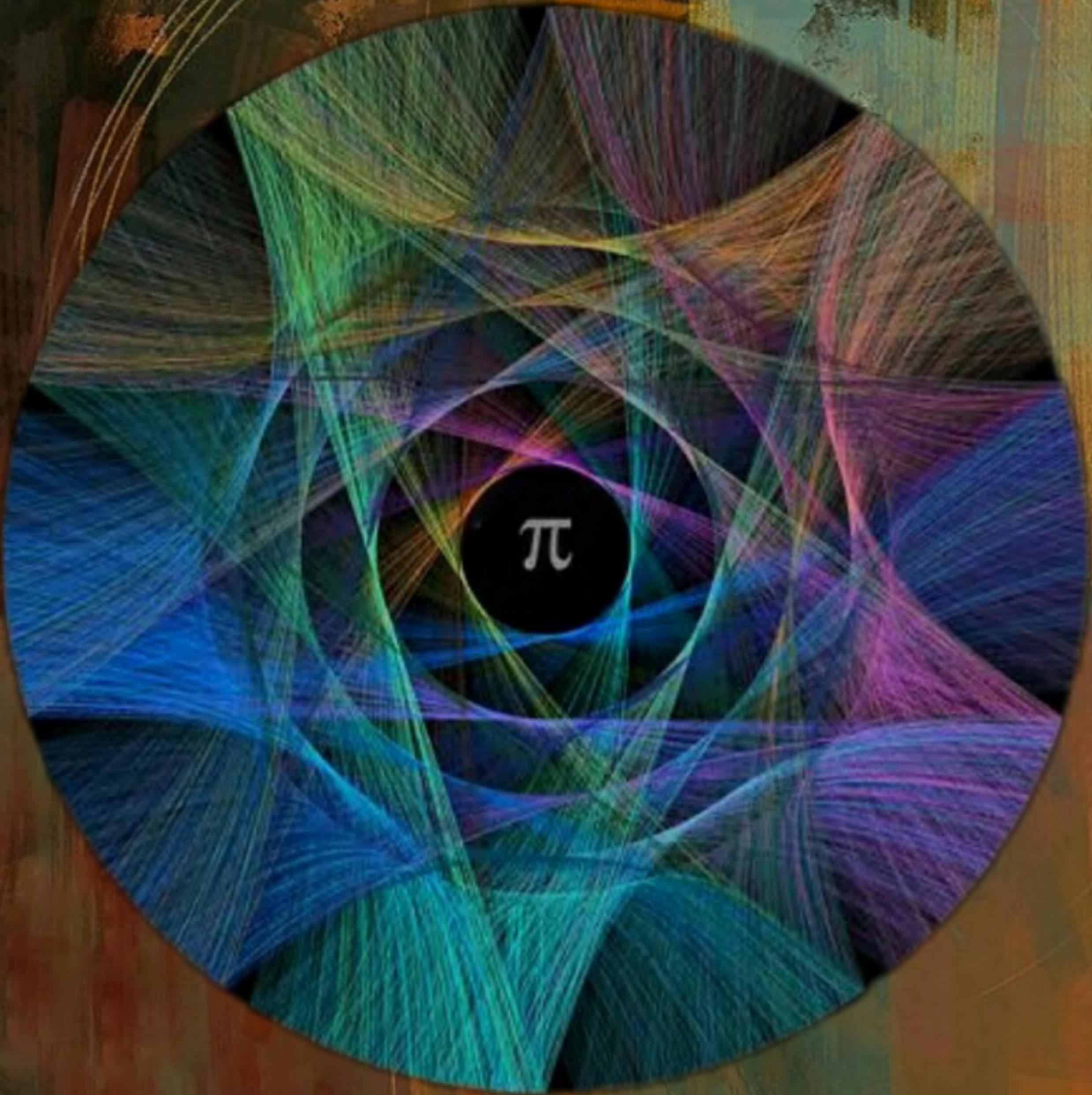
VOLUME 1, 2020

AANKALAN

THE ANNUAL JOURNAL OF DEPARTMENT OF MATHEMATICS, HANSRAJ COLLEGE



SET THEORY VERSUS CONTINUUM HYPOTHESIS

INTERVIEW WITH DR. S.R. ARORA

KAKURO: A PUZZLE

AANKALAN

Department of Mathematics

Hansraj College

Volume 1, 2020

From the Principal's Desk

It is an absolute pleasure and delight for me to pen down the introductory lines for 'Aankalan 2020': the first edition of the Annual Journal of our Mathematics Department.

Hansraj College has always been a unique blend of modern education and our traditional Vedic values. Mathematics department is one of the largest departments of the college, having some of the best faculty members and brightest of student minds. This institute has perpetually been supported by the talents and enthusiasm of young and budding mathematicians. This is what has always been the strength of the college. Breaking the shackles of the existing myths and conventional beliefs about mathematics, the entire editorial team of the department has worked relentlessly, with the keenest attention to details. It is evident that they did their utmost to bring out this journal as a concoction of fun and learning. The meticulous efforts put in by the students and teachers to bring out the best of this journal are truly appreciable.

I would also like to extend my gratitude towards Dr. Preeti Dharmarha for taking up such an initiative and guiding the young minds throughout the entire process, leaving no stone unturned. At every point, she was the one who ensured that this effort definitely comes through with flying colors.

May this journal reach untouched heights, and bring glory to our meritorious Mathematics Department and to the college itself! Many congratulations to the Editorial Board and the department.

Best Wishes and Warm Regards

Dr. Rama
Principal
Hansraj College

Note from Teacher-in-Charge

Mathematics has always been a fascinating subject, and it gives the department immense joy and delight to present before you the first volume of its journal. I extend my heartfelt congratulations to the newly appointed Editorial Board of the Mathematics Department Journal, 'Aankalan', who have successfully compiled this collection of mathematical articles and facts under the mentorship of Dr. Preeti Dharmarha. The publishing and launch of this journal would not have been possible without the support of our respected Principal, Dr. Rama.

The majority of the articles presented in this journal have been written by the students of various years of the undergraduate honours course in Mathematics. In the process of writing a conceptually sound and intellectually solid article, one learns many skills which help greatly in the sphere of academics. The journal, by giving a platform for the exhibition of such articles, will surely encourage and uplift the students.

Learning in modern times is not limited to just books and classrooms. Students need an exposure to the world beyond the classroom for a wholesome teaching-learning experience. I am happy that the entire process of creation and formulation of Aankalan provided one such experience to the members of the Editorial Board. The compilation is a major part of any academic publication, and the Editorial Team has done a fine job in this aspect too. The content is presented in a very systematic way, and the enthusiasm shown by them to launch this journal is applaudable.

I personally commend the Board for this great achievement, and wish that the precedent they have set will be followed and improved upon by the students of our department every year. Let's join hands to encourage such academic initiatives which will make the department as well as our college proud.

Dr. Harjeet Arora
Associate Professor

Note from Head of Advisory Editorial Board

It gives me immense delight and satisfaction in having been able to successfully guide the Editorial Team of extremely dedicated and focused students in bringing out ‘Aankalan’, the First Academic Publication of the Department. This would not have been possible if we did not have the support and will of our ever dynamic and encouraging Principal Dr. Rama.

I congratulate all the team members: Aman, Ashutosh, Gaurav, Ishita, Anvesha, Samarth and Utcarsh, who, despite the hurdles which arose from time to time, consistently devoted their efforts unabated.

The meaning of education has evolved these days and is not just limited to the traditional classroom. Modern education has a much wider horizon both in terms of teaching and learning, and in its role to prepare the learner for global leadership. To meet the new challenges in any field, one has to keep oneself updated with the new trends and new knowledge which becomes possible only when one develops a scientific aptitude of researching and exploring.

The undergraduate studies are the stepping stone to one’s career. Academic excellence is a hallmark of the Department of Mathematics at Hansraj College, with its foundations laid by very fine mathematicians such as Shanti Narayan ji, Prof. M.C. Puri, Prof. S. C. Arora and Dr. S. R. Arora. With Dr. Harbans Lal, Dr. K. L. Bhatla, Dr. N.M. Kapoor, Dr. Satpal, and Sh. J. P. Pruthi as guiding lights, the department has always strove to nurture and create global leaders. The department aspires that its students get the most out of their time studying at the college through classroom teaching, combined with co-curricular experiences.

The dream and desire of providing a learning platform to students beyond the classroom have been occupying my thoughts since the past year. What is amazing is that sharing my idea with department colleagues and Student Council of the Department was received with great enthusiasm. Our team got full support from Dr. Harjeet Arora as Teacher-in-Charge and Dr. Arvind as Convenor of the Departmental Student Council. Dr. Harjeet Arora, Mrs. Amita Aggarwal, Dr. Rakesh Batra and Dr. Mukund Madhav Mishra readily agreed to contribute as Advisory Editorial Board. Their inputs and thorough feedback aided immensely in improving the content.

This publication will greatly benefit the students in honing their research and exploratory skills, making them more confident. It will also cultivate and foster their penning down skills, equipping them with insight in the art of creating quality academic content. I am certain that this launching pad will provide wings to the inquisitive minds and inspire the learner to dive in the ocean of knowledge.

Dr. Preeti Dharmarha
Associate Professor

From the Editorial Board

Standing: (from left) **Utcarsh Mathur, Anvesha Kushwah, Samarth Rajput**
Sitting: (from left) **Ishita Srivastava, Aman Chaudhary, Abhishek Jain** (Head of Academic Activities), **Ashutosh Maurya, Gaurav Kumar**

"Mathematics is scary."
"It's all about hefty calculations and a list of never ending, lengthy formulae."
"It's a nightmare!"
"I really wish I could get rid of it soon."

Pretty common complaints, no? And all of us have heard them, or maybe even felt so, at some point in our lives. There is a set of people who consider mathematics to be the toughest thing on earth, whereas, the set complement consists of people for whom life is incomplete without this absolutely amazing subject. Apart from, of course, one's personal inclinations, have you ever tried to figure out the reason for this conflict in views? Yes, the answer is '*perception*'. So long as you consider maths to start and end at huge numbers and lengthy proofs, it would certainly be difficult for you to see how beautiful it actually is. All that it takes for you to appreciate its beauty is: "Even if just for once, try to dive deeper into this subject. You will realize that cumbersome calculations are just a part of mathematics, and not mathematics itself. There is so much more to it; so much more to know about, so much more to learn about". And that will be the moment when you start falling in love with it.

This journal is our first attempt at trying to provide a different perspective to mathematics. Right from including articles about a lot of interesting and captivating topics of pure and applied mathematics, to having engrossing puzzles and brain teasers, to sharing with you the journey and experiences of someone who has devoted his entire life to mathematics, trust us when we say that this journal truly has a LOT to offer to its readers. This will certainly be a roller coaster ride for you, challenging at some places, fun at others, but definitely a very different and new learning experience altogether.

So, for all those who are yet to discover the beauty and expanse of this subject, here is a small effort from all of us to bring out how maths can be a part of your daily life, and how everything around you is indeed, directly or indirectly connected to mathematics. Hope this will help you drop some preconceptions, and will assist you in looking at mathematics from a whole new perspective!

Sincere Regards
The Editorial Team
Aankalan-2020

The Team

“Maine zindagi mein bas ek hi baat seekhi hai . . . MEHNAT KARNA”

Dr. S.R. Arora and his wife, **Mrs. Naresh Arora** with Editorial Board representatives, (from left) **Utcarsh Mathur, Anvesha Kushwah, Ishita Srivastava** and **Gaurav Kumar**

It was a matter of great pride for the Editorial Board of the Department of Mathematics to hold a two-hour long interaction with a renowned personality in the world of mathematics, **Dr. S. R. Arora**, former Principal of Hansraj College. Dr. Arora has had the honor of holding several prestigious positions during his 48 year long professional career. Some of these include: Secretary of DAV College Managing Committee (current), Director of New Delhi Institute of Management (NDIM) from 2010 to 2017, and Vice Principal of Hansraj College, apart from being the college Bursar in 2001. A strict disciplinarian, hard work and supreme dedication to his duties have been the founding pillars of his life. A very warm hearted and cordial person, sir was kind enough to share a lot of bittersweet experiences of his life with us. Listening to Dr. Arora and his wife Mrs. Naresh Arora, we couldn’t help but feel awed by how far persistence and adherence to principles can take one in life, not just as a professional, but as an individual as well.
The interview was conducted by representatives of the Editorial Board, **Ishita Srivastava, Gaurav Kumar, Utcarsh Mathur and Anvesha Kushwah** at his residence in Gurugram, Haryana. Here we take down the answers to some of the most interesting parts of our conversation with them.

Ishita: We would like to embark upon the conversation with you telling us something about your journey and association with Mathematics before and after becoming a part of HRC.

Dr. Arora: My passion for mathematics developed in grade nine. I remember, my teacher used to get me books of advanced levels so as to provide me with a better understanding of concepts. By 11$^{\text{th}}$ standard, I had already made up my mind to pursue Mathematics. Thereafter, in 1961, I enrolled for honors in Mathematics at Hansraj College. I went on to complete my Masters from that very institute in 1966. Back then, Hansraj had a tradition of appointing the university topper as a lecturer. Being a top scorer of that year, I was asked by the then Principal, Dr.Shanti Narayan, to join as a faculty member. I served the college in the capacity of a Professor, Bursar, Vice-Principal and then finally retired as Principal in 2009. This 48-year long journey has made up a significant portion of my life.

Gaurav: Whom did you idolize as a mathematician or as a person during your student life?

Dr. Arora: I had a bunch of good teachers like Prof. MC Puri, Prof. Shanti Narayan, Dr. Lakhpat Rai and Dr. PV Mehra to guide and mentor my academic life. Undoubtedly, I credit my superb mathematical journey to these meticulous professors whom I was lucky to encounter quite early in life. I fondly remember my mentor, Prof. Munish Chander Puri. He was not just one of the best teachers, but also one among the finest individuals I've ever come across. He served at Hansraj College until 1984 and then joined IIT-D. I had always been amongst his favourite students. During the five years of my student life at Hansraj, I became extremely close to him. From having him as a teacher during my undergraduate and postgraduate days, to being with him even after becoming a lecturer in the same college, my association with Prof. Puri has been really long and worth cherishing. I feel truly blessed to have someone like him to guide me through most of my journey. Unfortunately, Prof. Puri was killed in a terrorist attack on 29th December 2005, at the 38th Annual Convention of ORSI at IISc, Bangalore. He was shot while attempting to save his students. Such a charismatic personality he was! He will always remain dear in my memories.

Anvesha: How would you rate the various experiences you had with HRC: being a student, a lecturer and a principal?

Dr. Arora: Despite having been associated with the college in different capacities for almost 50 years, I find it almost impossible to compare the various roles I played and the responsibilities I held during this journey with HRC. I had some of the best days of my life as a student. I had the responsibility of shaping the future of so many students during my lectureship days. And I had some of the toughest and most crucial challenges of life while I served as the principal. Each of these roles demands a different version of one's personality, and I have always tried to do justice to every role my academic and professional life has offered me. Like everything in life, each of these experiences came with their own set of pros and cons, and it's not easy for me to choose one over the other.

Utcarsh: What were the major highlights of your tenure as a professor at Hansraj? Can you also share some of the challenges you faced after you became the Principal of the college?

Dr. Arora: I treated all the college students as my own children. I considered it my prime responsibility to ensure that they did not face any problem while they were away from home. From taking care of the most basic amenities, to resolving the bigger problems with academics and life, I always ensured that students felt comfortable and satisfied with the resources provided to them. Still, there were certain things that came up as major challenges for me. I recall one particular day when due to certain reasons, the hostel food was not up to the mark. The agitated students came to me to complain about the food quality at midnight. I asked them to wait, while my wife prepared food for them. Even at that hour, we were willing to help them out, in every possible way. Another incident that comes to mind is an altercation between the hostellers of Hansraj and Kirori Mal College. The unfortunate incident happened late at night, and as it turned violent, the Delhi Police had to be involved. As soon as I was informed about the ongoing disruption, I reached the college campus and immediately called the Hansraj students to the college ground. They were quick to comply, and the matter was soon resolved.

Mrs. Arora: Although I tried to convince him that going out amidst such violence can be really fraught with danger. But for him, his college and students were the utmost priority. What we saw there was really disheartening. By the time things settled down and we reached back home, it was nearly four in the morning. But he still ensured that he did not miss his 8 a.m. lecture the very next morning.

Dr. Arora: These were some of the most challenging parts of my career as a principal, but I believe these are the things that have helped me shape my personality.

Gaurav: What major reforms did you bring in as the Principal of the college?

Dr. Arora: Every place, however good it may be, requires some changes and some modifications to help it grow and prosper. I also introduced some such reforms to make Hansraj run more efficiently. Firstly, I ascertained that the college library should start functioning early in the morning and stay open until midnight for the convenience of the students. I also made sure that students had enough study material to help them with academics. All attempts were made to ensure that whatever additional books our students required were made available to them the very next day.
I also got the college auditorium renovated. Further, when a group of students intimated me about the need for a seminar room, we realized that we didn't have sufficient space to get it constructed separately. So, I got the intervening wall demolished and got the adjacent rooms connected. That is how Hansraj got its first Seminar Hall!

I always wanted my students to keep pushing their limits. Just like admission cutoffs, I thought that hostel cutoffs would also motivate them to excel academically. Plus, since we had a limited number of rooms, this would also enable us to have a strong criterion for allotting rooms to students. So, I introduced the cutoff system in the hostel. Although this initiative was opposed by DUSU and some students, things eventually settled, and the system continues even today.

Ishita: Every successful person has some hardships in life. We are sure that there must have been certain tough times that moulded your personality. Can you share such difficulties you had to face during your student and early college life?

Dr. Arora: I had always been a bright student throughout school. Belonging to a very humble background, my family did not have sufficient resources to support my higher education. We didn't even have electricity connections at home back then. The days, when my friend and I used to sit at the petrol pumps near my house as late as two in the morning, just because the petrol pump had street lights, are still bright in my memory.
When I came to seek admission to Hansraj, I put my faith in Prof. Shanti Narayan, telling him about my financial limitations. All he asked was if I had secured a distinction in Mathematics. When I replied in affirmative, he asked me to fill out the admission form and join immediately, and assured me that I could pay my fees whenever I had sufficient money. I'll be eternally grateful to him for his help. I will always remember Prof. Shanti Narayan as a man of mathematics.

Gaurav: Would you please throw some light on your academic career?

Dr. Arora: As I've already told you, I was certain that I wanted to pursue Mathematics from 11th grade. I worked really hard throughout the five years of my college life and performed well academically. In my research, I came up with the Airline Crew Scheduling Problem. With a given number of aircraft and crew members, one had to decide their optimum scheduling. It was a Set Covering Problem and time taken should be minimum. This was extended to the Vehicle Routing Problem. I was very fond of Mechanics, Statistics, Differential Equations and Operations Research. I'd had a perfect score in mechanics, stats and differential equations. There was never a time when I felt that I am bored with mathematics. I have still safely stored all my books on OR and statistics, and I like to go through them every now and then! It was very satisfying to work with wonderful students and watch them bloom and achieve success in their lives, like Dr. Harjeet Arora, Dr. Preeti Dharmarha, Dr. Neelam Malhotra and many more. 15 students did Ph.D. and 25 did their M.Phil. under my guidance. I wrote more than 100 research papers all through these years.

Anvesha: What advice would you give to maths lovers concerning their academic pursuits and life in general?

Dr. Arora: *Maths insaan bana deti hai.* I would advise the students to try to understand this subject with real life examples. Even though we had few resources, we used to make full use of them. Students nowadays have better resources compared to what we had in our time. If they work with complete dedication, persistence, and sincerity, they will definitely achieve whatever they aim for.

Mathematics is a conceptual subject and before getting into it, one needs to understand that there is no place for rote learning or cramming here. This is something very logical. And as I already told you, my life predominantly revolves around the principle of hard work and supreme dedication towards my responsibilities and complete honesty with my career and professional life. I would advise the students to do the same.

Mrs. Arora: Experience comes from your dedication and hard work. This is true for everything in life.

"Aur phir humne to zindagi mein bas ek hi baat seekhi hai... Mehnat karna."

"Meeting Prof. S. R. Arora and Mrs. Naresh Arora was an absolute pleasure. Apart from other things, his love for his students is one of the most admirable traits of his personality. Be it for mathematicians, or non-mathematicians, his journey is an inspiration for all of us alike!"
Ishita Srivastava

"Sir has a charismatic figure. He had a wonderful academic life and seems quite content with it, which is rare to find these days. His love for maths is fascinating to me."
Gaurav Kumar

"Despite being a renowned personality, he is so down to earth and is a true example for us to look up to and take inspiration from. We need to multiply the words 'thank you' an infinite number of times to match it with his fatherly concern."
Anvesha Kushwah

"Always sporting a smile, Mr. and Mrs. Arora are one of the kindest, warmest and most radiant people I've come across. Their compassion and involvement in the lives of their students is admirable. Their outlook towards life is truly inspirational!"
Utcarsh Mathur

Contents

Set Theory versus Continuum Hypothesis

Dr. Preeti Dharmarha
Associate Professor

Since ancient times, the role of Mathematics for rational enquiry of the truth in the foundation of all scientific thoughts has always been acknowledged. Dawn of 19th century was marked by the beginning of systematic search for the foundations of Mathematics and after going through a series of difficulties in the early 20th century, the mathematical discoveries started stabilizing resulting in a large, intelligible body of mathematical knowledge which is still providing impetus to active research fields.

The wheel in the late nineteenth century turned in a new direction when a mathematical theory of sets was crafted and advanced by the renowned mathematician, Georg Cantor (1845-1918). The seed of this theory was sown when Cantor proved a key theorem in real analysis, through which a method for creating real number sets that elaborated on a countless iteration of the limit operation, was introduced. The novelty of this proof steered him into an insight of sets of real numbers and to the abstraction of his set theory. The conception of ideas given by Cantor has now permeated mathematics, offering an adaptable means for exploring even deeper concepts of infinity and sets of infinite measure.
The credit for investigating the following question goes to Cantor:

Can the concept of "size" be extended to infinite sets?

The uncountability of the set of real numbers led Cantor to establish the following result: the existence of "infinitely many different infinites", which had an obvious mathematical and philosophical implication.

In 1874, Cantor established that the set of natural numbers and the set of algebraic numbers were in one-to-one correspondence. At the same time, he established that no such one-to-one correspondence existed between sets of natural and real numbers. Cantor tried to explore the possibility of the existence of any infinite sets of real numbers that corresponded in one-to-one manner with the set of natural numbers, but not with the real numbers set. In 1878, the Continuum Hypothesis was proclaimed by Cantor after introducing uncountable sets, which stated that: **"every infinite set of real numbers matched in size with either the set of natural numbers or the entire set of real numbers and no set of intermediate size existed"**. Since this result led to the conclusion that there were more than one level of infinity, it faced opposition by many mathematicians of that time. Some denied its existence based on their understanding that infinity was a non-legitimate mathematical abstraction. On the other hand, Christian theologians held the view that his work was contrary to the uniqueness of the absolute infinity in the nature of God.

Throughout most of his career, Cantor grappled, without any success, to find a resolution to the Continuum Hypothesis. However, the problem continued to remain as one of the most prominent and baffling problems of the 20th century. In 1940, mathematician Kurt Gödel showed that it couldn't be disproved within the usual axioms of set theory. In the 1960s, mathematician Paul Cohen showed that the continuum hypothesis can't be proved by set theory. This won Cohen the Fields Medal, the highest honor in mathematics.

Eventually, Cantor's contribution to mathematical investigations was acknowledged. David Hilbert, a prominent mathematician of the 20^{th} century, described Cantor's work as "the finest creation of mathematical genius and one of the unbeatable achievements of purely scholarly human activity".

Hilbert, who had expertise in posing mathematical questions, published 23 open questions in the year 1900. Many have been solved but some still remain unanswered. But all endeavors to seek a solution to these problems have resulted in some very deep mathematics. Riemann hypothesis is one such example. The act lies in asking a good question.

