(mod\ n) \cdot 1 \equiv [a \cdot 1](mod\ n)$ (by M3)
$\equiv [a](mod\ n)$ (by I6)
Combining both: $a(mod\ n) \cdot 1 \equiv 1 \cdot a(mod\ n) \equiv a(mod\ n)$.

Let's assume for contradiction that ∃ more than one multiplicative identity in $\mathbb{Z}/n\mathbb{Z}$ and let them be $e_1$and e_2. Then for all a ∈ $\mathbb{Z}/n\mathbb{Z}$:

$$\text{a (mod n)} \cdot e_1 \equiv \text{a (mod n)}$$

Since $e_2 \in \mathbb{Z}/n\mathbb{Z}$, substituting a = e_2, we get:

$$e_2 \cdot e_1 \equiv e_2 \text{ (mod n)}$$

But since e_2 is also an multiplicative identity,

$$e_2 \cdot e_1 \equiv e_1 \text{ (mod n)}$$

is also true.

Equating both of the above equations we get:

$$e_1 \equiv e_2 \text{ (mod n)}$$

which is a contradiction. Therefore, multiplicative identity in $\mathbb{Z}/n\mathbb{Z}$ is unique and since $a(mod\ n). 1 \equiv 1. a(mod\ n) \equiv a(mod\ n)$ is true, the multiplicative identity must be only 1.

vi. <u>To prove:</u> $\forall a \in \mathbb{Z}/n\mathbb{Z}, \exists!\, a' \in \mathbb{Z}/n\mathbb{Z}$ such that $a \cdot a' \equiv a' \cdot a \equiv 1$ iff $gcd\ (a, n) = 1$.
This can alternatively be written as: $a \cdot a' \equiv a' \cdot a \equiv 1\ (mod\ n)$.

Let $a \in \mathbb{Z}$. Then:

$a \cdot a' \equiv 1\ (mod\ n)$
$n \mid (a \cdot a') - 1$ (by M1)

$(a \cdot a') - 1 = nk$ for some $k \in \mathbb{Z}$ (by divisibility)

$(a \cdot a') - nk = 1$ (by I1, I2, I3, I7)

Since $a, k, 1 \in \mathbb{Z}$, we can say $(a \cdot a') - nk = 1$ is of the form of a linear Diophantine equation. According to the def^{n} of linear Diophantine equations, there exists a solution for this particular equation iff $gcd\ (a, n)|1$. However, we know that the only factor of 1 is 1 itself and therefore, the equation $(a \cdot a') - nk = 1$ will have a solution iff $gcd\ (a, n) = 1$.

Combining this and $a \cdot a' \equiv a' \cdot a$ (from part *iii*), we can say that $\forall a \in \mathbb{Z}/n\mathbb{Z}$, there exists $a' \in \mathbb{Z}/n\mathbb{Z}$ such that $a \cdot a' \equiv a' \cdot a \equiv 1$ iff $gcd\ (a, n) = 1$.

Let's assume for contradiction that ∃ more than one additive inverse for $a \in \mathbb{Z}/n\mathbb{Z}$ and let them be a' and a''. Then:

$a \cdot a' \equiv 1\ (mod\ n)$ and $a \cdot a'' \equiv 1\ (mod\ n)$ ...*(i)*

We know that:

$a' \equiv a' \cdot 1$ (mod n) (from part *v*)

$a' \equiv a' \cdot (a \cdot a'')$ (mod n) (from eq. *(i)*)

$a' \equiv (a \cdot a') \cdot a''$ (mod n) (by part *ii* and *iii*)

$a' \equiv 1 \cdot a''$ (mod n) (from eq. *(i)*)

$a' \equiv a''$ (mod n) (from part *v*)

which is a contradiction. Therefore, multiplicative inverse for a in $\mathbb{Z}/n\mathbb{Z}$ is unique if it exists. Altogether, we can say, $\forall a \in \mathbb{Z}/n\mathbb{Z}$, $\exists!\ a' \in \mathbb{Z}/n\mathbb{Z}$ s.t. $a \cdot a' \equiv a' \cdot a \equiv 1$ iff $gcd\ (a, n) = 1$.

vii. To prove: If $\forall a, b, c \in \mathbb{Z}/n\mathbb{Z}$ and $gcd\ (a, n) = 1$, then: ab ≡ ac ⇒ b ≡ c and ba ≡ ca ⇒ b ≡ c.

This can alternatively be written as: ab ≡ ac (mod n) ⇒ b ≡ c (mod n) and ba ≡ ca ⇒ b ≡ c (mod n).

