From: Principal & Secretary

☎ +91 3213 255282
saratcentenary@gmail.com
sccollegednk.ac.in
Dhaniakhali, Hooghly, 712302

Sarat Centenary College

Dhaniakhali, Hooghly

Founded: 1976
Recognised Under UGC 2F&12B
WB Govt. Aided
Affiliated to The University of Burdwan

No: SCC/ Date:

Certified that following students of the Department of Mathematics and Commerce of our college of 2022-23 session has carried out the Project Works on their respective subject as a mandatory programme of the Course curriculum of The University of Burdwan.

Programme name	Program Code	List of students undertaking project work/field work/ internship
Project Work (Mathematics- Hons)	MTMH/BMH6PW01	Ankan Guchait
Project Work (Mathematics- Hons)	MTMH/BMH6PW01	Arpan Das
Project Work (Mathematics- Hons)	MTMH/BMH6PW01	Juhi Khatun
Project Work (Mathematics- Hons)	MTMH/BMH6PW01	Koyel Ghosh
Project Work (Mathematics- Hons)	MTMH/BMH6PW01	Pinaki Ghosh
Project Work (Mathematics- Hons)	MTMH/BMH6PW01	Rama Kairi
Project Work (Mathematics- Hons)	MTMH/BMH6PW01	Soumya Pal
Project Work (Mathematics- Hons)	MTMH/BMH6PW01	Suma Das
Project Work (Mathematics- Hons)	MTMH/BMH6PW01	Surapriya Samanta
Project Work (Mathematics- Hons)	MTMH/BMH6PW01	Soumyadeep Ghosh
Project Work (Accountancy- Hons)	COMH/6.4.2 CH	AMLAN CHAKRABORTY
Project Work (Accountancy- Hons)	COMH/6.4.2 CH	AZMIRA KHATUN
Project Work (Accountancy- Hons)	COMH/6.4.2 CH	DEBASHIS MAJHI
Project Work (Accountancy- Hons)	COMH/6.4.2 CH	MONDIRA MONDAL
Project Work (Accountancy- Hons)	COMH/6.4.2 CH	NILAVO BANERJEE
Project Work (Accountancy- Hons)	COMH/6.4.2 CH	SOUMESH MURMU
Project Work (Accountancy- Hons)	COMH/6.4.2 CH	SOUMODIP CHATTOPADHYAY
Project Work (Accountancy- Hons)	COMH/6.4.2 CH	SOUVIK KOLEY
Project Work (Accountancy- Hons)	COMH/6.4.2 CH	SOUVIK MAJHI
Project Work (Accountancy- Hons)	COMH/6.4.2 CH	SUBHAM AGASTI
Project Work (Accountancy- Hons)	COMH/6.4.2 CH	RAKIB MALLICK

SARAT CENTENARY COLLEGE Estd.- 1976 HOOGHLY DHANIAKHALI

Dr Sandip Kumar Basak
Principal & Secretary

DR. SANDIP KUMAR BASAK
Principal & Secretary
Sarat Centenary College
Dhaniakhali, Hooghly

Application of LPP in real field

Project work submitted for the B.SC Degree, 6th semester examination in mathematics

University of Burdwan

Under the supervision of

Shampa Dutta

By

Ankan Guchait

University Roll No - 200341200002

University Reg. No- 202001048575 of 2020-21

Department of Mathematics

Signature of the Student | Signature of the teacher | Signature of the H.O.D

ACKNOWLEDGEMENT

I am grateful to DR BIDYUT SANTRA, Assistant Professor, Department of Mathematics, SARAT CENTENARY COLLEGE under whose supervision the project work has been carried out. I am grateful to all the teacher including the head of the department of Mathematics, SARAT CENTENARY COLLEGE for the constant support throughout the work. I am thankful to the authors of various books, articles and webpages which have been consulted during the preparation of this project work. Finally I express my thanks to the staff members of the office, library of our college and the infrastructural support provided by the department.

Date :-

Signature of the student

CERTIFICATE

This is to certify that Arpan Das has worked out the project work entitled "Continued fractions and its applications", under my supervision. In my opinion the work is worthy of consideration for partial fulfilment of his B.Sc. degree in Mathematics.

Date:-

Signature of the teacher

CONTENTS

Introduction: origin and history of continued fraction

Continued fraction is a completely different approach of looking at numbers. It is one of the most powerful tools of mathematics that has a widespred applications in our daily life.

A continued fraction is a unique mathematical method of representing any real number by a sum of successive division of numbers.

The field of applications of continued fraction includes calendar construction, astronomy, music, electric circuits etc. It is used to find rational approximations to irrational numbers. Several computer algorithms do such approximations using continued fractions. Continued fractions are very useful in solving certain types of equations such as Diophantine equation, Pell's equation etc.

The origin of continued fraction is hard to pinpoint since examples of such fractions can be found through mathematics in the last 2000 year but its true foundation was not laid until the late 1600's and early 1700's.

The origin of continued fraction can be traditionally placed at the time of the creation of Euclid's algorithm to find the greatest common divisor (gcd) of two numbers. It is unclear whether Euclid and his contemporaries used the algorithm to derive continued fractions. But its close connection with continued fraction signifies the initial development of continued fractions.

For over a thousand of years, any work related to continued fraction was restricted to only specific examples. The Indian mathematician Aryabhata used continued frations to solve a linear indeterminate equation (an equation having multiple solutions such as $ax+by=c$). However, he did not generalise his method. Examples of such fractions can be found in Greek and Arabic writings also.

Two men from the city of Bologna, Italy, Rafael Bombelli and Pietro Cataldi made contributions in the progress. The former expressed $\sqrt{13}$ as a repeated continued fraction, and the latter did the same for $\sqrt{18}$.

In the late 1600's, continued fractions became a field in its right through the work of John Wallis. It was Wallis who first used the term "continued fraction". In his book Arithmatica Infinitorium (1655), he developed and presented the identity

$$\frac{4}{\pi} = \frac{3\cdot3\cdot5\cdot5\cdot7\cdot7\cdot9\cdots}{2\cdot4\cdot4\cdot6\cdot6\cdot8\cdot8\cdots}$$

Lord Bruneker, the first president of the Royal Society, later transformed the above identity into the form given below

$$\frac{4}{\pi} = 1 + \cfrac{1^2}{2 + \cfrac{3^2}{2 + \cfrac{5^2}{2 + \cfrac{7^2}{\ddots}}}}$$

Wallis then took the initiative and began to lay the foundations for some properties as it is known today. In his book Opera Mathematica, he explained how to compute the n^{th} convergent and discovered some properties of convergents.

The well-known Dutch mathematician and astronomer Christaan Huygens was the first to demonstrate a practical application of continued fraction.

His work was partially motivated by his desire to make a mechanical planetorium.

The field of continued fraction began to flourish in the 1700's when Euler, Lambert and Lagrange explored the topic. Euler laid down much of his theory in his work De Fractionlous Continious. He showed that any rational number can be written as a simple continued fraction. He also gave the continued fraction expansion for the number e and used it to show that e is an irrational number. Lambert generalised the works of Euler on e to show that e^x and $\tan x$ are irrational if x is rational. Lagrange used continued fractions to find the value of irrational roots and proved an important theorem.

Nineteenth century can probably be described as the golden age of continued fractions. It was the time in which "the subject was known to every mathematician". As a result, an explosion of growth in this field was felt. Some of the prominent mathematicians who made a significant contributions to this field during this period include Jacobi, Perron, Hermite, Gauss, Cauchy and Stieljes.

From the beginning of 20th century continued fractions continues to grow rapidly and make appearence in other fields too. Rob Corless examined the connection between continued fraction and chaos theory in his research. Continued fractions have also made their way into cryptography and hyperbolic geometry.

Though the initial developments seem to have taken a lot of time, once started, the field and analysis of continued fractions grew rapidly. Even today, the usage of such fractions signify that the field is too far from being exhausted.

In this project work, we shall make an approach to represent any number in the form of continued fraction and conversely, express a continued fraction by the corresponding number. We shall analyse the key properties of it. Lastly, we shall discuss some applications in brief.

Few basic definitions

Continued fraction

A mathematical expression of the form

$$a_1 + \cfrac{b_1}{a_2 + \cfrac{b_2}{a_3 + \cfrac{b_3}{a_4 + \cfrac{b_4}{\ddots}}}}$$

is said to be a continued fraction. The values of $a_1, a_2, a_3 \ldots\ldots$ and $b_1, b_2, b_3 \ldots\ldots$ can be either real or complex. A continued fraction may have a finite or infinite number of terms. If it contains a finite number of terms, then it is called a finite continued fraction, and if it contains an infinite number of terms, then it is called an infinite continued fraction. Note that, in the above expression, if $b_n = 0$, for any n, the continued fraction is always finite.

Simple continued fraction

A simple continued fraction is a continued fraction in which $b_n = 1$ for all n, that is

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{1}{\ddots}}}}$$

where a_n are positive integers for all $n \geq 2$; a_1 can take any integer value including 0. The numbers $a_1, a_2, a_3, \ldots$ are referred to as partial quotients or denominators of this fraction. The fraction can be put in a simpler form as $[a_1, a_2, a_3, \ldots]$ or as $a_1 + \frac{1}{a_2+}\frac{1}{a_3+}\cdots$

$[-1, 2, 7, 4, 13]$ and $[2, 9, 6, 3]$ are examples of finite simple continued fractions whereas $[5, 1, 17, 23, \ldots]$ and $[3, 8, 5, 26, 92, \ldots]$ are some examples of infinite simple continued fraction.

Convergents

The simple continued fraction $[a_1, a_2, \ldots, a_k]$ where k is such that $1 \leq k \leq n$, is called the k-th convergent of the simple continued fraction $[a_1, a_2, \ldots, a_n]$ or $[a_1, a_2, \ldots, a_n, \ldots]$. The k-th convergent is usually denoted by C_k. For example,

$$C_1 = 1, C_2 = \frac{3}{2} \text{ and } C_3 = \frac{10}{7}$$

are the three convergents of the simple continued fraction

$$1 + \frac{1}{2 + \frac{1}{3}}$$

Now we prove a theorem that gives a recursion formula to calculate the convergents of a continued fraction.

Theorem (continued fraction recursion formula): Consider a simple continued fraction $[a_1, a_2, \ldots, a_n, \ldots]$ then the numerator p_i and denominator q_i of the i-th convergent are defined for all $i \geq 0$ by the recursive definition:

$$p_i = a_i p_{i-1} + p_{i-2} \quad , \quad q_i = a_i q_{i-1} + q_{i-2}$$

where $p_{-1} = 0$, $p_0 = 1$, $q_{-1} = 1$ and $q_0 = 0$. Note that, in this case a_i can take any complex value

Proof: We shall prove the statement by using induction. Let the simple continued fraction $[a_1, a_2, \ldots, a_{n-1}, a_n, \ldots]$ be given. This may be finite or infinite. We first check the two base cases.

$$C_1 = a_1 = \frac{a_1 \cdot 1 + 0}{a_1 \cdot 0 + 1} = \frac{a_1 p_0 + p_{-1}}{a_1 q_0 + q_{-1}} = \frac{p_1}{q_1}$$

$$C_2 = a_1 + \frac{1}{a_2} = \frac{a_1 a_2 + 1}{a_2} = \frac{a_2 \cdot a_1 + 1}{a_2 \cdot 1 + 0} = \frac{a_2 p_1 + p_0}{a_2 q_1 + q_0} = \frac{p_2}{q_2}$$

Both these cases agree with the definition. We now assume that the statement is true for a positive integer k. We want to show that this statement is true for $k+1$ also.

Now $C_{k+1} = [a_1, a_2, \ldots, a_{k-1}, a_k, a_{k+1}]$

which can be rewritten as the following manner

$$C_{k+1} = [a_1, a_2, \ldots, a_{k-1}, (a_k + \frac{1}{a_{k+1}})]$$

This continued fraction now has k terms, where the value of each term is complex and by hypothesis

$$C_{k+1} = \frac{(a_k + \frac{1}{a_{k+1}}) p_{k-1} + p_{k-2}}{(a_k + \frac{1}{a_{k+1}}) q_{k-1} + q_{k-2}}$$

$$= \frac{(a_k a_{k+1} + 1) p_{k-1} + a_{k+1} p_{k-2}}{(a_k a_{k+1} + 1) q_{k-1} + a_{k+1} q_{k-2}}$$

$$= \frac{a_k a_{k+1} p_{k-1} + p_{k-1} + a_{k+1} p_{k-2}}{a_k a_{k+1} q_{k-1} + q_{k-1} + a_{k+1} q_{k-2}}$$

$$= \frac{a_{k+1}(a_k p_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_k q_k + q_{k-2}) + q_{k-1}}$$

$$= \frac{a_{k+1} p_k + p_{k-1}}{a_{k+1} q_k + q_{k-1}} \quad \text{[By our assumption]}$$

$$= \frac{p_{k+1}}{q_{k+1}}$$

thus the theorem is true for $k+1$ whenever it is true for k. Hence by induction the theorem must hold for all integers.

To illustrate how the formula works, we consider the following simple continued fraction

$$1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{4}}}$$

Then by the above theorem, we see that

$p_1 = a_1 p_0 + p_{-1} = 1 \cdot (1) + 0 = 1$, $p_2 = a_2 p_1 + p_0 = 2 \cdot (1) + 1 = 3$, $p_3 = a_3 p_2 + p_1 = 3(3) + 1 = 10$, $p_4 = a_4 p_3 + p_2 = 4 \cdot (10) + 3 = 43$ and $q_1 = a_1 q_0 + q_{-1} = 1 \cdot (0) + 1 = 1$, $q_2 = a_2 q_1 + q_0 = 2(1) + 0 = 2$,

$q_3 = a_3 q_2 + q_1 = 3(2) + 1 = 7$, $q_4 = a_4 q_3 + q_2 = 4(7) + 2 = 30$

Using these results, we can obtain the convergents of the continued fraction. They are $C_1 = 1$, $C_2 = \frac{3}{2}$, $C_3 = \frac{10}{7}$ and $C_4 = \frac{43}{30}$

Properties of continued fractions

Every rational number can be expressed as a finite simple continued fraction. Before giving a formal proof and method of expansion, we now introduce continued fractions by studying its connections with Euclid's algorithm which can be described as follows:

Take two integers a and b. Now since $\gcd(a,b) = \gcd(b,a) = \gcd(|a|,|b|)$, we may assume that $a \geq b \geq 0$. When we make use of the division algorithm multiple times we shall eventually reach 0 since the sequence of remainders is decreasing i.e., $b > r_1 > \ldots\ldots \geq 0$. One can proceed in the following manner

$a = q_1 b + r_1$ where $0 < r_1 < b$

$b = q_2 r_1 + r_2$ where $0 < r_2 < r_1$

$r_1 = q_3 r_2 + r_3$ where $0 < r_3 < r_2$

$\vdots \quad \vdots \quad \vdots$

$r_{n-2} = q_n r_{n-1} + r_n$ where $0 < r_n < r_{n-1}$

$r_{n-1} = q_{n+1} r_n + 0$

The last nonzero remainder r_n is the $\gcd(a,b)$. However, we are more interested in the process of this algorithm rather than the gcd itself. Every quotient $(q_1, q_2, \ldots\ldots, q_n)$ is an entry in the finite continued fraction representation. To verify this fact, we consider the following example

Suppose that we want to find the greatest common divisor (gcd) of 147 and 69. Then by using Euclid's algorithm, we have the equations

$147 = 2(69) + 9$

$69 = 7(9) + 6$

$9 = 1(6) + 3$

$6 = 2(3) + 0$

The last nonzero remainder is 3. So by Euclidean algorithm $\gcd(147,69) = 3$

To find the continued fraction representation, divide both sides of the first equation by 69 to get $\frac{147}{69} = 2 + \frac{9}{69}$

which can be rewritten in the reciprocal form as follows

$$\frac{147}{69} = 2 + \frac{1}{\left(\frac{69}{9}\right)} = 2 + \frac{1}{7+\frac{6}{9}} = 2 + \frac{1}{7+\frac{1}{\left(\frac{9}{6}\right)}} = 2 + \frac{1}{7+\frac{1}{1+\frac{3}{6}}} = 2 + \frac{1}{7+\frac{1}{1+\frac{1}{\left(\frac{6}{3}\right)}}} = 2 + \frac{1}{7+\frac{1}{1+\frac{1}{2}}}$$

Thus the continued fraction representation of $\frac{147}{69} = [2,7,1,2]$. Note that these are the entries from the quotients from the algorithm. Again by writing $\frac{147}{69} = [2,7,1,2]$ we do not mean an usual equality, but just a representation of the rational number $\frac{147}{69}$ by its equivalent continued fraction $[2,7,1,2]$

This particular example can be generalised for any rational number with the help of the following theorem.

Theorem-1: Any rational number can be represented as a finite simple continued fraction.

Proof: Let $\frac{a}{b}$, where $b>0$, be any rational number. The Euclidean algorithm is used for finding the gcd of a and b which gives us the following equations

$a = a_0 b + r_1$ where $0<r_1<b$

$b = a_1 r_1 + r_2$ where $0<r_2<r_1$

$r_1 = a_2 r_2 + r_3$ where $0<r_3<r_2$

$\vdots$

$r_{n-2} = a_{n-1} r_{n-1} + r_n$ where $0<r_n<r_{n-1}$

$r_{n-1} = a_n r_n + 0$

In the above algorithm, we have replaced q_i with a_i to fall in line with the finite continued fraction representation. Note that since each remainder r_k is a positive integer, the quotients $a_0, a_1, \ldots, a_n$ are all positive also. Now dividing the first equation by b we get

$$\frac{a}{b} = a_0 + \frac{r_1}{b} = a_0 + \frac{1}{\left(\frac{b}{r_1}\right)}$$

Similarly, for the remaining equations, we have

$$\frac{b}{r_1} = a_1 + \frac{r_2}{r_1} = a_1 + \frac{1}{\left(\frac{r_1}{r_2}\right)}$$

$$\frac{r_1}{r_2} = a_2 + \frac{r_3}{r_2} = a_2 + \frac{1}{\left(\frac{r_2}{r_3}\right)}$$

$$\vdots$$

$$\frac{r_{n-1}}{r_n} = a_n$$

By substitution: $\frac{a}{b} = a_0 + \frac{1}{\left(\frac{b}{r_1}\right)} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\frac{r_1}{r_2}}}$

In this result substitute the value of $\frac{r_1}{r_2}$ as given above

$$\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\left(\frac{r_2}{r_3}\right)}}}$$

This process can be repeated in the same way to get

$$\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \, \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}$$

Thus the continued fraction expansion of the rational number $\frac{a}{b}$ is given by $\frac{a}{b} = [a_0, a_1, \ldots\ldots, a_{n-1}, a_n]$ which is finite and simple. Hence each rational number can be expressed as a finite simple continued fraction.

Now let us try to think whether the converse part of the above theorem is true or not, that is, if a finite simple continued fraction be given, how can we find the rational number represented by it?

The answer is if a continued fraction (finite and simple) representation of a number y be given, the number y can be calculated by using the following relationship repeatedly:

$$[a_0, a_1, a_2, \ldots\ldots, a_{n-1}, a_n] = [a_0, a_1, a_2, \ldots\ldots, a_{n-1} + \tfrac{1}{a_n}]$$

To illustrate the fact, let us take a continued fraction [2,2,1,2,1] and suppose we want to know the rational number represented by this fraction.

Note that

$$\begin{aligned}[2,2,1,2,1] &= [2,2,1,2+\tfrac{1}{1}] \\ &= [2,2,1,3] \\ &= [2,2,1+\tfrac{1}{3}] \\ &= [2,2,\tfrac{4}{3}] \\ &= [2,2+\tfrac{1}{(\frac{4}{3})}] \\ &= [2,2+\tfrac{3}{4}] \\ &= [2,\tfrac{11}{4}] \\ &= [2+\tfrac{1}{(\frac{11}{4})}] \\ &= [2+\tfrac{4}{11}] \\ &= \tfrac{26}{11}\end{aligned}$$

So now we are ready to give a formal proof of the converse part of theorem 1.

Theorem-2: Every finite simple continued fraction represents a rational number.

Proof: Let $[a_0, a_1, \ldots, a_n]$ be a given n-th order simple continued fraction. We wish to show that the continued fraction represents a rational number by using the principle of induction on the number of partial quotients.

If $n=1$ then $[a_0, a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1}$

Since a_0 and a_1 are integers, $\frac{a_0 a_1 + 1}{a_1}$ is a rational number.

We assume that any finite simple continued fraction with $k(<n)$ partial quotients represents a rational number. We now show that the same result holds for $k+1$ partial quotients. Let X be the value of a continued fraction that has $k+1$ partial quotients. Then, we have

$$X = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{k-1} + \cfrac{1}{a_k}}}}} = a_0 + \frac{1}{Y}$$

Where Y is the continued fraction

$$Y = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \cfrac{1}{a_{k-1} + \frac{1}{a_k}}}}} = [a_1, a_2, \ldots, a_k]$$

Since $[a_1, a_2, \ldots, a_k]$ is a finite simple continued fractions with k partial quotients, it represents a rational number $\frac{p}{q}$. This implies that

$$X = a_0 + \frac{1}{Y} = a_0 + \frac{1}{\left(\frac{p}{q}\right)} = a_0 + \frac{q}{p} = \frac{a_0 p + q}{p}$$

Since a_0, as well as p and q are integers, X must be a rational. Thus, the theorem is true for k+1, and by induction, it must hold for all integers.

Now let us turn our attention to the discussions of infinite simple continued fraction.

Theorem-3: An infinite simple continued fraction represents an irrational number.

Proof: We shall prove this theorem by contradiction. Let x be the value of the infinite continued fraction $[a_0, a_1, a_2, \ldots]$ i.e., $x = \lim_{n\to\infty} [a_0, a_2, \ldots, a_n]$. Let the sequence convergents $C_n = [a_0, a_1, a_2, \ldots, a_n] = \frac{p_n}{q_n}$ where $p_k = a_k p_{k-1} + p_{k-2}$ and $q_k = a_k q_{k-1} + q_{k-2}$. Since $C_{n+1} < x < C_n$, we have

$$0 < |x - C_n| < |C_{n+1} - C_n| = \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \frac{1}{q_n q_{n+1}}$$

Assume that $x = \frac{a}{b}$, where a and b are positive integers. Then $0 < \left|\frac{a}{b} - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}}$

Multiplying throughout by bq_n, yields $0 < |aq_n - bp_n| < \frac{b}{q_{n+1}}$. If n is chosen large so that $b < q_{n+1}$, the result is $0 < |aq_n - bp_n| < 1$. This says that there is a positive integer between 0 and 1, which is a contradiction. Therefore, x must be an irrational number.

It is natural to ask whether the converse of this theorem holds or not. Is it possible to express any irrational number as an infinite continued fraction? In the next theorem, we are going to discuss this

Theorem-4: If w is an irrational number, then it has an infinite simple continued fraction representation.

Proof: Let the simple continued fraction expansion of the irrational w be finite. Thus the continued fration representing w has n terms, where n is a positive integer. But we have proved earlier that a continued fraction with a finite number of terms must be a rational number. Hence the continued fraction containing n terms is equivalent to a rational, and thus, it can never be equivalent to w. Therefore if w be an irrational, it cannot have a finite continued fraction representation. or in other words it must have an infinite simple continued fraction representation.

Let us now think of the method of expressing given any irrational number α as a continued fraction. To do this, we may use the following recursive formula

$$a_i = [\alpha_i]$$
$$\alpha_{i+1} = \frac{1}{\alpha_i - a_i}$$

where $\alpha_1 = \alpha$ and the function $[x]$ denotes the greatest integer function.

For example, consider the irrational number $\sqrt{15}$. We let $\alpha_1 = \sqrt{15}$. Then as $3 < \sqrt{15} < 4$, $a_1 = [\sqrt{15}] = 3$

$$\alpha_2 = \frac{1}{\sqrt{15}-3} = \frac{\sqrt{15}+3}{6} = 1 + \frac{\sqrt{15}-3}{6} \quad \therefore a_2 = 1$$

$$\alpha_3 = \frac{6}{\sqrt{15}-3} = \frac{6(\sqrt{15}+3)}{6} = \sqrt{15}+3 = 6 + (\sqrt{15}-3) \quad \therefore a_3 = 6$$

$$\alpha_4 = \frac{1}{\sqrt{15}-3} = \frac{\sqrt{15}+3}{6} = \alpha_2$$

Since $\alpha_2 = \alpha_4$, it is clear that we will begin to repeat $\alpha_3 = \alpha_5$ and so on. In this process, we can find all the a_i and $\sqrt{15} = [3; \overline{1, 6}]$ where the bar over 1 and 6 indicates that they are repeated over and over.

Applications of continued fractions

We have already dicussed about the way of finding the continued fraction representation of any real number, and vice-versa Moreover, continued fractions are an important tool for solving problems related with moments involving two different periods. This type of situations occur both in theoretical question of number theory, complex analysis, dynamical systems .... as well as in more practical questions of constructing calendar, tuning musical instruments, gears ... In this section, we shall discuss about some of these applications.

Constructing a calendar: Continued fractions can be apllied in designing a calendar. In a year, there are 365 days. However, astronomers tell that the earth completes its orbit around the sun in approximately 365.2422 days. The continued fraction of this number is

$$365.2422 = [365, 4, 7, 1, 3, 4, 1, 1, 1, 2]$$

The second convergent is $[365, 4] = 365.25 = 365 + \frac{1}{4}$

which means a calendar with 365 days per year but a leap year in every 4 years. If the fourth convergent is used, then a better approximation is found

$$[365, 4, 7, 1] = 365.2424 .... = 365 + \frac{8}{33}$$

The Gregorian calendar, named after Pope Gregorio XIII who introduced it in 1852, is based on a cycle of 400 years: there is one leap year every year which is a multiple of 4 but not of 100. unless it is a multiple of 400. In other words, in 400 years 3 leap years are omitted, thus there are

$$400 \cdot 365 + 100 - 3 = 146097$$

days. On the other hand, in 400 years if the number of days are counted with an year of $365+\frac{8}{33}$ days, then there are

$400\left(365+\frac{8}{33}\right)=146096.9696\ldots$ days in 400 years.

Which is an excellent approximation!

Solving linear Diophantine equations: Diophantine equation is named after Diophantus of Alexandrea, a Greek mathematician lived around 250 A.D. and wrote a book named 'Arithmatica' about these equations.

Diophantine equation is an algebraic equation in one or more than one variables with integral coefficients such that only integral solutions are sought. This type of equations may have no solution, unique solution or an infinite number of solutions. A Diophantine equation is said to be linear in two variables x and y if it has the form $ax+by=c$, where a, b and c are integers. Some examples of linear Diophantine equations (LDE) are $3x+5y=6$, $2x+7y=9$, $4x-2y=2$ etc.

Suppose we want to solve the LDE $Ax+By=C$, where A, B and C are integral coefficients.

The LDE is said to be solvable iff $\gcd(A,B)$ divides C. If so, divide both sides of the given LDE by $\gcd(A,B)$ to reduce it to the following form

$ax+by=c$, a, b, c are integers and $\gcd(a,b)=1$.

The first step in solving the LDE is to find a particular solution (x_0, y_0) of the LDE $ax+by=1$ using the simple continued fraction

$\frac{a}{b}=[a_0, a_1, \ldots, a_n]$

From $ax_0+by_0=1$ we have $a(cx_0)+b(cy_0)=c$

Thus (cx_0, cy_0) is a particular solution of the LDE $ax+by=c$

Finally any solution of this equation is a solution of the original given equation $Ax+By=C$ as well.

Pell's equation: Let d be a positive integer which is not a perfect square. Then the Diophantine equation $x^2-dy^2=1$ is known as Pell's equation. This type of equation was first studied in India starting with Brahmagupta, whose found an integer solution to $92x^2+1=y^2$.

The Pell's equation can be rewritten as $(x-\sqrt{d}y)(x+\sqrt{d}y)=1$; hence for $y>0$, we have that $\frac{x}{y}$ is a rational approximation of $\sqrt{d}$. This is the reason for using continued fraction expansion of $\sqrt{d}$ in solving Pell's equation.

It is quite interesting that for relatively small values of d, the solution can be very large. For example Fermat asked his friend William Brouncker to find a solution for $d=109$, saying that he chose a small value of d to make the problem not too difficult. However, the smallest solution was found to be $x=158070671986249$, $y=15140424455100$

which is also given by $\left(\frac{261+25\sqrt{109}}{2}\right)^6 = 158070671986249 + 15140424455100\sqrt{109}$

Continued fraction for $\sqrt{2}$: The square root of 2 satisfies the following

$$\sqrt{2} = 1+\frac{1}{\sqrt{2}+1}$$

while
$$\sqrt{2} = 1+\frac{1}{1+\frac{1}{\sqrt{2}+1}+1}$$

$$= 1+\frac{1}{2+\frac{1}{\sqrt{2}+1}}$$

This step is repeated again and again. Hence the continued fraction expansion of $\sqrt{2}$ is given by $\sqrt{2} = [1,2,2,\ldots] = [1,\overline{2}]$

Fibonacci sequence and Golden ratio: The Fibonacci sequence was introduced, by Leonardo Pisano, also known as Fibonacci. It is defined by $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$ for all integers $n \geq 2$. The first few Fibonacci numbers are $0,1,1,2,3,5,8,13,21 \ldots$

The unique positive numbers ϕ satisfying $\phi = 1 + \frac{1}{\phi}$ is given by $\phi = \frac{1+\sqrt{5}}{2}$ and it is known as the Golden Ratio. It makes appearences in many different contexts, from Mathematics to Arts.

From the above relation it is clear that continued fraction of ϕ is.

$$\phi = [1,1,1,\ldots] = [\overline{1}]$$

This is the simplest infinite continued fraction. Note that the convergents of ϕ are precisely the ratios of consecutive Fibonacci numbers i.e., $[1] = \frac{F_2}{F_1}$, $[1,1] = \frac{F_3}{F_2}$, $[1,1,1] = \frac{F_4}{F_3}$ and so on. So that $\phi = \lim_{n \to +\infty} \frac{F_{n+1}}{F_n}$

Continued fraction for e and π: Leonard Euler proved that the continued fraction representing e, is given by

$$e = [2,1,2,1,1,4,1,1,6,1,\ldots] = [2,\overline{1,2m,1}]_{m \geq 1}$$

This result implies that e is neither rational nor a quadratic irrational. Actually, Euler showed the more general result that for any integer $a \geq 1$, it holds

$$e^{\frac{1}{a}} = [1, a-1, 1, 3a-1, 1, 1, 5a-1, 1, \ldots]$$

$$= [\overline{1, (2m+1)a-1, 1}]_{m \geq 1}$$

Johan Heinrich Lambert proved that for any rational $v \neq 0$, $\tan(v)$ is irrational. Hence π is irrational since $\tan(\frac{\pi}{4}) = 1$. The continued fraction of π is given by $\pi = [3,7,15,1,292,1,1,1,2,1,3,1,14,2,1,1,\ldots]$ which is more mysterious than the one of e. It is still a problem to understand if the partial quotients of the continued fraction of π is bounded or not.

Quadratic numbers: Joseph Louis Lagrange proved that the continued fraction expansion of a real number x is ultimately periodic, i.e.,

$$x = [a_0, \ldots, a_k, b_1, \ldots, b_h, b_1, \ldots, b_h, \ldots]$$

iff x is a quadratic number, that is, x is a root of a quadratic polynomial with rational coefficients.

In such cases, we use the shorter notation

$$x = [a_0, \ldots, a_k, \overline{b_1, \ldots, b_h}]$$

Continued fractions for analytic functions: Some analytic funtions also have a kind of continued fraction expansion. For example, the tangent:

$$\tan(x) = \cfrac{x}{1 - \cfrac{x^2}{3 - \cfrac{x^2}{5 - \cfrac{x^2}{7 - \ddots}}}}$$

The study of continued fractions of analytic functions is strictly connected to the theory of Padé approximations, which are rational function approximations of analytic functions.

Generalisations of continued fractions in higher dimensions

Simultaneous rational approximations of real numbers is a much more difficult task to do rather than rational approximation of a single number.

In fact, the continued fraction expansion has so many specific features that no extension of it in higher dimension with same properties has been possible.

However, a few attempts were made, particularly the Jacobi-Perron algorithm uses a kind of ternery continued fraction expansion to deal with cubic irrationality. This topic is closely related with the geometry of numbers, started by Hermann Minkowski, which is the study of convex bodies and integer vectors in the n-dimensional Euclidean space R^n.

Recently, Wolfgang Schmidt, Leonhard Summerer and Damien Roy made significant progress in the so-called parametric geometry of numbers.

Concluding Remaks

From the continued fraction expansion algorithm we come to know that we can represent any rational number by a finite simple continued fraction and any irrational number by an infinite simple continued fraction. The converse cases are also true for both situations. The basic properties and applications of continued fractions are also studied. And of course, at the end of this work, we gained a lot of knowledge about continued fractions, a field of mathematics that seems to have been ignored before the projet work.

References

1) On continued fractions and its applications. Rana Bassam Badawi.

2) A study in applications of continued fractions. Karen Lynn Parrish

3) Continued fractions : Introduction and applications. Michel Waldschmidt, Carlo Sanna.

CYCLIC GROUP AND ITS APPLICATION

Project submitted for the B.S.C Degree, 6th semester Examination in Mathematics 2023

University of Burdwan

Under the supervision of
Dr. Ujjal Kumar Mukherjee

By

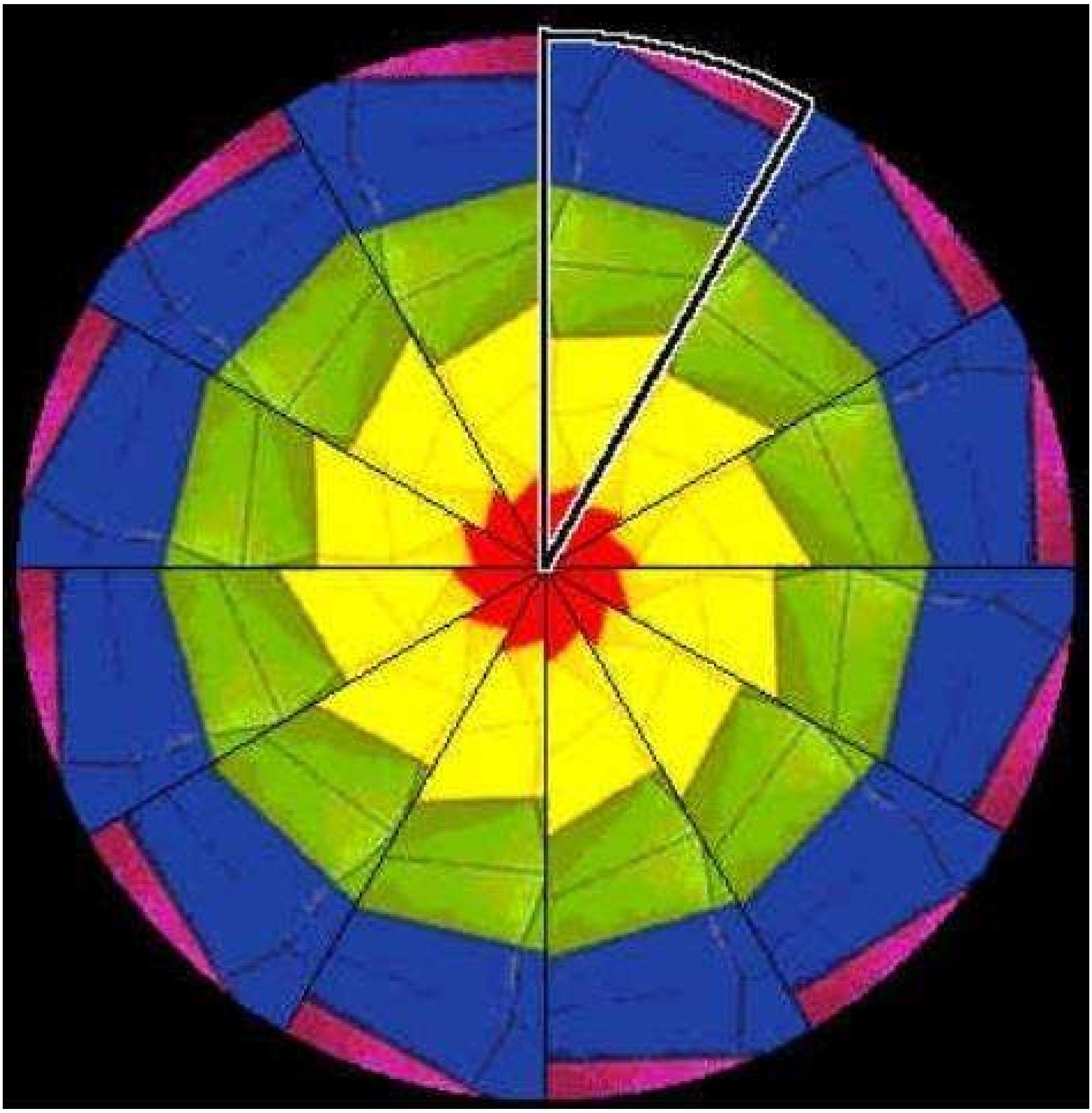
JUHI KHATUN

University Roll No. – 200341200007
University Reg. No. - 201801052194 of 2018-19
Department of Mathematics

……………………………… ……………………………… ………………………………

Signature of Student | Signature of Teacher | Signature of H.O.D

CYCLIC GROUP AND ITS APPLICATION



ACKNOWLEDGEMENT:

I AM GRATEFUL TO **DR UJJAL KUMAR MUKHERJEE** , HEAD OF THE DEPARTMENT OF MATHEMATICS , SARAT CENTENARY COLLEGE , UNIVERSITY OF BURDWAN UNDER WHOSE SUPERVISION THE PROJECT WORK HAVE BEEN CARRIED OUT. I AM ALSOGRATEFUL TO ALL THE PROFESSOR OF DEPARTMENT OF MATHEMATICS, BURDWAN UNIVERSITY FOR THEIR CONSTANT SUPPORT THROUGHOUT THE WORK . I AM THANKFUL TO THE AUTHORS OF VARIOUS BOOKS WHICH HAVE BEEN CONSULTED DURING THE PREPARATION OF THIS PROJECT WORK. FINALLY I EXPRESS MY SINCERE THANKS TO THE STAFF MEMBERS OF THE OFFICE , LIBRARY OF OUR DEPARTMENT AND ALSO THE DEPARTMENT FOR INFRASTRUCTURAL SUPPORT.

Date   Signature of the Teacher

CERTIFICATE:

THIS IS TO CERTIFY THAT JUHI KHATUN HAS WORKED OUT THE PROJECT WORK ENTITLED " CYCLIC GROUP" UNDER MY SUPERVISON . IN MY OPINION THE WORK IS WORTHY OF CONSIDERATION FOR PARTIAL FULFILMENT OF HER B.SC DEGREE IN MATHEMATICS.

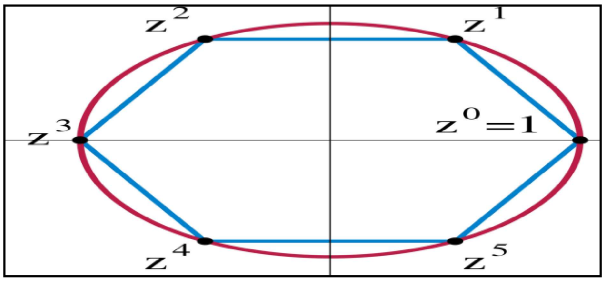
Date   Signature of the Teacher

CONTENTS

INTRODUCTION :

Certain groups and subgroups of groups have particularly nice structures. A locally **cyclic group** is a group in which each finitely generated subgroup is cyclic. Cyclic group is invented by Carl Friedrich Gauss, who considered the structure of multiplicative groups of residues mod n and established many properties of cyclic and more general abelian groups that arise in this way.

A cyclic group is a group which is equal to one of its cyclic subgroups: G = ⟨g⟩ for some element g, called a generator of G. For a finite cyclic group G of order n we have $G = \{e, g, g^2, \ldots, g^{n-1}\}$, where e is the identity element and $g^i = g^j$ whenever $i \equiv j \pmod{n}$; in particular $g^n = g^0 = e$, and $g^{-1} = g^{n-1}$.



GROUP: A group consists of a set and a binary operation on that set that fulfills certain conditions. Groups are an example of example of algebraic structures, that all consist of one or more sets and operations on theses sets.

In mathematics, the order of a finite group is the number of its elements. If a group is not finite, one says that its order is infinite.

The order of an element in a group is the smallest positive power of the element which gives you the identity element.

EXAMPLE:

Show that the set of all integers …**-4, -3, -2, -1, 0, 1, 2, 3, 4,** … is an infinite Abelian group with respect to the operation of addition of integers.

Solution:
Let us test all the group axioms for an Abelian group.

(G1) Closure Axiom: We know that the sum of any two integers is also an integer, i.e., for all $a,b \in Z$, $a+b \in Z$. Thus Z is closed with respect to addition.
(G2) Associative Axiom: Since the addition of integers is associative, the associative axiom is satisfied, i.e., for $a,b,c \in Z$∈ such that $a+(b+c)=(a+b)+c$
(G3) Existence of Identity: We know that $0$0 is the additive identity and $0 \in Z$0∈�,
i.e., $0+a=a=0+a \ \forall a \in Z$0+
Hence, additive identity exists.
(G4) Existence of Inverse: If $a \in Z$∈, then $-a \in Z$–∈. Also, $(-a)+a=0=a+(-a)$(–)
Thus, every integer possesses additive inverse. Therefore Z is a group with respect to addition.
Since the addition of integers is a commutative operation, therefore $a+b=b+a \ \forall a,b \in Z$
Hence $(Z,+)$(,+) is an Abelian group. Also, Z contains an infinite number of elements.
Therefore $(Z,+)$(,+) is an Abelian group of infinite order.

SUBGROUP: Let (G, ⋆) be a group and H be a non-empty subset of G, such that (H, ⋆) is a group then, "H" is called a subgroup of G.

That means H also forms a group under a binary operation, i.e., (H, ⋆) is a group.

Also, any subset of a group G is called a complex of G.

ORDER OF SUBGROUP: In general, the order of any subgroup of G divides the order of G. More precisely: if H is a subgroup of G, then ord(G) / ord(H) =

[G : H], where [G : H] is the index of H in G, an integer. This is Lagrange's theorem. If a has infinite order, then all powers of a have infinite order as well.

ORDER OF ELEMENTS OF SUBGROUP: The order of an element of a group (also called period length or period) is the order of the subgroup generated by the element.

EXAMPLE:consider the set of nonzero real numbers, R∗,�∗, with the group operation of multiplication. The identity of this group is 11 and the inverse of any element a∈R∗�∈�∗ is just 1/a.1/�. We will show that

Q∗={p/q:pandqare nonzero integers}and are nonzero integers}

is a subgroup of R∗.∗.

Solution

The identity of R∗∗ is 1;1; however, 1=1/11=1/1 is the quotient of two nonzero integers. Hence, the identity of R∗∗ is in Q∗.∗. Given two elements in Q∗,∗, say p/qand r/s, , their product pr/qs is also in Q∗.The inverse of any element p/q∈Q∗is again in Q∗since (p/q)−1=q/p1=. Since multiplication in R∗∗ is associative, multiplication in Q∗∗ is associative.

Definition of cyclic group: Cyclic groups are groups in which every element is a power of some fixed element. (If the group is abelian and I'm using + as the operation, then I should say instead that every element is a multiple of some fixed element.) Here are the relevant definitions. Definition. Let G be a group, g ∈ G. The order of g is the smallest positive integer n such that g n = 1. If there is no positive integer n such that g n = 1, then g has infinite order. In the case of an abelian group with + as the operation and 0 as the identity, the order of g is the smallest positive integer n such that ng = 0. Definition. If G is a group and g ∈ G, then the subgroup generated by g is hgi = {g n | n ∈ Z}. If the group is abelian and I'm using + as the operation, then hgi = {ng | n ∈ Z}. Definition. A group G is cyclic if G = hgi for some g ∈ G. g is a generator of hgi. If a generator g has order n, G = hgi is cyclic of order n. If a generator g has infinite order, G = h is infinite cyclic.

Example. (The integers and the integers mod n are cyclic) Show that Z and Zn for n > 0 are cyclic. Z is an infinite cyclic group, because every element is a multiple of 1 (or of −1). For instance, 117 = 117·1. (Remember that "117 · 1" is really shorthand for 1 + 1 + · · · + 1 — 1 added to itself 117 times.) In fact, it is the only infinite cyclic group up to isomorphism. Notice that a cyclic group can have more than one generator. If n is a positive integer, Zn is a cyclic group of order n generated by 1. For example, 1 generates Z7, since

+ 1 = 2 1 + 1 + 1 = 3 1 + 1 + 1 + 1 = 4 1 + 1 + 1 + 1 + 1 = 5 1 + 1 + 1 + 1 + 1 + 1 = 6 1 + 1 + 1 + 1 + 1 + 1 + 1 = 0

In other words, if you add 1 to itself repeatedly, you eventually cycle back to 0.

Order of cyclic group: let (G, ∘) be a cyclic group generated by a. The order of group G is equal to the order of the element a in G. In other words, |�|=|�|, where |�| denotes the order of the element g. Depending upon whether the group G is finite or infinite, we say G to be a finite cyclic group or an infinite cyclic group.

In the above example, (Z_4, +) is a finite cyclic group of order 4, and the group (Z, +) is an infinite cyclic group.

Order of elements of cyclic group: In a cyclic group of infinite order, identity has order 1 and all other elements have order . In a cyclic group of order , order of is n gcd (n , k) . Furthermore, the (distinct) elements which have order are { a d i : i ∈ Z n d ∗ } .

EXAMPLE.

A cyclic group is a group that is generated by a single element. Some examples of cyclic groups include:

- The group of integers modulo n, denoted Z/nZ, where n is a positive integer. This group is the set of integers {0, 1, 2, ..., n-1} with the operation of addition modulo n.
- The group of units modulo n, denoted (Z/nZ)*, which is the set of integers {1, 2, ..., n-1} that are relatively prime to n.
- The group of complex roots of unity, denoted C*n, where n is a positive integer. This group is the set of complex numbers of the form cos(2πk/n) + i*sin(2πk/n), where k is an integer between 0 and n-1.
- The group of permutations of a finite set, denoted S_n, where n is a positive integer. This group is the set of bijections from a set of n elements to itself, with the operation of composition of functions.

SOME PROPERTIES AND INTERESTING THEORM ,CONSULTINGCYCLIC GROUPS:

PROPERTIES:

- If a cyclic group is generated by a, then it is also generated by a^{-1}.
- Every cyclic group is abelian (commutative).
- If a cyclic group is generated by a, then both the orders of G and a are the same.
- Let G be a finite group of order n. If G is cyclic then there exists an element b in G such that the order of b is n.
- Let G be a finite cyclic group of order n and G=<a>. Then G=<a^r> if and only if r<n and gcd(r, n)=1. Thus the number of generators of a finite cyclic group of order n is Φ(n), where Φ is the Euler-Phi function.
- Every subgroup of a cyclic group is also cyclic.
- A cyclic group of prime order has no proper non-trivial subgroup.
- Let G be a cyclic group of order n. Then G has one and only one subgroup of order d for every positive divisor d of n.

- If an infinite cyclic group G is generated by a, then a and a^{-1} are the only generators of G.

THEORMS:

1; Theorem

Let g be an element of a group G and write hgi = {g k : k ∈ Z}. Then hgi is a subgroup of G

Proof. Since 1 = g 0 , 1 ∈ hgi. Suppose a, b ∈ hgi. Then a = g k , b = g m and ab = g k g m = g k+m. Hence ab ∈ hgi (note that k + m ∈ Z). Moreover, a −1 = (g k) −1 = g −k and −k ∈ Z, so that a −1 ∈ hgi. Thus, , we have checked the three conditions necessary for hgi to be a subgroup of G.

DEFINITION 2. If g ∈ G, then the subgroup hgi = {g k : k ∈ Z} is called the cyclic subgroup of G generated by g, If G = hgi, then we say that G is a cyclic group and that g is a generator OF G.

EXAMPLES. (1) If G is any group then {1} = h1i is a cyclic subgroup of G. (2) The group G = {1, −1, i, −i} ⊆ C∗ (the group operation is multiplication of complex numbers) is cyclic with generator i. In fact hii = {i 0 = 1, i1 = i, i2 = −1, i3 = −i} = G. Note that −i is also a generator for G since h−ii = {(−i) 0 = 1,(−i) 1 = −i,(−i) 2 = −1,(−i) 3 = i} = G. Thus a cyclic group may have more than one generator. However, not all elements of G need be generators. For example h−1i = {1, −1} 6= G so −1 is not a generator of G. (3) The group G = Z ∗ 7 = the group of units of the ring Z7 is a cyclic group with generator 3. Indeed, h3i = {1 = 30 , 3 = 31 , 2 = 32 , 6 = 33 , 4 = 34 , 5 = 35 } = G

Note that 5 is also a generator of G, but that h2i = {1, 2, 4} 6= G so that 2 is not a generator of G. (4) G = hπi = {π k : k ∈ Z} is a cyclic subgroup of R∗ . (5) The group G = Z ∗ 8 is not cyclic. Indeed, since Z ∗ 8 = {1, 3, 5, 7} and h1i = {1}, h3i = {1, 3}, h5i = {1, 5}, h7i = {1, 7}, it follows that Z ∗ 8 6= hai for any a ∈ Z ∗ 8 .

If a group G is written additively, then the identity element is denoted 0, the inverse of a ∈ G is denoted −a, and the powers of a become na in additive notation. Thus, with this notation, the cyclic subgroup of G generated by a is hai = {na : n ∈ Z}, consisting of all the multiples of a. Among groups that are normally written additively, the following are two examples of cyclic groups.

(6) The integers Z are a cyclic group. Indeed, Z = h1i since each integer k = k · 1 is a multiple of 1, so k ∈ h1i and h1i = Z. Also, Z = h−1i because k = (−k) · (−1) for each k ∈ Z. (7) Zn is a cyclic group under addition with generator 1.

2.THEORMS: Let g be an element of a group G. Then there are two possibilites for the cyclic subgroup of G.

Case 1: The cyclic subgroup hgi is finite. In this case, there exists a smallest positive integer n such that g n = 1 and we have (a) g k = 1 if and only if n|k. (b) g k = g m if and only if k ≡ m (mod n). (c) hgi = {1, g, g2 , . . . , gn−1 } and the elements 1, g, g2 , . . . , gn−1 are distinct. Case 2: The cyclic subgroup hgi is infinite. Then (d) g k = 1 if and only if k = 0. (e) g k = g m if and only if k = m. (f) hgi = {. . . , g−3 , g−2 , g−1 , 1, g, g2 , g3 , . . .} and all of these powers of g are distinct.

Proof. Case 1. Since hgi is finite, the powers g, g 2 , g 3 , . . . are not all distinct, so let g k = g m with k < m. Then g m−k = 1 where m − k > 0. Hence there is a positive integer l with g l = 1.

Hence there is a smallest such positive integer. We let n be this smallest positive integer, i.e., n is the smallest positive integer such that g n = 1.

If n|k then k = qn for some q ∈ n. Then g k = g qn = (g n) q = 1q = 1. Conversely, if g k = 1, use the division algorithm to write k = qn + r with 0 ≤ r < n. Then g r = g k (g n) −q = 1(1)−q = 1. Since r < n, this contradicts the minimality of n unless r = 0. Hence r = 0 and k = qn so that n|k.

(b) g k = g m if and only if g k−m = 1. Now apply Part (a).

(c) Clearly, {1, g, g2 , . . . , gn−1 } ⊆ hgi. To prove the other inclusion, let a ∈ hgi. Then a = g k for some k ∈ Z. As in Part (a), use the division algorithm to write k = qn+r, where 0 ≤ r ≤ n−1.Then,

a = g k = g qn+r = (g n) q g r = 1q g r = g r ∈ {1, g, g2 , . . . , gn−1 }

which shows that hgi ⊆ {1, g, g2 , . . . , gn−1 }, and hence that

hgi = {1, g, g2 , . . . , gn−1 }.

Finally, suppose that g k = g m where 0 ≤ k ≤ m ≤ n − 1. Then g m−k = 1 and 0 ≤ m − k < n. This implies that m − k = 0 because n is the smallest positive power of g which equals 1. Hence all of the elements 1, g, g2 , . . . , gn−1 are distinct.

Case 2. (d) Certainly, g k = 1 if k = 0. If g k = 1, k 6= 0, then g −k = (g k) −1 = 1−1 = 1, also. Hence g n = 1 for some n > 0, which implies that hgi is finite by the proof of Part (c), contrary to our hypothesis in Case 2. Thus g k = 1 implies that k = 0

(e) g k = g m if and only if g k−m = 1. Now apply Part (d).

(f) hgi = {g k : k ∈ Z} by definition of hgi, so all that remains is to check that these powers are distinct. But this is the content of Part (e).

Recall that if g is an element of a group G, then the order of g is the smallest postive integer n such that g n = 1, and it is denoted |g| = n. If there is no such positive integer, then we say that g has infinte order, denoted |g| = ∞. By Theorem 3, the concept of order of an element g and order of the cyclic subgroup generated by g are the same.

COROLLARY 4. If g is an element of a group G, then |g| = |hgi|.

Proof. This is immediate from Theorem 3, Part (c). If G is a cyclic group of order n, then it is easy to compute the order of all elements of G. This is the content of the following result.

THEOREM 3. Let G = hgi be a cyclic group of order n, and let 0 ≤ k ≤ n−1. If m = gcd(k, n), then |g k | = n m .

Proof. Let k = ms and n = mt. Then (g k) n/m = g kn/m = g msn/m = (g n) s = 1s = 1. Hence n/m divides |g k | by Theorem 3 Part (a). Now suppose that (g k) r = 1. Then g kr = 1, so by Theorem 3 Part (a) n|kr. Hence n m | µ k m ¶ r and since n/m and k/m are relatively prime, it follows that n/m divides r. Hence n/m is the smallest power of g k which equals 1, so |g k | = n/m.