In 1946, he presented 10 of these 23 problems at the first major international gathering of mathematics after the World War II, 'The Princeton University Bicentennial Conference on Problems of Mathematics'. The problem which topped the list still remains unreturned, and it is the famous 'Continuum Hypothesis'.

After Cantor's demise, most of the researchers in the field of set theory declared that the Continuum Hypothesis was unresolvable. From Cantor until 1940, Continuum remained the focus of the advancement in Set Theory. Although both, the set of natural numbers and that of real numbers, are infinite, there are more real numbers than the natural numbers; this commenced the journey to the exploration of different sizes of infinity. However, Cantor's ideas gained momentum and set theory gained significance in the unearthing and creation of new mathematical results, especially in fields like the theory of functions and measure theory. The efficacy of this tool regarding traditional mathematics was realized by the mathematical community and received acceptance due to corresponding change in the attitudes. The theory of abstract sets propounded by Cantor would revolutionize the mathematical progress in due course.

There are two general approaches to set theory "**Naïve set theory**" credited to Cantor and "**Axiomatic set theory**" which is due to Zermelo-Fraenkel (**ZFC**). The most important difference in the two approaches is that the naive theory doesn't have much by way of axioms.
As stated by Cantor:

> "A set is a gathering together into a whole of definite, distinct objects of our perception or of our thought-which are called elements of the set."

Cantor did not define the concept of 'set' in his Naïve set theory. The nature of elements of the sets was generally ignored. While the set was considered as a collection of objects, it was also presumed that any object can be a member of a set. "Naïve set theory" in the sense of naïve theory is a non-formalized theory wherein sets and operations on sets are styled using natural language. The terms and, or, if . . . then, not, for some, for every, are the same as in ordinary mathematics.

- **Membership**: x belongs to a set A, if x is a member of the set, and is denoted by $x \in A$.
- **Equality**: If every element of a set A is in a set B and every element of B is in A, sets A and B are defined to be equal.
- **Empty set**: The empty set, often denoted ϕ and sometimes $\{\}$, is a set with no members at all. Since the empty set has no members it is unique but it can be a member of other sets. This justifies $\phi \neq \{\phi\}$, because the former has no members and the latter has one member.
- **Specifying sets**: A set is defined extensionally by enclosing a list of its elements between curly braces and it is sufficient to describe the set.
- **Subsets**: Given two sets A and B, A is a subset of B if every element of A is also an element of B. In particular, each set B is a subset of itself; a subset of B that is not equal to B is called a proper subset.
  If A is a subset of B, then one can also say that B is a superset of A, that A is contained in B, or that B contains A.
- **Unions, Intersections, and Relative Complements**: Given two sets A and B, the set consisting of all objects which are elements of A or of B or of both is their union, denoted by $A \cup B$.

The set $A \cap B$ of all elements which are both in A and in B is the intersection of A and B. Finally, the set theoretic difference of A and B or the relative complement of B relative to A, is the set of all objects that belong to A but not to B. It is written as $A \backslash B$ or $A - B$.

- **Ordered pairs and Cartesian products**: Intuitively, it is a collection of two objects where one can be distinguished as the first element and the other as the second element with the fundamental property that, two ordered pairs are equal if and only if their first elements are equal and their second elements are equal.

Paradoxes are witnessed, without restriction, upon assuming that any property may be used to form a set, a common example being Russell's paradox; there is no set consisting of "all sets that do not contain themselves".

More set theories emerged from the questions raised on the unambiguity and consistency of what exactly comprised and what did not comprise a set. One such widely accepted theory is Zermelo-Fraenkel set theory.

An axiomatic structure was advocated by Ernst Zermelo and Abraham Fraenkel so as to frame a theory of sets restricting paradoxes such as Russell's paradox in the early twentieth century.

ZFC is the truncation of Zermelo-Fraenkel set theory with the debatable axiom of choice counted in, where C denotes "choice", and ZF stands for the axioms of Zermelo-Fraenkel set theory with the axiom of choice omitted. Following axioms comprise ZFC set theory:

- **Axiom A1 (Axiom of extent)**: For the classes x, A and B, $[A = B] \Leftrightarrow [x \in A \Leftrightarrow x \in B]$
- **Axiom A2 (Axiom of class construction)**: Let $P(x)$ designate a statement about x which can be expressed entirely in terms of the symbols $\in, \vee, \wedge, \neg, \rightarrow, \forall$, brackets and variables $x, y, z, \ldots, A, B, \ldots$. Then there exists a class C which consists of all the elements x which satisfy $P(x)$.
- **Axiom A3 (Axiom of pair)**: If A and B are sets, then the doubleton $\{A, B\}$ is a set.
- **Axiom A4 (Axiom of subsets)**: If S is a set and ϕ is a formula describing a particular property, then the class of all sets in S which satisfy this property ϕ is a set. More succinctly, every subclass of a set of sets is a set.
- **Axiom A5 (Axiom of power set)**: If A is a set, then the power set $P(A)$ is a set.
- **Axiom A6 (Axiom of union)**: For a set of sets A, $\bigcup_{C \in A} C$ is a set.
- **Axiom A7 (Axiom of replacement)**: Let A be a set. Let $\phi(x, y)$ be a formula which associates to each element x of A an element y in such a way that whenever both $\phi(x, y)$ and $\phi(x, z)$ hold true, $y = z$. Then there exists a set B that contains all elements y such that $\phi(x, y)$ holds true for some $x \in A$.
- **Axiom A8 (Axiom of infinity)**: There exists a non-empty class A called a set that satisfies the condition: $X \in A \Rightarrow X \cup \{X\} \in A$. (A set satisfying this condition is called a successor set or an inductive set.)
- **Axiom A9 (Axiom of regularity)**: Every non-empty set A contains an element x whose intersection with A is empty.

Another "special" and initially controversial axiom 'Axiom of choice' is usually stated separately.

Axiom of choice: For every set A of non-empty sets there is a function f, which associates to every set A in A, an element $a \in A$.

Sets have abundant significance in mathematics. In modern formal treatments, sets are used to define almost all mathematical objects like numbers, functions, relations, etc. Naïve set theory is sufficient for many reasons, as well as serves as a starting point for more formal treatments. If a naïve set theory correctly identifies the sets permissible to be studied, it is not essentially inconsistent.

Similarly, an axiomatic set theory is neither essentially stable nor essentially free of paradoxes as is evident from Gödel's incompleteness theorems.

The choice between an axiomatic approach and other approaches largely depends on convenience. As far as mathematics in everyday is concerned, informal use of axiomatic set theory may be the best choice. Depending on notation, this informal usage of axiomatic set theory can precisely have the form of naïve set theory, which is noticeably simpler to read, write and grasp.
P.R. Halmos lists these properties as axioms in his book "Naïve Set Theory" as follows:

1. Axiom of extension
2. Axiom of specification
3. Axiom of pairs
4. Axiom of union
5. Axiom of powers.
6. Axiom of infinity
7. Axiom of choice

The humble notion of a set is generally introduced casually and regarded as self-evident. Very deep and magnificent, yet fundamental and humble, the concepts of Set Theory pervade all branches of mathematics. Remarkably, all usual mathematical objects can be represented as sets. For example, within set theory, one can create the natural numbers as well as the real numbers. The formal language of pure set theory allows one to formalize all mathematical notions and arguments. All algebraic structures, functional spaces, vector spaces, and topological spaces can be regarded as sets in the universe of sets. Therefore, while mathematical theorems can be regarded as statements about sets, they can also be proven from ZFC, which, in turn, are the axioms of set theory. One can, hence, infer that mathematics is rooted in set theory.

Since all of conventional mathematics can be developed within set theory, one can view certain results in set theory as being part of **Metamathematics**, the specialized branch within mathematics, which encompasses available mathematical tools to explore the nature and potential of mathematics.

Both aspects of set theory, namely, the mathematical science of the infinite, and the foundation of mathematics, are of philosophical importance.

Bibliography

[1] Axioms and Set Theory: Robert Andre, ISBN 978-09-9384-850-6

[2] Article. Can the Continuum Hypothesis be Solved: Juliette Kennedy

[3] Wiki. Foundations of Mathematics

[4] Internet Encyclopedia of Philosophy (IEP)

[5] Wiki. Naïve Set Theory

[6] Stanford Encyclopedia of Philosophy

The Law of Excluded Middle

Shivam Baurai
B.Sc. (H) Mathematics, 2$^{\text{nd}}$ Year

This is an assessment of the much debated law of excluded middle, which has an intimate relationship with mathematical reasoning. This article will attempt to describe this law, establish its role in mathematics and explore the arguments against the law. An argument against the criticism will be provided to maintain neutrality in this discussion; this article is not written to take any particular side, it is written to introduce the field of metamathematics, using fairly familiar concepts.

This article refers to works of formal logic and philosophy. Both fields are treated to make them as irrelevant as possible for the purpose of this article, which is achieved by giving simplified, and not technical, explanations of concepts belonging to these fields.

The references given in the article provide a detailed discussion of the concepts this article introduces. The references, the reader will find, pertain mostly to the fields of logic and mathematical philosophy. Before beginning, it is important to introduce the ideas that are prerequisites for this article.

Following is a list of important symbols:

- $\mathbf{p}$: a proposition. In simple terms, this is a statement. For example, "This car is red".
- $\sim$: This symbol denotes negation. For example, $\sim\mathbf{p}$ reads "This car is not red".
- $\circ$: This symbol denotes the logical conjunction "and". The usage is similar to the use of the symbol $\cap$ in set theory. For example, given $\mathbf{p}$: "x is an even number" and $\mathbf{q}$: "x is a prime number", then $\mathbf{p} \circ \mathbf{q}$: "$x$ is an even number that is prime" or "$x = 2$".
- $\vee$: This symbol denotes the logical disjunction "or". The usage is similar to the use of the symbol $\cup$ in set theory. For example, given $\mathbf{p}$: "x is a positive real number" and $\mathbf{q}$: "x is a negative real number", one deduces that $\mathbf{p} \vee \mathbf{q}$: "$x \neq 0$".
- $\Rightarrow$: This symbol denotes implication. $\mathbf{p} \Rightarrow \mathbf{q}$ means that whenever $\mathbf{p}$ is true, $\mathbf{q}$ is true and whenever $\mathbf{p}$ is false, so is $\mathbf{q}$.

Now, we shall state a few important laws/principles/terms:

- **Principle of reductio ad absurdum**: A form of argument, where a proposition is disproven following its implication of the absurd. Symbolically put, the argument follows: Assume $\mathbf{p}$ is true, $\mathbf{p} \Rightarrow \mathbf{q}$, and $\mathbf{p} \Rightarrow\sim \mathbf{q}$. This means that $\mathbf{p} \Rightarrow (\mathbf{q}\circ \sim \mathbf{q})$, which cannot hold true (the proof of this will follow later in the article). For convenience, we shall call this **RAA**.
- **Tautology**: An assertion that is true for every possible interpretation. For example, $\mathbf{p}$: "The ball is green, or it is not green" is true whatever the colour of the ball.
- **De Morgan's Law**: $\sim (\mathbf{p} \circ \mathbf{q}) \Leftrightarrow\sim \mathbf{p}\vee \sim \mathbf{q}$.
- **Principle of vicious-circle**: "Whatever involves all of a collection must not be one of the collection". This principle is posited as an axiom.

Now, we can define the law of excluded middle (**LEM**), which we introduce as an axiom.

Given a proposition, either it is true or its negation is.

Symbolically,

$$\mathbf{p} \vee \sim \mathbf{p}$$

We now introduce the law of non-contradiction as a theorem:

Theorem (Law of non-contradiction - LNC)**.** *A proposition cannot be both true and false at the same time. Symbolically,* $\sim (\mathbf{p} \circ \sim \mathbf{p})$

Proof. Note that $\mathbf{p} \vee \sim \mathbf{p}$ (LEM).
Then, by De Morgan's law $\mathbf{p} \vee \sim \mathbf{p} \Rightarrow \sim (\mathbf{p} \circ \sim \mathbf{q})$. □

It has been shown that **LNC** is deducible from **LEM**. Further, we can now present a basic definition of **LEM**: *Given a proposition, either it is true or false.*
Note that **RAA** is due to **LNC**. In the definition of **RAA**, it was remarked that $\mathbf{p} \circ \sim \mathbf{p}$ is absurd. As per **LNC**, it has been established that this assertion is false, and therefore absurd.
Recall the technique of proof by contradiction. The technique is a direct application of **RAA** and **LEM**. Since it has been shown that **LEM** is responsible for **RAA**, we conclude that proof by contradiction is also due to **LEM**. Any question on the validity of **LEM**, therefore, has huge consequences for mathematics. Not only is the technique of proof by contradiction under the scanner, but a considerable part of mathematical reasoning needs to be revisited.

Validity of the Law of Excluded Middle

Consider the following proposition (**Liar's Paradox**):

I am lying

Let us consider the two possibilities permitted by **LEM**:

1. The proposition is true - This means I am lying, which implies that I am not lying. Therefore, the proposition is false, which cannot happen (**LNC**).

2. The proposition is false - This means I am not lying, which implies that I am lying. Therefore, the proposition is true. Again, this cannot happen.

Here, **LEM** fails to hold. However, this paradox is not without a solution. Before proceeding further, it should clearly be recorded that **LEM** is a tautology. (Notice that **LEM** clearly holds sometimes; for example, **p**: "x is a positive real number").

First of all, it should be remarked that natural language is far too incoherent and ambiguous to be formalized. Therefore, the solution must begin with the translation of this statement into the symbolic language of logic. Such an interpretation goes like this:

*There is a proposition **p**, that if I affirm it, it is false*

Now, we call our interpretation **q**. Note that **q** refers to all propositions **p**, since we claim that **LEM** is a tautology. The paradox arises because of self-reference; since **q** is defined for all propositions **p**, it must also be defined for **q**. This, as already seen, leads to contradiction of **LEM**. Here, the principle of vicious-circle must be referred. This principle prohibits **q** to refer to itself, and therefore, the paradox is blocked.

The principle is due to Bertrand Russell. He argued that all logical paradoxes arise because of the violation of this principle. To return to familiarity, it is useful to consider Russell's Paradox, which can be approached along similar lines. The paradox is as follows: Define $R := \{x | x \in x\}$ Then,

$$R \in R \Leftrightarrow R \notin R.$$

The principle of vicious circle solves the Russell's paradox. However, it is important here to give a slightly more academic treatment of this principle - that is, Russell's **Theory of types**.

Russell assigned *types* to sets. For example, sets of type I would be elements in a set of type II, and no element of type II or higher can be contained in a set of type II. Similarly, we can treat sets of type III, IV and so on, creating a hierarchy of sets. The hierarchy develops as follows: individuals are placed at the lowest level (for example, natural numbers), followed by a class of individuals (for example, a set of natural numbers), and then a class further up (For example, the set of sets of natural numbers), and so on.

It is now easy to see that the question whether R is contained in itself is trivially solved. A similar treatment of the Liar's paradox is possible. If **p** is a proposition of type n, then **q** becomes a proposition of type $n + 1$, and therefore, the paradox is solved.

Set theory in particular deals with paradoxes of this kind by introducing strict axioms (ZFC Set Theory), which blocks the construction of sets that contain themselves. Since the approach of Russell's solution is similar to this one (both introduce axioms to block self-reference), and since neither suggests against **LEM**, a detailed discussion on axiomatic set theory is omitted.

Returning to Liar's paradox, Russell's solution is not without criticism. The works of Tarski, Kripke, and Barwise and Etchemendy deal with these criticisms and provide arguably stronger solutions. They are, however, a break from the mathematics-centric perspective that this article attempts to take. It is important here to comment that the contradiction of **LEM** is far from being merely an abstract idea. Indeed, we have applications where there are more than two truth values (true and false). There is one example of the included middle in quantum mechanics - the famous thought experiment by Erwin Schrödinger (Schrödinger's cat), which argues that if a cat is sealed in a box with a radioactive item, one would not know whether the cat is dead or alive until the box is opened. In simple terms, the cat, in a sense, is both dead and alive until the box is opened. Further, it is possible to develop systems of logic where, given a proposition, it can have more than two truth values: finite-valued logic, which allows n truth values (applications are found in the field of Electronics Design, and study of stable states of circuits and integrated circuits), and infinite-valued logic, which allows infinitely many truth values (for example, fuzzy logic associates truth values with real numbers in the interval $[0, 1]$, and finds applications in facial recognition, as well as economics, particularly in risk assessment systems).

Constructivism in Mathematics

LEM does not find unanimous support amongst mathematicians. While everyone agrees that **LEM** holds when limited to finite collections, criticism arises when discussing the extension of **LEM** to the infinite (although there do exist examples where **LEM** holds for infinite sets - There are either finite primes or infinite; it cannot be generalized). Mathematics based on a logical system that does not assume **LEM** is called **Constructive Mathematics**. Constructivism is not merely mathematics without proofs by contradiction; the differences are far more fundamental. For example, in constructive mathematics, the phrase "there exists" is replaced by "we can construct". It does not suffice to prove the existence of a mathematical entity, we must also construct it. Constructive logic actually ties existence with construction with the help of the existence property: Whenever we prove constructively that there exists a $x \in X : P(x)$ is true, we actually find at least one $a \in X : P(a)$; we call a the witness.

Supporters of constructivism argue that these proofs are superior as they give an algorithm to construct such entities. A mathematical entity, constructivists say, is anything that can be constructed.

Classical logic (where **LEM** holds) also is not without supporters. Amongst them is David Hilbert, who remarked, "Taking the principle of excluded middle from the mathematician would be the same, say, as proscribing the telescope to the astronomer or to the boxer the use of his fists". Existence is free from contradiction, argues Hilbert. Therefore, if we can prove that an object, having particular properties, does not cause contradictions, then it exists, and constructing that object is not required. It is fascinating to note that while constructive mathematics and 'classical' mathematics differ at the foundational level, their works are remarkably similar. Foundations of *Constructive Analysis* by E.

Bishop develops much of 20th century analysis using the principles of constructive mathematics.

It is important now to see the working of constructive mathematics, and contrast it with non-constructive mathematics. The obvious place to begin is with the proof of the irrationality of $\sqrt{2}$.

Theorem. *$\sqrt{2}$ is irrational.*

Proof. Let $r = \frac{a}{b}$, where a, b are positive integers.
If a is even, b cannot be even.
Then, a^2 is doubly even (i.e. divisible by 4), while $2b^2$ is singly even (i.e. divisible by 2, but not 4).
Therefore, $2b^2$ and a^2 are distinct integers.
If a is odd, and b is even, $2b^2$ and a^2 are clearly distinct. And if a and b are both odd, we again reach the same conclusion.
So, we have $|2b^2 - a^2| \geq 1$. Dividing and multiplying by $\sqrt{2} + \frac{a}{b}$, we get

$$\left|\sqrt{2} - \frac{a}{b}\right| = \frac{|2b^2 - a^2|}{b^2(\sqrt{2} + \frac{a}{b})} \geq \frac{1}{b^2(\sqrt{2} + \frac{a}{b})} \geq \frac{1}{3b^2}$$

It has now been established that $\sqrt{2}$ is distinct from any rational number r. Therefore, $\sqrt{2}$ is irrational.
□

Consider the following theorem, which contrasts the mechanism of constructive and non-constructive proofs.

Theorem. *There exist two irrational real numbers a and b such that ab is rational.*

Proof. (Non-constructive) Let a and b be irrational real numbers. Consider ab. It must be either rational or irrational. If it is rational, we are done. Assume it is irrational. Suppose we have, $\sqrt{2}^{\sqrt{2}}$, which we assume is irrational. Then, $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2$, which is rational.
Proof. (Constructive) Consider the irrational numbers $a = \sqrt{2}$, and $b = \log_2 9$. Then $a^b = 2(log_2 3) = 3$, which is rational. □

Note that while the non-constructive proof also constructs irrational numbers a and b which satisfy the theorem ($\sqrt{2}^{\sqrt{2}}$ is indeed irrational), the proof is not constructive in nature because it explores the possibilities permitted by **LEM** and shows that one of them must satisfy the theorem, but does not commit to one possibility.

Conclusion

It is important to remark that the debate on the validity of **LEM** is by no means ‘solved’. However, the deductions that follow from it are still widely accepted in mathematics. Also, as mentioned already, logical systems with more than two truth values not only exist, but also find useful applications in many fields of science and technology. Further, it serves well to remind again of the introductory level of the knowledge provided here; there are sections, especially the one about the validity of **LEM**, that can be pursued productively, for there are avenues that can be explored (for example, Russell’s solution fails to hold when we strengthen the liar; *“The following statement is false”*, *“The previous statement is true”*).

It is a fascinating, almost amusing, fact that constructive proofs are not the new wave of mathematics, as it might seem from the presentation of this article. In fact, some of Hilbert’s earlier works, which were non-constructive, were infamously dismissed as theology. And the initial criticism of Cantor is well-documented. A fantastic presentation of the history of metamathematics and logic, and its protagonists can be found in *Logicomix: An Epic Search For Truth (2009)* by Apostolos Doxiadis and Christos Papadimitriou.

Bibliography

[1] Wiki. List of Logical Systems

[2] Principia Mathematica: A.N. Whitehead and B. Russell, ISBN 978-0-511-89347-6

[3] Wiki. De Morgan's Laws

[4] Article. Mathematical Logic as Based on the Theory of Types: Bertrand Russell

[5] Naive Set Theory: P.R. Halmos, ISBN 978-1-4757-1645-0

[6] Article. The Principle of Antagonism and the Logic of Energy: Stéphane Lupasco

[7] Wiki, Brouwer-Hilbert Controversy

[8] Foundations of Constructive Analysis: E. Bishop, ISBN 978-3-642-61667-9

[9] Constructivism in Mathematics: A.S. Troelstra and D. van Dalen, ISBN 978-0-444-70358-3

Subgroups of Dihedral Groups

Ekansh Jauhari
B.Sc. (H) Mathematics, 3rd Year

A **dihedral group** is a group of symmetries of a regular polygon, with respect to function composition on its symmetrical rotations and reflections, and identity is the trivial rotation where the symmetry is unchanged. For such an n-sided polygon, the corresponding dihedral group, known as D_n has order $2n$, and has n rotations and n reflections.

Let us denote the first rotation by y. Rotating the symmetry n times would again give the same position of the symmetry. So performing function composition y, n times, we get the identity e, therefore we can write it as $y^n = e$. Also, let us denote the first reflection by x. Reflecting the symmetry twice will give us symmetry with the original position. Thus, we denote $x^2 = e$, and similarly, every reflection has order 2.

Dihedral groups are generated by a reflection and a rotation, such that we write dihedral group D_n=$< y, x >$ (finitely generated). Here $y^n = e$ and $x^2 = e$. So, we get rotations of the form of integer powers of y. For reflections, we have them in the form of composition of x with some power of y, i.e., xy^k, k is between 0 and $n-1$ (both inclusive). Thus,

$$D_n = \{e, y, y^2, \dots, y^{n-1}, x, xy, xy^2, \dots, xy^{n-1}\}, \text{ and } |D_n| = 2n,$$

where $y^n = e$ and $x^2 = e$.
We can notice that the rotations in $G = D_n$ form a group in itself.
r So we take $H = \{e, y, y^2, y^3, \dots, y^{n-1}\}$ where $y^n = e$.
So $H < G$ (H is the subgroup of $G = D_n$). Clearly, $H =< y >$ is a cyclic group since all the elements of H, i.e., the rotations, are some integral powers of y. Thus, $|H| = n$.

If we find the index of H in G, then it would be $\frac{2n}{n} = 2$. Since H comes out to be a subgroup of Index-2, then we can say that any arbitrary subgroup of G will either be contained in H or will have exactly half of the elements as that in H. If $S < G$ is any arbitrary subgroup contained in H, then $S < H$, and since H is cyclic, S will also be cyclic.

Otherwise, if $S < G$ isn't contained in H, then it has exactly half rotations. Since $S < G$, it can have only rotations and reflections. Since there are half rotations in S, the other half are reflections in S. Thus, S is a dihedral group.

Any subgroup of a dihedral group is either cyclic group or dihedral group.