$gcd\ (a, n) = 1$ implies that *a* and *n* are co-prime ie. they have no other common factor than 1.

ab ≡ ac (mod n) (given)

=> *n | (ab) – (ac)* (by M1)

=> *(ab) – (ac) = nk* for some $k \in \mathbb{Z}$ (by divisibility)

=> $a(b - c) = nk$ (by I4)
=> $n \mid a(b - c)$ (by divisibility)

Therefore, since $n \mid a(b - c)$ and $gcd\ (a, n) = 1$, we can infer that (b – c) must be an integer multiple of n ie. $n \mid (b - c)$. This implies:

$n \mid (b - c)$
=> $b \equiv c\ (mod\ n)$ (by M1)

and: $ba \equiv ca\ (mod\ n)$ (given)
=> $n \mid (ba) - (ca)$ (by M1)
=> $(ba) - (ca) = nk$ for some $k \in \mathbb{Z}$ (by divisibility)
=> $(b - c)a = nk$ (by I4)
=> $n \mid (b - c)a$ (by divisibility)

Therefore, since $n \mid (b - c)a$ and $gcd\ (a, n) = 1$, we can infer that (b – c) must be an integer multiple of n ie. $n \mid (b - c)$. This implies:

$n \mid (b - c)$
=> $b \equiv c\ (mod\ n)$ (by M1)

Altogether, the seven properties (i) through (vii) are true, proving proposition 4. □

A.3. Conclusion

Through this project, we have identified that both addition and multiplication are indeed binary operations under $\mathbb{Z}$ and all number systems $\mathbb{Z}/n\mathbb{Z}$ where $n \in \mathbb{Z}$ and $n > 1$.

We have also identified and proved the properties of binary operation displayed by addition and multiplication in $\mathbb{Z}/n\mathbb{Z}$. Here is a compilation of all the observations made regarding the properties:

Properties of addition '+'

+	Binary?	P1	P2	P3	P4	P5	P6	P7	P8
$\mathbb{Z}/2\mathbb{Z}$	Yes	Yes	Yes	Yes	No	Yes (0)	Yes	No (but 0 is idempotent)	Yes

$\mathbb{Z}/3\mathbb{Z}$	Yes	Yes	Yes	Yes	No	Yes (0)	Yes	No (but 0 is idempotent)	Yes
$\mathbb{Z}/4\mathbb{Z}$	Yes	Yes	Yes	Yes	No	Yes (0)	Yes	No (but 0 is idempotent)	Yes
$\mathbb{Z}/5\mathbb{Z}$	Yes	Yes	Yes	Yes	No	Yes (0)	Yes	No (but 0 is idempotent)	Yes
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
$\mathbb{Z}/n\mathbb{Z}$	Yes	Yes	Yes	Yes	No	Yes (0)	Yes	No (but 0 is idempotent)	Yes

Properties of multiplication ‘·’

·	Binary?	P1	P2	P3	P4	P5	P6	P7	P8
$\mathbb{Z}/2\mathbb{Z}$	Yes	Yes	Yes	Yes	Yes (over ‘+’)	Yes (1)	Selectively (yes if a = 1)	No (but 0,1 are idempotent)	Selectively (yes if a = 1)
$\mathbb{Z}/3\mathbb{Z}$	Yes	Yes	Yes	Yes	Yes (over ‘+’)	Yes (1)	Selectively (yes if a = 1,2)	No (but 0,1 are idempotent)	Selectively (yes if a = 1,2)
$\mathbb{Z}/4\mathbb{Z}$	Yes	Yes	Yes	Yes	Yes (over ‘+’)	Yes (1)	Selectively (yes if a = 1,3)	No (but 0,1 are idempotent)	Selectively (yes if a = 1,3)
$\mathbb{Z}/5\mathbb{Z}$	Yes	Yes	Yes	Yes	Yes (over ‘+’)	Yes (1)	Selectively (yes if a = 1,2,3,4)	No (but 0,1 are idempotent)	Selectively (yes if a = 1,2,3,4)
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
$\mathbb{Z}/n\mathbb{Z}$	Yes	Yes	Yes	Yes	Yes (over ‘+’)	Yes (1)	Selectively (yes a iff *gcd(a,n)=1)*	No (but 0,1 are idempotent)	Selectively (yes a iff *gcd(a,n)=1)*

Bibliography:

1. https://www.doc.ic.ac.uk/~mrh/330tutor/ch03.html
2. https://kconrad.math.uconn.edu/blurbs/ugradnumthy/modarith.pdf
3. https://sites.millersville.edu/bikenaga/math-proof/modular-arithmetic/modular-arithmetic.html
4. https://en.wikipedia.org/wiki/Modular_arithmetic

Scalar and Vector Triple Products and their Geometrical Interpretation

Abstract:

This project explores the concept of triple products. It dives deep into the definition, geometrical interpretation, calculation and properties of scalar and vector triple products. It also introduces the concept of quadruple products.