THEORM 4: . Let G = hgi be a cyclic group where |g| = n. Then G = hg k i if and only if gcd(k, n) = 1.

Proof. By Theorem 5, if m = gcd(k, n), then |g k | = n/m. But G = hg k i if and only if |g k | = |G| = n and this happens if and only if m = 1, i.e., if and only if gcd(k, n) = 1.

EXAMPLE If G = hgi is a cyclic group of order 12, then the generators of G are the powers g k where gcd(k, 12) = 1, that is g, g 5 , g 7 , and g 11. In the particular case of the additive cyclic group Z12, the generators are the integers 1, 5, 7, 11 (mod 12).

Now we ask what the subgroups of a cyclic group look like. The question is completely answered by Theorem 8. Theorem 7 is a preliminary, but important, result.

THEORM 5: Every subgroup of a cyclic group is cyclic.

Proof. Suppose that G = hgi = {g k : k ∈ Z} is a cyclic group and let H be a subgroup of G. If H = {1}, then H is cyclic, so we assume that H 6= {1}, and let g k ∈ H with g k 6= 1. Then, since H is a subgroup, g −k = (g k) −1 ∈ H. Therefore, since k or −k is positive, H contains a positive power of g, not equal to 1. So let m be the smallest positive integer such that g m ∈ H. Then, certainly all powers of g m are also in H, so we have hg mi ⊆ H. We claim that this inclusion is an equality. To see this, let g k be any element of H (recall that all elements of G, and hence H, are powers of g since G is cyclic). By the division algorithm, we may write k = qm + r where 0 ≤ r < m. But g k = g qm+r = g qmg r = (g m) q g r so that

g r = (g m) −q g k ∈ H.

Since m is the smallest positive integer with g m ∈ H and 0 ≤ r < m, it follows that we must have r = 0. Then g k = (g m) q ∈ hg mi. Hence we have shown that H ⊆ hg mi and hence H = hg mi. That is H is cyclic with generator g m where m is the smallest postive integer for which g m ∈ H

THEORM 6: (Fundamental Theorem of Finite Cyclic Groups) Let G = hgi be a cyclic group of order n.

(a) If H is any subgroup of G, then H = hg d i for some d|n.
(b)) If H is any subgroup of G with |H| = k, then k|n.
(c) If k|n, then hg n/ki is the unique subgroup of G of order k.

Proof. (a) By Theorem 5, H is a cyclic group and since |G| = n < ∞, it follows that H = hg mi where m > 0. Let d = gcd(m, n). Since d|n it is sufficient to show that H = hg d i. But d|m also, so m = qd. Then g m = (g d) q so g m ∈ hg d i. Hence H = hg mi ⊆ hg d i. But d = rm + sn, where r, s ∈ Z,

g d = g rm+sn = g rmg sn = (g m) r (g n) s = (g m) r (1)s = (g m) r ∈ hg mi = H

This shows that hg d i ⊆ H and hence hg d i = H

(b) By Part (a), H = hg d i where d|n. Then k = |H| = n/d so k|n

(c) Suppose that K is any subgroup of G of order k. By Part (a), let K = hg mi where m|n. Then Theorem 5 gives k = |K| = |g m| = n/m. Hence m = n/k, so K = hg n/ki. This proves (c).

Note that hg mi ⊆ hg k i if and only if k|m. Hence the lattice diagram of G is:

G % - hg 2 i hg 3 i % - % hg 4 i hg 6 i - % h1i

APPLICATION: Number Theory. Cyclic groups are found in nature, patterns, and other fields of mathematics. A common application of a cyclic group is in number theory. The division algorithm is a fundamental tool for the study of cyclic groups.

Division algorithm for integers: if m is a positive integer and n is any integer, then there exist unique integers q and r such that

n = mq + r and 0 ≤ r < m.

Find the quotient q and remainder r when 45 is divided by 7 according to the division algorithm.

The positive multiples of 7 are 7, 14, 21, 28, 35, 42, 49 · · ·

45 = 42 + 3 = 7(6) + 3

The quotient is q = 6 and the remainder is r = 3.

You can use the division algorithm to show that a subgroup H of a cyclic group G is also cyclic

2. A subgroup of a cyclic group is cyclic.

Proof. Let G be a cyclic group generated by a and let H be a subgroup of G. If H = e, then H =< e > is cyclic. If H 6= e, then a n ∈ H for some n ∈ Z +.Let m

We must show that every b ∈ H is a power of c. Since b ∈ H and H ≤ G , we have b = a n for some n. Find a q and r such that

n = mq + r and 0 ≤ r < m.then,

a n = a mq+r = (a m) q a r ,so

a r = (a m) −q a r .

Since a n ∈ H, am ∈ H and H is a group, both (a m) −q and a n are in H. Thus (a m) −qn ∈ H, then a r ∈ H. Since m was the smallest positive integer such that a m ∈ H and 0 ≤ r < m, we must have that r = 0. Thus n = qm and

b = a n = (a m) q = c q , So b is a power of c

Cyclic Groups in Bell Ringing. Method ringing, known as scientific ringing, is the practice of ringing the series of bells as a series of permutations. A permutation f : 1, 2, . . . , n → 1, 2, . . . , n, where the domain numbers represent positions and the range numbers represent bells. f(1) would ring the bell first and bell f(n) last [6]. The number of bells n has n! possible changes [4].

The bell ringer cannot choose to ring permutations in any order because some of the bells continue to ring up to 2 seconds. Therefore no bell must be rung twice in a row. These permutations can all be played until it eventually returns to the original pattern of bells.
A common permutation pattern for four bells is the Plain Bob Minimus permutation (Figure 8). The Plain Bob pattern switches the first two bells then the second set of bells. They would start the bell ringing with 1234. The first bell would go to the second position and third would go to the fourth; therefore the next bell combination would be 2143. The next bell switch would be the two middle bells. Therefore the bell 2143 would turn to 2413. The bell ringers would repeat this pattern of switching the first two and second two, followed by switching the middle until about 1/3 of the way through the permutations. At the pattern 1324, we cannot switch the middle two. If we switched the middle two, we would get back to 1234. Therefore, the bell ringers figured out to switch the last two bells every 8 combinations. Then after 24 moves (4!) we get back to the bell combination of 1234. Since we made rotations of the bells and generated every combination of the set and are now back at the beginning, we can say that the bell ringing pattern is cyclic.

4 bells		
1234	2314	3124
1243	2341	3142
1423	2431	3412
4123	4231	4312
4213	4321	4132
2413	3421	1432
2143	3241	1342
2134	3214	1324
		(1234)

Clock Arithmetic. On a clock the numbers cycle from one to twelve. After circulating around the clock we do not go to 13 but restart at one. If it was 6 o'clock, what would it be in 9 hour.
There are other ways to cover all of the permutations without using the Bob Minimus method(Figure 9). Bob Minimus method is used because it is easy for bell ringers to accomplish because they do not have sheet music. Another common permutation method is following the last bell and moving it over one space to the left each ring then after it is on the left moving it back over to the right.

You can create a cyclic group with any number of bells. However, the more bells you add the longer the cycle will take. Assuming that each bell ring takes 2 seconds, someone can complete a set of three bells in 12 seconds. If we have 9 bells it could take up to 8 days and 10 hours [4]. The bell permutations can be expressed as a Hamiltonian graph. A Hamiltonian path is a undirected or directed graph that visits each vertex exactly once [6]. The Hamiltonian circuit can be drawn as a simple circuit that has a circular path back to the original vertex. Hamiltonian circuits for the symmetric group Sn mod cyclic groups Zn correspond to the change ringing principles on n bells.

Clock Arithmetic. On a clock the numbers cycle from one to twelve. After circulating around the clock we do not go to 13 but restart at one. If it was 6 o'clock, what would it be in 9 hours? 6am + 9 = 3pm. The set of the numbers on a clock are C = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11. This set of numbers is a group. The identity element is 0 what we will think of as 12. If we add 12 hours to anywhere on the clock we will end up in the same position.

REMARK OR CONCLUTION: The demonstration of the characteristics of cyclic group theory and its application shows the importance of cyclic group theory across multiple fields: its prominence within number theory in mathematics, uses within cryptography and possible applications across many other disciplines. Cyclic groups' distinctive nature of having one generative function allows them to play a pivotal role in observation, extrapolation, and implementation. By being generated by only one function and its respective operation, cyclic groups have the unique characteristic that they are inherently Abelian since any member of the group must be a power of the generative function. Therefore, the binary operation must be commutative under any circumstance. As such, this forces all simple cyclic groups to have the unique characteristic that they must have a prime cardinality.

Human minds are designed for pattern recognition and we can find algebraic structures in common objects and things around us. Cyclic groups are the simplest groups that have an object that can generate the whole set. The object can generate the set by addition, multiplication, or rotations. Cyclic groups are not only common in pure mathematics, but also in patterns, shapes, music, and chaos. Cyclic groups are an imperative part of number theory used with the Chinese remainder theorem and Fermats theorem. Knowing if a group is cyclic could help determine if there can be a way to write a group as a simple circuit. This circuit could simplify the process of generation to discover the most efficient way to generate the object for use of future applications in mathematics and elsewhere.

REFERENCE: 1] Fraleigh, J. 2003. A first course in abstract algeabra. Pearson Education.
2] Fraleigh, J. 1994. A first course in abstract algeabra. Addison Wesley
3] Guichard,D.R. 1999. When is U(n) cyclic? An Algebraic Approach. Mathematics Magazine. 72(2):139-142
4] Polster,B.Ross,M.2009.Ringing the changes.Plus Magazine.http://plus.maths.org/content/ringing-changes
5] Hazewinkel,M.2001. Cyclic group.Encyclopedia of Mathematics
[6] White,A.T.1993.Treble dodging minor methods: ringing the cosets, on six bells. Discrete Mathematics. 122(1- 3):307-323
7] Dougal,C.R.2008. Chaos chance money. Plus Magazine.http://plus.maths.org/content/chaos-chance-and-money
8: Trigg G L 2005 Mathematical Tools for Physicists (Wiley-VCH)
9: Rose J S 1994 A Course on Group Theory (Dover Publications Inc.)
10:] Wilson R A 2009 The Finite Simple Groups (Springer-Verlag London Limited)
11] Gorenstein D, Lyons R and Solomon R 1994 The Classification of the Finite Simple Groups (American Mathematical Society)
12:Heller A and Reiner I 1962 Representations of Cyclic Groups in Rings of Integers, I vol 76 (Annals of Mathematics) pp 73–92 [13] Fuchs L 1967 Abelian Groups (Springer Cham)
[13] Fuchs L 1967 Abelian Groups (Springer Cham)
[14] Shpilrain V and Zapata G 2006 Combinatorial Group Theory and Public Key Cryptography (Applicable Algebra in Engineering, Communication and Computing)

Cryptography

Project submitted for the B.SC Degree, 6th semester examination in Mathematics 2023

University of Burdwan

Under the supervision of

Shampa Dutta

By

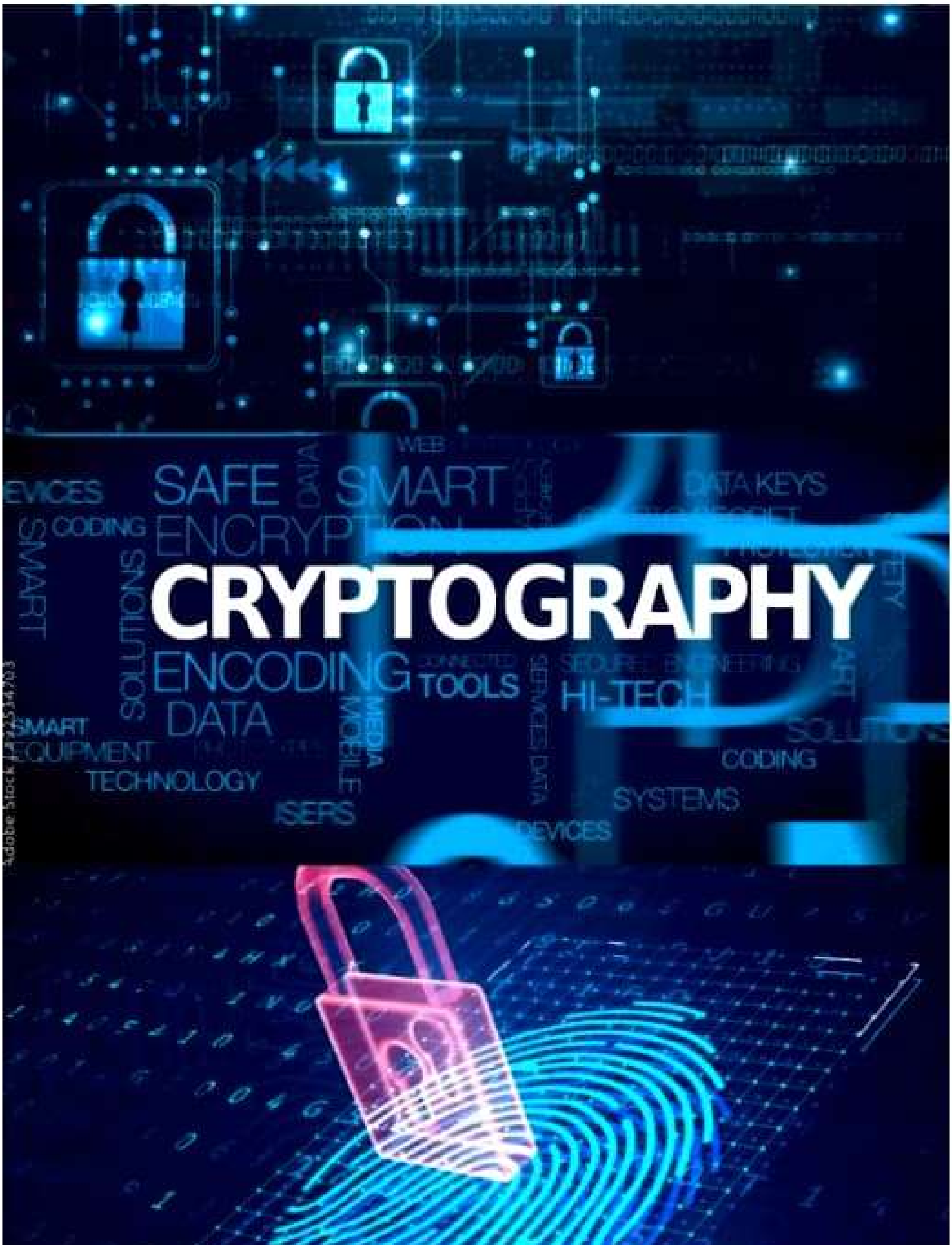
Koyel Ghosh

University Roll No. - 200341200008
University Reg. No. – 202001048580 of 2020-21

Department of Mathematics

Signature of the student | Signature of the teacher | Signature of the H.O.D

CRYPTOGRAPHY



ACKNOWLEDGEMENT

I am grateful to Ms. Shampa Dutta, State Aided College Teacher, Dept. of Mathematics, Sarat Centenary College, University of Burdwan under whose supervision the project work have been carried out. I am also grateful to all the professors of department of Mathematics, Burdwan University for their constant support throughout the work. I am thankful to the authors of various books which have been consulted during the preparation of this project work. Finally I express my sincere thanks to the staff members of the office, library of our department and also the department for infrastructural support.

Date:

....

Signature of the student

CERTIFICATE

This is to certify that Koyel Ghosh has worked out the project work entitled "CRYPTOGRAPHY" under my supervision. In my opinion the work is worthy of consideration for partial fulfilment of his B.Sc. degree in Mathematics`

Date:

....

Signature of the teacher

CONTENTS

INTRODUCTION

- Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography comes From Greek word "crypto" Means hiding and "graphy" Means writing. Cryptography literally means writing something secretly.

• Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

- While cryptography is the science of securing data, cryptanalysis is the science of Analyzing and breaking secure communication. Classical cryptanalysis involves an Interesting combination of analytical reasoning, application of mathematical Tools, pattern finding, patience, determination, and luck. Cryptanalysts are also Called attackers. Cryptology embraces both cryptography and cryptanalysis.

- Computer data often travels from one computer to another, leaving the safety of its protected physical surroundings. Once the data is out of hand, people with bad intention could modify or forge your data, either for amusement or for their own benefit.

- Cryptography can reformat and transform our data, making it safer on its trip between Computers. The technology is based on the essentials of secret codes, augmented by modern mathematics that protects our data in powerful ways.

Computer Security – generic name for the collection of tools designed to protect data and to thwart hackers.

Network Security – measures to protect data during their transmission.

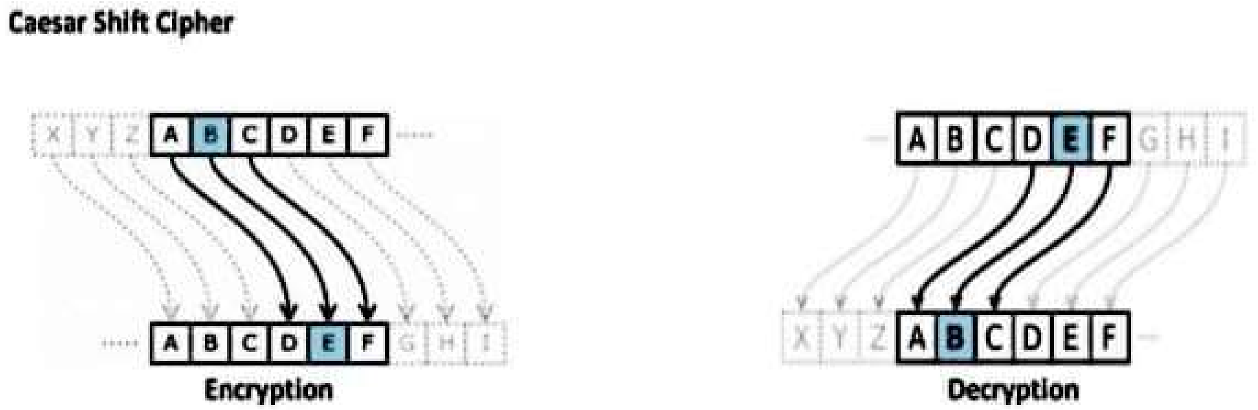
Internet Security – measures to protect data during their transmission over a collection of interconnected networks.

HISTORY OF CRYPTOGRAPHY

It all started around 2000 B.C. where Egyptians used to communicate important information through Egyptian hieroglyphs. Those hieroglyphs are a collection of pictograms with intricate designs and symbols that could be deciphered by only a knowledgeable few. These earliest uses of cryptography were found engraved on some stone.

Then, the trails of cryptography were found in one of the most popular eras of history, the Roman civilization. Julius Caesar, the great emperor of Rome, used a cipher where he used to shift every alphabet thrice to the left. Hence, D will be written in place of A and B will be substituted with an E. This cipher was used for confidential communication across Roman Generals and the emperor was named Caesar cipher after Julius Caesar.

The following figure Shows this process:-



PLAINTEXT : internet society ghana chapter

CYPHERTEXT : lqwhuqhw vrflhwb jkdqd fkdswhu

The Spartan military was known to have recognition for some old ciphers. They were also the ones to introduce steganography, hiding the existence of messages for absolute secrecy and privacy. The first known example of steganography was a hidden message in the tattoo over the shaved head of a messenger. The message was then concealed by regrown hair.

Later, Indians used Kamasutra ciphers, where either the vowels were substituted with some consonants based on their phonetics or used in pairings to substitute their reciprocals. Most of these ciphers were prone to adversaries and cryptanalysis until polyalphabetic ciphers were brought to the spotlight by Arabs.

The following figure Shows this process:-

Kamasutra Cipher

The techniques involves randomly pairing letters of the alphabet, and then substituting each letter in the original message with its partner.

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

The key is the permutation of the alphabet.

INTERNET SOCIETY GHANA CHAPTER

DWRCTWCR FKEDCRL VZJWJ EZJXRCT

Germans were found using an electromechanical Enigma machine for the encryption of private messages in World War II. Then, Alan Turing stepped forward to introduce a machine used to break codes. That was the foundation for the very first modern computers.

With the modernization of technology, cryptography got way more complex. Yet, it took a few decades of serving spies and militaries only before cryptography became a common practice in every organization and department.

Network security symbols

Notes, Cautions, and Warnings are used in the following ways.

Notes are extra, but important, information.

Note: A Note adds important information, but you could still use the product if you didn't have that information.

Cautions indicate the possibility of loss of data or minor damage to equipment.

Caution: A Caution tells you about a situation where there is the potential for loss of data or minor damage to equipment. Special attention should be paid to Cautions.

Warnings indicate the possibility of significant damage to equipment or injury to human beings.

Warning: A Warning means that your equipment may be severely damaged or someone could be injured. Please take Warnings seriously.

What is cryptography ?

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.

Cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email.

Cryptography is the study and practice of techniques for secure communication in the presence of third parties called adversaries. It deals with developing and analyzing protocols that prevents malicious third parties from retrieving information being shared between two entities thereby following the various aspects of information security.

Strength Of Cryptography

"There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files. This book is about the latter."

—Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C.

PGP is also about the latter sort of cryptography.

Cryptography can be strong or weak, as explained above. Cryptographic strength is measured in the time and resources it would require to recover the plaintext. The result of strong cryptography is ciphertext that is very difficult to decipher without possession of the appropriate decoding tool.

Cryptography can either be strong or weak considering the intensity of secrecy demanded by your job and the sensitivity of the piece of information that you carry. If you want to hide a specific document from your sibling or friend, you might need weak cryptography with no serious rituals to hide your information. Basic cryptographic knowledge would do.

However, if the concern is intercommunication between large organizations and even governments, the cryptographic practices involved should be strictly strong observing all the principles of modern encryptions. The strength of the algorithm, the time required for decryption, and resources used, determine the strength of the cryptosystem being utilized.

How does Cryptography work?

A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a key—a word, number, or phrase—to encrypt the plaintext. The same plaintext encrypts to different ciphertext with different keys. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key.

A cryptographic algorithm, plus all possible keys and all the protocols that make it work, comprise a cryptosystem. PGP is a cryptosystem.

What problems does it solve?

Cryptography ensures the integrity of the data in transit as well as in rest. Every software system has multiple endpoints and multiple clients with a back-end server. These client/server interactions often take place over not-so-secure networks. This not-so-secure traversal of information can be protected through cryptographic practices.

An adversary can try to attack a network of traversals In two ways. Passive attacks and active attacks. Passive attacks could be online where the attacker tries to read sensitive information during real-time traversal or it could be offline where the data is kept and read after a while most probably after some decryption. Active attacks let the attacker impersonate a client to modify or read the sensitive content before it is transmitted to the intended destination.

The integrity, confidentiality, and other protocols like SSL/TLS refrain the attackers from eavesdropping and suspicious tampering of the data. Data kept in databases is a common example of data in rest. It can also be protected from attacks through encryption so that in case of a physical medium getting lost or stolen, the sensitive information won't get disclosed.

Objectives of Cryptography

A trustworthy cryptosystem has to abide by certain rules and objectives. Any cryptosystem that fulfils the objectives mentioned below is considered safe and hence can be utilized for cryptographic properties. These objectives are as follows:

1.Confidentiality: Ensures that the information in a computer system a n d transmitted information are accessible only for reading by authorized parties. E.g. Printing, displaying and other forms of disclosure.

2.Authentication: Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.

3.Integrity: Ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages.

4.Non repudiation: Requires that neither the sender nor the receiver of a message be able to deny the transmission.

5.Access control: Requires that access to information resources may be controlled by or the target system.

6.Availability: Requires that computer system assets be available to authorized parties when needed.

Cryptography related Terminologies

- **Cryptography:- The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form.**
- **Plaintext:- The original intelligible message.**
- **Cipher text :-The transformed message.**
- **Cipher :- An algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods.**
- **Key :-Some critical information used by the cipher, known only to the sender& receiver.**
- **Encipher (encode) :-The process of converting plaintext to cipher text using a cipher and a key.**
- **Decipher (decode) :-the process of converting cipher text back into plaintext using a cipher and a key.**

- **Cryptanalysis:- The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key. Also called code breaking.**

- **Cryptographers:- People who do cryptography.**

- **Cryptanalysts:- Practitioners of cryptanalysis.**

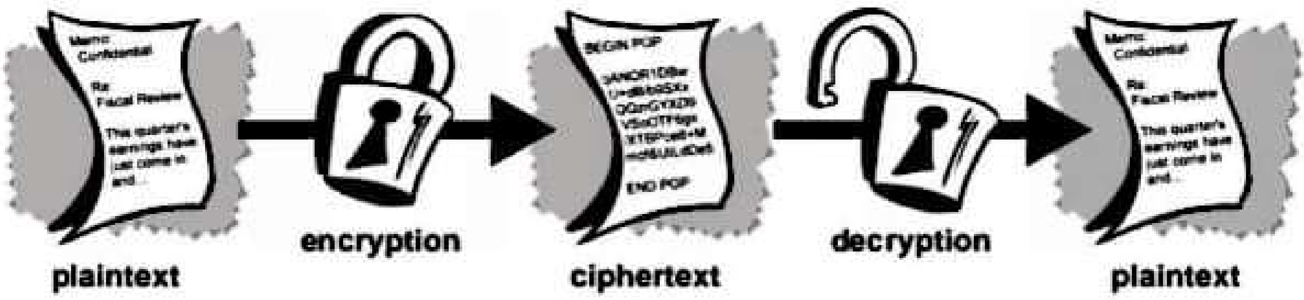
- **Cryptology:- The branch of mathematics that studies the mathematical foundations of cryptographic methods. Both cryptography and cryptanalysis.**

- **Code:- An algorithm for transforming an intelligible message into an unintelligible one using a code-book.**

Encryption & Decryption

Data that can be read and understood without any special measures is called plaintext or cleartext. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called ciphertext. You use encryption to make sure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting ciphertext to its original plaintext is called decryption.

The following figure shows this process:-



Encryption & Decryption process

Source:- Internet

Cryptographic Attacks

Passive Attacks

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Passive Attacks are of two types:

Release of message contents: A telephone conversation, an e-mail message and a transferred file may contain sensitive or confidential information. We would like to prevent the opponent from learning the contents of these transmissions.

Traffic analysis: If we had encryption protection in place, an opponent might still be able to observe the pattern of the message. The opponent could determine the location and identity of communication hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of communication that was taking place.

Passive attacks are very difficult to detect because they do not involve any alteration of data.

However, it is feasible to prevent the success of these attack.

Active attacks

These attacks involve some modification of the data stream or the creation of a false stream. These attacks can be classified in to four categories:

Masquerade – One entity pretends to be a different entity.

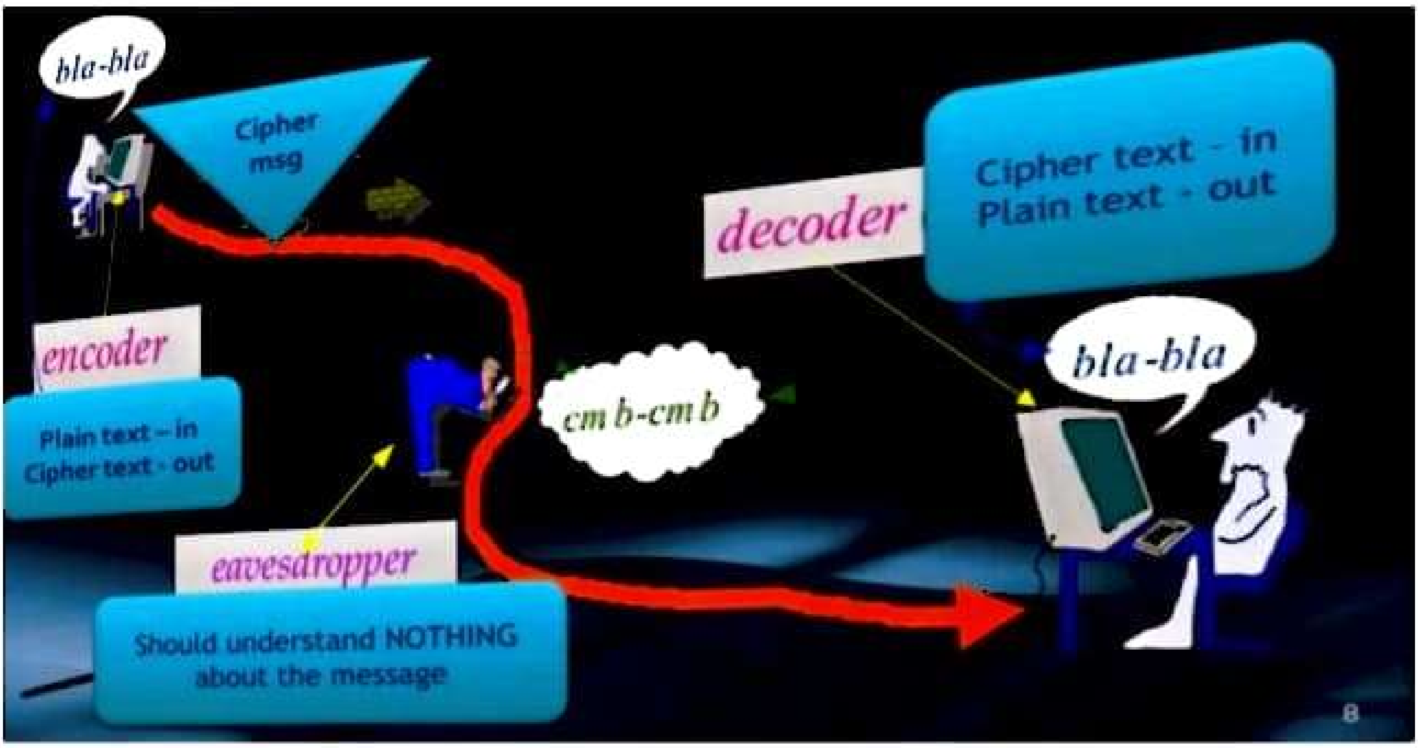
Replay – involves passive capture of a data unit and its subsequent transmission to produce an unauthorized effect.

Modification of messages – Some portion of message is altered or the messages are delayed or recorded, to produce an unauthorized effect.

Denial of service – Prevents or inhibits the normal use or management of communication facilities. Another form of service denial is the disruption of an entire network, either by disabling the network or overloading it with messages so as to degrade performance.

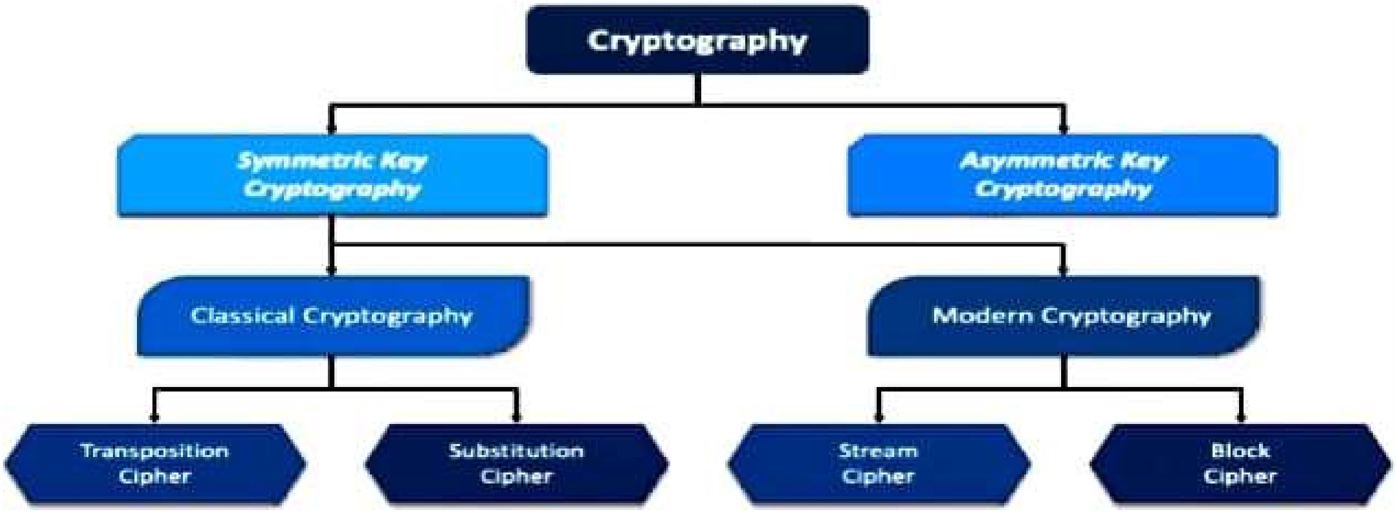
It is quite difficult to prevent active attacks absolutely, because to do so would require physical protection of all communication facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them.

Transmission Techniques



Source :- Internet

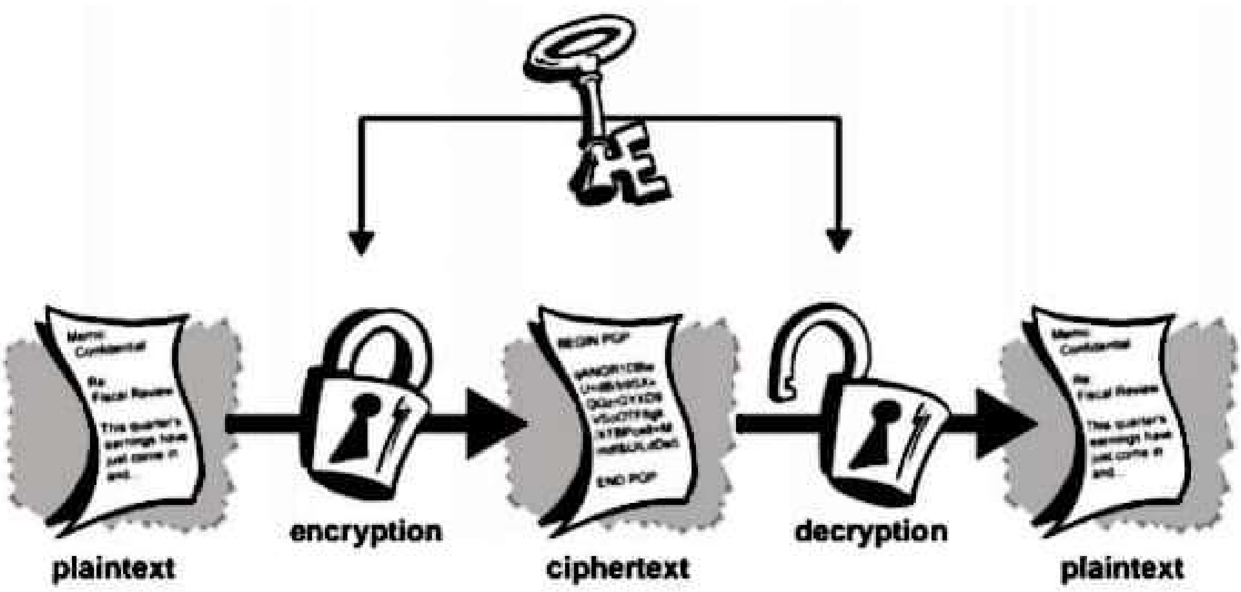
Classification



Symmetric key(secret key cryptography)

Symmetric-key cryptography has the same key for encrypting as well as decrypting the message. The sender is supposed to send the key to the recipient with the ciphertext. Both parties can communicate securely if and only if they know the key and nobody else has access to it. Caesar cipher is a very popular example of symmetric key or secret key encryption. Some of the common symmetric key algorithms are DES, AES, and IDEA etc.

The following figure shows this process:-



Source:- Internet

Classical Encryption Techniques:- There are two basic classical encryption techniques substitution and transposition.

Transposition Cipher

In classical cryptography, a transposition cipher (also known as a permutation cipher) is a method of encryption which scrambles the positions of characters (transposition) without changing the characters themselves. Transposition ciphers reorder units of plaintext (typically characters or groups of characters) according to a regular system to produce a ciphertext which is a permutation of the plaintext. i.e. the order of the character is changed.

Example:-

Plaintext : T R A N S P O S I T I O N

Keyword : 43152

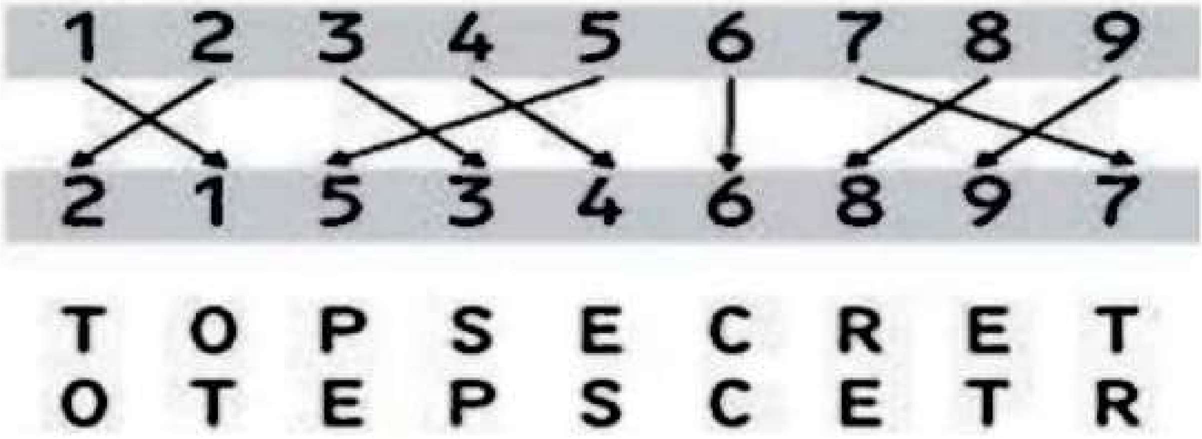
Ciphertext : N I X A S N T P I S T X R O O

1	2	3	4	5
T	R	A	N	S
P	O	S	I	T
I	O	N	X	X

4	3	1	5	2
N	A	T	S	R
I	S	P	T	O
X	N	I	X	O

Plaintext (43152) **Ciphertext**

The following figure shows this process:-



Transposition Cipher

Substitution Cipher

In classical cryptography, a substitution cipher is a method of encrypting in which units of plaintext are replaced with the ciphertext, in a defined manner, with the help of a key; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing the inverse substitution process to extract the original message.

There are a number of different types of substitution cipher. If the cipher operates on single letters, it is termed a simple substitution cipher; a cipher that operates on larger groups of letters is termed polygraphic. A monoalphabetic cipher uses fixed substitution over the entire message, whereas a polyalphabetic cipher uses a number of substitutions at different positions in the message, where a unit from the plaintext is mapped to one of several possibilities in the ciphertext and vice versa.

Example :-

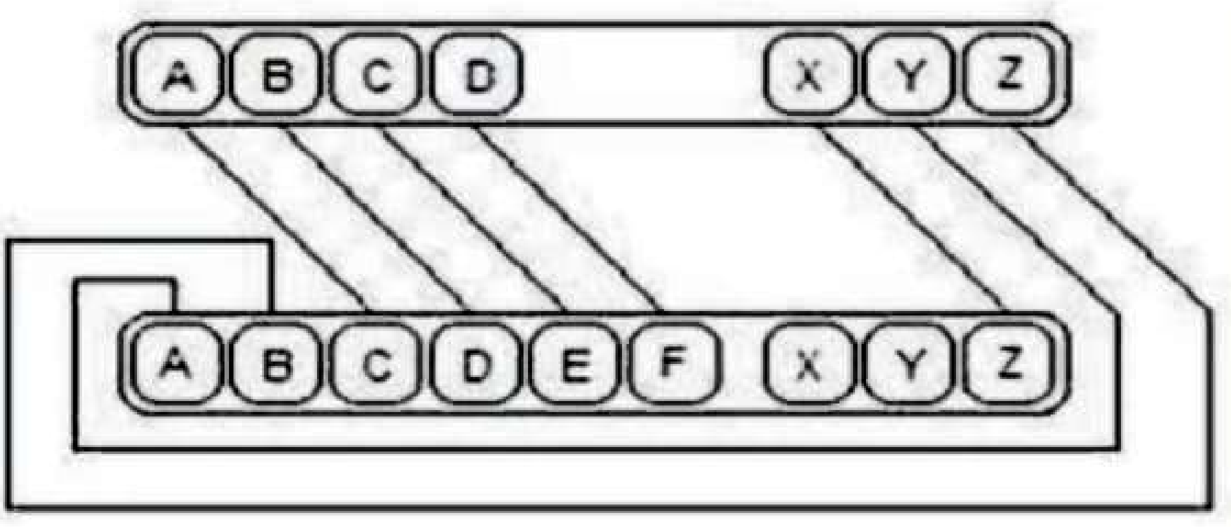
Plaintext : S U B S T I T U T I O N

Ciphertext : H F Y H G R G F G R L M

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

Y Z
B A

The following figure shows this process:-



Substitution Cipher

Source: Internet

Modern encryption and decryption Techniques:-
There are two types of modern encryption and decryption techniques Stream Cipher and Block Cipher.

Stream Cipher

In modern cryptography, a stream cipher is a method of encrypting text (to produce ciphertext) in which a cryptographic key and algorithm are applied to each binary digit in a data stream, one bit at a time. With a stream Cipher, the same plaintext but or byte will encrypt to a different bit or byte everytime it is encrypted. Some examples are RC4, A5/1.

Example:-

For Encryption :

Plaintext: pay 100

Binary of plaintext :01011001

Key stream: 10010101

Perform XOR : --------------------

Ciphertext: 11001100

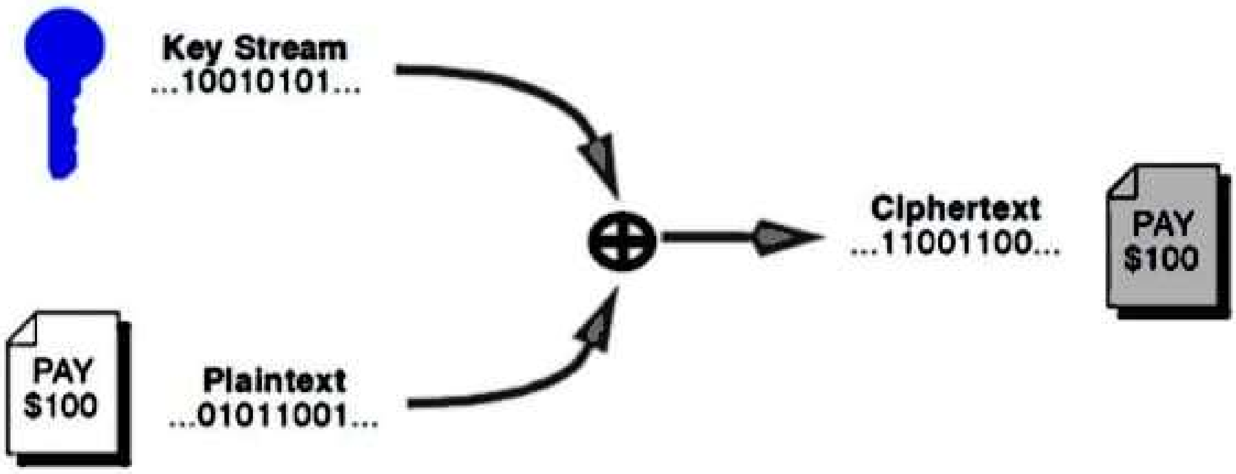
For decryption :

Ciphertext : 11001100

Key stream: 10010101
Perform XOR:------------

Plaintext : 01011001

The following figure shows this process:-



Stream Cipher

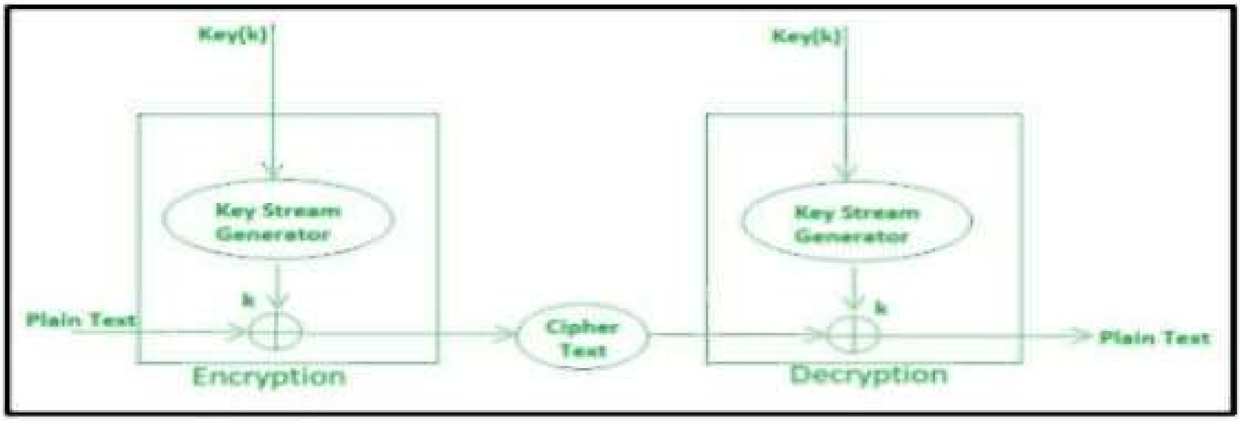


Diagram of Stream Cipher **Source: Internet**

Block Cipher

In modern cryptography, a block Cipher is a method of encrypting data in blocks to produce ciphertext using a Cryptographic key and algorithms. The Block cipher is an encryption algorithm that takes a fixed size of input say b bits and produces a ciphertext of b bits again. If the input is larger than b bits it can be divided further. Most modern block ciphers designed to encrypt data in fixed size blocks of either 64 or 128 bits. For different applications and uses, there are several modes of operations for a block cipher. Some of the common block Cipher modes are ECB, CBC, CFB, OFB etc.

Example:- some examples of block ciphers are Data Encryption Standard (DES), Triple DES(3DES or TDEA) and Advanced Encryption Standard (AES).

DES:

Plaintext : Satishcj

Binary of plaintext: 0111 0011 0110 0001 0111 0100 0110 1001
0111 0011 0110 1000 0110 0011 0110 1010

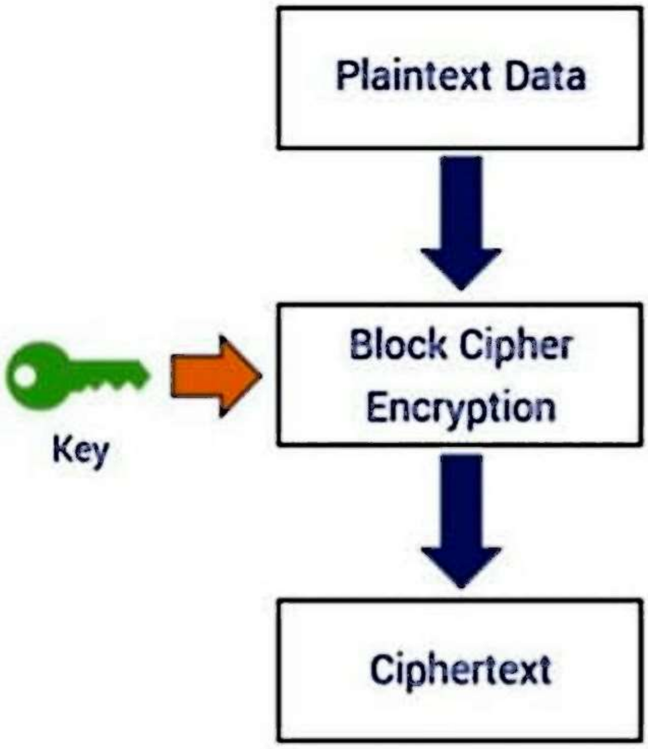
Key: 1010 1110 1011 1100 1010 1001 1011 0100
1101 1001 1100 0010 1100 1001 1100 0000

DES encrypt:- ---

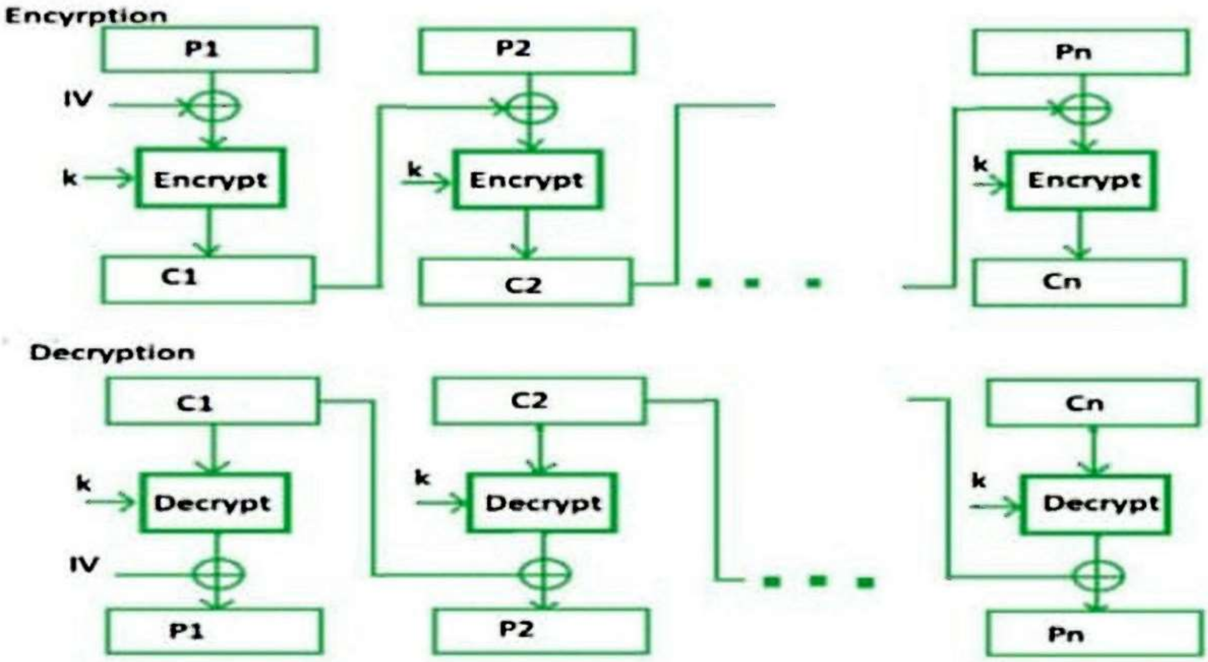
Ciphertext:- 1101 1101 1101 1101 1101 1101 1101 1101
1010 1010 1010 1010 1010 1010 1010 1010

The result is 64 bits or we can say sixteen group containing four bits.

The following figures shows this process:-



Basic Block Cipher



Cipher Block Chaining (CBC)

Differences between Stream Cipher and Block Cipher

Stream Cipher	Block Cipher
Takes one byte of plaintext at a time	Takes one block of plaintext at a time.
Need less time hence simple	Need more time hence complex
Uses exactly 8 bits	Uses 64 or more bits
Utilizes substitution methods	Utilizes transposition methods
No probability of redundency	Redundency might occure
Requires less code for implementation	Requires more code for implementation
Uses one key for one time	One key can be used multiple times
Suitable for implementation in hardwares	Suitable for implementation in softwares
Faster than block cipher	Slower than stream cipher
Vernam cipher is the main implementation	Feistel cipher is the main implementation
Easy to reverse encrypted text	Difficult to reverse encrypted text
Some examples are RC4, A5/1	Some examples are DES, AES

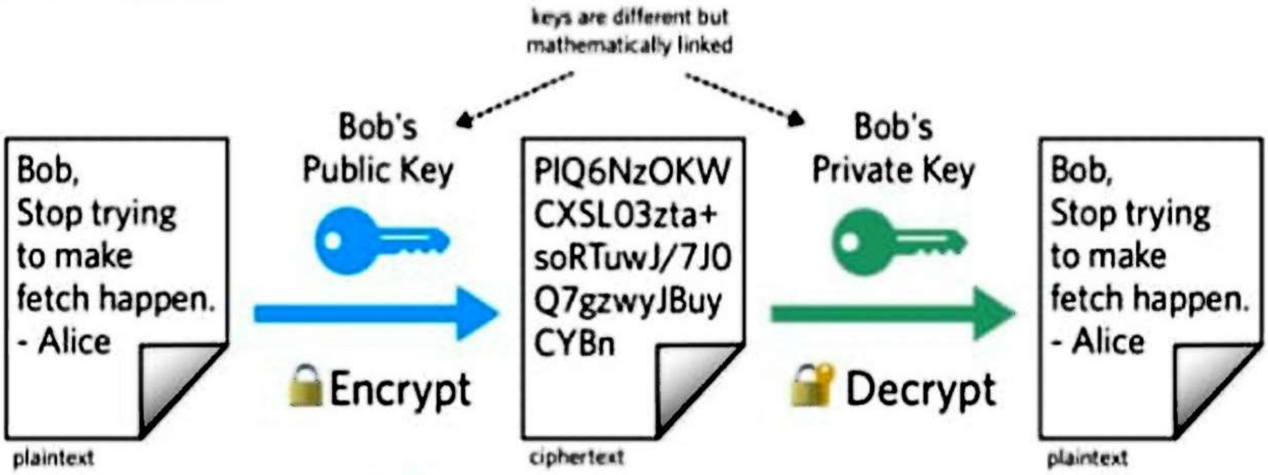
Asymmetric key cryptography (Public key cryptography)

Asymmetric cryptography, also known as Public key cryptography is the field of cryptographic systems that use pairs of related keys. Each key pair consists of a public key and a corresponding private key. Key pairs are generated with cryptographic algorithms based on mathematical problems termed one-way functions. Security of public-key Cryptography depends on keeping the private key secret; the public key can be openly distributed without compromising security. When someone wants to send an encrypted message, they can pull the intended recipient's

public key from a public directory and use it to encrypt the message before sending it. The recipient of the message can then decrypt the message using their related private key.

If the sender encrypts the message using their private key, the message can be decrypted only using that sender's public key, thus authenticating the sender. These encryption and decryption processes happen automatically; users do not need to physically lock and unlock the message. Some of the common asymmetric key algorithms are RSA, DSS, DSA, ECC etc.