Number of Cyclic Subgroups of a Dihedral Group

For any arbitrary $S < G$, if S is contained in H, then $S < H$, and S is cyclic. Since $H =< y >$ and subgroup $S << y >$, thus, S will be generated by some integer power of y where the integer power divides n, because $H =< y >$ and $y^n = e$, and thus, $S =< y^{n/d} >$ where $d|n$ (d divides n), for $1 \leq d \leq n$. For such $y^{n/d}$, clearly the order is d. Thus, y raised to the power of divisors of n generate S, for all possible divisors. So, there are as many as cyclic subgroups as there are divisors of n.

Number of Dihedral Subgroups in a Dihedral Group

For any arbitrary $S < G$, if S is not contained in H, then S is a dihedral group. So, S will be generated by a rotation and a reflection. For a reflection, we initially have n choices: $x, xy, xy^2, \ldots, xy^{n-1}$. For the rotation, since a rotation will again generate a cyclic subgroup within the new dihedral subgroup, and this new cyclic subgroup will certainly be a subgroup of H, and as $H =< y >$, therefore, the rotation can be of the form $y^{n/d}$ only, where $d|n$. Here, as mentioned above, the order of $y^{n/d}$ is d, and thus there are d rotations in S, and being a dihedral the same number of reflections also. So, we conclude that:
$S =< y^{n/d}, xy^p >$ for $d|n$ and $0 \leq p < n$.

For a given $d|n$, when we try generating S with the resulting $y^{n/d}$ and with all possible values of p between 0 and $n-1$, taken one by one, we find that we obtain exactly $\frac{n}{d}$ distinct dihedral groups (implying that there are exactly $\frac{n}{d}$ choices for p). This is because the dihedrals obtained when we take xy^p and $xy^{p+i(n/d)}$, where i is some non-negative integer, are the same.

The dihedrals obtained when we take xy^p and $xy^{p+i(n/d)}$ are same because for some p, we obtain a dihedral by performing the operation $xy^p \cdot y^{u(n/d)}$ for non-negative integer u, thus getting $xy^{p+u(n/d)}$. The same dihedral is obtained when we have $xy^{p+i(n/d)}$, and perform operation $xy^{p+i(n/d)} \cdot y^{t(n/d)}$ for some non-negative integer t, thus making the resultant as $xy^{p+(i+t)(n/d)}$ where $i+t$ is again a non-negative integer, which is equivalent to $xy^{p+u(n/d)}$. So basically, for each $d|n$, we have exactly $\frac{n}{d}$ number of dihedral subgroups, which is equivalent to saying that for d number of rotations and d number of reflections, we have exactly $\frac{n}{d}$ distinct such dihedral groups in D_n. So, for every divisor of n, there are that number of dihedrals present, which means that the total number of dihedral subgroups is the sum of all positive divisors of n.

Number of dihedral subgroups of $\mathbf{D_n}$ = sum of all positive divisors of n in $\mathbf{D_n}$

Number of Subgroups of $\mathbf{D_n}$ which are both Dihedral and Cyclic in nature

As $1|n$, so for $d = 1$ in the above setup, we get S $= < y^n, xy^p >$, or $S =< xy^p >$, making S cyclic. As there are $\frac{n}{1} = n$ choices for p, we conclude that there are n number of cyclic dihedral subgroups. So interestingly, they show both natures: dihedral because they have 1 rotation and 1 reflection, and cyclic because their order is 2.

Number of subgroups of $\mathbf{D_n}$ which are both dihedral and cyclic in nature = n

Number of Subgroups in a Dihedral Group

Now, we aim to find the exact number of subgroups present in D_n for any given order. For any arbitrary $S < G$, let us have $|S| = s$. If $S < H$, then $s|n$. Since there exists a unique subgroup of each possible order in a cyclic group, therefore, we have 1 cyclic subgroup for order s of S where $s|n$. If s does not divide n, then we don't have this subgroup. On the other hand, if S isn't contained in H, then S is dihedral of order s with $\frac{s}{2}$ rotations and $\frac{s}{2}$ reflections in S. If s is odd, $\frac{s}{2}$ is not an integer and therefore S does not exist. So for s being odd, we have no dihedral subgroups in D_n.

If s is even, then it is possible to have $\frac{s}{2}$ rotations and reflections. From previous argument, we had that for d number of rotations and d number of reflections, there were exactly $\frac{n}{d}$ distinct dihedral subgroups, and thus in analogy with this result, we get $\frac{n}{s/2}$ distinct dihedral subgroups, i.e., $\frac{2n}{s}$ dihedral subgroups.

So if $s|n$, we have a cyclic subgroup. If s doesn't divide n, then no such cyclic subgroup is present. Also, if n is even, we have $\frac{2n}{s}$ dihedral subgroups, but for n being odd, we don't have any dihedral subgroup in D_n.

For any S < G where |S| = s, we have following four cases:

- **If s|n and s is even, we have $\mathbf{1+\frac{2n}{s}}$ subgroups of order s in $\mathbf{D_n}$.**
- **If s|n and s is odd, we have only one subgroup of order s in $\mathbf{D_n}$,**
- **If s doesn't divide n, and s is even, we have $\mathbf{\frac{2n}{s}}$ subgroups of order s in $\mathbf{D_n}$.**
- **If s doesn't divide n, and s is odd, then there doesn't exist any subgroup of order s in $\mathbf{D_n}$.**

Example: In case of D_6, possible orders are $1, 2, 3, 4, 6, 12$. Total there are 4 cyclic and 12 dihedral subgroups.
For $s = 1$, there is only 1 subgroup (The trivial Identity group).
For $s = 2$, there are 7 subgroups.
For $s = 3$, there is only 1 subgroup.
For $s = 4$, there are 3 subgroups.
For $s = 6$, there are 3 subgroups.
For $s = 12$, there is only 1 subgroup (The Group itself).

Bibliography

[1] Wiki. Dihedral Groups

[2] Contemporary Abstract Algebra : Joseph A.Gallian, 5th Edition, ISBN 978-81-7319-269-2

Probability of Finding Generators of a Cyclic Group

Harshit Agrawal
B.Sc. (H) Mathematics, 3rd Year

Suppose we pick an arbitrary element from a group. Then what are the chances that the element will generate the group? If the group is non-cyclic, then the chances are obviously zero. But in a cyclic group, there is a possibility that the element could generate the group. Therefore, the above question makes sense in the case of a cyclic group. For instance, consider the group $\mathbb{Z}_4$. Here elements 1, 3 generate the group while 2, 4 do not. Thus, the probability of generating $\mathbb{Z}_4$ is $\frac{2}{4} = 0.5$. Similarly, we can also ask for the probability of generating other cyclic groups. This leads to the general question of the probability of finding generators of any cyclic group.

Infinite Cyclic Groups

Theorem. *Any infinite cyclic group has exactly 2 generators.*

Proof. Consider infinite group G such that $G =< a >$. Suppose $\exists\, b \in G$ such that b generates G. Then we must have $b = a^k$ for some $k \in \mathbb{Z}$. This means $\exists\, n \in \mathbb{Z}$ such that $(a^k)^n = a$. But since the order of a is not finite, therefore we know that for any $i, j \in \mathbb{Z}$, $a^i = a^j \Leftrightarrow i = j$. Therefore when $(a^k)^n = a$, we must have $kn = 1$. This means $k = \pm 1$ as $k, n \in \mathbb{Z}$. Therefore $b = a,\ a^{-1}$. Also, we know that in this case $a \neq a^{-1}$. Thus G will have exactly 2 generators.

Therefore $P(G) = 0$ when G is an infinite cyclic group, where $P(G)$ denotes the probability of generating G. □

Finite Cyclic Groups

For generating a finite cyclic group, we need to find its generators. For a finite cyclic group $G =< a >$, we know that $G =< a^k >$ if and only if $gcd(k, n) = 1$. Therefore, if $|G| = n$ then G has $\phi(n)$ generators where ϕ denotes the Euler-Phi function. As a result, the probability of any randomly chosen element to be a generator of the group is $\phi(n)/n$. Thus the probability of generating G which depends upon the generating capacity of its elements is $\phi(n)/n$. (It is assumed that all the elements are equally likely to be picked.)

As before, let $P(G)$ denote the probability of generating G. Now, let's examine the behaviour of $P(G)$ under different circumstances. (This goes without saying that G is cyclic in each case).

Case 1: When $|G| = p$, where p is prime. Here

$$P(G) = \frac{\phi(p)}{p} = \frac{p-1}{p} = 1 - \frac{1}{p}$$

Case 2: When $|G| = p^n$. Here,

$$P(G) = \frac{\phi(p^n)}{p^n} = \frac{p^n(1-\frac{1}{p})}{p^n} = 1 - \frac{1}{p}$$

It is worth noting that whether the order of G is p or p^n, $P(G)$ remains unchanged i.e. $1 - \frac{1}{p}$.

Case 3: When $|G| = p^m.q^n$ where $m, n \in Z$ and p, q are prime. Here

$$P(G) = \frac{\phi(p^m)(q^n)}{p^m q^n} = \frac{p^m(1-\frac{1}{p}).q^n(1-\frac{1}{q})}{p^m q^n} = \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)$$

.

Case 4: When $|G| = \prod_{i=1}^{k} {p_i}^{m_i}$, where $m_i \in \mathbb{Z}$ and p_i is prime $\forall$ $1 \leq i \leq k$. Here p_i must be distinct while m_i need not be distinct $\forall$ $1 \leq i \leq k$.

This is the most general case since any finite group's order can be broken down into the product of powers of primes by using the Fundamental Theorem of Arithmetic. Here,

$$P(G) = \frac{\phi(\prod_{i=1}^{k} {p_i}^{m_i})}{\prod_{i=1}^{k} {p_i}^{m_i}} = \frac{\prod_{i=1}^{k} \phi({p_i}^{m_i})}{\prod_{i=1}^{k} {p_i}^{m_i}} = \frac{\prod_{i=1}^{k} {p_i}^{m_i}(1-\frac{1}{p_i})}{\prod_{i=1}^{k} {p_i}^{m_i}} = \prod_{i=1}^{k} 1 - \frac{1}{p_i}$$

For example, consider $\mathbb{Z}_{90}$. Now, $|\mathbb{Z}_{90}| = 2 \cdot 3^2 \cdot 5$. Hence,

$$P(\mathbb{Z}_{90}) = \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = \frac{4}{15}$$

Now, consider $\mathbb{Z}_{360}$. Now, $|\mathbb{Z}_{360}| = 2^3 \cdot 3^2 \cdot 5$. Hence,

$$P(\mathbb{Z}_{360}) = \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = \frac{4}{15}$$

Thus, it is very easy to see that $P(G)$ rather than depending upon $|G|$ actually depends upon prime factors of $|G|$.

Let $\xi(G) = \{p \,|\, p \text{ divides } |G| \text{ and } p \text{ is prime}\}$

Therefore in general, for a finite cyclic group G,

$$P(G) = \prod_{p \in \xi(G)} \left(1 - \frac{1}{p}\right)$$

Theorem. *For finite cyclic groups G and H, if $\xi(G) = \xi(H)$ then $P(G) = P(H)$.*

Proof. We have,

$$P(G) = \prod_{p \in \xi(G)} \left(1 - \frac{1}{p}\right) = \prod_{p \in \xi(H)} \left(1 - \frac{1}{p}\right) = P(H)$$

□

The converse of this theorem also holds. Thus $P(G) = P(H) \Leftrightarrow \xi(G) = \xi(H)$. The proof is easy and left to the reader.

Hence it is proved that $P(G)$ depends directly on prime factors of $|G|$ and not on $|G|$ itself. This shows the importance of prime divisors of the order of a cyclic group in the probability of its generation via an arbitrary element.

Bibliography

[1] Article. The Probability of Generating a Cyclic Group: Deborah L Massari

[2] Contemporary Abstract Algebra : Joseph A.Gallian, 5th Edition, ISBN 978-81-7319-269-2

Fractals and Space-Filling Curves

Aman Chaudhary
B.Sc. (H) Mathematics, 2$^{\text{nd}}$ Year

Humans are fascinated by the beauty of nature, ranging from the Golden Ratio to the never ending nature of the Mandelbrot set (Fig 5.1), and the beauty it captures. An equally captivating idea is that of the Space-Filling Curves and Fractals. Mathematically speaking, **A Space-Filling Curve** is a curve whose range contains the entire 2-dimensional unit square. In simple terms, a curve that is capable of filling a given particular area (like a square grid), i.e. it passes through all the points that lie in that given space. It does seem quite fantastic when we find out that this continuous curve possesses infinite perimeter but doesn't occupy infinite area.

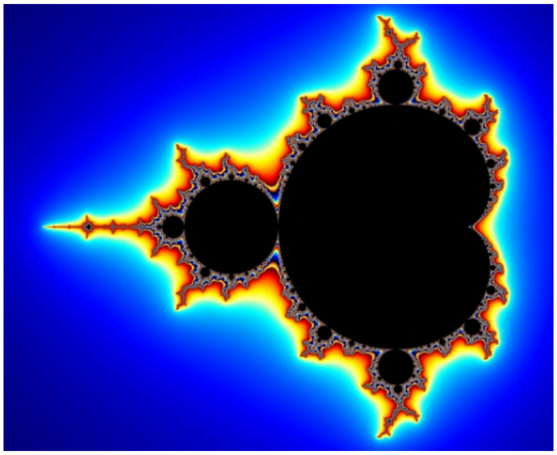


Figure 5.1: A Mandelbrot set

It all started in 1878, when the mathematician G. Cantor had the novel idea of establishing a relation between $\mathbb{R}$ (1 Dimensional Space) and an n-dimensional space $\mathbb{R}^n$. The aim was to somehow develop a surjective mapping from $\mathbb{R}$ to $\mathbb{R}^2$, which could include all the points in the plane, and such curves, as the name suggests, were called the Space-Filling Curves. Not going into the details of the topological space, we can think of Space-Filling Curve as a pattern shown in Fig 5.2. This seemingly alien curve, present in a unit square grid, when rearranged and replaced by four similar curves, gives us a continuous curve which looks four times denser than the previous one. Also, this process when iterated an infinite number of times, gives rise to the attractive pieces better known as fractals. Simply saying, Fractals are self-similar, never-ending, infinitely repeating patterns that look roughly the same no matter how much we zoom in.

The first Space-Filling Curve was proposed by **Peano** in 1890, and later on, similar curves were given by Hilbert, Moore, Sierpiński and many more. There lies an intimately close relation between Space-Filling Curves and Fractals. Space-Filling Curves have patrons and regularities that are highly linked to the self similar property of fractals. Though, the reader may note that not all the Space-Filling Curves are exactly self-similar. The curve mentioned above is the famous **Hilbert Curve**. The perimeter they encapsulate grows at an exponential rate. Given below are some beautiful seeds (basic iterator of the Space-Filling Curves).

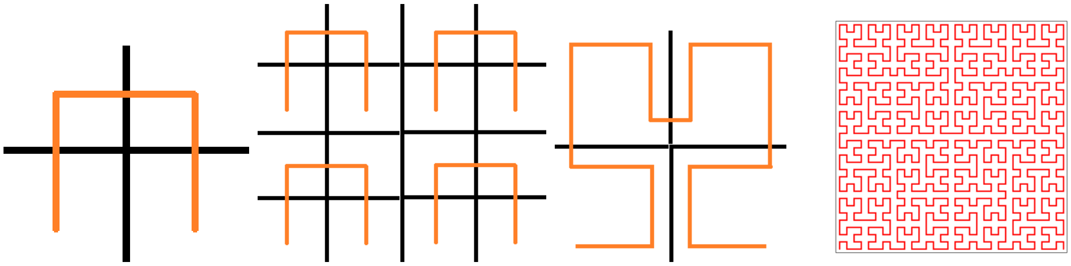


Figure 5.2: Rearranging and iterating a simple figure creates the amazing Hilbert curve

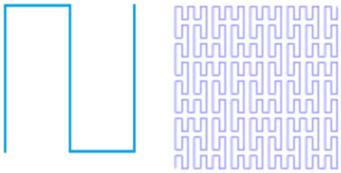


Figure 5.3: The seed and its resulting Peano Curve

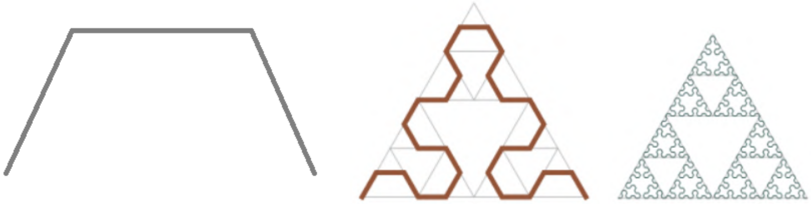


Figure 5.4: The seed and its Sierpiński Triangle

Let us now look into some more facts about the wondrous Space-Filling curves, using one of the most popular curves, The Van Koch Snowflake Curve.

Koch Snowflake or Koch Star

- **Constructing the infinite Snowflake:** Start with taking an equilateral triangle. Divide each side into three equal segments and impose an identical equilateral triangle onto the middle segment (each side is replaced by 4 sides after each iteration), repeating it infinite times, gives rise to the Koch Snowflake Curve, founded by Neils Fabian Helge Van Koch.

- **Infinite Perimeter:** Space-Filling Curves are said to have an infinite perimeter, because surely even in the snowflake case, each time the new figure posses 4 times as many line segments as the previous figure, with the length of each segment being one-third of the last one, i.e. the perimeter of the new one is 4/3 of the previous perimeter whenever a bump is added. So following this process of adding infinite bumps and multiplying a finite perimeter of the initial equilateral triangle by 4/3 an infinite number of times, we actually land up having an infinite perimeter of the resultant Koch Snowflake.

- **Finite Area:** It does seem quite outrageous that a curve having infinite length but the area it bounds is finite and computable. To get an intuition of the finite area, think of a hexagon or maybe a circle (having a finite area) that can encircle the whole Koch Snowflake (Fig 5.6),

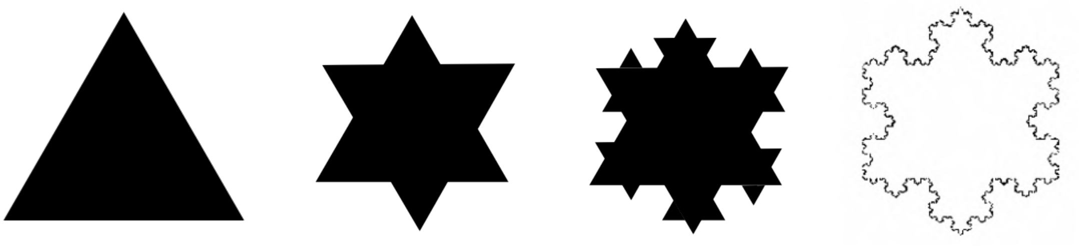


Figure 5.5: Construction of the infinite Snowflake

thereby having an area less than that of the hexagon. The exact area of the Snow Flake comes out to be $2\sqrt{3}/5$ times the area of the initial equilateral triangle (An exercise for the readers. Hint: Infinite G.P. concept).

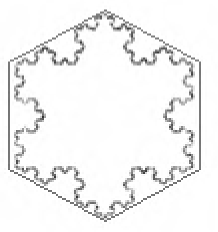


Figure 5.6: The Snowflake can be enclosed in a hexagon of finite area, hence its area is also finite

- **Continuous but not differentiable:** The Koch SnowFlake is continuous everywhere but differentiable nowhere. Proofs show that there doesn't lie even a one-sided tangent line at any point on this curve.

The Van Koch Snowflake Curve is a Fractal. A **Fractal** is a subset of a Euclidean space for which the fractal dimension strictly exceeds the topological dimension. In Fractal Geometry, a Fractal Dimension is a ratio providing a statistical index of complexity comparing how the detail in a Fractal pattern changes with the scale at which it is measured. It does not need to be a whole number.
The Koch Snowflake Curve is said to have a fractal dimension equal to $\log 4/\log 3 \approx 1.262$. Fractal Dimension of Sierpiński triangle is 1.585. It does seem uncanny to have such real valued dimensions, but that's how we mathematicians are like.

Cohen's Invention

In 1988, Nathan Cohen, a radio astronomer, came up with an idea of Infinite fractal antenna, since his landlord won't allow him to put an antenna on the rooftop. He used the Koch curve type of antenna instead of the normal antenna having limited area but capable of picking more signals and not just one. This idea was later on improvised when Menger Sponge, a fractal curve which is a 3D generalization of the 1D Cantor set and 2D Sierpiński carpet having infinite surface area but zero volume, was used in cell phones for the same.

Everything in this universe depicts some kind of a fractal (until you get to the atomic level of that item), like measuring the coastline of a country. Space-Filling Curves are widely used to solve combinatorial optimization problems in industrial contexts, making fractal antennas, computer science engineering, etc. Even chromatin is a fractal and keeps DNA from getting entangled. But above all is the property of the Space-Filling Curves that says, "Every point lying on the Space-Filling Curve (which is bound to happen), seems to approach a limiting point in the Space as our Space-Filling Curve seems to approach a limiting curve". Continuous Space-Filling Curves with this property find one of its uses in Google maps, to introduce cache locality: When you move a little bit while viewing the map, you want to be moving only a little bit in the memory, which is after all arranged linearly. So the next time you use the Google Maps, applaud the idea and charm of these Curves.

Bibliography

[1] Article. Koch Snowflake: David Maslanka

[2] Article. Fractal Antennas: Philip Felber

[3] Text. Applications of Space-Filling Curves: MathOverflow

[4] Wiki. Fractals

Cardinality of $\mathbb{R}^2$

Deepak Kumar
B.Sc. (H) Mathematics, 3$^{\text{rd}}$ Year

It is an established result that the $|\mathbb{R}| = |\mathbb{R}^2|$. The following proof establishes the same result from the aspects of "Linear Algebra".

Lemma. *The basis of* $\mathbb{R}(\mathbb{Q})$*, an infinite vector space, is uncountable.*

Proof. Let $\mathbb{R}(\mathbb{Q})$ have a countable dimension. Let B be the basis of $\mathbb{R}(\mathbb{Q})$. Then, $|B| \leq |\mathbb{N}|$
Since B spans $\mathbb{R}$, so by definition, every vector of $\mathbb{R}$ can be written as a finite linear combination of vectors of B.
Hence, we associate with every vector of $\mathbb{R}$, i.e. every real number, a unique infinite sequence of rationals (which are the coordinates with respect to B), having all but a finite number of non-zero values.
Let A = Set of natural sequences having all but finite number of non-zero values.
Since, $|\mathbb{Q}| = |\mathbb{N}|$, we can associate an injective function from the reals to the set A.
Let $(a_0, a_1, a_2, \ldots, a_k, 0, 0, 0, 0, \ldots)$ be any such sequence.
Define $f : A \to \mathbb{N}$

$$f\big((a_0, a_1, a_2, \ldots, a_k, 0, 0, 0, 0, \ldots)\big) = \prod_{i=1}^{k} {p_i}^{a_i}$$

where $p_i = i^{th}$ prime number.
By Fundamental Theorem of Arithmetic, f is an injective function.
So, $|A| \leq |\mathbb{N}|$, and hence, $|\mathbb{R}| \leq |\mathbb{N}|$
Thus, we get a contradiction.

