SCHOOL OF ARTS
AND SCIENCES

Azim Premji University

MATHAAPU

NOVEMBER 2025

VOLUME 3

PATTERNS, PROOFS, PEDAGOGY

A COLLABORATION OF THE MATHEMATICS COMMUNITY AT AZIM PREMJI UNIVERSITY, BENGALURU

PREFACE

Mathematics is a subject that has always stood at the crossroads of imagination and reason. It is a discipline that highlights abstractions while grounding its conclusions in logic and proof.

Mathaapu is a collective effort by the students majoring in Mathematics and the faculty from the Mathematics Group of the School of Arts and Sciences, Azim Premji University, Bengaluru. Through our third issue of *Mathaapu*, we invite you to step into the beautiful world of Mathematics- where curiosity fuels minds and encourages discovery, and where every question opens the door to countless others.

This edition presents to you several interesting and thought provoking articles based on Mathematics and its many endeavors. These articles are written by our very own students and professors at Azim Premji University Bangalore. They are based on both theoretical concepts and real life experiences, highlighting the significance of the subject in all aspects of life. From dealing with technical aspects and pedagogical techniques of the subject to knowing about its roots from ancient times, this edition brings to you a wide range of intriguing topics to read about!

Whether you are an experienced mathematician or a curious learner, we hope you will find something in these pages that sparks your imagination. You may encounter elegant proofs that reveal the hidden complexities behind certain aspects, or articles that demonstrate how mathematical thinking contributes to other fields.

We welcome you to this journey of celebrating Mathematics!

CONTENTS

EDITORIAL

It is our pleasure to present the third edition of the Mathaapu magazine to you!

One of the defining commitments of Mathaapu, reaffirmed in every edition since its start, is the decision to place as few restrictions as possible on what may count as a mathematical article. This edition follows the very same principle allowing everything from application of mathematics in different fields to growing up with math and the challenges that accompany. With this edition I hope the readers are able to appreciate the nature and perseverance of math within our daily lives, in a profound way or not.

The variety of contributions to this edition illustrates that philosophy in action. In addition to articles that make connections to music, art, pedagogy, history, computation, and everyday experience, readers will come across articles that investigate mathematics through formal reasoning and visualization. From appreciating early contributions to intimate experiences that shaped our students' idea of mathematics.

Experimentation is also made possible by this openness. Alongside more traditional investigations of ideas and structures are articles that integrate mathematics with music, storytelling, origami, computation, or visual design. The idea that mathematical thinking is not limited to a single linguistic or cultural register is reinforced by contributions in multiple languages. When taken as a whole, these decisions indicate that mathematics is something that should be discussed, questioned, understood, and even reimagined in addition to being a problem.

The title ‘Proofs, Patterns and Pedagogy’ aptly encapsulates the types of articles you will encounter as you read this edition of the magazine. From the emergence of mathematical ideas and the recognition of patterns, to reflections on how mathematics is perceived, learned, and taught, the articles explore mathematics in many forms. Together, they show the subject as both rigorous and creative, shaped as much by reasoning as by intuition and experience.

"A mathematician, like a painter or a poet, is a maker of patterns," - G. H. Hardy. Mathematics is both creative and rigorous, based on proof but motivated by the understanding of form, symmetry, and structure. Despite being frequently linked to abstraction and purity, Hardy's work serves as a reminder that mathematical reasoning is inextricably linked to creativity and aesthetic judgment. This edition aims to highlight the interaction between proof and pattern, formal reasoning and intuitive insight, while pedagogy gives these concepts their enduring life through learning and communication.

So sit back, grab a cup of your favorite beverage and enjoy!

With Sincerity,
Anirudh N.Rao
Managing Editor

THE MATH BEHIND 5G

All information transmitted wirelessly, from a simple text message to a 4K video stream, travels as an electromagnetic wave, most commonly a radio wave. The simplest and most fundamental way to model this wave is with the sine function. A sine wave is a smooth, periodic oscillation described by the equation: $y(t) = A \sin(2\pi ft + \varphi)$

- **Amplitude (A)**: This is the wave's height or intensity. Visually, it's the distance from the center line to the peak of the wave.

- **Frequency (f)**: This is the number of complete cycles the wave makes per second. A higher frequency means the waves are packed more closely together.

- **Phase (φ)**: This refers to the starting position of the wave in its cycle. A phase shift slides the entire wave forward or backward in time without altering its amplitude or frequency.

By altering one or more of these properties, bits can be embedded onto a carrier wave.

The most elementary form of digital communication involves manipulating just one of these properties: the phase. This technique is known as Phase Shift Keying (PSK). In its most basic form, Binary Phase Shift Keying (BPSK), one section of the wave represents a single bit of information. For example, a standard sine wave could represent a binary '0', while an altered wave represents a '1'. (Figure 1)

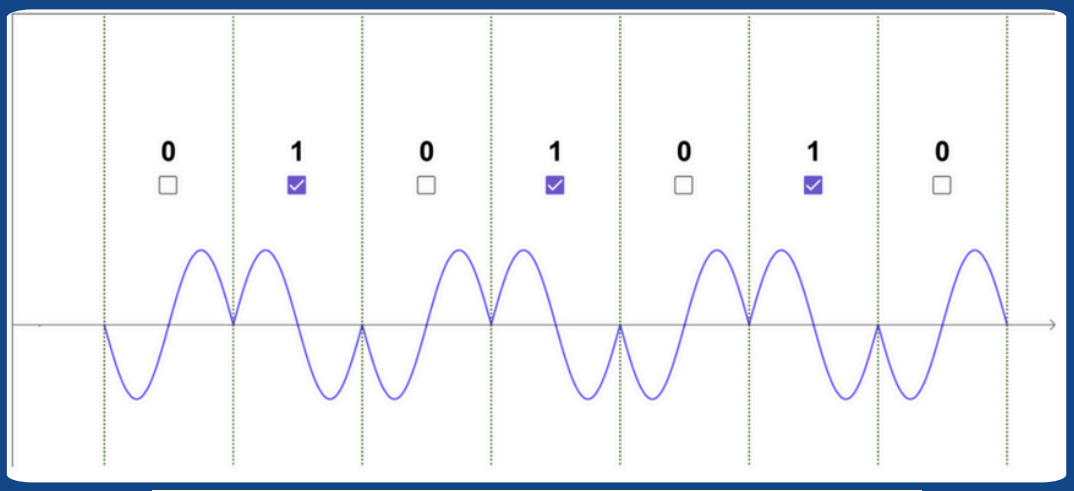


Figure 1. Standard Sine Wave

How is the wave altered? By "flipping" it. This flip is mathematically a phase shift of π radians (180 degrees), or half a wavelength. If the wave for '0' is represented by sin(x), the wave for '1' becomes sin(x+π), which is equivalent to -sin(x). This method allows for a clear distinction between a '0' and a '1'. (Figure 2)

For a larger amount of data to be sent without transmitting a greater amount of radio waves, Quadrature Phase Shift Keying (QPSK) was used in early iterations of mobile phones. Instead of just two possible phase states (0 and 180 degrees), QPSK uses four: 0, 90, 180, and 270 degrees. Since there are now four distinct states, each state can represent two bits of information (e.g. 00, 01, 10, 11).

By doubling the number of phase shifts, QPSK instantly doubled the amount of information that could be sent over the same period, without needing more of the radio spectrum.

To further increase the amount of data that devices can be capable of transmitting, the other properties of the sine wave need to be altered. This is where Quadrature Amplitude Modulation(QAM) comes in.

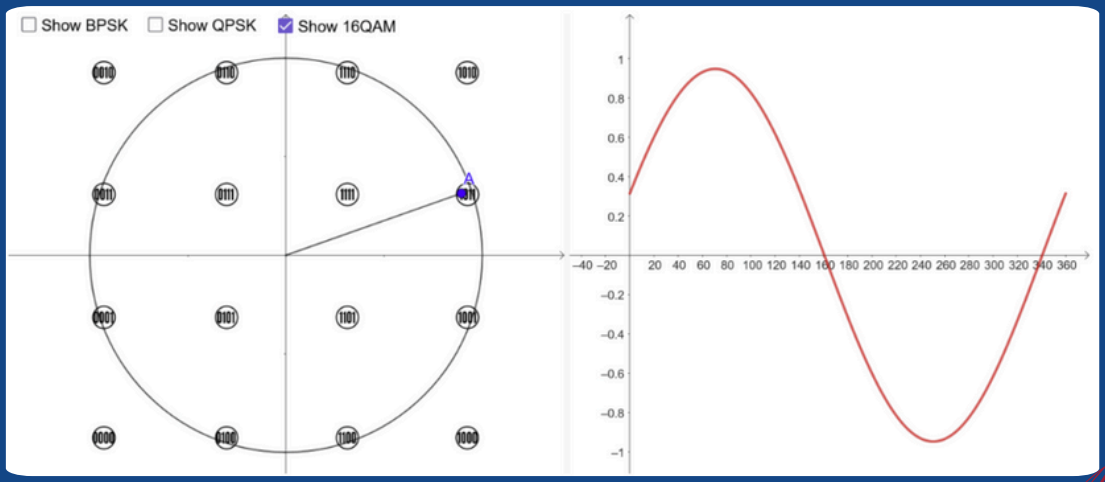
In a QAM system, each unique combination of a specific phase and a specific amplitude level represents a different multi-bit code word. For example, in a **16-QAM**, there are 16 unique symbols. Since $2^4 = 16$, each symbol can represent four bits of data. This is a fourfold increase in data density compared to BPSK.

The most intuitive way to visualize this is with a **constellation diagram** (Figure 3). This diagram is a 2D plot where the angle from the origin represents the phase shift and the distance from the origin represents the amplitude.

- In BPSK, the diagram is just two points on a line.
- In QPSK, it's four points, typically in a diamond or square shape.
- In 16-QAM, it's a grid of 16 distinct points.

Figure 2.Distinction between '0' and '1'

Figure 3. Constellation diagram



The goal is to generate a signal that corresponds precisely to one of these points. The receiver, which knows this "map," can then decode the received signal back into the original four bits it represents.

In an ideal world, the signal received would land exactly on a constellation point. However, the real world is filled with noise and interference from other devices, physical obstacles, and atmospheric effects. This noise can slightly alter the signal's phase and amplitude, causing the received point to be slightly off its target on the constellation diagram.

This is where the geometric nature of the diagram becomes crucial for robust communication. The receiver is programmed to make a "best guess." When it receives a signal that is slightly misaligned, it simply matches it to the closest valid constellation point. This decision-making process allows the system to correct for minor errors, ensuring that the data is interpreted correctly even in noisy environments.

Modern 5G systems push this concept to its limits, employing 64-QAM(6 bits per symbol) and even 256-QAM (8 bits per symbol). While the grids in these higher-order schemes are much denser, making them more susceptible to noise, advanced error-correction algorithms work alongside these mathematical principles to ensure reliability. The journey from a simple wave flip to a complex 256-point grid is a testament to how clever mathematics enables us to encode and transmit information with ever-increasing density and speed, forming the invisible backbone of our connected world.

Written by - ANIRUDDH RAGHAVAN

FROM COLOR TO CODE

HOW ELLIPTIC CURVES KEEP MESSAGES SAFE

"Messages and calls are end-to-end encrypted. Only people in this chat can read, listen to, or share them. Learn more."

Have you ever noticed this on WhatsApp? Have you ever wondered how end-to-end encryption works or how it ensures that only people within the chat have access to the conversation in the chat? WhatsApp uses something called elliptic curve cryptography, specifically the Curve25519 elliptic curve for end-to-end encryption. The signal protocol, which powers WhatsApp's encryption, uses this curve to facilitate secure key exchanges and message encryption (The signal protocol is a system that keeps messages private).

In the current data driven world where everything is digitized or is in the process of being digitized, digital security is the building block of trust, privacy and protection. To be digitally secure ensures that data remains untampered with, is confidential and accurate which enables people to use the data securely.

Cryptography: Foundations

Cryptography is a science that uses mathematical methods to protect data by transforming it into unreadable format so that only authorized persons are able to access it.

It ensures confidentiality, integrity and authentication of information during storage or communication between two or more parties. There are two primary types of cryptography- symmetric key(secret key) cryptography and asymmetric key(public key) cryptography. Symmetric key cryptography employs the same key for decryption and encryption whereas asymmetric key cryptography employs two unique but related keys for decryption and encryption.

Elliptic curve cryptography (ECC) is a type of modern asymmetric key cryptography which stems from the mathematical properties of elliptic curves over finite fields. A finite field is a set of numbers that can be added, subtracted, multiplied and divided (except by 0) whose results stay in the set. It is presently considered as one of the most efficient and secure systems of cryptography. Elliptic Curve Cryptography works on the challenging problem of the Elliptic Curve Discrete Logarithm Problem (ECDLP). ECC is relevant and important in today's world as it provides stronger security with smaller keys, performs efficiently, requires less memory and fewer transistors saving energy and power and is resilient against known attacks. Thus, Elliptic Curve

Cryptography offers powerful, efficient and secure encryption for modern systems due to its mathematical complexity.

Symmetric and asymmetric cryptography are two basic methods of securing digital communication, differentiated mainly by the way they employ encryption keys. Symmetric cryptography uses the same key for both encryption and decryption. This is fast and efficient, and it's well suited to encrypting huge amounts of data. But it demands that the two communicating parties securely exchange the key beforehand, which adds a potential security vulnerability if the key is intercepted. Early cryptographic systems worked on symmetric or public key algorithms.

Asymmetric cryptography, on the other hand, employs a pair of keys: an encryption public key and a decryption private key. The public key may be distributed freely, obviating the need for a secure channel to transfer keys. This is particularly valuable for digital signatures and secure key exchange, although it is typically slower and more demanding than symmetric techniques. In practice, asymmetric encryption is typically employed to set up a secure connection, following which a symmetric key is transferred and utilized for the rest of the communication. Examples include AES and DES for symmetric encryption, and RSA and ECC (Elliptic Curve Cryptography) for asymmetric encryption.

Why Elliptic Curve Cryptography?

Traditional systems such as RSA, are growing obsolete for several limitations. The most prominently noted of which is the necessity for RSA to use very large key sizes to enjoy robust security, thereby imposing a higher computational need, memory requirements, and high energy expenditure. For example, RSA requires a 3072-bit key to have the same level of security offered by only a 256-bit ECC key, which renders RSA less practical to use on new devices such as smartphones and Internet of Things (IoT) technologies.

On the other hand, ECC provides robust security with shorter keys, which makes it more scalable and more suitable to the minimum recommended 112-bit security level. Additionally, with the emerging threat of quantum computing, RSA and other such algorithms are deemed insecure, while ECC is seen as more secure and as a stepping stone towards post-quantum cryptographic solutions. Consequently, the NIST handbook suggests implementing ECC as a safer, more efficient, and forward looking crypto standard.

But why are key sizes so important? A key size determines to a great extent the security of a system. Key size is the number of bits that is used to generate the key, and the larger the number of bits, the

more combinations are possible—difficult for attackers to guess the key. For example, a 128-bit key employed in symmetric encryption (such as AES) provides robust protection, whereas asymmetric systems (such as RSA) require very large keys—such as 3072 bits—to establish similar safety.

National Institute of Science and Technology, USA (NIST) describes that as technology advances and becomes faster and more powerful, particularly with the potential in the future for quantum computers, smaller keys may no longer be secure. Therefore, selecting the appropriate key size is crucial, particularly if information to be safeguarded must remain private for years to come.

Cryptography is the science of hiding and verifying mainly digital information. It uses mathematical methods for exchange of information even over non secure channels. The primary goals of cryptography include confidentiality of data, maintaining integrity and accuracy of data, authentication and non-repudiation of data.

Mathematical Basis of ECC

Elliptic Curve Cryptography (ECC) is a modern and efficient method of public key cryptography that draws on the mathematics of elliptic curves over finite fields. Described independently by Neal Koblitz (professor of Mathematics) and Victor Miller (Mathematician) in 1985, ECC constructed cryptographic systems based on the set of points on an elliptic curve with certain algebraic properties. Points constitute what is known as an abelian group, supporting secure processes such as key generation, digital signatures, and encryption. An abelian group is a mathematical structure where elements can be added and the result would still belong to the group. In case of elliptic curves, there exists an element called O, which has an inverse, is reversible and follows commutative rules- much like regular addition but defined on points of a curve.