Example:-



Public key cryptography

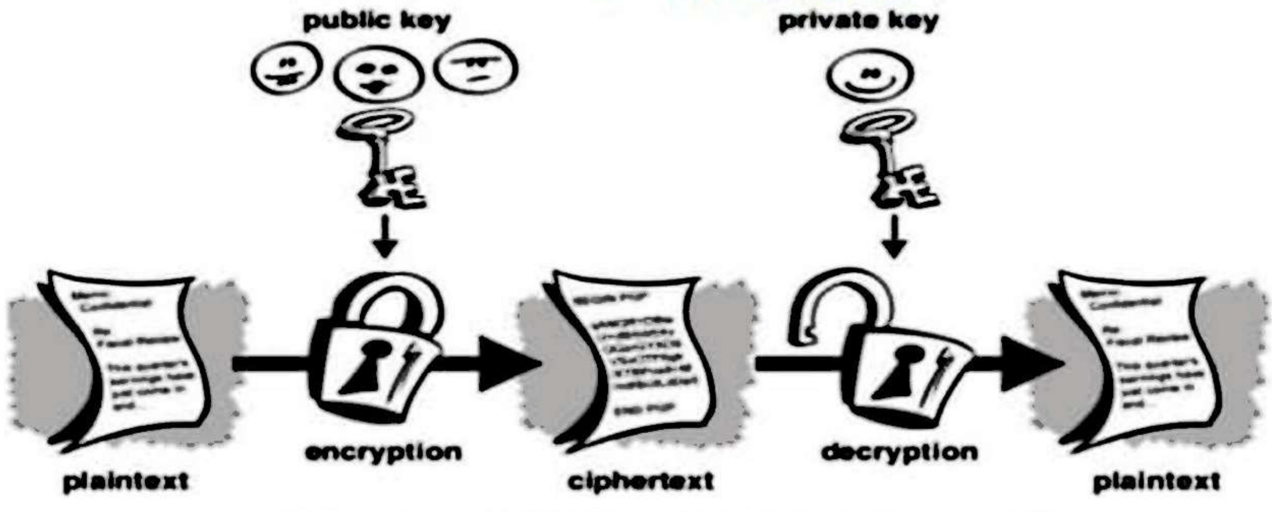


Diagram of public key cryptography

Differences between Symmetric & Asymmetric key cryptography

Symmetric Key cryptography	Asymmetrickey cryptography
• For Symmetric Cryptography, the same key is used for encryption and decryption	• For Asymmetri Cryptography, different keys are used for encryption and decryption
• In Symmetric Cryptography, the speed of encryption and decryption is very fast	• In asymmetric cryptography, the speed of encryption and decryption is slower
• The size of the encrypted text in symmetric cryptography is mostly like the size of the original plaintext	• In Asymmetric cryptography, the size of the text is more than the original plaintext
• Both parties should know the key in symmetric key encryption	• Only one of the keys is known by both the parties in asymmetric cryptography

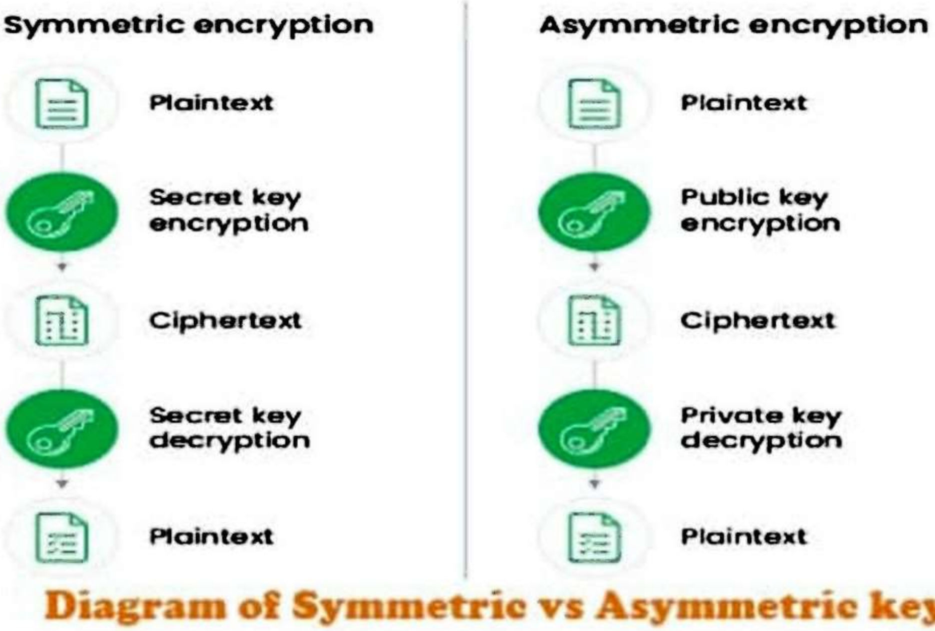


Diagram of Symmetric vs Asymmetric key Cryptography

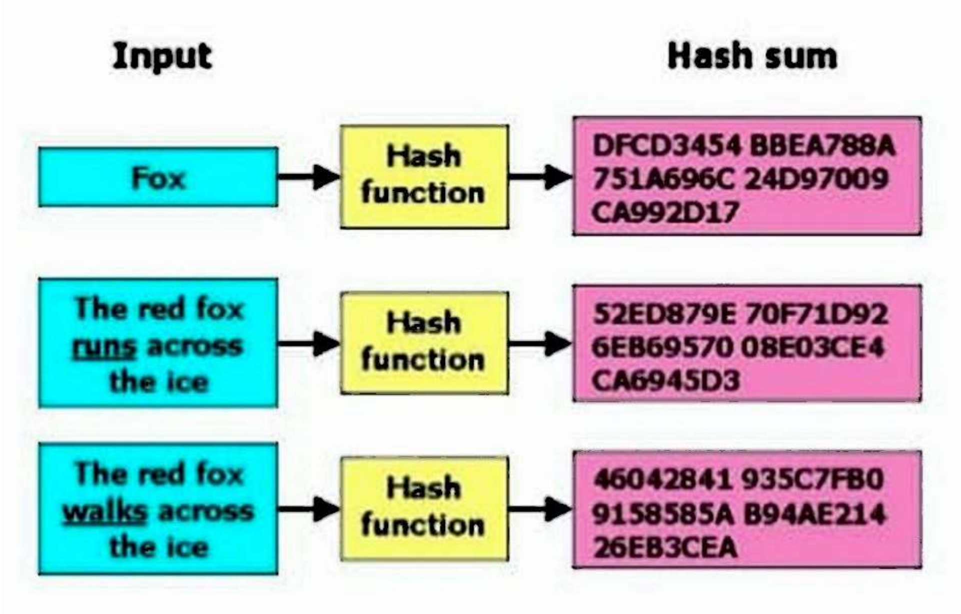
Hash Function

Another type of cryptography system is hash function. Hash functions use random input values and produce a fixed output value that can be used to identify the user for restoring private data. It is a more complex mechanism and hash algorithms are more secure cryptographic systems to use. Hashing is also known by different names such as Digest, Message Digest, Checksum etc.

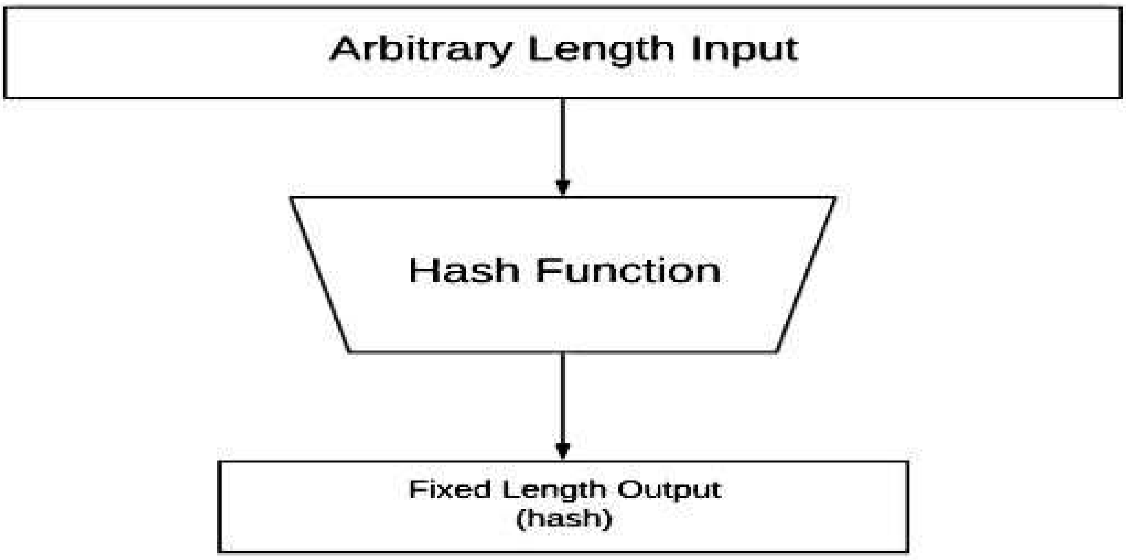
• A cryptographic hash function combines the message-passing capabilities of hash functions with security properties.

• Hash functions are used for cryptocurrency, password security, and message security.

Example:



The following figure Shows this process :



Cryptographic Hash Function

Applications of Cryptography in everyday life

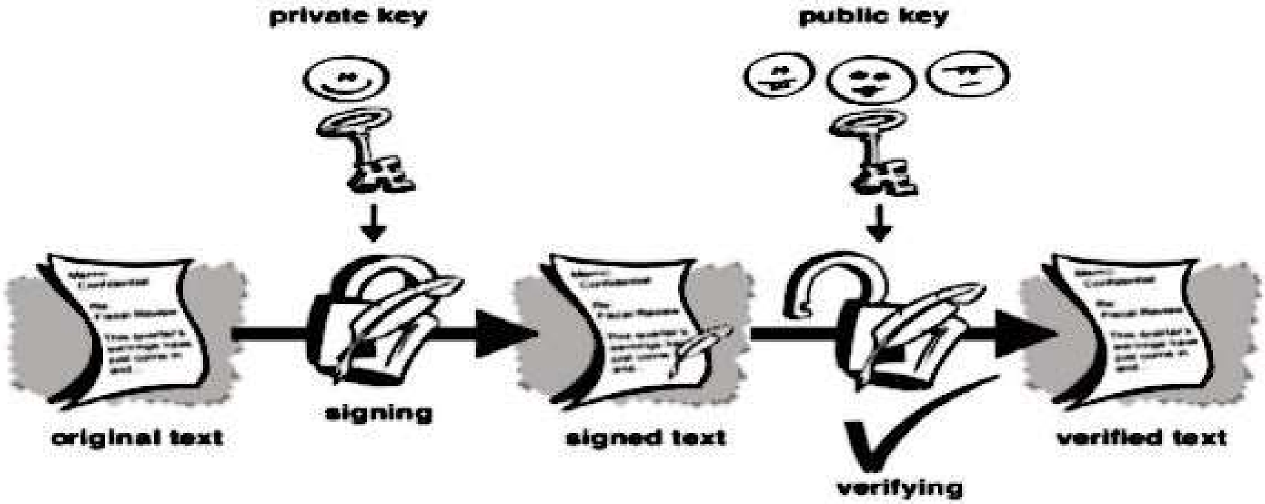
1.Digital Currency : A much-known application of cryptography is digital currency wherein cryptocurrencies are traded over the internet. Digital currency allows people to make payments directly to each other through an online system. Digital currencies have no legislated or intrinsic value; they are simply worth what people are willing to pay for them in the market. This is in contrast to national currencies, which get part of their value from being legislated as legal tender. There are a number of digital currencies the most well known of these are Bitcoin and Ethereum.

2. E-commerce:-With the current pandemic shackling us to our homes, the rise of ecommerce has been tremendous. These transactions are encrypted and perhaps cannot be altered by any third party. Moreover, the passwords we set for such sites are also protected under keys to ensure that no hacker gets access to our e-commerce details for harmful purposes.

3. Digital Signatures:- A major benefit of public key cryptography is that it provides a method for employing digital signatures. Digital signatures let the recipient of information verify the authenticity of the information's origin, and also verify that the information was not altered while in transit. Thus, public key digital signatures provide authentication and data integrity. A digital signature also provides non-repudiation, which means that it prevents the sender from claiming that he or she did not actually send the information. These features are every bit as fundamental to cryptography as privacy, if not more.

A digital signature serves the same purpose as a handwritten signature. However, a handwritten signature is easy to counterfeit. A digital signature is superior to a handwritten signature in that it is nearly impossible to counterfeit, plus it attests to the contents of the information as well as to the identity of the signer.

The basic manner in which digital signatures are created is shown in the following figure.



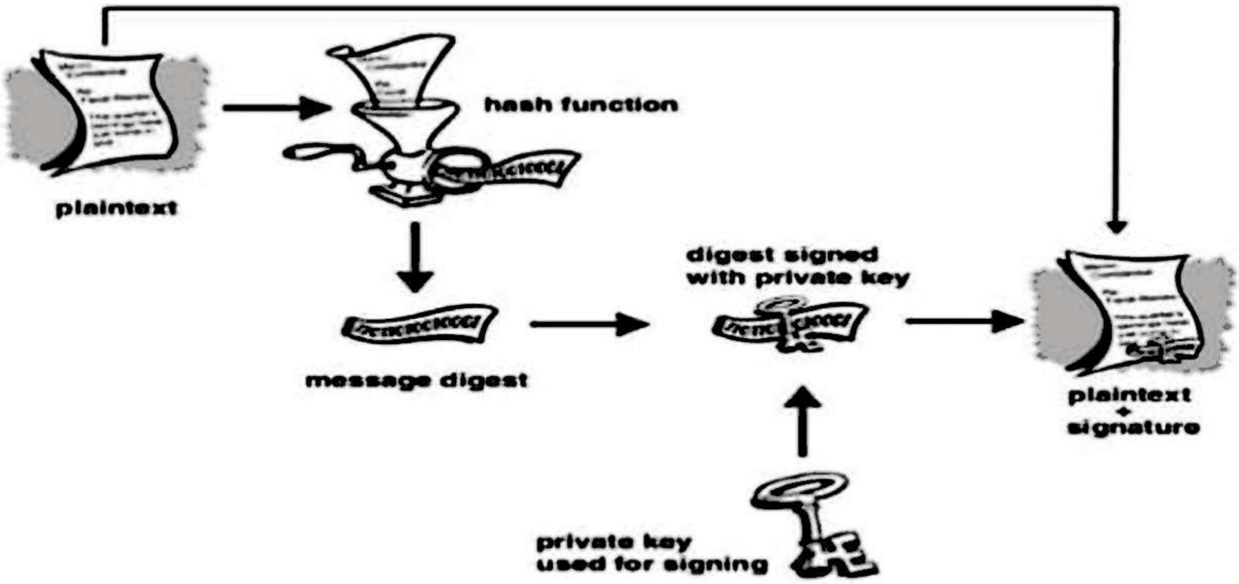
Simple Digital Signature

PGP uses a cryptographically strong hash function on the plaintext the user is signing. This generates a fixed-length data item known as a message digest. (Again, any change to the information results in a totally different digest.)

Then PGP uses the digest and the private key to create the "signature." PGP transmits the signature and the plaintext together. Upon receipt of the message, the recipient uses PGP to recompute the digest, thus verifying the signature. PGP can encrypt the plaintext or not; signing plaintext is useful if some of the recipients are not interested in or capable of verifying the signature.

As long as a secure hash function is used, there is no way to take someone's signature from one document and attach it to another, or to alter a signed message in any way. The slightest change to a signed document will cause the digital signature verification process to fail.

The following figure Shows this process:-



Digital signatures play a major role in authenticating and validating the keys of other PGP user.

4.Digital Certificates: **A digital certificate functions much like a physical certificate. A digital certificate is information included with a person's public key that helps others verify that a key is genuine or valid. Digital certificates are used to thwart attempts to substitute one person's key for another.**

A digital certificate consists of three things:

- **A public key**
- **Certificate information ("Identity" information about the user, such as name, user ID, and so on.)**
- **One or more digital signatures**

The purpose of the digital signature on a certificate is to state that the certificate information has been attested to by some other person or entity. The digital signature does

not attest to the authenticity of the certificate as a whole; it vouches only that the Signed identity information goes along with, or is bound to, the public key.

Thus, a certificate is basically a public key with one or two forms of ID attached, plus a hearty stamp of approval from some other trusted individual.

The following figure shows this process:-

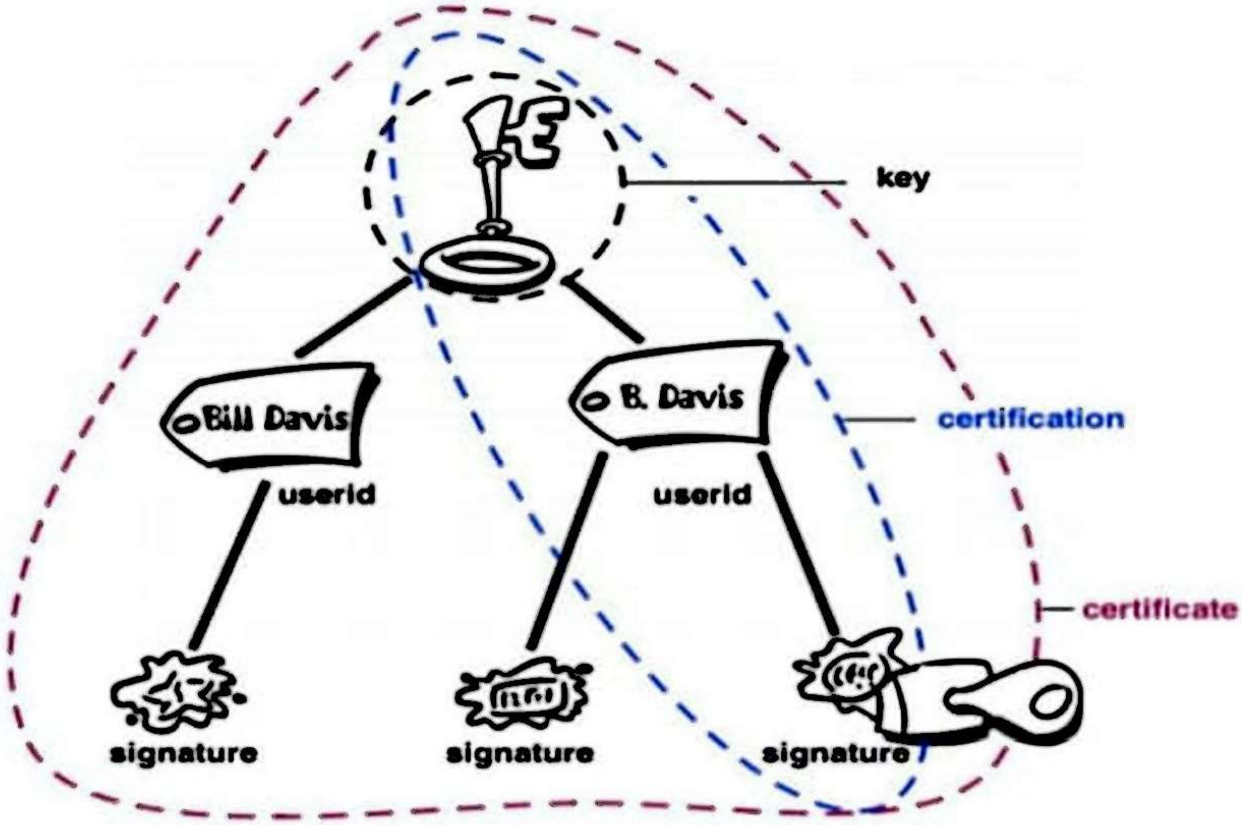


Diagram of Digital Certificate

Cryptanalysis

The process of attempting to discover X or K or both is known as cryptanalysis. The strategy used by the cryptanalysis depends on the nature of the encryption scheme and the information available to the cryptanalyst.

There are various types of cryptanalytic attacks based on the amount of information known to the cryptanalyst.

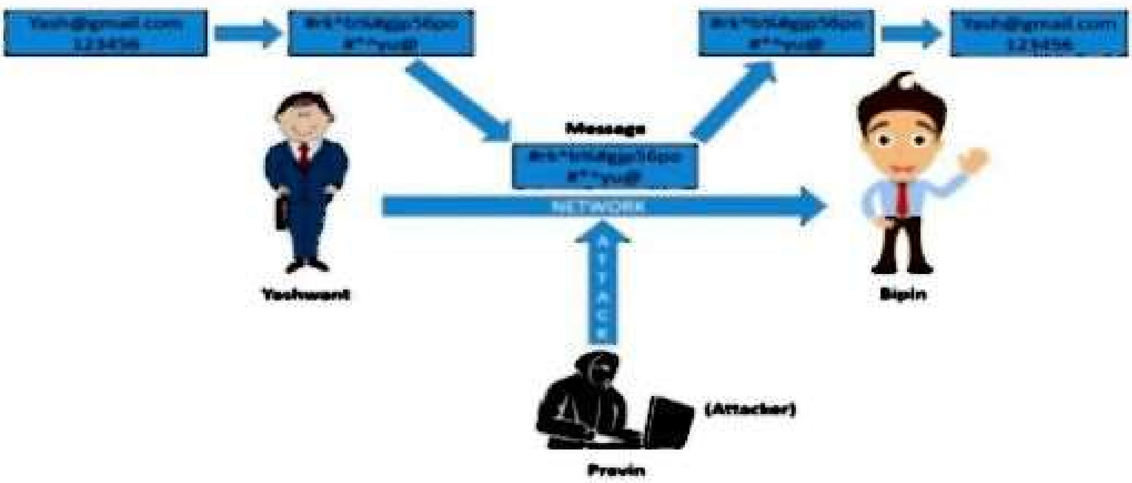
Cipher text only – A copy of cipher text alone is known to the cryptanalyst.

Known plaintext – The cryptanalyst has a copy of the cipher text and the corresponding plaintext.

Chosen plaintext – The cryptanalysts gains temporary access to the encryption machine. They cannot open it to find the key, however; they can encrypt a large number of suitably chosen plaintexts and try to use the resulting cipher texts to deduce the key.

Chosen cipher text – The cryptanalyst obtains temporary access to the decryption machine, uses it to decrypt several string of symbols, and tries to use the results to deduce the key.

The following figure Shows this process:-



Cryptanalysis

Counter Measures

- Use rubber keyboard or virtual keyboards to prevent keystroke sounds.
- Use acoustic printers.
- Use acoustic case for CPU.

Conclusion

- Cryptography, being an art of encrypting and decrypting confidential information and private messages, should be implemented in the network security to prevent any leakageand threat.
- It can be done by using any of these techniques discussed above for fortifying the personal data transmission as well as for secure transaction.
- By using cryptography techniques confidentiality, authentication, integrity, access control and availability of

data is maintained.

- Secure communication is obtained.
- The current trend in society indicates that cryptography is gaining importance. One day cryptography may be widely used throughout the Internet: for electronic mail, for sending documents that are sold over the Web, and even perhaps for all network communication between routers orswitches in the Internet. The use and debate on cryptography promises to be prominent for many more years.

References

1."Handbook of Applied Cryptography" by Alfred J Menezes andScott A Vanstone.

2."Introduction to Cryptography" by Johannes A Bachmann.

3.Bruce Schneier, "Applied Cryptography". John Wiley, New York 1996(2), ISBN 0471-11709-9.

4.Klaus Schmeh, "Cryptography and Public Key Infrastructure on the Internet". John Wiley, New York 2003, ISBN 978-0-470-84745-9.

5.Christopher Swenson, "Modern Cryptanalysis". Wiley Publishing, Indianapolis 2008. ISBN 978-0-470-13593-8.

6.Joan Daemen, Vincent Rijmen, The Design of Rijndael. "AES The Advanced Encryption Standard". Springer-Verlag, Berlin 2002. ISBN 3-540-42580-2.

7. Randall K. Nichols, "Classical Cryptography Course, Volume I& II". Aegean ParkPress, Laguna Hills 1996. ISBN 0-89412-2630& 0-89412-264-9.

8.Dorothy Elizabeth Robling Denning, "Cryptography and Data Security". AddisonWesley, Reading Mass. 1982, ISBN 0-201-10150-5.

9.D. R. Stinson, "Cryptography – Theory and Practice". CRC Press, Boca Raton 1995. ISBN 0-8493-8521-0.

FRACTAL AND ITS APPLICATION

Project submitted for the B.SC Degree, 6th semester examination in Mathematics 2023

University of Burdwan

Under the supervision of

Dr. Ujjal Kumar Mukherjee

By

PINAKI GHOSH

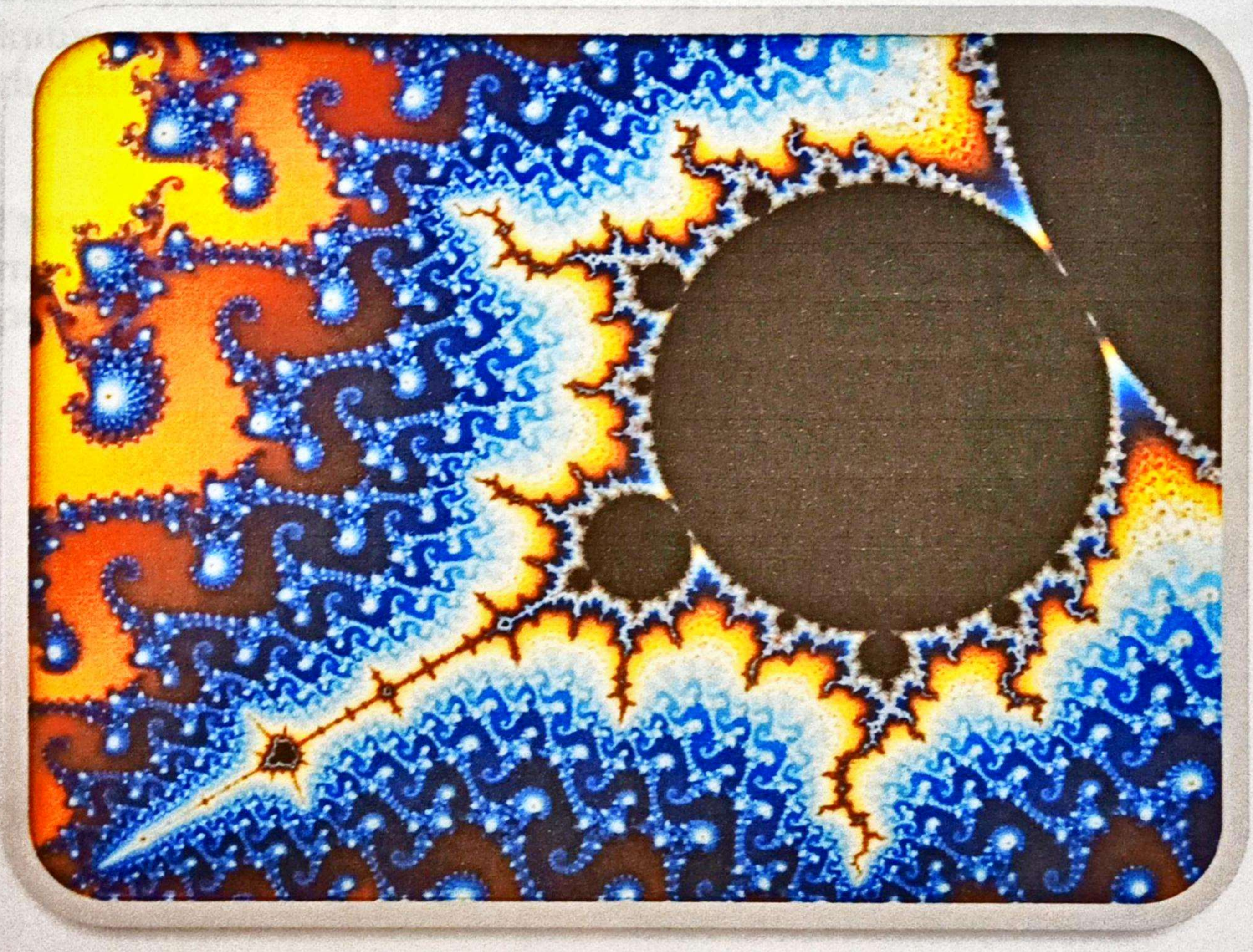
University Roll No. - 200341200009

University Reg. No. - 202001048582 of 2020-21

Department of Mathematics

Signature of the Student	Signature of the Supervisor	Signature of the H.O.D.

FRACTAL
AND
ITS APPLICATION



<u>ACKNOWLEDGEMENT</u>

I would like to thank my Supervisor ***Dr. Ujjal Kr Mukherjee*** and our principal Dr. Sandip Kr Basak for giving me a wonderful opportunity to work on this project "Fractal & it's Application". This project has helped me in doing a lot of research and came to know about a lot of new things. For this experience, I am really thankful.

I would also like to extend my gratitude towards my parents and my project mates who have helped me a lot in finishing the project within the given time frame.

DATE

NAME

Pinaki Ghosh

CERTIFICATE

This is to certify that Pinaki Ghosh has worked out the project work entitled "FRACTALS AND ITS APPLICATIONS" under my supervision. In my opinion the work is worthy of consideration for partial fulfilment of his B.Sc. degree inMathematics.

Date:

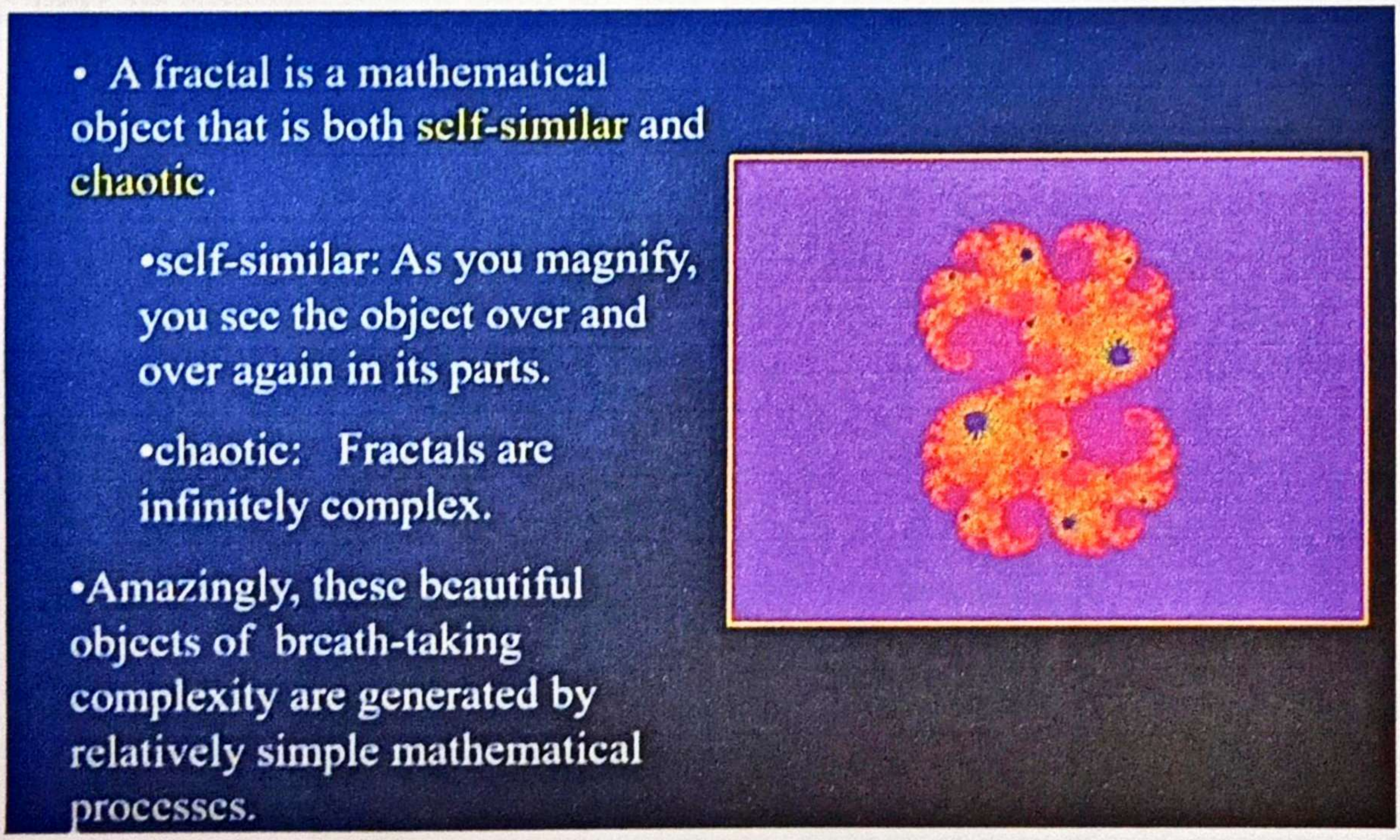
....
Signature of the supervisor

CONTENTS

1. ETYMOLOGY

The term „FRACTAL' was coined by the mathematician Benoit Mandelbrot in1975. Mandelbrot based it on the latine FRACTUS, meaning 'broken' or 'fractured' and used it to extend the concept of theoretical fractional dimensions to geometric patterns in nature.

FRACTALS



INTRODUCTION

Fractals are objects that are self similar at different scales. Think of a tree- it has a trunk that has branches and those branches self have branches coming off of them and those have sub-branches and so on. So that is a fractal.

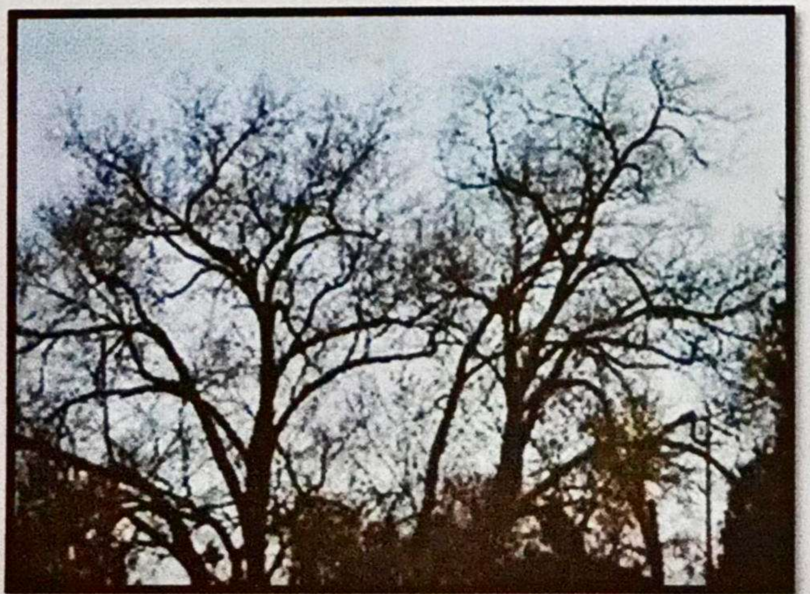
Fractals turn out to be a good way to describe many objects in nature.In this unit we will explore fractals, both visually and mathematically.

It is striking how many natural objects there are with this kind of property. Let"s lookat a simple example,

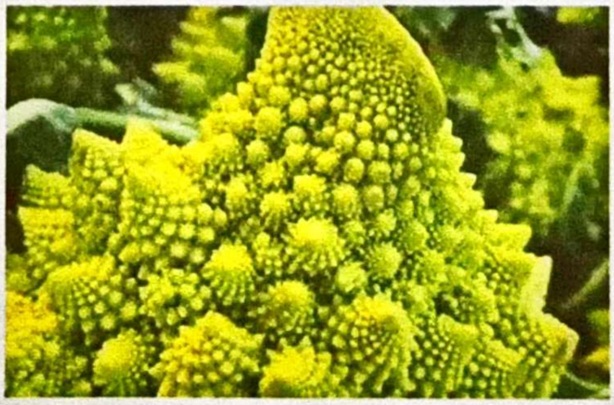
Trees- Trees are fractal and let be explain the notion of self similarity.

Let"s take a picture of a tree. Now we will take part of that picture and crop it out andblow it up. We can see that the structure of this blown up part of this picture is very similar to the structure of the whole picture itself. Let"s do it again. Let"s take a part of this picture within the red box and let"s blow it up. Again, the structure that you see inside the blown up part of this picture looks very similar to the previous two pictures and notice that this third picture is a very tiny part of this original picture.

Now we can do the same thing again. Take a part of the third picture , blow it up again we have structures that look very tree-like. So, no matter how far down you goup to a certain point in these picture you can keep taking little crops, blowing them up and seeing that they have very similar kinds of structure. That"s the crux of the notion of self-similarity at different scales.



shutterstock.com · 417080200



Picture: Fractal In Flowers & Fruits

The actual definition of fractal means that the object is perfectly self similar at all possible scales.

So the objects that we are going to talk about in nature are only fractal-like. They are not real fractals from the mathematical sense, but I am going to use the term **'fractal'** to describe them anyway. So here is a picture of a special kind of broccoli that has fractal properties. We can see that each of these little broccoli mounds consist of other little mounds that themselves have the same structure and so on.

Leaf veins are fractal in the same way that trees are fractal.

Broccoli

Broccoli Mounds

Leaf

HISTORY

The history of fractals traces a path from chiefly theoretical studies To modern applications in computer graphics, with several notable people contributing canonical fractal forms along the way. A common theme in traditional African architecture is the use of fractal scaling, whereby small parts of the structure tend to look similar to larger parts, such as a circular village made of circular houses.

According to Pickover, the mathematics behind fractals began to take shape in the 17th century when the mathematician and philosopher Gottfried Leibniz pondered recursive self-similarity (although he made the mistake of thinking that only the straight line was self-similarin this sense).

In his writings, Leibniz used the term "fractional exponents", but lamented that "Geometry" did not yet know of them. Indeed, according to various historical accounts, after that point few mathematicians tackled the issues and the work of those who did remained obscured largely because of resistance to such unfamiliaremerging concepts, which were sometimes referred to as mathematical "monsters". Thus, it was not until two centuries had passed that on July 18, 1872 Karl Weierstrass presented the first definition of a function with a graph that wouldtoday be considered a fractal, having the non-intuitive property of being everywhere continuous but nowhere differentiable at the Royal Prussian Academy of Sciences.In addition, the quotient difference becomes arbitrarily large as the summation indexincreases. Not long after that, in 1883, Georg Cantor, who attended lectures by Weierstrass, published examples of subsets of the real line known as Cantor sets, which had unusual properties and are nowrecognized as fractals. Also in the last part of that century, Felix Klein and Henri Poincaré introduced a category of fractal that has come to be called "self-inverse" fractals.One of the next milestones came in 1904, when Helge von Koch, extending ideas of Poincaré and dissatisfied with Weierstrass's abstractand analytic definition, gave a more geometric definition including hand-drawn images of a similar function, which is now called the Koch snowflake. Another milestone came a decade later in 1915, when Wacław Sierpiński constructed his famous triangle then, one year later, his carpet. By 1918, two French mathematicians, Pierre Fatou and Gaston Julia, though working independently, arrived essentially simultaneously at results describing what is now seen as fractal behaviour associated with mapping complex numbers and iterative functions and leading to further ideas about attractors and repellors (i.e., points that attract or repel other points), which have become very important in the study of fractals.Very shortly after that work was submitted, by March 1918, Felix Hausdorff expanded the definition of "dimension", significantly for the evolution of thedefinition of fractals, to allow for sets to have non-integer

dimensions. The idea of self-similar curves was taken further by Paul Lévy.

FRACTAL GEOMETRY

The word fractal from the Latin word „Frangere" which means to break, was coined by Benoit Mandelbrot in 1975.

"Fractal objects contain structures nested within one another. Each smaller structure is a miniature, though not necessarily identical, version of the larger form (Peterson,1988,pp.114-115)." In other words, one part of the object is a scaled down version of the entire object. The Koch curve and the Sierpiński gasket are classic, yet simple, examples of self-similar objects.

❖ Geometry of Fractal

Most of the fractals are self-similar geometrical objects.

Several parts of a fractal look similar as the entire image.

It is possible to copy the fractal several times on itself.

Examples are : clouds, forests, galaxies, leaves, feathers, carpets, bricks etc.

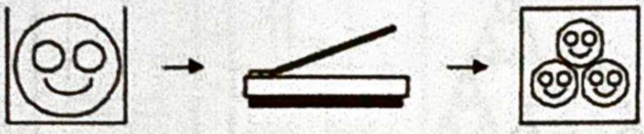
They are complex at your first sight, while in fact can be described by a simple algorithm.

They can be generated by repeated self copy or partial self copy.

Therefore, the redundancy is very high.

Transformation between Fractals

- Imagine a special type of photocopying machine that reduces the image to be copied by a half and reproduces it three times on the copy.

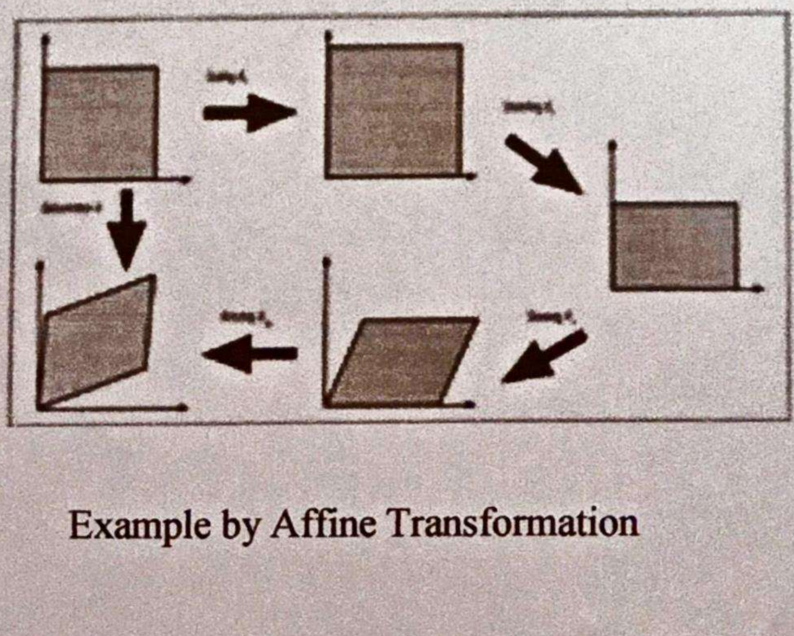


Transformation

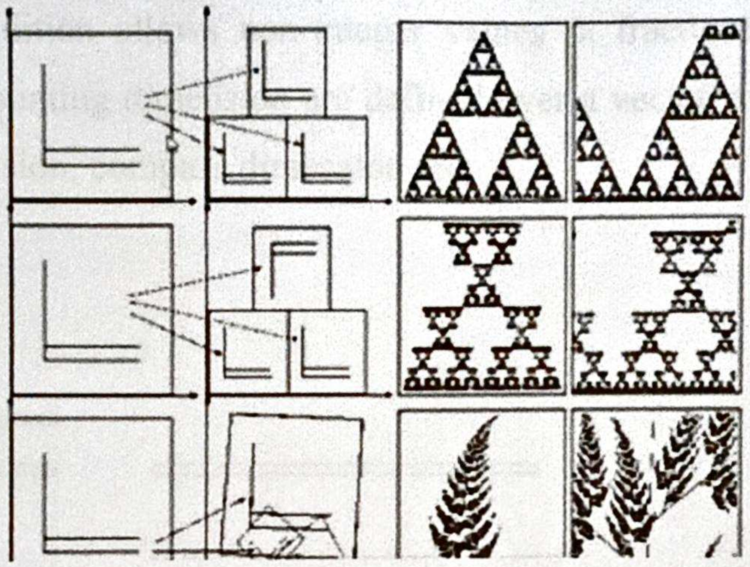
- All the copies seem to be converging to the same final Image.
- We call the final image the attractor of the copy machine.
- Because the copying machine reduces the input image, any initial image will be reduced to a point as we repeated run the machine.
- Thus, the initial image placed on the copying machine does not affect the Final Attractor.
- In fact, it is only the position and the orientation of the copies that determines what the final image will look like.
- We only describe these transformations.
- Different transformations lead to different Attractors.
- The transformations must be Contractive.
- In practice, Affine transformations are rich enough and yield interesting set of Attractors.

$$t_i \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} a_i & b_i \\ c_i & d_i \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} e_i \\ f_i \end{bmatrix}$$

Each Affine transformation can skew, stretch, scale and translate an input image.



Example by Affine Transformation



Examples by Affine Transformation

- Each Affine transformation t_i is defined by 6 numbers a_i, b_i, d_i, e_i and f_i.
- Storing images as collections of transformation leads to image.

➤ Dimensions

Dimension is a property of a mathematical object that refers to the extent it occupies the space in which it is embedded. There are many formal definitions of dimension, if the definition allows non-integer values (a fraction), it is a Fractal dimension. The box-counting dimension are defined over a vector space, but there is also the packing dimension, compass dimension etc.

Regular dimensions

D=1

Magnify by R =2

Get N= 2

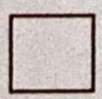
copies $N=R^1$

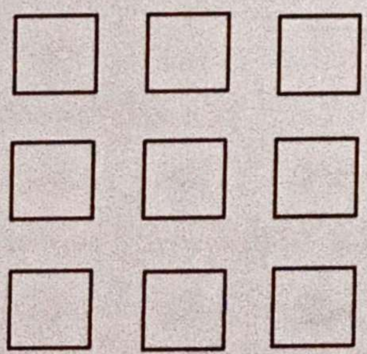
2D (D=2)

Magnify by R

= 3 Get N = 9

copies $N= 3^2 = R^2$





General rule for Dimensions

- A figure is in D dimensions
- If I magnify the length by R, then I would get R^D copies
- $N = R^D$

The dimension formula

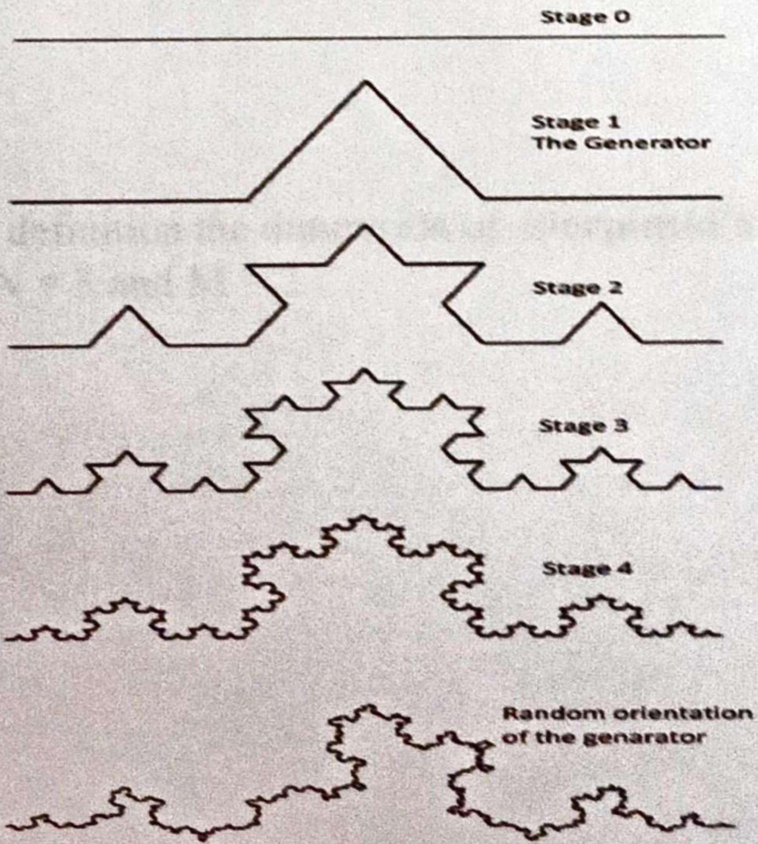
Define R as the magnifying factor,

Define N as the number of identical("self-duplicating") copies.Then the dimension of a figureis:

$$D = \frac{log(N)}{log(R)}$$

IT'S DIMENSION FOR SOME SHAPES

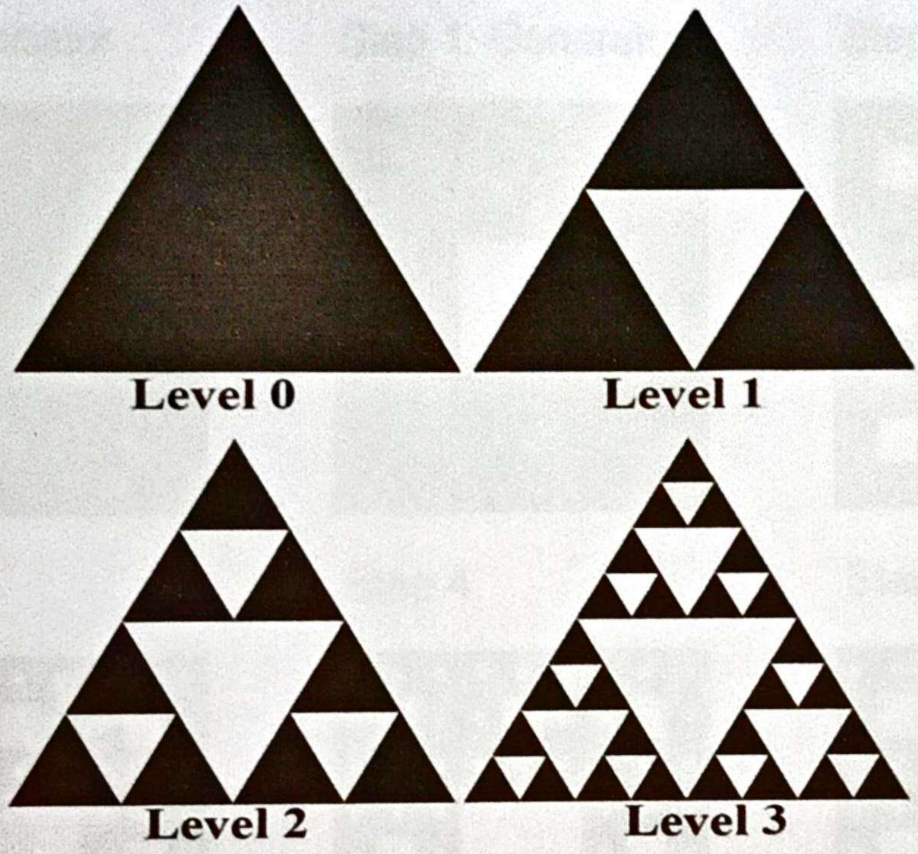
Koch Curve:



According to the definition the dimension of **Koch Curve** is,

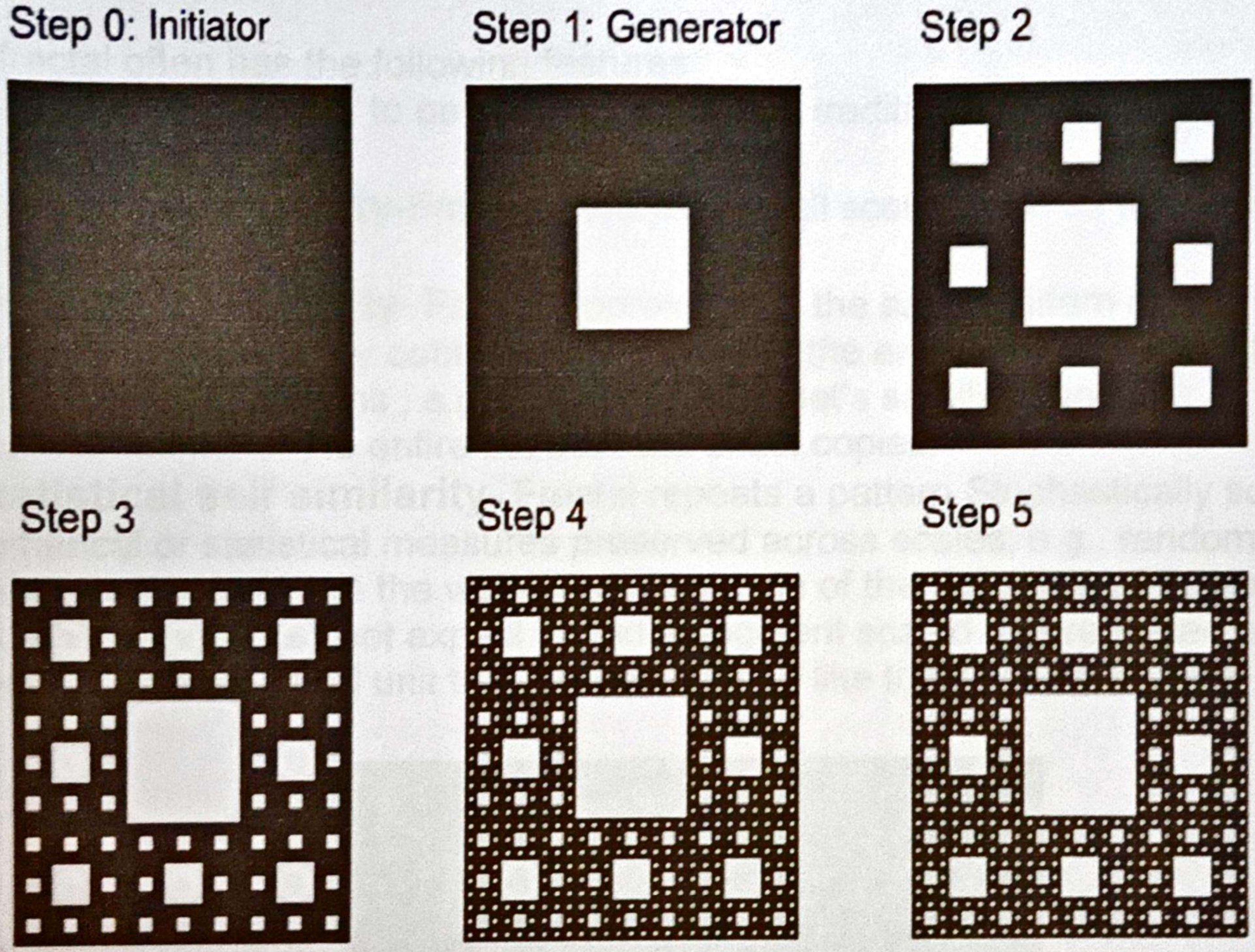
D = $\frac{log4}{log3}$ **= 1.26**, N = 4 and M = 3

Sierpinski's Triangle:



According to the definition the dimension of **Sierpinski's Triangle** is,
$D = \frac{log3}{log2} = 1.53$, N = 3 and M = 2

Sierpinski's Carpet:



According to the definition the dimension of **Sierpinski's Carpet** is,
$\mathbf{D} = \frac{\log 8}{\log 3} = \mathbf{1.89}$, N = 8 and M = 3

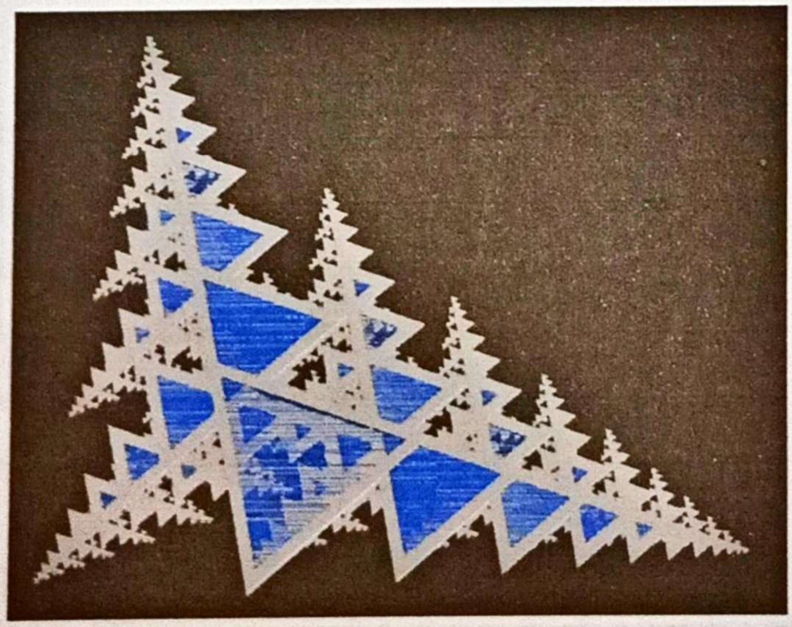
❖ CHARACTERISTICS OF FRACTAL

A fractal often has the following features:-
Fractal is too irregular to be easily described in traditional euclidean geometriclanguage.