□

Claim 1: Let B be a basis for $\mathbb{R}(\mathbb{Q})$. Let $S_1 = \{(x, 0) \,|\, x \in B\}$ and $S_2 = \{(0, x) \,|\, x \in B\}$. Then, $S = S_1 \cup S_2$ is a basis for $\mathbb{R}^2(\mathbb{Q})$

Proof. Note that $Span(S_1) = \{(x, 0) \,|\, x \in \mathbb{R}\}$ and $Span(S_2) = \{(0, x) \,|\, x \in \mathbb{R}\}$
And, $Span(S_1) \cap Span(S_2) = \{(0, 0)\}$ And, $\mathbb{R}^2(\mathbb{Q}) = Span(S_1) \oplus Span(S_2)$
Thus, $\mathbb{R}^2(\mathbb{Q}) = Span(S_1 \cup S_2) = Span(S)$
Hence, S is a basis for $\mathbb{R}^2(\mathbb{Q})$ □

Corollary. $\mathbb{R}^2$ *over the field of* $\mathbb{Q}$ *is an infinite dimensional vector space with uncountable basis.*

Claim 2: $|S| = |B|$

Proof. Since, $|B| = |\mathbb{R}| = |[0, 1)| = |[1, 2)| = |(0, 2)|$,
$|S_1| = |B| = |[0, 1)|$ and $|S_2| = |B| = |[1, 2)|$
And since, $S_1 \cap S_2 = (0, 0)$
Thus, $|S| = |S_1 U S_2| = |(0, 1) \cup [1, 2)| = |(0, 2)| = |B|$

□

Claim 3: $|\mathbb{R}| = |\mathbb{R}^2|$

Proof. Let $g : B \to S$ be the bijective function whose existence is shown in Claim 2.
Let $r \in \mathbb{R}$, then

$$r = \sum_{i=1}^{k} c(i)\, b(i)$$

where $c(i) \in \mathbb{Q}$ and $b(i) \in B$ is a finite linear combination of vectors from B.
Define $h : \mathbb{R} \to \mathbb{R}^2$

$$h(r) = h\left(\sum_{i=1}^{k} c(i)\, b(i)\right) = \sum_{i=1}^{k} c(i)\, g\big(b(i)\big)$$

Since g is bijective and each real number has unique coordinates with respect to B, h is injective.
Since every $(a, b) \in \mathbb{R}^2$ has unique coordinates with respect to S as well, so h is surjective.
So, h is bijective.
Hence, $|\mathbb{R}| = |\mathbb{R}^2|$ □

Corollary. $|\mathbb{R}| = |\mathbb{R}^n|$, *where* $n \in \mathbb{N}$.

Bibliography

[1] Linear Algebra: K. Hoffman and R. Kunze, 2nd Edition, ISBN 978-81-2030-270-9

[2] Abstract Algebra: David S. Dummit and Richard M. Foote, 3rd Edition, 978-04-7143-334-7

[3] Topics in Algebra: I. N. Herstein, 2nd Edition, ISBN 978-04-7101-090-6

Introduction to Cryptography

Shubham Kumar Yadav
B.Sc. (H) Mathematics, 3$^{\text{rd}}$ Year

Cryptography is the technique of securing information and communications through the use of codes so that only those people for whom the information is intended can understand it and process it. Sounds too dull and cumbersome, doesn't it? Well, in layman terms, it simply means the art of restricting the access of our data to the attackers. The term data here refers to information, which can be as small as the click of a mouse button to as important as the data residing with the FBI. Technically speaking, the process of scrambling this data so that it is illegible to the attacker is called encryption, and the reverse process of recovering the original message from this scrambled text is termed as decryption. These two processes form the backbone of what is known as the encryption system.

The next question is: to achieve a better encryption system, which one of the two processes should be strengthened? Some might answer the former, while others might opt for the latter. Interestingly enough, it is indeed a vague question and generally, the level of complexity of the encryption scheme is roughly of the same order as the decryption scheme, and one cannot upgrade the first much without improving the second too. In simpler terms, it means that as the lock of a door gets upgraded (say, for example, from a simple padlock to a sophisticated fingerprint scanner) the corresponding key will also get upgraded (from a simple padlock's key to a complex fingerprint sensor).

Historically, cryptography and encryption have been wrongly used interchangeably, and this can even be found today. Psychologically, the people are not to blame here, because the term cryptography did not gain its actual meaning until the recent onset of computers, digital currency, improved banking facilities, password management, etc. The next curious observation would be as to how the improvement in the aforementioned fields has led to an increased emphasis being given in the field of cryptography.

To answer this, we need to understand the four features which cryptography provides us with- the information cannot be comprehended by anyone for whom it was unintended (*confidentiality*), the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected (*integrity*), the creator/sender of information cannot deny his or her intention to send information at a later stage (*non-repudiation*) and the identities of the sender, the receiver and the destination/origin of the information is confirmed (*authentication*). These four are the basic necessities when dealing with a computer network and hence call for improved and secure cryptographic systems.

Applications

Today, cryptography finds its uses in an array of fields, and one can witness its applications round the clock: from receiving a Good Morning message on WhatsApp to sending a mail via Gmail, from making online purchases via debit/credit cards to watching Sacred Games on Netflix, everything is protected against the use by non-authorised parties.

The recent advancement in the arena of shopping has been the introduction of the online platforms, thereby bringing in ease and comfort. However, these platforms rely heavily on cryptographic standards for their functioning, as integrity, non-repudiation and authentication are a must while placing an order. So, the simple button of 'Add to cart', must have been a long and tiring challenge for the cryptographers to assure that the aforementioned objectives are achieved. Surfing movies and TV shows on Netflix and dish connections also involve cryptography.

The subscription which is bought on these platforms authorises the customers to use them. The scrambled data received from the satellites is unscrambled with the help of a unique number associated with the subscription which you buy. In the event of an unauthorised person trying to access the signals and lack of this unique number, the decryption will not occur in the manner it should have been and hence binge-watching would only be a dream for such souls.

Cryptography also comes into play while withdrawing money from an ATM, or sending emails that might contain sensitive information which the user might not want to make available to everyone. With the advancement of machine learning and artificial intelligence, the data of the consumers has started gaining importance and advertisement companies are willing to pay hefty amounts for the same. Cryptographers play a crucial role to play here to prevent crimes such as data theft and data selling. The most prominent examples in this aspect are the Facebook-Cambridge Analytica scandal, and the Aadhaar Data Breach wherein the entire data of an individual registered with the UIDAI's Aadhaar Card was being sold for less than a buck.

Cryptography even helped during World War II, wherein the Germans inflicted terrible atrocities upon the world. An English mathematician and computer scientist, Alan Turing, devised a machine which, as per the Morten Tyldum directed movie 'The Imitation Game', starring Benedict Cumberbatch, was termed as Christopher. Christopher was successfully deployed to crack Enigma, the secured device used by the Nazis to communicate their plan of action in the war. Turing, along with his team and the use of statistics, was not only able to turn the table in favour of the Allies but was also successful in reducing the duration of the war by up to 2 years, thereby avoiding the loss of millions of dollars and billions of lives!

Conclusion

So, when you wake up tomorrow and open WhatsApp, pay a second or two, recognising the efforts and the cryptography involved in making the transmission of that message possible. In a nutshell, unless we pack together all the computers, mobile phones and all other digital devices and throw them in an abyss (which is an improbability), we all will be having data and its security will undoubtedly call for cryptography and its unending applications.

Bibliography

[1] Data Security-Applications, Chapter 8, Contemporary Abstract Algebra : Joseph A.Gallian, 4th Edition, ISBN 978-81-7319-269-2

[2] Article. Aadhaar: BBC

[3] Preface, Cryptography and Network Security Principles and Practice: William Stallings, 5th Edition, ISBN 978-81-3176-166-3

RSA-129

Gaurav Kumar
B.Sc. (H) Mathematics, 2nd Year

RSA-129 is one of the first *Public-key Cryptosystems* and is widely used for securing data transmission over devices. *Public-key Cryptosystems* means a cryptosystem which uses two keys 1.) Encryption Key 2.) Decryption Key and the encryption key is made public which means the method of encrypting data is available to everyone, the decryption key is kept private. It was developed by Ron Rivest, Adi Shamir and Leonard Adelman and the abbreviation RSA is made of initial letters of their surnames.

Description

RSA-129 is one of the first *Public-key Cryptosystems* and is widely used for securing data transmission over devices. *Public-key Cryptosystems* means a cryptosystem which uses two keys 1.) Encryption Key 2.) Decryption Key. The encryption key is made public, which means the method of encrypting data is available to everyone, but the decryption key is kept private. It was developed by Ron Rivest, Adi Shamir and Leonard Adelman and the abbreviation RSA is made of initial letters of their surnames.

Description

The RSA algorithm consists of four steps: key generation, key distribution, encryption and decryption. The basic principle of RSA depends on the fact that factoring a number into its prime factors is hard based on the size of the number. For example, factorizing 75 is quite easy as $75 = 5^2 \times 3$. But the difficulty increases with every increase in the number of factor. So, it is practical to find 3 very large positive integers e, d, n such that with modular exponentiation for all integers m $(with\ 0 \leq m < n)$, $(m^e)^d \equiv m(\text{mod } n)$.

Algorithm of Creating Keys

- It basically starts with taking two large, distinct prime numbers say, p and q.
- Set $n = p \times q$.
- Set $\lambda(n) = (p-1) \times (q-1)$.
- Choose any integer e : $1 < e < \lambda(n)$ and gcd$(e, \lambda(n))$=1 i.e., e and $\lambda(n)$ are co-prime.
- Choose an integer d such that $d \times e \equiv 1(\text{mod } \lambda(n))$, which means it is the multiplicative inverse of e modulo $\lambda(n)$.
- Now the encryption key is $(e, \lambda(n))$ which is made public and the decryption key is $(d, \lambda(n))$ which is kept private.

Algorithm for using the Keys

We will look at an example to get a better understanding of the topic and how RSA works. We have to make the Keys for which we'll follow the algorithm.

- Choose 2 random primes $p = 7$ and $q = 11$.
- Then $n = 7 \times 11 = 77$.
- Now, $\lambda(n) = (7 - 1) \times (11 - 1) = 60$
- Consider any number $e : 1 < e < \lambda(n)$. Let $e = 17$.
- We have to find an integer : $d \times e \equiv 1(\text{mod } \lambda(n))$.
  A simple method to find this is by calculating $e^{p-2} \equiv d(\text{mod } p)$, then d is the number such that $e \cdot d \equiv 1(\text{mod } p)$. This is based on Fermat's Little Theorem, which will be discussed later.
- So, *Encryption Key* is $(17, 77)$ and *Decryption Key* is $(53, 77)$.

Now to illustrate their use:

- The first thing we need to look at is that the message should be converted into a mathematical message. For Example, consider the message "PASSWORD". We convert it into a message $(16, 1, 19, 19, 23, 15, 18, 4)$ which is an n-Tuple.
- Then we have to encrypt it using the encryption key. Here's how we will do it.

  Every element of the tuple will be raised to the power of e then will be divided by n and the remainder r is the answer.
  Here we'll illustrate using a number: $16^{17} \equiv r(\text{mod } n)$. This calculation, which looks complex, can be made easy by using the properties of Modular Arithmetic:
  $16^3 = 4096 \equiv 15(\text{mod } 77)$
  $\Rightarrow (16^3)^5 \equiv 15^5 = 759,375 \equiv 1(\text{mod } 77)$
  $\Rightarrow (16^{15}) \times 16^2 \equiv 1 \times 16^2 = 256 \equiv 25(\text{mod } 77)$
  $\Rightarrow 16^{17} \equiv 25(\text{mod } 77)$
  Now $r = 25$. Similarly every element of the tuple can be reduced to mod 77 after exponentiation by 17.
  Now the tuple has become $(25, 1, 24, 24, 67, 71, 72, 16)$. This tuple/message is the encrypted data which can't be decrypted without using the unique decryption key.

- Decryption takes place similarly, where the encrypted message will be taken and then exponentiated with the help of Decryption key which is $(53, 77)$. The calculation may seem very lengthy, but it can be easily done using few tricks. Decryption of one of the element is shown :
  $25^{53} \equiv r(\text{mod } 77)$
  $25 \times 25 = 625 \equiv 9(\text{mod } 77)$
  $\Rightarrow 25^4 \equiv 9^2 = 81 \equiv 4(\text{mod } 77)$
  $\Rightarrow (25^4)^3 \equiv 4^3 = 64 \equiv -13(\text{mod } 77)$
  $\Rightarrow (25^{12})^4 \equiv (-13)^4 = 28561 \equiv 71(\text{mod } 77)$
  $\Rightarrow 25^{48} \times (25^2)^2 \times 25 \equiv 71 \times 81 \times 25 \equiv 16(\text{mod } 77)$
  $\Rightarrow 25^{53} \equiv 16(\text{mod } 77)$
  Here we can see that original element 16 (the first element of tuple) is obtained back, which verifies that Decryption is accurate.
  After doing the same process with all those elements the new tuple will be exactly the same as the original tuple/message, that is, $(16, 1, 19, 19, 23, 15, 18, 4)$.

Mathematics behind RSA

Obviously, this astonishing cryptosystem is based on rigorous maths. It basically depends on two major facts: Existence of unique Inverses in a Group, and Fermat's Little Theorem.
Before getting into further details of the system, a brief about these:

- Groups are algebraic structures in maths. It is basically a Set equipped with a binary operation on it and with some postulates that it holds:
    - Associativity
    - Existence of unique Identity element.
    - Existence of unique Inverse of each element.

  Example: Set of Integers under addition.

- Fermat's Little Theorem states that for any prime p

$$a^{p-1} \equiv 1 (\text{mod } p) \ \ \forall\, a \in \mathbb{Z},\ \gcd(a,p) = 1$$

Now, choosing p and q arbitrarily, set $n = p \times q$ and $\lambda(n) = (p-1)(q-1)$.
Choose e such that $1 < e < \lambda(n)$ and $\gcd(e, \lambda(n)) = 1$.
The first question arises with existence of $d : e \times d \equiv 1 (\text{mod } \lambda(n))$.

Using Bézout's identity that for every 2 integers $e,\ \lambda(n)$ $\exists$ integers x and $y : ex + \lambda(n)y = \gcd(e, \lambda(n))$.
Now since $\gcd(e, \lambda(n)) = 1$, there exists an integer $x : e \times x \equiv 1 (\text{mod } \lambda(n))$.
Now by Euclid's division algorithm $x = n \cdot q + d$, $0 \le d < n$ and $e \times d \equiv 1 (\text{mod } n)$.
Let's pick any number g which is a message, $g < n$. g will be encrypted using(e, n).
Let $g^e \equiv r_1 (\text{mod } n)$,encrypted message will be $r_1, 0 \le r_1 < n$.

Now Decryption will take place the same way $r_1^d \equiv (g^e)^d \equiv r_2 (\text{mod } n), 0 \le r_2 < n$. . . . (1)
Since $ed \equiv 1 (\text{mod}\lambda(n)) \Rightarrow ed = 1 + k \times \lambda(n))$
and since $\lambda(n) = (p-1)(q-1) \Rightarrow g^{ed} = g^1 \times (g^{(p-1)(q-1)})^k$
Now, $g^{(p-1)} \equiv 1 (\text{mod } p) \Rightarrow (g^{(p-1)})^{(q-1)} \equiv 1^{(q-1)} \equiv 1 (\text{mod } p)$ . . . (2)
Similarly, $(g^{(q-1)})^{(p-1)} \equiv 1 (\text{mod } q)$ . . . (3)
From (2) & (3), and since p and q are co-prime $\Rightarrow g^{(p-1)(q-1)} \equiv 1 (\text{mod } p \times q)$ . . . (4)
From (1) & (4) and since $n = pq \Rightarrow g^{ed} \equiv r_2 \equiv g \times 1 (\text{mod } n)$
It shows that message will be obtained back after Decryption accurately because $r_2 - g$ is a multiple of n and $0 \le r_2, g < n$, hence $r_2 - g = 0$ and hence they are equal.

Also, $e^{p-2} \equiv d (\text{mod } p)$ gives the inverse of e because of Fermat's Little theorem
$e^{p-1} \equiv 1 (\text{mod } p) \Rightarrow e \cdot e^{p-2} \equiv 1 (\text{mod } p) \Rightarrow e \cdot d \equiv 1 (\text{mod } p)$, hence inverse.

Advantages of RSA

After looking at how it works, we shall now discuss its features and advantages:

- The foremost benefit is that factoring becomes very hard after the integers get really big and, in fact, RSA-129 uses two 64 and 65 digit primes, leading to a 129 digit long number. It takes a lot of computation to factor a number. Moreover, to increase the level of difficulty, the difference between the two primes is chosen to be small compared to their size because otherwise, it can be easily determined.

- Here, the factors are important because without determining the factors p and q the Decryption key d can't be determined because it depends on $\lambda(n)$ which we can't determine without knowing p and q.

- Now, to get an idea as to why finding d is so hard, note that d is the multiplicative inverse of e with respect to mod $\lambda(n)$, and since it forms a group with respect to the operation multiplication mod $\lambda(n)$, it will have a unique inverse, and to find the inverse of any element we need to know the operation since inverse changes with the operation, like the additive inverse of 2 is -2 but the multiplicative inverse is $\frac{1}{2}$. So. to find the operation, we must know $\lambda(n)$.
- Also, if you can't find d then you have to approach from a different direction. For example, let r be the ciphered element. Then we have to look solutions for $x^e \equiv r (\text{mod } n)$, which is basically the same as looking for an e_{th} root of $r(\text{mod } n)$, which is also not easy because the length of numbers chosen are arbitrarily long.

Disadvantages of RSA

Every code is not perfect and it can have loopholes which the hackers can exploit.

- Using lower encryption exponents can lead to easy calculation of the e_{th} root of the encrypted text.
- If the same e is used for encrypting the same texts with different p and q, which means different n, then by using the *Chinese Remainder Theorem* we can calculate the original message using encrypted message.
- The RSA is not semantically secure since it follows a fixed process and no random techniques. The hacker can use this flaw to exploit it by encrypting similar messages and checking whether the encrypted texts are also similar and hence it becomes easy for him to crack the code by working backwards.

Conclusion

In the end, what matters is the security of a cryptosystem, which is based on how hard it is to break it. The Original RSA-129 took more than 20 years to break. The original number was $n =$
114381625757888867669235779976146612010218296721242362562562....
...5618429357069352457338978305971235639587050898075147599290026879543541.
The length of the number shows that complexity increases with length and in contemporary times, computers like NATWEST BANK uses n with 2048 bits, which is so long that it might take years to be factorized. Everything can be calculated or estimated in this age of technology, even the growth of computers, but the complexity and power of algorithms in the future is something that grows beyond our comprehension, and this fact allows the possibility of one which makes factoring easy. But until such technology arises, RSA-129 continues to be one of the most effective cryptosystems one can employ.

Bibliography

[1] Wiki. RSA (cryptosystem)

[2] Encryption and HUGE numbers: Numberphile

[3] Contemporary Abstract Algebra : Joseph A.Gallian, 4^{th} Edition, ISBN 978-81-7319-269-2

[4] Wiki. Bézout's Identity

[5] RSA-129: Numberphile

Pigeonhole Principle

Ashutosh Maurya
B.Sc. (H) Mathematics, 2$^{\text{nd}}$ Year

When an intrinsically trivial and intuitive statement has deep implications and consequences, it is naturally intriguing for people, mathematicians and non-mathematicians alike. One such statement is that of the Pigeonhole principle. This article shall discuss the various nuances of this principle, highlighting the dependence of mathematics on basic thoughts and pure logic.

Introduction

We begin, as the introduction to a mathematical concept should, with the statement and proof of the Pigeonhole principle.

The pigeonhole principle states that if n items are put into m containers, with $n > m$, then at least one container must contain more than one item.

The principle is believed to be formalized by Peter Gustav Lejeune Dirichlet. Since he published his works in both French and German, he used the terms *Schubfach* in German and *tiroir* in French to describe what in English may refer to as a drawer. These terms were morphed to the word *pigeonhole*, which is one of the reasons of the intrigue associated with this principle.

Although the statement seems intuitive and obvious, we shall give a formal proof. We shall use one of the most potent tools to establish proofs in mathematics: proving by contradiction.

Let us assume that no container contains more than one item. So, each of the m containers will either have 0 or 1 item. If the number of containers with 0 items is k, then certainly, $k \geq 0$. So, the number of containers with 1 item will be $m - k$. So, the number of items in k containers will be $m - k$. But $k - m < k < n$, and n items had been put in k containers. Therefore, we arrive at a contradiction, which arose due to the wrong assumption. Hence, at least one container must contain more than one item.

Apart from the statement mentioned above, there are several versions of the Pigeonhole principle, some of which are worth mentioning here. A simple generalization of the principle exists, which deals with multiple "pigeons". It says:

Let n, m and r be positive integers so that $n > rm$. If n items are put into m containers. then at least one container must contain more than r items.

This generalization can be proved in a similar fashion to establish its verity. It is sometimes called the Second Pigeonhole Principle, while the first statement is called the First Pigeonhole Principle.

Another version was given by Edsger W. Dijkstra, the pioneering computing scientist. According to him, the usual statements of the principle "contain a lot of misleading noise, are overspecific, and hide the principle's arithmetic nature". He composed a formulation free of metaphors and "misleading visualizations". It says:

For a nonempty, finite bag of real numbers, the maximum is at least the average (and the minimum is at most the average)

Though this “stronger” form may lead to easier interpretation and solving of certain problems, sometimes, it may complicate them too. While the traditional statement forces us to explicitly identify “pigeons” and “holes”, or items and compartments, this form may need the same process, in addition to worrying about the numbers and the average.

Popular Examples and Applications

The simplicity of the Pigeonhole principle does not understate its importance. From numerical analysis to computer sciences, the principle finds its applications in multiple, seemingly unrelated fields.

A particularly famous example is the Birthday Paradox. It is not a paradox per se, but it is called so because it is unbelievably counterintuitive.

The birthday problem or birthday paradox concerns the probability that, in a set of n randomly chosen people, some pair of them will have the same birthday.

Since there are 365 days in one year (366 in a leap year), with a group of just 367 randomly chosen people, the probability reaches 100%. This is a simple application of the Pigeonhole principle, since the number of people is greater than the number of days, more than one person will be associated with a particular date. Moreover, using probability, it can also be shown that even with just 70 people, 99.9% probability is reached, and with just 23 people, 50% is reached.

Another important application of the pigeonhole principle is found in the proof of Dirichlet’s Approximation Theorem. In number theory, Dirichlet’s theorem on Diophantine approximation, also called Dirichlet’s approximation theorem, states that for any real numbers α and N, with $1 \leq N$, there exist integers p and q such that $1 \leq q \leq N$ and

$$|q\alpha - p| \leq \frac{1}{N}$$

The theorem provides a way to find “good” approximations of irrational numbers, using a fraction with a relatively small denominator. It should be pointed out that by using fractions with large denominators, the process of approximation becomes clumsy and unreliable. The theorem can be proved using the pigeonhole principle.

Consider the set $A = \{j\alpha \,|\, 0 \leq j \leq N\}$. So $|A| = N + 1$. Now, we take partitions of the set $[0, 1)$ such as $\big[0, \frac{1}{N}\big)$, $\big[\frac{1}{N}, \frac{2}{N}\big)$, and so on. There will be N such partitions.
Since there are $N + 1$ numbers and N partitions, by the Pigeonhole principle, there must be at least two numbers that belong to the same partition. Let these numbers be $r\alpha$ and $s\alpha$, and without loss of generality, let $r\alpha < s\alpha$.
Now, there must be an integer p such that $0 \leq r\alpha - s\alpha \leq \frac{1}{N}$, since the partitions are defined so. Let $q = r - s$. So, we have

$$p \leq q\alpha \leq \frac{pN + 1}{N}$$

Subtracting p and dividing by q, we get

$$0 \leq \alpha - \frac{p}{q} \leq \frac{1}{qN} \leq \frac{1}{q^2}$$

or

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2}$$

which is the desired result.

Moreover, the Thue-Siegel-Roth theorem states that every irrational algebraic number α has approximation exponent equal to 2. The approximation exponent is the measure of “closely” it can be approximated by rationals. This guarantees that results like the following inequality are not possible:

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^3}$$

Klaus Friedrich Roth won the Fields Medal for proving this theorem.

Conclusion

The Pigeonhole Principle doesn't seem to be any more than just a "truth" about counting, yet many advanced theorems have been borne out of it. It continues to have real life applications in various aspects, and its thorough understanding yields greater mastery as well as appreciation towards mathematics in general.

Bibliography

[1] Topics In Algebra: Herstein, I. N., Blaisdell Publishing Company, ISBN 978-111-4541-01-6

[2] Article. Pigeonhole Principle: Real Life Applications and Mathematical Investigation; Pengsheng Guo, Qing Yu, Yang Wang, Yiwei Gong

[3] Transcript. Edsger W. Dijkstra.