Mathematically, an elliptic curve is defined by an equation of the form:

$y^2 = x^3 + Ax + B$

with the condition, $4A^3 + 27B^2 \neq 0$ which ensures the curve is smooth and free of sharp corners. A and B are curve parameters which define the shape and properties of the curve. In cryptography, operations are performed using the addition of points on the curve, and the security of ECC relies on a difficult problem known as the Elliptic Curve Discrete Logarithm Problem – given two points P and $Q = kP$, it is computationally infeasible to determine the integer k.

Watercolor Analogy

Watercolors are an interesting medium of paint as every time one paints on an already existing paint

using the same color, the output color slightly changes and hence produces a different shade. So, if one repaints one part of the painting using the same color multiple times, the end output shows a new color. This however cannot be reversed. If I paint over twice, a slightly different color is formed but if I paint over the same area 100 times, one cannot predict what color would be the final output. Anyone who sees the painting will be able to see the final color but not be able to tell how many times I have painted over the same thing to achieve that particular shade of color. If in a large group, my friend and I want to share a common color without anyone else being able to understand how we arrived at the same shade without prior discussion, we can do it by picking a random number each.

Let's see how this works. Let's assume that I pick the number 6 and my friend picks the number 10. Let us also assume that I pick the color blue and my friends pick the color yellow. I paint blue over my canvas 6 times while my friend paints yellow 10 times over their canvas. The final output after the paint has dried will be called our 'public' color. This is because everyone can see the final output but not the numbers that have led to the respective results. To share the same color with my friend, we exchange our canvases. My friend paints their yellow color over my blue canvas 10 times, while I paint yellow over their blue canvas 6 times. The final result on both canvases ends up being the same color. This is exactly how the concept of elliptic curve cryptography works.

This watercolor analogy is the explanation to how elliptic curve key exchange takes place. The secret numbers chosen by my friend and I denote our respective private keys. The public color refers to the public key and the common final result denotes the secret key. Even if everyone knows the public key, it is practically impossible to determine what the exact required private keys were in order to arrive at the final result. This analogy also demonstrates why the system of elliptic curve cryptography is secure.

Watercolor analogy for Key Exchange

In the watercolor analogy, the repeated painting on the canvas is similar to applying a private key on a public base value. As each individual in the analogy paints their canvas a certain number of times with their color, in ECC, each user multiplies a base point on the elliptic curve by their private key to get a public key.

Here is how it corresponds to actual elliptic curve cryptography operations:

- The underlying color (blue/yellow) symbolizes the public point (G) on the elliptic

curve which is publicly shared.

- The number of times one paints over their color denotes a private key (a or b) which is an arbitrarily selected number that remains a secret.

- The resulting public hue is analogous to calculating aG or bG which is disclosed publicly.

- When canvases are swapped and painted over again, it is the same as:

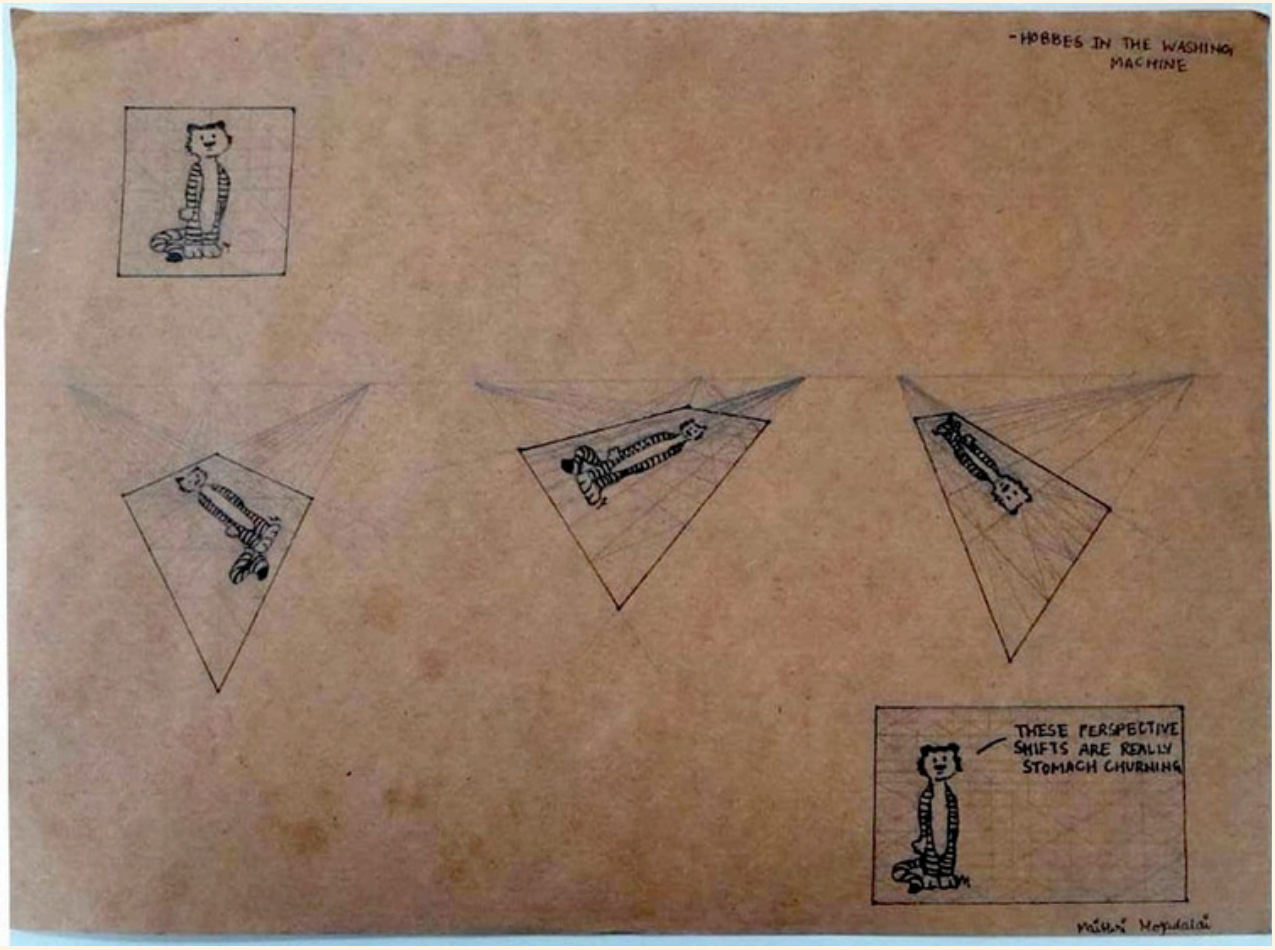
- One user calculating abG and the other calculating baG.
- Algebraically, both calculate the same common key abG, though they used different orders and keys.

Just as it is difficult for anyone seeing the last color to tell how many layers of paint were applied, in ECC, even if an attacker knows the public key, it is extremely hard to figure out the private key with which it was created. This is because it is hard due to the Elliptic Curve Discrete Logarithm Problem (ECDLP), which is computationally infeasible to invert. Although the watercolor analogy is a simplification for intuitive reasons, the strength of ECC is fields of mathematics like abstract algebra and number theory where the operations are carried out using points on curves in finite fields.

Conclusion

As the world gets increasingly interconnected and data-centric, secure communication has never been more crucial. From messaging apps to digital payments and Internet-of-Things (IoT) devices, data integrity and privacy are pillars of modern digital life. Elliptic Curve Cryptography (ECC) is a mathematically elegant and highly efficient cryptographic technique. By offering robust security with smaller keys, ECC meets the demands of today's high-performance, lightweight digital systems while being immune to new threats. As we continue toward a quantum computing and expanding digital ecosystem world, ECC continues to be a cornerstone in pursuit of smarter and more secure communication.

Written by - CHAITANYASRI KOKUL



Calvin and Hobbes: Perspective Shifts - A Comic

THE RISE OF THE MEDICI

In the mid-1300s, a man named Giovanni di Bicci de' Medici, who came from a family of doctors - who, while certainly not poor, were not from noble lineage - migrated to Florence, Italy. His family later became one of the most influential and powerful families in Italy. Within the span of 100 years, the Medici transformed Florence. Among other things, they were avid patrons of the arts and sciences, supporting some of the most celebrated artists and thinkers of the Renaissance, such as Michelangelo and Galileo. The Medici Bank, founded in 1367, gained enormous success and introduced important banking inventions that are still used today. In a short period of time, the Medici rose to power and wealth through strategic wielding of clever alliances. Thus, this family has been studied avidly not only by historians but also by mathematicians, whose curiosity was ignited in the 1990s by two political scientists.

"Robust Action and the Rise of the Medici, 1400-1434", by Padgett and Ansell, was a landmark article that used mathematics, specifically a field called social network theory, to analyze a network of Florence's powerful families and understand the Medici's rise to power.

Social network analysis utilizes graph theory to help model and understand networks of people. A network is usually represented by a graph, which is a collection of points called nodes, and lines connecting them, which are called edges. The image below (Figure 1) shows a network representing fifteen of Florence's most powerful families at the time.

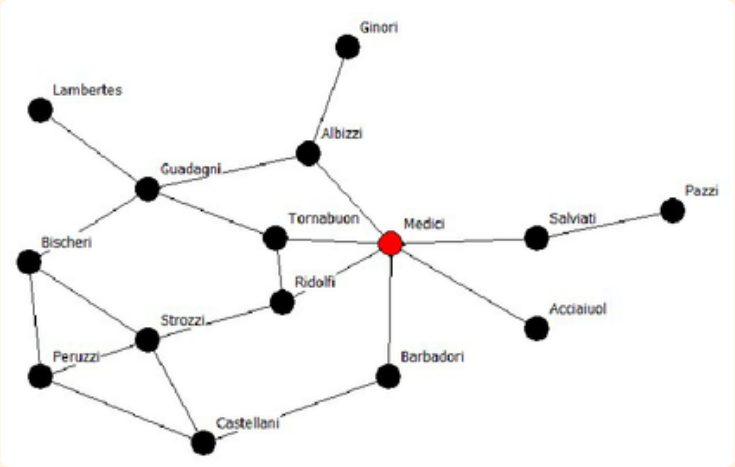


Figure 1. A network representing Florence's powerful families in the 15th century

In this graph (Figure 1), each node represents a family, and each edge represents a marital alliance- that is, two families have an edge connecting them if there has been a marriage between them. The Medici are colored in red for convenience.

We would now like to quantify the idea that the Medici were 'central' in this network due to their strategic alliances, which is formally known as measuring centrality.

One way we would discern who is most influential or central is by seeing who has the most alliances. The number of alliances a family has, that is, the number of other families they are connected to, is called the degree of a family. The degree of a node is the number of other nodes it is connected with. For example, the Strozzi family has a degree of 4 (Figure 2). Using this measure, we find that the Medici are connected to the most families (degree 6). However, degree centrality measures only connectedness and may miss out on other aspects of influence.

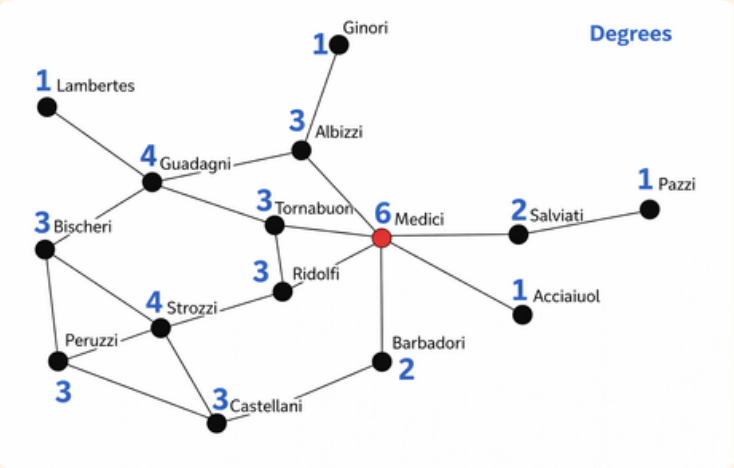


Figure 2. Degree centrality of a network representing Florence's powerful families in the 15th century

A neighbor of any node is another node that is directly connected to it. For example, Castellani is Barbadori's neighbor, but Ridolfi is not.

Eigenvector centrality is a more complex measure of centrality that gives importance to how well connected your neighbors are, over how many people you're connected to. For example, both the Pazzi and Acciaiuoli families have the same degree centrality, meaning they are only connected to one family. However, the Acciaiuoli can be considered more central because their neighbor, the Medici, is well connected, whereas the Pazzi's neighbor, Salviati, is less connected. Thus, Acciaiuoli may be able to exert influence through their neighbor, the Medici, while the Pazzi may have less influence.

Eigenvector centrality uses a weighted formula (whose details I will not go into detail here) that takes into consideration both the connectedness of the node and the connectedness of its neighbors. While calculating the eigenvector centrality, the Medici still remains to be the most central family.

As we have established, connections hold a lot of power; being in between other connections gives quite a lot of leverage. If two families are not directly connected by an edge, there exists a shortest path in the network through which families are connected. For example, in Figure 3, the shortest path between the Peruzzi and the Ridolfi is through the Strozzi. In some cases, there can be more than one shortest path.

The betweenness centrality of a node is the number of shortest paths that pass through that node. A node has the highest betweenness centrality if many of the shortest paths pass through it. Once again, the Medici, is the most central

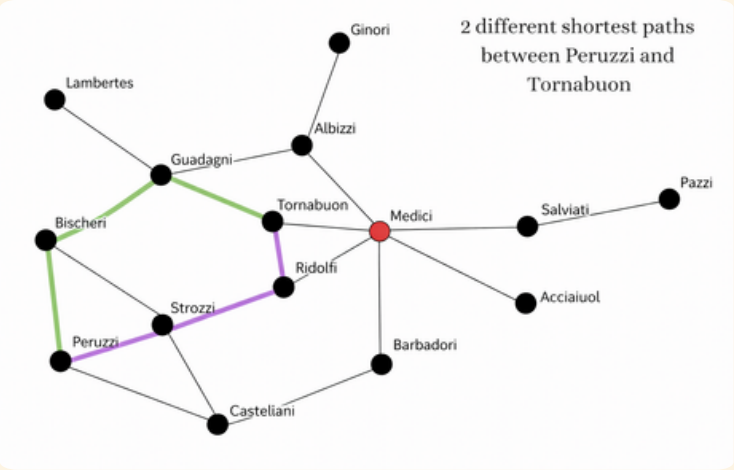


Figure 3. Two different shortest paths between Peruzzi and Tornabuon

family and holds power by acting as the bridge for many connections.

The farness of a node is the average distance of the shortest path from that node to other nodes. Closeness is the reciprocal of farness, and it measures how "close" a family is to the other families in the network.

Once again, we see that the Medici has a very low distance to the other families and can reach any given family in a distance of three, while other nodes, like the Pazzi, are very far from the network.

By exploring different measures of centrality, we see that the Medici are truly central to the network. They were connected to many families directly, played an important role as an intermediary in other families' indirect connections, and had the most efficient reach to all other nodes. This undoubtedly played a very important in their rise to power, as the centrality in the network comes with a lot of power.

While this may seem irrelevant and outdated to some, it stood out to me because of the simplicity in which it demonstrates something larger, the power of connections. Social network theory is used today to understand and predict human relationships and plays an important role in social media algorithms. It also helps to model and study the spread of diseases, which was widely used during the COVID-19 pandemic.

This article has only touched upon a vast field that is still largely unknown, but I hope this provides a tiny spark in you to read up more about it.

I also hope that through this, we can appreciate that the rise of the Medici was not merely a fascinating historical event, but also a timeless testament to the power of connections.

Written by - INIYA A

MATHEMATICS - ITS APPLICABILITY, VALUE, AND OUR PERCEPTION OF BOTH

For young Mathematicians entering the field, it may be difficult to see beyond their understanding and love for the Mathematics they know. On one hand, it is good to take one's time exploring, reaching self-discoveries and coming up with opinions, but at times we fail to see the conditioning that we have received and the preconceived notions that we have. Often, the underlying motive to do Mathematics is application-based. In this process, we lose track of how beautiful Math can actually be. There are many aspects to what makes good Mathematics, apart from the ones which we are unconsciously motivated by. In this day and age, it is increasingly becoming a fashion to be aware of what one already likes, and know one's specialisation. People are quick to dismiss a subject, branch, or topic based on biases and assumptions. Some people decide to do math which has gained popularity at the moment; one might compare this to fast fashion (which we often see in clothes). But not a lot of people stop to think about the field (nascent or not) and where it is going to be. So it is important to find and remind ourselves what Mathematics truly is, and what might be the "correct" way to take an approach to our work as academics.