Exact self similarity-Fractal is identical at all scales such as the Koch snowflake.

Quasi self similarity- Fractal approximates the same pattern at different scales. It may contain small copies of the entire fractal in distorted and degenerated forms ; e.g. the Mandelbrot Set's satellites are approximations of the entire set but note exact copies.

Statistical self similarity- Fractal repeats a pattern Stochastically so numerical or statistical measures preserved across scales; e.g., randomly generated fractals like the well-known example of the Coastline of Britain for which one would not expect to find a segment scaled and repeated as neatly asthe repeated unit that defines fractals like the Koch snowflake.



2×120 degrees recursive IFS

It has a Hausdroff dimension which is Greater than its topologicalDimension (although this requirement is not met by space filling Curves such as the Hilbert Curve). It has a simple and recursive definition.

❖ Fractal

A Fractal is a never- ending patters. Fractals are infinitely complex patterns that are self-similaracross different scales.

Fractals are considered to be important because they define images that are otherwise cannot bedefined by Euclidean geometry.

Self-Similar Objects and Fractal Dimensions

- Fractal dimension is a measure of how "complicated" a self-similar figure is.
- i.e., to measure the fractal Dimension, the picture must be self-similar.
- Self-similar regular shapes: Line, Plane, Cube
- Self-similar irregular shapes: cauliflower, Galaxy, Coast Line.

Scaling Factor

We can divide the object in N self-similar pieces then, how to get original object from size of theseN pieces?

Scaling Factor: If we want to get original object from any part of self-similar then wehave to scale the object using scaling factor.

For example:

If we divide the line in 2 equal pieces then

SF is 4,If we divide the plane in 4 equal

pieces then SF is 2

Mandelbrot defined a fractal to be a set with Hausdroff dimension strictly greater than its topological dimension. (The topological dimension of a set is always an integer and is 0 if it is totally disconnected. If each point has arbitrarily small neighbourhoods with boundary of dimension 0 and so on.)

The **Hausdroff dimension**, more specifically, is a further dimensional number associated with a given set, where the distances between all members of that set are defined. Such a set is termed a metric space. The dimension is drawn from the extended real numbers, R, as opposed to more intuitive notion of dimension, which is not associated to general metric spaces, and only takes values in the non-negative integers.

2.7 Fractal Dimension (Or Non-integer dimension)

Input:

- No of self-similar pieces
- Scaling Factor

Fractal Dimension=log (No. Self-Similar Object)/log ***(Scaling Factor)***

Dimension for the plane=2

Dimensions for the cube=3

While the Hausdroff dimension of a single point is zero, that of a line segment is 1,of a square is2,and of a cube is 3,for fractals such as this, the object can have a non-integer dimension.

Example of non-integer dimensions:

Division of certain sets into four parts. The parts are similar to the whole with ratios:

1. $\frac{1}{4}$ for line segment
2. $\frac{1}{2}$ for square
3. $\frac{1}{9}$ for middle third Cantor set
4. $\frac{1}{3}$ for von Koch curve

❖ Cantor Set

The Cantor ternary set is created by iteratively deleting the open middle third from a set of line segments.

Choose a particular portion say between two points

0 and 1.Let $F_0 = [0,1]$.

We first remove the open middle third segment $(\frac{1}{3}, \frac{2}{3})$ of [0,1]. Then define F_1 as

$F_1 = [0, \frac{1}{3}] \cup [\frac{2}{3}, 1]$

Next, we remove the open middle third of each of the two closed intervals in F_1 to obtain the set F_2

$F_2 = [0, \frac{1}{9}] \cup [\frac{2}{9}, \frac{3}{9}] \cup [\frac{6}{9}, \frac{7}{9}] \cup [\frac{8}{9}, 1]$

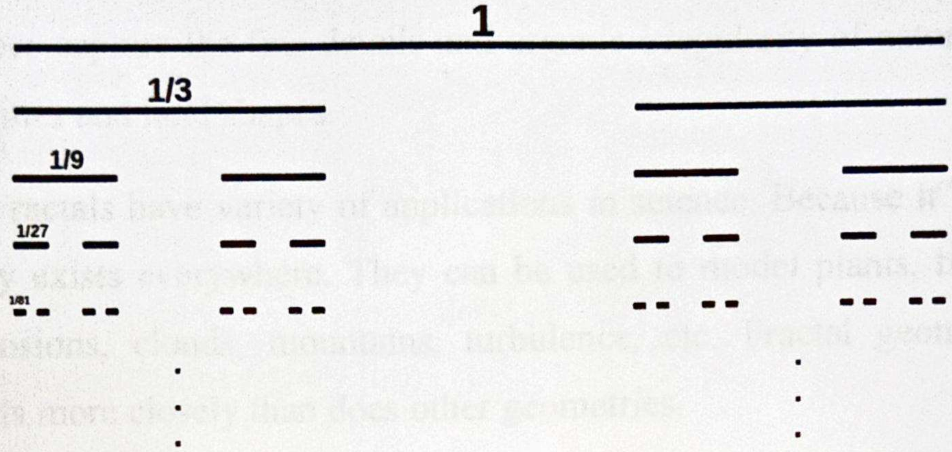
We see that F_2 is the union of $2^2 = 4$ closed intervals each of which is of the form $[k / 3^2, (k+1) / 3^2]$ each having length $1/3^2$.

Next, we remove the open middle thirds of each of the sets to get F_3. Then F_3 is the union of $2^3 = 8$closed intervals of length $1/3^3$.

Continuing this way, we obtain a sequence of closed sets F_n such that

- $F_1 \supset F_2 \supset F_3 \supset \ldots$
- F_n is the union of 2^n interval of the form $[k/ 3^n, (k+1) / 3^n]$ each of length $1/3^n$
- F_{n+1} is obtained from F_n by removing the open middle third of each of the intervals in F_n.

The set $F = \cap_{n} \in_{N} F_n$ is called the Cantor set. The Cantor ternary set contains all points in the interval[0,1] that are not deleted at any step in this infinite process.



Cantor Set

❖ Non – Integer Dimension

Using this fractal as an example, we can prove that the fractal dimensions is not an integer. Looking at the picture of the first step in building the Sierpiński Triangle, we can notice that if the linear dimension of the basis triangle is doubled, then the area of the whole fractal (black triangles) increasesby a factor of three.

Using the pattern given above, we can calculate a dimension for the Sierpiński Triangle.

$$D = \frac{\log 3}{\log 2} = 1.585$$

The result of this calculation proves the non-integer fractal dimension.

The number of triangles in the Sierpiński Triangle can be calculated with the formula:

$N = 3^k$

Where N is the number of triangles and k is the number of iterations.

APPLICATIONS OF FRACTAL GEOMETRY

The facts that fractals are abundant in nature and natural phenomena, is itself a testimony to the potential applicability and design efficiency of these shapes. Fraction shapes capture the fine details and organic irregularity of natural forms like clouds, cost lines and land shapes.

Fractals have variety of applications in science. Because it"s properly of self-similarity exists everywhere. They can be used to model plants, blood vessels, nerves, explosions, clouds, mountains, turbulence, etc. Fractal geometry models natural objects more closely than does other geometries.

Engineers have begun designing and constructing fractals in order to solve partial engineering problems. Fractals are also used in computer graphics are even in composing music.

Fractal geometry has permeated many areas of science. Such as astrophysics, biological science, and has become one of the most important techniques in computer graphics. Architects are using fractal geometries to create more impressive buildings. Digital artists use fractal geometries to create interesting art work which engages views at variable scales Game designers are always seeking to create natural organic environments. Which do not seem to be constructed and synthetic. Fractal geometry can be applied in such environments to include random elements which can enrich user experience.

Fractals are also used to generate natural patterns which can create effective camouflage and preclude artificial repetitive motifs. Fractals have been used by seismologists to understand earthquake phenomena and gain deeper understanding of the earth physical constitution. As well as the distribution pattern of earthquakes. Financial theorists have even applied fractals to understand and forecast stock market Patterns

❖ Fractals in Surface Physics

Fractals are used to describe the roughness of surface is characterized by a combination of two different fractals.

❖ Fractals in Computer Graphics

The biggest usage of fractals in everyday life is in computer science. Many images compression schemes use fractal algorithms to compress computer graphics files to less than a quarter of their original size.

Computer graphics artists uses many fractals forms to create text termed landscapes and other intricate models.

It"s possible to create all sorts up realistic "Fractal forgesies" images of natural scene, such a lunar landscape, mountain ranges and coastlines. We can see them it may special effects in Hollywood movies and also in television ads. The "genesis effect" in the films "star trek II". "The worth of khan" was created using fractal used to create the geography of a moon. and to draw the outline of dreaded "death star". But fractal signals can be used to model natural objectives. Allowing up to define mathematically our environment with a higher accuracy than ever before.

❖ Fractals in Biological Science

Biological scientists have traditionally model nature using Euclidean representations of natural object or series. They represented heartbeats as sine waves. Conifer trees as cones, animals habit a simple area, and cell membranes as curves or simple surfaces however scientists have come to recognize that many natural constructs are better characteristic using fractal geometry. Biological systems and processes are typically characterized by many levels of substructure with some general pattern repeated in an ever-decreasing cascade.

Scientists discovered that basic architecture of a chromosome in tree like: every chromosome consist of many "mini chromosomes" and therefore can be treated as fractal for a human chromosome, for in theory one can argue that everything existent on this world is fractal: -

- The branching of tracheal tubes
- The leaves in trees
- The veins in hand
- Water swirling and twisting out of a tap
- A puffy cumulus clouds
- Tiny oxygen molecules or the DNA molecules
- The stocks market

All of these are fractals from people ancient civilizations to the marker of star trek II: The worth of khan scientists. Mathematicians and artists alike have been captivated by fractal and have utilized them in their work.

❖ Fractals in Film Industry

One of the more trivial applications of fractals is their visual effect. Not only do fractals have a stunning aesthetic value that is, they are remarkably pleasing to the eye, but they also have a way to trick the mind. Fractals have been used commercially in the film industry. Fractal images are used as an alternative to costly elaborate sets to produce fantasy land scape.

❖ Fractals in Astrophysics

Nobody really how many stars actually glitter in our skies, but have you ever wondered how they were formed and ultimately found their home in the world? Astrophysicist believe that the key to this problem in the fractal nature of interstellar gas. Distributions are hierarchical, like smoke trails or billow cloud in the sky and the clouds in space. Giving them an irregular but repetitive pattern that would be impossible to describe without the help of fractal geometry.

❖ **Fractals in Image Compression**

Most use full application of fractals and Fractal geometry in image compression it is also one of the more controversial ideas. The basic concept behind of fractal image compression is to take an image and express it as an it rated system of functions the image can be quickly displayed, and at any magnification with infinite levels of fractal details. The largest problems behind its ideas is deriving the system of functions which describe an image.

❖ **Fractals in Fluid Mechanics**

The study of turbulence in flows is very adapted to fractals. Turbulent flows are chaotic and very difficult to model correctly. A fractal representation of them helps engineers and physicists to better understand complex flows. Flames can also be simulated. Porous media have a very complex geometry and are well represented by fractal. This is actually used in petroleum science.

❖ **Fractals in Medicine**

Biosensor interactions can be studied by using fractals

❖ **Fractals in Astronomy**

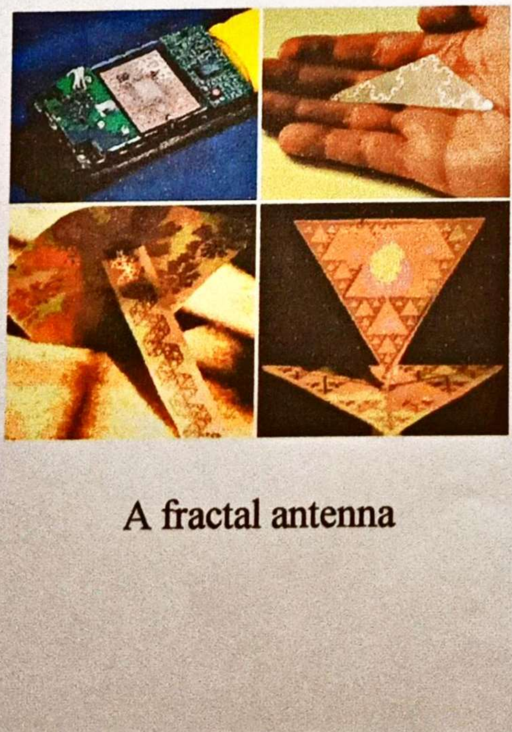
Fractals will may be revolutionize the way that the universe is seen. Cosmologists usually assume that matter is spread uniformity across space. But observations show that is not true. Astronomers agree with that assumptions on "small" scales. But most of them think that the universe is smooth at very large scales. However, a dissident group of scientists claims that the structure of the universe is fractal at all scales. If this new theory is proved to be correct, even the big bung models should be adapted. Some years ago, we proposed a new approach for the analysis of galaxy and cluster correlations abused on the concepts and methods of modern statistical physics. This led to the surprising result that galaxy correlations are fractal and not homogeneous up to the limits of the available catalogues. In the meantime, many more redshifts have been measured and we have extended our method also to the analysis of number counts and angular catalogues. The result is that galaxy structures are highly irregular and self-similar. The usual statistical method, based on the assumption of homogeneity, are therefore inconsistent for all the length scales probed until now. A new move general conceptual frame work is necessary to identity the real physical properties of these structures. But present cosmologists need more data about the matter distribution in the universe to prove (or not) that we are living in a fractal universe

❖ **Fractals in Telecommunications**

A new application is fractal- shaped antennae that reduce greatly the size and the weight of the antennae. Fractenna is the company which sells these antennae. The benefits depend on the fractal applied, frequency of interest, and so on. In general, the fractal parts produce „fractal loading" and makes the antenna smaller for given frequency of use. Practical shrinkage of 2-4 times is realizable for acceptable performance. Surprisingly high performance is attained.

❖ **Fractal Antenna**

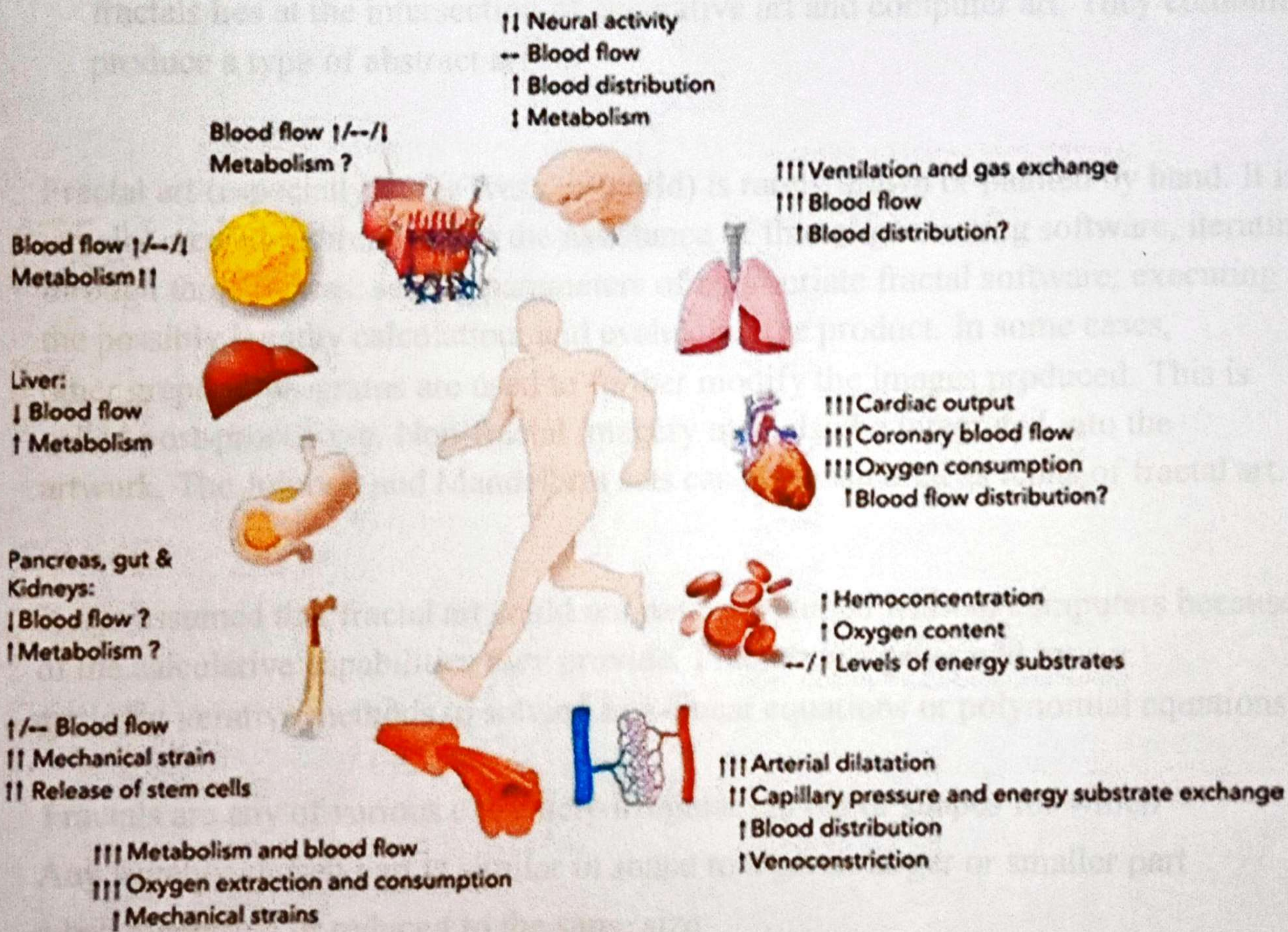
A fractal antenna is an antenna that uses a fractal, self-similar design to maximize the length, or increase the perimeter (on inside section or the outer structure), of material that can receive or transmit electromagnetic radiation within a given total surface area or volume. cohen use this concept of fractal antenna. And it is theoretically it is proved that fractal design in the only design which receives multiple signals.



A fractal antenna

Physiological Responses

Humans appear to be especially well-adapted to processing fractal patterns with D values between 1.3 and 1.5. When humans view fractal patterns with D values between 1.3 and 1.5, this tends to reduce physiological stress.



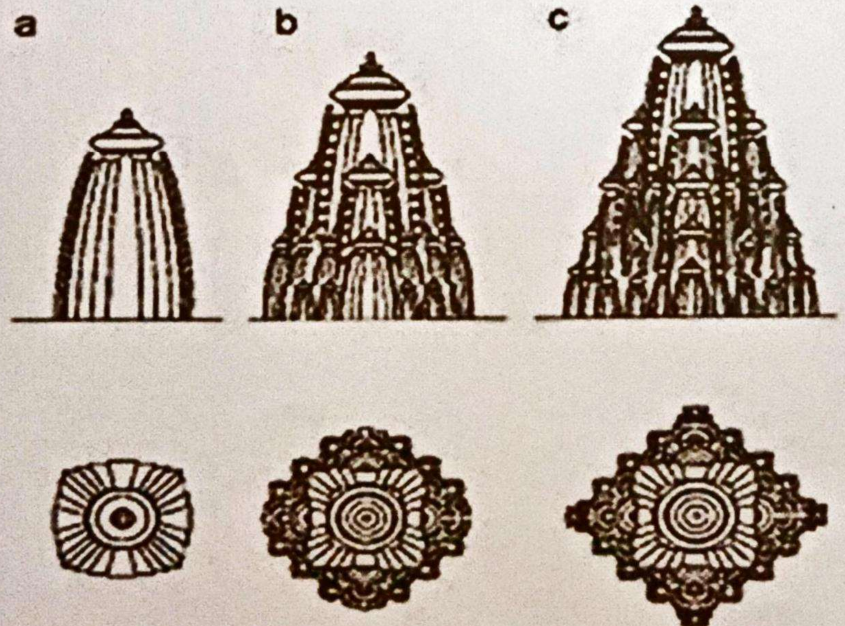
FRACTAL ART

Fractal art is a form of algorithmic art created by calculating fractal objects and representing the calculation results as still digital images, animations, and media. Fractal art developed from the mid-1980s onwards.It is a genre of computer art and digital art which are part of new media art. The mathematical beauty of fractals lies at the intersection of generative art and computer art. They combine to produce a type of abstract art.

Fractal art (especially in the western world) is rarely drawn or painted by hand. It is usually created indirectly with the assistance of fractal-generating software, iterating through three phases: setting parameters of appropriate fractal software; executing the possibly lengthy calculation; and evaluating the product. In some cases, other graphics programs are used to further modify the images produced. This is called post-processing. Non-fractal imagery may also be integrated into the artwork. The Julia set and Mandelbrot sets can be considered as icons of fractal art.

It was assumed that fractal art could not have developed without computers because of the calculative capabilities they provide. Fractals are generated by applying iterative methods to solving non-linear equations or polynomial equations.

Fractals are any of various extremely irregular curves or shapes for which Any suitably chosen part is similar in shape to a given larger or smaller part when magnified or reduced to the same size.



APPLICATIONS IN TECHNOLOGY

- Detecting 'life as we don't know it' by fractal analysis
- Enzymes (Michaelis-Menten kinetics)
- Generation of new music
- Signal and image compression
- Creation of digital photographic enlargements
- Fractal in soil mechanics
- Computer and video game design
- Computer Graphics
- Organic environments
- Procedural generation
- Fractography and fracture mechanics
- Small angle scattering theory of fractally rough systems

- Digital sundial
- Technical analysis of price series
- Fractals in networks
- Medicine
- Neuroscience
- Diagnostic Imaging
- Pathology
- Geology
- Geography
- Archaeology
- Soil mechanics
- Seismology
- Search and rescue
- Technical analysis

5. BIBLIOGRAPHY

1. Mandelbrot, Benoît B. (1983). The fractal geometry of nature Macmillan.
2. Falconer, Kenneth (2003). Fractal Geometry: Mathematical Foundations and Applications. John Wiley & Sons.
3. Fractal – Wikipedia
4. Fractal – antenna
5. Website : https://fractalfoundation.org

THE UNIVERSITY OF BURDWAN

DEPARTMENT OF MATHEMATICS

Project work submitted for the B.Sc Semester VI (Honours) Examination in Mathematics 2023

Under the Supervision of

Dr. Pramit Rej

By

Rama Kairi

University Roll No -200341200011

University Reg No -202001048584 of 2020-21

Signature of the student

Signature of the teacher

Signature of the H.O.D

ACKNOWLEDGEMENT

I am grateful to **Dr. Pramit Rej,** Assistant professor, Department of Mathematics and Sarat Centenary College affiliated to The University of Burdwan under whose supervision the project work has been carried out.I am grateful to all my faculties including the HoD of Mathematics, Sarat Centenary College for their constant support throughout the work . I am thankful to the authors of various reference books which have been consulted during the preparation of this project work . Finally I expressed my sincere gratitude to all staff members of the office, library of our college and infrastructure support provided by the department.

Date Signature of the student

CERTIFICATE

This is to certify that **RAMA KAIRI** has worked out the project work entitled ***Algebraic computation and plotting using Wolfram Mathematica*** under my supervision. In my opinion the work is worthy of consideration for partial fulfillment of his B.Sc. degree in Mathematics.

Date -

Signature of the teacher

Wolfram Mathematica

Content

Introduction

Wolfram Mathematica is a software system with built in libraries for several areas of technical computing . It is conceived by Stephen the beginning of modern technical computing.It allows machine learning statistics, symbolic computation, data manipulation, network annalysis, time seris analysis , NLP, optimization, plotting functions and various types of data ,implementstion of algorithms , creation of user interfrance ,and interfacing with programs written in other programming language.

Details

Developer	Wolfram Research
Initial release	June 23 , 1988
Stable release	February 10, 2023
Written in	Wolfram language
Platform	windows ,macos ,linux online service All platform support 64-bit Implementations
Available in	English,Chinease , Japanese
Type	Computer algebra , numerical Computation ,information visualization Statistics , user interface creation

Importance of Mathematica

When Mathematica version 1 was released ,the New York Times wrote that " the importance of the programe can not be overlooked" , and Business Week later ranked Mathematica among the ten most important new products of the year. Mathematica was also hailed in the technical community as a major intellectual and practical revolution . Atfirst , Mathematica's impact was felt mainly in the physical science , engineering and mathematics . But over the years Mathematica has become important in a remarkably wide range of fields .Mathematica is used today throughout the sciences physical ,biological ,social and other and counts many of the world's foremost scientists among its enthusiastic supporters .It has played a crucial role in many important discoveries and has been the basis of thousands of technical papers .

History of Mathematica

For more than 50 years Mathematica has been at the forefront of assessing the effectiveness o policies and programs to improve public well-being .

The improvement of Mathematica are as follows :

VERSION	RELEASE DATE
1	June 1988
2	January 1991
3	September 1996
4	May 1999
5	June 2003
6	May 2007
7	November 2008
8	November 2010
9	November 2012
10	July 2014
11	August 2016

12 April 2019
13 December 2021

Now february 10 ,2023 the stable version was released .This is the latest version of Wolfram Mathematica

Uses of Mathematica

Mathematica can be used wherever & whenever calculations and computations are needed.It can be used to solve very simple addition problems or to solve complex equations and advanced physics problems.The visualisations & graphical capabilities if Mathematica make it very useful for plotting all kinds of data & functions.The uses of Mathematica are as follows :

1)Differential calculus:

We can calculate limit, derivatives, Maximum & minimum values, power series using Mathematica.

2) Integral Calculas:

We can easily calculate anti-derivative, definite integrals, Riemann sums using this.

3) Multivariate Calculas :

Partial derivatives, maximum minimum values, the total differential, multiple integrals are also calculated by Mathematica.

4)Ordinary Differential Equations:

Analytical solutions, numerical L transformation are calculated by Mathematica.

5)Two & Three Dimensional Graphics:

We can use this for plotting functions of a single variable and two variables. we also use this for two and three dimensional plotting.

6)**Linear Algebra:**

We can calculate vectors & matrices, we can do matrix operation ,matrix manipulation, test orthogonality and diagonalization, and also find eigen values & eigen vectors.

Application of Mathematica in other fields

Mathematica is used almost all the field, like as follows :

- Chemical engineering
- Electrical engineering
- Software engineering
- Web development
- Business analysis
- Operation research
- Finance
- Aerospace
- Defence
- Statistics
- Mathematics
- BioScience
- Chemistry
- Physics
- Astronomy
- Bioinformatics
- Education etc.

Algebraic computation

```
Sqrt[2] // N
```

1.41421

```
Exp[2 + 9 I] // N
```

-6.73239 + 3.04517 i

```
Solve [x^3 - 2 * x + 1 == 0, x]
```

$\{\{x \to 1\}, \{x \to \frac{1}{2}(-1 - \sqrt{5})\}, \{x \to \frac{1}{2}(-1 + \sqrt{5})\}\}$

```
Prime [1000]
```

7919

```
Quotient [62173467, 9542]
```

6515

```
N[Pi]
```

3.14159

```
Solve[ArcSin[x] == 0, x]
```

{{x → 0}}

```
Solve [(x^2 + 2 x) * (x^2 - 2 x) == 0, x]
```

{{x → -2}, {x → 0}, {x → 0}, {x → 2}}

```
Solve[{x - y == 0, x^2 + y^2 == 1}, {x, y}]
```

$\{\{x \to -\frac{1}{\sqrt{2}}, y \to -\frac{1}{\sqrt{2}}\}, \{x \to \frac{1}{\sqrt{2}}, y \to \frac{1}{\sqrt{2}}\}\}$

```
Expand[(1 + x + 3 * y) ^4]
```

$1 + 4x + 6x^2 + 4x^3 + x^4 + 12y + 36xy + 36x^2y + 12x^3y + 54y^2 + 108xy^2 + 54x^2y^2 + 108y^3 + 108xy^3 + 81y^4$

```
Factor[x^10 - 1]
```

$(-1 + x)(1 + x)(1 - x + x^2 - x^3 + x^4)(1 + x + x^2 + x^3 + x^4)$

```
Integrate [Exp[-x^2], {x, 0, Infinity}]
```

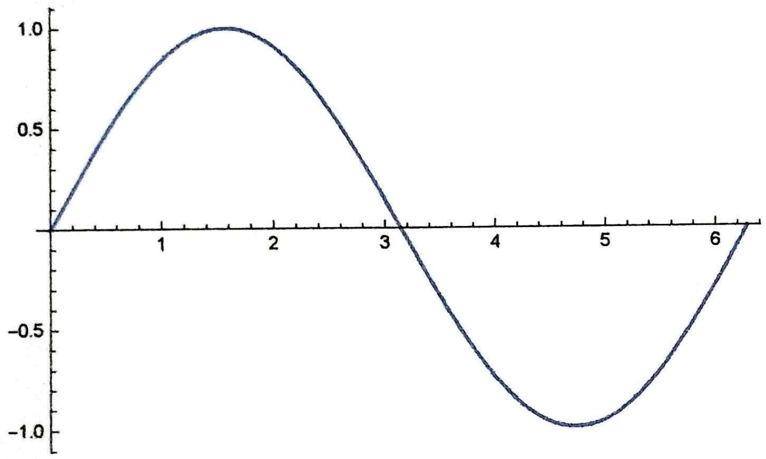
$\frac{\sqrt{\pi}}{2}$

PLOTTING OF 2 D & 3 D FIGURE USING WOLFRAM MATHEMATICA

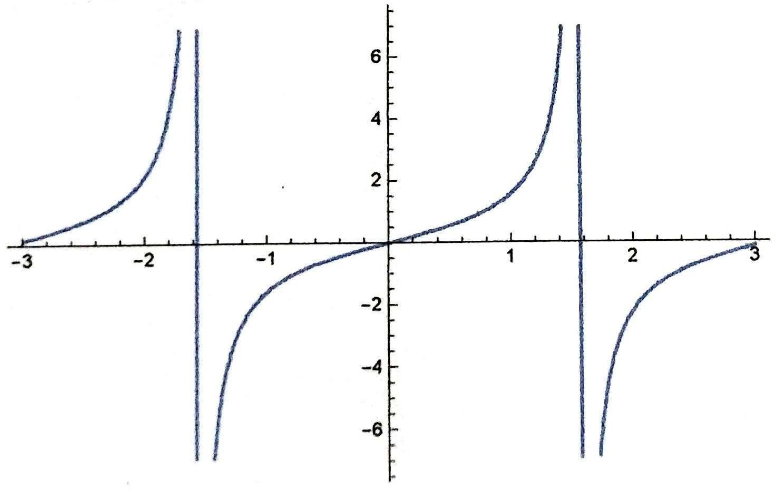
The Wolfram Mathematica has many way to plot function and data.It automates many details of plotting such as sample rate , aesthetic choice , focusing on the region . Plot is a simple two dimentional plotting function in Mathematica .Plot takes two arguments when it is called and these and these arguments contain numerous parts.

Here we discuss this with some folloing example

```
Plot[Sin[x], {x, 0, 2 * Pi}]
```

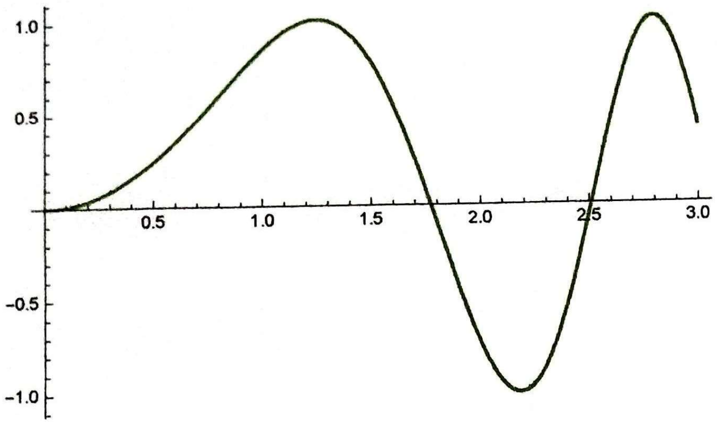


```
Plot[Tan[x], {x, -3, 3}]
```

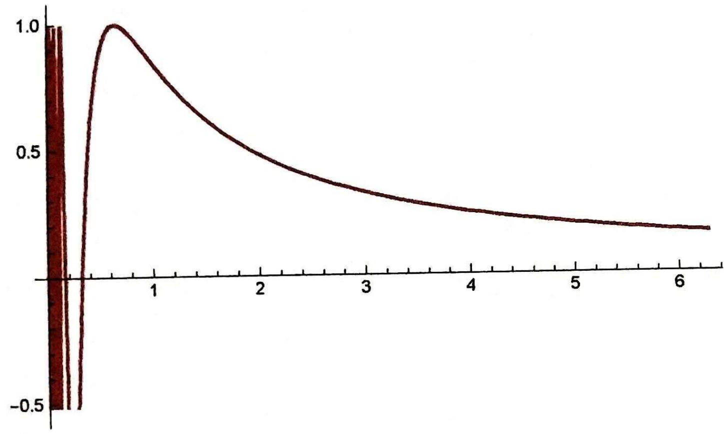


→

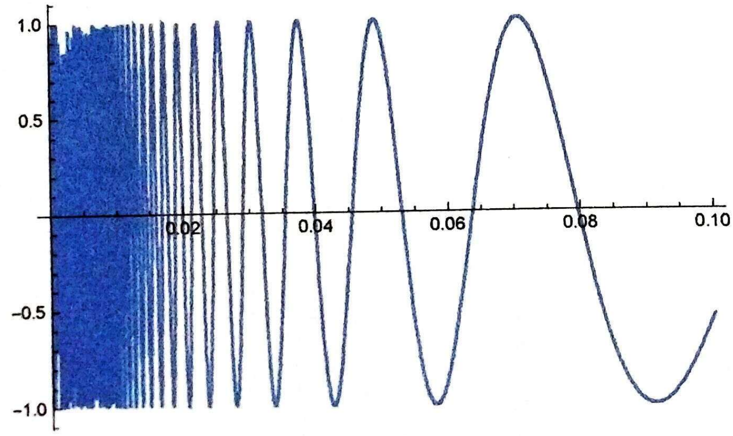
```
Plot[Sin[x^2], {x, 0, 3}, PlotStyle → RGBColor[0., 0.56, 0.06]]
```



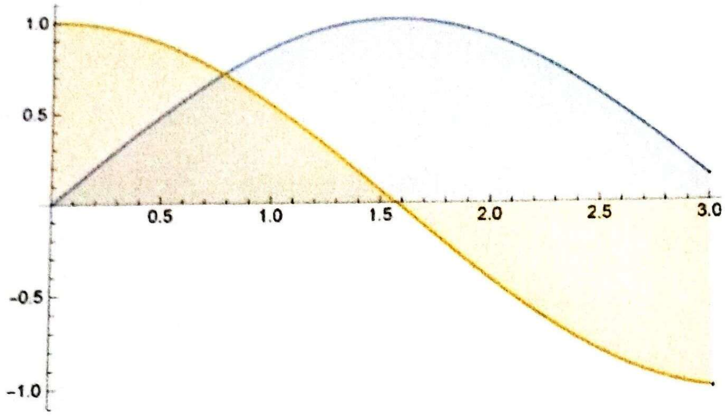

```
Plot[Sin[1/x], {x, 0, 2 π}, PlotStyle → RGBColor[0.72, 0.09, 0.]]
```



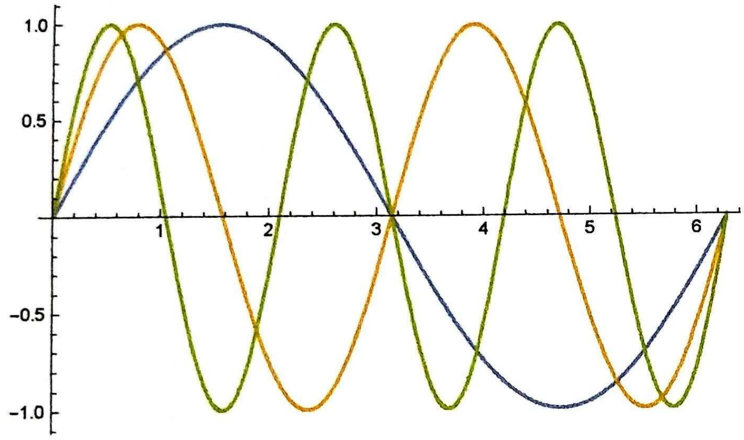

```
Plot[Sin[1/x], {x, 0, .1}]
```



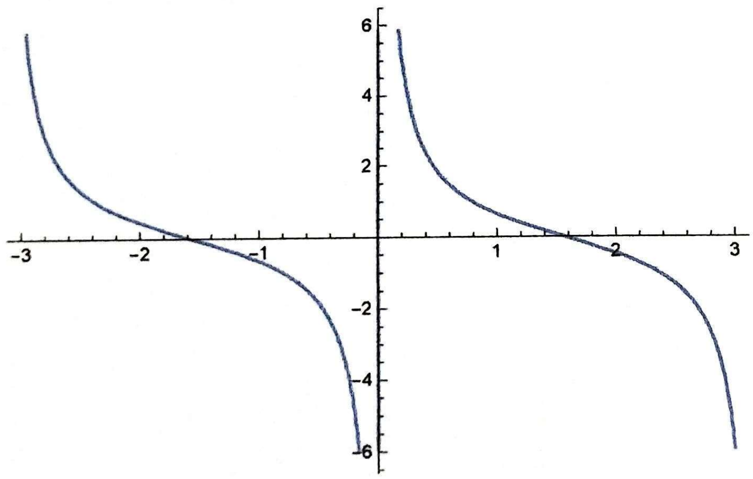
```
Plot[{Sin[x], Cos[x]}, {x, 0, 3}, Filling → Automatic]
```



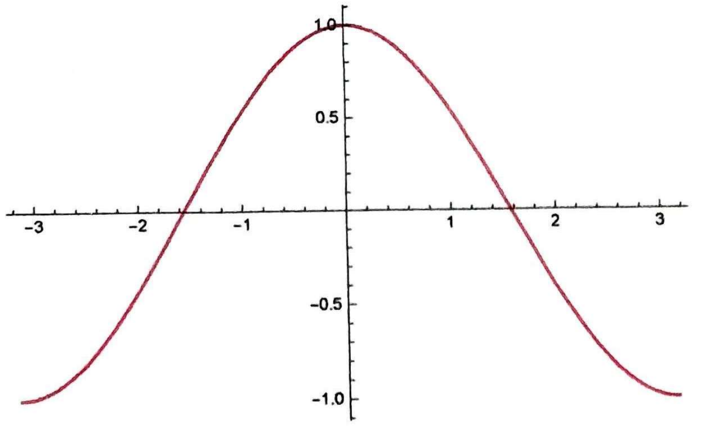

```
Plot[{Sin[x], Sin[2 x], Sin[3 x]}, {x, 0, 2 * Pi}]
```



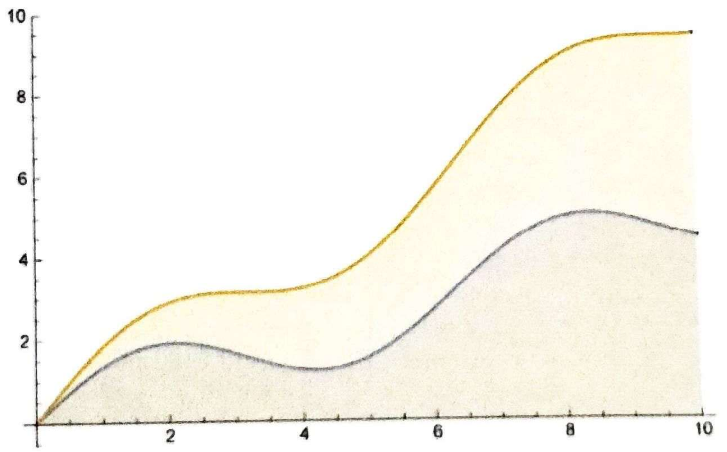

```
Plot [Cot[x], {x, -3, 3}]
```



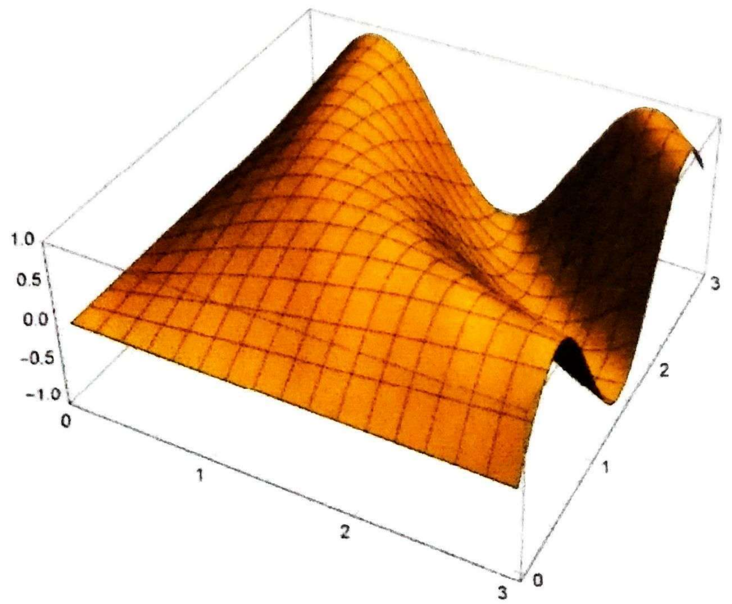
```
Plot[Cos[x], {x, -π, π}, PlotStyle → RGBColor[1., 0.11, 0.33]]
```



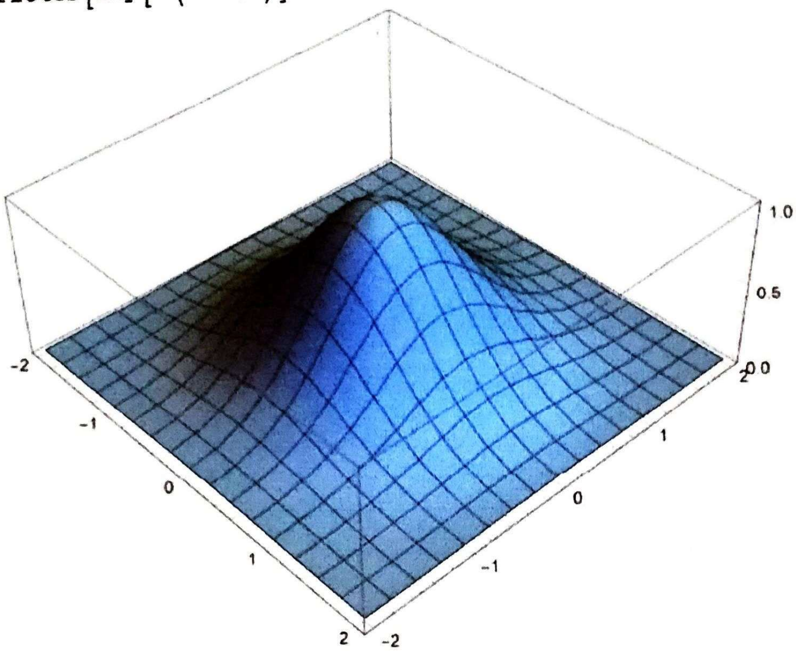

```
Plot[{Sin[x] + x/2, Sin[x] + x}, {x, 0, 10}, Filling → Automatic]
```



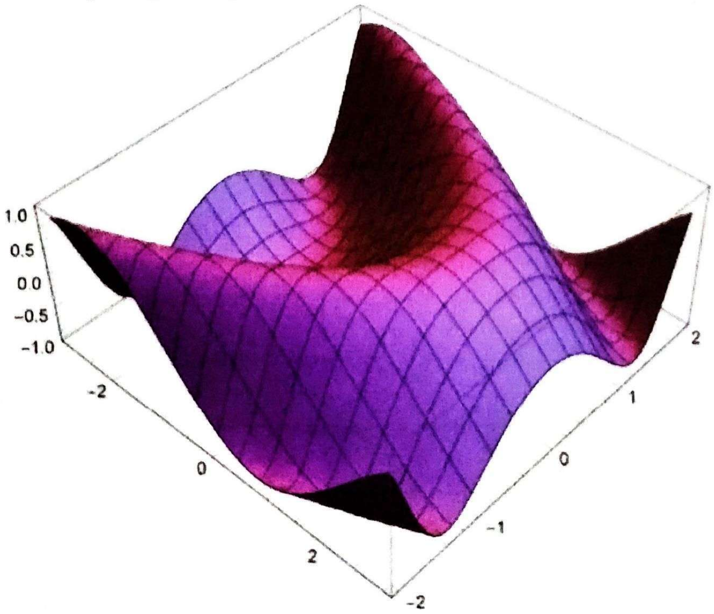

```
Plot3D[Sin[x * y], {x, 0, 3}, {y, 0, 3}]
```



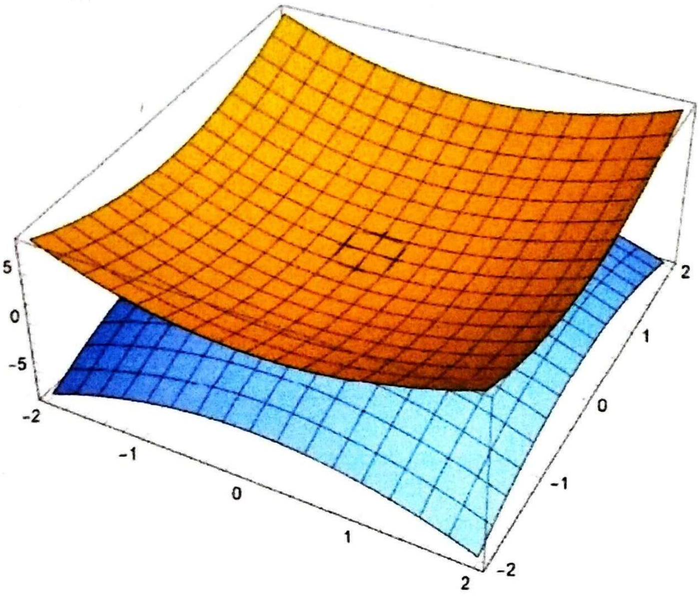
```
Plot3D[Exp[-(x^2 + y^2)], {x, -2, 2}, {y, -2, 2}, PlotStyle → RGBColor[0.44, 0.69, 1.]]
```




```
Plot3D[Sin[x + y^2], {x, -3, 3}, {y, -2, 2}, PlotStyle → RGBColor[0.75, 0.44, 1.]]
```



```
Plot3D[{x^2 + y^2, -x^2 - y^2}, {x, -2, 2}, {y, -2, 2}]
```



Inverse of a 2×2 matrix:

Inverse[{{1.4, 2}, {3, −6.7}}]

{{0.435631, 0.130039}, {0.195059, −0.0910273}}

Enter the matrix in a grid:

$$\textbf{Inverse}\left[\begin{pmatrix} 1 & 2 & 3 \\ 4 & 2 & 2 \\ 5 & 1 & 7 \end{pmatrix}\right]$$

$$\left\{\left\{-\frac{2}{7}, \frac{11}{42}, \frac{1}{21}\right\}, \left\{\frac{3}{7}, \frac{4}{21}, -\frac{5}{21}\right\}, \left\{\frac{1}{7}, -\frac{3}{14}, \frac{1}{7}\right\}\right\}$$

Inverse of a symbolic matrix:

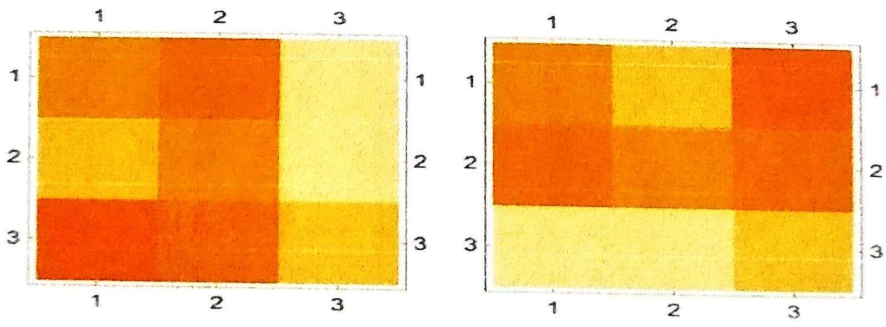
Inverse[{{u, v}, {v, u}}]

$$\left\{\left\{\frac{u}{u^2-v^2}, -\frac{v}{u^2-v^2}\right\}, \left\{-\frac{v}{u^2-v^2}, \frac{u}{u^2-v^2}\right\}\right\}$$

Transpose a 3×3 numerical matrix:

{{3, 2, 5}, {4, 3, 4}, {1, 1, 2}}

Visualize the transposition operation:



Transpose a 2×3 symbolic matrix:

$$\begin{pmatrix} a & x \\ b & y \\ c & z \end{pmatrix}$$

Eigenvalues of an exact matrix:

```
Eigenvalues[{{1, 2, 3}, {4, 5, 6}, {7, 8, 9}}]
```

$$\left\{\frac{3}{2}\left(5+\sqrt{33}\right), \frac{3}{2}\left(5-\sqrt{33}\right), 0\right\}$$

Symbolic eigenvalues:

```
Eigenvalues[{{a, b}, {c, d}}]
```

$$\left\{\frac{1}{2}\left(a+d-\sqrt{a^2+4bc-2ad+d^2}\right), \frac{1}{2}\left(a+d+\sqrt{a^2+4bc-2ad+d^2}\right)\right\}$$

Find the determinant of a symbolic matrix:

$$\text{Det}\left[\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}\right]$$

$$-a_{1,2}\, a_{2,1} + a_{1,1}\, a_{2,2}$$

The determinant of an exact matrix:

```
Det[{{1, 2, 3}, {4, 5, 6}, {7, 8, 9}}]
```

0

Derivative of a defined function:

```
1 » f[x_] := Sin[x] + x^2
```

```
2 » f'[x]
```

```
2 › 2 x + Cos[x]
```

This is equivalent to $\frac{\partial f(x)}{\partial x}$:

```
3 » D[f[x], x]
```

```
3 › 2 x + Cos[x]
```

Derivative at a particular value:

```
4 » f'[0.5]
```

```
4 › 1.87758
```

This is equivalent to $\frac{\partial f(x)}{\partial x} \Big|_{x=0.5}$:

```
5 » D[f[x], x] /. x → 0.5
```

```
5 › 1.87758
```

The second derivative:

```
6 » f''[x]
```

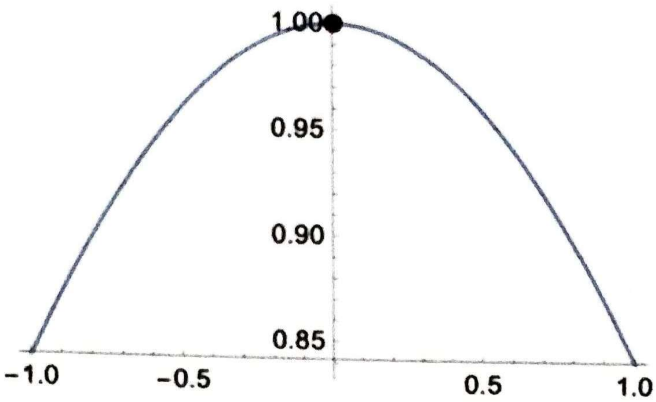
```
6 › 2 - Sin[x]
```

Limit at a point of discontinuity:

```
Limit[Sin[x]/x, x -> 0]
```

```
1
```

```
Plot[Sin[x]/x, {x, -1, 1}, Epilog → {PointSize[Large], Point[{0, 1}]}]
```

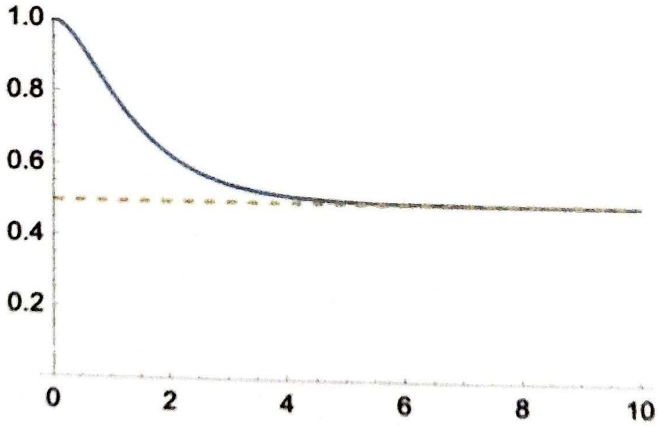


Limit at infinity:

$$\text{Limit}\left[\frac{1 + \text{Sinh}[x]}{\text{Exp}[x]}, x \to \infty\right]$$

$$\frac{1}{2}$$

$$\text{Plot}\left[\left\{\frac{1 + \text{Sinh}[x]}{\text{Exp}[x]}, \frac{1}{2}\right\}, \{x, 0, 10\},\right.$$
$$\left.\text{PlotStyle} \to \{\text{Automatic, Dashed}\}, \text{PlotRange} \to \{0, 1\}\right]$$



Advantages of Mathematica

- The coding of Mathematica is a simple one .
- It has good hardware options.
- Very powerful language
- Name convention are great .
- Many paradigms OOP/List/pattern matching /logic programming.
- Very strong symbolic computation
- Ability of compile mode of some code
- Very good visualisation

Disadvantages of Mathematica

- Its cost is high.
- Its GUI is not so good
- Cost for extensions
- Long learning curve
- Slow interpreter
- It is hard to write modular code
- OOP is possible but very unusual.