[4] Wiki. Birthday Problem

[5] Article. Dirichlet's Approximation Theorem

[6] Wiki. Roth's theorem

[7] Wiki. Liouville Number

Frobenius Numbers

Shubham Kumar Yadav
B.Sc. (H) Mathematics, 3$^{\text{rd}}$ Year

This article draws its inspiration from an example laid out in one of the books prescribed for the students undertaking a Major in Mathematics in the Delhi University circuit. The example 10 (Ch. 0, Pg. 15) in the book titled "Contemporary Abstract Algebra" (Fourth Edition) by Joseph A. Gallian states a problem adapted from the 'Brain Boggler' section of the January 1988 issue of the science magazine Discover. The excerpt from the same goes like this:

The Quakertown Poker Club plays with blue chips worth $5.00 and red chips worth $8.00. What is the largest bet that cannot be made?

Though the text makes a very good attempt at finding the solution (by hit and trial) to be *$27.00* and verifying it by the principles of mathematical induction, yet it fails at delivering the intuition as to why it is *$27*, and how this number is obtained. This article attempts to present an algorithm to figure out a general formula for working out this *'largest unobtainable bet number'* (technically referred to as the Frobenius number of a given set of numbers) for any given numbers, say m and n. For simplicity, we shall use the term Frobenius number to denote the Frobenius number of a set containing only two elements, namely m and n, where $m < n$.

Finite Check Strategy

Apart from the methods mentioned in the book, a simple method for verifying that a given number N, is indeed a Frobenius number has been described below:

- Check if N is expressible as a linear combination of m and n. If not, then proceed to the further steps.
- Express $(N + 1)$ as a linear combination of m and n, i.e. find natural numbers x and y satisfying $(N + 1) = mx + ny$.
- Continue expressing the numbers $(N + 2), (N + 3), \cdots, (N + m)$ as a linear combination of m and n with non-negative integer weights. Note that we need not check the countably infinite numbers succeeding N. We only need to check these m number of elements whether or not they are spanned by m and n.

This method works quite well for small values of m and n. If the second and the third step can be accomplished, then any number greater than N can be expressed as a linear combination of m and n. This is due to the fact that all numbers greater than $(N + m)$ can be obtained by adding multiples of m to these numbers only. For instance, $(\overline{N + m} + 1) = (N + 1) + m, (\overline{N + m} + 2) = (N + 2) + m$, etc. Skipping the details, this result is a cakewalk with a little knowledge of modular arithmetic.

Claim: The Frobenius number N of co-primes m and n is $N = mn - m - n = (m - 1)(n - 1) - 1$.

Proof. Assume, without loss of generality that $0 < m < n$, and $p = n - m > 0$. The claim boils down to show that for the given numbers m and n, the Frobenius number is the greatest value of

any whole number k_1 such that $k_1 \notin K = \{ma + nb \,|\, a, b \in \mathbb{Z}^+ \cup \{0\}\,\}$. Now, let $k \in K$, then $k = ma + nb = ma + (m + p)b$, since $p = n - m$. This implies that $k = m(a + b) + pb$.
Secondly, note that $gcd(m, n) = 1$ is required for the Frobenius problem to be well defined. This is because, for any given linear combination w of m and n, we can always find a number co-prime to $d = gcd(m, n) \neq 1$ and strictly greater than w. A simple hack for choosing such a number would be to choose a prime number not occurring in the prime factorisation of d and call it P. Then define the sequence $P_n = \{P^n \,|\, n \in \mathbb{N}\}$ and choose the desired number from P_n. Thus, for non co-prime numbers, the Frobenius number will cease to exist because $d = gcd(m, n) \neq 1$, and, $d|m$ and $d|n$ implies $d|(am + bn)$. Thus, every linear combination of m and n is a multiple of d, and the existence of the sequence P_n with increasing terms assures that no stage can be attained after which every number will be expressible as a linear combination of m and n.
So, we have, $k = m(a + b) + pb$, and now, the following cases arise.

Case 1: If $b = 0$, then $k = m(a + 0) + p.0 = ma$. Thus, k can assume any value of the form ma, and hence, K contains all multiples of m.

Case 2: If $b = 1$, then $k = m(a + 1) + p.1 = m(a + 1) + p$. Thus, k can assume any value of the form $(mq + p)$, where $q = a + 1$, and $q \neq 0$ (as $q = 0 \Rightarrow a + 1 = 0 \Rightarrow a = -1$, for $a \in \mathbb{Z}^+ \cup \{0\}$, leading to a contradiction). So, the value of the form $(mq + p)$, which is not possible, occurs at $q = 0$, and the value is $(m.0 + p) = p$. Hence, K contains all numbers of the form $(mq + p)$ except p.

Case 3: If $b = 2$, then $k = m(a + 2) + p.2 = m(a + 2) + 2p$. Thus, k can assume any value of the form $(mq + 2p)$, where $q = a + 2$, and $q \neq 0$ and $q \neq 1$ (as $q = 0$ or $q = 1 \Rightarrow a + 2 = 0$ or $a + 2 = 1 \Rightarrow a = -2$ or $a = -1$, for $a \in \mathbb{Z}^+ \cup \{0\}$ leading to a contradiction). So, the values of the form $(mq + 2p)$ which are not possible occur at $q = 0$ and $q = 1$, and the values are $(m.0 + 2p) = 2p$ and $(m.1 + 2p) = m + 2p$. Hence, K contains all numbers of the form $(mq + 2p)$ except $2p$ and $(m + 2p)$.

Continuing in a similar manner and using the intuition of the modular arithmetic involved in the finite check strategy mentioned above, we can see that there will be a total of m cases, as we are counting under modulo m. This is because if the value of b in $k = m(a + b) + pb$, is at least m then, the first term being a multiple of m will absorb the excess multiples of m from b, giving rise to a modular arithmetic structure.

Case m (Last case): If $b = m - 1$, then $k = m(a + \overline{m - 1}) + p(m - 1) = m(a + m - 1) + p(m - 1)$. Thus, k can assume any value of the form $(mq + (m - 1)p)$, where $q = a + m - 1$, and $q \neq 0, 1, \ldots, m - 2$ (as, if $q = 0, 1, \ldots, m - 2 \Rightarrow a + m - 1 = 0, 1, \ldots, m - 2 \Rightarrow a = 1 - m, 2 - m, \ldots, -1$, each of which is negative for $a \in \mathbb{Z}^+ \cup \{0\}$ leading to a contradiction). So, the values of the form $mq + (m - 1)p$ which are not possible occur at $q = 0, 1, \ldots, m - 2$ and the unobtainable values are:
$\alpha = \{(mq + (m - 1)p) \,|\, q = 0, 1, \ldots, m - 2\} = \{(m - 1)p, m + (m - 1)p, \ldots, m(m - 2) + (m - 1)p\}$

Hence, K contains all numbers of the form $(mq + (m - 1)p)$ except those belonging to the set α. Note that the largest value N, among the elements of the set α (being an indexed set of increasing values) is $m(m - 2) + (m - 1)p = m(m - 2) + (m - 1)(n - m) = m^2 - 2m + mn - m^2 - n + m = mn - m - n$. □

It has been left for the reader as an exercise to determine that out of all the numbers which could not be formed using the linear combinations of m and n, the element $mn - m - n$ is the largest. Thus, we have given a constructive proof of the Frobenius number of two numbers.

As an extension, for non-co-prime numbers, each of their combination is a multiple of their greatest common divisor, but is it necessarily the case that each multiple of their gcd can be obtained by the linear combinations. The answer is no, and the greatest multiple of the gcd of the two numbers which can't be obtained by their linear combination is called the Frobenius number of these non co-prime numbers.
If $gcd(m, n) = d \neq 1$, then $m = d.m_1$ and $n = d.n_1$, such that $gcd(m_1, n_1) = 1$, then Frobenius number

of m_1 and n_1 (co-prime numbers) is $N_1 = m_1n_1 - m_1 - n_1$. It is left as an exercise to the reader to show that the Frobenius number N, of m and n (non co-prime numbers), is d times the Frobenius number of m_1 and n_1. Thus,

$$N = d.N_1 = d(m_1n_1 - m_1 - n_1) = d\left(\frac{mn}{d^2} - \frac{m}{d} - \frac{n}{d}\right) = \frac{mn}{d} - m - n$$

Hence, in the general case, the Frobenius number N of the numbers m and n is:

$$N = \frac{mn}{gcd(m,n)} - m - n$$

Thus, all multiples of $gcd(m,n)$ can be obtained except for a finitely few, the greatest of which is mentioned above. Try substituting $m = 4$ and $n = 8$, and try to justify the negative sign.

An interesting example

Until 2012, McDonald's sold nuggets in packets of 6, 9 and 20 nuggets respectively. The Frobenius number found an interesting application when Numberphile, in its video *'How to order 43 Chicken McNuggets?'* puzzled the staff by placing an order of McNuggets exactly equal to the Frobenius number of 6, 9 and 20. So, how do we go about obtaining the Frobenius number of 6, 9 and 20, since there is no clear cut formula for the same?

Let's try to obtain what all combinations of McNuggets are possible to order. Let $k_1 = 6a + 9b$ for $a, b \in \mathbb{Z}^+ \cup \{0\}$, then $k_1 = 3(2a+3b)$. As Frobenius number of 2 and 3 is 1, hence $(2a+3b)$ can assume values of all natural numbers and zero except for 1, and for $(2a+3b) = 1$, $k_1 = 3(2a+3b) = 3(1) = 3$. Hence k_1 consists of the residue class of 0 modulo 3, except for the number 3 itself, i.e. $3\mathbb{Z}\backslash\{3\}$.

Next, consider the number $k_2 = 6a+9b+20 = 3(2a+3b)+3(6)+2 = 3(2a+3b+6)+2 = 3(t+6)+2$, with $t = 2a+3b$, where t can assume values of all natural numbers and zero except for 1. For $t = 1$, $k_2 = 3(t+6)+2 = 3(1+6)+2 = 23$. Hence k_2 consists of the residue class of 2 modulo 3, except for 23, i.e.$(3\mathbb{Z}+2)\backslash\{23\}$.

Finally, consider the number $k_3 = 6a+9b+40 = 3(2a+3b)+3(13)+1 = 3(2a+3b+13)+1 = 3(t+13)+1$, with $t = 2a+3b$, where in t can assume values of all natural numbers and zero except for 1. For $t = 1$, $k_3 = 3(t+13)+1 = 3(1+13)+1 = 43$. Hence k_3 consists of the residue class of 1 modulo 3, except for 43 i.e.$(3\mathbb{Z}+1)\backslash\{43\}$.

Every natural number must belong to one of the three residue classes modulo 3, each of which can be generated by the linear combinations of 6, 9 and 20, except for a finitely few, which are the numbers 3, 23 and 43, the largest of which is 43. Hence the Frobenius number of 6, 9 and 20 is 43.

Brainteaser: For the inquisitive minds, here is a fun puzzle based on the Frobenius number. A question paper has 50 questions to be attempted by each candidate. The candidate is awarded +5 marks for each correct answer, -2 for each unattempted question and -3 for a wrong answer. If a student can attempt any number of questions, what are the minimum possible positive marks he/she cannot obtain?
Answer: The answer is 250; $\text{FrobeniusNumber}(7,8) = 209$.

Applications

Pouring over the possibilities of ordering chicken nuggets might seem like a trivial affair, however, the idea of the Frobenius Number shows up in significant parts of reality. It's the beginning of thinking about optimization in certain areas, like the coin-based currencies we use worldwide. What denominations of coins are best mathematically? For paying at a shop, we pay the amount using a 'number' of coins, the choice of which is decided by the Greedy algorithm - using the largest available coins without getting over. Jeffrey Shallit, University of Waterloo, in 2003 found out that in the American system (using coins of 1, 5, 10, and 25 cents), the average number of coins given as a change was 4.7 coins per transaction. His research paper aimed at reducing this average, and he achieved an average of 3.89 coins per transaction, a moderately better optimization, by replacing the 10 cent coin with an 18 cent coins. He also found that optimization could also be achieved by adding new denominations. Indeed, the addition of a 32 cent coin would reduce the average to 3.46, and the addition of 83 cents would cut it down by almost a coin and a half. It can also be conferred that this average can be reduced to a remarkable 2 coins per transaction, but the denominations, in that case, would have to be 1 cent, 3 cents, 4 cents, 9 cents, 11 cents, 16 cents, 20 cents, 25 cents, 30 cents, 34 cents, 39 cents, 41 cents, 46 cents, 47 cents, 49 cents, and 50 cents. But this is not as easy as it seems, because replacing denominations to not so pleasant looking ones makes the greedy algorithm tough for the newbies-obviously counting in multiples of 10 is easier than counting in multiples of 18. Also, the addition of new denominations induces the cost in terms of carrying coins of different denominations and searching coins of a given denomination when paying the change in a transaction. Considering this trade-off, there has been no emphasis on achieving mathematical optimization in terms of the number of coins. The initiatives, if any, include the introduction of denominations of smaller rounded off denominations like those of 2 cents and 3 cents.

Bibliography

[1] Contemporary Abstract Algebra : Joseph A.Gallian, ISBN 978-81-7319-269-2

[2] The Nuggets Algorithm: VSauce

[3] Article. Sylvester's Problem

[4] How to order 43 Chicken McNuggets: Numberphile

Trisecting an Angle

Ishita Srivastava
B.Sc. (H) Mathematics, 2nd Year

Angle trisection, as the name signifies, refers to dividing a given angle into three equal parts. Though this seems quite simple, here is a very trivial point, which seeks to ask: "Is it always possible to trisect any randomly chosen angle using a compass and an unmarked straight-edge only?" This has been a classical problem of ancient Greek mathematics and art of construction. This article aims to provide a basic insight into the concept of angular trisection.

It has already been proven geometrically by Pierre Wantzel in the 19th century that it is not possible to trisect every angle. However, this, in no way, intends to say that no angle, whatsoever, can be trisected using a compass and an unmarked ruler. If we consider a compass-constructible angle θ, then an angle of measure 3θ can be trisected trivially by a compass. In fact, certain angles that are not constructible, can still be trisected with ease. For instance, given an angle $\frac{6\pi}{11}$ [$\approx 98.18°$], on trisection yields an angle of $\frac{2\pi}{11}$. This angle cannot be constructed by a compass, but four such angles can be combined to form $\frac{24\pi}{11}$, which is a 2π radian circle, leaving an extra angle measuring $\frac{2\pi}{11}$, which is equal to one-third of the original angle, and thus, its trisection. However, this method cannot be applied to all angles since all angles might not always follow a similar calculation. Angles as simple as $\frac{\pi}{6}$ cannot be trisected using this method, and hence are not 'trisectible' using a compass-straight edge combination. In addition to this, the trisection of this, which is $\frac{\pi}{18}$ radians or 20° is not compass-constructible.

After the preceding discussion, it has become clearly evident that we need a different process for trisecting angles. Apart from using highly advanced geometrical equipments or its electronic counterparts, there is a simpler way of achieving this seemingly difficult task. This is done by using Japanese Origami paper folding technique.

Origami['Ori': folding, 'kami/gami': paper] *It is the art of paper folding, which is often associated with Japanese culture. The goal is to transform a flat sheet of square paper into a finished sculpture through folding and sculpting techniques. A few Origami folds can be combined in a number of ways to make intricate designs. The best known model is the Japanese paper crane.*

Follow these basic steps in order to trisect an angle:

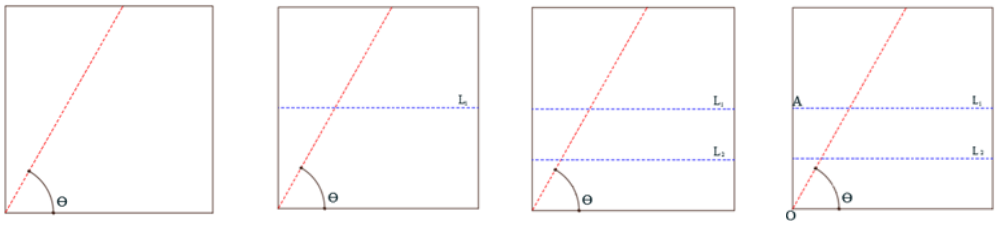


Figure 11.1: Steps 0-3

Step 0: Take a piece of square sheet and create an arbitrary angle by folding the paper such that the edge of the paper acts as the base of the angle and the crease created by the fold (which meets the base edge at the bottom left corner) acts as the arm of the angle. Mark this as θ. Unfold it and proceed.

Step 1: Fold the paper into half horizontally, and call this crease L_1. Unfold it.

Step 2: Then, fold the lower edge upto L_1 and call this second crease as L_2.

Step 3: Mark the lower left point of the paper (that is, the point where angle θ originates) as O and the left end of crease L_1 as A.

Step 4: Fold the paper such that point O matches (or lies on) the lower crease, that is, L_2 and the point A matches the crease which defines the angle θ. Press the paper at this step to create another crease L_3.

Step 5: Mark the point on L_2 where point O matches the crease, during the creation of L_3 as B.

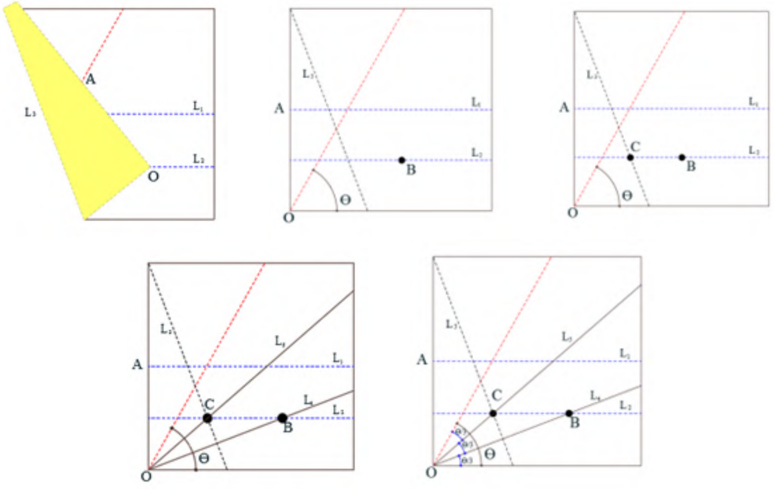


Figure 11.2: Steps 4-8

Step 6: Unfold the paper and locate the point where L_3 intersects L_2. Mark this point as C.

Step 7: Now, fold the paper so as to form two new creases; one which connects O and B, and the other which connects O and C. Call them L_4 and L_5 respectively.

Step 8: The newly formed creases L_4 and L_5 are the ones which trisect the angle θ.

Thus, we see that trisecting an arbitrary angle, which is not always possible using a compass and a straight-edge only, can easily be done through this simple paper folding technique.

Now, the careful and curious reader must have a very genuine question in mind, and without answering it, this article would be incomplete. You must have pondered upon 'the secret super powers' of Origami. Putting the question into simpler words, "What does Origami do to the paper, which a compass and a straight-edge are unable to, that allows trisecting an angle with such ease?" This property is owed to the methods that Origami provides for finding the solutions (or roots) not just of quadratic, but of cubic equations as well. The answer to this question lies in the fact that L_3 is a shared tangent of two parabolas (as mentioned earlier), combined with the methods of Origami for finding roots of quadratic and cubic equations. This is what makes an angle 'trisectible' using the techniques of Origami.

Bibliography

[1] Wikipedia : Origami

[2] How to trisect angle using Origami: Numberphile

[3] Article. Angle Trisection: DivisByZero

[4] Trisecting an Angle: plus Magazine

The Bizarre 25-Card Trick

Aman Chaudhary
B.Sc. (H) Mathematics, 2$^{\text{nd}}$ Year

Magic, especially with cards, has been a source of interest for people of all ages since a long time. Mathematics, which seems monotonous from a superficial view, has given rise to countless fantastic tools. One such amazing trick, dealing with 25 cards, shows how many lighthearted applications have deeply rooted mathematical concepts.

Aim: You are going to ask your friend to pick a number from 1 to 25 and also any card from the shown 25 cards. By performing the steps below, you will be able to "magically" make the chosen card appear at the very chosen number.

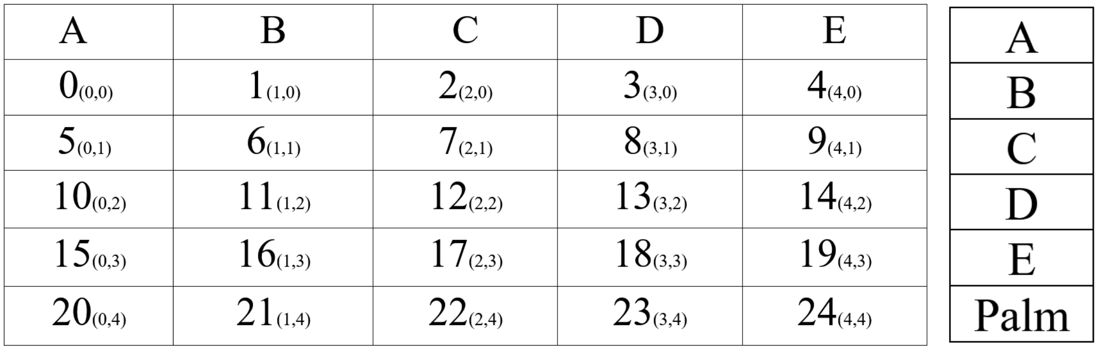
The trick is performed by the steps given below. Consider your friend's name to be Ram. Also consider side A of a card to be the "face", or the side denoting the suit and number of the card, and side B to be the "back", or the side which is blank.

1. Take out 25 cards randomly from a usual deck of 52 cards to play the trick with.

2. Showing the deck to Ram, ask him to pick any card from the 25-card deck. Also, ask him to choose any number between 1 and 25 and let you know his choice.

3. Now consider, he chooses 12 as his number and Ace of Spades (present in those 25 cards) as his card.

4. Hold the deck such that side A faces downward in your palm. Now distribute the 25 cards one by one such that side A faces upward while the cards are laid out into 5 piles having 5 cards each (Fig. 1 illustrates that the cards are distributed in such a way that the 1$^{\text{st}}$ card lies in 1$^{\text{st}}$ pile, 2$^{\text{nd}}$ card in 2$^{\text{nd}}$ pile and so on until the 5$^{\text{th}}$ card, and then the 6$^{\text{th}}$ card in the 1$^{\text{st}}$ pile and the 7$^{\text{th}}$ card in the 2$^{\text{nd}}$ pile again and so on).



A	B	C	D	E
$0_{(0,0)}$	$1_{(1,0)}$	$2_{(2,0)}$	$3_{(3,0)}$	$4_{(4,0)}$
$5_{(0,1)}$	$6_{(1,1)}$	$7_{(2,1)}$	$8_{(3,1)}$	$9_{(4,1)}$
$10_{(0,2)}$	$11_{(1,2)}$	$12_{(2,2)}$	$13_{(3,2)}$	$14_{(4,2)}$
$15_{(0,3)}$	$16_{(1,3)}$	$17_{(2,3)}$	$18_{(3,3)}$	$19_{(4,3)}$
$20_{(0,4)}$	$21_{(1,4)}$	$22_{(2,4)}$	$23_{(3,4)}$	$24_{(4,4)}$

A
B
C
D
E
Palm

Figure 12.1: The 25 cards in five piles

5. Meanwhile, you unfold the cards, Ram will notice his card going in any of the 5 piles. Since the required card is unknown to you, ask Ram to tell which pile contained his required card. Consider he replies "the first pile".

6. Then, collect all the cards pile wise (side A facing upwards) without disturbing their positions and place the 1^{st} pile (containing the required card) at the second position i.e. at position B (as shown in Fig. 1). While placing them back in the palm for the next distribution, rotate the cards upside down such that side A faces downward, and distribute the cards again likewise as done in Step 4. Note that while placing the piles back into the palm, no internal position of cards of any pile is disturbed.

7. Again, ask for the pile of 5 cards containing the required card. Suppose he says the 1^{st} pile again. Gather the cards again (as done in the last step), but this time placing the required pile as the 3^{rd} position from the top of your palm (side A facing up).

8. Start unrolling the cards one by one and here it is, the selected card. The Ace of Spades comes up on the 12^{th} position at chosen in the deck of 25 cards.