Philosopher Isaac Berlin first suggested that we can think about two contrasting cognitive styles, and he used an ancient Greek proverb to describe this idea. This was later referenced by Terrence Tao in his essay, "What makes good Mathematics". According to this, one thing to note is that there can be two types of Mathematicians: the hedgehogs, those who are highly knowledgeable in one field of Mathematics and the other ones are foxes, who know a little about everything. Collaborations between hedgehogs and foxes always tend to result in very good collaborations. One must note that a Mathematician can always switch between being a hedgehog and a fox. Sometimes in a collaboration, one might be a hedgehog, specialising in the field, and in other instances, the same Mathematician might be a fox. Something which is also important to understand and plays a difference in the way we understand hedgehogs and foxes is that people have very different ways of understanding particular pieces of Mathematics. Two Mathematicians who have different branches of Mathematics backgrounds will have vastly different understandings of the same concept.

Trefethen, in his essay - An applied Mathematician's apology, highlights the importance given to certain branches of Mathematics

over the others. He talks about the Math that most field medalists have done (which is mostly what is considered to be "pure" Math), and the relevance it has to the Mathematics he does. Numerical analysis, something he works on and places under the umbrella of Mathematics, is too mathematical to be called Computer Science, and too programming-based for Mathematics. He talks about this dilemma, where he doesn't know how to put across the importance of this field. However, one thing which makes itself clear from this essay is the seeming need to prioritise one branch over the other. He argues that although the Math which promises to have relevance 10 years down the lane should be given importance, it is also just as crucial to recognise the work which is relevant and essential for the current time. From this, it is also clear that some Mathematics cannot be specifically put into categories, or require very specific conditions, which are redundant. This is important to keep in mind when talking of hedgehogs and foxes, for it also shows that sometimes, being a hedgehog requires us to be a fox.

Therefore, it is safe to say that we need to widen our perception of Math, because this will enable us to not only improve our level of Mathematics (in all senses of the word), but also allow us to spread the "joy of Math" as one may call it. Because of the sheer depth and dimensionality of math, and the unpredictable and adaptive nature of its evolution gives rise to many qualities. Each of the qualities offers a different motive and approach to Mathematics. Mathematicians may be better suited to certain tasks and more comfortable with certain specific underlying motives than others. This diversity is good for Mathematics as a whole. It provides a healthy balance and restricts Mathematics from becoming increasingly ad hoc or convoluted (Tao, 2007). We cannot also say that all motives of Mathematics have equal importance, doing so will sap Mathematics of its sense of direction.

Focusing on a particular quality, something we will refer to as "local" quality, can be unnecessary when done in excess. For example, if one focuses on writing as concise a proof as possible. It may result in an opaque and rigid two-line proof, which has lost all its joy and beauty.

Therefore, it is important to not only be focused on local qualities but also on global qualities and how it fits into the bigger mathematical picture. Everything in Math has equal and great potential.

"Empirical ideas are necessary to conserve the freshness and vitality of Mathematics, and this will remain equally true in the future." -John von Neumann (von Neumann, 1947)

Parallelly, one might wonder whether we can have Math with no inherent application? Is it possible for "pure Math" (Mathematics which is believed to be purely theoretical and not have any practical value) to actually exist? If Mathematics is a language, and we use it to describe the world as we see and understand it, then doesn't that imply that math, no matter which branch, will always have an application?

What Mathematicians find intellectually interesting turns into something having value in the physical world. This is illustrated in many instances. One notable example is the life and work of the Mathematician G.H. Hardy. He authored the essay "A Mathematician's Apology", wherein he apologises for the work he has done. He believed that all the work he had done was for purely selfish reasons, and thought none of his work was useful, and that his research did not contribute anything to society. Funnily, all the work he has done is now being used, all of it having a practical purpose. Recently, concepts in topology, which is considered a "pure Math" branch, have been used in creating algorithms, problem-solving and statistics. And so, it is certainly safe to conclude that any Mathematics is useful and important.

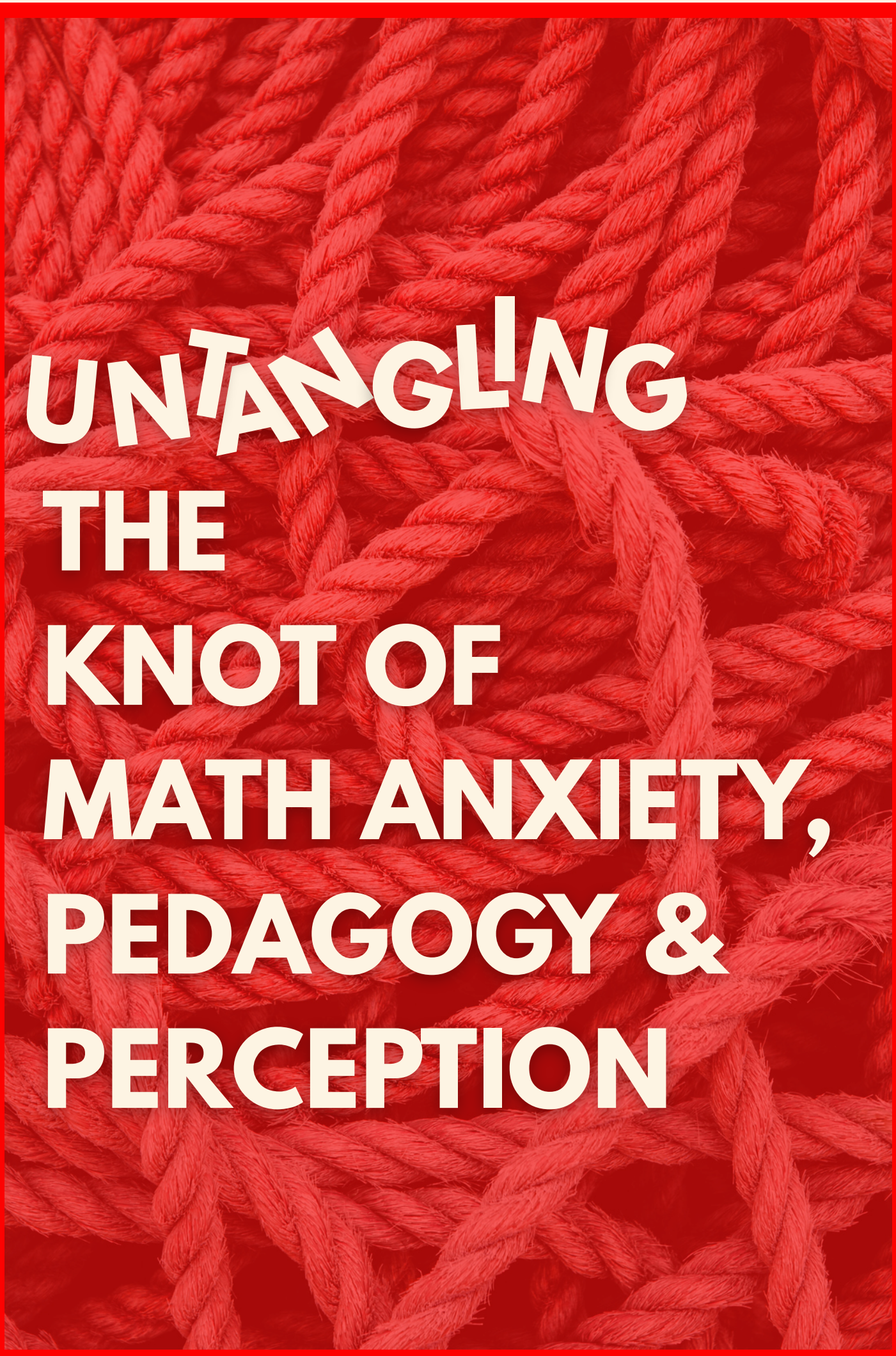
Wigner, in his essay, The Unreasonable Effectiveness of Mathematics concludes with the words "We should be grateful for it and hope that it will remain valid in future research and that it will extend, for better or for worse, to our pleasure, even though perhaps also to our bafflement, to wide branches of learning." This instance highlights the fact that Mathematics is, in a sense, the language with which we describe the world. It prevails in any and every field in the known world. Recently, there have been huge leaps in the research of molecular structures using mathematical techniques, leading to the emergence of a new field called Molecular Topology. Biology is a field which most people expect that Math will not penetrate. In recent years, this notion has been disproved. Hence, any Mathematics, whether "pure" or "applied" or something that cannot be comfortably put into either category, is "usable" in some sense.

Bill Thurston explores very relevant and important questions in his essay "On Proof and Progress in Mathematics". He explores the question of what it is that Mathematicians accomplish, where he says that "In other words, as Mathematics advances, we incorporate it into our thinking. As our thinking becomes more sophisticated, we generate new mathematical concepts and new mathematical structures: the subject matter of Mathematics changes to reflect how we think." This is a really interesting and insightful way to think about

Mathematics. It provides us with a comfortable way of thinking about Mathematics not only as a field, but also as a language. Our basic ideas become our alphabets, making all Math useful. One cannot say that certain words of a given language are useless, in the same way that certain sentences (results of Mathematics) cannot be called useless.

One essential takeaway is that we should always do Math with the intent of looking at the global qualities. Getting caught up in the fine print might result in the field losing its charm. Hedgehogs and foxes will only take you so far; there might even be instances where you cannot make distinctions between the two, simply because of the structure of the specific branch. There should be a good balance between specialising in a branch and being adequately educated in the others. That is, we need to remind ourselves that both the local and the global qualities are important. And although doing this is important, one does not always have to think about the greater implications. What I mean by this is that Mathematicians should have certain motives, but they should not be completely controlled by these motives. Many times, exceptional Mathematics can arise from work that was done without any particular intent. Mathematics, however theoretical and impractical it may seem, always has some sort of application. Although the math we do does not always have to be motivated by finding applications, it is almost a given that it is useful one way or the other. Many people look at the "scope" of a field before entering, and although one might not be able to lead an extravagant life on a Mathematician's salary, it is absolutely fair to conclude that the satisfaction of our work makes up for the other fallacies of life. I personally believe that if someone wishes to enter academia (in the context of Mathematics, especially), they should not only look at the applicability of the work they do. Sometimes it is best to simply work for the joy of the work one does, and in this process, any work which is done sincerely and devotedly is bound to have some greater meaning.

Written by - MAITHRI MOGADALAI


UNTANGLING
THE
KNOT OF
MATH ANXIETY,
PEDAGOGY &
PERCEPTION

What is it that makes Math different from other subjects? What makes students fear Mathematics? This fear and widespread dislike of Mathematics is not a natural state of affairs. It is a symptom caused by a complex interplay of deeper issues: a misunderstood subject, flawed teaching methods, a crowded curriculum, and a toxic societal narrative.

In this piece, we will try to untangle 5 core problems that make Math a complicated subject to both teach and learn and discuss some solutions for the same.

Nature and language of the subject:

Mathematics is undeniably very different when compared to other subjects in terms of language and real-life relevance. How so? Unlike in subjects like Social Science or Natural Sciences, the connection between Mathematics and real life often cannot be seen immediately. This leads to students questioning the relevance of the subject itself. This is because we confuse lack of visibility with absence; For example, students may not understand the purpose of learning LCM and HCF, but it later helps with fractions, which is quite useful in daily life. The cumulative nature of Math also makes it tricky; If you don't understand trigonometry, you will struggle with differentiation, and if you don't understand differentiation, you will struggle with integration, and so on. Many students find it difficult to go from the abstract 2+3=5 to a word problem, essentially asking to do the same. This is where language comes in, and for many students, it's tough to figure out what operations need to be used to solve a word problem. For example, Ria has 7 apples, and Sonu has 3 apples. How many more apples does Ria have? In this question, students may think that since the word "more" is there, they need to add, but that is wrong.

Problems with pedagogy and teachers' beliefs:

Many teachers believe that teaching Mathematics is possible through only the lecture method. This, however, encourages only one-way flow of information. They teach the students one method of doing a question and follow the same method for other such questions to get the "right answer". The focus is on the answer rather than the reasoning behind it. This kills the creativity of the subject, which makes students feel like a function whose job is just to produce the answer using a single formula. A teacher's lack of content knowledge can also discourage students from coming up with different methods, as the teacher themselves would not be sure if it is correct. Math classes are exam-centric (focusing on what is important for "board exams") rather than student-centric (letting them figure out the solution with some help and encouraging new approaches). This doesn't properly serve the purpose

of making students rational, autonomous individuals.

Curriculum and assessment:

The curriculum immensely focuses on the “what” and does not include the “how” as much. By this time, we should be clear with the fact that what makes Mathematics interesting is its nature of approaching a solution through different ways using appropriate reasoning.

The curriculum misses this point, which makes the subject very monotonous and mechanical. Different students may understand a concept in a different way, but to score, they must stick to one method, which makes it difficult for them to understand the concept. Examination has become the sole purpose of studying, which makes it compulsory for teachers to complete the syllabus within a given period of time. Due to this, they don’t have the time to let students discuss, discover and explore.

Curriculums are often overloaded with topics, forcing teachers to rush through content. This prioritises coverage over mastery. Students get a superficial exposure to many concepts but never have the time to develop a deep understanding of any of them. This is why students often forget everything after an exam.

Society’s views on Mathematics:

“Not being good at math = not being smart enough”.

This subject shoulders the heavy load of being a measure of the students' overall capabilities according to society. Children learn around 5 subjects, but we don’t easily hear someone say “He is not that sharp since he always scores less in Social Science”; But, it is apparently okay to say this for Mathematics. As there is a large hype for engineering in India, most parents want their children to be good at Math even if they lag in other subjects a little.

All this creates a great deal of pressure on the child, because if they don’t score well, they will be labelled as “dumb” or “thick-headed”. A subject which is difficult and is forced upon them will make them resent it, and thus they will not be able to perform well in that.

While these problems are daunting, they are not insurmountable. Addressing them requires a shift in mindset from performance to understanding, from speed to depth, and from fear to curiosity.

We need to make classrooms more student-centric, where the focus is not on teaching Math, but teaching the students Mathematics (I would recommend you read that line again). The focus should be shifted from getting the answer to the reasoning behind it and inculcating mathematical thinking in students.

There are many ways of doing this in an actual classroom, like to understand a new concept rather than directly explaining it at the beginning. This can be done by means of a group activity or discussion guided by questions that would lead students to the answer.

For example, give students a piece of paper in the shape of a parallelogram, and ask them to cut it into 2 parts such that at least one of the parts is a triangle, and let them figure out the relation between rectangles, parallelograms and triangles.

This sounds good, but it may not be possible for all concepts. For those cases, try to connect the concept to something they would have already studied, and while solving problems, fish for different approaches to the same problem. For example, to teach exponents, a teacher can relate to the idea that just like multiplication is repeated addition, exponents are repeated multiplication. If the students need to find the area of the parallelogram, ask for different ways of doing so (area of 2 triangles, area of a small triangle and a rectangle etc.), rather than just stopping as soon as one of the students gives the correct answer.

In such a classroom, the teacher's job is to facilitate students' learning rather than just passing information. Questions like "Why did you choose that method?", "Can you explain that another way?" and "Does that always work?" should be asked. Teachers need to be very patient and give wait time (wait time - a short gap after asking a question for the students to process the question and think of the answer) whenever they ask a question. Preferably, none of the students should answer immediately after a question is asked, even though they want to, so that all the students can independently think without being influenced by any one answer.

Do these cover all the solutions? Absolutely not. There are many other ways to help students get comfortable with the subject and explore the wonders of Mathematics. By embracing these practices, teachers can transform their classrooms into vibrant workshops where fear is replaced by curiosity, and Mathematics is not a barrier to overcome, but a language to be discovered.

Written by - MANYA

INDIAN MATHEMATICS

AN EARLY CONTRIBUTION TO MATH AND SCIENCES

Worldwide, Indians are known to be good at Mathematics. This is the land which gave the foundational concepts like zero, infinity, and representing numbers in terms of their place value, later known as the Hindu-Arabic numbers. Mathematics is a subject disliked by many, but it is one of the only tools (along with language) which is used in most of the fields, from grammar - Paanini's Ashtadhyayi, engineering - may it be modern software or Sthapatya Veda, or may it be dance - Natyashastra, we all use Mathematics.

In Al-Khwarizmi's work, a 9th century Persian Mathematician, particularly his treatise "Kitab al-jabr wa'l-muqabala" (The Compendious Book on Calculation by Completion and Balancing), acknowledged the contributions of Indian Mathematicians, including the Hindu numeral system. The same Mathematics and the methodology of solving that he quotes to that learnt by Indian texts, later in time, when translated into European languages, were known as 'Algebra' and 'Algorithms' after his name and the Hindu numeral system was known as Hindu-Arabic numerals.