Conclusion:

Mathematica has attracted wide attention in the world.The diversity of Mathematica's user base is striking. Ever since Mathematica was first released, it's user base has grown steadily and by now total number of users is above a million . Mathematica is used almost all the field Engineering, Statistics, Mathematics, Finance Computational field . Mathematica is also heavily used in education.It has become an important tool for both technical & non technical field.

Bibliography

1) www.wekipedia.com
2) www.wolfram.com
3) Writings.stephenwolfram.com
4) The Mathematica Book - Stephen Wolfram.
5) Mathematica (Schaum's outlines) - Eugene Don, PH.D

DISCUSSION ON

GAME THEORY AND ITS APPLICATION

The University Of Burdwan

Project work submitted for the B.SC. Semester-VI (Honours) Examination in Mathematics 2023

Under the supervision of:

SHAMPA DUTTA

By:

SOUMYA PAL

ROLL NO: 200341200022

Registration no: 202001048596 of 2020-2021

Department Of Mathematics

--- --- ---

Signature of The Student Signature of The Teacher Signature of The H.O.D

ACKNOWLEDGEMENT

I am grateful to Mrs.Shampa Dutta,State Aided College Teacher, Department of Mathematics, Sarat Centenary College, The University of Burdwan under whose supervision the project work have been carried out. I am grateful to all the teachers including the HOD of Mathematics, Sarat Centenary College for their constant support throughout the work. I am thankful to the authors of various reference books which have been consulted during the preparation of this project work. Finally I express my sincere gratitude to all staff members of the office, library of our college and infrastructural support provided by the department.

Date:-

Name of The Student

CERTIFICATE

This is to certify that Soumya pal has worked out the project work entitled "Game theory and its Application" under my supervision. In my opinion the work is worthy of consideration for partial fulfilment of his B.Sc. degree in Mathematics.

Date:-

Signature Of the Teacher

CONTENTS

GAME THEORY

INTRODUCTION

WHAT IS GAME THEORY?

The game theory is said to be the science of strategies which comes under the probability distribution. It determines logical as well as mathematical actions that should be taken by the players in order to obtain the best positive outcomes for themselves in the game. The games studied in the game theory may range from chess to tennis and from child-rearing to takes over. But there is one thing common that such an array of games in independent, out-comes for each players depends upon the strategies of all.

In other words, games theory deals with mathematical models of co operation and conflict between rational decision marks game theory can be define as the study of decision–making in which the players must make strategies affecting the interests of other players.

USEFUL TERMS IN GAME THEORY

Any time we have a situation with two or more players that involve known payouts or quantifiable consequences, we can use game theory to help determine the most likely outcomes. Let's start by defining a few terms commonly used in the study of game theory:

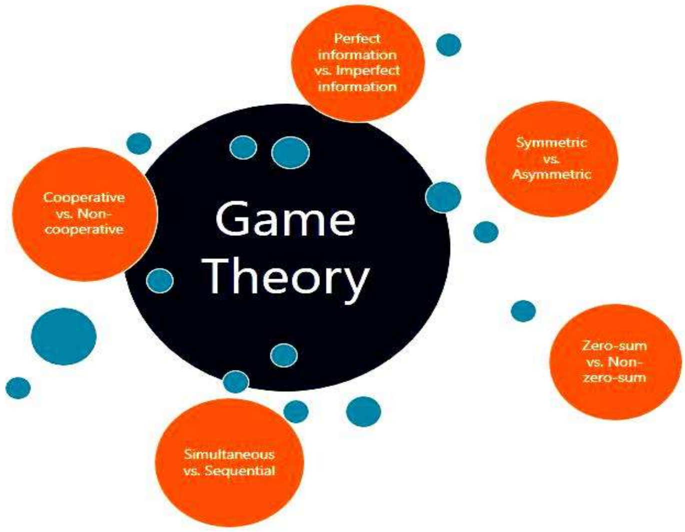
- **Game**: A competitive situation will be called a game.
- **Players**: A strategic decision-maker within the context of the game.
- **Strategy**: A complete plan of action a player will take given the set of circumstances that might arise within the game.
  A strategy may be two types:-
  i)Pure Strategy
  ii)Mixed strategy
- **Optimal Strategy**: The course of action which maximizes the profit of a player or minimizes his loss is called an optimal strategy.
- **Payoff**: The outcome of playing the game is called payoff.

- **Payoff Matrix**: It is a table showing the outcome or payoff of different strategies of the game.
- **Equilibrium**: The point in a game where both players have made their decisions and an outcome is reached.
- **Value of the game**: It refers to the expected outcomes par play. When players follow their optimal strategy. It is generally denoted by V.

LITERATURE REVIEW

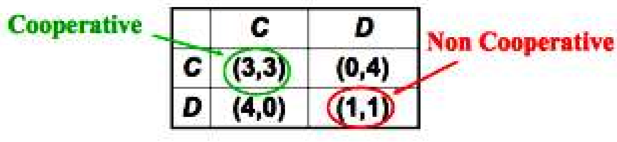
Game theoretical concepts have been utilized to analyze problems for millennia, long before game theory was a formally-defined field. One interesting example is that the Talmud, the Jewish holy book that provides the basis for Jewish law, prescribes solutions for allocation of disputed resources that confounded scholars until the 1980s when mathematicians Robert Aumann and Michael Maschler solved the problem using the tools of modern game theory. As it turns out, the solution given by the Talmud is to split the disputed amount equally . Another example is when James Madison considered the effects of different taxation systems with game theoretical concepts. The list goes on, as conflict resolution and strategic decision-making have been important issues throughout all of human history. The first work that brought about game theory as a formal field of mathematics was Hungarian mathematician John von Neumann's paper The Theory of Games in 1928. This paper had three major results. The first was reducing a game to the cases where each player knows either everything or nothing about the other player's previous moves. He also proved the mini-max theorem for two person zero-sum games, and he analyzed three person zero-sum games. Economist Oskar Morgenstern connected with von Neumann in 1938, and the two then worked together on Theory of Games and Economic Behavior, published in 1944. This work was huge in the development of game theory. They expanded on von Neumann's previous work with an in-depth analysis of situations where players have only partial knowledge of other players' previous decisions, whereas The Theory of Games made the assumption that players knew either everything or nothing about previous decisions. They also expanded the definition of payoffs; previously payoffs were generally considered to be only monetary, but von Neumann and Morgenstern developed the theory of utility, which is still used today in many fields such as economics. Since von Neumann and Morgenstern laid the foundation for game theory, it has 15 been added to by many mathematicians, such as John Nash in the 1950s. However, the main development over the following decades was increasingly widespread application to many fields. While certainly important in the field of economics, the use of game theory has expanded to extensive use in biology, and it is also very important to the development of military strategy. Interestingly, the five game theorists who have won the Nobel Prize for economics also worked as advisors to the Pentagon over the courses of their careers. Game theory has also been applied in fields such as computer science and moral philosophy.

TYPES OF GAME



1) Non-cooperative versus Cooperative Games

There are two branches of the game theory, viz. cooperative and noncooperative game theory. Under the cooperative game theory, groups or sub-sets of the players make a binding agreement to reach an outcome that is best for the group as a whole and is shared equally among the members. In contrast to this, under non-cooperative game theory, players cannot write binding contract. Players are guided by self-interest, each player acts as an individual who is normally assumed to maximize his own utility without caring about the effects of his choice on other players in the game. The outcome of the game, however, is jointly determined by the strategies chosen by all players in the game. As a result, each player's welfare depends, in part, on the decisions of other players in the game. An example of cooperative game is two firms negotiating a joint investment to develop a new technology. An example of non-cooperative game is two competing firms taking into account each other’s behavior when setting their prices independently. Self-interested behavior does not always lead to an outcome that is best for the players as a group. This we will come across when we discuss different illustrations of the games. Non-cooperative game theory is more widely used by economist; nevertheless, cooperative game theory has been used to model bargaining games and political processes.

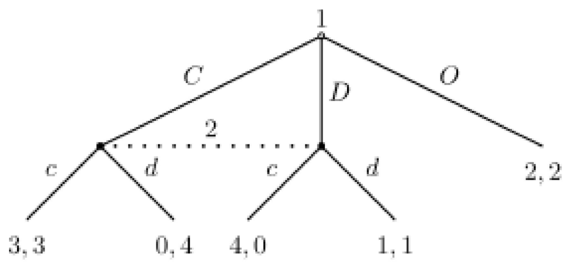


2)Perfect vs Imperfect Information

Games of imperfect information have information hidden from players during the game. And, although games of perfect information have all information shown during a game, the need for strategy in the game doesn't necessarily differ between the two.

Perfect information games such as chess, backgammon, and go require a decent amount of thought and strategy to play. Players have to process what they see on the board and determine what their opponent is likely to do while working towards the ultimate goal of winning. On the other hand, perfect information games such as candy land, mousetrap, and tic-tac-toe don't need practically any strategy to play. Players simply have to roll a die or pick up a card and move their piece to a set space. Even a game like tic-tac-toe, where there is arguably a strategy involved, has practically no real thought put into the game.

Imperfect information games such as poker, 20 questions, and rummy require thought and strategy to play. Players have to take into account the information that they have been given already to try to figure out how they should act next in order to win. Where imperfect information games such as guess who, apples to apples, and go-fish don't really require much strategy to play. Although there is arguably some strategy to these games, the players don't have to do much other than ask a question or seeing a card and getting rid of some of your hand as a response.



A Game of imperfect information the dotted line represent ignorance or the part of player2 from called an information set

3)Simultaneous-move versus Sequential-move Games

The order of moves is significant in the game theory. Players in a game may move simultaneously or sequentially which in turn results in different outcomes of the game. A simultaneous-move game is a game in which neither player knows the other's action when moving, that is, players take their action simultaneously without knowing the action that have been chosen by the other player(s). For instance, in Cournot model of oligopoly, each firm decides its profit maximizing levels of output simultaneously. In contrast, in sequential-move games, the order of moves comes into picture. In this case, one player moves first which is then observed by his opponent. The player(s) who moves afterwards gets to observe and learn information about the course of the game up to that point, including what actions other players have chosen. These observations can then be used by that player to decide his (her) own optimal strategies than simply choosing an action. This way, strategies of the players depend on what the other player(s) before have done already.

		Player II		
		rock	paper	scissors
Player I	rock	(0, 0)	(-1, 1)	(1, -1)
	paper	(1, -1)	(0,0)	(-1,-1)
	scissors	(-1, 1)	(1, -1)	(0, 0)

4) Zero-sum versus Non-Zero Sum Games

A zero-sum game is the one in which the gain of one player comes at the expense of the other player and is exactly equal to the loss of the other player. In other words, the sum of the payoffs of the two players always adds to zero. An economic application can be the transaction between a buyer and a seller at the cost price. A non-zero sum game is when gain or loss does not come at the expense of the other player. An example of this might arise if increased advertisement leads to higher profits for both the firms.

	A	B
A	–1, 1	3, –3
B	0, 0	–2, 2

A zero-sum game

		Husband	
		Boxing Match	Ballet
Wife	Boxing Match	2, 3	1, 1
	Ballet	1, 1	3, 2

The Battle of the Sexes is a simple example of a typical non-zero-sum game

5)Symmetric vs Asymmetric Games

The main feature of symmetric game is that all the players in these games adopt the same strategies. This is usually applicable in the short duration games because in the long duration games the players get a more number of options. In symmetric games the decisions do not depend upon the players, in fact, it is best on based on the types of strategies used. The decisions in the symmetric games remain the same even if the players are interchanged the game. The prisoner's dilemma is the prominent example of the symmetric games. This example is discussed further in this article. In the case of asymmetric games, the decisions depend upon the player. In these games, if a particular strategy provides benefit to one players, other players will also get equal benefits. A prominent example of asymmetric games is the decision of the company to enter the new market.

		Player 2	
		C	D
Player 1	C	14,14	7,17
	D	17,7	10,10

(i) Symmetric payoff matrix

		Player 2	
		C	D
Player 1	C	44,36	8,44
	D	52,0	32,28

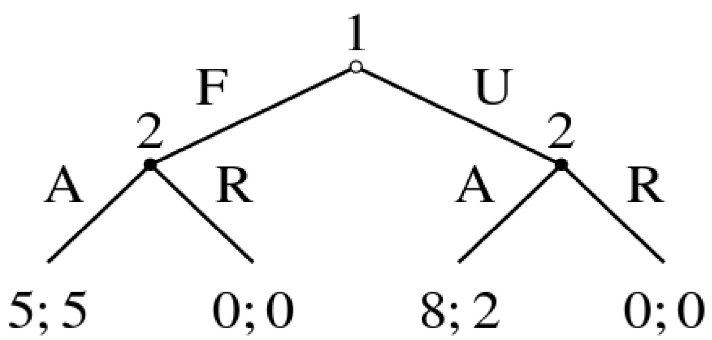
(ii) Asymmetric payoff matrix

REPRESENTATION OF GAMES

The games studied in game theory are well-defined mathematical objects. The games studied in game theory are well-defined mathematical objects.

Extensive form:-

The extensive form can be used to formalize games with a time sequencing of moves. Extensive form games can be visualized using game trees (as pictured here). Here each vertex (or node) represents a point of choice for a player. The player is specified by a number listed by the vertex. The lines out of the vertex represent a possible action for that player. The payoffs are specified at the bottom of the tree.



The game pictured consists of two players. The way this particular game is structured (i.e., with sequential decision making and perfect information), *Player 1* "moves" first by choosing either *F* or *U* (fair or unfair). Next in the sequence, *Player 2*, who has now observed *Player 1*'s move, can choose to play either *A* or *R*. Once *Player 2* has made their choice, the game is considered finished and each player gets their respective payoff, represented in the image as two numbers, where the first number represents Player 1's payoff, and the second number represents Player 2's payoff. Suppose that *Player 1* chooses *U* and then *Player 2* chooses *A*: *Player 1* then gets a payoff of "eight" (which in real-world terms can be interpreted in many ways, the simplest of which is in terms of money but could mean things such as eight days of vacation or eight countries conquered or even eight more opportunities to play the same game against other players) and *Player 2* gets a payoff of "two".

Normal Form:-

	Player 2 chooses *Left*	Player 2 chooses *Right*
Player 1 chooses *Up*	4, 3	−1, −1
Player 1 chooses *Down*	0, 0	3, 4

Normal form or payoff matrix of a 2-player, 2-strategy game

The normal game is usually represented by a matrix which shows the players, strategies, and payoffs (see the example to the right). More generally it can be represented by any function that associates a payoff for each player with every possible combination of actions. In the accompanying example there are two players; one chooses the row and the other chooses the column. Each player has two strategies, which are specified by the number of rows and the number of columns. The payoffs are provided in the interior. The first number is the payoff received by the row player (Player 1 in our example); the second is the payoff for the column player (Player 2 in our example). Suppose that Player 1 plays *Up* and that Player 2 plays *Left*. Then Player 1 gets a payoff of 4, and Player 2 gets 3.

CALCULATION OF GAME THEORY

Game theory can be defined as the study of mathematical models of conflict and cooperation between intelligent and rational decision makers .Game-theory concepts apply in economy, sociology, biology, and health care, and whenever the actions of several agents (individuals, groups, or any combination of these) are interdependent. We present a new command game to represent the extensive form (game tree) and the strategic form (payoff matrix) of a non-cooperative game and to identify the solution of a nonzero and zero-sum game through dominant and dominated strategies, iterated elimination of dominated strategies, and Nash equilibrium in pure and fully mixed strategies. Further, game can identify the solution of a zero-sum game through max-min criterion and the solution of an extensive form game through backward induction.

Strategic game:-

Whenever the strategy spaces of the players are discrete (and finite), the game can be represented compactly as a matrix. In such a game, player 1 has R possible actions, and player 2 has C possible actions; the payoff pairs to any strategy combination can be neatly arranged in an R×C table; and the game is easily analyzable (table 1). A payoff is a number, also called a utility, that reflects the desirability of an outcome to a player, for whatever reason. We denote the set of strategies for player 1 and player 2 with S1 = (1, 2, . . . , r, . . . , R) and S2 = (1, 2, . . . , c, . . . , C). The numbers of S1 and S2 may have labels. There are two elements (u1rc; u2rc) within each cell of the table. The first subscript takes only two values (1, 2) and simply denotes player 1 or player 2. The subscripts r and c denote, respectively, the strategies played by player 1 and player 2. Thus u1rc is the payoff for player 1 when player 1 chooses strategy r and player 2 chooses strategy c, whereas u2rc is the payoff for player 2 when player 1 chooses strategy r and player 2 chooses strategy c. Many methods are available to seek the solution of the game. We start analyzing the game by collecting the maximum payoffs and their related subscripts for each player given the choice of the other player into lists of numbers.

Table 1: Notation for an $R \times C$ payoff matrix

	S_2					
S_1	1	2	...	c	...	C
1	$(u_{111}; u_{211})$	$(u_{112}; u_{212})$	...	$(u_{11c}; u_{21c})$	...	$(u_{11C}; u_{21C})$
2	$(u_{121}; u_{221})$	$(u_{122}; u_{222})$	...	$(u_{12c}; u_{22c})$	...	$(u_{12C}; u_{22C})$
...	...	...	...	...	...	...
r	$(u_{1r1}; u_{2r1})$	$(u_{1r2}; u_{2r2})$	...	$(u_{1rc}; u_{2rc})$	...	$(u_{1rc}; u_{2rC})$
...	...	...	...	...	...	...
R	$(u_{1R1}; u_{2R1})$	$(u_{1R2}; u_{2R2})$	...	$(u_{1Rc}; u_{2Rc})$	...	$(u_{1RC}; u_{2RC})$

Let's define the maximum payoff MU1rc of player 1 if player 2 plays strategy c as the highest value on the left side of column c Formally,

$MU_{1rc} = \max\{u_{11}\ , u_{12c}, \dots\dots.., u_{1rc} \dots..u_{1Rc}\}$ with c = 1, 2,...,C

Let's define the maximum payoff MU2rc of player 2 if player 1 plays strategy r as the highest value on the right side of the row r. Formally,

$MU_{2rc} = \max\{u_{2r1}, u_{2r2}, \dots u_{2rc} \dots, u_{2rC}\}$ with r = 1, 2,...,R

We create a list, SMU_1, of C elements containing the subscripts r of all maximum payoffs MU_{1rc} for player 1 and a list, SMU_2, of R elements containing the subscripts c of all maximum payoffs MU_{2rc} for player 2. Furthermore, we create a list, SU_1, of subscripts for all possible strategies of player 1 (1, 2, . . . , R) and a list, SU_2, of subscripts for all possible strategies of player 2 (1, 2, . . . , C). These lists of numbers are useful for seeking the solution of a general R by C payoff matrix.

Nash's equilibrium in pure and fully mixed strategies:-

Another way to find the solution of the game is through Nash's equilibrium in pure and fully mixed strategies. A Nash equilibrium, also called a strategic equilibrium, is a list of strategies, one for each player, which has the property that no player has incentive to deviate from his strategy and get a better payoff, given that the other players do not deviate. A mixed strategy is a strategy generated at random according to a particular probability distribution that determines the player's decision. As a special case, a mixed strategy can be a deterministic choice of one of the given pure strategies. A Nash equilibrium in pure strategy specifies a strategy for each player in such a way that each player's strategy yields the player at least as high a payoff as any other strategy of the player, given the strategies of the other player. Based on our notation, we can say that Nash equilibriums in pure strategies are all pairs of strategies for which MU1rc and MU2rc have the same pairs of subscripts r and c. In other words, we proceed in two steps: first, we determine the best response; and second, we find the strategy profiles where strategies are best responses to each other. See section 6 for a worked example. A Nash equilibrium in mixed strategy specifies a mixed strategy for each player in such a way that each player's mixed strategy yields the player at least as high an expected payoff as any other mixed strategy, given the mixed strategies of the other player. Fully mixed strategies mean that the probability associated with each strategy cannot be equal to zero or one. The command game can find Nash equilibrium in fully mixed strategies if R = 2 and C = 2 (table 2)

Table 2: Payoff matrix if each player has two strategies

S_1	S_2: 1	S_2: 2
1	$(u_{111}; u_{211})$	$(u_{112}; u_{212})$
2	$(u_{121}; u_{221})$	$(u_{122}; u_{222})$

Player 1 would be willing to randomize between S_1=(1) and S_1=(2) only if these strategies gave him the same expected utility. More formally, we seek the probability p so that both sides of (1) are equal.

$p \times u_{111} + (1 - p) \times u_{112} = p \times u_{121} + (1 - p) \times u_{122}$ ……………………………………….(1)

Thus player 2's strategy in the equilibrium must be equal to

$p \times S_2(1) + (1 - p) \times S_2(2)$

To make player 1 willing to randomize between $S_1(1)$ and $S_1(2)$. $S_1(1)$ and $S_1(2)$ indicate the strategies for player 1, while $S_2(1)$ and $S_2(2)$ indicate the strategies for player 2. Similarly, player 2 would be willing to randomize between S_2 = (1) and S_2 = (2) only if these strategies give him the same expected utility. Again we seek the probability q such that both sides of (2) are equal.

$q \times u_{211} + (1 - q) \times u_{221} = q \times u_{212} + (1 - q) \times u_{222}$ ……………………………………….(2)

Thus player 1's strategy in the equilibrium must be equal to

$q \times S_1(1) + (1 - q) \times S_1(2)$

to make player 2 willing to randomize between S2(1) and S2(2). The Nash equilibrium in fully mixed strategies must be equal to (3).

$\{p \times S_2(1) + (1 - p) \times S_2(2), q \times S_1(1) + (1 - q) \times S_1(2)\}$ ……………………………………….(3)

We find the solution of (1) and (2) by using explicit formulas.

Solution of 2×2 Ractangular Games without a saddle point:-

Let us consider a 2×2 two – person Zero-sum game without any saddle point having the following pay-off matrix for the row player A.

Player-B

$$\text{Player-A}\quad \begin{array}{c} \\ A_1 \\ A_2 \end{array} \begin{array}{c} \begin{matrix} B_1 & B_2 \end{matrix} \\ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \end{array}$$

Since this pay-off matrix has no saddle point so, both A & B have to apply mixed strategy.

Let P_1, P_2 be the probabilities for selecting the strategies A_1 *and* A_2 respectively for the player-A and q_1, q_2 be those for selecting the strategies B_1*and* B_2 respectively for the player- B.

Then, $p_1 + p_2 = 1 = q_1 + q_2$ ....(i)

Now, for the player A, the expected gain for selecting the strategy B_1 by the player B is

$$a_{11}p_1 + a_{21}p_2$$

and those for the strategy B_2 is

$$a_{12}p_1 + a_{22}p_2$$

Now, for the player A,

$$a_{11}p_1 + a_{21}p_2 = v = a_{21}a_1 + a_{22}p_2 \qquad \text{..(ii)}$$

Similarly for the player-B, and optimal strategy, then,

$$a_{11}q_1 + a_{12}q_2 = v = a_{21}q_1 + a_{22}q_2 \qquad \text{...(iii)}$$

Form (ii) and (iii), we get,

$$\frac{p_1}{p_2} = \frac{a_{22}-a_{21}}{a_{11}-a_{12}}$$

And $\frac{q_1}{q_2} = \frac{a_{22}-a_{21}}{a_{11}-a_{12}}$

Now using (i), we get,

$$p_1 = \frac{a_{22}-a_{21}}{(a_{11}+a_{22})-(a_{12}+a_{21})}$$

$$p_2 = 1 - p_1$$

$$= \frac{a_{11}-a_{12}}{(a_{11}+a_{22})-(a_{12}+a_{21})}$$

And similarly,

$$q_1 = \frac{a_{22}-a_{12}}{(a_{11}+a_{22})-(a_{12}+a_{21})}$$

$$q_2 = 1 - q_1$$

$$q_2 = \frac{a_{11} - a_{21}}{(a_{11} + a_{22}) - (a_{12} + a_{21})}$$

In this case, the value of the game will be

$$v = a_{11}p_1 + a_{21}p_2$$

$$= \frac{a_{11}a_{22} - a_{12}a_{21}}{(a_{11} + a_{22}) - (a_{12} + a_{21})}$$

For a game with 2×2 pay-off matrix with a saddle point, the value of v may not be correctly obtained by using formula.

Graphical method of solution of 2×n or m×2 games :-

When the pay-off matrix of a two –person zero sum games of size 2×n of m×2 when in the game, one of the two players has only two pure strategies and also when the game has no saddle point solution the graphical method is a very used full method for solving such problems using this method any 2×n or m×2 pay-off matrix can be reduce to a 2×2 matrix and ultimately it can be solved by algebraic method.

Let us consider the following 2×n pay-off matrix of a game without a saddle point:-

	B_1	B_2	B_3	...	B_n
A_1	a_{11}	a_{12}	a_{13}	...	a_{1n}
A_2	a_{21}	a_{22}	a_{23}	...	a_{2n}

Let a mixed strategy of the row-player A be given by (p_1, p_2) where, $p_1 + p_2 = 1$, $p_1 \geq 0$ and $p_2 \geq 0$. Now, for each of the pure strategies available to the column-player-B, the expected pay-off for the player-A will as follows :

B's Pure Strategies	**A's Expected pay-off E(p)**
B_1	$E_1(p) = a_{11}p_1 + a_{21}p_2 = a_{11}p_1 + a_{21}(1 - p_1)$ $= (a_{11} - a_{21})p_1 + a_{21}$
B_2	$E_2(p) = (a_{12} - a_{22})p_1 + a_{22}$
:	:::
B_n	$E_n(p) = (a_{1n} - a_{2n})p_1 + a_{2n}$

Now, it is obvious that B would like to select that pure strategy B_j against A's move for which $E_j(p)$ will be minimum, j = 1,2,...,n. Let us denote this minimum expected Pay – off for A by

$$v = Min\,\{E_j(p)\}, j = 1,2,\ldots,n$$

The player-A will try to select p_1 and (hence) p_2 in such a way that v will be as large as possible. This may be done by plotting the straight lines.

$$E_j(p) = (a_{1j} - a_{2j})p_1 + a_{2j}, j = 1,2,\ldots\ldots,n$$

As linear functions of p_1.

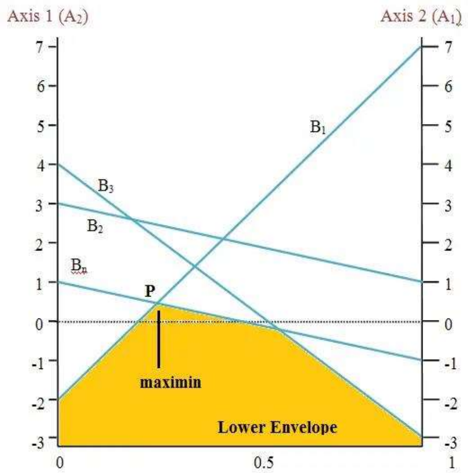
Again since, $0 \leq p_1 \leq 1$, so

$$E_j(p) = a_{2j}, when\; p_1 = 0$$

$$= a_{1j}, when\; p_1 = 1,$$

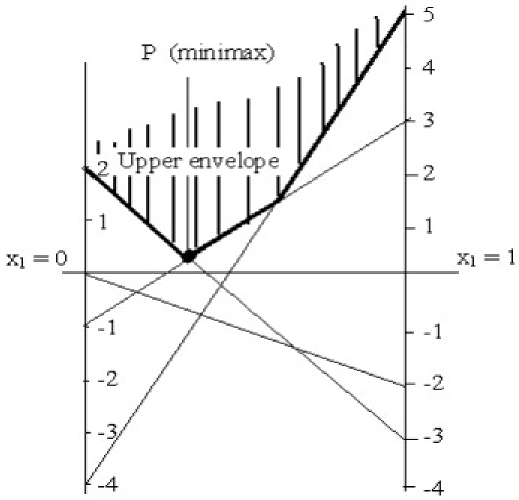
And hence, $E_j(p)$ represents a line segment joining the points $(0,a_{2j})$ and $(1,a_{1j})$.

To represent thus line segment graphical ,we first draw two parallel vertical line ,the distance between then being one unit of length . The first one represent the line p_1=0 and the second one represent the line p_1 =1 . Now ,we draw the line segment joining the point $(0,a_{2j})$ and$(1,a_{ij})$ j=1,2,..........,n .the lower bounded of these line will from a lower envelops and will give the minimum expected pay-off for the row-player as a function of p_1. The highest point on this lower envelope will given maximum expected pay off among the minimum expected pay-off of the row-player A and the optimal value of his probabilities (p_1,p_2). In this way we may get two strategies for the column-player B corresponding to the two lines passing thought the maximum point of the lower envelops. This helps us to reduce the size of the pay-off matrix to 2×2 and which ultimately can be solved by algebraic method.



LOWER ENVELOP

The m×2 game can similarly be treated. In this case; we consider the lower point of the upper envelope to get two strategies for the row – player-A and the optimal value of the probabilities (q_1,q_2) of the column player-B.



UPPER ENVELOP

APPLICATION OF GAME THEORY :-

Economic :- Game theory ,being concerned with the behavior of decision makers and their interactions ,seems to have limited applicability in economics.

Price war

This is a similar outcome but for two firms that can keep prices high and stable or start a price war. The best outcome for both firms is (a) \$40, \$40.

Firm B

Firm A

Price War	Stable prices	Price war
Stable prices	\$40, \$40 (a)	\$0, \$60 (b)
Price war	\$60, \$0 (c)	\$3, \$3 (d)

However, when prices are stable, if one firm cuts prices (starts price war) it will see profits rise to $60. However, the other firm who keeps prices high will lose market share and get zero profits. Therefore, the firm who loses out will almost certainly retaliate and the outcome will move to (d) with both firms just making $3 profit. Therefore, there is strong incentive to avoid price war.

• **Co-ordination playoff**

Firm B

Firm A

Co-ordination playoff	New technology	No investment
New technology	$200, $200 (a)	$0, $30 (b)
No investment	$30, $0 (c)	$50, $50 (d)

- In this example, if neither firms invest, they will make $50 each. However, if they both invest in new technology, which will become new market standard, they will both get substantially better pay off (a) with $200 each.
- However, if one firm invests in new technology and the other doesn't, then they will be left with $0 (it is not widely shared). In this case, the firm will probably start investing too, as they would be better off.
- However, the key thing is whether one firm is willing to take the plunge and make zero profits in the short-run. It may not be able to afford this outcome.
- The issue with this game theory dilemma is that there are strong rewards from co-operating. But, in the real world, for various reasons, co-operation may not be there.

Matching pennies

Player B

Player A

Matching pennies	Heads	Tails
Heads	+1,-1 (a)	-1, +1 (b)
Tails	-1, +1 (c)	+1, -1 (d)

- This is a game with two players. They both put a penny on the table.
- If the pennies are Heads/heads or tails/tails – then Player A wins both pennies. He gains 1, (player B loses 1)
- If the pennies are mixed (heads/tails) or tails/heads then play B wins both pennies.
- This is an example of a zero-sum game – the net benefit is always zero. For everyone who gains, there is an equal and opposite loss.

Zero-sum game

Firm B

Firm A		Enters market	Leaves market
	Enters market	1,-1	3, - 3
	Leaves market	-2, 2	0, 0

In this situation, we have another zero-sum game situation. If a firm enters or leaves, there is always a net benefit of zero.

For firm A, its dominant strategy is to enter the market, because 1 is greater than -2.

For firm B, its dominant strategy is also to enter the market because -1 is greater than -3. Firm B would prefer both firms to leave the market so it can get to zero. But, in this model, it can't do that because it know if A enters, it will have to enter or face the costs of -3.

Tariff or trade war

Country B

Country A	**Trade**	**High Tariff**	**Low Tariff**
	High Tariff	£1m – A £1m – B	£2m – A £1.5m - B
	Low Tariff	£1.5m A £2m for B	£3m £3m

- In this case, if both countries, pursue low tariffs, the outcome is £3m net welfare for each country. If A places tariff, then its net welfare will be £2m, and country B who keeps low tariffs will make £1.5m.
- If B retaliates and places tariffs on too, it will make itself worse of – welfare falls to £1m, but it will effectively punish A whose welfare falls from £2m to £1m.
- If firms wish to maximize welfare, they would stick to low tariffs. That is their dominant strategy and nash equilibrium.
- However, in the real world, there may be political pressures (e.g. protect domestic industry, even at expense of higher prices for consumers, which encourages countries to place tariffs.

Prisoner's dilemma

Suspect B

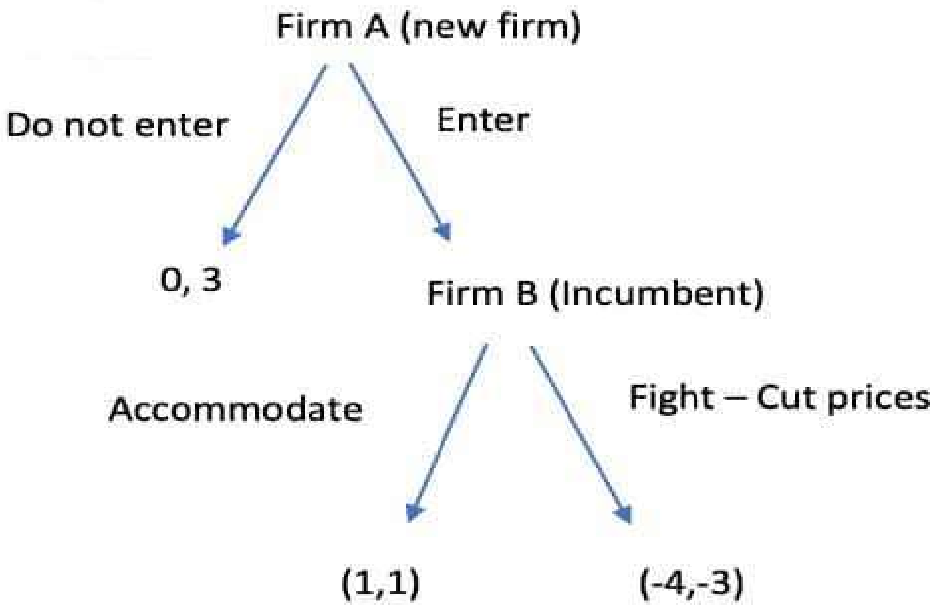
Prisoner's dilemma	Do Not Confess	Confess
Suspect A – Do Not Confess	A = 1 year B = 1 year	A= 0 years B = 20 years
Suspect A – Confess	A = 20 years B = 0 years	A = 5 years B = 5 years

The prisoner's dilemma is a classic example of game theory.

- There are two prisoners held in solitary confinement. They can either confess to crime or stay silent (not confess)
- If both stay silent, they both get light sentence of 1 year.
- If they both confess, they get 5 years each.
- However, if one confesses to the crime and betrays the other, then the one who confesses is given immunity for giving information. But the other who remained silent gets 20 years.
- Therefore, a prisoner would only choose to remain silent, if they can guarantee the other prisoner will remain silent.
- The dominant strategy for both players is to confess. At worst they will get 5 years, at best they will get 0 years.
- The Nash equilibrium is confess/confess (5 years each). Because if a player acted unilaterally, it would be worse off.

Decision Tree

Another way of describing game theory is through a decision tree.



- In this example, Firm A can choose to enter or leave. Firm B (the incumbent can then decide to fight (cut prices) or accommodate.
- If it fights, both firms make a lost (-4, -3). Therefore the dominant strategy for Firm B appears to be accommodate, leaving both firms with (1,1)
- However, firm B may make the calculation that it is worth making a temporary loss, in order to try and force the new firm out of business. Also, if firm B fights, it may deter other entrants.

Dominant strategy

A dominant strategy occurs when there is an optimal choice of strategy for each player no matter what the other does.

		P2	
		LEFT	RIGHT
P1	UP	**8,6**	5,4
	DOWN	7,5	2,4

- If P2 chooses left P1 will choose UP
- If P2 chooses right P1 will choose UP
- Therefore UP is a dominant strategy for P1
- P2 will always choose right no matter what P1 does
- The unique equilibrium is (up, left). This is best for both.

Nash Equilibrium

A Nash equilibrium occurs when the payoff to player one is the best given the other's choice.

		P2	
		LEFT	RIGHT
P1	UP	6,6	4,7
	DOWN	7,4	**5,5**

- In this case If P1 chooses down, P2 will choose right
- If P1 choose UP, P2 will choose right. But, if P2 choose right, P1 will want to choose down.
- The Nash equilibrium will be downright, (5,5) despite UP left being the optimal Pareto outcome.

Evolutionary:-

Evolutionary Game theory is the application of Game theory to evolving population in biology.

Hawk Dove

❖ ***Payoff matrix for hawk dove game***

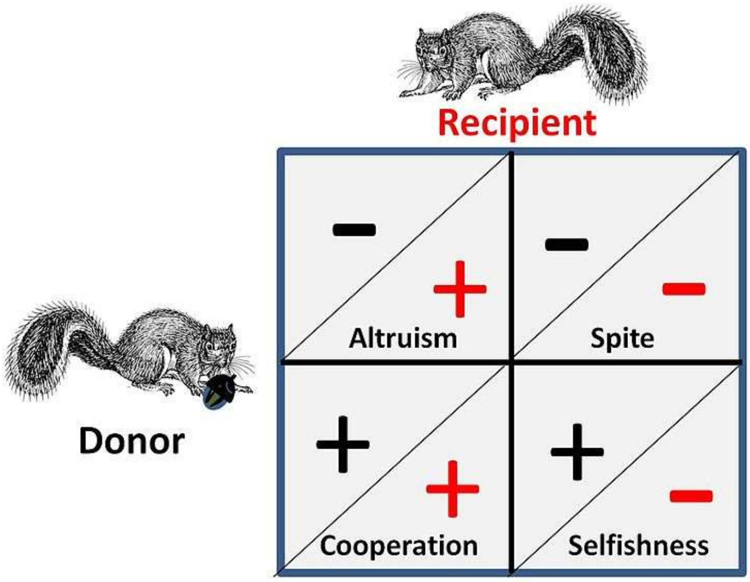
	Meets hawk	Meets dove
If hawk	V/2 – C/2	V
If dove	0	V/2

Given that the resource is given the value V, the damage from losing a fight is given cost C:-

- If a hawk meets a dove, the hawk gets the full resource V
- If a hawk meets a hawk, half the time they win, half the time they lose, so the average outcome is then V/2 minus C/2
- If a dove meets a hawk, the dove will back off and get nothing – 0
- If a dove meets a dove, both share the resource and get V/2

The actual payoff, however, depends on the probability of meeting a hawk or dove, which in turn is a representation of the percentage of hawks and doves in the population when a particular contest takes place.

Social Behaviour



Games like hawk dove and war of attrition represent pure competition between individuals and have no attendant social elements. Where social influences apply, competitors have four possible alternatives for strategic interaction. This is shown on the adjacent figure, where a plus sign represents a benefit and a minus sign represents a cost.

- In a cooperative or mutuality relationship both "donor" and "recipient" are almost indistinguishable as both gain a benefit in the game by co-operating, i.e. the pair are in a game-wise situation where both can gain by executing a certain strategy, or alternatively both must act in concert because of some encompassing constraints that effectively puts them "in the same boat".
- In an altruistic relationship the donor, at a cost to them self provides a benefit to the recipient. In the general case the recipient will have a kin relationship to the donor and the donation is one-way. Behaviors where benefits are donated alternatively (in both directions) at a cost, are often called "altruistic", but on analysis such "altruism" can be seen to arise from optimized "selfish" strategies.
- Spite is essentially a "reversed" form of altruism where an ally is aided by damaging the ally's competitors. The general case is that the ally is kin related and the benefit is an easier competitive environment for the ally. Note: George Price, one of the early mathematical modelers of both altruism and spite, found this equivalence particularly disturbing at an emotional level.
- Selfishness is the base criteria of all strategic choice from a game theory perspective – strategies not aimed at self-survival and self-replication are not long for any game. Critically however, this situation is impacted by the fact that competition is taking place on multiple levels – i.e. at a genetic, an individual and a group level.

Description and Modeling:-

The primary use of game theory is to describe and model how human populations behave. Some scholars believe that by finding the equilibrium of games they can predict how actual human populations will behave when confronted with situations analogous to the game being studied. This particular view of game theory has been criticized. It is argued that the assumptions made by game theorists are often violated when applied to real-world situations. Game theorists usually assume players act rationally, but in practice, human rationality and/or behavior often deviates from the model of rationality as used in game theory. Game theorists respond by comparing their assumptions to those used in physics. Thus while their assumptions do not always hold, they can treat game theory as a reasonable scientific ideal akin to the models used by physicists. However, empirical work has shown that in some classic games, such as the centipede game, guess 2/3 of the average game, and the dictator game, people regularly do not play Nash equilibrium. There is an ongoing debate regarding the importance of these experiments and whether the analysis of the experiments fully captures all aspects of the relevant situation.

Game Theory in Politics:-

Game theory is widely used in political affairs, which is focused on the areas of international politics, war strategy, war bargaining, social choice theory, Strategic voting, political economy etc. Game theory is an effective tool in the hands of diplomats and politicians to analysis any situation of conflict between individuals, companies, states, political parties. Rationality of actors and the choice of strategies are one of the basic assumptions of game theory. Game theory seems to be useful tool for research on terrorism because it captures the interaction between attacked subject and terrorist organization, when the steps are interdependent and therefore cannot be analyzed separately (Sandler and Arce M, 2003).

By using Prisoner's dilemma, we will focus situation where governments choose between active and reactive counter terrorism policies.

Let, There are two countries- Bangladesh and India. Both countries face common threat of terrorist attacks, and both must agree on whether or not to jointly apply active counter- terrorism policy.

Bangladesh

India		active	reactive
	active	(4, 4)	(-2, 6)
	reactive	(6, -2)	(0, 0)

We assumed that active policy for individual countries gains benefits of 6 and costs of 8 for country that applied active policy. If the India is applying active policy and the Bangladesh will be the state that will only get benefits associated with it, then Bangladesh will have the advantages of the 6. India gets -2 (6-8). Cost of 8 shall be deducted from the benefits of 6. Otherwise, if the India is a free-rider, the benefits are reversed.

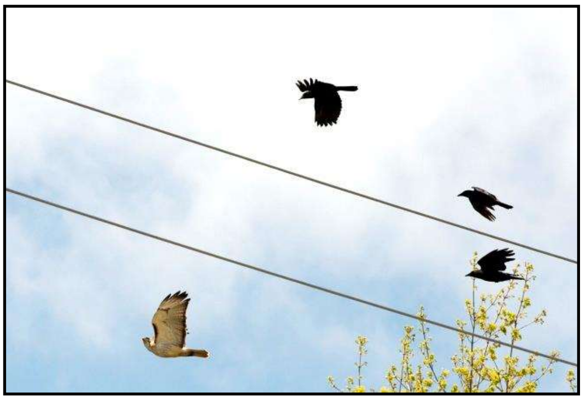
If both countries are active policy, then everyone gets the benefit of -4 (8- 2×6).

The result is prisoner's dilemma game, in which no country wants to apply active counter-terrorism policy.

Biology:-

In biology, game theory has been used as a model to understand many different phenomena. It was first used to explain the evolution (and stability) of the approximate 1:1 sex ratios. (Fisher 1930) suggested that the 1:1 sex ratios are a result of evolutionary forces acting on individuals who could be seen as trying to maximize their number of grandchildren.

Additionally, biologists have used evolutionary game theory and the ESS to explain the emergence of animal communication. The analysis of signaling games and other communication games has provided insight into the evolution of communication among animals. For example, the mobbing behaviour of many species, in which a large number of prey animals attack a larger predator, seems to be an example of spontaneous emergent organization. Ants have also been shown to exhibit feed-forward behavior akin to fashion.



American crows (*Corvus brachyrhynchos*) mobbing a red-tailed hawk (*Buteo jamaicensis*)

The occurrence of mobbing behavior across widely different taxa, including California ground squirrels, is evidence of convergent evolution

Biologists have used the game of chicken to analyze fighting behavior and territoriality.

According to Maynard Smith, in the preface to *Evolution and the Theory of Games*, "paradoxically, it has turned out that game theory is more readily applied to biology than to the field of economic behavior for which it was originally designed". Evolutionary game theory has been used to explain many seemingly incongruous phenomena in nature.

One such phenomenon is known as biological altruism. This is a situation in which an organism appears to act in a way that benefits other organisms and is detrimental to itself. This is distinct from traditional notions of altruism because such actions are not conscious, but appear to be evolutionary adaptations to increase overall fitness. Examples can be found in species ranging from vampire bats that regurgitate blood they have obtained from a night's hunting and give it to group members who have failed to feed, to worker bees that care for the queen bee for their entire lives and never mate, to vervet monkey that warn group members of a predator's approach, even when it endangers that individual's chance of survival. All of these actions increase the overall fitness of a group, but occur at a cost to the individual.

Adult vervet monkey

The co-operative behaviour of social insects like the honey bee can be explained by kin selection.

Evolutionary game theory explains this altruism with the idea of kin selection. Altruists discriminate between the individuals they help and favor relatives. Hamilton's rule explains the evolutionary rationale behind this selection with the equation $c < b \times r$, where the cost c to the altruist must be less than the benefit b to the recipient multiplied by the coefficient of relatedness r. The more closely related two organisms are causes the incidences of altruism to increase because they share many of the same alleles. This means that the altruistic individual, by ensuring that the alleles of its close relative are passed on through survival of its offspring, can forgo the option of having offspring itself because the same number of alleles are passed on. For example, helping a sibling (in diploid animals) has a coefficient of $\frac{1}{2}$, because (on average) an individual shares half of the alleles in its sibling's offspring. Ensuring that enough of a sibling's offspring survive to adulthood precludes the necessity of the altruistic individual producing offspring. The coefficient values depend heavily on the scope of the playing field; for example if the choice of whom to favor includes all genetic living things, not just all relatives, we assume the discrepancy between all humans only accounts for approximately 1% of the diversity in the playing field, a coefficient that was $\frac{1}{2}$ in the smaller field becomes 0.995. Similarly if it is considered that information other than that of a genetic nature (e.g. epigenetic, religion, science, etc.) persisted through time the playing field becomes larger still, and the discrepancies smaller.

Philosophy:-

Game theory has been put to several uses in philosophy. Responding to two papers by W.V.O. Quine (1960, 1967), Lewis (1969) used game theory to develop a philosophical account of convention. In so doing, he provided the first analysis of common knowledge and employed it in analyzing play in coordination games. In addition, he first suggested that one can understand meaning in terms of signaling games. This later suggestion has been pursued by several philosophers since Lewis. Following Lewis (1969) game-theoretic account of conventions, Edna Ullmann-Margalit (1977) and Bicchieri (2006) have developed theories of social norms that define them as Nash equilibria that result from transforming a mixed-motive game into a coordination game.

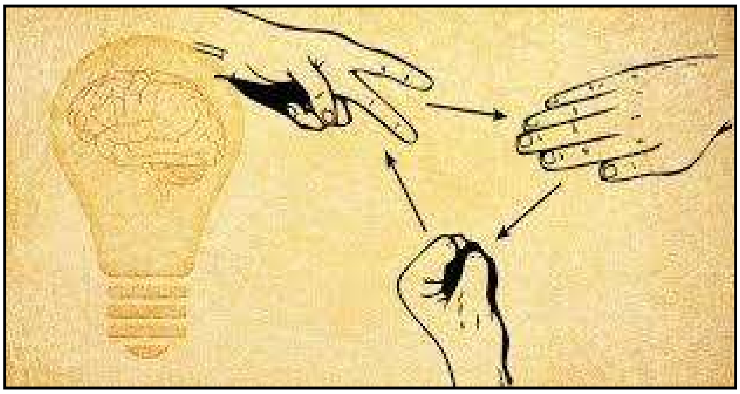
Game theory has also challenged philosophers to think in terms of interactive epistemology: what it means for a collective to have common beliefs or knowledge, and what are the consequences of this knowledge for the social outcomes resulting from the interactions of agents. Philosophers who have worked in this area include Bicchieri (1989, 1993), Skyrms (1990), and Stalnaker (1999).

In ethics, some (most notably David Gauthier, Gregory Kavka, and Jean Hampton)[authors have attempted to pursue Thomas Hobbes' project of deriving morality from self-interest. Since games like the prisoner's dilemma present an apparent conflict between morality and self-interest, explaining why cooperation is required by self-interest is an important component of this project. This general strategy is a component of the general social contract view in political philosophy (for examples, see Gauthier (1986) and Kavka (1986)).

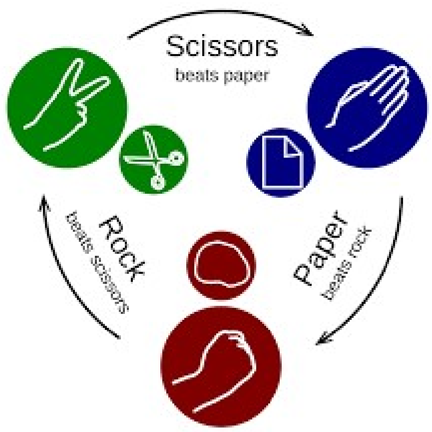
Other authors have attempted to use evolutionary game theory in order to explain the emergence of human attitudes about morality and corresponding animal behaviors. These authors look at several games including the prisoner's dilemma, stag hunt, and the Nash bargaining game as providing an explanation for the emergence of attitudes about morality.

Rock paper scissors game theory:-

Nash Equilibrium is a pair of strategies in which each player’s strategy is a best response to the other player’s strategy. In a game like Prisoner’s Dilemma, there is one pure Nash Equilibrium where both players will choose to confess. However, the players only have two choices: to confess or not to confess.



What happens if there are more choices? For example, in the classic game of rock, paper, and scissors, there are three choices. How can we find the Nash Equilibrium then? And if we do, is it helpful? See the following article: In the above article, the author discusses the application of Nash Equilibrium to games like Rock, Paper, and Scissors. Recall from class that in game theory, games can have: (1) Only one pure Nash Equilibrium (e.g. in Prisoner's Dilemma) (2) Only one mixed Nash Equilibrium and no pure Nash Equilibrium (e.g. Kicker/Goalie Penalty kicks) (3) Multiple pure Nash Equilibrium (e.g. Hawk-Dove Game) (4) Pure and mixed (e.g. Hawk-Dove Game) So which category does the game Rock, Paper, and Scissors fall under?



According to the article, Rock, Paper, and Scissors fall under (2) – only one mixed Nash Equilibrium. However, you can easily arrive at this conclusion by applying your knowledge of game theory and Nash equilibrium – all topics we learned in INFO 2040.

Let p = player one and q = player two. (For the sake of simplicity, there will only be two players) First, the reason why there isn't a pure Nash Equilibrium is that there is no way a player will 100% of the time choose one choice. For example, let's take player 1. If he consistently plays rock, then player 2 will always choose paper. Player one will never win. Likewise, if player 2 always choose paper, player one will always choose scissors. Player two will always lose. The two players will then fall into a cycle of rock, then paper, then scissors. Thus, there is no equilibrium – it just doesn't make sense for one player to ALWAYS pick one choice for the whole game – it's just too predictable. Now let p(rock) be the probability that player 1 pick rock, p(scissors) be the probability that player 1 pick scissors, and p(paper) be the probability that player 1 chooses paper. Likewise, q(rock), q(scissors), and q(paper) for player 2. We know that none of these probabilities is fully a 1 (always choose).

The expected value for player 2 is:

EV[q(rock)] = 0*p(rock) + (-1)*p(paper) + 1* (p(scissors))
EV[q(paper)] = 1*p(rock) + 0*p(paper) + (-1)*(p(scissors))

EV[q(scissors)] = (- 1)*p(rock) + 1*p(paper) + 0*(p(scissors))

Also, p(rock) + p(paper) + p(scissors) = 1

Using these equations, you will eventually reach that the Nash Equilibrium for the game Rock, Paper, and Scissors is:

For player 1,

p(rock) = 1/3, p(paper) = 1/3, and p(scissors) = 1/3 and

similarly, For player 2,

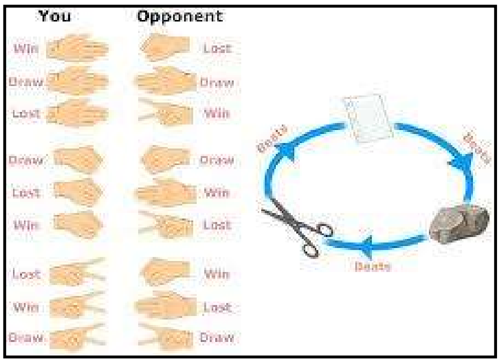
q(rock) = 1/3, q(paper) = 1/3, and q(scissors) = 1/3

So that's the Nash Equilibrium.