Now let us discuss the underlying procedure and start unwrapping the mystery.

Consider that the 25 cards are laid down such that side A faces up in five decks of five each as shown in the Figure 1 with A, B, C, D, E denoting each pile of 5 cards. This shows how those 25 cards have been distributed and since all this is random, any card of any suit and number may be present at any place. The reader might wonder at once why the cards numbered 0 to 24 and not 1 to 25. It is at this point that we demystify the trick.

1. Subtract 1 from the number Ram has chosen then express the resultant in the *base* 5 notation. So, if number is k, write $k-1$ in the form $k-1=a+5b$ with each of $0 \leq a, b \leq 4$. The values of (a, b) pairs are shown in subscript of each number in the table.

2. We then picked up the cards pile wise and positioned them such that side A faces up in your palm. But here lies the real trick in placing the piles in their appropriate position. Consider numbering up the decks as $0, 1, 2, 3$ and 4, such that 0 lies on the top of your palm and then followed below by $1, 2, 3$ and then the pile numbered 4 at the bottom. Since $k-1$ was represented as $k-1=a+5b$, so the very first time we pick the piles, the pile that contains Ram's card should be placed at the a^{th} position on your palm and all the other decks can be placed elsewhere. As we took for example that he chose 12, we express $11 = 1 + 5 * 2$ and that's why the pile he pointed first time was put at the second position from the top (numbered 1 in *base* 5 as per our notation).

3. Flip the cards (side A faces down in your palm), and distribute them again in 5 piles as was done above and again ask Ram to tell the pile that contains his card. Again pick up the cards pile wise (side A faces up), and now place the pile with the required card at the b^{th} position on your palm. That's why the pile pointed by ram for the second time was put at the 3^{rd} position from the top (numbered 2 in *base* 5 as per our notation). Put the gathered deck of those 25 cards (side A facing up) in your palm. Count out the cards from the top, and here it is k^{th} card turned over is the very same card that Ram selected.

Here we are with the deep mathematical insight for *base* 5:

Think of the 5 piles of cards as the zeroth pile, the first pile, the second pile, the third pile, and the fourth pile, and think of the a^{th} card in each pile where $0 \leq a \leq 4$. Thus we count our piles and cards in each pile starting with 0 instead of 1 just as we did while numbering the cards in the deck from 0 to 24 rather than from 1 to 25. For the trick to work, we first determine where the chosen card appears as the a^{th} card in the b^{th} pile after the two dealing with $0 \leq a, b \leq 4$.

Illustration: Consider for $a = 3$, the cards of the selected pile will appear as card numbered 3 in all the piles number $0, 1, 2, 3$ or 4 and as soon as the pile of cards is pointed out the second time, placing the pile at any position $b = 0, 1, 2, 3$ or 4 gives the resultant $3, 8, 13, 18$ or 23 respectively, since we know that these values of b correspond to the upper resultants in the *base* 5 decoded version. And hence a total of $5 * b + a$ cards appear on the top of the required card giving the required card at $((5 * b + a) + 1)^{\text{th}}$ position from the top, when the cards are being rolled out (side A facing up in the palm) for the required number with the value of k chosen as $4, 9, 14, 19$ or 24.

Trivially, looking for $a = 0$, the cards of the pointed pile will appear on the 0^{th} position in all the 5 piles (facing upwards) and on pointing the pile the second time and placing it as the b^{th} pile leads to positioning of the required card on required numbers as $1, 6, 11, 16$ or 21 for different choices of b.

But you might be thinking what is bizarre about this trick. Let us understand why this card trick is so beguiling. Not only this trick deals with number asked randomly from the person, but, if you have a pack of x^y cards in total, then you can show this trick by distributing the cards into x piles, and doing the distributing task y times, you can place the required card at any given position in the deck with the newly specified number of cards. Following the same steps: decrease one from the designated position number, and convert the result to *base* x as a y digit number. The ones digit of the computed number tells you where to place the pile containing the required card after the first deal with $n - 1$ as the bottom pile and 0 as the topmost one, and the procedure continues for the remaining $y - 1$ deals as well.

Bibliography

[1] Article. Mathematics, Magic, and Mystery: Mathaware

[2] Article. The Twenty-Seven Card Trick: Calvin T. Long

[3] brilliant.org

The Bedrock of Artificial Intelligence

Sahil Singh
B.Sc. (H) Mathematics, 1st Year

Famous American Mathematics and Science writer Martin Gardner once said, "Mathematics is not only real, but it is the only reality." It is indeed true. Mathematics in itself is an extremely vast subject and to add to that, it is the basis of a number of other fields. One such field is Artificial Intelligence.

Introduction

We have all heard how mathematics is all around us, but what we might not realise is that Artificial Intelligence is all around us too. In the midst of the conversations about the marvelous (and sometimes dangerous) future which AI holds for us, with its autonomous cars, AI robots, huge potential in healthcare, education and so on, we fail to acknowledge its contribution in our current day to day lives.

Google's AI-Powered Predictions for Google Maps analyses the movement of traffic at any given time by collecting anonymous location data from mobile devices; ride sharing apps like Ola and Uber use the help of AI in determination of price, minimization of wait time and detours; commercial flights use AI autopilots, reducing human involvement time to 7 minutes, that too only for take-off and landing; in email, the spam filter and the smart categorization of email; plagiarism checker; in banking/personal finance, AI is used to determine and prevent fraudulent transactions, and also in credit decisions; in social networking, Facebook uses AI to recognize faces and suggest tags, Instagram uses machine learning to identify contextual meaning of emojis, even the Snapchat filters are possible because of AI; online shopping sites use our search to automatically recommend relevant items etc.

The list is indeed long, and it also includes our current favorites of AI applications, which is Smart Personal Assistants. Be it Google Assistant, Siri, Alexa or Cortana, these assistants have played a huge role in making our lives more convenient, all by using voice-to-text technology. They are still going strong in cementing the pathway between humans and "smart" homes. And this is just the beginning.

One of the biggest reasons Artificial Intelligence has been able to achieve so much, and still has the potential to achieve so much more, is mathematics. Professor Angel Garrido, Faculty of Science, UNED, Madrid wrote, "Mathematics and Artificial Intelligence are two branches of the same tree." To put it simply, Artificial Intelligence is mainly a blend of mathematics and programming.

Having a mathematical degree is not an absolute necessity in order to make neural networks for AI, but the people who write the algorithms, do the research and investigate the boundaries of AI capabilities cannot go far without learning the mathematics involved. This is why mathematics is essential for AI and machine learning, because it guides us in how we can solve very difficult deep abstract problems and it does that by using methods and techniques already known. Artificial intelligence is described as a technology which enables a machine to simulate human behavior and machine learning is a division of AI which allows a machine to automatically learn from past data without having to be explicitly programmed to do so.

Mathematics Branches Essential for Artificial Intelligence

The topics of mathematics that are used in AI include Calculus, Linear Algebra, Probability & Statistics.

- **Linear Algebra**: Used in Machine Learning to define the parameters and structure of different machine learning algorithms. This helps understand how neural networks are put together and how they are operating.

  Important topics are:

  - Singular value decomposition
  - Special Matrices and Vectors Eigenvalues and
  - Matrix Norms
  - Principal component analysis
  - Scalars, Vectors, Matrices, Tensors

- **Calculus**: Used to augment the sophistication part of machine learning. This is what makes AI learn from examples, update the parameters of different models from time to time and make the performance better altogether.

  Important topics are:

  - Derivatives (Scalar Derivative-Chain rule), Partial and Directional Derivative
  - Integrals
  - Differential Operators
  - Gradients
  - Convex Optimization
  - Gradient algorithms- local/global maxima and minima, SGD, NAG, MAG, Adams

- **Probability Theory**: Used for making assumptions about the underlying data when we are designing these deep learning or AI algorithms. It is essential to understand the key probability distributions.

  Important topics are:

  - Random Variables
  - Distributions (Binomial, Bernoulli, Poisson, Exponential, Gaussian)
  - Variance and Expectation
  - Elements of Probability
  - Bayes' Theorem, MAP, MLE
  - Special Random Variables

Conclusion

The foundation of artificial intelligence, like more or less everything related to computers, is based on mathematical concepts. If we discuss about deep learning (a subpart of AI), a lot of it is based on mathematics taught at the undergraduate level, such as the concepts of matrices, calculus and so on.

Different research papers in the pertinent areas and careful examination into any effective algorithms in Artificial Intelligence can make it clear that the pillar of it is pure mathematics. In ANN (Artificial Neural Network), which is an algorithm in AI, the principal working of it is designed using differential calculus, and it holds true for other learning algorithms. The core plan is almost always a result of a set of equations. Therefore, for research on finding new algorithms, some might even feel mathematics is more relevant than even computer science in the field of Artificial Intelligence.

Bibliography

[1] Article. Mathematics for AI: Medium

[2] Article. Everyday Examples of Artificial Intelligence and Machine Learning: Emerj

[3] Article. Mathematics and Artificial Intelligence: Science Direct

[4] Article. The Future Of Artificial Intelligence Builtin

Mathematics in Art

Utcarsh Mathur
B.Sc. (H) Mathematics, 1st Year

One of the biggest misconceptions prevailing in society is that Mathematics is just about numbers, equations and complex formulae. However, Mathematics encompasses much more than these. Mathematics is a discipline connected to many others and cannot be studied in isolation. Historically, Mathematics has been intimately related to art. Many mathematicians have, in fact, called Mathematics an art itself.

The relationship between Mathematics and Art bloomed from the 15th century onwards, during the Renaissance Period, particularly during the High Renaissance. Works of artists focused on what came to be known as "Realism", that sought to depict the world as is; with its perfection as well as its fallacies. An intricate knowledge of geometry, ratio and proportion also aided the artists. In fact, the concept of a 'Renaissance Man' came into being; a person with multiple talents and knowledge in multiple disciplines. Works of artists such as Leonardo da Vinci (1452-1519) and Albrecht Dürer (1471-1528) depict the same. One particular work of art, The Vitruvian Man by Leonardo da Vinci, highlights how Mathematics and Art were intertwined.

Also called "The Proportions of the Human Body according to Vitruvius", the Vitruvian Man is a 15th century drawing that is accompanied with notes (written in mirror writing) that depict the ideas of Roman architect Marcus Vitruvius Pollio, as described in Book III of his treatise De Architectura. Rendered in pen, ink and metal point on paper, the drawing depicts a man standing within a circle and a square. It shows the man with his legs vertical and arms horizontal superimposed on the image of him with arms and legs stretched out. It may be noticed by examining the drawing that the combination of arm and leg positions creates sixteen different poses.

Squaring a Circle

The Vitruvian Man is believed to be Leonardo's attempt to solve the ancient greek geometric problem of Squaring a Circle. The challenge is to construct a square and a circle of equal area using only a compass and a straightedge. It has been proved, however, that it is impossible to solve this problem due to the transcendental nature of Pi. Vitruvius believed that the naval was the center of the human body that could be inscribed in a circle with arms and legs stretched out. He also believed that the armspan was equal to the height of the human and thus could place the body perfectly inside a square. Leonardo used the ideas of Vitruvius to metaphorically solve the problem by depicting mankind to fit the square and the circle. He thus uses the human body as a possible solution.

Perfect Proportions

Leonardo also depicts ideal body proportions in the drawing. He has drawn the Vitruvian Man with utmost dexterity. The accompanying notes explain the same:

- four fingers equal one palm

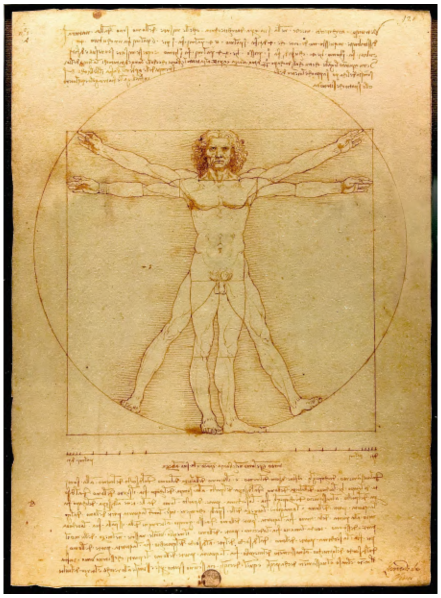


Figure 14.1: The Vitruvian Man by Leonardo da Vinci

- four palms equal one foot
- six palms make one cubit
- four cubits equal a man's height
- four cubits equal one pace
- 24 palms equal one man

Further, in the second block of notes in the drawing, da Vinci discusses "15 proportional rules" for drawing the human body that may be summarized as follows:

- The length of the outspread arms is equal to the height of a man
- From the hairline to the bottom of the chin is $1/10^{\text{th}}$ of the height of a man
- From below the chin to the top of the head is $1/8^{\text{th}}$ of the height of a man
- From above the chest to the top of the head is $1/6^{\text{th}}$ of the height of a man and so on

Leonardo's collaboration with Luca Pacioli, the author of *Divina proportione* (Divine Proportion) have led some to speculate that he incorporated the golden ratio in Vitruvian Man, but this is not supported by any of Leonardo's writings, and its proportions do not match the golden ratio precisely. The Vitruvian man is likely to have been drawn before Leonardo met Pacioli. Leonardo, through the Vitruvian Man, sought to depict the perfection of nature manifested in the form of a human being. Both him and Vitruvius believed that just like the human being was perfect and proportionate, so should architecture be. Many architects such as Andrea Palladio (1508-1580) also applied the ideals of proportion but forth by Leonardo and Vitruvius in his works.

The Vitruvian Man has many layers of meaning. Many believe that da Vinci was trying to depict the Neoplatonic idea of 'The Great Chain of Being'. This idea is prevalent in many religions. It follows that the world is hierarchically divided into a chain consisting of different elements of the Earth, and mankind is placed right in the middle of this chain.

Conclusion

Mathematics is a dynamic discipline that can be seen everywhere. Italian astronomer Galileo Galilei, in his *Il Saggiatore* wrote that "[The universe] is written in the language of mathematics, and its characters are triangles, circles, and other geometric figures." Besides the Vitruvian Man, artworks such as The Mona Lisa and The Last Supper, also by da Vinci have a mathematical dimension to it. Mathematics can likewise be seen in architecture, for example, in the Notre Dame, Paris, the Great Mosque of Kairouan, the Parthenon and so on, which are said to be demonstrated by the golden ratio. Mathematics has roused textile arts, such as quilting, knitting, cross-stitch, crochet, weaving etc, Turkish and other rug making, as well as kilim. In Islamic craftsmanship, symmetries are obvious in structures as varied as the Persian girih and Moroccan zellige tilework, Mughal jali punctured stone screens, and across the board muqarnas vaulting.

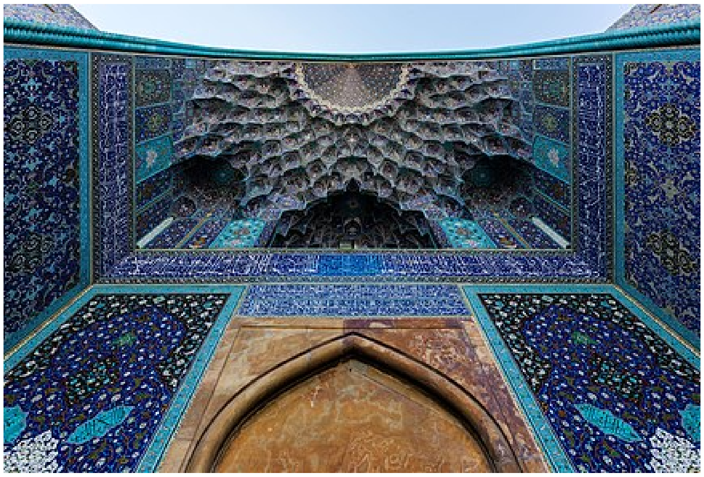


Figure 14.2: Shah Mosque, Isfahan, Iran

The mathematician Jerry P. King describes mathematics as an art, stating that "the keys to mathematics are beauty and elegance and not dullness and technicality", and that beauty is the motivating force for mathematical research. The beauty of Mathematics is in fact, enhanced when incorporated with other disciplines, especially art.

Bibliography

[1] Wiki. The Vitruvian Man

[2] Article. The Elegant Mathematics of the Vitruvian Man

[3] Article. The Significance of Da Vinci's Vitruvian Man

[4] A Human Body Mathematical Model Biometric Using Golden Ratio: Evon Abu-Taieh, Hamed S. Al-Bdour

[5] Human Modeling in Information Technology Multimedia Using Human Biometrics Found in Golden Ratio, Vitruvian Man: Evon Abu-Taieh, Minwer El-Maheed, El-Maheed, Alia Abu-Tayeh, Jeihan Abu Tayeh, Abdullah El-Haj

Pi and the Great Pyramid of Giza

Anvesha Kushwah
B.Sc. (H) Mathematics, 1st Year

The oldest of the Seven Wonders of the Ancient World, The Great Pyramid of Giza, also known as the Pyramid of Khufu or the Pyramid of Cheops, situated in Cairo, Egypt, is really a thought provoking enigma.

The value of the mathematical constant π seems to have designed into the Great Pyramid to a value of about 3.1419. But we know that this value of π was not discovered at that time with such accuracy. A very interesting point here is that how did the Egyptians know or use an approximate value of π? The explanation of this question involves a simple scientific logic. Let us find it out.

Measurements of the Great Pyramid of Giza

We can't get the exact measurement of the Great Pyramid because of the removal of the outer limestone layer and the top capstone for other construction projects. So the measurements vary slightly according to the different sources.

The Egyptians used a different unit of length measurement, royal cubit. A royal cubit is the distance from the elbow to the extended middle finger.

$$1\,Royal\,Cubit = 52.37cm$$

The original height of the Pyramid was about 146.64m or 280 cubits before the removal of the top capstone blocks. The length of the four sides of the Great Pyramid of Giza vary from 230.25m to 230.45m or about 440 cubit long (or 230.25m, 230.36m, 230.39m, 230.45m).

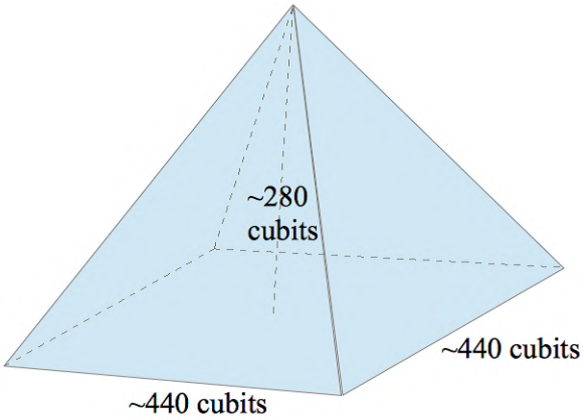


Figure 15.1: Dimensions of the Great Pyramid of Giza

Now with these details, if we take half of the perimeter of the Pyramid's base

$$230.25 + 230.36 + 230.39 + 230.45 = 921.45m$$

$$\Rightarrow \frac{921.45m}{2} = 460.275m$$

And if we divide it by its height, the result is very close to π.

$$\frac{460.275m}{146.64m} = 3.1419 = \pi$$

Or alternatively if we use the cubit unit measurements we get

$$\frac{440\,cubit * 2}{280\,cubit} = \frac{22}{7} = 3.1429$$

The key to the mystery of how the Egyptians incorporated π was derived by the another mystery of The Great Pyramid of Giza. How were they able to make the lengths of all the four sides of the Great Pyramid so precise (within 10 cm) to each other over a distance of 230m? The only technology that existed at that time that would give the Egyptians the precision they needed to match all the four side lengths was a trundle wheel. If π was involved, it indicates that a wheel, which has π built-in, was somehow involved. A trundle wheel is just a wheel that is rolled a number of times in order to measure distance and it is a technology that is commonly used even today on sports fields and by surveyors.

It is believed that the Egyptians made a trundle wheel carved out of rock with diameter of exactly 1 cubit. Then they rolled it on flat ground so the trundle wheel rock rolled exactly 140 times around for each of the four sides of the Pyramid. Therefore, it was rolled a total of 280 times around from one corner of the Great Pyramid to the farthest corner on the other side. Through this they obtained precise locations of the corners of the Great Pyramid and then they started to pile the massive blocks to build the pyramid. They piled the blocks of the pyramid until they obtained a height of 280 cubits. The point to note here is that they couldn't easily roll the trundle wheel straight up, so instead, they counted the same number of cubits to obtain the height. So they counted 280 turns of the trundle wheel from one corner to the opposite corner and measured 280 cubits high from the ground to the peak. Because they used a trundle wheel which has the value of π built into it with the relationship between the circumference and the diameter, the value of π was automatically built into the Great Pyramid without the Egyptians knowing the value of π.

$$\frac{Distance\ from\ one\ corner\ to\ the\ opposite\ corner}{Height\ of\ the\ Great\ Pyramid} = \frac{280 * \pi * 1\,cubit\ diameter}{280\,cubit\ diameter} = \pi$$

But the next point to observe is that even with a base having four exact measured sides, the Egyptians could have made a rhombus not a square. According to one source, the difference in the distances between the opposite corners is within 17cm, which means they indeed obtained corner angles very close to 90°. They got this angle by measuring the diagonals to be of matching length or used the Pythagoras theorem.

The Pyramid's dimensions suggest that the Egyptians may have known about some Pythagoras Triangles. According to one source they called such triangles as "Holy Triangles". But if we apply the Pythagoras Theorem, we obtain 197.99 turns for the diagonal, or hypotenuse, which is not an integer value but still very close. Perhaps, the Egyptians didn't know about Pythagoras triplets, but instead knew "Pythagoras Isosceles Triplets" which are close to being integers. And as a matter of fact, there will never be exact Pythagorean isosceles triplet because the hypotenuse will be $\sqrt{2}$ times the triangle side and $\sqrt{2}$ is irrational. They used 70-70-99 triplet option to make the pyramid design much more feasible.

One more interesting fact about this pyramid is that $140/99 = 1.4141\ldots$ which is close to $\sqrt{2}$, so were the Egyptians aware of this number? But this is the case with all the Pythagorean Isosceles Triplets and of course these patterns will naturally always be built-in with a square base.

But if the Egyptians used the above design of 70-70-99 triplet, they would have used exactly 99 turns of the trundle wheel for the diagonal which would have made the expected right angle inaccurate because of the error in Pythagorean Isosceles Triplets. Using the Cosine Law: $c^2 = a^2 + b^2 - 2ab\cos C$ which gives C=90.00585°, which is slightly more than right angle. This implies that the Pyramid would be slightly indented half way on each side towards the middle of the pyramid because the angle

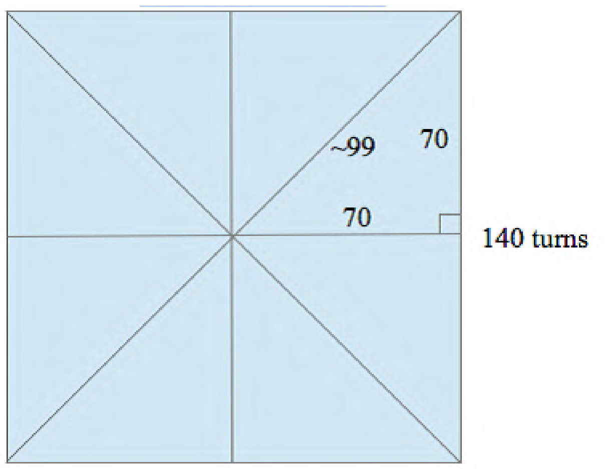


Figure 15.2: 70-70-99 Pythagorean Triplet in Pyramid's base

in the middle would be double of 90.00585° which is 180.0117°. And this indent actually exists in The Great Pyramid of Giza. It is the only Pyramid to have this characteristic. So the above 70-70-99 design seems to confirm the hypothesis of the construction of The Great Pyramid of Giza.