B.1. Introduction:

In geometry and algebra, the triple product is a product of three 3-dimensional vectors, usually Euclidean vectors. The name "triple product" is used for two different products, the scalar-valued scalar triple product and, less often, the vector-valued vector triple product. Before we explore these triple products, let's first define some basic terms associated with the concept.

B.1.1. Scalar Product

The scalar product, also known as the dot product or inner product, is a mathematical operation that takes two vectors and produces a scalar quantity. It is defined for vectors in Euclidean space but can also be extended to other vector spaces.

For two vectors $A = (A_1, A_2, A_3, \ldots, A_n)$ and $B = (B_1, B_2, B_3, \ldots, B_n)$, the scalar product is calculated as follows:

$$A \cdot B = A_1B_1 + A_2B_2 + A_3B_3 + \ldots + A_nB_n$$

Alternatively, it can be expressed using the summation notation as:

$$A \cdot B = \sum_{i=1}^{n} (A_i\, B_i)$$

Scalar product can also be given as:

$$A \cdot B = |A|\,|B| \cos\theta$$

where θ is the angle between A and B.

The result of the scalar product is a scalar value, not a vector, which represents the magnitude of the projection of one vector onto the other. Geometrically, it represents the product of the lengths of the vectors and the cosine of the angle between them.

The scalar product has several important properties, including commutativity ($A \cdot B = B \cdot A$), linearity ($A \cdot (B + C) = A \cdot B + A \cdot C$), and distributivity with scalar multiplication ($k(A \cdot B) = (kA) \cdot B = A \cdot (kB)$).

B.1.2. Vector Product

The vector product, also known as the cross product, is a mathematical operation that takes two vectors in three-dimensional space and produces a new vector perpendicular to the original two vectors. Unlike the scalar product, which results in a scalar, the vector product produces a vector.

For two vectors $A = (A_1i + A_2j + A_3k)$ and $B = (B_1i + B_2j + B_3k)$, the vector product is calculated as follows:

$$A \times B = (A_2B_3 - A_3B_2)i + (A_3B_1 - A_1B_3)j + (A_1B_2 - A_2B_1)k$$

Alternatively, it can be expressed using the determinant notation:

$$A \times B = \begin{vmatrix} i & j & k \\ A_1 & A_2 & A_3 \\ B_1 & B_2 & B_3 \end{vmatrix}$$

Where i, j, and k are the unit vectors along the x, y, and z axes, respectively.

The cross product A × B produces a new vector that is orthogonal (perpendicular) to both A and B. The magnitude of the resulting vector is equal to the product of the magnitudes of A and B multiplied by the sine of the angle between them. The resulting vector follows the right-hand rule ie., if you point your right thumb in the direction of A and curl your fingers towards B, the direction your extended fingers point in will be the direction of the resulting vector.

Geometrically, the cross product represents a vector that is perpendicular to the plane formed by A and B. If you imagine extending A and B to form a parallelogram, the cross-product gives the area of the parallelogram.

The vector product has several important properties, including anti-commutativity ($A \times B = -B \times A$), linearity ($A \times (B + C) = A \times B + A \times C$), and distributivity with scalar multiplication ($k(A \times B) = (kA) \times B = A \times (kB)$).

B.1.3. Some Other Definitions

Here are some other definitions that is used ahead:

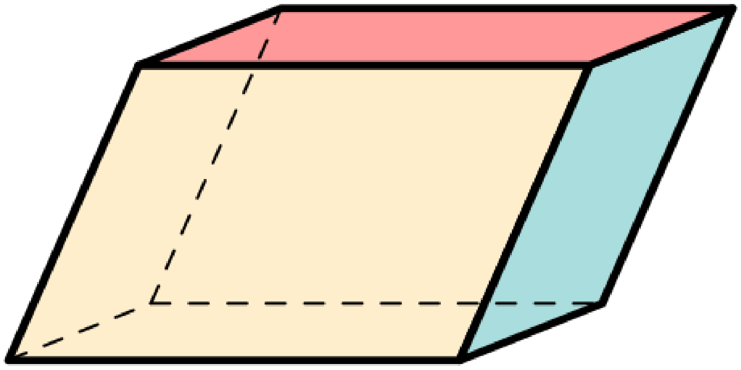
1. Parallelepiped: A parallelepiped is a three-dimensional geometric shape formed by six parallelograms as its faces. It is a generalization of a parallelogram to three dimensions.