	Rock	Paper	Scissors
Rock	0, 0	-2, 2	1, -1
Paper	2, -2	0, 0	-1, 1
Scissors	-1, 1	1, -1	0, 0

But how useful is it? Why Nash Equilibrium may not apply to a game like Rock, Paper, and Scissors There is another major difference between a game like Prisoner's Dilemma and Rock, Paper, and Scissors (besides the number of choices) and that is: The players will play again and again. In Prisoner's Dilemma, they play one round and so they must pick the dominant strategy in that game, but in Rock, Paper, and Scissors, the two players repeatedly play. The article states that in such a case, it's best for the players to stick to about 1/3 for rock, paper, or scissors throughout the game. However, is that really the best? See the following article: In this article, a large amount of people repeatedly play rock, paper, and scissors against each other and the results are: "Upon review of the results, Wang did find numbers that backed up the Nash Equilibrium theory coming into play. He also found the above-mentioned pattern: winners were the players who stayed loyal to their strategy and losers were the players who switched. In game theory, this is called "conditional response." In fact, the conditional strategy proved to be 10 percent more reliable for winning than did the Nash Equilibrium." From this, you should definitely be more cautious in using the Nash Equilibrium. Of course, we did find the Nash Equilibrium for Rock, Paper, and

Scissors but we cannot say that will be the best strategy. In fact, often times it's not (as we have found out in class). Thus, as shown in class and here, we can find the Nash Equilibrium in cases where there are more than two choices but we also need to be careful when applying it – even if it's a game as simple as Rock, Paper, and Scissors. Side Notes: (1) I recommend readers to look up "conditional response" (2) For the game Prisoner's Dilemma, a tournament was held where players repeatedly play Prisoner's Dilemma and one strategy that did well was called "tit for tat." See: dilemma Comments Download PDF Abstract: Rock-Paper-Scissors (RPS), a game of cyclic dominance, is not merely a popular children's game but also a basic model system for studying decision-making in non-cooperative strategic interactions. Aimed at students of physics with no background in game theory, this paper introduces the concepts of Nash equilibrium and evolutionarily stable strategy, and reviews some recent theoretical and empirical efforts on the non-equilibrium properties of the iterated RPS, including collective cycling, conditional response patterns, and microscopic mechanisms that facilitate cooperation. We also introduce several dynamical processes to illustrate the applications of RPS as a simplified model of species competition in ecological systems and price cycling in economic markets. From: Hai-Jun Zhou [view email] [v1] Thu, 14 Mar 2019 13:40:11 UTC (220 KB) Want more? Advanced embedding details, examples, and help! . ."All will be well if you use your mind for your decisions, and mind only your decisions." Since 2007, I have devoted my life to sharing the joy of game theory and mathematics. Mind Your Decisions now has over 1,000 free articles with no ads thanks to community support! Help out and get early access to posts with a pledge on Patron. One of the most common questions I get is, "Can you recommend an introductory book on game theory-a book without a lot of math?"When I first got this question, I was hard pressed to find an answer. Game theory is a mathematical science, and many presentations can be intimidating. For example, many journals and textbooks are so complicated that it takes a mastery of Bayesian probability, set theory, and real analysis just to understand the problems! This is a tragedy, for a subject as interesting as game theory should be made accessible. So over the last few years I have kept a special eye out for books aimed at general audiences. And I am glad to say there are a few good books on game theory. I have listed the books I have especially enjoyed in a separate blog page about recommended books.



And to do them justice, I plan to write full reviews on each of my favorites so you get a better idea of them. Today I will discuss Rock, Paper, Scissors: Game Theory in Everyday Life by Len Fisher. What the book is about there are two quotes in the "praise" section that nicely summarize the book:"Why be nice? In answering this simple question, Len Fisher takes us on a wry, fascinating tour of one of the most momentous sciences of our time. You couldn't ask for a better guide to all the games we play." –William Poundstone, author of Gaming the Vote and Fortune's Formula "Rock, Paper, Scissors is a refreshingly informal as well as insightful account of key ideas in game theory. Len Fisher gives many examples, several from his own life, of games that post harrowing choices for their players. He shows how game theory not only illuminates the consequences of these choices but also may help the players extricate themselves from situations likely to cause anger or grief." –Steven J. Brams, New York University, author of Mathematics and Democracy My one sentence summary is: Rock, Paper, Scissors is a popular science book that connects game theory to everyday situations and suggests several strategies for achieving cooperation.(As you can tell, this book is a different style from other books I like such a Thinking Strategically or The Art of Strategy. This book is a lighter read and connects more to anecdotes and science.)Book highlights will warn you that the book starts off a little bit slowly. The first chapter "trapped in a matrix" mainly describes the Prisoner's dilemma and gives the negative connotation that the Nash equilibrium is a logical trap. The matrix graphics are not that illuminating either. Luckily, these setbacks didn't stop me from reading the rest of the book which is full of interesting examples and explanations. The second chapter "I cut and you choose" is where the book picks up. This chapter offers a nice introduction to the concepts of mini-max and fair division. Fisher illuminates fair division with anecdotes like how he got in trouble as a kid shooting fireworks, and as a consequence had to yield fireworks with his brother. The answer he intuitively arrived to as a kid was what he know realizes was an application of the mini-max principle. I was also impressed that Fisher discusses the principle of equal division of the contested sum, which I have discussed twice before (regarding religion and homeowner fees).Chapter three is about seven of the most interesting game theory problems, which Fisher aptly dubs "the seven deadly dilemmas." Here Fisher offers a great summary of such problems as the free rider issue and the game of chicken. Chapter four is a humorous one, and is about the game "rock, paper, scissors." It was new to me that rock, paper, scissors is in fact played in most of the world (though under various other names). I was also amused at how rock, paper, scissors can be used in conflict resolution. The reason is that the game has no pure strategy that dominates the others. Hence situations and games which seem to be at a standstill (say too many free-riders in overfishing) can be solved by adding strategies and converting them to rock-paper-scissors situations. Chapters five through eight are all about cooperation: how we can achieve trust, bargain effectively, and change the game to avoid the “trap” of the Prisoner’s dilemma and other undesirable outcomes. I won’t go into detail, as the main fun points are similar in nature to the other chapters: the narratives and interesting examples from science. Read the end notes! One of the best parts of this book is the “Notes” section at the end. This is a substantial part of the book and it is full of narratives, jokes, and random trivia.

The end notes are over 50 pages long-and this is for a book that is about 250 pages in total! I am still following up on many of the references and this alone has been worth the read. Final thoughts hope this review gives you a better idea of the book. It is a great introductory read and a good addition for real-life examples of game theory. Check it out:*I also owe a special thanks to the book publisher for providing a review copy If you purchase through these links, I may be compensated for purchases made on Amazon. As an Amazon Associate I earn from qualifying purchases. The puzzles topics include the mathematical subjects including geometry, probability, logic, and game theory. Math Puzzles Volume 1 features classic brain teasers and riddles with complete solutions for problems in counting, geometry, probability, and game theory. Volume 1 is rated 4.4/5 stars on 112 reviews. Math Puzzles Volume 2 is a sequel book with more great problems. (rated 4.2/5 stars on 33 reviews)Math Puzzles Volume 3 is the third in the series. (rated 4.2/5 stars on 29 reviews)KINDLE UNLIMITED Teachers and students around the world often email me about the books. Since education can have such a huge impact, I try to make the eBooks’ available as widely as possible at as low a price as possible. Currently you can read most of my eBooks’ through Amazon's "Kindle Unlimited" program. Included in the subscription you will get access to millions of eBooks’. You don't need a Kindle device: you can install the Kindle app on any Smartphone/tablet/computer/etc. I have compiled links to programs in some countries below. Please check your local Amazon website for availability and program terms. US, list of my books (US) UK, list of my books (UK) Canada, book results (CA) Germany, list of my books (DE) France, list of my books (FR) India, list of my books (IN) Australia, book results (AU) Italy, list of my books (IT) Spain, list of my books (ES) Japan, list of my books (JP) Brazil, book results (BR) Mexico, book results (MX) MERCHANDISE Grab a mug, t-shirt, and more at the official site for merchandise: Mind Your Decisions at Tee spring.

LIMITATIONS OF GAME THEORY

The biggest issue with game theory is that, like most other economic models, it relies on the assumption that people are rational actors that are self-interested and utility-maximizing. Of course, we are social beings who do cooperate often at our own expense. Game theory cannot account for the fact that in some situations we may fall into a Nash equilibrium, and other times not, depending on the social context and who the players are.

In addition, game theory often struggles to factor in human elements such as loyalty, honesty, or empathy. Though statistical and mathematical computations can dictate what a best course of action should be, humans may not take this course due to incalculable and complex scenarios of self-sacrifice or manipulation. Game theory may analyze a set of behaviors but it can not truly forecast the human element.

CONCLUSION

i) Game theory is exciting because although the principle are simple, the application are for reaching.

ii) Game theory is the study of cooperative and non cooperative approaches to games and social situations in which participants must choose between individual benefits and collective benefits.

iii) Game theory can be used to design credible commitments threats or promises and statements offered by others.

iv) Game theory is a powerful theoretical tool for understanding cooperation and the conditions under which it can occur.

v) Game theory, however, makes an assumption, in the context of cooperation, that can limit its application: Players are disembodied.

vi) By using agent-based models, we can investigate embodied agents and discover that in many cases, stable game-theoretic solutions depend on embodiment and context.

REFERANCES

- Theory of Games and Economic Behavior, 1944.
- Game Theory by Guillermo Owen, 2nd edition, Academic Press, 1982.
- Game Theory and Strategy by Philip D. Straffin, published by the Mathematical Association of America, 1993.
- C. Camerer, Behavioral game theory: Experiments in strategic interaction: Princeton University Press, 2003.
- Kreps, D. M., & Wilson, R. (1982). Sequential equilibria. Econometrica: Journal of the Econometric Society, 863-894.
- Myerson, R. B. (1985). Bayesian equilibrium and incentive-compatibility: An introduction. Social goals and social organization: Essays in memory of Elisha Pazner, 229-260.
- Hotz, Heiko. (2006). A Short Introduction to Game Theory. Retrieved on 21.09.2017 from: http://www.theorie.physik.lmu.de.
- Neumann, John von and Morgenstern, Oskar. (1944). The Theory of Games and Economic Behavior. Princeton: Princeton University Press.
- Varian, H. R. (2010). Intermediate Microeconomics: A modern approach (8thed.). New York: W.W. Norton & Co.
- Gibbons, R. (1992). Game Theory for Applied Economists. Princeton, New Jersey: Princeton University Press.
- Nicholson & Snyder. Intermediate Microeconomics and its Application (11thed).South-Western Cengage Learning.
- “Notes 6: Game theory”. retrieved from http://www2.econ.iastate.edu/classes/econ335/lewin/games.pdf

DISCUSSION ON

The cantor set as a fractal and its application

The University of Burdwan

Project Work Submitted For The B.SC. Semester *VI* (Honours) Examination in Mathematics

2023

Under the supervision of:

Shampa Dutta

By

Soumyadeep Ghosh

ROLL NO:200341200023

REGISTRATION NO: 2001048597 OF 2020-21

DEPARTMENT OF MATHEMATICS

………………………………………	………………………………………	………………………………………
Signature of the Student	*Signature of the Teacher*	*Signature of the H.O.D*

Acknowledgement

I am grateful to Mrs. Shampa Dutta, State Aided College Teacher, Department of Mathematics, Sarat Centenary College, The University of Burdwan under whose supervision the project work have been carried out. I am grateful to all the teachers including the HOD of Mathematics, Sarat Centenary College for their constant support throughout the work. I am thankful to the authors of various reference books which have been consulted during the preparation of this project work. Finally I express my sincere gratitude to all staff members of the office, library of our college and infrastructural support provided by the department.

Date: --

Name of the Student

CERTIFICATE

This is to certify that **Soumyadeep Ghosh** has worked out the project work entitled **“The Cantor Set As a Fractal And Its Artistic Application”** under my supervision. In my opinion the work is worthy of consideration for partial fulfilment of his B.Sc. degree in Mathematics.

Date ---

Signature of the Teacher

CONTENTS

The Cantor Set as a Fractal and its Artistic Applications

Abstract

The Cantor middle-thirds set is an interesting set that possesses various, sometimes surprising math- ematical properties. It can be presented through ternary representation and obtained through an iterative process. This paper will discuss selected topological properties of the Cantor set, as well as its connection to fractal geometry. It will then discuss the existence of the Cantor set in a variety of artistic contexts.

Introduction

Georg Cantor (1845-1918) was a German mathematician and the creator of transfinite set theory (Dauben 1). Cantor's work was often regarded as controversial, partially because of the use of infinity in his mathematics (Dauben 1). He was also the first to publish the traditional middle-thirds set, which we refer to as the Cantor set. Though the Cantor set was an abstract concept at the time of its publication in 1883, Cantor explored many of its deep mathematical qualities. The Cantor set is a fractal and can be achieved through use of dynamical systems. The problem of the dynamics of iteration and fractals was briefly explored in the early 19th century, but it was not until the use of computers that it was developed in more depth (Mandelbrot 23). Here, we will discuss some of the topological properties of the Cantor set. We will consider the Cantor set as both a one-dimensional and two-dimensional dynamical system. Lastly, we will discuss the Cantor set as a fractal.

Benoit Mandelbrot developed fractal geometry in the 1970's. He referred to his math as a new "geometric language" (Mandelbrot 21). People were slow to accept the new mathematical concept of fractals, but eventually Mandelbrot published a paper about his findings (Mandelbrot 22). Mandelbrot considered fractals to be artistic objects. Here, we will discuss the connection between the Cantor set fractal and art. We can find resemblance to fractals, particularly the Cantor set, in many artistic contexts. We will focus on its presence in architecture and Chinese art. These connections to art make a fascinating topic in mathematics applicable in a non-scientific context.

The Cantor Middle-Thirds Set

The traditional Cantor middle-thirds set is constructed through an iterative process. Beginning with

the closed set [0, 1], the open middle third (1/3, 2/3) is removed. Two closed sets remain. The middlethird is then removed from each of these sets, namely the intervals (1/9, 2/9) and (7/9, 8/9) repeated infinitely many times, and the set that remains is the Cantor middle-thirds set. More formally,consider the sets $I_0, I_1, I_2 \ldots$,where

$$I_0 = I = [0,1]$$

$$I_1 = I \setminus (1/3, 2/3)$$

$$I_2 = I_1 \setminus (1/9, 2/9) \cup (7/9,8/9)\ldots$$

We define the Cantor set to be $C = \bigcap_{k=0}^{\infty} I_k$, or the intersection of $I_0, I_1, I_2 \ldots$ we can illustrate C by depicting each iteration of removing middle-thirds on a separate line (Figure 1).

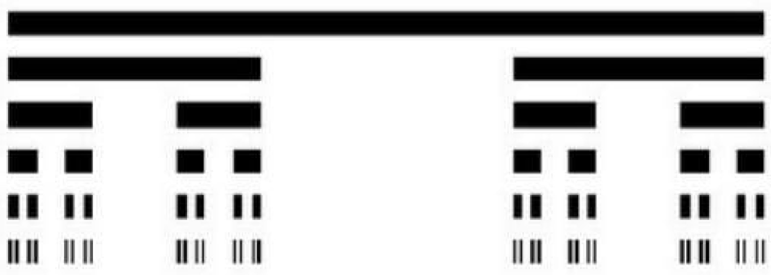


Figure 1: Typical representation of the Cantor Set, Tex Stack Exchange.

After the first iteration, the Cantor set consists of two disjoint intervals of length 1/3. After the second iteration, the Cantor set consists of 4 disjoint intervals of length 1/9. At the kth iteration, the Cantor set consists of 2^k intervals of length $1/3^k$.

Proof. Proceeding by induction, we consider $I_0 = [0, 1]$:

$$\frac{1}{3^0} = \frac{1}{1} = 1.$$

At this iteration, C has $2^0 = 1$ interval. Now, assume that the set I_k has 2^k disjoint intervals of length

$1/3^k$. If we remove the middle third from an interval, each subinterval will be one-third the length of

the original interval:

$$\frac{1}{3^k} \cdot \frac{1}{3} = \frac{1}{3^{k+1}}.$$

Also, the 2^k intervals are all split into two intervals :

$$2^k \cdot 2 = 2^{k+1}$$

By induction, I^k consists of 2^k disjoint intervals of length $1/3^k$.We have described the classic middle-thirds Cantor set. However, note that any set that is constructed by an iterative process of removal of some constant portion of the set can be considered a Cantor set.

Topological Properties

Ternary Representation

The Cantor middle-thirds set can be expressed through ternary representations. Recall that a geometric

Series $\sum_{i=0}^{\infty} a^i = 1 + a + a^2 + a^3 \ldots$ converges absolutely to $\frac{1}{1\text{-a}}$ if |a|<1 consider the series $\sum_{i=1}^{\infty} \frac{s_i}{3_i}$.

Suppose that each s_i is either 0; 1 or 2. Then the series $\sum_{i=1}^{\infty} \frac{s_i}{3_i}$ is dominated by the convergent geometric

Series $\sum_{i=1}^{\infty} \frac{2}{3_i}$. Thus, by the Comparison Test, $\sum_{i=1}^{\infty} \frac{s_i}{3_i}$ converges and 0 ≤ $\sum_{i=1}^{\infty} \frac{s_i}{3_i}$ ≤1.

Ternary Expansion

We call 0:$s_1s_2s_3$... the ternary expansion of x if x = $\sum_{i=1}^{\infty} \frac{s_i}{3_i}$, where each s_i is either 0; 1 or 2.

We claim that every x 2 [0; 1] has a ternary expansion. Let s_1 be the largest among 0; 1; 2 for which

s. Then, pick the largest s_2 for which $x - \frac{s_1}{3} \geq \frac{s_2}{3^2}$ Proceed inductively to get the largest s_n for which $x - \sum_{i=1}^{n-1} \frac{s_i}{3_i} \geq \frac{s_n}{3^n}$. Then note that $x - \sum_{i=1}^{n-1} \frac{s_i}{3_i} \leq \frac{1}{3^n}$ and so, we see that the infinite series $\sum_{i=1}^{\infty} \frac{s_i}{3_i}$ will converge to x.

We claim that each point x of the Cantor set can be represented as a ternary expansion 0.$s_1s_2s_3$... where each s_i is 0 or 2. If x has a ternary expansion for which some s_i = 1, then x lies in a middle third interval that has been removed. This is because x would be past the left third interval, but it would not yet reach the right third interval. For example, if s_1 = 1, x ≠1/3 will be greater than 1/3=.1, but it will not yet reach 2/3=.2, placing it in a middle third. This idea can be applied to any s_i. Thus, no Cantor set element ternary expansion contains a 1, excluding the endpoints, which may have a 1 as the right-most digit of their ternary expansion. In this case, x has an alternative expansion that contains no 1's. For example, the ternary representation for 1/3 is .1 and is equivalent to the representation .0222....So, we can consider the Cantor set to be the set of real numbers in the unit interval [0, 1] with ternary 0representations containing only 0's and 2's.

Similarly, we can represent any x in [0, 1] by a binary expansion $\sum_{i=1}^{\alpha} \frac{s_i}{2_i}$ consisting of 0's and 1's. We will

use this expansion in the next section.

Uncountable

When we consider the construction of the Cantor set, it seems like we "throw out" most points of the unit interval. Intuitively, we would think that *C* should be a small set. The fact that the Cantor set is actually uncountable is one of the surprising topological properties of the set. We will prove this here:

Proof. If x is in the Cantor set, it has a unique ternary expansion using only 0's and 2's. By changing every 2 in the expansion of x to a 1, the ternary expansions of the Cantor set can be mapped to binary expansions, which have a one-to-one correspondence with the unit interval. This can also be done in the opposite direction to map binary expansions to ternary expansions. The only exceptions to this correspondence are the binary expansions ending in infinitely many 0's or 1's and the ternary expansions ending in infinitely many 0's or 2's. However, these exceptions are countable because there are finitely many ways to begin a binary representation before ending in an infinite string of 0's or 1's, and there are finitely many ways to begin a ternary representation before ending in an infinite string of 0's or 2's. Thus, there is a one-to-one correspondence between the binary and ternary exceptions. Since each real number in [0, 1] can be represented as a binary expansion, the Cantor set has a one-to-one correspondence with the unit interval. Now, [0, 1] is uncountable, and so the Cantor set is uncountable.

Closed, Perfect, and Compact

Here, we will discuss why the Cantor set is closed, perfect, and compact. By construction, each I_k is

closed because it is the complement of an open set. Thus, $\bigcap_{k=0}^{\infty} I_k$ is closed because the intersection of closed sets is also closed. Therefore, the Cantor set is a closed set. We will now see that the Cantor set

is perfect.

Isolated Point point x in set S is an isolated point if €-ball B(x,€) surrounding x does not contain another point in S.

Perfect Set S is perfect if it contains no isolated points.

We claim that the Cantor set is perfect.

Proof. Consider x € C. For any €, we have the open ball B(x,€). We can choose k so that $\frac{1}{3_k} < \epsilon 1$ .Let I_k be the union of 2^k disjoint intervals of length $1/3^k$. Then, x € I_k. Let x be in subinterval s € I_k, and then s _ B(x,€). In the k + 1 iteration, s is split into subintervals a and b. Let x be in a. By self-similarity, we know that there must be points of C in b. Thus, there are points of C in B(x€) not equal to x, and x is not an isolated point. Therefore, no point in *C* is an isolated point, and C is perfect.

Now, recall that the unit interval [0; 1] is closed and bounded. Thus, it is compact by the Heine-Borel Theorem (Ross 90). We see that the Cantor set is compact because every closed subset of a compact

space is compact (Willard 119). We have now shown that the Cantor set is closed, perfect, and compact.

Totally Disconnected

We also can prove that the Cantor set is totally disconnected.

Totally Disconnected A set is totally disconnected if it contains no subintervals.

This is another non-intuitive property of the Cantor set. We have already proved that C is perfect, or has no isolated points. We would then expect the Cantor set to contain subintervals. Here, we will prove

this to be false.

Proof. Consider a; b ∈ C. Recall that I_k consists of finitely many disjoint intervals of length $1/3_k$. We can find k where $\frac{1}{3^k} < |b-a|$. So, if the distance between a and b is more than $1/3_k$, a and b must belong

to different subintervals of I_k. By the construction of I_k, there must be an interval in (a,b) that is not

in I_k. Thus, there exists z =2 I_k with a < z < b. Therefore, I_k does not contain (a; b). Since $C = \bigcap_{k=0}^{\alpha} I_n$
C does not contain any interval (a, b). Thus, C is totally disconnected.
Each of the previously discussed topological properties relate to an important theorem (Willard 217): the Cantor set is the only totally disconnected, perfect, compact metric space (up to homeomorphism).
This is an interesting theorem that requires more complicated topology than we have discussed, so we
will not prove it here.

Homeoporphism.

Defenition A homeomorphism is a continuous bijection between topological spaces that has a continuous inverse [3]. Homeomorphism is an important concept in topology, since it expresses a notion of topological equivalence. Thus, two sets which are homeomorphic share many topological properties.
Theorem All Cantor sets are homeomorphic to each other.
Proof. Given two Cantor sets C and C′ on the unit interval, suppose they are constructed by the intersection of $C_0, C_1, C_2 \ldots$ and $C'_0, C'_1, C'_2 \ldots$ let f_0 be the linear map bijection from C_0 to C'_0, both of which are entire intervals, sending endpoint to endpoint. $f_0(x)$ is continuous within its domain. Similarly, as shown in figure 3, let f_1 be the combination of linear map from the left interval of C_1 to left interval C'_1, and likewise for the right intervals..., and let f_k analogue for the kth sets. All these maps are continuous, because they are continuous on disjoint closed intervals.
Figure 3.

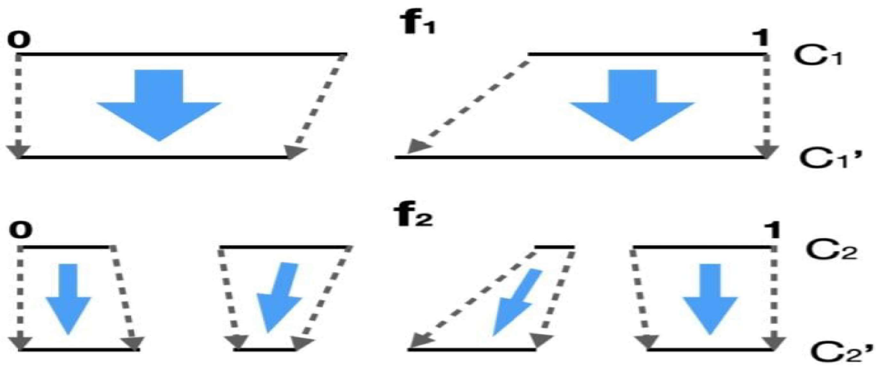


FIGURE 3. Examples of the maps

Now, define g_k as the restriction of f_k that maps only C to C_k. Since the domain C is a subset of all C_k for k ∈ **N,** we derive that g_k is continuous for all k > N. We want to show that these g_k converge uniformly to some map g. The range of g will have to be the intersection of all C'_k, so C′.
Denote M_k as the one among 2_k intervals of C'_k with the maximum length.
Since the Cantor sets are always nowhere dense, we deduce that $\lim_{k \to \infty} M_k = 0$.
Specifically, if the value of $\lim_{k \to \infty} M_k = 0$ is positive, then a subset of the Cantor set contains at least one interval, contradicting that its closure has empty interior.
Now denote N_k as the supremum of $|g_k - g_m|$ on the entire unit interval for any m > k. Therefore, given ∈> 0, there always exists K such that for all k > K,
$|g_k - g_m| \leq N_k \leq M_k < \in$ for all x 2 C and m > k. The sequence is Cauchy in the uniform norm, so it uniformly converges to the desired function g.
We have successfully shown that g_n converge uniformly to g. g is, therefore, a continuous map from C to C′. By the same token, we are able to construct a continuous map from C′ to C by simply reversing the positions of C and C′ and keeping all other aspects of our argument the same.
As a result, in order for there to be a continuous bijection between C and C′,

we only need to prove that the map from C to C′ is bijective. In fact, each element in C and C′ can be considered as an infinite sequence of L and R, where L stands for choosing the left interval and R stands for choosing the right interval in a given iteration. A bijective map between a point in C and one in C′ can be established if they have identical L/R sequences, but it is easy to see that g_k gives these identical sequences for the first k L/R choices, so g itself gives the desired mapping for all of the infinitely many L/R choices.
Therefore, we have proven that Cantor sets C and C′ are homeomorphic to each other. Since C and C′ can be any arbitrary Cantor sets, we deduce that all the Cantor sets are homeomorphic to each other.

Cantor Set as a Dynamical System

We have discussed the traditional construction of the Cantor set and some of its topological properties.
We can also reach the Cantor set through the use of dynamical systems. We will explore two di_erent ways this can be achieved.

Iterated Function System

The Cantor set can be produced by the iteration of a function system.

Consider the two linear functions (Devaney, 192) from $\mathbf{R}^2 \rightarrow \mathbf{R}^2$:

$$A_0\begin{pmatrix}x\\y\end{pmatrix} = \frac{1}{3}\begin{pmatrix}x\\y\end{pmatrix}$$

$$A_1\begin{pmatrix}x\\y\end{pmatrix} = \frac{1}{3}\begin{pmatrix}x-1\\y\end{pmatrix} + \begin{pmatrix}1\\0\end{pmatrix}$$

We claim that if x is an element of the Cantor set, then this iterated function system will send the point
(x, y) to another point of the form (c, y_1) where c is in the Cantor set. In other words, this system fixes the Cantor set. Recall that the Cantor set consists of all points in the interval [0,1] with ternary expansions containing only 0's and 2's. We see that A_0 shrinks the x-coordinate by 1/3, and its corresponding
ternary representation by .1. For example, consider x = :0022022 ∈ C. A_0 would shrink x by .1 to .00022022. This ternary representation consists of only 0's and 2's, so it is still contained in the Cantor
set. A_1 shrinks the x-coordinate by 1/3 and shifts it by 2/3, or by its ternary representation of :2. For example, A_1 would shift x = .0022022 to .20022022. This ternary representation also consists of only 0's and 2's, so it is still contained in the Cantor set. So, we see that the system of equations A_0, A_1 takes points of the Cantor set back into the Cantor set. These functions, no matter the order they are performed, leave the Cantor set fixed.

The Cantor set is called the attractor of this iterated function system. This means that any point in the plane with any y-coordinate will eventually be “pulled into" the Cantor set when this function system is applied. That is, after enough iterations, every point in the plane will converge to a point (c,0) where c is in the Cantor set. To see this, we consider any number of iterations of A_0 and A_1 in a random order. We can represent this random sequence of choice of A_0 or A_1 by a sequence $(s_1 s_2 s_3 \ldots s_n)$ where each s_i is either 0 or 2 representing the application of A_0 and A_1 respectively. Now let x ∈ **R**, and let x_n be the

result of the applied sequence of A_0 and A_1. We see that:

$$x_n = x.\frac{1}{3^n} + \frac{s_1}{3^{k-1}} + \frac{s_2}{3^{k-2}} + \cdots + \frac{s_n}{3^{k-n}}$$

When we take the limit of x_n as $n \to \infty$, we see that the _rst term $x/3^k$ approaches 0. The remainder of

this expression is of the form $\sum_{i=1}^{\alpha} \frac{s_i}{3_i}$ with each s_i equal to 0 or 2, which we know means it is an element

of the Cantor set. The y-coordinate will be sent to 0. Thus, we see that any point in the plane will converge to a point (c; 0), where c is in the Cantor set, after enough iterations of A_0 and A_1 in a random order.

Iterated Tent Function

We can also produce the Cantor set by a different dynamical system. To illustrate this, we consider the

Tent Function:

$$T(x) = \begin{cases} 3x & \text{if } x \leq 1/2 \\ 3 - 3x & \text{if } x > 1/2 \end{cases}$$

We claim that by iterating this function, the points that are not sent to infinity are exactly the Cantor set.

If $x < 0$, then $T(x) < 0$. At the next iteration of the Tent Function, $T^2(x) = 9x < T(x)$. At the third iteration, $T^3(x) = 27x < T_2(x)$. We see that as $n \to \infty$, $T^{(n)} \to -\infty$ for $x < 0$.

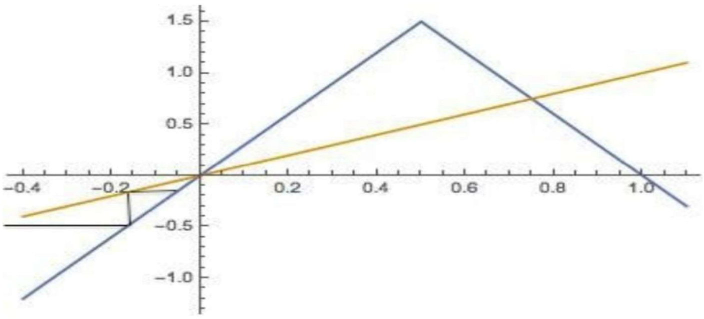


Figure 2: Tent Function, map of point x < 0

Graphically, we trace a point from the tent map to the line y = x. We begin with a graph of the tent function and the function y = x. At an x value outside of our interval [0, 1], we map from y = x to the tent function. At that y value, we map back to y = x. Then, from that x value, we map back to the tent function. By repeating this process, we see that the point we have been mapping goes to negative

infinity. Figure 2 depicts this process for x < 0.

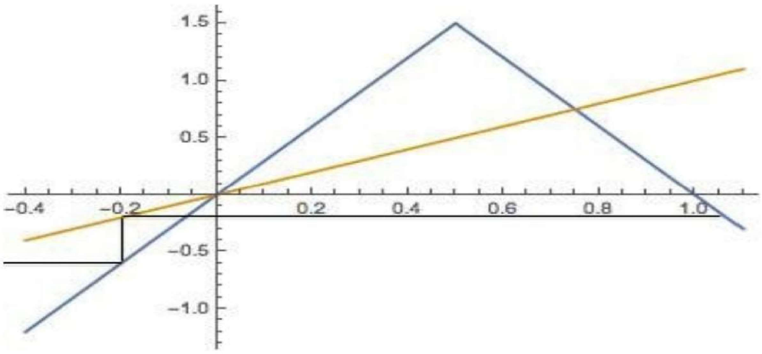


Figure 3: Tent Function, map of point x > 1

If we choose x > 1, after the first iteration T(x) < 0. Recall that as $n \to \infty$, $T^{n}(x) \to -\infty$ for x < 0. Therefore, for x > 1, x is sent to -∞, as depicted in Figure 3. Thus, we find that for $x \notin [0,1]$, x is sent to negative infinity by iterating the Tent Function.

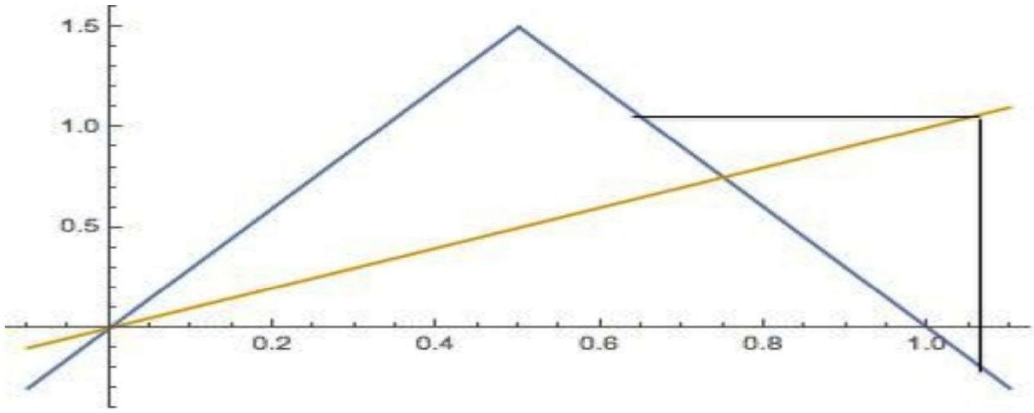


Figure 4: Tent Function, map of point $\frac{1}{3} < x < \frac{2}{3}$

By this same process, we also see that if $x \in (\frac{1}{3},\frac{2}{3})$, then x is sent to infinity (Figure 4). For example, T(1/2)=3/2. We saw above that this is eventually sent to -∞ because x > 1.

In fact, any point in a middle third will be sent to -∞. For example, if $x \in (\frac{1}{9},\frac{2}{9})$ then it is sent to $(\frac{1}{3},\frac{2}{3})$ in one iteration of the Tent Function, which we discussed above. This is supported algebraically: if 1/9 < 2/9 then 1/3 < T(x) = 3x <2/3. This is true for any x in a middle third interval.

Any point that is in the Cantor set, with the exception of the endpoints, will be sent back to itself after enough iterations of the Tent Function. We will not provide a formal argument for this, but we will explore an example. Consider 3/13, which is not an endpoint. Now, we will see that 3/13 is sent back to itself after three iterations of the Tent Function:

$$T(\frac{3}{13}) = 3(\frac{3}{13}) = \frac{9}{13}$$

$$T^2\left(\frac{3}{13}\right) = 3\text{-}3\left(\frac{9}{13}\right) = \frac{12}{13}$$

$$T^3\left(\frac{3}{13}\right) = 3 - 3\left(\frac{12}{13}\right) = \frac{3}{13}$$

The ternary representation of 3/13 is :02002...., which confirms that it is in the Cantor set.

We also see that at the x values 0 and 3/4, there is no line to be mapped graphically. These points are where the tent function and x = y intersect, and are called fixed points. This is supported algebraically:

$$3(0) = 0$$

$$3 - 3\left(\frac{3}{4}\right) = \frac{3}{4}$$

If we consider the endpoints of the Cantor set intervals, we find that they eventually are attracted to the fixed point 0. These are called *eventual fixed points*. For example, endpoint 1=3 is attracted to the fixed point 0 after the second iteration of the Tent Function:

$T\left(\frac{1}{3}\right) = 3\left(\frac{1}{3}\right) = 1$

We will now prove that each endpoint is an eventual fixed point and is sent to 0:

Proof. All endpoints of the Cantor set are of the form $\sum^n$

3_k because they must be rational. Recall that

the endpoints can contain a 1 in the right-most digit place, but these can be rewritten in terms of 2's. That is, $s_n = 1$ is possible if x is an endpoint. If $s_1 = 0$ then T(x) = 3x. This shifts the left-most ternary digit left by 1. If $s_1 = 2$, then $T(x) = 3\text{-}3x = 3\text{-}2.s_2s_3...s_n = 3\text{-}(2+.s_2s_3...s_n) = 1\text{-}.s_2s_3...s_n$. We see that $T(1 - .s_2s_3...s_n) = T(.s_2s_3...s_n)$ because T(x) is symmetrical about the line x = 1/2. We can repeat this process until we reach s_n. If $s_n = 0$ or 2, then we repeat one last time, and we reach 0. If $s_n = 1$, we apply T(x) again and reach 1, which is sent to 0 by another iteration of T(x). Thus, We see that the endpoints are eventually sent to the fixed point 0.

Here, we see an example of this process. Consider the endpoint 7/9=.21.

$$3(.21) = 2{:}1$$

T(.21) = 3 - 2:1 = 3 - (2 + .1) = 1 -.1

T(1 -.1) = T(.1) = 1

T(1) = 3 -3(1) = 0

We see that the endpoints are eventually sent to the fixed point 0. The endpoints are not sent to infinity, which means they are part of the Cantor set. This correlates with our analysis of their ternary representations in Section 2.1.

Iterating the Tent Function sends all points of C back to themselves or to a fixed point. Thus, we see that iterating the Tent Function fixes exactly the Cantor set.

The Cantor Set is a Fractal

The classic Cantor middle-thirds set is a mathematical object called a fractal.

Fractal A fractal is a subset of R_n that exhibits self-similarity on all scales and has fractal dimension. A fractal does not necessarily have topological dimension.

Informally, self-similarity means that we can apply a rescaling function to the set and the image of the set will look the same. Benoit Mandelbrot provided an informal definition of a fractal: \Fractals are geometric shapes that are equally complex in their details as in their overall form. That is, if a piece of a fractal is suitably magnfied to become of the same size as the whole, it should look like the whole,

either exactly, or perhaps only after a slight limited deformation" (Mandelbrot 22). We can see that the Cantor set is self-similar by examining C at a different scale. Recall that I_1 consists of two intervals of length 1=3. If we magnify one of these subintervals by 3 and continue the process of removing the middle

third, we see that we have an exact copy of the full-scale Cantor set.

3.4 Fractal Dimension

We will now discuss the difference between fractal and topological dimension. The type of dimension that

we are most familiar with is topological dimension. A point is of dimension 0, a line is one-dimensional,
a square is two-dimensional, and a cube is three-dimensional. Logically, we understand these dimensions
as the number of "linearly independent" directions we can move along an object (Devaney 185). For example, we can move along the length and width of a square, so we understand it to be two-dimensional.
We define topological dimension here:

Topological Dimension k

An open set S has topological dimension k if each point in S has an arbitrarily small neighborhood homeomorphic to $\mathbf{R}^k$ (Devaney 186).

For example, an open square has topological dimension 2 because the points in a square have arbitrarily
small neighborhoods that are two-dimensional.
Notice this applies when k = 0. In that case, every point in the set has a neighborhood that is homeomorphic to a zero-dimensional object, such as a point. For example, a discrete set has dimension 0.

It remains to show that the Cantor set has fractal dimension. Finding the dimension of the Cantor set is more complicated then finding the dimension of simpler objects. We proved that *C* contains no subintervals. This implies that the Cantor set contains no point with a neighborhood that is homeomorphic
to $\mathbf{R}^1$. Thus, the Cantor set is not one-dimensional. However, *C* is also perfect and contains no isolated points, so it does not have dimension 0. Therefore, the Cantor set has dimension in between 0 and 1. We can think of the Cantor set as somewhere in the middle of unconnected isolated points and pieces of
straight lines (Peak, Frame 92). At every scale, *C* appears to be linear stretches, though we know that each of these stretches is broken up at the next iteration (Peak, Frame 92). To consider the dimension of the Cantor set, we must define a new type of dimension: fractal dimension. First, we must note that only sets that are affinely self-similar have a well-defined fractal dimension (Devaney 186).

Affine Self-similar

A set *S* is called affine self-similar if *S* can be subdivided into k congruent subsets,
each of which may be magnified by a constant factor *M* to yield a whole set *S* (Devaney 187).

As we discussed in Section 3.3, the Cantor set is affine self-similar.

Fractal Dimension

Suppose the affine self-similar set *S* may be subdivided into k congruent pieces,
each of which may be magnified by a factor of *M* to yield the whole set *S*. Then, the fractal dimension *D* of *S* is (Devaney 188):

$$D = \frac{logk}{logM}$$

To understand fractal dimension, first we consider a square. We see that if we break the square into pieces that are 1/n the size of the original square, we need n^2 pieces to reassemble the square. The fractal dimension of a square is (Devaney 189):

$$D = \frac{logn^2}{logn} = \frac{2logn}{logn} = 2$$

We see that the topological and fractal dimensions of the square are equal.

The Cantor set has a well-defined fractal dimension. The Cantor set has 2^n intervals and a

magnification
factor of 3^n at any stage, so the fractal dimension of C is (Devaney 190):

$$D = \frac{log2^n}{log3^n} = \frac{nlog2}{nlog3} = 0.6309...$$

As we predicted, the dimension of the Cantor set is between 0 and 1. The Cantor set does not have topological dimension, but it does have a well-defined fractal dimension. This shows that the Cantor set
is indeed a fractal.

Applications in measure theory

The measure of Cantor sets.
Definition of Lebesgue measure. Now that we have discussed the topological properties of Cantor sets, it is fundamental question also to ask how "big" they are. This idea is trivial for finitely many disjoint intervals just add up the lengths - yet in the infinite case is somewhat more complicated. The concept of the Lebesgue measure, one particularly useful type of measure in mathematics, is basically the total length of the shortest possible intervals that encapsulate a given subset. A full discussion of this measure is beyond the scope of this paper, but it success to note that it gives a more rigorous notion of size to sets.
The Lebesgue measure on R satisfy the following properties:

1. m(A) ≥ 0
2. m(Ø) = 0
3. m([a,b]) = b − a
4. It is countably additive. Namely, for all countable collections $\{E_k\}\infty$ of pairwise disjoint sets in ∑,

$$\left(\bigcup_{k=1}^{\infty} E_k\right) = \sum_{k=1}^{\infty} m\left(E_k\right)$$

As an immediate consequence of properties 1 and 4, if A Type equation here. B then m(A) ≤ m(B).
It is easy to check that this consequence along with property 3 implies that points have measure 0, and in fact, countable sets also have measure 0. We can also calculate the measure of the standard Cantor set.

The standard Cantor set. Since we remove the middle 1/3 of each remaining interval in each iteration, the Lebesgue measure of C_n is $(2=3)_n$ (2_n intervals each of length 3 $_n$). Each C_n contains C, so the measure of C is no larger than that of any C_n. Taking the limit of it as n goes to infinity gives us zero, which is a fairly counterintuitive result: countable sets all have measure zero, but the Cantor set gives an example of a set that is uncountable and also measure zero.
Now, generalizing the standard Cantor set can lead to even more counter-intuitive results. We begin with a theorem.

Theorem . There exists a nowhere dense set with positive measure.
This theorem can be illustrated by the following category of Cantor sets.
3.1.3. Fat Cantor sets. Instead of removing a constant portion of the original set in each iteration, fat Cantor sets are created by removing progressively smaller portions of the original set in each step such that the ratio of what is being removed to the interval it is being removed from goes to 0 as n goes to infinity.
Ex: remove the middle $(1=k)^n$ of C_{n-1}, where k > 3.

Figure 4. Example of a fat Cantor set

Unlike the standard ternary cantor sets, these fat Cantor sets have a positive measure, which is odd because they are nowhere dense and don't contain even one interval. Take the example mentioned earlier that removes the middle intervals of lengths $(1=k)^n$ from C_{n-1}, k > 3.

The Lebesgue measure of the removed intervals

$$
\begin{aligned}
&= 1/k + (1/k)^2 * 2 + (1/k)^3 * 4 + ... \\
&= 1/2 * (2/k + (2/k)^2 + (2/k)^3 + ...) \\
&= 1/2 * 2/k * 1/(1 - 2/k) \\
&= (1/k) * (k/k - 2) \\
&= 1/(k - 2).
\end{aligned}
$$

Therefore, the Lebesgue measure of the corresponding fat Cantor set is (k-3)=(k-2)

An example of the fat Cantor set is the Smith{Volterra{Cantor set (SVC): k = 4 in this case, and its Lebesgue measure is 1=2.

Dimension.

Definition. In mathematics, the notion of fractional dimension, an intrinsic property of a set, is an extension of the idea that a line is one-dimensional, a plane is two-dimensional, and space is three-dimensional. First, let us explore one way to approach how the dimensions of, say, a line segment and a rectangle are defined.

A line segment has dimension 1, because as we stretch it to twice its original length, its 'substance'{length{doubles as well. In the case of a rectangle, if we stretch all sides to twice their original scales, its substance{namely the area{ quadruples. Taking the logarithm of 4 over 2 gives us 2.

Put in an equation, we can write that

$$\frac{S_1}{S_2} = S^D$$

where S_1 is the new substance, S_2 is the old substance, S stands for the stretch, and D is the dimension. The dimension is the exponent by which the size changes when scaled by a certain amount.

As in the two examples above, you might expect that only integer dimensions are taken. As will be shown below, however, the dimension of mathematical objects are not necessarily integers and can take on many arbitrary values.

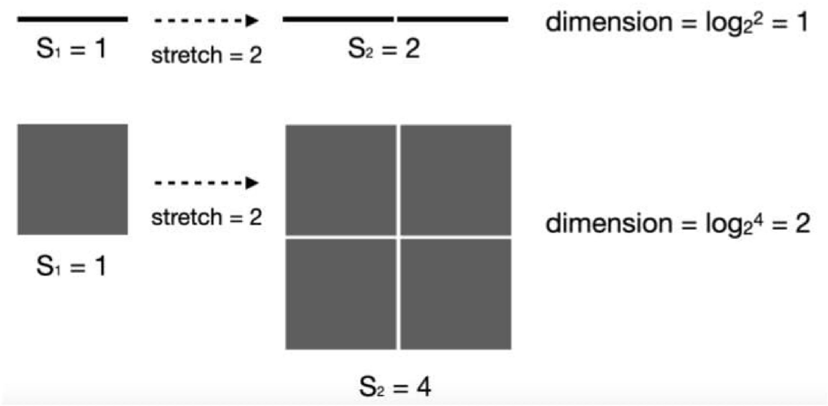


Figure 5. dimensions of line segments and squares

Fractals in Art

Benoit Mandelbrot considered his fractal geometry to be a new form of art (Mandelbrot 21). He claims
fractal geometry as an \art for the sake of science," and refers to the fractal as a useful beauty (Mandelbrot
22). Art historians and mathematicians, such as Mandelbrot, have been pondering the connections between the fields of art and mathematics for decades. Here, we will connect the Cantor set to art and
architecture.

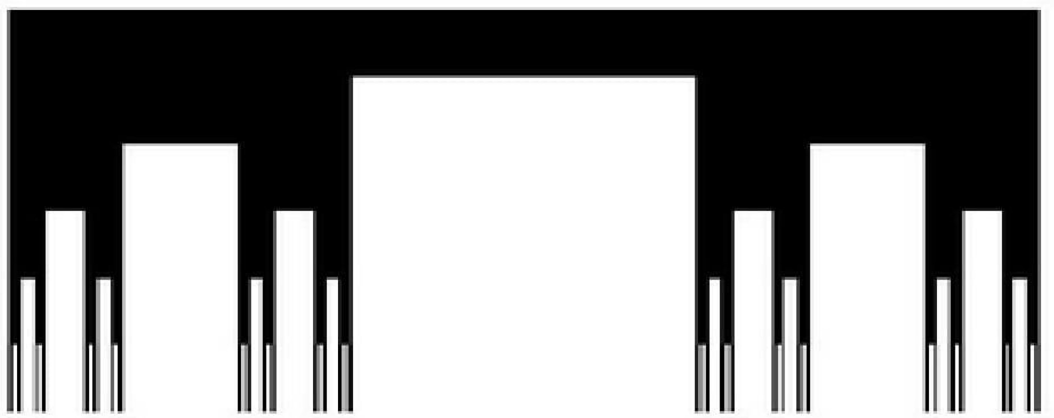


Figure 6: Connected Cantor Set, (Tex Stack Exchange).

Mandelbrot finds the coexistence of order and chaos in the issue of dynamics of iteration beautiful in itself (Mandelbrot 23). He also finds images of fractals artistic. In many cases, the traditional image of a
common fractal is altered to make it more aesthetically pleasing. For example, the representation of the
Cantor set above connects each iteration to the previous iteration. This Connected Cantor set (Figure 6) is more artistic than the usual representation of the set.

This image still represents the Cantor Set. Instead the of the traditional representation that consists of
a set of separated lines, this representation exhibits one continuous object. It is a more organic image, which makes it more aesthetically pleasing. We can find examples in Chinese art and Architecture that
resemble both this Connected Cantor set, as well as the traditional representation of the Cantor set.

Chinese Art

Fractals appear in many pieces of Chinese art. We can even find resemblance to the Cantor set, particularly the Connected Cantor set. Mandelbrot claims that fractals can serve as representations for natural
objects (Mandelbrot 22), and we will apply this idea to Chinese art.

We first turn to the work of Guo Xi (1020-1090), a Chinese artist of the Northern Song dynasty (Bentley).
Guo Xi painted in the black and white monumental landscape rugged style (Murashige 343). The rugged
monumental landscape style originated in the previous Five Dynasties period and was initiated by painter
Li Cheng (Bentley). It featured \crab-claw," defoliated tree branches. During the Northern Song period, Guo Xi adapted this monumental style, accentuating the crab-claw branches (Bentley). Though Guo's work came long before the Cantor set was discovered, we can find a resemblance to the set in his art.

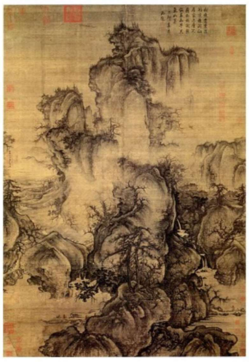


Figure 7: Early Spring, Guo Xi, ink on paper; 1072.

We consider Early Spring, one of Guo Xi's most famous works (Figure 7). This piece, painted in 1072, features the twisting crab-claw branches that the artist was known for (Murashige 343). The branches begin with a thick branch size, and a smaller arm branches o_ from each larger branch. This process is repeated on each smaller branch until the brush stroke becomes too thin to possibly be drawn. This process is reminiscent of the iterative process we use to construct the Cantor set. These branches also
resemble our representation of the Connected Cantor set in Figure 6. This Cantor set representation shows each iteration connected to the next iteration in a branch-like way. The trees in Guo Xi's Early Spring resemble a version of our connected Cantor set in which the branches have been turned and twisted in different directions.

Guo Xi worked in a time where Song neo-Confucianism was the most prominent philosophy accepted by
the people of China. This philosophy influenced both the subject matter and style of the work at the time (Bentley). A major concept explored in this type of neo-Confucianism is li, which means \inner structure." There are three different levels of li : the human level, the natural level, and the heavenly level (Li, Yan 205). The goal of each person is to align her own moral inner structure, which has been corrupted by emotions, with those of nature and heaven (Bentley). These philosophical levels are fractal-
like. The ultimate goal would be for the li to be \self-similar" at each level. The human at the _rst

philosophical level would like to make her inner structure \look" like the the inner structure of the next two levels. No matter the level, li should look the same. In other words, li should be self-similar. The concept of li is defined in a similar way to the way we define a fractal. Thus, even the philosophy behind
Guo Xi's Early Spring resembles a fractal structure.

Figure 8: Seven Junipers, Wen Zhengming; Ming dynasty.

We will also consider Wen Zhengming (1470-1559), a Chinese scholar and painter from the Ming dynasty
(Bentley). His famous Seven Junipers features twisted Juniper tree branches (Figure 8). These branches
share the same resemblance to the Connected Cantor set representation in Figure 6 as those of Guo Xi's trees. This is an even more distorted version of our Connected Cantor set, but it still exhibits the thinning out effect we observed in Early Spring. By examining the works of Guo Xi and Wen Zhengming,
we find a resemblance to the Cantor set. We see that the Cantor set, and fractal structure in general, can be applied in the context of Chinese art.

Architecture

Fractals also appear in architecture. We can find the Cantor set in the patterning of windows or other features on buildings. For example, we look to the AT&T building, now known as the Sony Tower, in New York City (Figure 9). The building was completed in 1984 and was designed by architect Philip Johnson and his partner John Burgee. To find a Cantor set, we consider the pattern of the windows on
the front face of the building.
The top level of windows is in a symmetrical pattern. From the left, there is one medium-width window,
then three large-width windows. The central section of windows contains eight window sections with small widths. The windows on the right side of the central section mimic the pattern of those on the left
side. We will consider the windows themselves as part of our Cantor set and the concrete as the part we remove. At the next level of windows, each large-width window is “split" into four windows. At this iteration of the set, more points, represented by the concrete, have been removed. We can think of the pattern of the windows as a Cantor set. This is an example of a Cantor set that is not the traditional middle-thirds set.

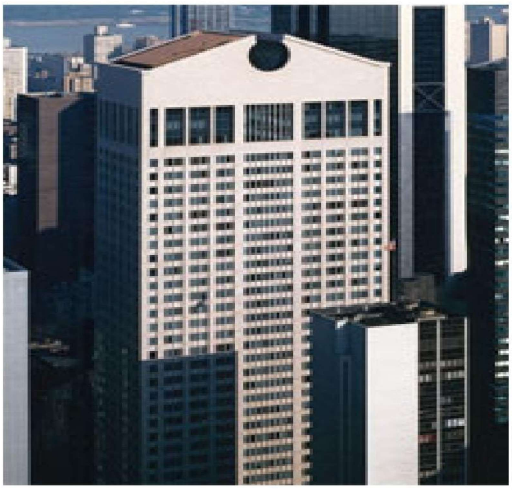


Figure 9: Sony Tower, Philip Johnson and John Burgee, New York City, New York; 1984.