Bibliography

[1] Wiki. Great Pyramid of Giza

[2] Wiki. Ancient Egyptian units of measurement

[3] Article. Pi and the Great Pyramid of Giza article: Blair Yochim

[4] Article. Great Pyramid Edges

Mathematical Facts

Gaurav Kumar
B.Sc. (H) Mathematics, 2^{nd} Year

1. **A prime number p (greater than 2) can be represented as a sum of 2 squares if and only if it is of the form $\mathbf{p = 4k + 1}$.**

   Let p be a prime that can be represented as a sum of 2 squares.
   Let $p = a^2 + b^2$, $a \equiv$\{0,1,2,3\}(mod 4) and $a^2 \equiv \{0, 1, 4, 9\}$(mod 4) or simply saying $\{0, 1\}$(mod 4) because $9 \equiv 1$(mod 4) and $4 \equiv 0$(mod 4).
   Similarly, $b^2 \equiv \{0, 1\}$(mod 4) and adding both will give $a^2 + b^2 \equiv \{0 + 0, 1 + 1, 0 + 1\}$(mod 4) or $p \equiv \{0, 1, 2\}$(mod 4) since $p = a^2 + b^2$.
   If $p \equiv 0$(mod 4) or $p \equiv 2$(mod 4) then p will be a multiple of 2, which can't be true since p is a prime greater than 2.
   So $p \equiv 1$(mod 4), or $p = 4k + 1$, which was to be shown.

   But the converse is not that simple. A (relatively) small proof was given by *Zagier*.
   Let $p = 4k + 1$ be prime , let $\mathbb{N}$ denote the natural numbers, and consider the finite set $S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$ of triples of numbers.
   It is non-empty because the values $x = 1$, $y = 1$, $z = k$ satisfy $x^2+4yz = p$. Then S has two involutions *(An Involution is a function $f : S \to S$ such that $f(f(x)) = x$)*: one is $(x, y, z) \to (x, z, y)$ and it only has fixed points of type (x, y, y) and these fixed points corresponds to representations of p as sum of 2 squares $p = x^2 + (2y)^2$.
   A more complicated involution is

$$(x, y, z) \to \begin{cases} (x + 2z, z, y - x - z), & if\ x < y - z \\ (2y - x, y, x - y + z), & if\ y - z < x < 2y \\ (x - 2y, x - y + z, y), & if\ x > 2y \end{cases}$$

   This involution has only fixed point $(1, 1, k)$. For every values of (x, y, z) the mapping of x is $(x + 2z)$ or $(x - 2y)$ or $(2y - x)$ only. For a fixed point, it has to map to one of the 3 points. If $x = x + 2z$, then $z = 0$. If $z = 0$ then $p = x^2$ which is not true since p is prime.
   Similarly x can't map to $x - 2y$, so it can only map to $2y - x$ which means $2y - x = x \Rightarrow x = y$. Now since $x = y \Rightarrow\ p = x^2 + 4xz \Rightarrow\ p = x(x + 4z)$ and $x = 1$ because p is prime and can't have any factors other than 1.

   Two involutions on the same finite set must have sets of fixed points with same parity, and since the second involution has odd number of fixed points, the first involution will also have a fixed mapping. Hence $\exists$ integers $x, y : p = x^2 + (2y)^2$. Thereby proving the theorem.

2. **Cross-Ratio of four collinear points on a line is constant**
   Cross-Ratio of four collinear points on a line is defined as $(A, B; C, D) = \frac{AC \cdot BD}{BC \cdot AD}$
   Now here we have 4 distinct lines $A^{'}S, B^{'}S, C^{'}S, D^{'}S$ which pass through the same point S and here the cross ratio of lines is invariant which means,

$$\frac{AC \cdot BD}{BC \cdot AD} = \frac{A^{'}C^{'} \cdot B^{'}D^{'}}{B^{'}C^{'} \cdot A^{'}D^{'}}$$

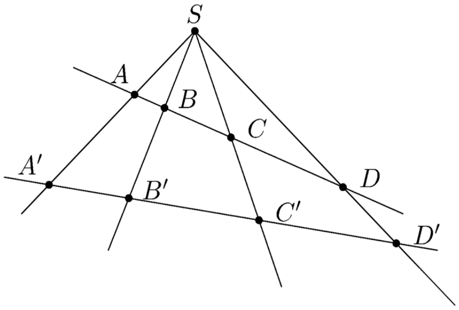


Figure 16.1: Invariance of Cross-Ratio

Consider the line AD and the triangles $\triangle ASD, \triangle BSC, \triangle BSD, \triangle ASC$.
Now By *Law of Sines* in $\triangle ASC$

$$\frac{\sin(\angle ASC)}{AC} = \frac{\sin(\angle SCA)}{SA} \Rightarrow AC = \frac{\sin(\angle ASC)}{\sin(\angle SCA)} \cdot SA$$

Similarly,

$$BD = \frac{\sin(\angle BSD)}{\sin(\angle SDA)} \cdot SB\,, BC = \frac{\sin(\angle BSC)}{\sin(\angle SCA)} \cdot SB \textit{ and } AD = \frac{\sin(\angle ASD)}{\sin(\angle SDA)} \cdot SA$$

Now, by putting these values in cross-ratio and simplifying we get,

$$\frac{AC \cdot BD}{BC \cdot AD} = \frac{\sin(\angle ASC) \cdot \sin(\angle BSD)}{\sin(\angle BSC) \cdot \sin(\angle ASD)}$$

We can see the cross-ratio comes in terms of angles between the 4 lines $A^{'}S, B^{'}S, C^{'}S, D^{'}S$, which are fixed as the value of angles do not change. Hence we can deduce that :

$$\frac{AC \cdot BD}{BC \cdot AD} = \frac{A^{'}C^{'} \cdot B^{'}D^{'}}{B'C' \cdot A'D'} = \frac{\sin(\angle ASC) \cdot \sin(\angle BSD)}{\sin(\angle BSC) \cdot \sin(\angle ASD)} = \text{K(Constant)}$$

3. **There are infinitely many primes.**
To prove this, let's suppose there are finitely many primes. So we can have a set
$S = \{p_i | p_i \text{ is a prime}\}$ and the set will be finite. Let $|S| = n$ and now consider the number

$$P = p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1$$

Now, by Fundamental Theorem of Arithmetic, any natural number can be written as product of prime numbers. Now since we have finite primes, P can only be written as a product of primes $p_i \in S$. Since P itself is not a prime due to the hypothesis that there are finitely many primes. So $\exists\ p_i \in S : p_i | P$ and also $p_i | (P-1)$ because $P-1$ is a product of all those primes. Hence p_i must divide 1 because it is a factor of $P, P-1$, which is a contradiction since $p_i \geq 2$. Thereby proving the result.

4. **Fermat's Last Theorem**, also known as **FLT**, states that there are no integer solutions of the equation $x^n + y^n = z^n$ for $n \geq 3$. It was conjectured by *Fermat* in the margin of the book he was reading, *Arithmetica* by Diophantus. He wrote in Latin "rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non capere" which meant "I have discovered a truly marvellous demonstration of this proposition that this margin is too narrow to contain." Fermat had written a lot of these annoying notes in that book. His son published a new version

of *Arithmetica* with all these notes printed in the text. One by one, all the undiscovered proofs of all those notes/conjectures were found, except for this case, for which no one discovered a proof. Fermat's Last Theorem is called so because it was the last conjecture that wasn't proved. Everyone tried a lot, but failed to prove this conjecture, which made it even more marvellous. Even after 300 years after publishing the book no one was able to find a proof.

Now, the happy ending starts with a 10 year old *Andrew Wiles*, who was reading *The Last Problem* by ET Bell. He found the Fermat's Last Theorem and was fascinated by it. He talked about the problem with his fellow students, his teachers, and attempted to prove it, but couldn't. He went on to purusue his Ph.D, he was still obsessed with the problem. There was a conjecture known as the "Taniyama-Shimura-Weil conjecture", which stated that elliptic curves over rational field are related to modular forms. In 1986 *Gernhard Frey* suggested that Taniyama-Shimura conjecture for semi-stable elliptic curves implies **FLT** which was later on proved by *Jean Pierre Serre*. With the news of this proof, Andrew Wiles' ambition to prove the Fermat's Last Theorem was reignited and he thought he could prove the Taniyama-Shimura conjecture. Since it was such an ambitious project, Wiles decided to work on it secretly. He started to spend a lot of his time on the problem, and worked for **7 years** in complete secrecy. At the end of those 7 years, he realized that he had proved the Taniyama-Shimura conjecture for semi-stable elliptic curves. He went to Cambridge and presented a proof of the theorem. The world cheered for him and he became a heroic figure. His paper was massive in size and scope. But in the proof-reading, a flaw was found in his paper. Wiles thought he could fix it, but the more he tried, the worse the problem became and it took him almost an year with his student *Richard Taylor* to solve the problem. Finally in 1995, a formal proof was published. In the end, the quote by Piet Hein

"Problems worthy of attack
prove their worth by fighting back."

is suitable for this situation. It seemed like **FLT** was fighting hard, but Wiles' dedication and his proof were just too good.

5. **Riemann Hypothesis** is one of the **7 unsolved Millennium prize problems** offered by the *Clay Institute of Mathematics.* It states that the value of Riemann zeta ζ function has its zeroes only at the negative even integers and with complex numbers having real part $\frac{1}{2}$. It is one of the most important unsolved problem in mathematics. It was based on the work of *Bernhard Riemann*, done in 1859.
Now, Riemann Zeta function ζ is defined for complex number s as,

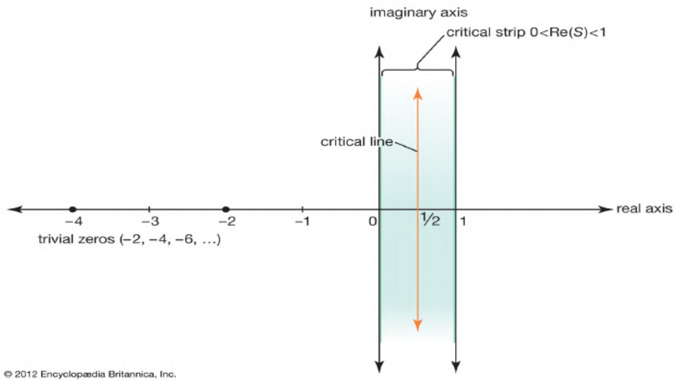
$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

For example, for $s = 2$, we get $\zeta(2) = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots$ which is a convergent series and it converges to the value $\frac{\pi^2}{6}$. The definition given above for the ζ function is only applicable for s with real part greater than 1. This series was already considered by *Leonhard Euler* and it was used to solve the Basel problem.
Now, for $s > 1$, it is quite easy for discussing the value of Riemann Zeta function, because it can be easily shown that the series will be convergent. Riemann tried to make sense of the function outside the set $S = \{s = a + \mathbf{i}b,\ a > 1,\ s \in \mathbb{C}\}$. He tried to extend the domain of ζ function using analytic continuation. One of the examples is shown below:

$$\left(1 - \frac{2}{2^s}\right) \zeta(s) = \eta(s) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n^s}$$

The series on the right is convergent for s whose $\text{Re}(s) > 0$. In this fashion the domain of the ζ function can be extended to the Complex plane. The argument doesn't work for $s = 1$; the function is not defined at $s = 1$. Also, *Euler* found that :

$$\zeta(s) = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1} = \frac{1}{\left(1-\frac{1}{2^s}\right)\left(1-\frac{1}{3^s}\right)\left(1-\frac{1}{5^s}\right)\left(1-\frac{1}{7^s}\right)\cdots}$$



© 2012 Encyclopædia Britannica, Inc.

Figure 16.2: Riemann conjectured that all zeroes of the ζ function lie on the critical line

The trivial zeroes of the ζ function are the negative even integers. It can be shown easily that for negative even integers, the ζ function is 0. Also, the ζ function is never zero when $\text{Re}(s) < 0$ except for the negative even integers. So, the zeroes must lie in the strip from 0 to 1 and hence Riemann started to find a few of them. He found that a few of the zeroes lie on the critical line and then he conjectured that all the zeroes lie on the critical line.

The Riemann Hypothesis is quite useful for finding the distribution of prime numbers. Prime numbers are of great significance in Number Theory. It can also be used to find strong bounds on a lot of arithmetic functions including the prime counting function. Many propositions across modern mathematics depend on the unproven Riemann Hypothesis. If someone is able to prove it, then a lot of conjectures in maths will become theorems in one go. It is considered as the hardest problem of math, so there is surely a great piece of information hidden in the Riemann Zeta function and its zeroes.

At the 2018 Heidelberg Laureate Forum (HLF), Sir Michael Atiyah gave a lecture in which he claimed to have found a proof for the Riemann hypothesis. The proof is still under scrutiny, as many previous attempts to solve the hypothesis have failed. Unfortunately, he passed away on 11 January 2019, aged 89, and sadly, won't be able to see the fate of his proof.

6. Mathematicians always try to find a set of axioms that can form the basis of mathematics and also try to make maths more rigorous. *Gottlob Frege* was a German philosopher, logician, and mathematician. He wrote *Begriffsschrift, eine der arithmetischen nachgebildete Formelsprache des reinen Denken*, a book on logic . The book marked a turning point in history of logic. He wanted to show that mathematics grows out of logic. Frege did a huge amount of work on axiomatizing everything in terms of Set Theory. He defined the concept of numbers using the sets, for example, the number 2 is the set of all the sets that contained 2 elements in it, like {Black, White}, {0,1}, etc. The number n is the extension of the concept of union of all the sets that contains that many elements. In the early years of 20th century, he sent a copy of his book to *Bertrand Russell* who was also a mathematician and logician.

   In 1902, Russell discovered a flaw in his system, he wrote a letter to Frege telling him about that flaw. He asked Frege to consider **The set of all sets that do not contain themselves as their memebers**. He asked him if the set will contain itself. To understand this, let S be the aforementioned set. Let's assume $S \in S$ so, since S belongs to itself, by the definition of set, it must not be a part of itself, which is a contradiction to what we assumed. On the other hand, let's assume $S \notin S$, then by definition of the set, it must be a part of itself, again a contradiction. It can also be stated mathematically as follows :

$$\text{Let } R = \{x | x \notin x\},\ \text{ then } R \in R \Leftrightarrow R \notin R$$

So this type of statement is regarded as undecidable in a set of axioms. Frege received the letter when he was about to publish the second edition of his book. This ruined the Frege's whole system because Russell's Paradox leads to a contradiction in his theory. It was disastrous because it can prove anything, which destroys the conventional meaning of truth and falsity (*ex falso sequitur*). His system of axioms became inconsistent, leading to paradoxical situations and all of his work became worthless. Unable to handle such a blow to his work and passion, he had a mental breakdown so severe that he had to be admitted to the hospital. Frege replied to Russell:

> "My efforts to throw light on the question surrounding the word 'Number' seem to have ended in complete FAILURE..."

7. **Fibonacci sequence** is a fascinating sequence of numbers. It is named after famous Italian mathematician *Leonardo of Pisa*, later known as Fibonacci. The sequence is such that each number in the sequence is the sum of the two previous ones. Mathematically,

$$F_0 = 0,\ F_1 = 1,\ F_n = F_{n-1} + F_{n-2} \text{ for } n > 1$$

A few terms of the sequence are $0, 1, 1, 2, 3, 5, 8.13, 21, 34, 56, 90 \ldots$
Fibonacci Sequence satisfies the stronger divisibility property, $n|m \Leftrightarrow F_n|F_m$.
To show this we'll start with the that fact the matrix

$$M = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \text{ satisfies that } M^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}.$$

It can be easily shown by induction on n. For $n = 1$, it is trivially true.
Let's assume it is true for $n = k$ which means $M^k = \begin{bmatrix} F_{k+1} & F_k \\ F_k & F_{k-1} \end{bmatrix}$.
Now for $n = k+1$, $M^{k+1} = M^k * M = \begin{bmatrix} F_{k+1} & F_k \\ F_k & F_{k-1} \end{bmatrix} * \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} F_{k+2} & F_{k+1} \\ F_{k+1} & F_k \end{bmatrix}$
which shows that it is true $\forall\, n \in \mathbb{N}$.

Now for the theorem, let's assume $n|m$. Then $m = n \cdot k$. Now, since

$$\begin{aligned} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^m &= \left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n \right)^k \\ \begin{bmatrix} F_{m+1} & F_m \\ F_m & F_{m-1} \end{bmatrix} &= \left(\begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} \right)^k \\ \begin{bmatrix} F_{m+1} & F_m \\ F_m & F_{m-1} \end{bmatrix} &= \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}^k \end{aligned}$$

Taking mod F_n on both the sides, we have

$$\begin{aligned} \begin{bmatrix} F_{m+1} & F_m \\ F_m & F_{m-1} \end{bmatrix} &\equiv \begin{bmatrix} F_{n+1} & 0 \\ 0 & F_{n-1} \end{bmatrix}^k \pmod{F_n} \\ \begin{bmatrix} F_{m+1} & F_m \\ F_m & F_{m-1} \end{bmatrix} &\equiv \begin{bmatrix} (F_{n+1})^k & 0 \\ 0 & (F_{n-1})^k \end{bmatrix} \pmod{F_n} \end{aligned}$$

By comparing the corresponding elements, we can conclude $F_m \equiv 0 \pmod{F_n}$ which means $F_m = l \cdot F_n$ or $F_n | F_m$ where $l \in \mathbb{N}$.
Now, conversely, let $F_n | F_m$, or $F_n \equiv 0 (\text{mod } F_m)$. Then $n \leq m$ because it is an increasing sequence. So $m = n \cdot q + r$ where $0 \leq r < n$.

$$\begin{aligned}
\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^m &= \left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n \right)^q \times \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^r \\
\begin{bmatrix} F_{m+1} & F_m \\ F_m & F_{m-1} \end{bmatrix} &= \left(\begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} \right)^q \times \begin{bmatrix} F_{r+1} & F_r \\ F_r & F_{r-1} \end{bmatrix}
\end{aligned}$$

Taking mod F_n on both the sides, we have

$$\begin{aligned}
\begin{bmatrix} F_{m+1} & 0 \\ 0 & F_{m-1} \end{bmatrix} &\equiv \begin{bmatrix} F_{n+1} & 0 \\ 0 & F_{n-1} \end{bmatrix}^q \times \begin{bmatrix} F_{r+1} & F_r \\ F_r & F_{r-1} \end{bmatrix} \pmod{F_n} \\
\begin{bmatrix} F_{m+1} & 0 \\ 0 & F_{m-1} \end{bmatrix} &\equiv \begin{bmatrix} (F_{n+1})^q & 0 \\ 0 & (F_{n-1})^q \end{bmatrix} \times \begin{bmatrix} F_{r+1} & F_r \\ F_r & F_{r-1} \end{bmatrix} \pmod{F_n} \\
\begin{bmatrix} F_{m+1} & 0 \\ 0 & F_{m-1} \end{bmatrix} &\equiv \begin{bmatrix} (F_{n+1})^q \cdot F_{r+1} & (F_{n+1})^q \cdot F_r \\ (F_{n-1})^q \cdot F_r & (F_{n-1})^q \cdot F_{r-1} \end{bmatrix} (\text{mod} F_n)
\end{aligned}$$

By comparing the corresponding elements, we have $(F_{n-1})^q \cdot F_r \equiv 0 (\text{mod } F_n)$.
Now F_{n-1} is co-prime to F_n. If F_n and F_{n-1} shared a common divisor then so will F_{n-2} because $F_n - F_{n-1} = F_{n-2}$. Similarly F_{n-3} will share that same divisor and this will be true for all the terms till the 1st term. But this can't be true since $F_1 = 1$ and hence F_{n-1} is co-prime to F_n.
Since they are co-prime ⇒ $F_r \equiv 0 (\text{mod } F_n)$ from above. Also $F_r < F_n$ because $r < n$ as it is an increasing sequence. Now, $F_r = 0$ because $F_r \equiv 0 (\text{mod } F_n)$ and $F_r < F_n$.
So, $r = 0$, $m = q \cdot n$ or $n | m$.

Quod Erat Demonstrandum

8. *Euclid* was a brilliant mathematician who was born in Mid-4th century BC. He is often referred to as "Father of Geometry." He published his book called *Euclid's Elements* which contained theorems and proofs about geometry and arithmetic in 300 BC. His book 1 contains 5 postulates about geometry which he thought to be universal truths. The most famous one was his 5th postulate which states that :

> *"If a line segment intersects 2 straight lines forming 2 interior angles on the same side that sum to less than 2 right angles, then the 2 straight lines, if extended infinitely, meet on that side on which the angles sum to less than 2 right angles."*

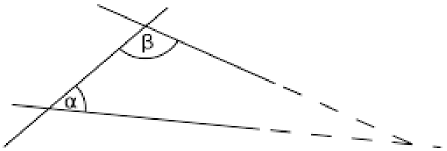


Figure 16.3: Illustration of Euclid's 5th postulate

Since the publication of his book, many geometers have made numerous attempts to prove the 5th postulate using the other 4 simple postulates. It was because the other 4 postulates were really obvious that it stands out from all them. Later on, after having a lot of unsuccessful attempts of proving it they thought of ditching the 5th postulate. What would geometry look like if we ditched the *parallel postulate*? This led to the discovery of **Hyperbolic Geometry.** In the 19th century, hyperbolic geometry was explored extensively by *János Bolyai, Nikolai Lobachevsky* and *Carl Friedrich Gauss.* They realized they had discovered a new geometry. Since the parallel postulate was removed, it was replaced by other postulate :

For any given line R and point P not on R, in the plane containing both line R and point P, then there are at least 2 distinct lines through P that do not intersect R.

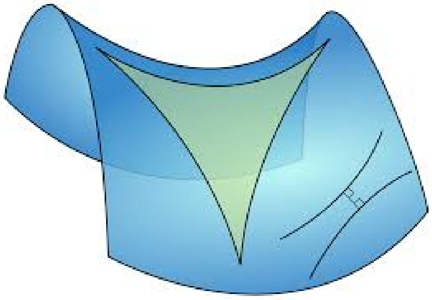


Figure 16.4: Triangle on a Hyperbolic Surface

Hyperbolic Geometry is also known as geometry of *saddle surfaces.* It is a plane having negative *Gaussian curvature.* It is different from the Euclidean geometry in terms that there are an infinite number of lines passing through a point parallel to other line. Also, the parallel lines in Hyperbolic geometry tend to move apart from each other unlike parallel lines in Euclidean geometry which stay at a same distance. It has a lot of different properties like the sum of triangles in a triangle is less than 180°.

This shows that the meaning of truth and falsity depends on the context in which it is used. Mathematics helps us to find the truth, but it depends on the axioms you choose. So it is important to clearly establish the axioms before working on any system. Moreover, it is really important to break the rules so as to form new branches or structures of mathematics, as it was in the case of finding imaginary number $a + b\mathbf{i}$, which led to the foundation of an enriching and beautiful branch of mathematics. Hyperbolic geometry is really useful in theory of relativity, particularly *Minowski* space-time and gyro-vector space.