   A parallelepiped has eight vertices, twelve edges, and six faces. Each face is a parallelogram, and opposite faces are parallel and congruent. The edges of a parallelepiped are shared by two faces, and the angles between adjacent faces are equal.

   Three equivalent definitions of parallelepiped are

   - a polyhedron with six faces (hexahedron), each of which is a parallelogram,
   - a hexahedron with three pairs of parallel faces, and
   - a prism of which the base is a parallelogram.

   The shape of a parallelepiped is determined by the lengths of its three pairwise non-parallel edges and the angles between them. These edges are usually referred to as the base vectors or sides of the parallelepiped.



2. Vector Projection:

   The vector projection of one vector over another vector is the length of the shadow of the given vector over another vector. It is obtained by multiplying the magnitude of the given vector with the cosine of the angle between the two vectors ie.the projection of one vector u onto another vector v is given by:

$$\frac{u \cdot v}{|u|}$$

   The resultant of a vector projection formula is a scalar value.

B.2. Scalar Triple Product:

B.2.1. Definition

The scalar triple product (also called the mixed product, box product, or triple scalar product) is defined as the dot product of one of the vectors with the cross product of the other two i.e., if a, b, c are three vectors, then their scalar triple product is:

$$a \cdot (b \times c)$$

Symbolically, it is also written as:

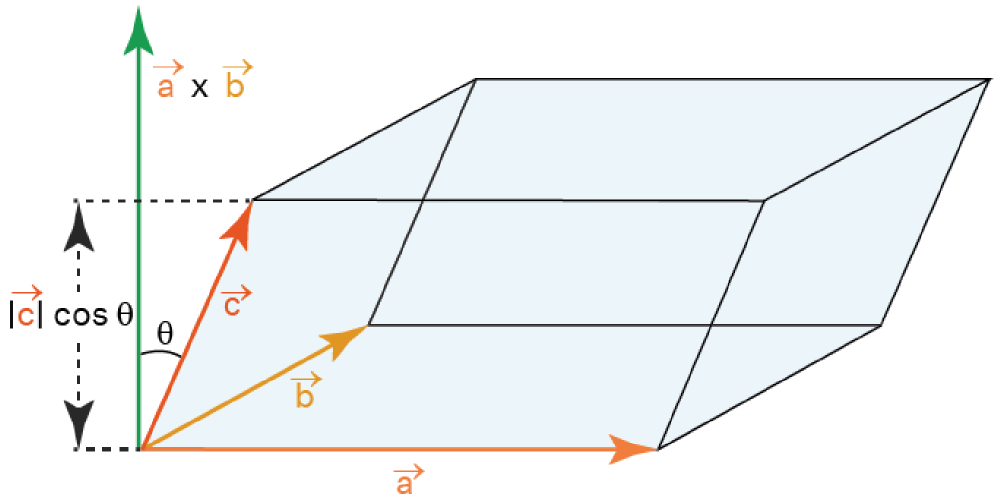
$$[a\ b\ c] = [a, b, c] = a \cdot (b \times c).$$

B.2.2. Geometrical Interpretation

Proposition 1. Geometrically, the scalar triple product:

$$c \cdot (a \times b)$$

is the (signed) volume of the parallelepiped defined by the three vectors a, b, c.



<u>Proof:</u>

The volume of the parallelepiped is the base area times the height. The base area, as you know, is the magnitude of the area of the parallelogram formed by vectors a and b which is equal to |a× b| by def^{n} of the vector product. Using the definition of cross product, we also know that a × b is perpendicular to the plane containing vectors a and b. Then the height of the parallelepiped is given by the projection of c along (a × b), which is equal to:

$$\frac{c \cdot (a \times b\,)}{|a \times b|}$$

Then:

$$\text{Volume} = \text{Base} \cdot \text{Height}$$

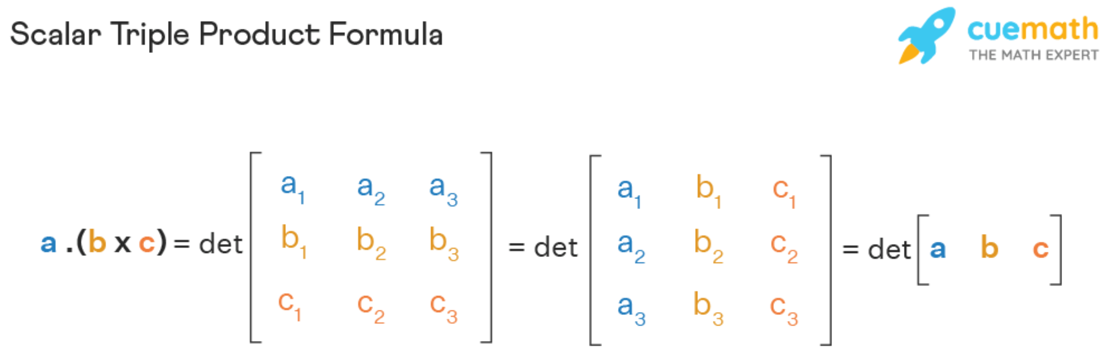
$$=> \qquad \text{Volume} = |\text{a} \times \text{b}| \cdot \frac{c \cdot (a \times b\,)}{|a \times b|}$$