For another depiction of the Cantor set in architecture, we turn to a much older example. We can find the Cantor set in the capitals of Egyptian columns. For example, consider this column capital from the Temple of Dendur from 15 BC, which now resides in the Metropolitan Museum of Art in New York City (Figure 10).

Figure 10: Column Capital from Temple of Dendur, Metropolitan Museum of Art, 15BC.

The capital features bundles of papyrus stalks and lotus leaves, which take the form of a curve. The top
curves are split into two smaller curves by removing a center section. The two smaller curves also shift
away from the center of the larger curve. This process is repeated three times on this particular capital.
This capital resembles a Cantor set in that various intervals of marble are removed through an iterative
process. The Egyptians may have even intentionally used an iterative process to create this motif.

Applications in the real world: fractal phenomena

Because of its self-similar nature, the standard Cantor set is the prototype of a fractal. In fact, a well established mathematical branch, fractal geometry is widely applied to study patterns and phenomena in various aspects of our lives, and in this paper, we picked three examples with the closest relationships to the Cantor sets.

Fractal Geometry in Nature.

Among the numerous fractal structures observed in nature{spirals, tree branches, snow flakes{ Saturn's rings have a special relationship to the Cantor sets.
Note the different sizes in the gaps of Saturn's rings in below , which look like the intervals removed from a Cantor set. The figure on the right consists of the product of fat Cantor set and a circle. The fat Cantor set has positive measure,

Figure:11 Left: Saturn's rings (NASA). Right: a product of a Cantor set and a circle.

specifically provides an interesting comparison with Saturn, because if the rings' cross section were a different Cantor set of zero area, the rings would have almost zero area to reflect light and so would be almost invisible.

Mandelbrot and the Fractal Market.

Compared to unambiguous self- similar patterns in art and nature, the applications of Cantor sets and fractals to the financial world come in a more subtle way. Mathematician Benoit Mandelbrot (1987) once compared markets to turbulent seas in his "Ten Heresies of Finance," where he argues that :" the very heart of finance is fractal." In discussing the applications of fractals to analyzing markets, he states that the simplest fractals scale

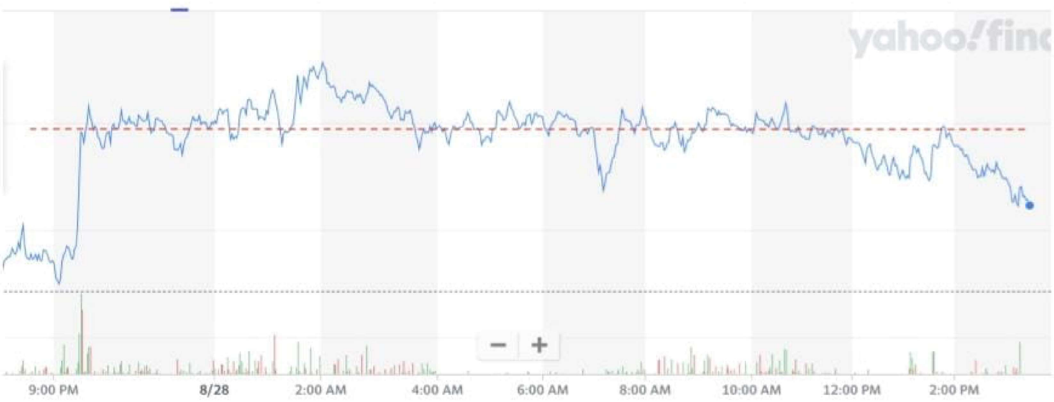


Figure 12:Bitcoin Price, for example, in the past 18 hours, with an estimated Hurst Coeffcient of around 0.4-0.5

the same way in all directions, hence are called self-similar. If the fractals scale in many different ways at different points{the exact reality of the markets ... their mathematical properties become intricate and powerful."
The comparisons with nature lead to idea that financial markets are similar to the behavior of various

natural phenomena in the world. The history of shifts from classical to modern views on the market modeling were

Figure13 : Turbulent sea

outlined, visualizing some misconduct of classical approach to market modeling and providing examples of
utilizing the fractional approach.

The fractal market hypothesis.

An alternative to EMH. For decades, the Efficient Market Hypothesis has been the dominant foundation for the modeling of financial markets. It states that stocks always trade at their fair value on exchanges, making it impossible for investors to purchase undervalued stocks or sell stocks for inflated prices. The core
idea of the Efficient Market Hypothesis lie in the observation that stock prices exhibit random walks, which can be modeled by something called geometric Brownian motion. Modeling with geometric Brownian motion suggests that the percentage change of a stock price in a given future time interval is completely independent of its previous prices. Furthermore, the distribution of the percentage changes after a given time has passed t should be normally distributed, with variance proportional to t. The model of geometric Brownian motion is useful, but not perfect. For instance, one can modify it by adding a "drift" term to capture the reality that stock prices tend to increase over time. A more core issue, though, is the idea of fat tails, which reflect the disproportionate influence of rare events on the economy. The reality of
fat tails has laid the foundation of a new theory { the \Fractal Market Hypothesis".
One of the central arguments in the fractal marker hypothesis is that the frequency distribution of returns looks the same at different investment horizons, which is the total length of time that an investor expects to hold a security or a portfolio. The longer-term horizons are based more upon fundamental information, and shorter-term investors base their views on more technical information. As long as the market maintains this fractal structure, with no characteristic time scale, the market remains stable because each investment horizon provides liquidity to the others.
As a result, the geometric Brownian motion, as a stochastic process to model stock movements in EMH according to the Black{Scholes model, can be potentially replaced by the fractional Brownian motion with a special parameter Hurst coefficient "H". For self-similar time series, H is directly related to fractal dimension, D, where $1 < D < 2$, such that $D = 2 - H$. Increments are independent only when $H = 1/2$, for $H > 1/2$, increments are positively correlated and for $H < 1/2$ they are
negatively correlated. [14]

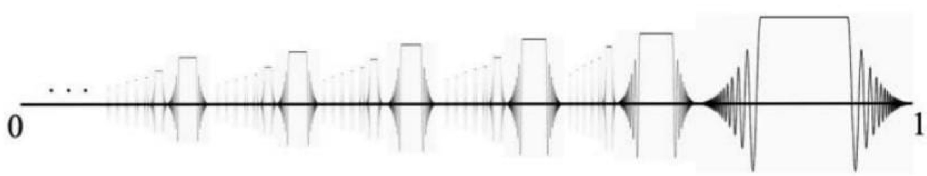


Figure 14. Volterra's Function

The values of the Hurst exponent vary between 0 and 1, with higher values indicating a smoother trend, less volatility, and less roughness.

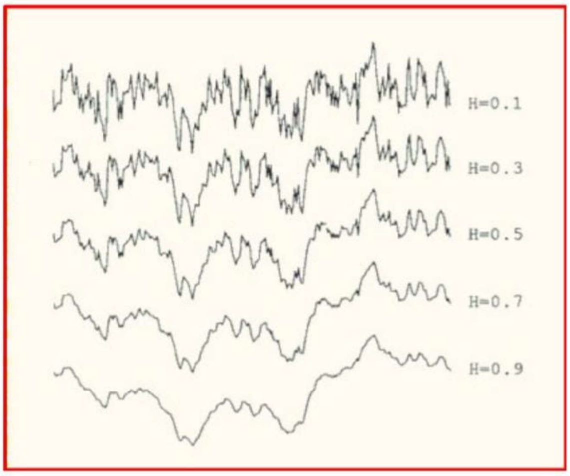


Figure 15. Patterns corresponding to different H coefficients

An intriguing point where Cantor sets come into play is when we observe the level set of a one dimensional fractional Brownian motion mentioned above. Assuming in case of figure 8 that the H index of bitcoin price is around 0.5 (0.495 ± 0.102) according to [11], the chance of the stock price going up or down is close to random.
Therefore, any typical level set (e.g. the red line in figure 7) is a closed, perfect set resulting from the properties of Brownian motions (both fractional and geometric) [12]. Furthermore, the level sets will almost surely not contain any intervals, meaning with the above properties that they must be Cantor sets.

Conclusion

Georg Cantor's classical middle-thirds set exhibits intriguing mathematical properties. We showed that the Cantor set is uncountable, which is surprising because it seems that it should be a small set. We also proved the non-intuitive quality that though the Cantor set contains no subintervals, it also contains no isolated points. We can produce the Cantor set through a two-dimensional system of two functions.
This study revealed the Cantor set as an attractor to an iterated function system. We also considered the Cantor set as a one-dimensional system of points that are not sent to infinity through exploration of the Tent Function. Discussion of the Cantor set as a fractal led us to find that C has a fractal dimension

between 0 and 1.
Benoit Mandelbrot considered his fractal geometry an art form. We considered the Cantor set as an artistic form, with a focus in two different areas. Our Connected Cantor set representation resembles the
trees in works by Chinese painters Guo Xi and Wen Zhengming. We also found a resemblance to this Connected Cantor set in the Song Tower of New York City. Lastly, we considered the column capital of
the Egyptian Temple of Dendur and found a more classic representation of the Cantor set.
We have taken a complex mathematical set and applied it to the world of art. The Cantor set not only proves to be a set with interesting mathematical properties, but also a beautiful mathematical object with multiple applications in an artistic context.

References

"Drawing Cantor Set." Stack Exchange. 25 Feb. 2012. Web. 7 Apr. 2015. http://tex.stackexchange.com/questions/31999/drawing-cantor-set.

Bentley, Tamara. Personal Communication, November 2014.

Dauben, Joseph Warren. *Georg Cantor: His Mathematics and Philosophy of the Infinite. Cambridge*: Harvard University Press, 1979. Print.

Devaney, Robert L. *A First Course in Chaotic Dynamical Systems: Theory and Experiment*. Perseus Books Publishing, LLC., 1992. Print.

Li, Jinglin, and Xin Yan. "The Ontologicalization of the Confucian Concept of `Xin Xing:' Zhou Lianxi's Founding Contribution to the Song-Ming Neo-Confucianism." Frontiers of Philosophy in China 1.2 (2006): 204-21. JSTOR. Web. 7 Apr. 2015. http://www.jstor.org/stable/30209964.

Mandelbrot, Benoit B. "Fractals and an Art for the Sake of Science." Leonardo Supplemental Issue 2 (1989): 21-24. JSTOR.Web. 7 Apr. 2015. http://www.jstor.org/stable/1557938.

Murshige, Stanley. "*Rhythm, Order, Change, and Nature in Guo Xi's Early Spring*." Monumenta Serica 43 (1995): 337-64. JSTOR. Web. 7 Apr. 2015. http://www.jstor.org/stable/40727070.

Peak, David and Michael Frame. *Chaos Under Control: The Art and Science of Complexity.* W.H. Freeman, 1992. Print.

Ross, Kenneth A. Elementary Analysis: *The Theory of Calculus.* Springs Science+Business Media, 2013. Print.

Willard, Steven. *General Topology*. Reading: Addison-Wesley Publishing Company, 1970. Print.

Visual Proof Of Some Selected Inequality And Infinite Series

Project submitted for the B.SC Degree, 6th semester examination in Mathematics 2023

Under the supervision of

Dr. Bidyut Santra

By

Surapriya Samanta

University Roll No. - 2 0 0 3 4 1 2 0 0 0 2 5
University Reg. No. – 202001048599 of 2020-21

Department of Mathematics

Signature of the student

Signature of the teacher

Signature of the H.O.D

ACKNOWLEDGEMENT

I am grateful to ***DR. BIDYUT SANTRA****, Assistant Professor, Department of Mathematics and SARAT CENTENARY COLLEGE, under whose supervision the project work has been carried out. I am grateful to all the teachers including the Head, Department of Mathematics, SARAT CENTENARY COLLEGE for their constant support throughout the work. I am thankful to the authors of various books, Articles and Webpages which have been consulted during the preparation of this project work. Finally, I express my sincere thanks to the staff members of the office, library of our college and infrastructural support provided by the department.*

Date: -

Signature of the student

CERTIFICATE

*This is to certify that Su*rapriya Samanta *has worked out the project work entitled "visu*al proof of some selected inequality and infinite series" *under my supervision. In my opinion the work is worthy of consideration for partial fulfilment of his B.Sc. degree in Mathematics.*

____

Date: -

Signature of the teacher

CONTENT

INTRODUCTION

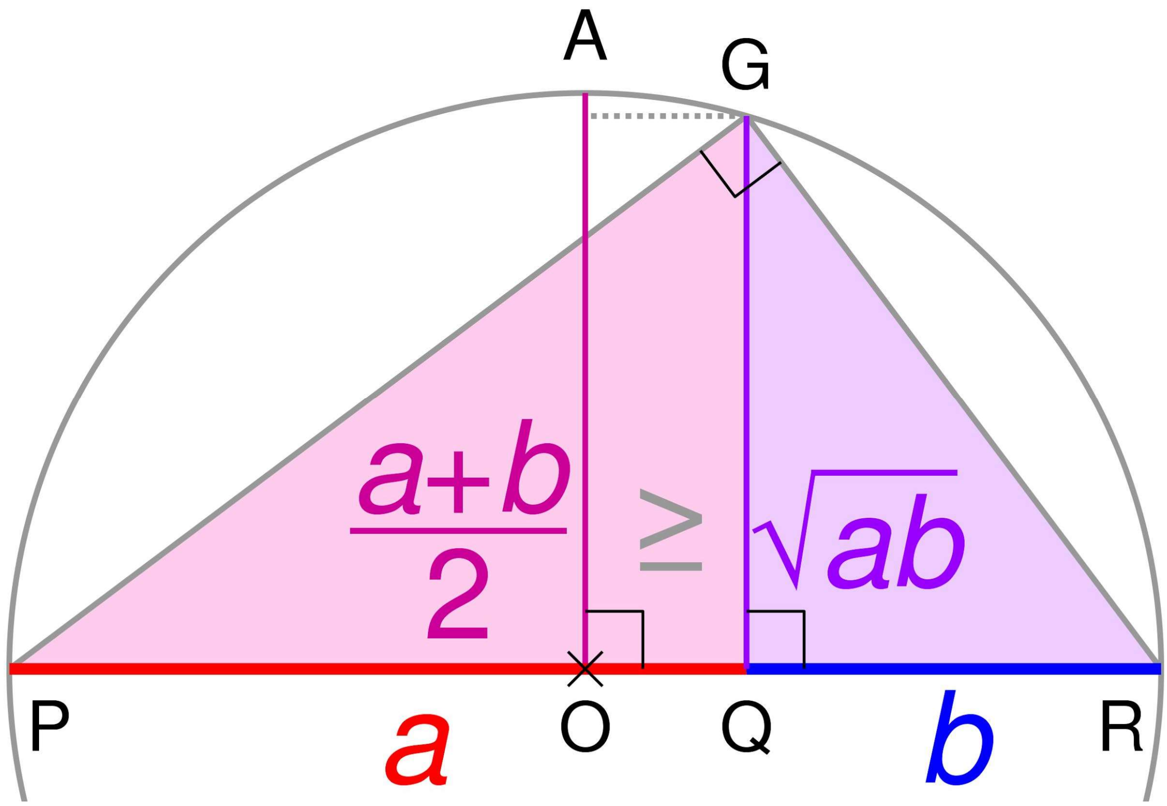
Visual proofs are not really proofs.Its therefore Eisenberg and Tommy Dreyfus note in their paper"on the reluctance to visualise in mathematics",some consider such visual arguments to be of little value,and "that there is one and only one way to communicate mathematics, and visual proofs are not acceptable.But to counter this viewpoint, Eisenberg and Dreyfus go on to give us some quotes on the subject:

(Paul)Halmos, speaking of Solomon Lefschetz stated"He saw mathematics not as logic but as pictures". Speaking of what it takes to be a mathematician,he stated:"To be a scholar of mathematics you must be born with…..the ability to visualise "and must teachers try to develop this ability in their students

So if visual proofs are not proffs,what are they? Generally visual proofs are pictures or diagrams that help the observer see why a particular statement may be true.and also to see how one might begin to go about proving it's true.In some equation or two may appear in order to guide the observer in this process.But the emphasis is clearly on providing visual clues to the observer to stimulate mathematical thoughts.

So, here I presented some inequality and infinite series with visual proofs which helps students to find enjoyment in discovering or rediscovering some elegant visual demonstration of certain mathematical idea,that teachers will want to share many of them with their students and that all will find stimulation and encouragement to try to create new "visual proofs" or "visual proofs of inequality and infinite series "

1. A.M-G.M inequality



Here, Comparing, ΔPGQ and Δ RGQ We get, GQ/b=a/GQ

GQ=√(ab)

Hence complete the proof.

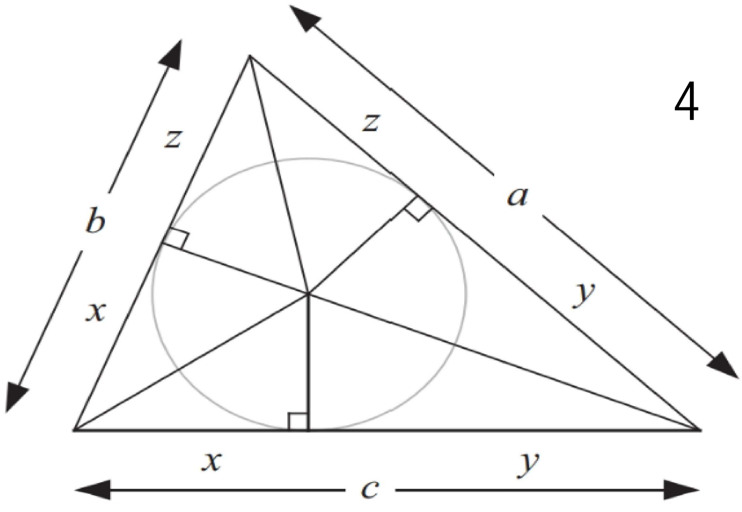
Proof : ab=(a+b)^2/4 - (a-b)^2/4

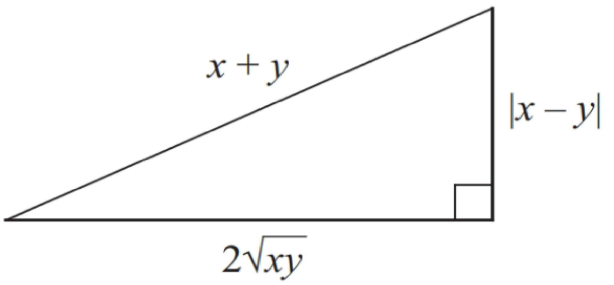
≤(a+b)^2/4

(a+b)/2=√(ab)

Padoa's inequality

$$abc \geq (a+b-c)(b+c-a)(c+a-b).$$





$$\begin{aligned} abc &= (y+z)(z+x)(x+y) \\ &\geq 2\sqrt{yz}\cdot 2\sqrt{zx}\cdot 2\sqrt{xy} \\ &= (2z)(2x)(2y) \\ &= (a+b-c)(b+c-a)(c+a-b). \end{aligned}$$

$$x+y \geq 2\sqrt{xy}.$$

Solution : We have $a^2 \geq a^2-(b-c)^2 = (a+b-c)(a+c-b)$.

Analogously $b^2 \geq (b+a-c)(b+c-a)$ and $c2 \geq (c+a-b)(c+b-a)$.

$$a^2b^2c^2 \geq (a+b-c)^2(b+c-a)2(c+a-b)2$$

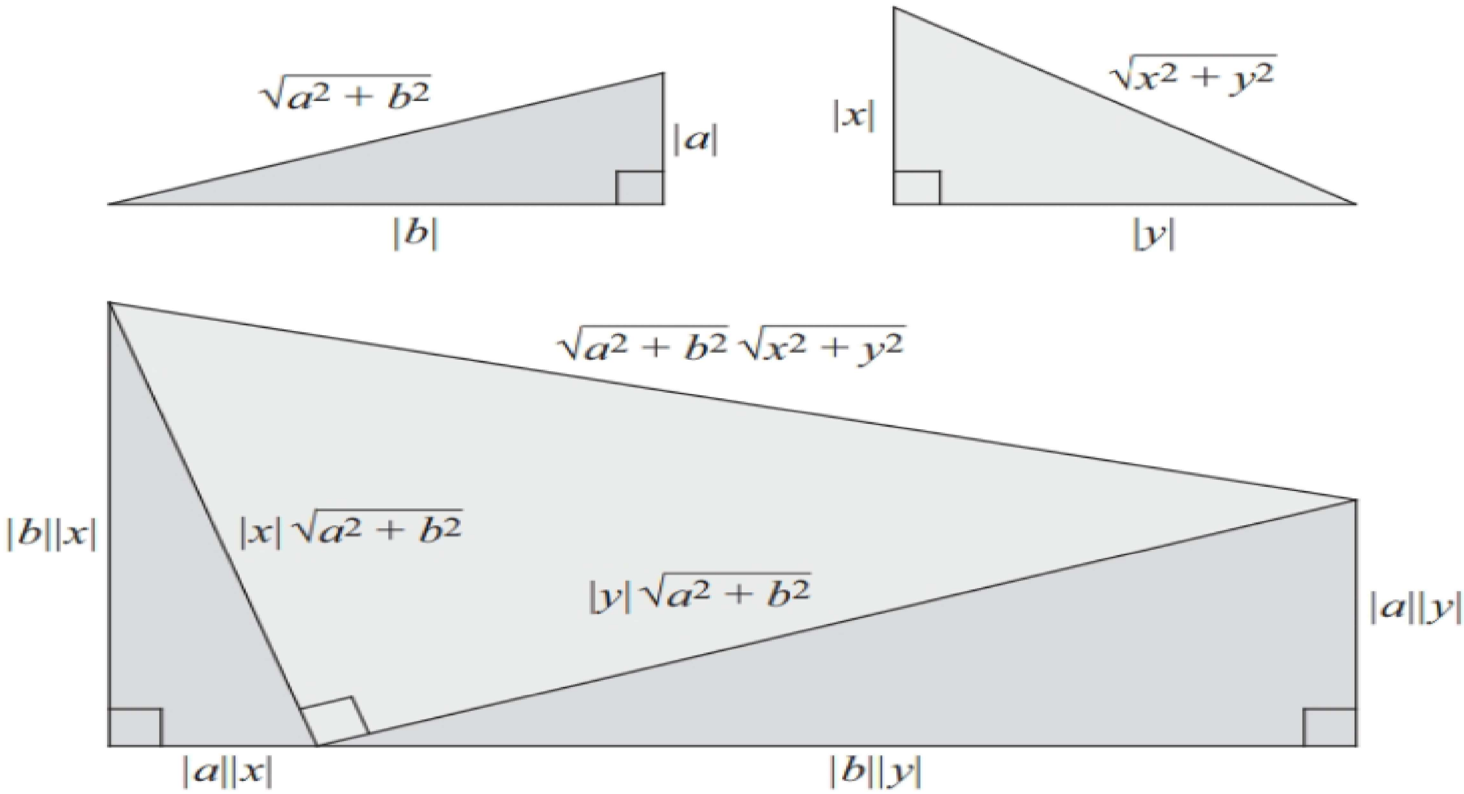
$abc \geq (a+b-c)(b+c-a)(c+a-b)$.

Equality holds if and only if $a = b = c$, i.e.

the triangle is equilateral.

Cauchy Schwartz inequality

$$|ax + by| \leq \sqrt{a^2 + b^2}\sqrt{x^2 + y^2}$$ 5



$$|ax + by| \leq |a|\,|x| + |b|\,|y| \leq \sqrt{a^2 + b^2}\sqrt{x^2 + y^2}.$$

Proof: Let (a,b) and (x,y) be not proportional.

Let us consider the expression

$(a-kx)^2+(b-ky)^2$, where k is real.

For all real k,the expression is greater or equal to zero.

The equality occurs only when a-kx=0,b-ky=0.Let ,

$(a-kx)^2+(b-ky)^2>0$

Or,$(a^2+b^2)-2k(ax+by)+k^2(x^2+y^2)>0$

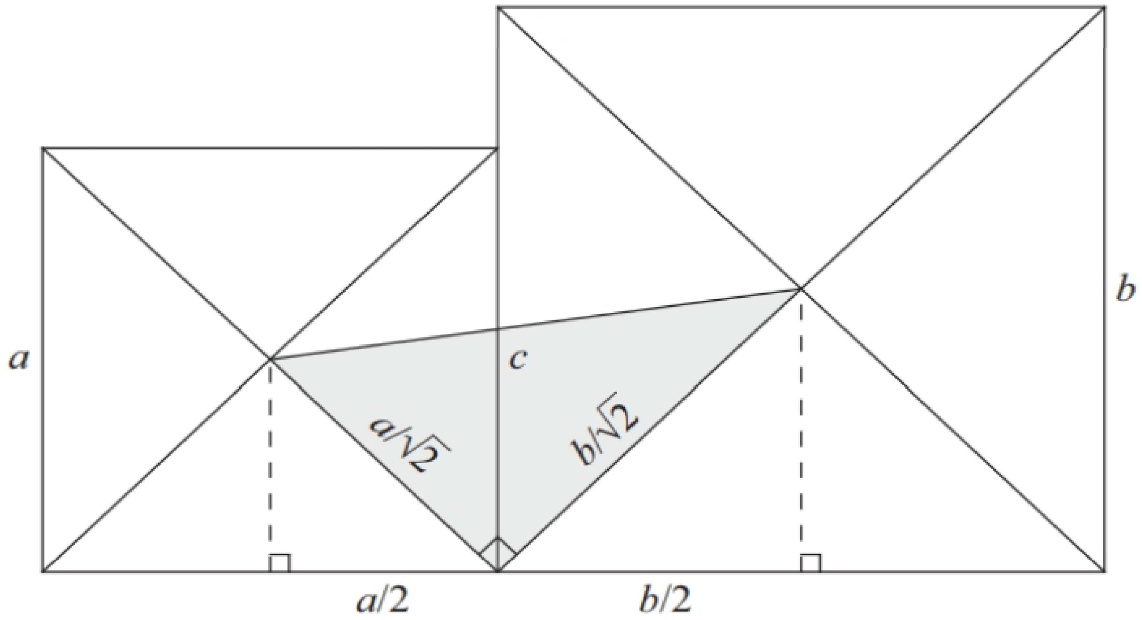
It is obvious that,

$(a^2+b^2)(x^2+y^2)>(ax+by)$

Hence complete the proof.

Arithmetic mean -root mean square inequality

$$a, b \geq 0 \quad \Rightarrow \quad \frac{a+b}{2} \leq \sqrt{\frac{a^2+b^2}{2}}$$



$$c^2 = \left(\frac{a}{\sqrt{2}}\right)^2 + \left(\frac{b}{\sqrt{2}}\right)^2 = \frac{a^2}{2} + \frac{b^2}{2},$$

$$\frac{a}{2} + \frac{b}{2} \leq c \quad \Rightarrow \quad \frac{a+b}{2} \leq \sqrt{\frac{a^2+b^2}{2}}.$$

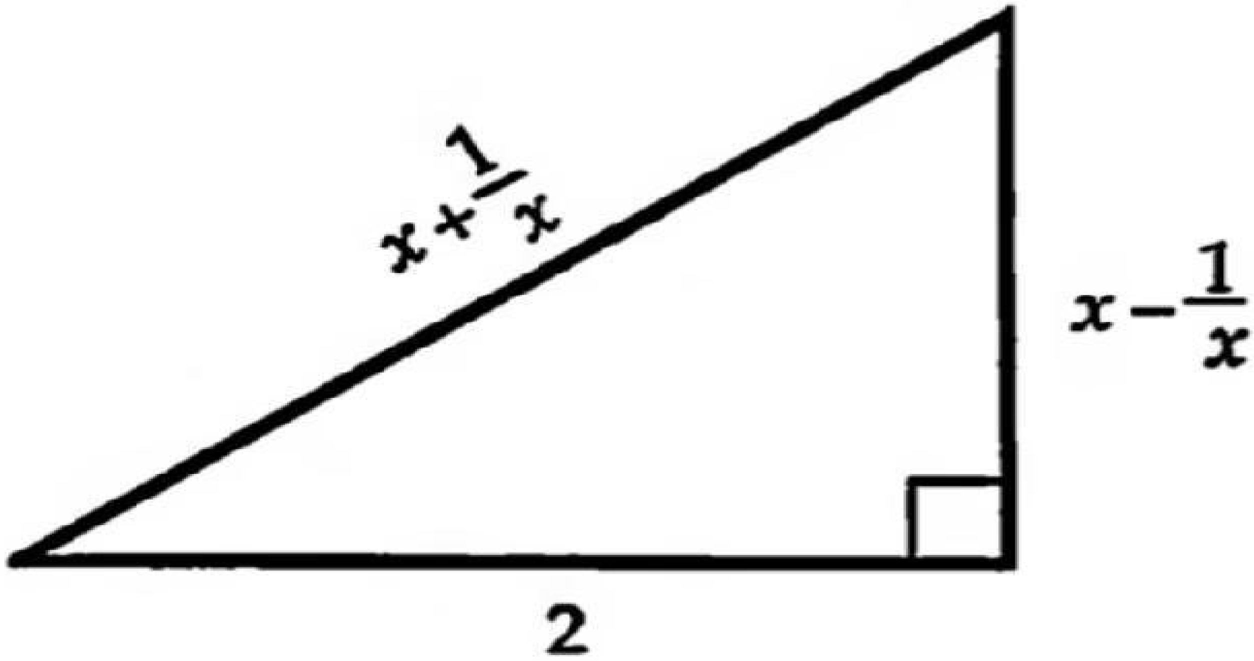
Proof : $(a-b)^2 \geq 0$. $\Leftrightarrow a^2+b^2 \geq 2ab$

$\Leftrightarrow 2(a^2+b^2) \geq a^2+b^2+2ab \Leftrightarrow 2(a2+b^2) \geq (a+b)2 \Leftrightarrow$

$(a^2+b^{2)}/2 \geq (a+b)^2/4$. Hence $(a^2+b^2)/2 \geq (a+b)2/4$.

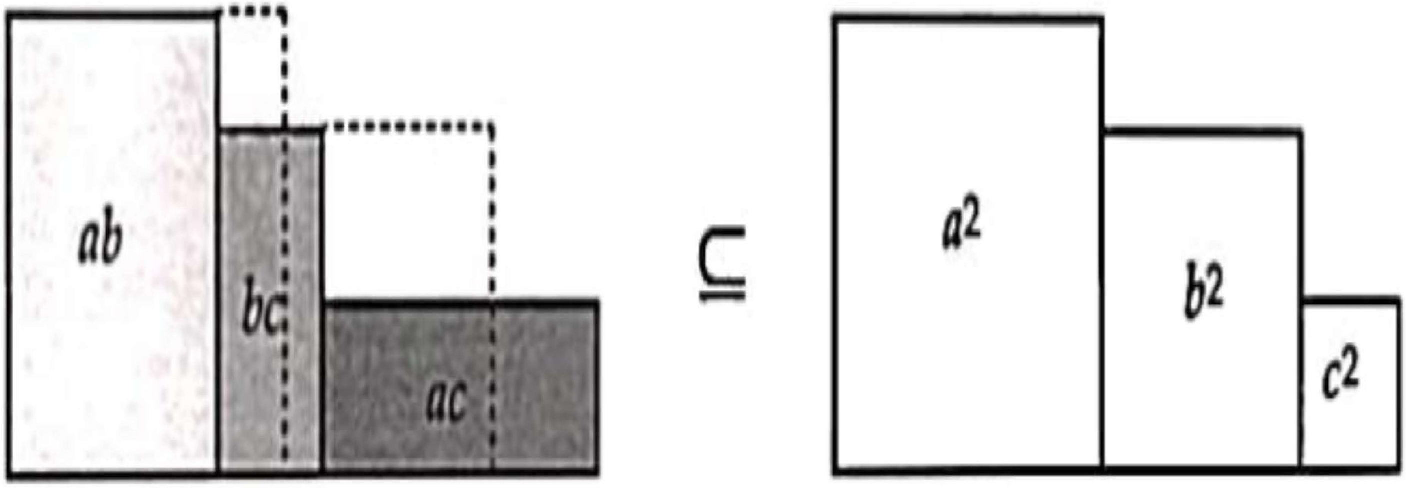
Equality holds if and only if a – b = 0, i.e. a = b.

For Any x>0,then (x+1/x)is greater or equal to 2



Solution From the obvious inequality $(x-1)2 \geq 0$. we have $x^2-2x+1\geq 0 \Leftrightarrow x2+1 \geq 2x$, and since $x>0$ if we divide by x we get the desired inequality. Equality occurs if and only if $x-1=0$, i.e. $x=1$.

LEMMA: $ab+bc+ac \le a^2+b^2+c^2$



$a,b,c \in R$. Prove the inequality

$a^2+b^2+c^2 \ge ab+bc+ca$.

:Since $(a-b)^2+(b-c)2+(c-a)2 \ge 0$. we

$2(a^2+b^2+c^2) \ge 2(ab+bc+ca) \Leftrightarrow a^2+b^2+c^2 \ge ab+bc+ca$. Equality occurs if and only if $a=b=c$.

Infinite series

Let $\{a_n\}$ be a sequence of real numbers.
Then the expression $a_1+a_2+a_3+$.......
Will be called an infinite series.

Geometric Series:
The infinite Geometric Series
$a+ar+ar^2+$..... $(a>0)$ is
(a)convergent if the common ratio r lies between -1and +1.in this case the sum of the series is a/(1 -r)
(b) properly divergent if r is greater or equal to 1.
© Oscillates finitely if r=-1 and Oscillates infinitely if r<-1.
(improperly divergent)
Proof :
$S_n=a(r^n-1)/(r-1)$. r is not equal to 1.
(a)
If n tends to infinite then S=a/(1-r)
(d)

Infinite series

If $r=-1$, we have

$S_n = a-a+a-a+ \ldots\ldots$ to n terms.

If n is odd, then the sum is a,

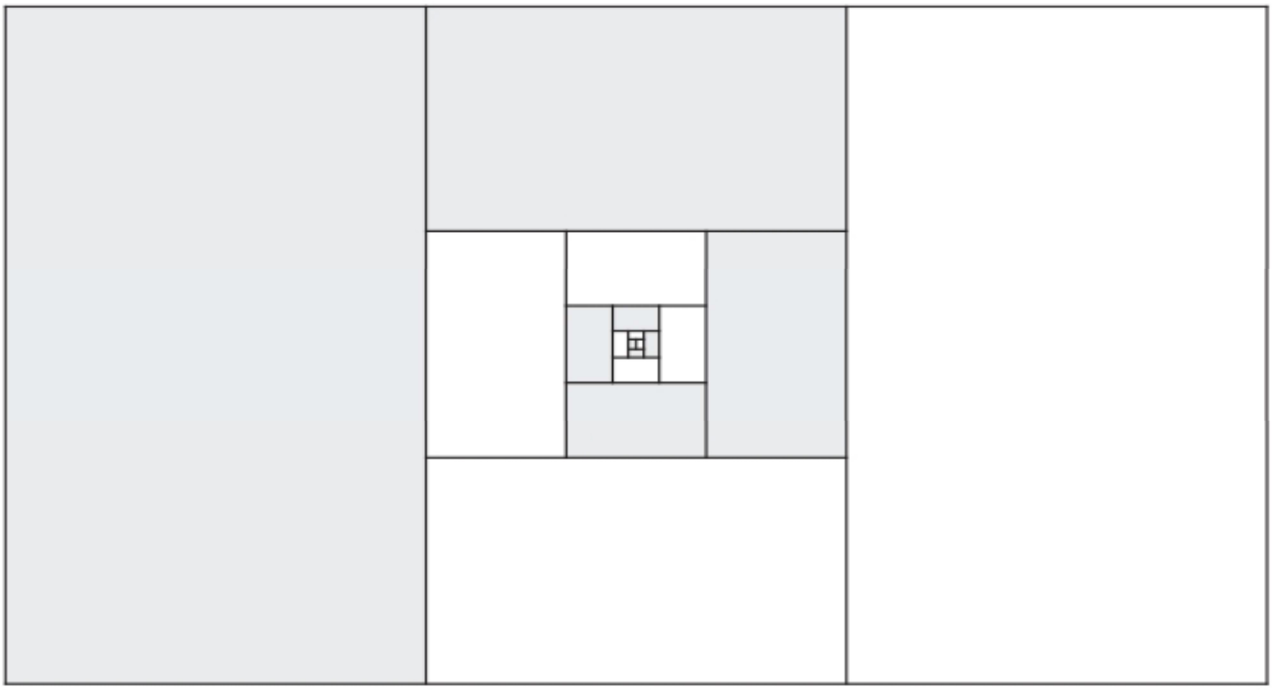
If n is even, then the sum is 0.

The series Oscillates infinitely.

So, the Geometric Series coverges Only when $|r|<1$.

Some visual proof of infinite series

7. $(\frac{1}{3})+(\frac{1}{3})^2+(\frac{1}{3})^3 \ldots\ldots=\frac{1}{2}$ (proof



Proof : we know that ,

$a+ar+ar^2+\ldots.=a/(1-r)$ where r is less than 1.

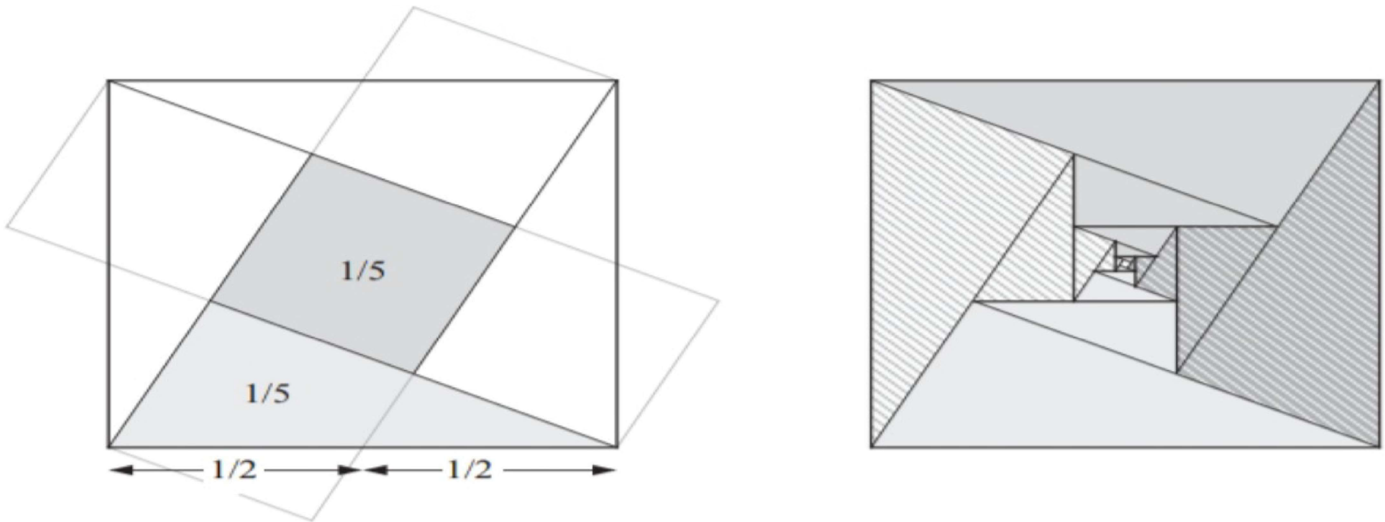
Here $a=\frac{1}{3}, r=\frac{1}{3}$

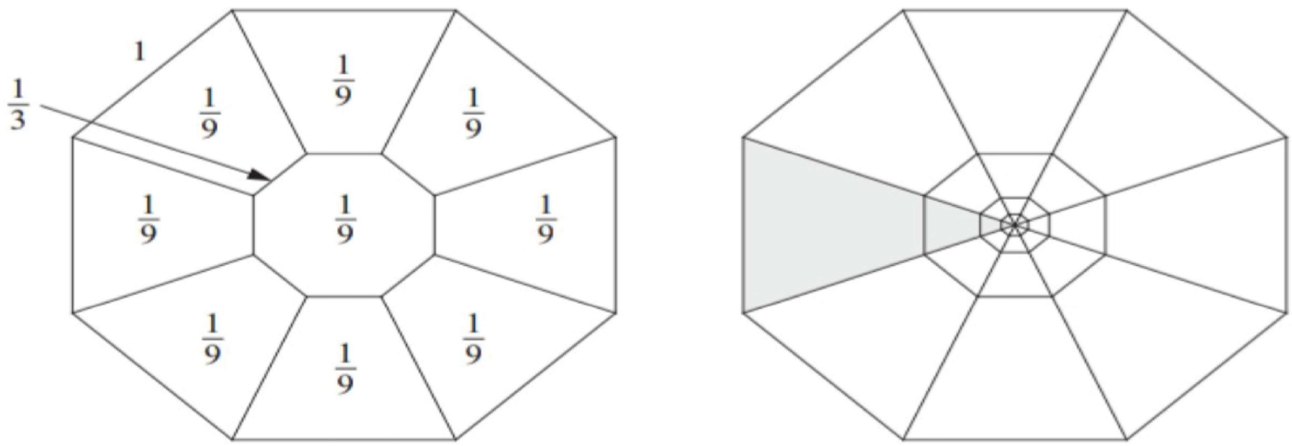
Hence sum of the series is ,

$(\frac{1}{3})/\{1-(\frac{1}{3})\}=\frac{1}{2}$

Some other examples,

II. $\frac{1}{5} + \left(\frac{1}{5}\right)^2 + \left(\frac{1}{5}\right)^3 + \cdots = \frac{1}{4}$:





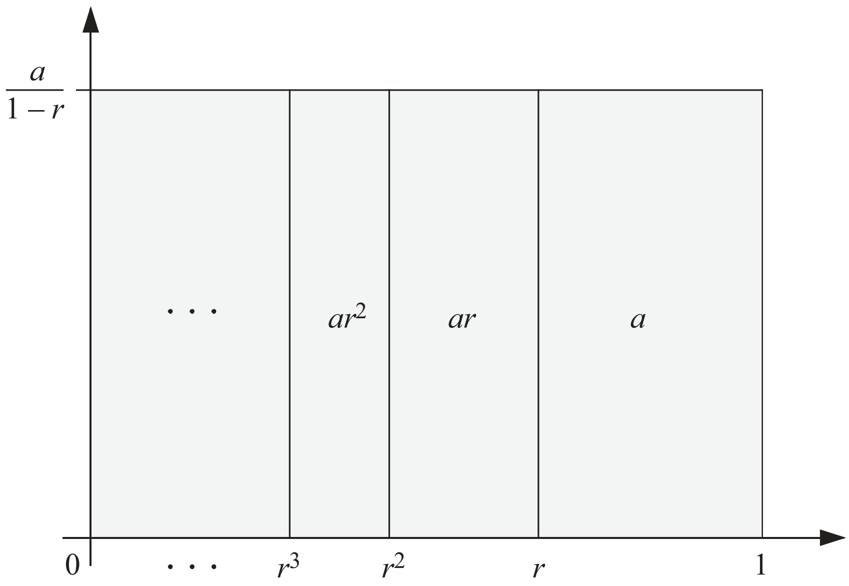
$$\frac{1}{9} + \frac{1}{9^2} + \frac{1}{9^3} + \cdots = \frac{1}{8}.$$

By this three above examples,

The general result $1/n+1/n^2+1/n^3+.......=1/(n-1)$

can be proved using this construction with a regular (n-2)gon.

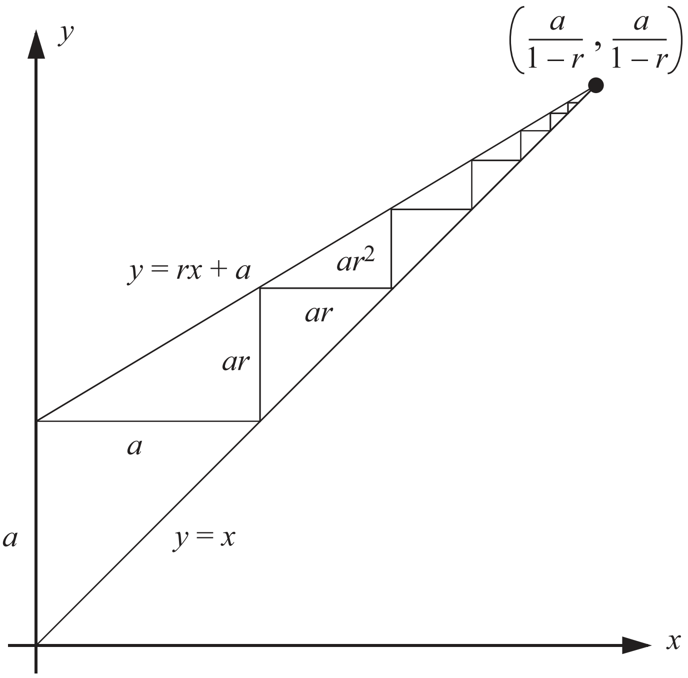
Geometric Series



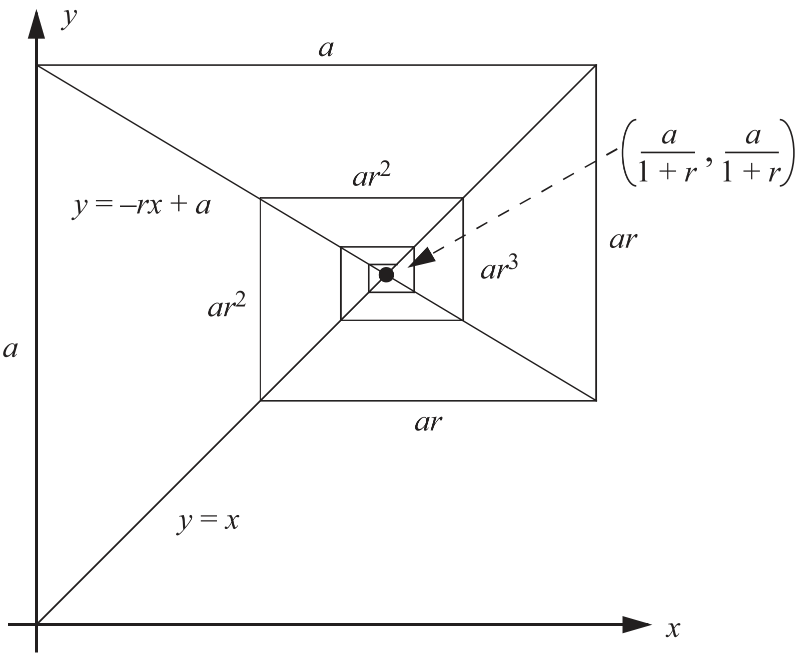
$$a > 0,\ \ r \in (0,1) \quad \Rightarrow \quad a + ar + ar^2 + ar^3 + \cdots = \frac{a}{1-r}.$$

Geometric Series

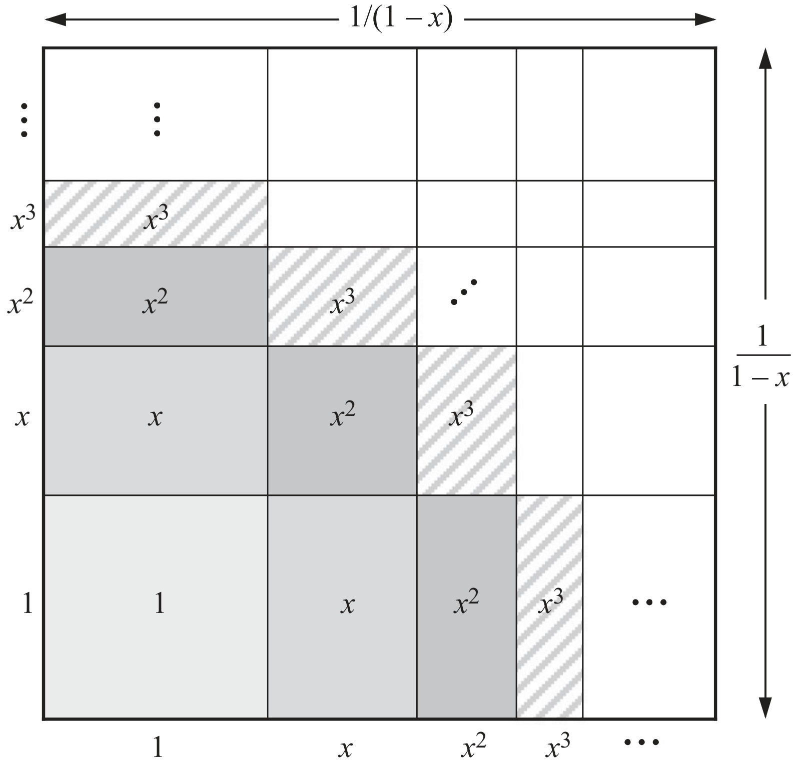
I. $a + ar + ar^2 + \cdots = \frac{a}{1-r}, \quad 0 < r < 1$:



II. $a - ar + ar^2 - \cdots = \frac{a}{1+r}, \quad 0 < r < 1$:



Differentiated Geometric Series



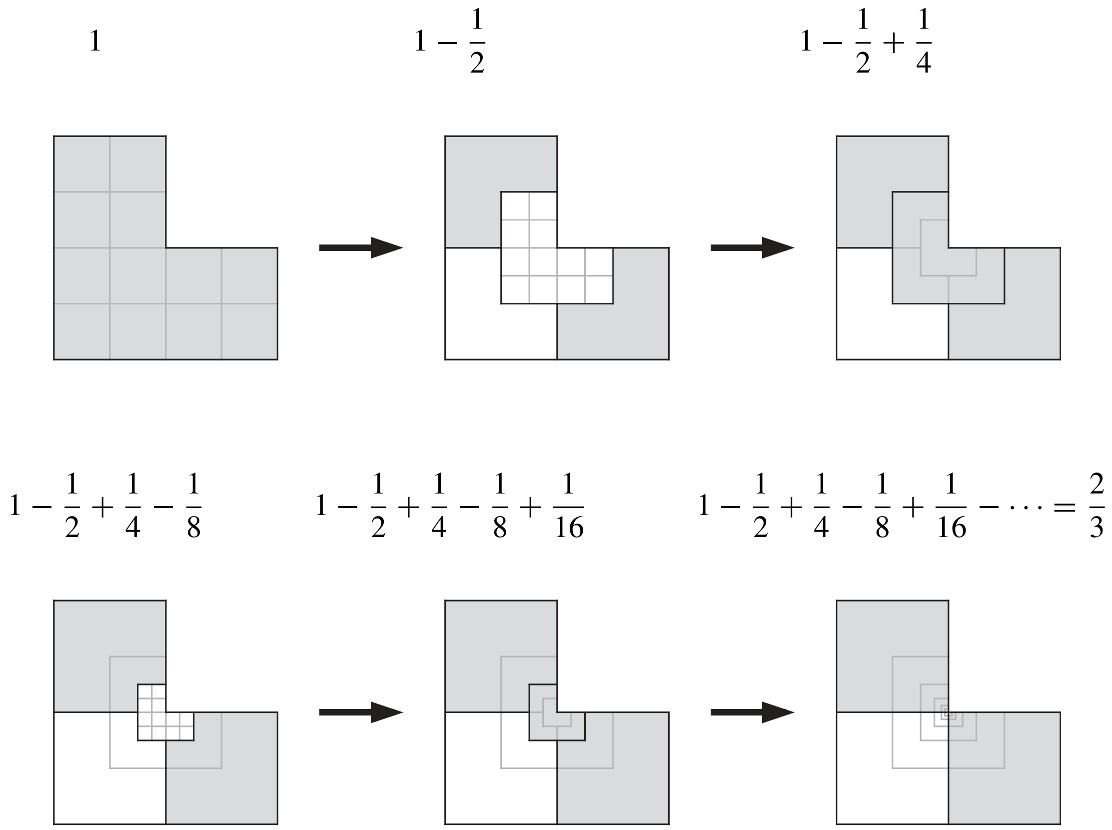
$$x \in [0, 1) \quad \Rightarrow \quad 1 + 2x + 3x^2 + 4x^3 + \cdots = \left(\frac{1}{1-x}\right)^2$$

.