Bibliography

[1] Wiki. Proofs of Fermat's theorem on sums of 2 squares

[2] Wiki. Cross-ratio

[3] The Cross Ratio- Numberphile

[4] An Introduction to Number Theory : Graham Everest, Thomas Ward, ISBN 978-81-8128-803-5

[5] Wiki. Fermat's Last Theorem

[6] Fermat's Last Theorem- Numberphile

[7] Wiki. Riemann hypothesis

[8] Riemann Hypothesis- Numberphile

[9] Wiki. Gottlob Frege

[10] Wiki. Russell's paradox

[11] Russell's Paradox - A Ripple in the Foundations of Mathematics

[12] Barber & Russell Paradoxes (History of Undecidability Part 2) - Computerphile

[13] Wiki. Fibonacci number

[14] Wiki. Hyperbolic geometry

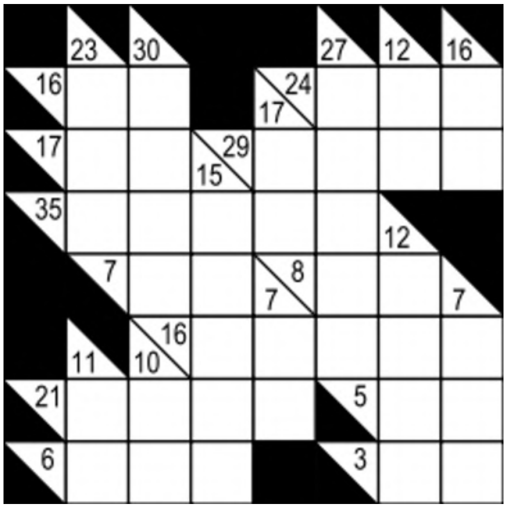
[15] Ditching the Fifth Axiom - Numberphile

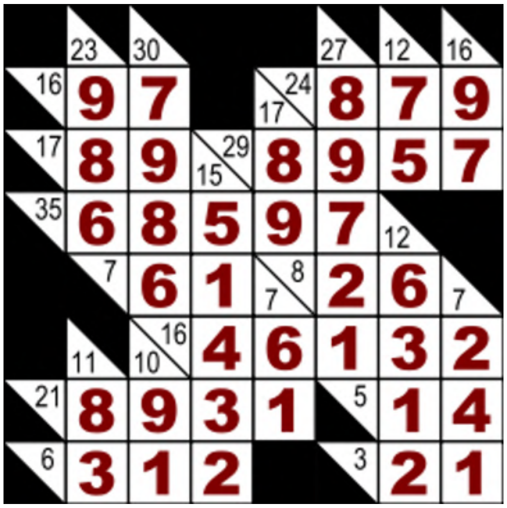
Kakuro: A Puzzle

Ashutosh Maurya
B.Sc. (H) Mathematics, 2$^{\text{nd}}$ Year

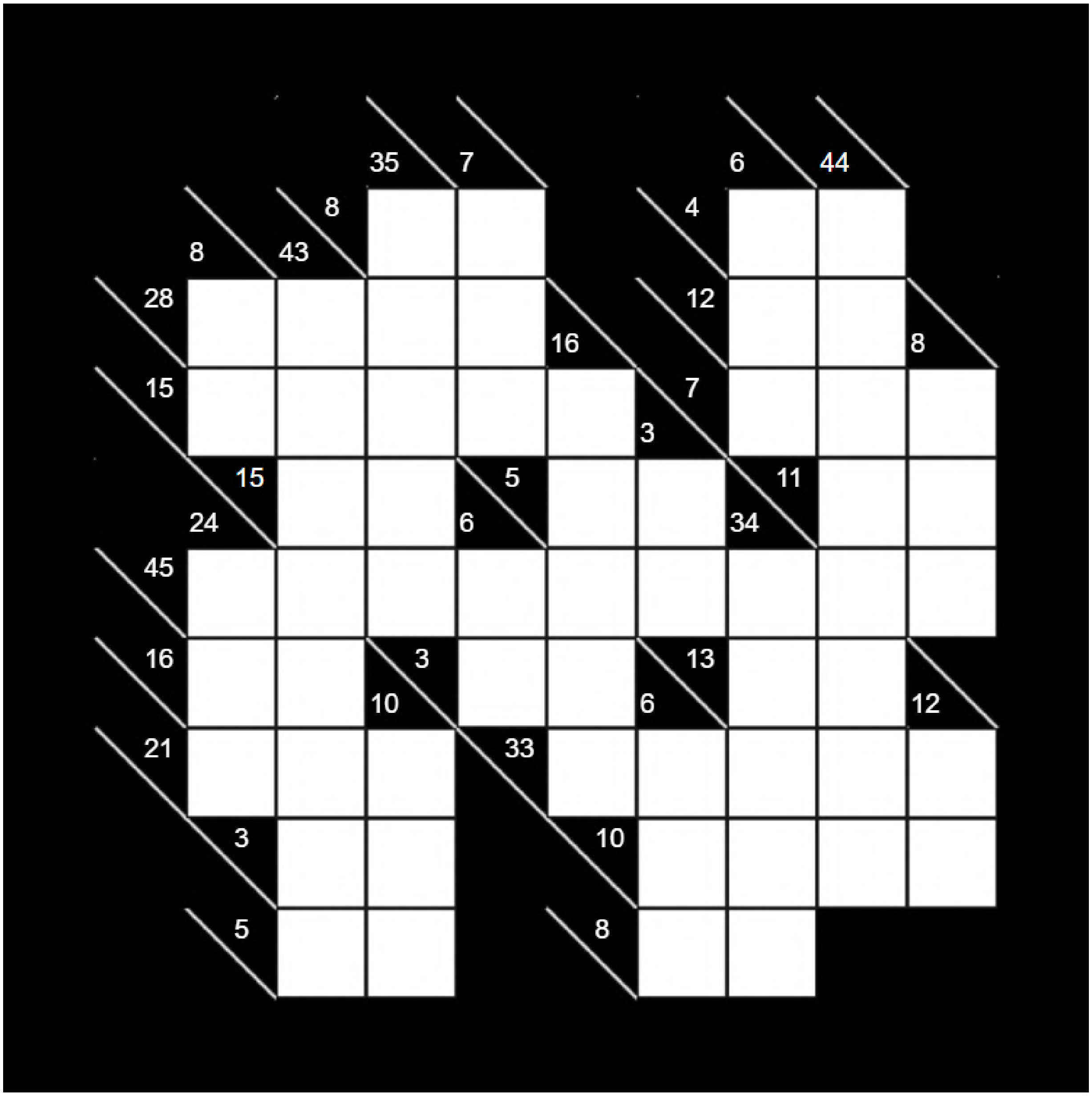
A Kakuro is a number and logic puzzle, like the famous Sudoku. It appears to be highly similar to a crossword, the word puzzle, since it has horizontal and vertical "runs", and "clues" pertaining to the entries to be filled in the runs. But the differences, apart from the language one, begin to unravel when an attempt is made to solve one. We shall now learn the basics of Kakuro and experience its complex simplicity.

A Kakuro puzzle consists of black and white cells. All the white cells are initially empty, and are bounded by black cells to make "runs". A run-total is given in a black "clue" cell, which is on top of a vertical run and on left of a horizontal run, and the puzzle is solved by entering numbers from 1 to 9, both inclusive, such that the sum is equal to the run-total, and no number is repeated in a run. Since numbers from 1 to 9 are used, a run can be between 1 and 9 cells long, and the run-total of a run can be between 1 and 45. An example puzzle and its solution are given below to familiarize the reader with the puzzle.





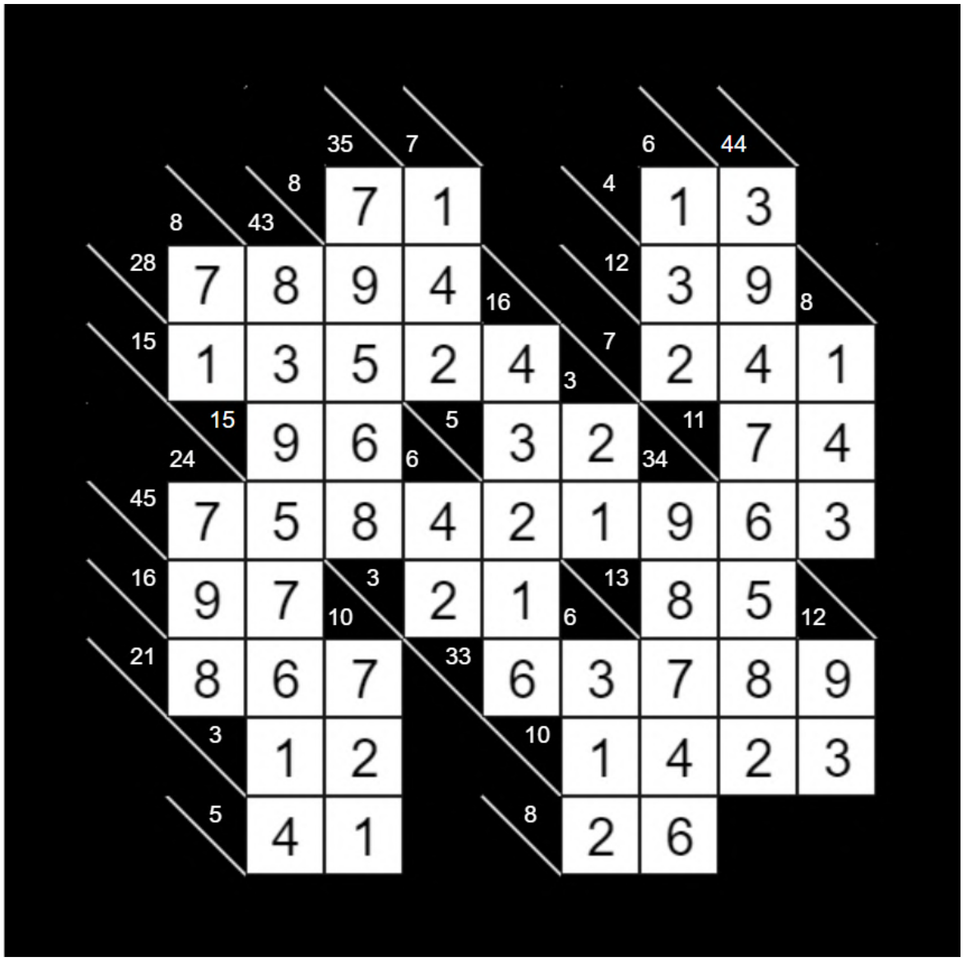
Like Sudoku, one progresses in the puzzle by eliminating possibilities based on logic. But Kakuro employs combinations far superior to those of Sudoku. A specific run-total can be represented in a number of ways. For example, a run-total of 3 in a 2 cell run can only be represented by (12), but a run-total of 20 in a 4 cell run can be represented by (1289), (1379), (1469), (1478), (1568), (2369), (2378), (2459), (2468), (2567), (3458), (3467). Therefore, though a person fluent with just addition and subtraction is capable of attempting this puzzle, it takes a bit more to taste the satisfaction of actually solving one. The reader shall now be given an opportunity to take a shot at this fruit of satisfaction and triumph. Following is an original Kakuro puzzle at the reader's service.



Bibliography

[1] Wiki. Kakuro

Solution to the puzzle:



			35\	7\			6\	44\	
	8\	43\8	7	1		\4	1	3	
\28	7	8	9	4	16\	\12	3	9	8\
\15	1	3	5	2	4	3\7	2	4	1
	24\15	9	6	6\5	3	2	34\11	7	4
\45	7	5	8	4	2	1	9	6	3
\16	9	7	10\3	2	1	6\13	8	5	12\
\21	8	6	7	\33	6	3	7	8	9
	\3	1	2		\10	1	4	2	3
	\5	4	1		\8	2	6		

Major Events of the Department

- **Seminar on "Career Opportunities in Management Sector"**: The series of seminars and workshops for the academic year 2019-20 kick-started with a very enlightening and informative session on the various possibilities, students from a wide variety of diverse streams have, when it comes to pursuing a career in the management sector. This very knowledgeable seminar was conducted by Mr. Bharat Sharma, Regional Manager, Career Launcher, Delhi on February 25th, 2019. Keeping in mind the large number of students from non-engineering and non-technical backgrounds who aspire for a professional career in management and aim to crack the CAT, the session turned out to be quite successful and popular amongst MBA aspirants. From telling the basics of CAT preparation, to letting the students know about life in top B-Schools, Mr. Sharma won over the audience with his excellent anecdotal wisdom. Apart from enlightening students about the never-ending possibilities the management sector seeks to offer, the students also got to know a lot about how and why MBA can give a strong boost to the professional lives and career. All in all, the seminar was a huge success.

- **"Identity'19"**: The Annual Fest of the Department of Mathematics, Identity, keeps achieving impossible heights and setting higher benchmarks every passing year. This edition of Identity was no exception. Organized on March 12th, Identity'19 saw a whole new level of enthusiasm and dedication from each and every member of the mathematics family of Hansraj College. The event attracted more than 2500 students from various colleges all over the capital territory, with no less than 1000 students participating in different games and other activities organised by the department. The day saw a lot of craze and excitement for various games, the most popular ones amongst which included the Mathonald, Pyramid, Scavenger Hunt, Gol Gappa Challenge, Momo Attack, Funtakshri, GoPagal and Carrom with a twist. A total of 400 participants won different rounds and were awarded cash prizes, discount coupons and prize vouchers. We also take the privilege of thanking our sponsors. We extend heartfelt gratitude towards our title sponsor, DIPS Academy, our associate sponsor, YourShell, our food partner, Aam Aadmi Ke Pakwaan and our media partners, DU Beat, DU Updates, DU Express and Vision, Hansraj College. Without a possibility of doubt, this fest will always remain in the category of "the most cherished college memories" for all of us.

- **Seminar on "GeoGebra and Mathematical Modelling Softwares"**: The department concluded the fest season by holding an academic seminar to make the students aware of an interactive geometry and algebra application called GeoGebra, among other mathematical modeling softwares. The session was held on March 14th, 2019. Apart from convincing the audience about the beauty of this wonderful software application, the speaker, Dr. Jonaki Ghosh, Lady Shri Ram College, also made an attempt to highlight a number of practical aspects of classroom mathematics, such as modelling and simulation of various real life problems, using spreadsheets. Amongst others topics, Fibonacci series and the famous Monty Hall Problem were the major points discussed by the speaker. The seminar was highly appreciated by faculty members and students alike, and has been one amongst the most impactful academic sessions, thus far.

- **General Mathematics Quiz**: Not everything can be learnt from lectures, workshops and interactive sessions. At times what we, as students, learn more from are examinations and competitions, which not only test, but also strengthen our conceptual knowledge. Acknowledging this fact, the department organized a quiz competition for the students, right after Dr. Ghosh's lecture. The highlight of the event was that, despite being a mathematics-intensive round, the event was still open to students from all fields of study. The quiz invited participants from all colleges and all years alike. It was an absolute delight for the department to welcome student participants from various colleges. The freshmen, sophomores and the final years participated with equal enthusiasm and determination. The competition was conducted in two rounds. The first one being an objective MCQ round, and was conducted by Ekansh Jauhari, Ex-General Secretary, Department of Mathematics, whereas as the second round was hosted by the famous quiz master, Mr. Duttnath Thakur and Parth Chawla, Ex-Vice President of the department. The quiz competition turned out to be highly knowledge-imparting.

- **Workshop on "Applications of Linear Algebra"**: The department went on to further its string of events by organizing an interactive workshop by Prof. Shobha Bagai from Cluster Innovation Center, University of Delhi. The topic of emphasis for this workshop was 'Linear Algebra and its Applications.' The event was held on September 23rd. Aiming to develop a better understanding of the unlimited concepts and the expanse Linear Algebra seeks to offer, this seminar served as an excellent opportunity for the student participants and teachers to exchange their ideas and opinions with the eminent speaker. The students were able to have a hands-on experience of the topics covered by Prof. Bagai in her lecture by the use of the software *Mathematica*. The success of the seminar was clearly evident by fact that all the teachers of the Mathematics Department of the college, along with 120 students from different years of study attended it. Making her talk more connected to the practical aspects of her topic, Prof. Shobha made an attempt to emphasize the importance of Linear Algebra in our everyday lives in a very innovative and convincing manner.

- **Seminar on "Foreign Eduacation"**: The department successfully conducted another seminar for the students. The session was hosted by Dr. Anusha Shrivastava, Director of Career Development and Alumni Relations, Department of Statistics, University of Columbia. Dr. Shrivastava discussed the education opportunities in the reputed institutes outside India and the admission formalities. Elaborating about the opportunities and scholarships available, the online courses and the admission procedures in the University of Columbia, the speaker also told the students about her own academic and professional life. Being mathematics students, we naturally have an edge when it comes to subjects like Statistics, and this is what Dr. Anusha wanted to draw our attention to. She made the audience aware of the various opportunities we, as future professionals have, if we pursue a career in the field of Statistics, after obtaining a master's degree. Dr. Shrivastava was kind enough to conclude her session by having an interactive question-answer time with the students and clearing even the smallest of doubts that they had.

- **Seminar on "Data Analytics as a Career Choice"**: This was the first seminar that the department organised in the new year. Delivered by Prof. Sat Gupta, the seminar, held on January 7th, 2020, focused on the career opportunities available in the field of Data Analytics. Prof. Gupta is the Head of the Department of Mathematics and Statistics at the University of North Carolina, Greensboro, in addition to being a fellow of the American Statistical Association. He has been providing 'Statistics Consultancy' to on-campus and off-campus students for over 30 years. He enlightened students about the perks of pursuing a career in the field of data and analytics and also about acquiring admission in the masters and Ph.D. programme at his prestigious university. He also presented a few basic problems on managing and handling data and working with it. At the end of his talk, the professor invited questions from teachers and students.

Career Opportunities in Mathematics

“Mathematics is a great motivator for all humans because its career starts with zero but it never ends.”

The importance of mathematics and the need for trained mathematicians is increasing at a very fast pace nowadays as the use of computers and automation has spread to almost all sectors of our economy. Whereas in the past, advanced mathematics was generally restricted to the physical sciences and engineering, today there is an ever growing demand for mathematical expertise in the biological and social sciences, as well as in finance and business management and in the burgeoning field of data science. Some career options are:

- **Actuarial Sciences**: Actuaries are business executives who use mathematical and statistical skills to define, analyze, and solve complex problems arising in insurance and pension fields. The duty of an actuary is to create and manage programs to reduce the financial impact of events such as illness, accidents, unemployment or premature death. Generally, actuaries model matters of uncertainty by applying rigorous mathematics.
- **Cryptography**: A Cryptographer’s work is to develop algorithms to encrypt sensitive information and to provide privacy for people and corporations. This is one of the best jobs for mathematics majors. It’s not just intelligence agencies that hire cryptographers, one could focus on encoding signals for cable companies or encrypting transactions for financial institutions. One can get started in this career just after graduation, particularly if your coursework includes some computer science classes.
- **Data Scientist** : Like Data Analysts, Data Scientists focus is to extract useful information from complex data. However, while data analysts examine data using existing tools and systems, data scientists can develop new tools and algorithms to solve business problems. This is one of the best jobs for math majors with advanced quantitative skills: Data scientist topped the list of satisfying careers in one survey. Most positions call for at least a master’s degree in math and statistics.
- **Mathematical Modeler**: The job of a Mathematical Modeler is to create computer simulations to illustrate processes or complex problems. They can work in many areas ranging from animation and video game design to aerospace engineering or biological research. One needs at least a master’s degree in applied mathematics to get a job in this field.
- **Meteorologist**: Meteorologists use advanced modeling techniques to forecast atmospheric conditions. Many of them work for agencies like National Oceanic and Atmosphere Administration (NOAA) or the National Center for Atmospheric Research. In this field, job opportunities are also available with airlines, consulting firms, and agricultural companies. One needs graduate-level training for research positions, a bachelor’s in mathematics plus a master’s in meteorology is one possible route.
- **Geodesist**: A Geodesist’s work is to precisely measure things like distances between the earth and other planets, changes in the Earth’s gravitational pull, and movements in the Earth’s Crust using applied mathematics. Their work helps scientist to assess changes in the landscape and shape of the earth. An Advanced degree in maths is a good starting point for this career.

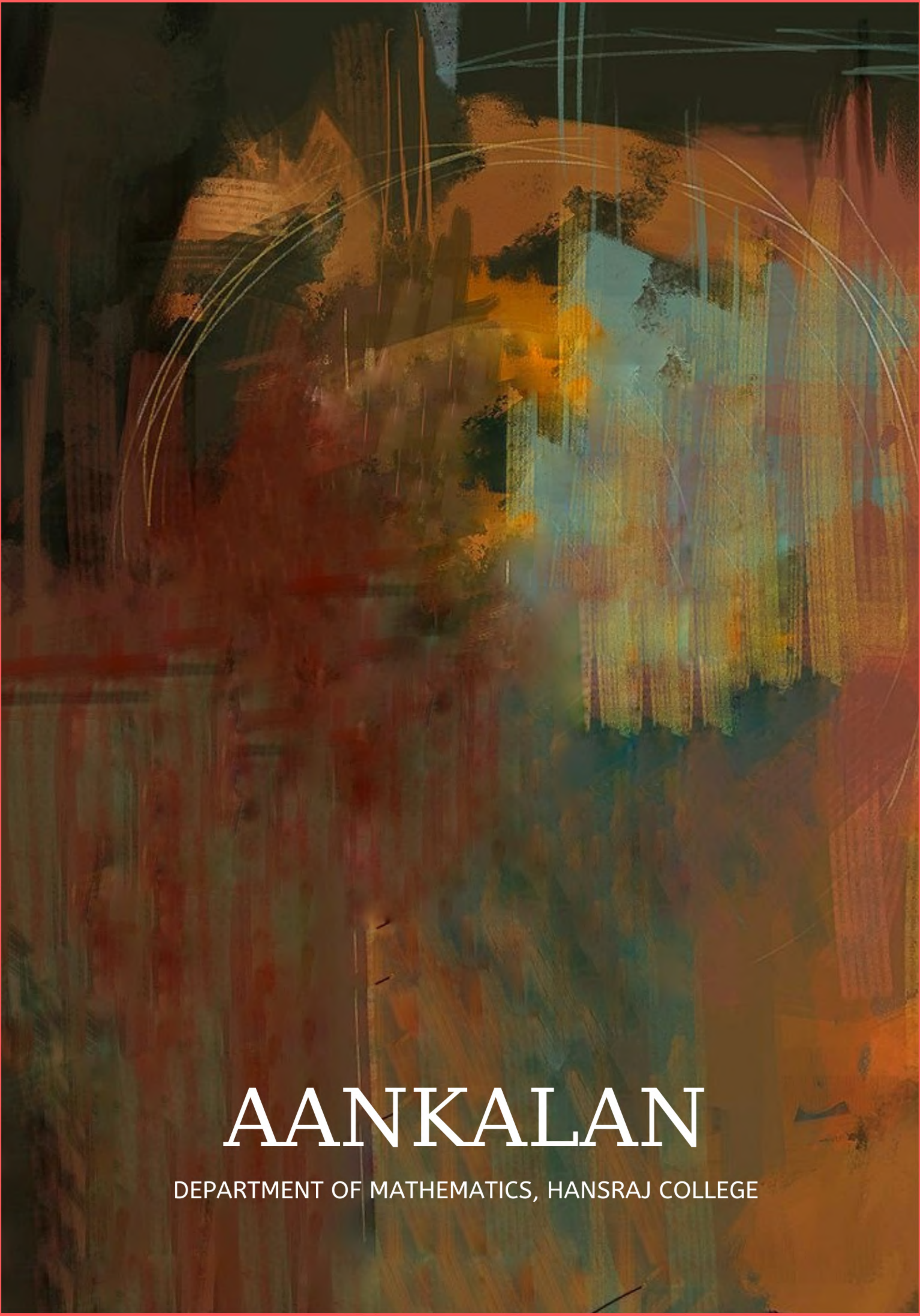
- **Algorithm Engineer**: This job requires a solid understanding of both math and technology. The job of these professionals is to develop detailed step-by-step sets of instructions that tell a computer how to operate and what to do. One can design algorithms for anything from biometric fingerprint recognition to automated driving applications in this job. Most positions require a master's degree in mathematics or computer science.

- **Inventory Control Specialist**: Most of the manufacturing and merchandising companies rely on inventory control specialist to maintain a balance between having enough stock on hand to meet orders and having too much stock taking up space in the warehouse. Their job is to use analytical skills to develop policies and procedures that can keep inventory levels at appropriate levels.

- **Systems Engineer**: Data analysis and problem solving skills are key to this job. Many electronics and communication companies hire math majors as entry level systems engineers. One should be comfortable learning new technologies in this job. It's good to get as much internship experience in electronics technology as possible.

- **Economist**: An Economist's job is to study market data and use mathematical models and statistical analysis to understand and explain economic trends. They monitor market conditions to help corporations in maximizing their profits. Economists can work for various levels of government, examining issues related to employment, taxes and interest rates. Many of the entry level positions are available to those with bachelor's degree in math, but more advanced training is preferred to work in private sector.

One can always go for higher studies after bachelor's in Mathematics in many courses like MBA from IIMs, M.Sc. from IITs followed by a Ph.D. or an M.Phil., MCA etc. Thus, after getting degree in Mathematics there are huge career options available in research and teaching field.



AANKALAN

DEPARTMENT OF MATHEMATICS, HANSRAJ COLLEGE