$$=> \qquad \text{Volume} = |c \cdot (a \times b\,)|$$

which is the scalar triple product of the vectors. □

B.2.3. Calculation of Scalar Triple Product

Proposition 2. For any three vectors a = a_1i + a_2 j + a_3k, b = b_1i + b_2 j + b_3k, and c = c_1i + c_2j + c_3k, the62161ir scalar triple product is given by the determinant of the components of the three vectors, ie:



Scalar Triple Product Formula

$$\mathbf{a}\,.(\mathbf{b} \times \mathbf{c}) = \det\begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{bmatrix} = \det\begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{bmatrix} = \det\begin{bmatrix} \mathbf{a} & \mathbf{b} & \mathbf{c} \end{bmatrix}$$

cuemath
THE MATH EXPERT

Proof:

Using the definition of the cross product and dot product, we have:

$$a \cdot (b \times c) = \vec{a} \cdot \begin{vmatrix} \hat{i} & \hat{j} & \hat{k} \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix}$$

$$= [(b_2c_3 - c_2b_3)\hat{i} - (b_1c_3 - c_1b_3)\hat{j} + (b_1c_2 - c_1b_2)\hat{k}] \cdot (a_1\hat{i} + a_2\hat{j} + a_3\hat{k})$$

$$= (b_2c_3 - c_2b_3)a_1 + (c_1b_3 - b_1c_3)a_2 + (b_1c_2 - c_1b_2)a_3$$

$$= \begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix}$$

□

B.2.4. Properties of Scalar Triple Products

We have explored the concept of the scalar triple product along with its geometrical interpretation and formula. Let us now go through some of its important properties for a better understanding of the concept:

1. Swapping the positions of the operators without re-ordering the operands leaves the triple product unchanged. This follows from the preceding property and the commutative property of the dot product:

$$a \cdot (b \times c) = (b \times c) \cdot a$$

2. The scalar triple product is unchanged under a circular shift of its three operands (a, b, c) due to the property of determinants:

$$\mathbf{a} \cdot (\mathbf{b} \times \mathbf{c}) = \mathbf{b} \cdot (\mathbf{c} \times \mathbf{a}) = \mathbf{c} \cdot (\mathbf{a} \times \mathbf{b})$$

$$\boldsymbol{abc} = \begin{vmatrix} a_x & a_y & a_z \\ b_x & b_y & b_z \\ c_x & c_y & c_z \end{vmatrix} = \begin{vmatrix} c_x & c_y & c_z \\ a_x & a_y & a_z \\ b_x & b_y & b_z \end{vmatrix} = \begin{vmatrix} b_x & b_y & b_z \\ c_x & c_y & c_z \\ a_x & a_y & a_z \end{vmatrix} .$$

3. Swapping any two of the three operands negates the triple product. This follows from the circular-shift property and the anticommutativity of the cross product can be shown using the property of determinants:

$$\begin{aligned}\mathbf{a}\cdot(\mathbf{b}\times\mathbf{c}) &= -\mathbf{a}\cdot(\mathbf{c}\times\mathbf{b})\\ &= -\mathbf{b}\cdot(\mathbf{a}\times\mathbf{c})\\ &= -\mathbf{c}\cdot(\mathbf{b}\times\mathbf{a})\end{aligned}$$

$$\boldsymbol{abc} = \begin{vmatrix} a_x & a_y & a_z \\ b_x & b_y & b_z \\ c_x & c_y & c_z \end{vmatrix} = -\begin{vmatrix} b_x & b_y & b_z \\ a_x & a_y & a_z \\ c_x & c_y & c_z \end{vmatrix} = -\begin{vmatrix} a_x & a_y & a_z \\ c_x & c_y & c_z \\ b_x & b_y & b_z \end{vmatrix},$$

4. If any two vectors in the scalar triple product are equal or parallel, then its value is zero:
$$\mathbf{a}\cdot(\mathbf{a}\times\mathbf{b}) = \mathbf{a}\cdot(\mathbf{b}\times\mathbf{a}) = \mathbf{a}\cdot(\mathbf{b}\times\mathbf{b}) = \mathbf{b}\cdot(\mathbf{a}\times\mathbf{a}) = 0$$

5. If a, b, c are coplanar, then $a \cdot (b \times c) = 0$ since $b \times c$ produces a vector that is perpendicular to a and the scalar product of two perpendicular vectors is zero. Geometrically, we can explain this as possible because the parallelepiped defined by them would be flat and have no volume.