16

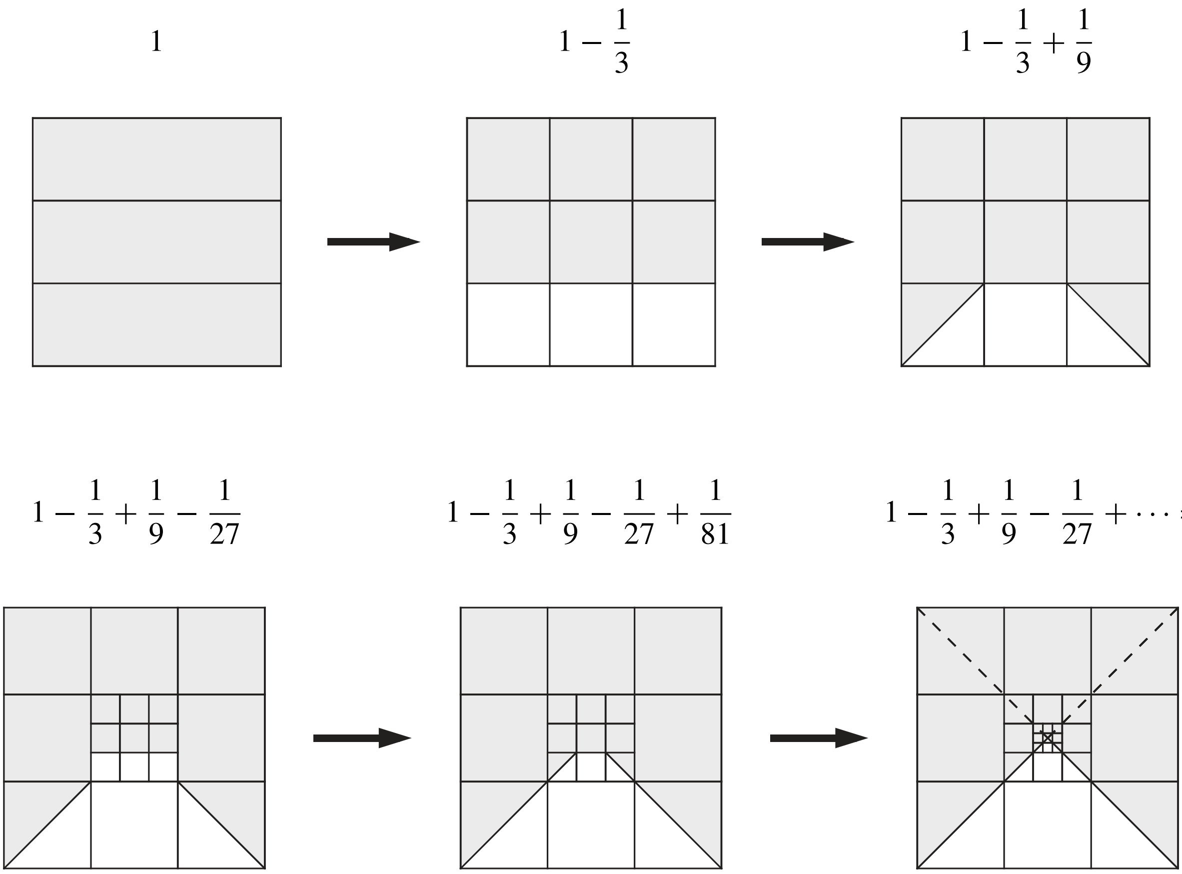
alternating series

$$1 - \frac{1}{2} + \frac{1}{4} - \frac{1}{8} + \frac{1}{16} - \cdots = \frac{2}{3}$$



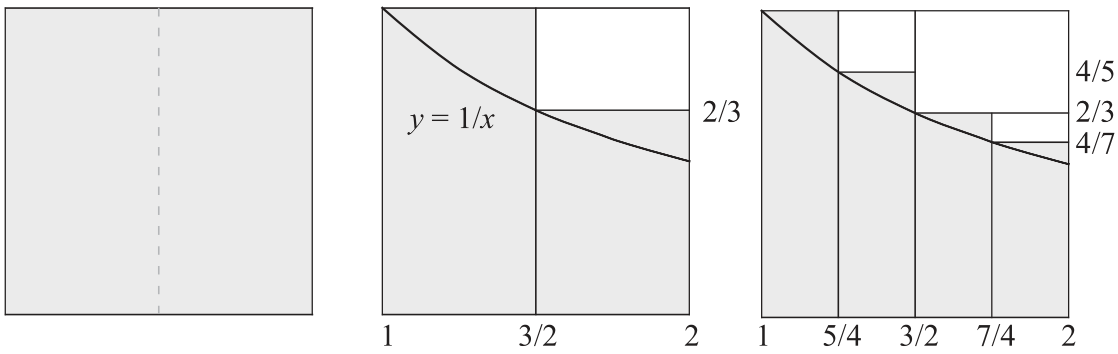
alternating series

$$1 - \frac{1}{3} + \frac{1}{9} - \frac{1}{27} + \frac{1}{81} - \cdots = \frac{3}{4}$$

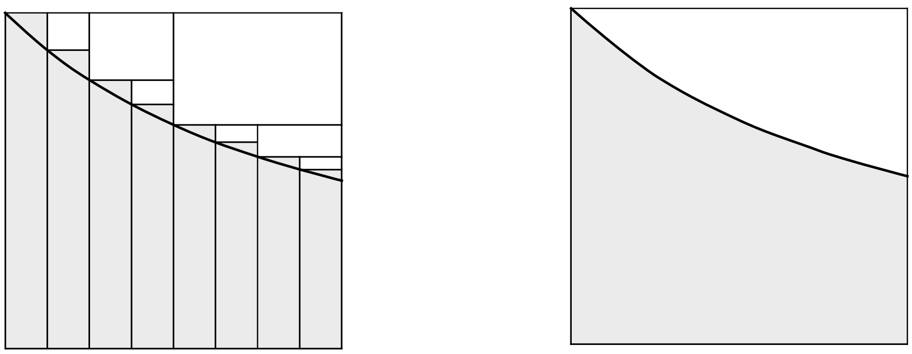


Alternating harmonic Series

$$\sum_{n=0}^{\infty}(-1)^n\frac{1}{n+1}=\ln 2$$



$1\cdots$ $\qquad -\frac{1}{2}+\frac{1}{3}\cdots$ $\qquad -\frac{1}{4}+\frac{1}{5}-\frac{1}{6}+\frac{1}{7}\cdots$



$$-\frac{1}{8}+\frac{1}{9}-\frac{1}{10}+\frac{1}{11}-\frac{1}{12}+\frac{1}{13}-\frac{1}{14}+\frac{1}{15}\cdots \qquad =\int_1^2\frac{1}{x}dx=\ln 2.$$

REFERENCES

Mathematics Magazine, vol. 79, no. 1 (Feb. 2006), p. 60.
College Mathematics Journal, vol. 32, no. 2 (March 2001), p. 109.
Mathematics Magazine, vol. 74, no. 4 (Oct. 2001), p. 320.
College Mathematics Journal, vol. 32, no. 4 (Sept. 2001), p. 257.
American Mathematical Monthly, vol. 109, no. 6 (June-July 2002), p. 52
4.*College Mathematics Journal*, vol. 43, no. 5 (Nov. 2012), p. 370.
College Mathematics Journal, vol. 40, no. 1 (Jan. 2009), p. 39.
College Mathematics Journal, vol. 36, no. 1 (Jan. 2005), p. 72.
Mathematics Magazine, vol. 83, no. 4 (Oct. 2010), p. 294.
College Mathematics Journal, vol. 36, no. 3 (May 2005), p. 198.
Mathematics Magazine, vol. 73, no. 5 (Dec. 2000), p. 363.
Mathematics Magazine, vol. 75, no. 5 (Dec. 2002), p. 388.
Mathematics Magazine, vol. 75, no. 4 (Oct. 2002), p. 283.
Mathematics Magazine, vol. 79, no. 5 (Dec. 2006), p. 359.
Mathematics Magazine, vol. 79, no. 2 (April 2006), p. 149.
Mathematics Magazine, vol. 78, no. 1 (Feb. 2005), p. 14.
College Mathematics Journal, vol. 45, no. 3 (May 2014), p. 179.
American Mathematical Monthly, vol. 107, no. 9 (Nov. 2000), p. 841.
Mathematics Magazine, vol. 77, no. 1 (Feb. 2004), p. 55.
College Mathematics Journal, vol. 38, no. 4 (Sept. 2007), p. 296.
Mathematics Magazine, vol. 80, no. 3 (June 2007), p. 182.
Mathematics Magazine, vol. 78, no. 3 (June 2005), p. 226.
Littlewood's Miscellany, Cambridge U. Pr., 1986, p. 55.
A Mathematical Space Odyssey, MAA, 2015, pp. 127–128.

DISCUSSION ON

THE FIBONACCI NUMBERS AND ITS APPLICATIONS

The University of Burdwan

Project Work Submitted For The B.SC. Semester VI (Honours) Examination in Mathamatics 2023

Under the supervision of:

Shampa Dutta

By:

Suma Das

ROLL NO: 200341200024

Registration no: 202001048598 of 2020-2021

Department of Mathematics

------------------------------ ------------------------------ ------------------------------

Signature of the Student *Signature of the teacher* *Signature of the H.O.D*

ACKNOWLEDGEMENT

I am grateful to **Mrs. Shampa Dutta**, State Aided College Teacher, Department of Mathematics, Sarat Centenary College, The University of Burdwan under whose supervision the project work have been carried out. I am grateful to all the teachers including the HOD of Mathematics, **Sarat Centenary College** for their constant support throughout the work. I am thankful to the authors of various reference books which have been consulted during the preparation of this project work. Finally I express my sincere gratitude to all staff members of the office, library of ourcollege and infrastructural support provided by the department.

Date:

Name of the student

CERTIFICATE

This is to certify that **Suma Das** has worked out the project work entitled **"The Fibonacci Numbers and its Applications"** under my supervision. In my opinion the work is worthy of consideration for partial fulfillment of his B.Sc. degree in Mathematics.

Date:

____

Signature of the teacher

CONTENTS

THE FIBONACCI NUMBERS AND ITS APPLICATIONS

WHAT IS FIBONACCI NUMBER?

A Fibonacci number is a series of numbers in which each Fibonacci number is obtained by adding the two preceding numbers. It means that the next number in the series is the addition of two previous numbers. Let the first two numbers in the series be taken as 0 and 1. By adding 0 and 1, we get the third number as 1. Then by adding the second and the third number (i.e) 1 and 1, we get the fourth number as 2, and similarly, the process goes on. Thus, we get the Fibonacci series as 0, 1, 1, 2, 3, 5, 8, ……. Hence, the obtained series is called the Fibonacci number series or Fibonacci Sequence.

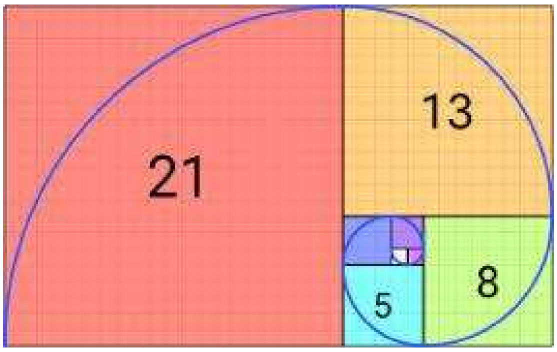
LIST OF THE FIBONACCI NUMBERS

The list of numbers of Fibonacci Sequence is given below. This list is formed by using the formula, which is mentioned in the above definition.

Fibonacci Number Series

0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, 6765, 10946, 17711, 28657, 46368, 75025, 121393, …………………………

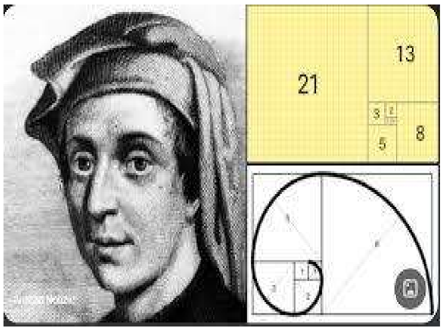
When we make squares with those widths, we get a nice spiral, which is called Fibonacci spiral.



LITERATURE REVIEW

The Fibonacci numbers were first described in Indian mathematics, as early as 200 BC in work by Pingala on enumerating possible patterns of Sanskrit poetry formed from syllables of two lengths. They are named after the Italian mathematician Leonardo of Pisa, also known as Fibonacci, who introduced the sequence to Western European mathematics in his 1202 book *Liber Abaci*.

The Fibonacci sequence appears in Indian mathematics, in connection with Sanskrit prosody. In the Sanskrit poetic tradition, there was interest in enumerating all patterns of long (L) syllables of 2 units duration, juxtaposed with short (S) syllables of 1 unit duration. Counting the different patterns of successive L and S with a given total duration results in the Fibonacci numbers: the number of patterns of duration m units is F_{m+1}.



Knowledge of the Fibonacci sequence was expressed as early as Pingala (c. 450 BC–200 BC). Singh cites Pingala's cryptic formula *misrau cha* ("the two are mixed") and scholars who interpret it in context as saying that the number of patterns for m beats (F_{m+1}) is obtained by adding one [S] to the F_m cases and one [L] to the F_{m-1} cases. Bharata Muni also expresses knowledge of the sequence in the *Natya Shastra* (c. 100 BC–c. 350 AD). However, the clearest exposition of the sequence arises in the work of Virahanka (c. 700 AD), whose own work is lost, but is available in a quotation by Gopala (c. 1135):

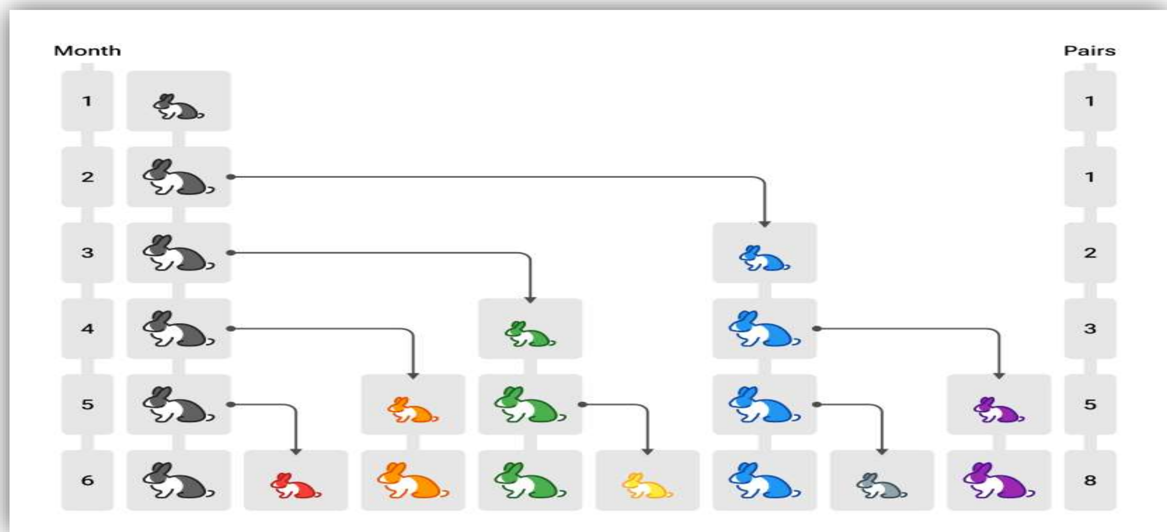
Hemachandra (c. 1150) is credited with knowledge of the sequence as well, writing that "the sum of the last and the one before the last is the number ... of the next mātrā-vṛtta."

The Fibonacci sequence first appears in the book *Liber Abaci* (*The Book of Calculation*, 1202) by Fibonacci where it is used to calculate the growth of rabbit populations. Fibonacci considers the growth of an idealized (biologically unrealistic) rabbit population, assuming that: a newly born breeding pair of rabbits are put in a field; each breeding pair mates at the age of one month, and at the end of their second month they always produce another pair of rabbits; and rabbits never die, but continue breeding forever. Fibonacci posed the puzzle: how many pairs will there be in one year?

- At the end of the first month, they mate, but there is still only 1 pair.
- At the end of the second month they produce a new pair, so there are 2 pairs in the field.

- At the end of the third month, the original pair produce a second pair, but the second pair only mate to gestate for a month, so there are 3 pairs in all.
- At the end of the fourth month, the original pair has produced yet another new pair, and the pair born two months ago also produces their first pair, making 5 pairs.

At the end of the *n*th month, the number of pairs of rabbits is equal to the number of mature pairs (that is, the number of pairs in month $n - 2$) plus the number of pairs alive last month (month $n - 1$). The number in the *n*th month is the *n*th Fibonacci number.



The name "Fibonacci sequence" was first used by the 19th-century number theorist Édouard Lucas.

We celebrate Fibonacci Day Nov. 23rd not just to honor the forgotten mathematical genius Leonardo Fibonacci, but also because when the date is written as 11/23, the four numbers form a Fibonacci sequence. Leonardo Fibonacci is also commonly credited with contributing to the shift from Roman numerals to the Arabic numerals we use today.

CALCULATIONS OF THE FIBONACCI NUMBERS

USING FORMULA

The Fibonacci numbers may be defined by recurrence relation.

$$F_0 = 0, F_1 = 1$$

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

under some older definitions, the value $F_0 = 0$ is omitted, so that the sequence starts with $\mathbf{F_1 = F_2 = 1}$ and the recurrence $\mathbf{F_n = F_{n-1} + F_{n-2}}$ is valid for n>2, where F_n is the n^{th} Fibonacci number in the sequence.

The only problem with this formula is that it's a recursive formula, meaning it defines each number of the sequence using the preceding numbers. So if you wanted to calculate the tenth number in the Fibonacci sequence, you'd need to first calculate the ninth and eighth, but to get the ninth number you'd need the eighth and seventh, and so on.

To find any number in the Fibonacci sequence without any of the preceding numbers, you can use a closed-form expression called Binet's formula:

$$F_n = \frac{\phi^{n} - (-\phi)^{-n}}{\sqrt{5}}$$

In Binet's formula, the Greek letter phi (φ) represents an irrational number called the golden ratio: (1 + √ 5)/2, which rounded to the nearest thousandths place equals 1.618.

You can also calculate a Fibonacci Number by multiplying the previous Fibonacci Number by the Golden Ratio and then rounding.

USING PROGRAM

C- Program to compute 1st n terms of the Fibonacci Sequence

```
//Fibonacci Sequence - 1st n terms with t1=0, t2=1
#include<stdio.h>
#include<math.h>
 main()
{
   int t1,t2,t3,n,i;
   t1=0; t2=1;
   printf("Please let me know how many terms you want, it
should be a natural number\n");
   scanf("%d",&n);
   printf("You have entered n= %d \n",n);
   printf("First %d terms of the Fibonacci Sequence are as
follows:\n",n);
   for (i=1;i<=n;i++)
   {
   printf("term %d is %d \n",i,t1) ;
```

```
    t3=t1+t2;
    t1=t2;
    t2=t3;
        }
}
```

Output of the Program:

Please let me know how many terms you want, it should be a natural number
10
You have entered n= 10
First 10 terms of the Fibonacci Sequence are as follows:
term 1 is 0
term 2 is 1
term 3 is 1
term 4 is 2
term 5 is 3
term 6 is 5
term 7 is 8
term 8 is 13
term 9 is 21
term 10 is 34

C- Program to compute Fibonacci Sequence terms upto a natural number n

```
//Fibonacci Sequence terms upto a given positive integer n
// 1st two terms are t1=0, t2=1
#include<stdio.h>
#include<math.h>
 main()
{
   int t1,t2,t3,n,i;
   t1=0; t2=1;
   printf("Enter the natural number n upto which you want
the Fibonacci sequence terms \n");
   scanf("%d",&n);
   printf("You have entered n= %d \n",n);
   printf("Fibonacci Sequence terms upto %d are as
follows:\n",n);
   printf("%d, %d",t1, t2);
   t3=t1+t2;
   while (t3 <= n)
   {
   printf(", %d",t3);
       t1=t2;
       t2=t3;
       t3=t1+t2;
      }

}
```

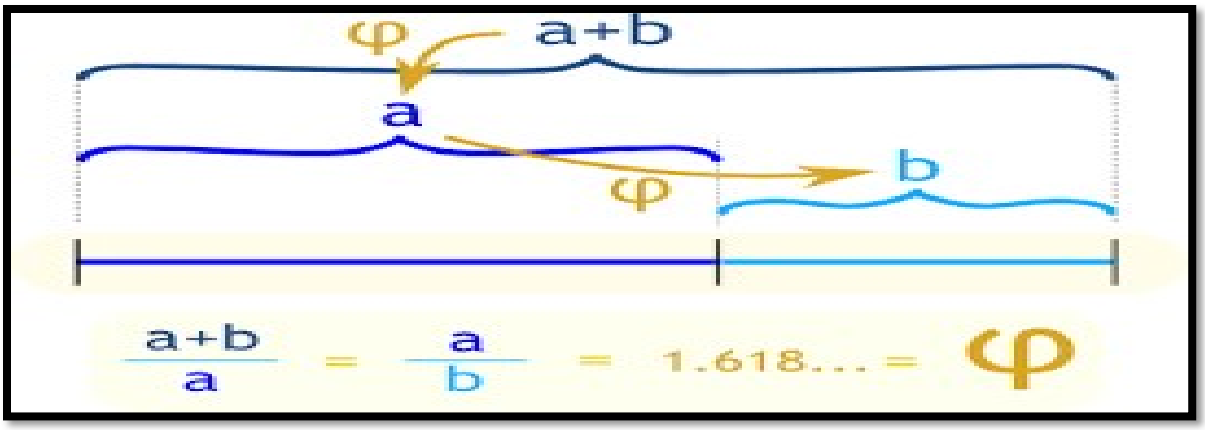
Output of the Program:

Enter the natural number n upto which you want the
Fibonacci sequence terms
150
You have entered n= 150
Fibonacci Sequence terms upto 150 are as follows:
0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144

THE FIBONACCI NUMBERS AND GOLDEN RATIO

Two quantities are said to be in golden ratio, if their ratio is equal to the ratio of their sum to the larger of the two quantities. The golden ratio is approximately equal to 1.618.

For example, if "a" and "b" are two quantities with a>b>0, the golden ratio is algebraically expressed as follow:



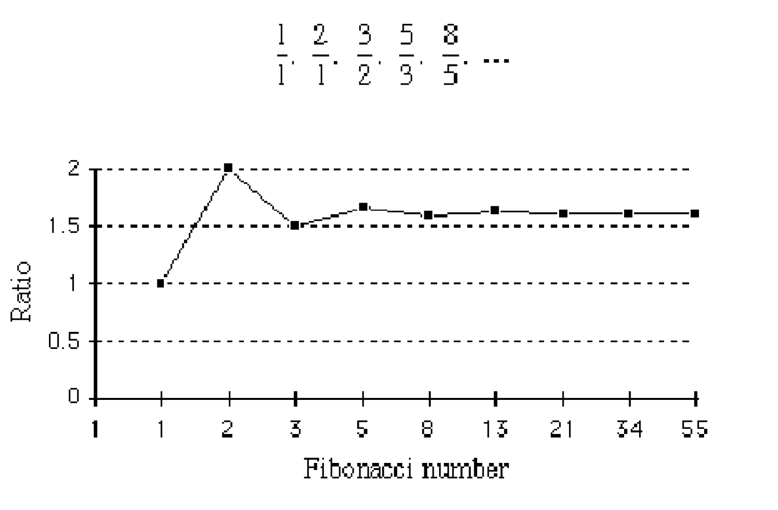
The golden ratio is an irrational number, which is the solution to the quadratic equation $x^2-x-1=0$.

There is a special relationship between the Golden ratio and the Fibonacci number. When we take any two successive Fibonacci numbers, their ratio is very close to the Golden ratio.

In fact, the bigger the pair of Fibonacci Numbers, the closer the approximation. Let us try a few:

A	**B**	**B / A**
2	3	1.5
3	5	1.666666666...
5	8	1.6
8	13	1.625
...	...	...
144	233	1.618055556...
233	377	1.618025751...
...	...	...

$$\lim_{n \to \infty} \frac{F_{n+1}}{F_n} = 1.618$$



If you take two successive terms of the series, a, b, and $a+b$ then

$$\frac{b}{a} \cong \frac{a+b}{b}$$
$$\cong \frac{a}{b} + 1$$

We define the golden section, ϕ (*phi*), to be the limit of $\frac{b}{a}$, so:

$$\phi = \frac{1}{\phi} + 1$$
$$\phi^2 - \phi - 1 = 0$$
$$\phi = \frac{1+\sqrt{5}}{2} \approx 1.618$$

THE PROPERTIES OF THE FIBONACCI NUMBERS

The following are the properties of the Fibonacci numbers.

- In the Fibonacci series, take any three consecutive numbers and add those numbers. When you divide the result by 2, you will get the three numbers.

  For example, take 3 consecutive numbers such as 1, 2, 3. when you add these numbers, i.e. 1+ 2+ 3 = 6. When 6 is divided by 2, the result is 3, which is 3.

- If you take any three consecutive Fibonacci numbers, the square of the middle number is always one away from the product of the outer two numbers i.e $F_{n+1} \cdot F_{n-1} - F_n^2 = (-1)^n$

For Example, is we take the consecutive triplet 8, 13, 21, you can see that 168 – 169 = -1. If you look at a later triplet 89, 144, 233 we see that 20737 – 20736 = 1.

- Take four consecutive numbers other than “0” in the Fibonacci series. Multiply the outer number and also multiply the inner number. When you subtract these numbers, you will get the difference “1”.

For example, take 4 consecutive numbers such as 2, 3, 5, 8. Multiply the outer numbers, i.e. (2 X 8) and multiply the inner number, i.e. (3 X 5). Now subtract these two numbers, i.e. 16-15 =1. Thus, the difference is 1.

- The sequence goes even, odd, odd, even, odd, odd, even, odd, odd, ... :

0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89……………………….

Since adding two odd numbers produces an even number, but adding even and odd (in any order) produces an odd number.

- If we take any four consecutive Fibonacci number, then subtracting the sum of the second and third numbers from the sum of the first and fourth numbers will always yield the first of those four numbers.

For example, if we take any four consecutive Fibonacci numbers such as 3, 5, 8, 13. Then (13+3)-(5+8)=16-13=3, the first number of those four numbers.

APPLICATION

FIBONACCI SEQUENCE IN NATURE

Fibonacci can be found in nature not only in the famous rabbit experiment, but also in beautiful flowers. On the head of a sunflower and the seeds are packed in a certain way so that they follow the pattern of the Fibonacci sequence. This spiral prevents the seed of the sunflower from crowding themselves out, thus helping them with survival. The petals of flowers and other plants may also be related to the Fibonacci sequence in the way that they create new petals .

Petals on flowers

Probably most of us have never taken the time to examine very carefully the number or arrangement of petals on a flower. If we were to do so, we would find that the number of petals on a flower that still has all of its petals intact and has not lost any, for many flowers is a Fibonacci number .

1 petal: white cally lily

2 petal: Euphorbia milii,
Asiatic dayflower

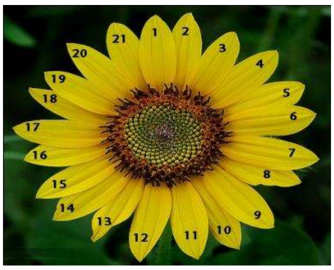
3 petals: lily, iris

5 petals: buttercup, wild rose, Frangipani, Crepe Jasmine

8 petals: delphiniums

13 petals: ragwort, corn marigold, cineraria,

21 petals: aster, black-eyed susan, chicory



34 petals: plantain, pyrethrum

55, 89 petals: michaelmas daisies, the asteraceae family

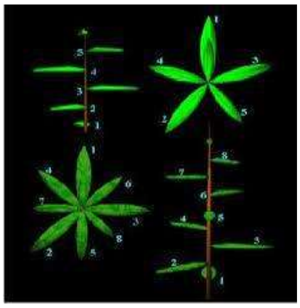
Ever plucked rose petals? Even if you tear it, you must not have seen how many petals there are. They have 13,21,34,55 or 89 numbers petals.

Leaves and branches on trees

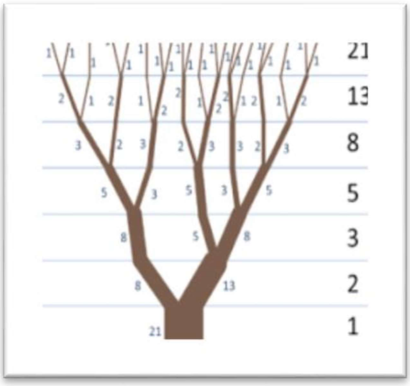
Plants show the Fibonacci numbers in the arrangements of their leaves. Three clockwise rotations, passing five leaves two counter-clockwise rotations. Sneezewort (Achillea ptarmica) also follows the Fibonacci numbers.

Schematic diagram (Sneezewort)

Why do these arrangements occur? In the case of leaf arrangement, or phyllotaxis, some of the cases may be related to maximizing the space for each leaf, or the average amount of light falling on each one.



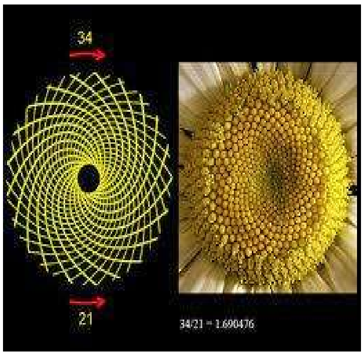
The Fibonacci sequence can also be seen in the way tree branches form or split. A main trunk will grow until it produces a branch, which creates two growth points. Then, one of the new stems branches into two, while the other one lies dormant. This pattern of branching is repeated for each of the new stems. A good example is the sneezewort. Root systems and even algae exhibit this pattern.



FIBONACCI SPIRAL

Seed heads

The head of a flower is also subject to Fibonaccian processes. Typically, seeds are produced at the center, and then migrate towards the outside to fill all the space. Sunflowers provide a great example of these spiraling patterns.



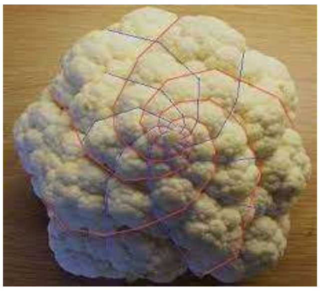
There are 55 spirals spiraling outwards and 34 spirals spiraling inwards in most daisy or sunflower blossoms. Pinecones clearly show the Fibonacci spirals.

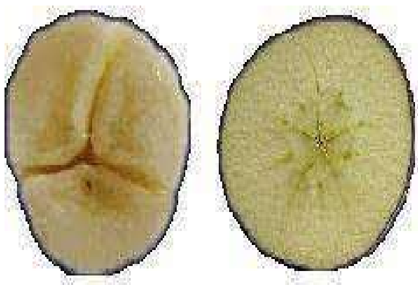
Pinecones

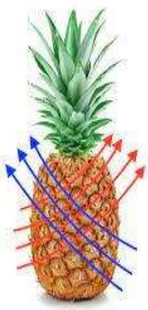
The seed pods on a pinecone are arranged in a spiral pattern. Each cone consists of a pair of spirals, each one spiraling upwards in opposing directions. The number of steps will almost always match a pair of consecutive Fibonacci numbers. For example, a 3-5 cone is a cone which meets at the back after three steps along the left spiral, and five steps along the right.

Fruits and Vegetables

Fibonacci spiral can be found in cauliflower. The Fibonacci numbers can also be found in Pineapples and Bananas (Lin and Peng). Bananas have 3 or 5 flat sides and Pineapple scales have Fibonacci spirals in sets of 8, 13, and 21. Inside the fruit of many plants we can observe the presence of Fibonacci order.

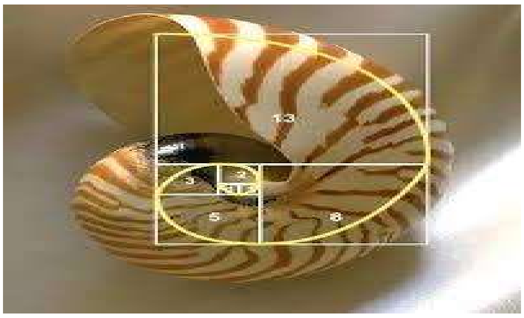






Shells

Fibonacci spiral are also found in Snail shells and nautilus shells. It can also be seen in the horns of certain goats, and the shape of certain spider's webs.



Spiral Galaxies

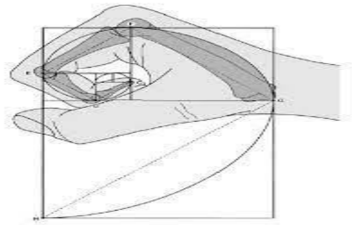
Not surprisingly, spiral galaxies also follow the familiar Fibonacci pattern. The Milky Way has several spiral arms, each of them a logarithmic spiral of about 12 degrees. As an interesting aside, spiral galaxies appear to defy Newtonian physics.

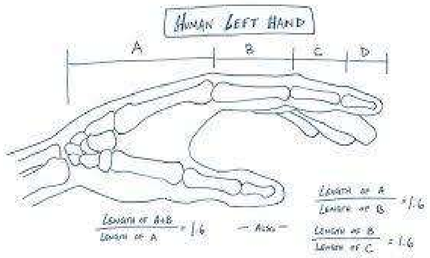
Storms

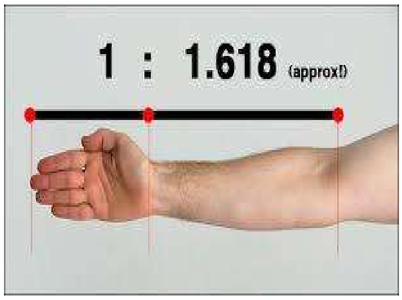
Storm systems like hurricanes and tornadoes often follow the Fibonacci sequence. Next time you see a hurricane spiraling on the weather radar, check out the unmistakable Fibonacci spiral in the clouds on the screen.

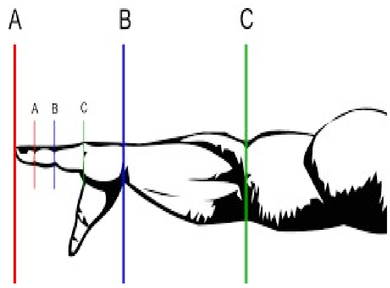
FIBONACCI IN ORGANS OF THE HUMAN BODY

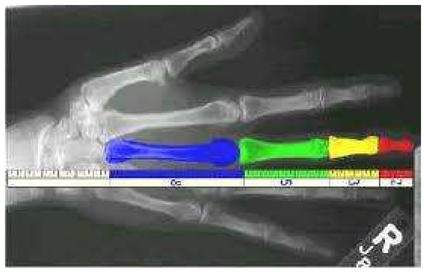
Humans exhibit Fibonacci characteristics. Every human has two hands, each one of these has five fingers and each finger has three parts which are separated by two knuckles. All of these numbers fit into the sequence. Moreover the lengths of bones in a hand are in Fibonacci numbers.

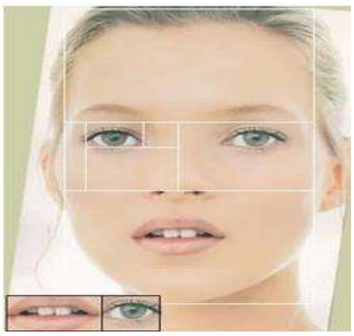






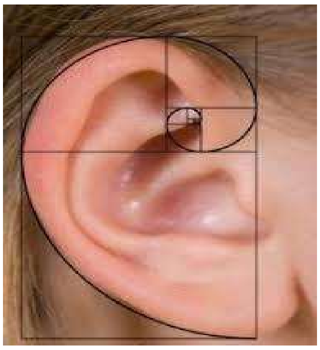






The mouth and nose are each positioned at golden sections of the distance between the eyes and the bottom of the chin. Similar proportions can been seen from the side, and even the eye and ear itself (which follows along a spiral).

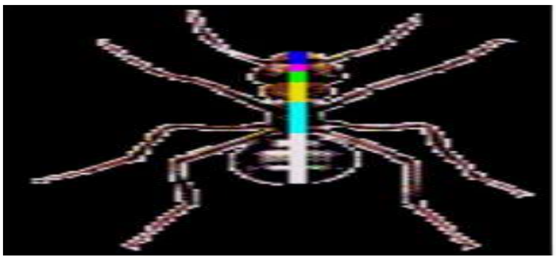
It's worth noting that every person's body is different, but that averages across populations tend towards phi. It has also been said that the more closely our proportions adhere to phi, the more "attractive" those traits are perceived. As an example, the most "beautiful" smiles are those in which central incisors are 1.618 wider than the lateral incisors, which are 1.618 wider than canines, and so on. It's quite possible that, from an evo-psych perspective, that we are primed to like physical forms that adhere to the golden ratio — a potential indicator of reproductive fitness and health.

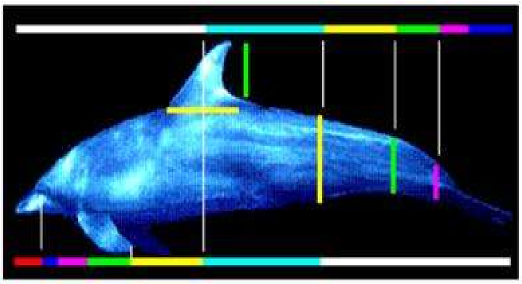


The cochlea of the inner ear forms a Fibonacci spiral.

FIBONACCI IN ANIMAL BODIES

Even our bodies exhibit proportions that are consistent with Fibonacci numbers. For example, the measurement from the navel to the floor and the top of the head to the navel is the golden ratio. Animal bodies exhibit similar tendencies, including dolphins (the eye, fins and tail all fall at Golden Sections), starfish, sand dollars, sea urchins, ants, and honey bees.





FIBONACCI IN RETRODUCTIVE DYNAMICS

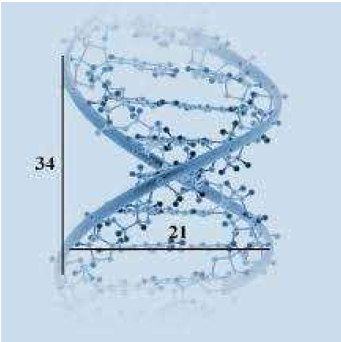
Speaking of honey bees, they follow Fibonacci in other interesting ways. The most profound example is by dividing the number of females in a colony by the number of males (females always outnumber males). The answer is typically something very close to 1.618. In addition, the family tree of honey bees also follows the familiar pattern. Males have one parent (a female), whereas females have two (a female and male). Thus, when it comes to the family tree, males have 2, 3, 5, and 8 grandparents, great-grandparents, gr-gr-grandparents, and gr-gr-gr-grandparents respectively. Following the same pattern, females have 2, 3, 5, 8, 13, and so on. And as noted, bee physiology also follows along the Golden Curve rather nicely.

FIBONACCI IN ANIMAL FIGHT PATTERNS

When a hawk approaches its prey, its sharpest view is at an angle to their direction of flight — an angle that's the same as the spiral's pitch.

FIBONACCI IN DNA MOLECULES

Even the microscopic realm is not immune to Fibonacci. The DNA molecule measures 34 angstroms long by 21 angstroms wide for each full cycle of its double helix spiral.



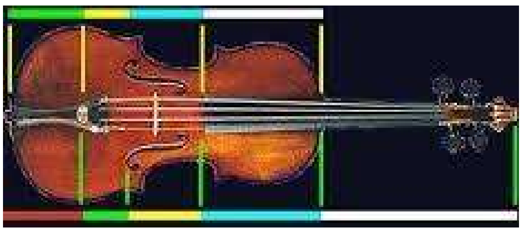
These numbers, 34 and 21, are numbers in the Fibonacci series, and their ratio 1.6190476 closely approximates Phi, 1.6180339.

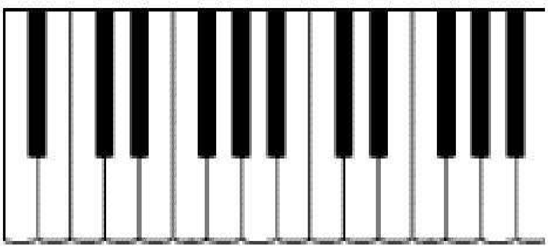
FIBONACCI IN MUSIC

The Fibonacci sequence of numbers and the golden ratio are manifested in music widely. The numbers are present in the octave, the foundational unit of melody and harmony.

Stradivarius used the golden ratio to make the greatest string instruments ever created.

Howat's(1983) research on Debussy's works shows that the composer used the golden ratio and Fibonacci numbers to structure his music. The *Fibonacci Composition* reveals the inherent aesthetic appeal of this mathematical phenomenon. Fibonacci numbers harmonize naturally and the exponential growth which the Fibonacci sequence typically defines in nature is made present in music by using Fibonacci notes. The intervals between keys on a piano of the same scales are Fibonacci numbers (Gend, 2014).





FIBONACCI IN DISTANCE

Take any two consecutive numbers from this series as example 13 and 21 or 34 and 55.

Now smaller number is in miles = the other one in Kilometer or bigger number is in Kilometers = the smaller one in Miles (The other way around).

34 Miles = round (54.72) Kilometers = 55 Kilometers

21 Kilometers = round (13.05) Miles = 13 Miles

For distances which are not exact Fibonacci values you can always proceed by splitting the distance into two or more Fibonacci values.

As example, for converting 15 km into miles we can proceed as following:

15 km = 13 km + 2 km

13 km -> 8 mile

2 km -> 1 mile

15 km -> 8+1 = 9 mile

Another example, for converting 170km into miles we can proceed as:

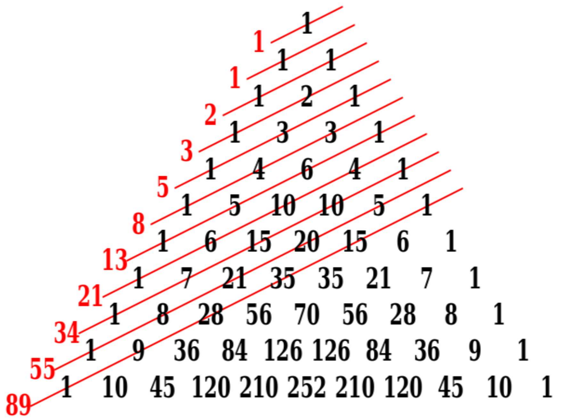
170 km = 10*17 km

17 km = 13 km + 2 km + 2 km = 8 + 1 + 1 miles = 10 miles (approximately) Now, 170 km = 10*10 miles = 100 miles (approximately)

So, either way we can proceed. For bigger numbers we can proceed as above. (Ref: Sudip Maji, B.C.Roy Engineering College)

FIBONACCI NUMBER IN PASCAL'S TRIANGLE

The Fibonacci Numbers are also applied in Pascal's Triangle. Entry is sum of the two numbers either side of it, but in the row above. Diagonal sums in Pascal's Triangle are the Fibonacci numbers. Fibonacci numbers can also be found using a formula



FIBONACCI NUMBER IN CODING

Recently Fibonacci sequence and golden ratio are of great interest to the researchers in many fields of science including high energy physics, quantum mechanics, Cryptography and Coding. Raghu and Ravishankar(2015) developed a paper of application classical encryption techniques for securing data.(Raphael and Sundaram,2012) showed that communication may be secured by the use of Fibonacci numbers. Similar application of Fibonacci in Cryptography is described here by a Simple Illustration.

Suppose that Original Message"CODE" to be Encrypted. It is sent through an unsecured channel. Security key is chosen based on the Fibonacci number. Any one character may be chosen as a first security key to generate cipher text and then Fibonacci sequence can be used. Agarwal et al (2015) used Fibonacci sequence for encryption data.

Method of Encryption

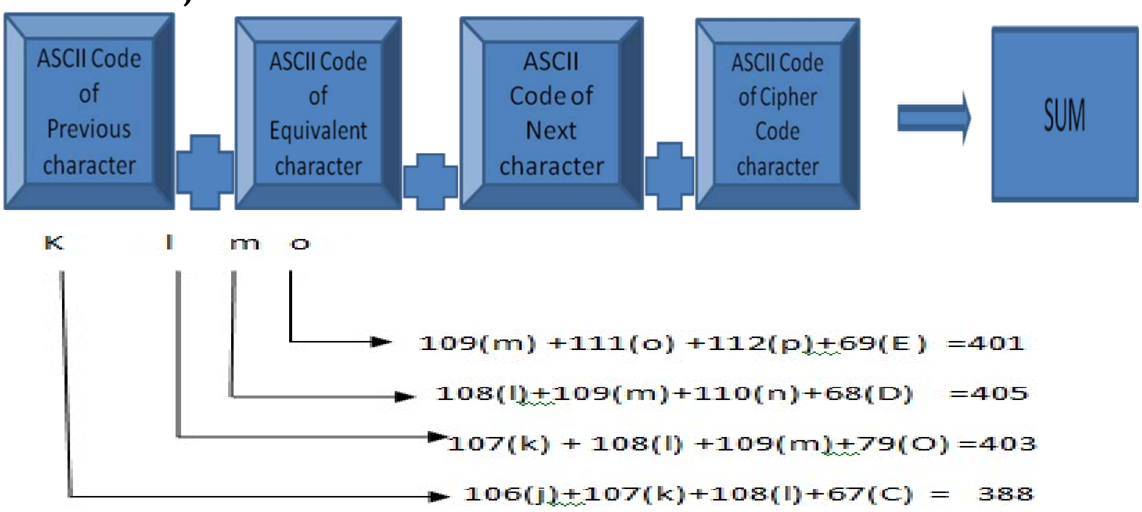
For instance, let the first security key chosen be ‘k’.
Plain Text: **C O D E**
Characters: **k l m o** p q r s t u v w x y z a b c d e f g h I j k l ….
Fibonacci : **1 2 3 5** ……..
Cipher Text: **k l m o**

Cipher Text is converted into Unicode symbols and saved in a text file. The text file is transmitted over the transmission medium. It is the first level of security.

Cipher text to Unicode

In the second level of security, the ASCII code of each character obtained from the cipher text plus the ASCII code of its previous character, and next character is added to the ASCII code of the equivalent character in the original message. Here, ASCII codes of four characters are used as a security key to further encode the characters available in the cipher text to Unicode symbols.

For instance,



By looking at the symbols in a text file no unknown persons can identify what it is and the message cannot be retrieved unless the re-trivial procedure is known.Mukherjee and Samanta(2014) developed a paper where they used Fibonacci numbers in hiding image cryptography.

Decryption method

The Decryption process follows a reverse process of Encryption. Recipient extracted each symbol from the received text file and mapped to find its hexadecimal value .Obtained value is converted into a decimal value to find out the plain text using the key. Without knowledge of the key an unknown person cannot understand the existence of any secret message.

FIBONACCI SEQUENCE IN ART-USING THE FIBONACCI SPIRAL

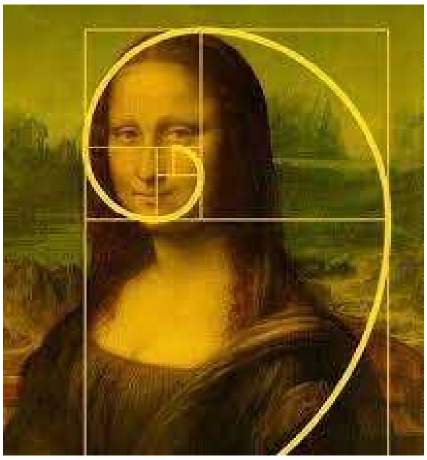
It didn't take long for painters, particularly those well-versed in the multidisciplinary approach that traditional and Renaissance art represented at the time, to see that this idea, as appealing as it is in all other elements of life, should also be reflected in their paintings.

During this era, incorporation was purposeful, but through de facto artistic evolution, the sequencing and ratios started to infuse themselves into the artistic method of those who

followed and has become an almost essential component of the artistic arrangement, both in realistic and non-figurative paintings. As a result, the Fibonacci spiral and Golden Ratio, as seen centuries ago, are today as visible in art and our perception of them as they are in nature.

What is special about the sequence is that many artists will intentionally use its aesthetic benefits, while other highly respected photographic artworks may discover – totally by chance – that it can be reproduced onto their artwork, so much so that it has even been spotted in war photos. When it comes to establishing an aesthetic or a design new for a project, there are no restrictions for designers.

The Golden Ratio in connection to design is a source of contention among mathematicians, graphic designers, and scientists. But there is ample proof, both in nature and in produced design, that a ratio is a reliable tool for creators. It can be used for constructing a grid for a layout, determining the best cropping for a photo, or determining sizes for type hierarchy when highlighting material, to mention a few examples. Overall, we believe it's an intriguing approach to look at excellent design via a mathematical lens, and it's amazing to see where and how it's employed in the environment around us.



Leonardo *da Vinici*, no that's not a typo, is well known for his usage of the Fibonacci Sequence. One notable example is his most famous work, The Mona Lisa. Da Vinci utilized the sequence with the Golden Spiral, which stems from the

Perfect Rectangle. The Perfect Rectangle is formed by creating rectangles within the corresponding dimensions of 1.618, from each descending Fibonacci Number (8, 5, 3, 2, 1, etc.) The spiral comes from touching each side in the Perfect Rectangle.

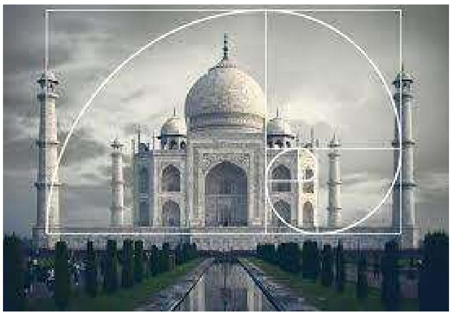
So how exactly did Leonardo da Vinci go about utilizing the Golden Spiral? First, he uses it to frame the woman in the painting. The spiral begins at her left wrist then travels to the background of the image, which contrasts the beauty of her face. It then skims over her forehead and continues turning until it kisses her chin. It rises, going past the slight of her dimple. Lastly, it completes one rotation which ends at the tip of her nose.

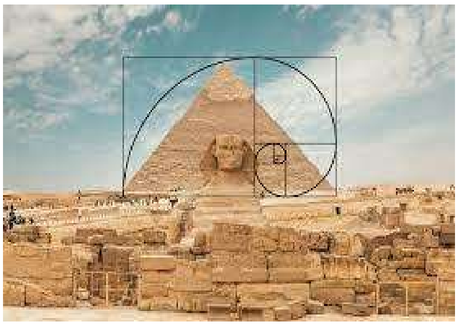
When making eye contact with someone, the ideal place to look is actually their nose, as it centers the face. And with the Mona Lisa, once ease your focus, you immediately notice the eyes. Her most remarkable feature that follows you everywhere you go.

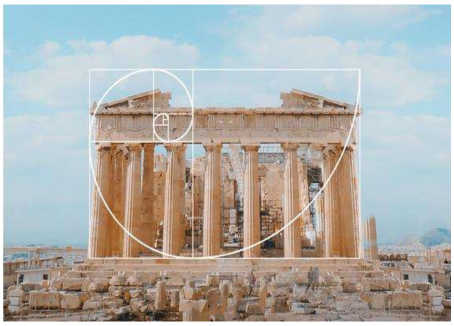
FIBONACCI SEQUENCE IN ARCHITECTURE

Antiquity already studied this proportion given by the number of gold and applied it in their constructions and artistic works, as it was said that it has the characteristic of being naturally pleasing to the human eye. Therefore, it can be verified in several architectural works such as the Parthenon, in which the width and height of the facade follow the golden proportion; in the Egyptian Pyramids, in which each block is 1.618 times larger than the block on the level immediately above, and in some of them the inner chambers are 1,618 times as long as they are wide; and even at the Taj Mahal, which some theorists link its design to the golden ratio.

These ratios of proportions bring several possible readings in how the scale of architecture and the way a building is designed is given, even unconsciously, by the Fibonacci sequence, since one of the attributions of a building made by an architect is that it is beautiful, pleasing to the eye: quality generated by the proportion given by this mathematical series.







CONCLUSION

The Fibonacci numbers are Nature's numbering system. They appear everywhere in Nature, from the leaf arrangement in plants, to the pattern of the florets of a flower, the bracts of a pinecone, or the scales of a pineapple. The Fibonacci numbers are therefore applicable to the growth of every living thing, including a single cell, a grain of wheat, a hive of bees, and even all of mankind. Nature follows the Fibonacci numbers astonishingly. But very little we observe the beauty of nature. The Great poet Rabindranath Tagore also noted this. If we study the pattern of various

natural things minutely we observe that many of the natural things around us follow the Fibonacci numbers in real life which creates strange among us. The study of nature is very important for the learners. It increases the inquisitiveness among the learners. The topic is chosen so that learners could be interested towards the study of nature around them. .Security in communication system is an interesting topic at present as India is going towards digitalization. A little bit of concept for securing data is also provided in this model. Let us finish by the words of Leonardo da Vinci "Learn how to see, Realize that everything connects to everything else".

REFERENCES

1) Agarwal,P., Agarwal,N., Saxena,R.,2015, Data Encryption through Fibonacci Sequence and Unicode Characters, MIT International Journal of Computer Science and Information Technology Vol. 5(2), 79-82.
2) Bortner, Cashous W. and Peterson, Allan C., 2016, The History and Applications of Fibonacci Numbers. UCARE Research Products. 42. (http://digitalcommons.unl.edu/ucareresearch/42)
3) Garg, M, Garg, P, Vohra, R. K., 2014, Advanced Fibonacci sequence with Golden Ratio, International Journal of Scientific & Engineering Research, Vol 5(6), 388-391.
4) Gend ,V,R., 2014 The Fibonacci sequence and the golden ratio in music, Notes on Number Theory and Discrete Mathematics,Vol. 20(1), 72–77.
5) Howard, E (ed.), 2004, Applications of Fibonacci Numbers, Proceedings of the Tenth International Research Conference on Fibonacci Numbers and their Applications, Vol9, 19-24.

6) Howat, R., 1983,Debussy in Proportion: A Musical Analysis. Cambridge: Cambridge UP, p.1.
7) http://evolutionoftruth.com/goldensection/goldsect.htm

8) http://www.helixglass.co.uk/images/leaded/thumbnails/fibonacci.jpg
9) http://pass.maths.org.uk/issue3/fiibonacci
10) http://maths.survey.ac.uk/hosted-sites/R.Knott/Fibonacci numbers in real life (date of access 24.01.2017)

11) http://www.mcs.surrey.ac.uk/Personal/R.Knott/Fibonacci/fib.html
12) http://www.mcs.zinn-x.com/images/fibonacci-nature-nautilus4.jpg.
13) http://plus.maths,org/content/sites/plus.maths .org/fibonacci numbers in real life (date of access 24.01.2017)
14) http://www.popmath.org.uk/rpamaths/rpampages/sunflower.html
15) .http://www. Quora.com/what-are-the-real-life-applications of Fibonacci (date of access 24.01.2017)
16) Lin, Y., Peng, W., , Liu, Ya, H., Fibonacci Numbers in Daily Life
17) Mukherjee,M, Samanta,D., 2014, Fibonacci Based Text Hiding Using Image Cryptography, Lecture Notes on Information Theory, Vol. 2,(2),172-176.
18) Nikhat,P, Fibonacci in nature(http://www.fibonacci in nature(date of access15.01.2017))
19) Numbers in Nature (http://webecoist.com/2008/09/07 /17-amazing-examples-of-fractals-in-nature)
20) Raghu, M. E., Ravishankar, K. C., 2015, Application of classical encryption techniques for securing data- a threaded approach, International Journal on Cybernetics & Informatics (IJCI) Vol. 4,(2),125-132,DOI: 10.5121/ijci.2015.4.212.
21) Raphael, J.A., Sundaram, V., 2012, Secured Communication through Fibonacci Numbers and Unicode Symbols, International Journal of Scientific & Engineering Research, Vol 3(4), 1-5.