Indians were one of the first pioneers of Mathematics. One of the early texts which included Maths was the four Shulva sutras, shulva meaning thread and sutras are concise formulas or rules. This text talks about Vedic fire rituals, and it also includes mathematical formulas and values of constants. The Shulva sutra written by Baudhayana includes Pythagorean theorem (*not Pythagoras theorem) and irrational constants like the value of pi and √2 and more.

Later in time came astronomical texts, which included mathematical concepts like geometry, plane trigonometry, spherical trigonometry, both plane and spherical coordinate systems, sequences and calculus.

There were also texts which only constituted Mathematics, like "Lilavati" written by Bhaskaracharya. In this book, he explains methods of finding squares, square roots, cubes, cube roots, combinatorics, series, eight rules concerning zero and many more.

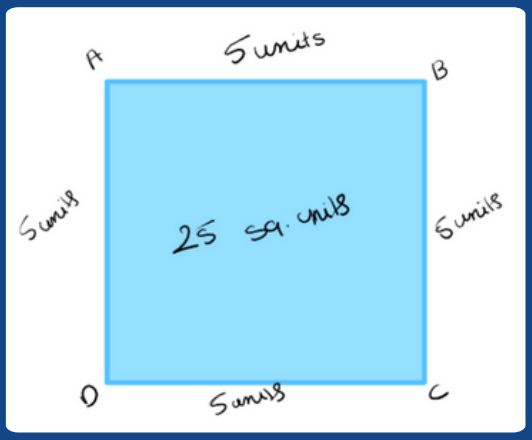
Now, this was all beautiful to state the contributions by Indians in the field of Mathematics. But I can also assure you that it will be more fun when we dive into some problems from these texts. Like, finding the value of root 2 from Baudhayana's Shulva sutras and a problem proposed by Bhaskaracharya on combinatorics.

Value of √2

As mentioned earlier, the Shulva sutras are ritual texts on fire-altar constructions using geometrical concepts. There are four Shulva sutras written respectively for the four Vedas. Baudhayana's Shulva sutra being the oldest, followed by Apastamba, Manava and Katyayana. As India mainly transferred knowledge based on oral tradition, it is hard to date when these were composed, but they were possibly written around 800 BC - 500 BC.

The value of the root 2 in Baudhayana's Shulva sutra is given in the second chapter, "Transformations of Geometric Figures", 12th sutra. But before understanding the method, let us revisit some basics.

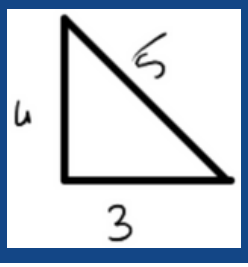
Let's say we have a square ABCD of area 25 square units. Now the length of each side of the square ABCD is 5 units.

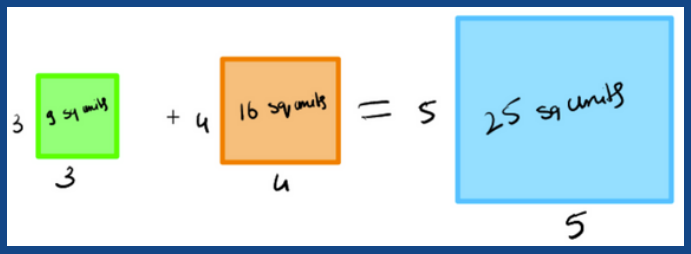


We know the formula of the area of a square of side a is a^2, therefore if the length of each side of the square is 3, then the area would be $3^2 = 9$.

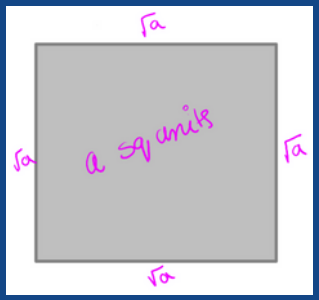
One more example, if each length of the square is 4, then the area of the square is 4^2, that is 16.

Also, in a right-angled triangle, the square of the longest side, which is the hypotenuse, is equal to the sum of the squares of the other two sides. This formula is also covered in the 2nd chapter of his book. For example, $3^2 + 4^2 = 5^2$.





If the value of the area of square is given to be a, then the sides of the square will be √a.



So if we have a square of area 2, then the length of each side of the square will be the square root of that area, that is √2. But we know √2 is an irrational number that is non-terminating, meaning the digits after the decimal never ends and non-recurring, meaning the same pattern of the digits after the decimal does not repeat frequently or at all.

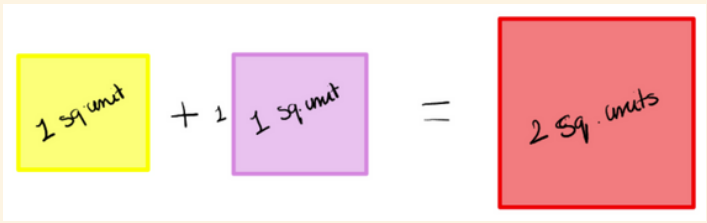
Here is the sutra and the value of √2 stated by Baudhayana

"samasya dvikaraṇī. pramāṇaṃ tṛtīyena vardhayet tac caturthenātmacatustriṃśonena saviśeṣaḥ"

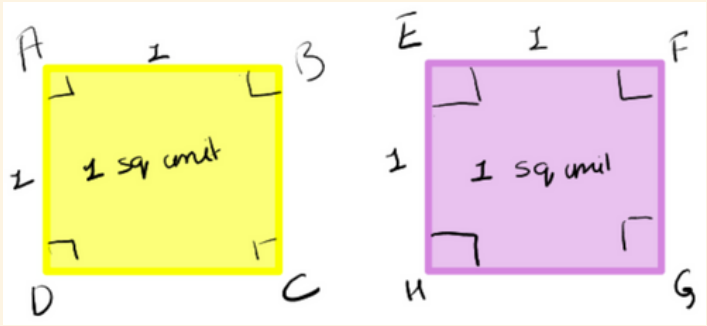
Value given by Baudhayana:
√2 ≈ 1 + 1/3 + 1/(3×4) - 1/(3×4×34)

Now we have all the tools to flow with the process of finding the value of √2.

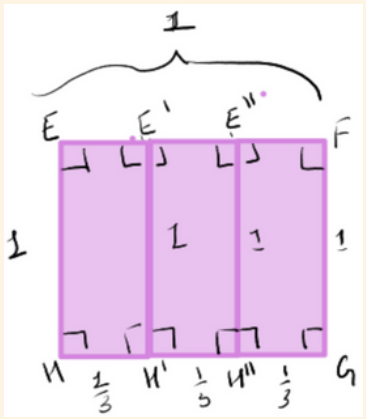
From Baudhayana's theorem, we know:
$1^2 + 1^2 = (\sqrt{2})^2 = 2$



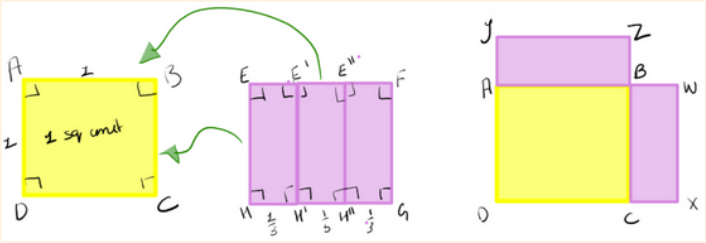
Now let's consider two unit squares, ABCD and EFGH. Here we have to somehow add these two unit squares so that we get a bigger square, which obviously has an area of 2 sq units.



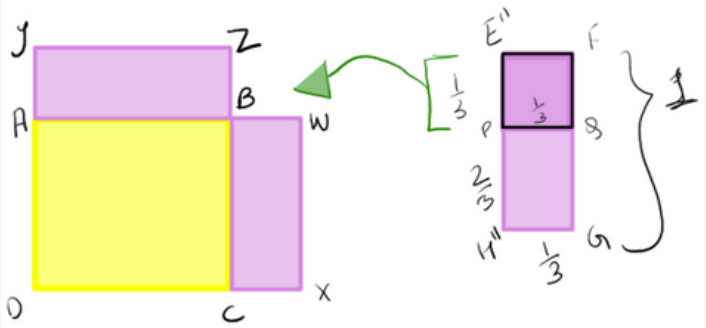
Now we vertically divide the EFGH square into 3 equal parts.



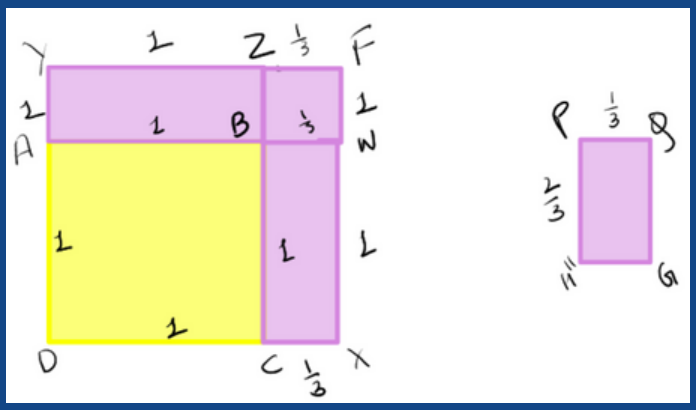
Now, join the EH side of the EFE'H' rectangle onto the BC side of the ABCD square, call the attached side BC itself and one parallel to it as WX. Similarly, join E'H' side of the E'H'E"H" rectangle onto the AB side of the ABCD square, and now call the attached side AB itself and one parallel to it as YZ.



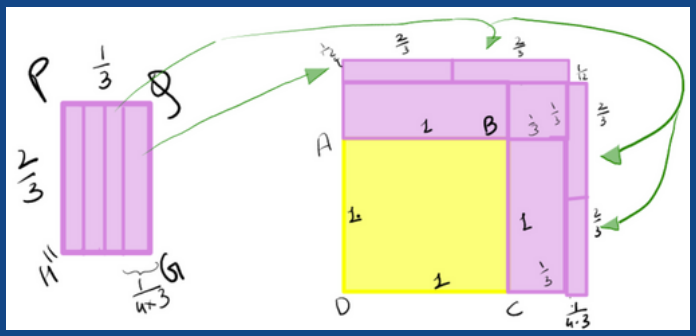
Now, with the remaining rectangular strip E"FGH", divide it 2/3 vertically using a horizontal line PQ. Now, let the 1/3.1/3 square E"FQP attach BZ with E"P and call it BZ itself, and the line that meets PQ and BW, let it be called BW itself.

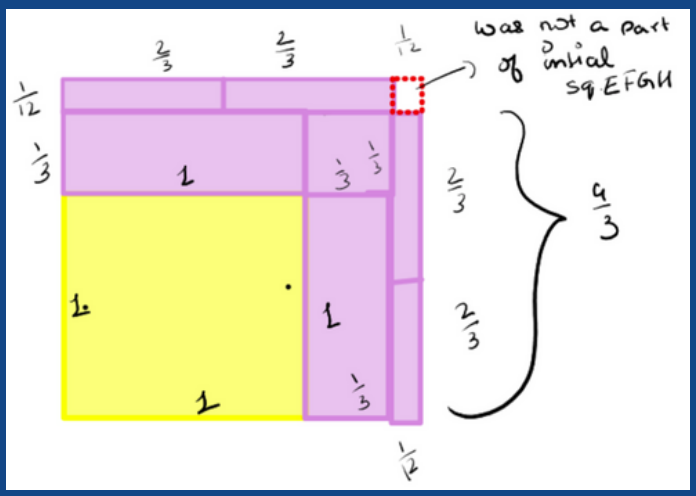


Now we have a square YFXD with given dimensions in the diagram and a rectangular strip PQGH" with dimensions 1/3.2/3 unit square.



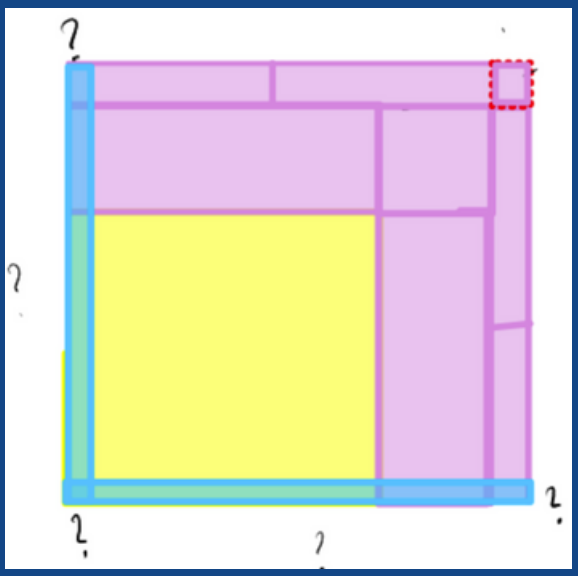
Now we divide the rectangular strip PQGH" vertically into 4 equal parts. Then, attach them as given in the diagram.



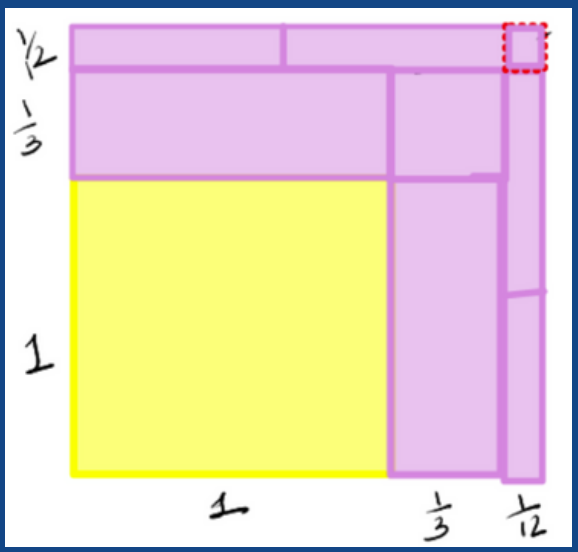


If we notice, the red dotted 1/12.1/12 square was never a part of square EFGH. To form a perfect square, we have to consider the red dotted square of area 1/12.1/12, and we have to negate the same area of 1/12.1/12 in the bigger attached pieces, such that we get a square of area 2.

So if we want to remove the excess area of 1/12. 1/12 and still keep it a square of area 2, we have to remove the 2 blue perpendicularly placed rectangular strips of area as shown below.



Now it is arithmetic time!



[area of sq. ABCD] + [area of sq. EFGH] + [area of 1/12.1/12 sq.] = [area of bigger sq.]
[area of sq. ABCD] + [area of sq. EFGH] = [area of bigger sq.] - [area of 1/12.1/12 sq.]

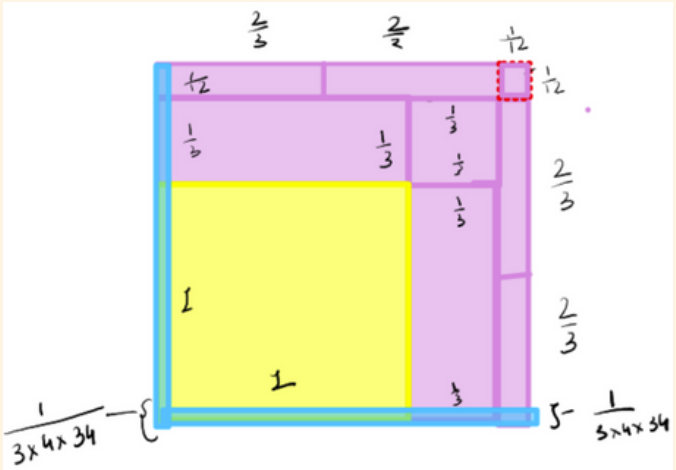
Now we have to calculate the length

L and the breath B of the two blue rectangular strips (here we are going with longer side length notation).

Now, each side of this bigger square, without the excess area stripped out, is = 1 + 1/3 + 1/12 = 17/12 units.

Therefore, the length L of the blue rectangles is 17/12.

We know the area of two strips of rectangles are same, and the sum of their area must be 1/12.1/12 = 1/144, because of the excess red dotted square.
=> [area of rectangle + area of rectangle] = 1/144
=> 2[area of rectangle] = 1/144
=> 2[L x B] = 1/144
=> 2[17/12 x B] = 1/144
=> B = 1/144 x 12/34



=> B = 1/12 . 1/34 or 1/(3. 4. 34) as Baudhayana represented.