6. $[\lambda a\ b\ c] = [a\ \lambda b\ c] = [a\ b\ \lambda c] = \lambda\ [a\ b\ c]$, where λ is a real number because:
$[\lambda a\ b\ c] = (\lambda a) \cdot (b \times c) = \lambda \cdot(a \cdot (b \times c)) = \lambda\ [a\ b\ c]$
$[a\ \lambda b\ c] = [\lambda b\ c\ a] = (\lambda b) \cdot (c \times a) = \lambda \cdot(b \cdot (c \times a)) = \lambda\ [b\ c\ a] = \lambda\ [a\ b\ c]$
$[a\ b\ \lambda c] = [\lambda c\ a\ b] = (\lambda c) \cdot (a \times b) = \lambda \cdot(c \cdot (a \times b)) = \lambda\ [c\ a\ b] = \lambda\ [a\ b\ c]$

7. $[(a + b)\ c\ d] = [a\ c\ d] + [b\ c\ d]$ because:
$[(a + b)\ c\ d] = (a + b) \cdot (c \times d) = a \cdot (c \times d) + b \cdot (c \times d) = [a\ c\ d] + [b\ c\ d]$

and $[a\ (b+c)\ d] = [a\ b\ d] + [a\ c\ d]$ because:
$[a\ (b+c)\ d] = a \cdot ((b+c) \times d) = a \cdot ((b+c) \times d) = a \cdot (b\times d + c \times d) = a \cdot (b\times d) + a \cdot (c \times d)$
$= [a\ b\ d] + [a\ c\ d]$

and $[a\ b\ (c+d)] = [a\ b\ c] + [a\ b\ d]$ because:
$[a\ b\ (c+d)] = a \cdot (b \times (c+d)) = a \cdot ((b \times c)+(b \times d)) = a \cdot (b \times c) + a \cdot (b \times d) = [a\ b\ c] +$
$[a\ b\ d]0$

8. The simple product of two triple products (or the square of a triple product), may be expanded in terms of dot products:

$$((\mathbf{a}\times\mathbf{b})\cdot\mathbf{c})\,((\mathbf{d}\times\mathbf{e})\cdot\mathbf{f}) = \det\begin{bmatrix} \mathbf{a}\cdot\mathbf{d} & \mathbf{a}\cdot\mathbf{e} & \mathbf{a}\cdot\mathbf{f} \\ \mathbf{b}\cdot\mathbf{d} & \mathbf{b}\cdot\mathbf{e} & \mathbf{b}\cdot\mathbf{f} \\ \mathbf{c}\cdot\mathbf{d} & \mathbf{c}\cdot\mathbf{e} & \mathbf{c}\cdot\mathbf{f} \end{bmatrix}$$

B.3. Vector Triple Product:

B.3.1. Definition and Geometric Interpretation

The vector triple product is defined as the cross product of one vector with the cross product of the other two:

$$a \times (b \times c)$$

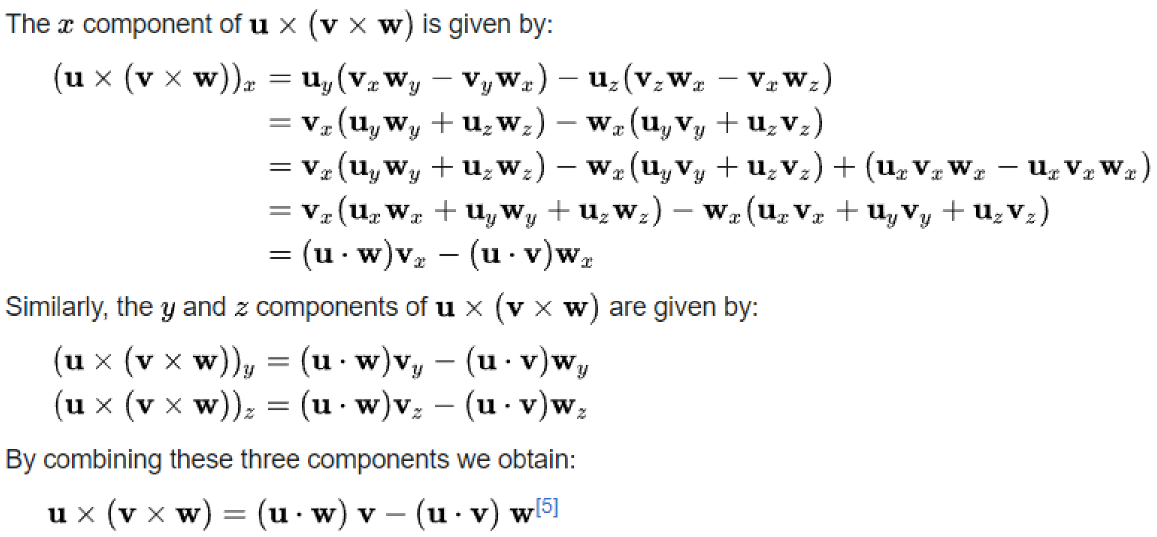
A vector triple product usually represents another vector geometrically. This is because the vector product of two vectors gives a vector and the cross product of this vector with the third vector also results in another vector.

B.3.2 Calculation of Vector Triple Product

Proposition 3. The vector cross-product can be solved by the below relationship (known as triple product expansion, or Lagrange's formula):

$$\mathbf{a}\times(\mathbf{b}\times\mathbf{c}) = (\mathbf{a}\cdot\mathbf{c})\mathbf{b} - (\mathbf{a}\cdot\mathbf{b})\mathbf{c}.$$

<u>Proof:</u>



The x component of $\mathbf{u}\times(\mathbf{v}\times\mathbf{w})$ is given by:

$$\begin{aligned}(\mathbf{u}\times(\mathbf{v}\times\mathbf{w}))_x &= \mathbf{u}_y(\mathbf{v}_x\mathbf{w}_y - \mathbf{v}_y\mathbf{w}_x) - \mathbf{u}_z(\mathbf{v}_z\mathbf{w}_x - \mathbf{v}_x\mathbf{w}_z) \\ &= \mathbf{v}_x(\mathbf{u}_y\mathbf{w}_y + \mathbf{u}_z\mathbf{w}_z) - \mathbf{w}_x(\mathbf{u}_y\mathbf{v}_y + \mathbf{u}_z\mathbf{v}_z) \\ &= \mathbf{v}_x(\mathbf{u}_y\mathbf{w}_y + \mathbf{u}_z\mathbf{w}_z) - \mathbf{w}_x(\mathbf{u}_y\mathbf{v}_y + \mathbf{u}_z\mathbf{v}_z) + (\mathbf{u}_x\mathbf{v}_x\mathbf{w}_x - \mathbf{u}_x\mathbf{v}_x\mathbf{w}_x) \\ &= \mathbf{v}_x(\mathbf{u}_x\mathbf{w}_x + \mathbf{u}_y\mathbf{w}_y + \mathbf{u}_z\mathbf{w}_z) - \mathbf{w}_x(\mathbf{u}_x\mathbf{v}_x + \mathbf{u}_y\mathbf{v}_y + \mathbf{u}_z\mathbf{v}_z) \\ &= (\mathbf{u}\cdot\mathbf{w})\mathbf{v}_x - (\mathbf{u}\cdot\mathbf{v})\mathbf{w}_x\end{aligned}$$

Similarly, the y and z components of $\mathbf{u}\times(\mathbf{v}\times\mathbf{w})$ are given by:

$$\begin{aligned}(\mathbf{u}\times(\mathbf{v}\times\mathbf{w}))_y &= (\mathbf{u}\cdot\mathbf{w})\mathbf{v}_y - (\mathbf{u}\cdot\mathbf{v})\mathbf{w}_y \\ (\mathbf{u}\times(\mathbf{v}\times\mathbf{w}))_z &= (\mathbf{u}\cdot\mathbf{w})\mathbf{v}_z - (\mathbf{u}\cdot\mathbf{v})\mathbf{w}_z\end{aligned}$$

By combining these three components we obtain:

$$\mathbf{u}\times(\mathbf{v}\times\mathbf{w}) = (\mathbf{u}\cdot\mathbf{w})\,\mathbf{v} - (\mathbf{u}\cdot\mathbf{v})\,\mathbf{w}$$ [5]

B.3.3. Properties of Vector Triple Product

1. Since scalar product is commutative, $a \times (b \times c) = (a \cdot b)c - (a \cdot c)b = c(a \cdot b) - b(a \cdot c)$.
2. Since vector product is anticommutative:

$$(\mathbf{a} \times \mathbf{b}) \times \mathbf{c} = -\mathbf{c} \times (\mathbf{a} \times \mathbf{b}) = -(\mathbf{c} \cdot \mathbf{b})\mathbf{a} + (\mathbf{c} \cdot \mathbf{a})\mathbf{b}$$