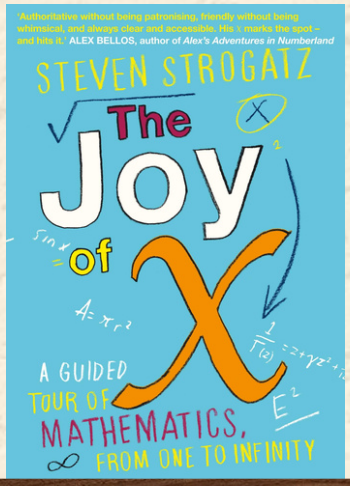
As discussed earlier, we have arrived from Baudhayana's theorem $1^2 + 1^2 = (\sqrt{2})^2 = 2$, through geometric manipulation. The last step is to sum all the pieces of the side to get the value of the root from the square of area 2.

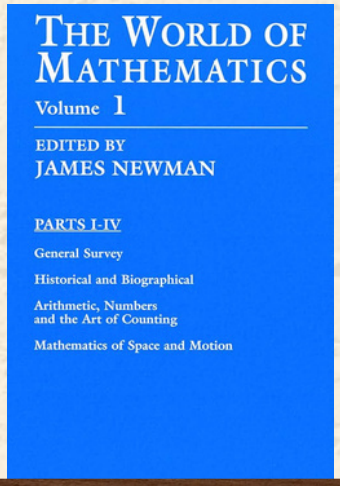
From the above diagram value of 2, which is the side of the bigger square, is approximately equal to (1 + 1/3 + 1/3 .4)- (1/3. 4. 34). +1 from square ABCD, + 1/3 from one-third of square EFGH, + 1/(3.4) from the one-fourth of the remaining one-third of square EFGH, and - 1/(3.4.34) subtracting from the excess area from geometric manipulation.

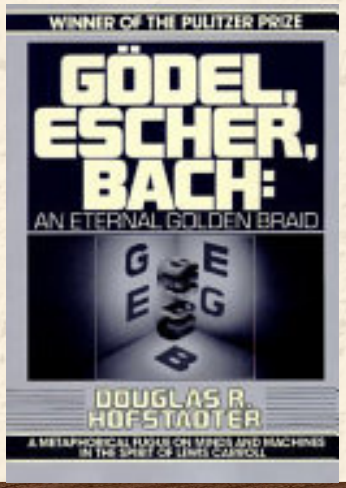
$\sqrt{2} \approx 1.41421568627$

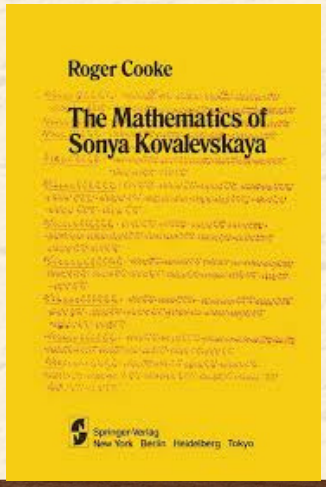
The value given by Baudhayana is correct upto 5 decimal places. The value of √2 is seen to be used in trigonometry, engineering, computer science and many other fields.

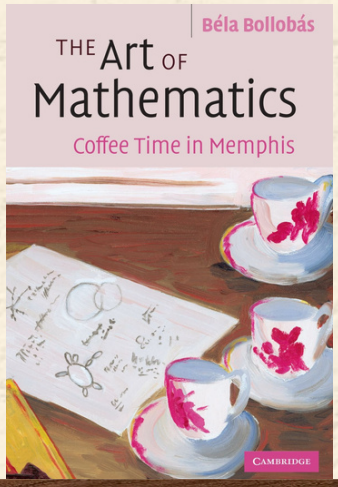
Written by - PRANAVA SHASTRY

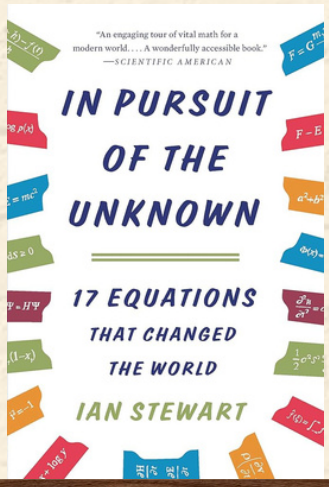


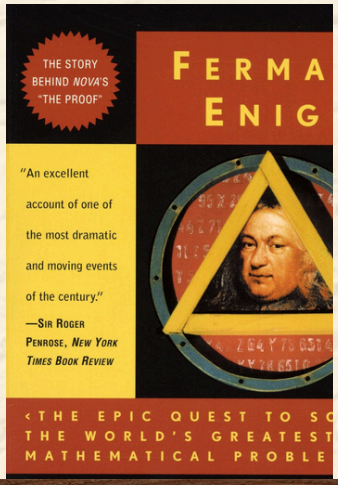


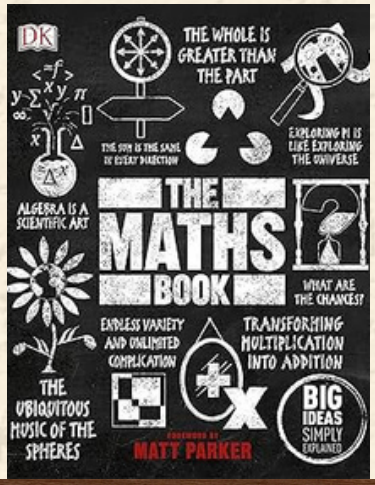












THE MATH SHELF

CLICK ON BOOKS FOR REVIEWS!

ಗಣಿತ:
ನನ್ನ ಗುರುಗಳ ದೃಷ್ಟಿಕೋನ

ಶಾಲೆಗಳಲ್ಲಿ ಬಹುತೇಕ ವಿದ್ಯಾರ್ಥಿಗಳ ಹೃದಯ ಬಡಿತ ಹೆಚ್ಚಿಸುವ ವಿಷಯವೆಂದರೆ ಅದೇ ಗಣಿತ!. ಆದರೆ ನನ್ನ ಗಣಿತ ಶಿಕ್ಷಕರ ದೃಷ್ಟಿಯಲ್ಲಿ ಅದು ಕೇವಲ ಅಂಕಿಗಳ ಲೆಕ್ಕಾಚಾರವಲ್ಲ. ಬದಲಿಗೆ ಅದು ಬದುಕಿನ ಬಹುಮುಖ್ಯ ಭಾಗ. ಈ ಲೇಖನದಲ್ಲಿ ನಾನು ನನ್ನ ಗುರುಗಳಾದ ಶ್ರೀ ಬಸವರಾಜು ಅವರು ಸರ್ಕಾರಿ ಹಿರಿಯ ಪ್ರಾಥಮಿಕ ಶಾಲೆ ಕಸುವಿನಹಳ್ಳಿಯಲ್ಲಿ ಗಣಿತ ಶಿಕ್ಷಕರಾಗಿ ಕಾರ್ಯ ನಿರ್ವಹಿಸುತ್ತಿದ್ದಾರೆ. ಅವರ ಸಂದರ್ಶನದಲ್ಲಿ ಆಯ್ದ ವಿಚಾರಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳುತ್ತೇನೆ.

ಗಣಿತದತ್ತ ಪ್ರಯಾಣ:

ನಮ್ಮ ಶಿಕ್ಷಕರು ಅವರ ಬಾಲ್ಯದ ನೆನಪುಗಳನ್ನು ಹಂಚಿಕೊಂಡರು. "ನಾನು ಹತ್ತನೇ ತರಗತಿ ವಿದ್ಯಾಭ್ಯಾಸ ನಡೆಸುತ್ತಿದ್ದ ದಿನಗಳಲ್ಲಿ ಅಂಕಿಗಳ ಆಟವೇ ನನಗೆ ಸ್ವರ್ಗವೆನಿಸುತ್ತಿತ್ತು". "ಒಂದು ದಿನ ನಮ್ಮ ಶಿಕ್ಷಕರು ನೀಡಿದ ಕಠಿಣವಾದ ಸಮಸ್ಯೆಯನ್ನು ಬಿಡಿಸಿದಾಗ ನನ್ನ ಸಂತೋಷಕೆ ಪಾರವೇ ಇರಲಿಲ್ಲ. ಇದೆ ನನ್ನ ಗಣಿತದತ್ತ ದಾರಿ ತೋರಿದ ತಿರುವು." ಎಂದು ನಗುತ್ತಾ ಹೇಳಿದರು.

ಪ್ರೇರಣೆಯ ಶಕ್ತಿ ನನ್ನ ಗುರುಗಳು:

ಅವರು ತಮ್ಮ ಪ್ರೌಢಶಾಲೆಯ ಶಿಕ್ಷಕರು ಶ್ರೀ ಬೆಳ್ಳೇಗೌಡರವರು ನನ್ನ ಪ್ರೇರಣೆ ಎಂದು ಹೇಳಿದರು. ಮತ್ತು ಅವರು ತಮ್ಮ ಗುರುಗಳತ್ತ ಕೃತಜ್ಞತಾ ಭಾವವನ್ನು ವ್ಯಕ್ತಪಡಿಸಿದರು. ಏಕೆಂದರೆ ಅವರು ಪಾಠದಲ್ಲಿನ ಯಾವುದೇ ಸಾಧಿಸುವ ಲೆಕ್ಕಗಳು ಮತ್ತು ಅದನ್ನು ಬಿಡಿಸುತ್ತಿದ್ದ ವಿಧಾನವೇ ಇದಕ್ಕೆ ಕಾರಣ. ಅವರು ಪಾಠ ಮಾಡುವ ವಿಧಾನ ಎಲ್ಲರನ್ನು ವಿಷಯದ ಕಡೆ ಗಮನಹರಿಸುವಂತೆ ಮತ್ತು ಬೇರೆಡೆ ಲಕ್ಷ್ಯನೀಡದಂತೆ ಮಾಡುತ್ತಿತ್ತು."ನಮ್ಮ ಶಿಕ್ಷಕರೇ ನನಗೆ ಗಣಿತ ಶಿಕ್ಷಕ ವೃತ್ತಿಯನ್ನು ಆಯ್ಕೆಮಾಡಲು ಸಹಾಯ ಮಾಡಿದ್ದು".

ಭೋದನೆಯ ಸಿಹಿ ಅನುಭವಗಳು :

"ಸರ್, ನನಗೆ ಗಣಿತ ಅರ್ಥವಾಗುವುದೇ ಇಲ್ಲ." ಎಂದು ವಿದ್ಯಾರ್ಥಿಯೊಬ್ಬ 8 ನೇ ತರಗತಿಯಲ್ಲಿ ಹೇಳಿದ ಮಾತು. ಆದರೆ "ಅದೇ ವಿದ್ಯಾರ್ಥಿಗೆ ಹೆಚ್ಚಿನ ತರಗತಿ ತೆಗೆದುಕೊಂಡು ಕಠಿಣ ಸಮಸ್ಯೆಯನ್ನು ಚಿಕ್ಕ ಚಿಕ್ಕ ಹಂತಗಳಲ್ಲಿ ಕಲಿಸಲು ಪ್ರಾರಂಭಿಸಿದೆ. ಅದೇ ವಿದ್ಯಾರ್ಥಿ 9 ನೇ ತರಗತಿಯಲ್ಲಿ ಸಮಸ್ಯೆ ಬಗೆಹರಿಸುವಲ್ಲಿ ತೋರಿದ ಹುಮ್ಮಸ್ಸು, ಸಂತೋಷ ಹೇಳತೀರದು. ಆದರೆ ಅದೇ ವಿದ್ಯಾರ್ಥಿ ತನ್ನ 10 ನೇ ತರಗತಿಯಲ್ಲಿ ಒಳ್ಳೆಯ ಅಂಕಗಳನ್ನು ಗಳಿಸಿದಾಗ ನನಗೆ ಆದ ಸಂತೋಷ ವ್ಯಕ್ತಪಡಿಸಲು ಸಾಧ್ಯವಿಲ್ಲ. ಇದೆ ಶಿಕ್ಷಕರಿಗೆ ದೊರೆಯುವ ದೊಡ್ಡ ಬಹುಮಾನ". "ವಿದ್ಯಾರ್ಥಿಗಳ ಕಲಿಕಾ ಮಟ್ಟಕ್ಕೆ ಇಳಿದು ಭೋದಿಸುವುದು ಮತ್ತು ಗಣಿತ ಸುಲಭ ವಿಷಯ ಎಂದು ಮಕ್ಕಳಿಗೆ ಸುಲಭ ಆಸಕ್ತಿಯುತ ಲೆಕ್ಕಗಳನ್ನು ಬಿಡಿಸುವುದರ ಮುಖಾಂತರ ಅರ್ಥಯಿಸುವುದು ನನಗೆ ಖುಷಿ ನೀಡುತ್ತದೆ".

ವಿದ್ಯಾರ್ಥಿಗಳ ಸಮಸ್ಯೆಗಳು ಶಿಕ್ಷಕರು ಕಂಡಂತೆ

- ವಿದ್ಯಾರ್ಥಿಗಳು ಮೊದಲೇ ಗಣಿತವನ್ನು ಕಷ್ಟವೆಂದು ಭಾವಿಸುತ್ತಾರೆ ಈ ಭಯವೇ ಅವರ ಭವಿಷ್ಯದ ಅತಿ ದೊಡ್ಡ ಶತ್ರು.
- ವಿದ್ಯಾರ್ಥಿಗಳು ಸರಿಯಾದ ಅಭ್ಯಾಸ ಮಾಡದಿರುವುದು.

ಮೆಚ್ಚಿನ ಗಣಿತದ ಭಾಗ:

ನಿಬಂಧಿತ, ನಿತ್ಯಸಮೀಕರಣ, ತ್ರಿಕೋನಮಿತಿ ಎಂದರೆ ನಮ್ಮ ಶಿಕ್ಷಕರಿಗೆ ಬಹಳ ಅಚ್ಚುಮೆಚ್ಚು. ಏಕೆಂದರೆ ಈ ವಿಷಯಗಳನ್ನು ನಮ್ಮ ದೈನಂದಿನ ಜೀವನದಲ್ಲಿ ಉಪಯೋಗಿಸಬಹುದು. ಲಾಭ, ನಷ್ಟ ಮತ್ತು ಶೇಕಡಾವಾರು ಇದು ವಿದ್ಯಾರ್ಥಿಗಳು ಶಾಲೆಯ ಚೌಕಟ್ಟನ್ನು ಮೀರಿ ಉಪಯೋಗಿಸುವ ವಿಷಯ. ಗಣಿತವು ಜೀವನದಲ್ಲಿ ನಿಖರತೆ ಮತ್ತು ಶಿಸ್ತನ್ನು ರೂಪಿಸಿಕೊಳ್ಳಲು ಬಹಳ ಸಹಕಾರಿ.

ವಿದ್ಯಾರ್ಥಿಗಳಿಗೆ ಸಲಹೆಗಳು:

- ತಪ್ಪುಗಳಿಗೆ ಯಾವುದೇ ಕಾರಣಕ್ಕೂ ಹೆದರಬೇಡಿ. ಏಕೆಂದರೆ ಅದೇ ನಿಮ್ಮ ಕಲಿಕೆಗೆ ಮಾರ್ಗದರ್ಶನ.
- ನಿಯಮಿತ ಅಭ್ಯಾಸ.
- ಶಿಕ್ಷಕರಿಗೆ ಪ್ರಶ್ನೆ ಕೇಳಲು ಹಿಂಜರಿಯಬೇಡಿ -ಏಕೆ

?,ಹೇಗೆ?,ಏನು?..... ಈ ಕುತೂಹಲವೇ ಗಣಿತದ ಜೀವಾಳ.

- ಪಠ್ಯಪುಸ್ತಕದ ಹೊರತು ಪಜಲ್, ಸಮಸ್ಯೆಗಳು,ಆಟಗಳು,ಪುಸ್ತಕಗಳಿಂದ ಗಣಿತವನ್ನು ಕಲಿಯಿರಿ.
- ಕಲಿಕೆಯನ್ನು ಮಾಡುವಾಗ ಚಟುವಟಿಕೆಗಳ ಮೂಲಕ ಮಾಡಿರಿ.

ಈ ಸಂದರ್ಶನದಿಂದ ನನಗೆ ತಿಳಿದು ಬಂದ ಸಂಗತಿಯೆಂದರೆ -ಗಣಿತವೆಂದರೆ ಅಂಕಿಗಳ ಕಾಡಲ್ಲ.ಅದು ಚಿಂತನೆಯ ಹಾದಿ. ವಿದ್ಯಾರ್ಥಿಗಳು ಗಣಿತವನ್ನು ಭಯದಿಂದ ನೋಡಿದರೆ ಅದು ಕಠಿಣವಾಗುತ್ತದೆ. ಆದರೆ ಅದನ್ನು ಕುತೂಹಲದಿಂದ ಅಭ್ಯಾಸ ನಡೆಸಿದರೆ, ಅದು ನಮ್ಮ ಬದುಕಿನ ಆತ್ಮೀಯ ಸ್ನೇಹಿತನಾಗುತ್ತದೆ. ಗಣಿತವನ್ನು ಪ್ರೀತಿಸಿ. ಅದು ನಮ್ಮ ಬದುಕನ್ನು ಬೆಳಗಿಸುವ ದಾರಿದೀಪವಾಗಬಹುದು.

SCAN FOR TRANSLATION!

Written by - PRANAVASHREE

BLOCKCHAINS AND RINGS

Unlike the traditional databases that are used by government entities and banks, blockchains are special databases that hold collections of data and records, primarily transactions. We can think of it as a ledger. The traditional databases are not effective and are prone to numerous vulnerabilities such as server crashes, cyber attacks, any sort of technical issue, transfer limit, transaction fee.

Blockchains address all these issues, first they do not require a central authority making them decentralized, highly immune to counterfeiting activities and are also protected by complex algorithms such as- SHA256, ETHAASH. This makes all the transactions highly secure. By keeping its data decentralized, it allows full access of the database among all of its users and gives maximum transparency, making it highly resistant to frauds. On the other hand, banks give only limited access of its database to its users.

Essentially, blockchains are like digital ledgers that consist of a sequence of blocks. Each block contains information related transactions such as time of transaction, amount of transaction and hash code of the previous block. One use case of blockchain is that it enables direct and secured payments and encrypted messages across multiple different nodes making it very efficient.

Some Core Concepts of Blockchain:

1. **Immutability:**
Refers to the property of blockchain i.e. once the block has been made and the data inside the blocks is stored then it cannot be altered making it a permanent record. Once the sequence of blocks is made then it cannot be changed. In blockchains, this is achieved by hashing.

2. **Hashing:**
A mathematical function which receives one input (that input is mainly transaction data) and then gives out an alphanumeric string as output which is encrypted and secure. That string is called Hash code. The information present inside the block also consists of the hash code of itself and the hash code of previous block. This property makes it very secure and immutable.

3. **Cryptographic security:**
The databases used in blockchains

are protected by complex algorithms which provide trust and shield the database from external frauds. Such as SHA-256 used by Bitcoins or ETHASH used by Ethereum cryptocurrency.

4. **Public Key:**
It serves as an identity across a network where nodes operate, similar to an email address. This can be shared among different computers and also is used to receive information from other nodes.

5. **Private key:**
This is known only to the user and it is required in confirming a transaction between nodes. We can think of the private key as our UPI-pin that we use daily for our transactions.

Modulo arithmetic

As mentioned earlier, traditional banking systems rely on individuals to record transactions and keep our money and assets safe. But, as humans, there is always room for some error to creep in, corruption or worst case even hacking. This is where blockchains are different, replacing human trust with a solid mathematical proof. Using modulo arithmetic, users can create digital signatures and can secure their transactions, even verifying ownership. At every step, the chain uses math, so none of its users can cheat the system.

Let us look at some of this math.

The core of this system operates within a structure we learnt in class called rings. Now, each transaction that is done has a digital signature, a way to prove that the transaction is valid, without giving away any private data. The way that this works is, each user has a private key(a secret key only they possess). This private key corresponds to a public key, which can be shared with others. Therefore, a user can use their private key to create a signature for a transaction, and others can use the public key associated with it, to check the authenticity of the transaction.

At the center of the process lies modulo arithmetic. To understand, let's look at an example. It was computed on pen and paper, and then typed up.

Imagine we are signing a message in a basic cryptographic system, let's use small numbers.

- Let p = 97. ‘p’ is the large prime, and the modulus we work in.
- We also use a generator g = 5. The generator is like a point to start, that helps us get all the other elements in the group, by doing operations of multiplication and addition multiple times.
- Lets take our private key = 23
- Our public key = $g^d \bmod p = 5^{23} \bmod 97 = 38$

Now, if we sign some message like “ receive coins”, and lets say it comes to some hash 42. We also have

to choose something called a ‘nonce’. It's a random number, and it's used only one time in a transaction. It's mainly used to ensure that older transactions and data cannot be reused and it also ensures that each transaction is unique. Let's say our nonce k = 17.

Let us compute $r = g^k \bmod p$ (r ties the signature to the nonce k)
$r = 5^{17} \bmod 97$
Computing:
$5^1 = 5$
$5^2 = 25$
$5^4 = (5^2)^2 = 625 \bmod 97$
$625 = 6 \cdot 97 + 43$
$5^4 \equiv 43 \pmod{97}$

Next, $5^8 = (5^4)^2 = 43^2 \pmod{97}$
$43^2 = 1849$
$1849 = 19 \cdot 97 + 6$
$5^8 \equiv 6 \pmod{97}$

Now, we can express 5^{17} as:
$5^{17} = 5^{16} \cdot 5 = 5^{8 \cdot 2} \cdot 5 = (5^8)^2 \cdot 5$

We know from above that:
$5^8 \equiv 6 \pmod{97}$
So, $(5^8)^2 \equiv 6^2 \pmod{97}$

Now,
$5^{17} = (5^8)^2 \cdot 5 \equiv 36 \cdot 5 \pmod{97}$
$36 \cdot 5 = 180$
$180 = 1 \cdot 97 + 83$
$5^{17} \equiv 83 \pmod{97}$

Therefore, r = 83

Now, to tie together the hash, r, and the private key, we use the formula:
$s = k^{-1} (\text{hash} + r \cdot d) \pmod p$
Here, k is the nonce. We now find the modular inverse of the nonce:

$k^{-1} \pmod p$
$17^{-1} \pmod{97}$
$k^{-1} \equiv 40 \pmod{97}$
since, $17 \cdot 40 = 680 = 7 \cdot 97 + 1$

Now, to find s:
$s = 40 \cdot (42 + 83 \cdot 23) \pmod{97}$
First compute $r \cdot d$:
$r \cdot d = 83 \cdot 23 = 1909$
$1909 = 19 \cdot 97 + 66 = 66 \pmod{97}$

Substituting back:
$s = 40 \cdot (42 + 66) \pmod{97}$
$42 + 66 = 108$
$108 = 1 \cdot 97 + 11 = 11 \pmod{97}$
So, $s = 40 \cdot 11 \pmod{97}$
$s = 440 \pmod{97}$
$440 = 4 \cdot 97 + 52 = 52 \pmod{97}$

Therefore, finally we have a digital signature, which is (r, s). We found it to be (83, 52).

Now, you may ask, is it possible to find a private key from the public key, in say bitcoin? The answer is no, since usually in bitcoin, the private key is a big number, and its generated by multiplying it with some fixed elliptical curve defined over 256 bit prime field. It's pretty easy to calculate the public key from the private key, but the other way is extremely difficult. The number of possible private keys is 2256 an extremely big number. Even if we try to brute force, it would take an unimaginable amount of time to calculate. Moreover, currently there is no mathematical shortcut to solve this issue. This function is called a trap door function, in the sense that, since d is in the

power, we'll be able to find the public key, but won't be able to figure out the power d.

Encryption and Decryption

Let's imagine you and I are in a classroom, and we want to pass along notes to each other. We must also ensure that only the two of us can understand (decipher) the messages we send. Let us use a simple cryptographical cipher known as the Caesar Cipher. What the Caesar Cipher does is for any letter you may wish to write, you write the letter 3 "spaces" ahead of it. For example, if I wanted to write the letter 'A' I would write 'D' instead.

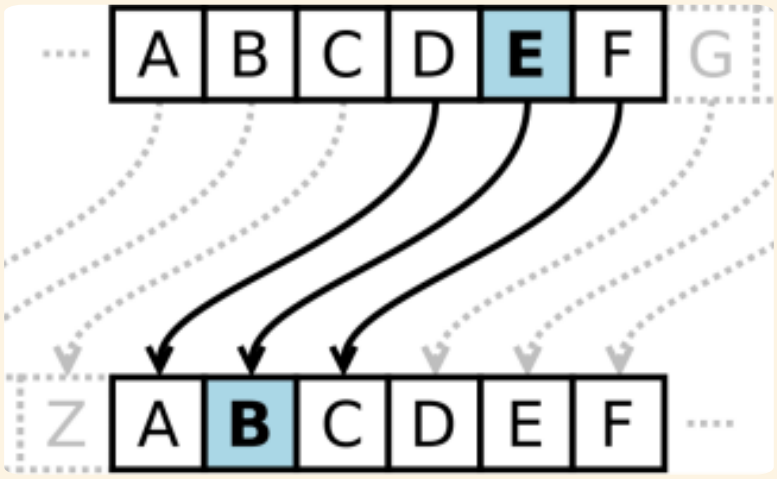


Figure 1.Caesar Cipher

So if I wanted to send you the message "Hello", I would instead send the message "KHOOR". Now since you and only you know how the message is encrypted, you also know how to decrypt it. An issue may arise here, if someone intercepts many messages over a period of time they may figure out the pattern of encryption and be able to decipher it themselves. However, we do see the foundations of cryptography in a sense. We know there will be a:

PLAINTEXT (Our Message) → CIPHERTEXT (Our Message but Encrypted) → DECIPHERED TEXT (Our Encrypted Message but Decrypted)

Now we may try to make our method of encryption more complex, such as by using a sort of encryption key. Let's say our encryption key was the word "COMPUTER"; how would we use this while still using a concept similar to that of the Caesar Cipher? Let's say our message is the phrase "You Can't Trust Me".

Now we apply our encryption key to it.

```
Youcantrustme
+ computercompu
_____________

Bdhsvhyjxhgcz
```

Now, how did we obtain this? Well when we "add" **c** to **y**, what we are actually doing is noting that since **c** is the third letter of the alphabet, we write decrypted **y** as the letter 3 spaces from **y**, and since **y** is the 25th letter of the alphabet, we need the 28th letter of the alphabet which, if we wrap around all the letters is the letter **b**. Similar process for the remaining letters. Note that if the number of letters of our message exceeds our encryption key, we just keep repeating the key for as many letters that remain.

Now we see something quite

interesting being developed here, B is the 2nd letter of the alphabet, as well as the 28th letter of the alphabet, it is also, in a sense, the 54th letter of the alphabet, and even the 80th. This gives us an intuition into the concept of equivalence classes in modular arithmetic. The 28th letter is equivalent to the 2nd letter.

This can also be seen in clocks.

While 1 o'clock can be denoted as 1:00, it can also be 13:00 (ignoring AM/PM). Now 11+2 = 13 (in a clock), which is equivalent to 1. Formally, this means that 13 ≡ 1 (Mod12), or 13 when divided by 12, gives a remainder of 1. The entire system of time measurement is based on this concept.

Let us now have a look at Fermat's Little Theorem. It states:
If P is a prime number, and A is an integer not divisible by P, then
$A^{(p-1)} \equiv 1 \pmod{P}$.

Now we examine the concept of relatively prime. Two numbers (x and y) are relatively prime if GCD(x, y) = 1.

Euler's Totient Function, Φ(x), outputs all numbers less than a given number 'x' that are relatively prime to x.
For example: Φ(10) = {1,3,7,9}

Now we notice something interesting, if x is prime then every number up to x is relatively prime to x.
For example: Φ(7) = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}

We observe that the length of the set Φ(p), where p is prime, is actually p-1. Now recall:
$A^{(p-1)} \equiv 1 \pmod{P}$ We can substitute the value of p-1 as Φ(p). We obtain: A^(Φ(p)) ≡ 1 (Mod P).

This lead to Euler coming up with a more general theorem which stated:
A^(Φ(n)) ≡ 1 (Mod(n))
Using what we just discussed we will now further explore an extremely famous algorithm known as the RSA encryption algorithm.

RSA algorithm

First, we take two random primes 'p' and 'q'. And we have an n = pq. We also obtain Φ(n). Something interesting to note at this stage is that n = pq is a product of the primes p and q, and Φ(n) = Φ(pq), which ,quite interestingly, is (p-1) x (q-1).

In our next step we select two integers 'e' and 'd' such that:
ed ≡ 1 (Mod(Φ(n)))

Our numbers e and n, are public information, for our convenience represented as (e, n). This is also known as a public key.
Our number d, however, is secret (Private Key).

Now is a good time to note that despite knowing e and n, and knowing ed ≡ 1 (Mod(Φ(n))), it is infeasible to work back and obtain

the value of d. This is equivalent to saying the best method to try and find d would be to randomly try and guess it. Which, as mentioned before, is infeasible, and even a high-tech computer cannot find it in a reasonable amount of time.

Getting back to our algorithm, if someone wants to say send a message M, we convert it into some number (there are ways to do this that we haven't mentioned, but a video explaining it is linked under the references section). Now we take M and raise it to the power e, and then modulo n , which gives us some number y.

M^e (Mod(n)) = y

Now, once I receive this message, to decrypt it, I take y, raise it to the power of d, and apply modulo n. And I get back my number M, which I can then convert back to the text through the same method I initially converted it.

Let us further understand this with an example, let us take:
P = 5
Q = 11
N = PQ = 5x11 = 55
Φ(N) = (5-1) x (11-1) = 4x10 = 40
E = 7 and D = 23 such that 7x23 ≡ 1(Mod(Φ(N))

Let us say our message M was converted to the number 2.

I would receive 27 Mod(N) = 18

With the number 18, I would decrypt it by: 1823 Mod(N) = 2. Hence I got back the message. Here is a proof to display why it always works:
Proof:

So I receive a message in the form: Me (Mod(n)), and raise it to the power d. So we get (Me)d = Med - (1)

And we know ed ≡ 1 (Mod(Φ(n))), which means ed - 1 = k.(Φ(n)), k is some integer. Which implies ed = 1 + k.Φ(n). Now substitute the value of ed in (1). Med = M1 + kΦ(n) = (MΦ(n))k. M

Now we know A^(Φ(n)) ≡ 1 (Mod(n))
So [{M^(Φ(n))}^k].M = 1k . M = M
Hence, we get M back and can read the message!

Blockchains

Let's say you and a bunch of friends decide to keep track of who owes whom money. You could write it all down in a notebook—every time someone pays someone else, you log it. But now comes a classic problem: who keeps the notebook? If only one person does, everyone else has to trust them not to cheat, not to make mistakes, and not to misplace it. That's a lot of trust.

So instead, you agree: everyone will keep their own copy of the notebook. Anytime someone makes a payment—say, Alice gives Bob $5—everyone adds that to their notebook. This way, there's no central authority; everyone agrees on a shared record. That's the basic idea behind decentralization.

Now, you might think: "What if someone tries to cheat? What if Charlie tries to change a past transaction in his copy to say Bob paid him $100?" That's where blockchains become clever.

Rather than just writing transactions one after another, you organize them into blocks—chunks of data that each contain a group of transactions. Once a block is full, you seal it using something called a hash. You can think of a hash as a digital fingerprint: you feed in the transactions, and the hash function spits out a string of numbers and letters, like 000cf7a34b.... Importantly, this output is completely determined by the block's contents—but even the tiniest change will completely change the hash. Output might look like:

9b1c0c5d8edb0ed7c67c5d4d95b4ccdb7e7
3f3c1450adbd79f69f4c71e2f3ef4

Change even one letter, and the hash becomes totally different. That makes hashes great for detecting tampering.

But the blockchain idea goes one step further. Each new block doesn't just store its own data—it also stores the hash of the previous block. That links them together into a chain.

So if someone tries to alter Block 1, they'd change its hash. That invalidates Block 2, which invalidates Block 3, and so on. To change a past transaction, you'd need to recompute the hash for that block and every block after it—which requires enormous computational effort.

But wait—who gets to add the next block? We don't want just anyone to be able to scribble things down. This is where Proof of Work comes in.