3. The vector triple product satisfies: $\mathbf{a} \times (\mathbf{b} \times \mathbf{c}) + \mathbf{b} \times (\mathbf{c} \times \mathbf{a}) + \mathbf{c} \times (\mathbf{a} \times \mathbf{b}) = \mathbf{0}$ because: $a \times (b \times c) + b \times (c \times a) + c \times (a \times b) = (a \cdot b)c - (a \cdot c)b + (b \cdot c)a - (b \cdot a)c + (c \cdot a)b - (c \cdot b)a = (b \cdot c)a - (c \cdot b)a + (c \cdot a)b - (a \cdot c)b + (a \cdot b)c - (b \cdot a)c = (b \cdot c)a - (b \cdot c)a + (a \cdot c)b - (a \cdot c)b + (a \cdot b)c - (a \cdot b)c = 0$ which is the Jacobi identity for the cross product.

B.4 Quadruple Products

Looking beyond the triple products, there also exists a concept called the quadruple products. It is a product of four vectors in three-dimensional Euclidean space. The name "quadruple product" is used for two different products, the scalar-valued scalar quadruple product and the vector-valued vector quadruple product.

B.4.1. Scalar Quadruple Product

The scalar quadruple product is defined as the dot product of two cross products:

$$(a \times b) \cdot (c \times d)$$

where a, b, c, d are vectors in three-dimensional Euclidean space. It can be evaluated using the identity:

$$(a \times b) \cdot (c \times d) = (a \cdot c)(b \cdot d) - (a \cdot d)(b \cdot c)$$

or by using the determinant:

$$(\mathbf{a} \times \mathbf{b}) \cdot (\mathbf{c} \times \mathbf{d}) = \begin{vmatrix} \mathbf{a} \cdot \mathbf{c} & \mathbf{a} \cdot \mathbf{d} \\ \mathbf{b} \cdot \mathbf{c} & \mathbf{b} \cdot \mathbf{d} \end{vmatrix}.$$

B.4.2. Vector Quadruple Product

The vector quadruple product is defined as the cross product of two cross products:

$$(a \times b) \times (c \times d)$$

where a, b, c, d are vectors in three-dimensional Euclidean space. It can be evaluated using the identity:

$$(a \times b) \times (c \times d) = [a\ b\ d]c - [a\ b\ c]d$$

where $[a\ b\ c] = a \cdot (b \times c)$.

B.5 Conclusion:

In addition to their mathematical elegance, triple and quadruple products have numerous practical applications in various fields. Here are a few notable examples:

1. Physics and Mechanics: In physics, the scalar triple product helps calculate the work done by a force in moving an object, and the vector triple product is essential for determining torque and angular momentum. These concepts are fundamental in studying rotational motion, rigid bodies, and the behavior of physical systems.
2. Geometry and Graphics: In computer graphics, the vector triple product is used to calculate surface normals, which determine how light interacts with 3D objects, leading to realistic shading and rendering effects. In geometry, they help solve problems related to areas, volumes, and determining the relationships between vectors and shapes.
3. Electromagnetism: In electromagnetic field theory, the vector triple product is used to determine the direction and strength of magnetic fields generated by current-carrying wires or coils. This knowledge is vital for designing electric motors, transformers, and other electromagnetic devices.
4. Engineering and Robotics: In structural engineering, the scalar triple product helps determine the stability and equilibrium of structures, while the vector triple product is used to calculate moments and forces acting on various components. In robotics, these concepts are utilized for motion planning, kinematics, and controlling robot manipulators.
5. Fluid Dynamics: Triple products are used in fluid dynamics to analyze flow patterns and turbulence. They help calculate vorticity, which describes the rotation and circulation of fluid particles. Understanding vorticity is crucial for studying fluid behavior, such as the formation of eddies, flow separation, and the interaction between fluids and solid objects.

These are just a few examples of the wide-ranging applications of triple and quadruple products. Their utility extends to various scientific and engineering disciplines, allowing researchers, engineers, and scientists to analyze complex systems, solve problems, and gain deeper insights into the physical world.

In conclusion, the concept of triple products, including scalar and vector triple products, provides valuable mathematical tools for analyzing geometric relationships and solving problems in various fields. Additionally, the introduction of quadruple products expands our understanding of higher-dimensional spaces. Overall, triple and quadruple products offer elegant solutions and enhance problem-solving capabilities in mathematics and physics.

Bibliography:

1. https://www.cuemath.com/algebra/scalar-triple-product/
2. https://en.wikipedia.org/wiki/Triple_product
3. https://mathinsight.org/scalar_triple_product
4. https://mathworld.wolfram.com/topics/VectorAlgebra.html