To add a block, a participant (called a miner) has to solve a computational puzzle. Specifically, they try to find a number—called a nonce—such that when added to the block's data and hashed, the resulting hash starts with a certain number of zeros, like: 000000abcde923…

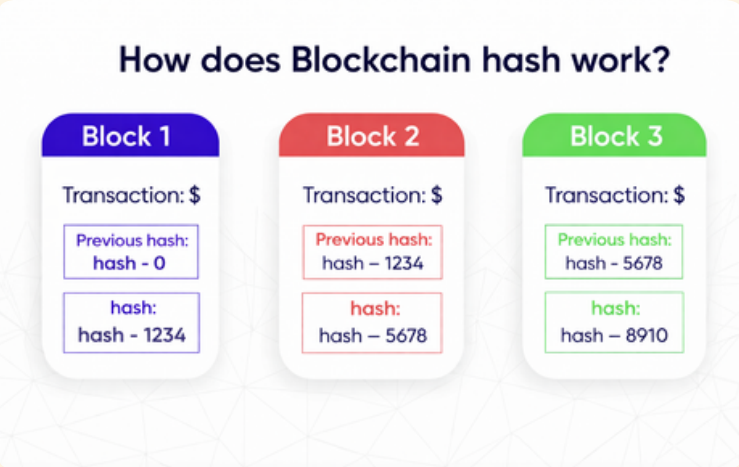


Figure 2

It's like a lottery: you keep trying different nonces until one works. This takes time and energy, so it's hard to fake. But once someone finds a valid solution, they broadcast the block to the network. Everyone else can verify the work very quickly and add the block to their own chain.

This is intentionally simplified,

but it shows the basic idea: trial and error until you get a hash with enough leading zeros.

So why would anyone do all this work? Because the network rewards miners. In Bitcoin, for example, the successful miner earns some newly minted bitcoins plus transaction fees. This incentivizes people to secure the network and validate transactions honestly. But what if two miners find a valid block at almost the same time? For a short while, there might be a disagreement—some people have one version of the chain, others have a different one. That's okay. Everyone just keeps building on the version they have.

Eventually, one version will get longer have more blocks and the network agrees to accept the longest valid chain. The other chain is abandoned.

This strategy is powerful. To forge a transaction, an interested but unwelcome party would have to redo all the proof-of-work for their fake chain faster than the rest of the network combined. This is infeasible.

For more on Modular Arithmetic, refer to this link!

Origami Hydrangea, A Tessellation

WHERE DOES MATH ANXEITY COME FROM?

Mathematics is often considered the scarier subject for most students than any other subject, across all age groups. Many wonder why math anxiety is so common among people and why math is often considered a threshold subject in competitive exams. For example, suppose in a competitive exam, both students A and B scored 75 out of 100. In the mathematics section, A scored 17 out of 25 and B scored 21 out of 25. In order to rank the candidates, examiners compare their marks in mathematics to break the tie. In that case, B gets priority over A. Hence, math is considered to be a threshold. To understand this issue, let us first dive into its root.

The National Education Policy (NEP) says that all subjects are mandatory till grade 10, giving equal importance to every subject. When we ask students where they use the concepts that they study in social science, they will at least try to provide some real-life examples. However, when the same students are asked about the application of mathematical concepts, such as algebra and trigonometry, many fail to answer. I feel this is a setback in mathematics education.

Up to primary and mid-secondary school, students learn about concepts that they can observe and use in their daily life. Then suddenly, there is a shift. The concepts become abstract and everything they learnt till yesterday doesn't seem relevant to them anymore.

Algebra, geometry and trigonometry are introduced to students with dozens of proofs and hundreds of formulas. The brains which used to retain small concepts are now overloaded with all these proofs and formulas. Textbooks that once seemed interesting and engaging are now filled with dense proofs. Everything feels unfamiliar and intimidating. This abstract nature of concepts leaves students anxious. The situation gets worse when board exams step in. Expectations from parents and society and the inherent complexity of the subject, everything around them are no longer the same as before.

Once they clear the board exams, then come competitive exams to get into college (11th and 12th grade), which again require mathematics for preparations. Even when two students score the same score, higher rank or admission preference will be given to the one who scored more in math. This adds another level of stress for students. This doesn't end with college; the same applies when students apply for universities.

All these reasons combined make math scary for students, thus resulting in hatred towards the subject. Another reason is parental and societal expectations to take up sciences and not arts, since it is considered to be a better option for future opportunities. Although there are many such underlying reasons, one of the most significant reasons is the abrupt shift from simplicity to complexity for math being a hated subject for students across the globe.

LABYRINTHINE AREA PUZZLE AND COMBINATORICS

Sid Sackson was a famous game designer and in 1969 published a book called Gamut of Games. This featured a game called LAP named after its Polish designer Lech Pijanowski and also called Labryinthine Area Puzzles. This game became very popular. In his fantastic book Math games with Bad drawing, Ben Orlin devotes a whole chapter to LAP. His criteria for including a game: it should be fun, lead to a lot of variations of the game, and the game should not take more than an hour and half to play. Does LAP satisfy these criteria?

This is a two player game. Each player has a 6 by 6 board that has 36 squares. Players 1 and 2 divide their board into four connected regions(Diagonal squares are not allowed). Let us call the regions of player 1 - A, B, C, D and player 2 - α, β, γ, δ. The goal of the game is to guess the four regions of the opponent before they do. This is somewhat like a battleship, where you are allowed to ask the opponent questions. The question a player can ask is as follows: Take a 2 by 2 square(example: Rows 1, 2 and Column 1', 2'). How many of these
4 squares are of type A, B, C, D. The opponent's replies may be of the following form: all A, all B, all C, all D, 1 C and 3 B, 2 A and 2 C etc. The exact placement is not revealed. The game proceeds by asking more questions and piecing the information together to get a map of the opponents board. When a player has figured out the opponents board, they shout out and then check if their answer is right. Here is a simple example of dividing a 6x6 board.

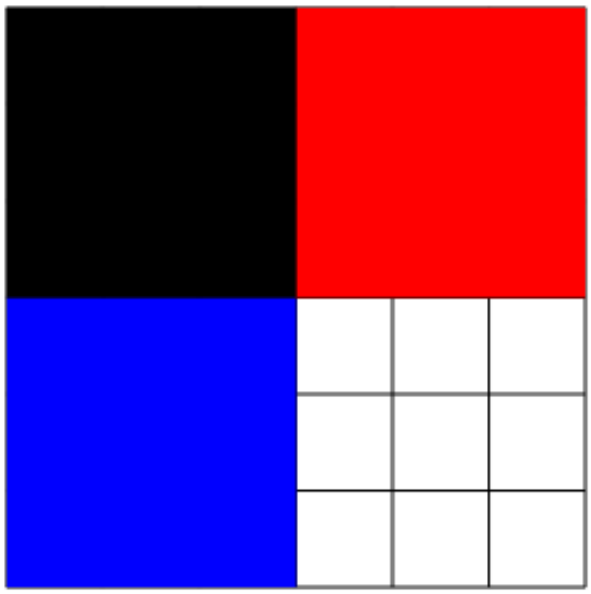


Figure 1: Example of dividing a 6x6 board

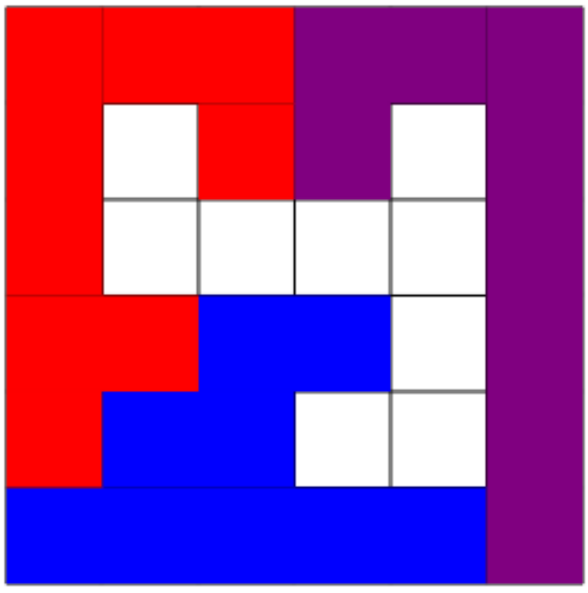


Figure 2: Example of dividing a 6x6 board

Go ahead, find a player and play several rounds of this game.

How did you play the game? Did you try to guess the four corners of your opponent's board or did you try to figure out the center of the board and then go outward? When you got information that contradicted your guess, what was your strategy? What was the approach of your opponent? What was the minimum number of questions? Is there a component of luck?

While there are several question regarding strategy of the players in asking questions, let us spend some time on how we divide the board into four connected regions, each with 9 squares. This beautiful question can lead to interesting combinatorial questions.

- How many different boards are possible?
- How many of these are symmetric boards?
- If one cannot find closed formula, are there more symmetric boards or non symmetric boards?

The natural thing is to try to systematically list all possible boards and then feel exhausted! In situations like this, it would be good to step back and try to solve a simpler problem. (That is what George Polya recommends) Since we want the board to consist of 4 connected regions, we can start with a board that has 16 square (multiple of 4). Clearly there are two possible rectangular boards, 4×4 and 8×2. Now the problem becomes more tractable. The possible regions should have 4 squares and be connected. Consider the first case: 2 row and 8 column. These are precisely tetraminoes. Let us understand the number of ways in which we can cover a square board with tetrominoes. These shapes are very popular because of the game called Tetris. Consider the first case: 2 row and 8 columns. We can cover this using 4 square (yellow) pieces. or 4 red I shaped pieces. We can also join two orange L shaped pieces to make a 2×4 grid. Use two of these to cover the 2×8 rectangle. These are the easy cases. What about using only the T-shape or only he green Z-shape. These leave gaps no matter how hard we try. We realize that even though the area of the four pieces add up to sixteen we are not able to cover this rectangle using the piece exclusively. So things are getting complicated!

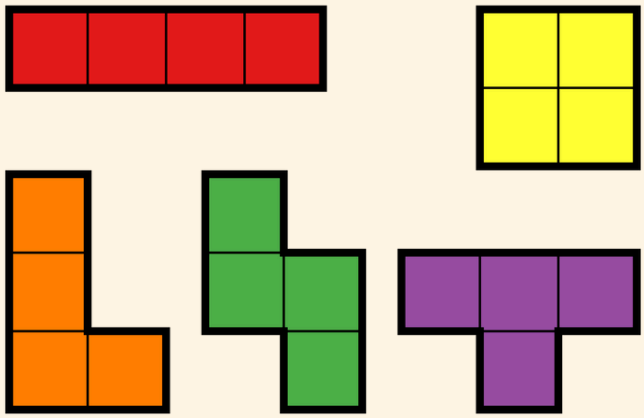


Figure 3: Tetrominoes

Consider the second case: Consider the second case of 4 × 4 square grid. Clearly, we can use four of the straight I shaped (red) tetrominoes to cover the board. Similarly, we can use four of the yellow (square) tetrominoes. These are boring! We notice that if we take two L shaped pieces (orange colored) then we can form a 2 by 4 rectangle and then put two of these 2 by 4 rectangles to form a 4 × 4 square board. Can we cover the 4 × 4 board using only the purple T shaped piece? Can we cover the 4X4 board using 4 different types of tetrominoes?

So now coming to our case 6 board into four connected regions of equal area. Each region will have 9 squares. So now we have to make a list of nonominoes and see which ones fit into this board. There are 1,285 nonominoes and 37 of them have holes in them. So we have a really tough job if we want to list out all possible configurations. The study of such questions is part of recreational mathematics and also connects with the branches of geometry, combinatorics, computer science and algorithms, optimization, statistical physics, coding theory etc.

THE FIBONACCI SEQUENCE AND A CONSTANT-TIME ALGORITHM

The Fibonacci sequence is one of the most famous sequences in Mathematics. It often appears in nature, Computer Science, and art. The sequence begins with the number 0 and 1. Every new number in the sequence is created by adding the two numbers that came just before it.

For example: F(0) = 0, F(1) = 1

F(2) = F(1) + F(0) = 1 + 0 = 1

F(3) = F(2) + F(1) = 1 + 1 = 2

F(4) = F(3) + F(2) = 2 + 1 = 3

So, the sequence goes

0, 1, 1, 2, 3, 5, 8, 13, 21, 34,...

The Problem of Computing Fibonacci Numbers

If we want to know F(n), the n^{th} Fibonacci number, the definition tells us to add the two previous numbers. That means we have to calculate all the earlier Fibonacci numbers first. This can be very slow for large n.

A Surprising Shortcut: Binet's Formula

There exists a clever formula that allows us to jump directly to the n^{th} Fibonacci number without calculating all the previous ones. This formula is called **Binet's Formula.**

Step 1: Writing the Rule as an Equation

The Fibonacci sequence is defined by the following rule:

F(n) = F(n-1) + F(n-2)

This is called a **recurrence** relation because each term is defined in terms of earlier ones. To solve this, mathematicians often guess that the solution looks like this:

$F(n) = r^n$

for some number r.

Step 2: The Characteristic Equation

If we substitute $F(n) = r^n$ into the recurrence relation, we get:
$r^n = r^{n-1} + r^{n-2}$
Now divide both sides by r^{n-2} (assuming $r \neq 0$):
$r^2 = r + 1$
This equation is called the characteristic equation. It tells us which values of r make the recurrence true.

Step 3: Solving the Characteristic Equation

The characteristic equation is:
$r^2 - r - 1 = 0$
Using the quadratic formula:
$r = (1 \pm \sqrt{1 + 4})/ 2 = (1 \pm \sqrt{5})/ 2$
So, the two solutions are:
$\varphi = (1 + \sqrt{5})/ 2$ and $\psi = (1 - \sqrt{5})/ 2$
Notice that the two solutions are the Golden ratio (φ) and its conjugate (ψ).

Step 4: Combining the Solutions

Because both φ^n and ψ^n satisfy the recurrence relation, the general solution is a combination:
$F(n) = A \cdot \varphi^n + B \cdot \psi^n$
where A and B are constants determined by the starting values.

Step 5: Finding A and B

We know: $F(0) = 0$, $F(1) = 1$
Substitute $n = 0$:
$F(0) = A \cdot \varphi^0 + B \cdot \psi^0 = A + B = 0$
So, $B = -A$ substitute $n = 1$:
$F(1) = A \cdot \varphi + B \cdot \psi = A\varphi - A\psi = A(\varphi - \psi)$
Since $F(1) = 1$, we get:
$A = 1 / (\varphi - \psi)$
But notice:
$\varphi - \psi = (1 + \sqrt{5})/2 - (1 - \sqrt{5})/2 = \sqrt{5}$
So, $A = 1/\sqrt{5}$, $B = -1/\sqrt{5}$

Final Formula - Binet's Formula

Substitute A and B:
$F(n) = 1/\sqrt{5} \cdot (\varphi^n - \psi^n)$
This is Binet's Formula.

Why This Matters

The formula allows us to compute F(n) directly, without calculating all previous Fibonacci numbers. It only uses a few multiplications and powers, so the time needed is always the same, no matter how large n is. This is called constant time, or O(1).

Limitation

During computation, the formula uses decimal approximations, which can cause small errors for very large n. You cannot represent an irrational number in a floating-point format because floating-point numbers have a fixed, finite number of bits, while irrational numbers have non-terminating and non-repeating decimal(or binary) expansions. This finite storage capacity means that an irrational number's infinite sequence of digits must be truncated or rounded, resulting in a rational approximation rather than the exact irrational number. Since the solution to the characteristic equation is irrational, their value

must be truncated in order to use it for computation.

Conclusion

The Fibonacci sequence is simple to define but deeply connected to many areas of mathematics. By turning the recurrence into the characteristic equation and solving it step by step, we reach Binet's Formula. This formula gives us a direct way to compute Fibonacci numbers in constant time O(1), showing the beauty of mathematical problem solving.

PERFECT CUBOIDS

An Euler brick is a cuboid in which all three sides are of integer length, and the diagonal on each face also measures an integer length. Finding Euler bricks was a popular mathematical pastime in the 18th century (no internet, etc.,). The first known example- a cuboid with sides 44, 117, and 240 was given by the German mathematician and calendar maker Paul Halcke in 1719 which still remains to be the smallest possible Euler brick.

After Halcke's discovery, mathematician Nicholas Saunderson found an entire family of such cuboids. Saunderson was an English mathematician and dedicated teacher, best known for his pioneering work in probability theory; some even credit him with formulating an early version of Bayes' theorem. He lost his eyesight at an early age and developed a mechanical calculator to assist in his work. He demonstrated that for any three numbers a, b, c satisfying $a^2 + b^2 = c^2$, one can construct an Euler brick with sides $x = |a(4b^2 - c^2)|$, $y = |b(4a^2 - c^2)|$, and $z = |4abc|$.

Euler bricks in which the space diagonal is also integer length are called "perfect cuboids". These have so far proven elusive. In Halcke's cuboid, the face diagonals are integers, but the space diagonals are irrational. (If the space diagonal were rational, we would be able to scale the side so that all dimensions, including the diagonal, become integers)

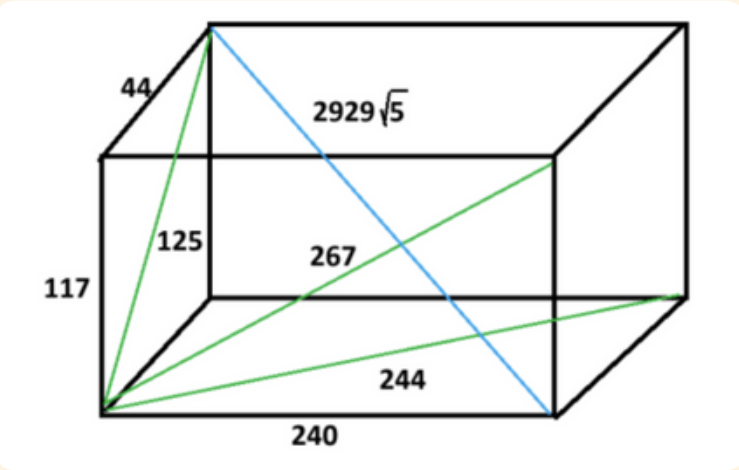


Figure 1. Halcke's cuboid

Halcke's example and Saunderson's constructions therefore do not lead to perfect cuboids. The general belief among mathematicians is that perfect cuboids do not exist, although the problem remains open.

The question about the existence of perfect cuboids can be stated mathematically as follows:
Label the vertices of the cuboid A, B, ..., H as in the diagram below:

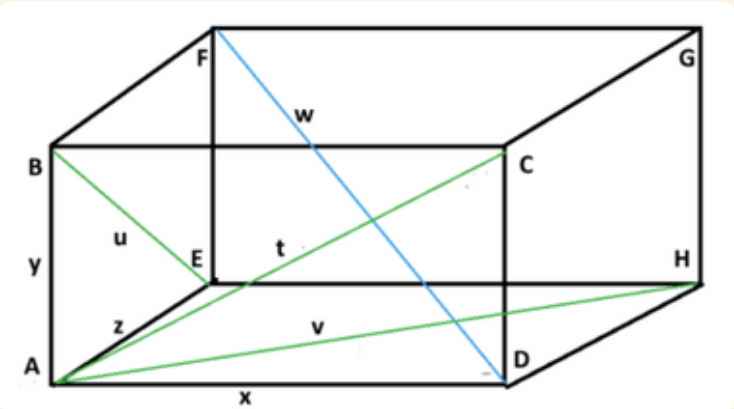


Figure 2. Halcke's cuboid(Labeled)

Then we want integer solutions to the following system of equations:
$AB^2 + BC^2 = AC^2$; $AB^2 + AE^2 = BE^2$; $AD^2 + AE^2 = AH^2$;
$AD^2 + AB^2 + AE^2 = FD^2$

That is, we want integer solutions t, u, v, w, x, y, z to the following system:
$x^2 + y^2 = t^2$; $y^2 + z^2 = u^2$; $x^2 + z^2 = v^2$; $x^2 + y^2 + z^2 = w^2$

Equations of this sort- polynomial equations with integer coefficients whose integer solutions we seek- are called Diophantine equations. They appear in many areas of mathematics; for instance, Fermat's Last Theorem is also a well known Diophantine problem. Finding a perfect cuboid, therefore means solving this particular system of Diophantine equations.

So what do we know about perfect cuboids? And how have people tried to find them? The first equation in the system above is another well-known Diophantine equation, whose solutions are the Pythagorean triples.

When looking for Pythagorean triples, people are often interested in primitive triples, that is, integers a, b, c such that $a^2 + b^2 = c^2$ and a, b, c have no common factor greater than 1. One can show that all Pythagorean triples are of the form $(2pq, p^2 - q^2, p^2 + q^2)$, where p and q have no common factors and are of opposite parity (one even, one odd). For example, p = 2 and q = 3 give the triple (12, 5, 13)

A nice geometric proof of this fact can be given by observing that finding a Pythagorean triple (a, b, c) is equivalent to finding a rational point (a/c, b/c) on the unit circle ($x^2 + y^2 = 1$). Drawing a line from (0, 1) to the x-axis and checking where it meets the circle gives a rational point—and hence a Pythagorean triple. Every other triple can then be obtained as multiples of these primitive ones.

An interesting result that follows is that in any Pythagorean triple, at least one of the shorter sides is even.

Following this line of reasoning, we can look for primitive perfect cuboids. We can argue that if a perfect cuboid exists then two sides must be even and one side must be odd. To see this, substitute $x^2 + y^2 = t^2$ into $x^2 + y^2 + z^2 = w^2$ to get $t^2 + z^2 = w^2$. So either t or z must be even; let's say t. But we also know that either x or y is even, so in fact they must both be even. If z is also even, the cuboid won't be primitive, so z must be odd. Similarly, if z is even, exactly one among x or y must be even. In either case, we see that a perfect cuboid, if it exists, must have two even sides and one odd side—and therefore an odd space diagonal.

The same reasoning used for Pythagorean triples extends to

other Diophantine equations, including the search for perfect cuboids. Some people instead look for rational points on special three dimensional surfaces related to these equations, a geometric way of approaching the problem.

Another direction involves looking for specific constraints on the cuboid's sides. For example, it is known that if a perfect cuboid exists, then one side must be divisible by 9, another by 3, one by 7, and another by 11.

As an example of how such results can be proven, here is an argument given by mathematician Tim Roberts showing that one edge must be divisible by 7. First, note that every integer has a remainder of 0, 1, ..., 6 when divided by 7. One can calculate that the square of a number leaves a remainder of only 0, 1, 2, or 4 when divided by 7. Suppose the sides of the perfect cuboid are x, y, z. Then x^2 mod 7, y^2 mod 7, z^2 mod 7 can each take one of the values {0, 1, 2, 4}, leading to 64 possible triples.

But some can be ruled out because, for example, $(x^2 + y^2)$ mod 7 must also be a square mod 7 and thus fall within the same set. For instance, if x^2 mod 7 = 1 and y^2 mod 7 = 2, then $(x^2 + y^2)$ mod 7 = 5, which is not a possible square so that combination is impossible. By eliminating such cases, one finds that at least one of x, y, z must have remainder 0 that is, one side must be divisible by 7.

Results about parity and divisibility like these have practical computational value: they allow researchers to rule out huge numbers of impossible cases. However, it has already been shown that if a perfect cuboid exists, its smallest side must be longer than 10^{11} so even with modern computers, a brute-force search is not easy.

There are also many statements that have been shown to be equivalent to the existence or perfect cuboids, or consequences of a solution existing to the perfect cuboid problem, which may also be approaches taken to prove or disprove their existence. Over the years, mathematicians have found many statements that are equivalent to, or would follow from, the existence of a perfect cuboid. Exploring these connections is another route toward solving the problem. For example, mathematician Florian Luca has shown that the existence of a perfect cuboid is equivalent to the existence of a triangle in which each side is a perfect square and each angle bisector has integer length.

Like all good mathematical puzzles, the search for perfect cuboids has inspired a range of related questions. For instance, what if we require any six of the seven lengths (three sides, three face diagonals, and one space diagonal) to be integers—what solutions exist then? Or we can ask whether perfect parallelepipeds three-dimensional

figures where all sides, face d diagonals, and the space diagonal have integer length—exist. In a 2009 paper with the spoiler-filled title “Perfect Parallelepipeds Exist,” mathematicians Jorge Sawyer and Clifford Reiter used brute-force techniques to find some examples. They also proposed further questions, such as whether such figures can have rational coordinates or integer volume.

Unlike many open problems in mathematics, the perfect cuboid question is easy to state and visualize. New attempts and claimed proofs still appear on resources like arXiv, but none have yet been verified to be correct. Given the number of years for which the question has remained open, settling it may require heavier mathematical machinery. However, it is inviting and intriguing enough for anyone with some exposure to elementary number theory to play around with.

Written by - TULSI SRINIVASAN (FACULTY)

Torus made using PHiZZ units

A HARMONY OF LANGUAGE AND MATHEMATICS

A lot of students tend to see Mathematics and English as two separate subjects, two separate disciplines. However, research shows that there is a correlation between learning English and learning Mathematics.

By bringing attention to the connection between Mathematics and English from an early age, students can perform better in Mathematics.

A language is defined as "a set of rules relating symbols to meaning which allow the forming of an infinite number of utterances from a finite number of elements".The English Language consists of 26 alphabets, 16 punctuation marks, and a handful of other special characters. There are a finite number of elements - characters, and there are infinitely many ways these can be arranged- words, sentences, paragraphs, books, speeches and so on. All of this adheres to a certain set of rules such as grammar and phonetics.

Similarly, Mathematics can be viewed as a language consisting of a set of elements: numbers, arithmetic symbols and symbols relating to other branches of Math. Again, this is a finite set of characters that are arranged in infinitely many ways, with infinite numbers, different equations, and infinite possibilities, all based on certain rules of Mathematics.

However, learning English is treated as learning a language, but Mathematics isn't treated similarly in most educational institutions. In fact, Mathematics and English tend to be looked at as opposites by students. According to Ostler. E. and Bruckner. J, "Educators share a common notion that as learners, we spend the first three to five years of our academic lives learning to read, and the remaining years of our lives reading to learn."

The foundation to learning English, or any other language for that matter, is learning how to read the language. Similar importance to "reading" Mathematics isn't given over crucial years of education to students. Mathematics syllabus and teaching methods are extremely streamlined, not focusing on the basics as much and giving more importance to more complex topics such as Calculus and Trigonometry.

When teaching Mathematics to students that are inclined to be better at English, a useful strategy to employ would be to relate English language tools to Mathematical notions. For example, when we look at narrative writing, there is a "formula" that is followed. There is an exposition, an incident, rising

action, a dilemma, climax, and a denouement.

Similarly, when it comes to Mathematics, solving a problem can come with a formula, or a way to solve a problem. For example, The Principle of Mathematical Induction is a series of steps to prove a theorem. When these steps are fulfilled, you get the answer.

When approached with the same mindset, both English and Mathematics can be easy to learn. To see solving a problem as writing a story could help in improvement. Language can also benefit Mathematics by learning the register and grammar of Mathematics. The register of Mathematics includes symbolic notation, oral and written language, and graphs and visual displays.

Learning the register of Mathematics allows students to grasp problems presented to them easier. Verbalizing problems and reading word problems with more care can give students a deeper understanding that aids in problem solving.

The language in which an instructor teaches Mathematics is extremely important. When taught in languages in which a Mathematical register is fully developed, students are more likely to understand it and be able to solve problems. For example, Adler (1998) talks about a teacher in a South African classroom in Tswana teaching advanced mathematics where the teacher "runs out of words" explaining a concept, as the native language has not developed a mathematical register.

English on the other hand, has built an extensive vocabulary and register with Mathematics. Teaching and practicing mathematics using this register can enhance a student's capabilities in problem solving.

Bruckner, J. and Ostler, C. E. constructed a table relating English and Mathematical categories and the purpose of these categories.

English	Mathematics	Purpose
Noun/Pronoun	Variable/Constant	Antecedent object or idea
Verb	Operator	Action, function, operation
Adjective/Adverbs	Coefficient/Exponent	Modifier or descriptor
Conjunction	Groupings	Connects/joins phrases

Figure 1. Table

Using this table we can construct mathematical sentences. For example, John sold 5 chocolates and 2 lollipops can be written as S(5c + 2l) where S() is the function/action of selling (the verb), c is a chocolate, with an adjective of 5, and l is the lollipops.

Similarly, writing functions, equations, and inequalities can be thought of as constructing sentences in Mathematics. "Redundancy is one characteristic of ordinary English that has a significant influence on how students (mis)read mathematical English because ordinary English has a high degree of it". While English tends to be descriptive, giving plenty of context, Mathematics tends

to be the opposite; The “sentences” being straightforward and to the point, leaving more room for interpretation, and hence more room for error.

When students focus on learning the nuances, then they can read the mathematical sentences with higher fluency. All these tools and comparisons mentioned above focus on the reading and writing of the mathematical language. Not only are we letting Mathematics be a medium of communication, we are also learning how to use Mathematics to communicate.

When instructors teach these tools to students, students can better understand the language of Mathematics. The National Council of Teachers of Mathematics was one of the first organizations to accept and apply this line of thinking. While the nuances of “Mathematics as communication” is still being discussed and solidified, it is clear that this is the line of thought that The National Council of Teachers of Mathematics would like to follow.

These skills can be nurtured in classrooms when the awareness of the correlation is brought to the teacher’s attention. When a course teaches a student to construct and understand mathematical sentences, learn mathematical registers, and use them to write mathematical stories, they stop learning Mathematics; They rather learn the language.

Language and communication are something that comes naturally to children, learning to communicate from birth. This method of teaching appeals to that nature, bringing in cohesiveness between Mathematics and Language. As the interdependence is enhanced, both subjects and the understanding of both these subjects are strengthened in a student.

Therefore, I believe that teachers across the world should apply these methods to better the learning of their students.

Written by - VAGMI

THE TEAM

MANAGING EDITIOR
ANIRUDH N. RAO

DESIGN
CHAITANYASRI KOKUL
MAITHRI MOGADALAI

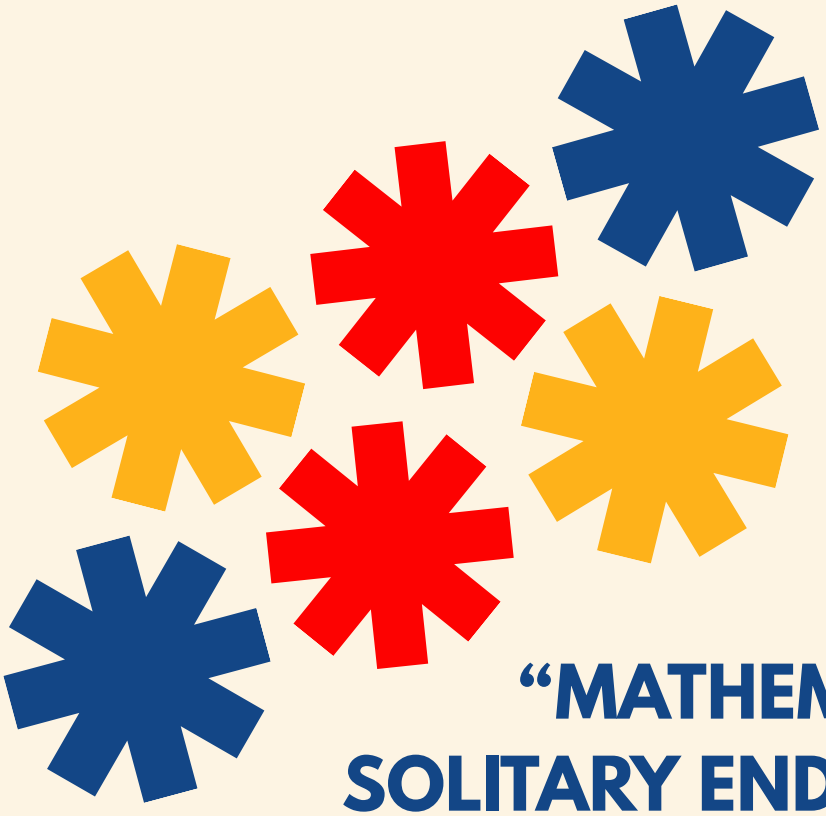
FACULTY
VIJAY RAVIKUMAR

MATHAAPU FONT (FRONT PAGE)
CHAITANYASRI KOKUL

EDITORIAL
ANIRUDH N. RAO
ANIRUDDH RAGHAVAN
CHAITANYASRI KOKUL
MAAYA KASHYAP
MAITHRI MOGADALAI
SHREYA JOSEPH

TRANSLATION
ANIRUDH N. RAO

TESSALATION (FRONT PAGE)
MAITHRI MOGADALAI



"MATHEMATICS IS NOT A SOLITARY ENDEAVOUR; IT IS A SHARED LANGUAGE."
— HENRI POINCARÉ

ACKNOWLEDGEMENTS

We would like to thank to begin by thanking our Contributors

Aniruddh Ragahvan, Arpit, Chaitanyasri Kokul, Iniya A, Maithri Mogadalai, Pranava Shastry, Pranavashree, Rayirth Sen, Roshan Noah, Saipriya, Shanta Bhushan, Sohan Karnagshettru, Tulsi Srinivasan and Vagmi Bhat.

We would like to thank the rest of the Math community at Azim Premji University, Bengaluru, for their time, support and spirit of collaboration.