International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 10, October 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

Origin of Mathematical Models in Recent Technology

Kamaljeet Kaur[1], Nirupma[2]

Asstt Prof. Mathematics, Guru Nanak College for Girls, Sri Muktsar Sahib

I. INTRODUCTION

The great mathematicians have played a significant part in evolution of scientific and philosophical thought comparable to the philosophers and scientists themselves. The mathematics is assumed to have started with the origin of numbers. The core of actual theory is credited to Pythagoreans and his disciples started around 569 B.C. Pythagoras started a school concentrated on four subjects, called as '*mathemata*' namely *arithematica, harmonia* (music), *geometria* and *astrologia*. With the passage of time a trivium of logic, grammar and rhetoric was added and these seven subjects came to be looked upon as necessary course of study for an educated person.

1.1 Origin and ordering of numbers

The Pythagoreans philosophy is a sort of super numerology which assigned a number to everything. It is found in his writings that 1 represented reason, for reason could produce only one consistent body of truths; 2 stood for man and 3 for woman; 4 for justice, being first number which is sum and product of two equals; 5 for marriage, being sum of 2 and 3; and so on. These speculations must be borne in mind that the intellectuals of the classical Greek period were the ones who were engaged in laying the foundations for mathematics as a system of thought, making the society as male dominant.

During the middle ages, numerology took a form named *gematria* or *arithmology*, where by assigning numerical values to the letters of an alphabet in some order, each word was given an individual number. Two words were considered equivalent if the sum of numbers represented by their letters is same. For an instance, the word "amen" is $\alpha\mu\eta\nu$ in Greek with values 1, 40, 8 and 50 respectively whose sum is 99. In many old editions of the Bible, the number 99 appears at the end of a prayer as a substitute for amen.

In the modern ages, Galileo Galilei (1564–1642) said, "The universe cannot be read until we have learned the language and become familiar with the characters in which it is written. It is written in mathematical language, and the letters are triangles, circles and other geometrical figures, without which means it is humanly impossible to comprehend a single word. Without these, one is wandering about in a dark labyrinth. Carl Friedrich Gauss (1777–1855) referred to mathematics as "the Queen of the Sciences". Through this paper, I wish to share some areas, where mathematics is being used.

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 10, October 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

II. APPLICATIONS IN REAL LIFE:

2.1. RSA Cryptography

The process RSA, named after its inventors Rivest, Shamir and Adleman, is a public key cryptosystem used to secure data transmission. In this process, two very large primes (usually more than 100 digits) are taken by receiving computer and the product called public key is published. The sending computer uses this product to encrypt the message and send it to receiver. The public key can be used by anyone to encrypt the message but the information of primes is required to decrypt the message.

The keys for the RSA algorithm are generated the following way:

a) Choose two distinct prime numbers p and q.

b) Compute $n = pq$; n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.

c) Compute $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) = n-(p+q-1)$, where φ is Euler's totient function. This value is kept private.

d) Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$

e) Determine d as $d \equiv e^{-1} \pmod{\varphi(n)}$, i.e. solve for d given $d \cdot e \equiv 1 \pmod{\varphi(n)}$

f) e is released as the public key exponent.

g) d is kept as the private key exponent.

h) The message m can be encrypted to c by using encryption function

$$c \equiv m^e \pmod{n}$$

And message c can be decrypted using private key component d

$$c^d \equiv (m^e)^d \equiv m \pmod{n}$$

Example: Suppose two distinct chosen prime numbers are: $p = 61$ and $q = 53$

so that the product $pq = n = 3233$ and $\varphi(n) = (p-1)(q-1)$

$$\Rightarrow \varphi(3233) = (61-1)(53-1) = 3120$$

Now Choose a number e so that $1 < e < 3120$ which is co-prime to 3120, say $e = 17$

The corresponding value of $d=2753$ is the unique solution of $17d \equiv 1 \ (mod 3120)$, incongruent modulo 3120

Now, if we want to encrypt m=65, then using the congruence $c(m) = 65^7 \ (mod 3233)$ the encrypted message becomes c= 2790

Now, to decrypt c=2790, we need the use of private key (d=2753),

We calculate $m = 2790^{2753} (mod\ 3233)$, which gives unique solution m=65 incongruent modulo 3233.

2.2. MRI and Tomography:

The word tomography taken from Greek word tomos, "section" and grapho, "to write" refers to imaging by sections through the use of any kind of penetrating waves. The MRI scanners can create 3- dimensional images of the human body by taking countless 2- dimensional pictures from different directions. The process of recovering the original 3-dimensional model using the 2- dimensional pictures is called Tomography and this is done with the help of advanced mathematics, such as "Radon Transforms". The method is used in radiology, archaeology, biology, atmospheric science, geophysics, oceanography, plasma physics, materials science, astrophysics, quantum information, and other sciences. In most cases it is based on the mathematical procedure called tomographic reconstruction. The projection of an object, resulting from the tomographic measurement process at a given angle θ, is made up of a set of *line integrals* (see Fig. 1). As set of many such projections under different angles organized in 2D is called sonogram (see Fig. 3). In X-ray CT, the line integral represents the total attenuation of the beam of x-rays as it travels in a straight line through the object. The resulting image is a 2D (or 3D) model of the attenuation coefficient. That is, we wish to find the image $\mu(x, y)$. The simplest and easiest way to sonogram the method of scanning is the system of parallel projection, as used in the first scanners. For this discussion we consider the data to be collected as a series of parallel rays, at position r, across a projection at angle θ. This is repeated for various angles. Attenuation occurs exponentially in tissue:

$$I = I_0 \exp\left(-\int \mu(x, y)\, ds\right)$$

Where $\mu(x)$ is the attenuation coefficient at position x along the ray path. Therefore generally the total attenuation p of a ray at position r, on the projection at angle θ, is given by the line integral:

$$p(r, \theta) = \ln(I/I_0) = -\int \mu(x, y)\, ds$$

Using the coordinate system of Figure 1, the value of r onto which the point (x, y) will be projected at angle θ is given by:

$$x \cos\theta + y \sin\theta = r$$

So the equation above can be rewritten as

$$p(r, \theta) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x, y)\delta(x \cos\theta + y \sin\theta - r)\, dx\, dy$$

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 10, October 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

Where $f(x,y)$ represents $\mu(x,y)$. This function is known as the Radon transform (or *sonogram*) of the 2D object.

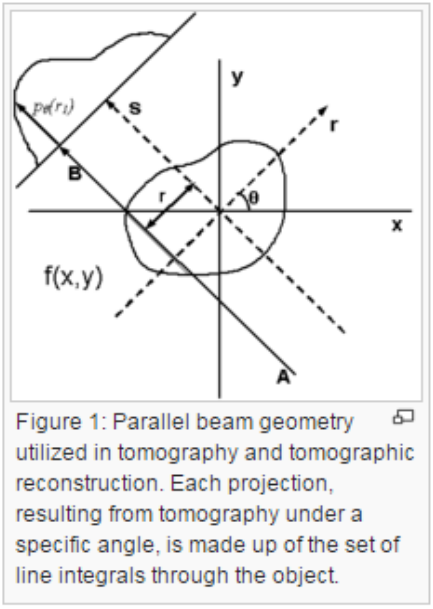

Figure 1: Parallel beam geometry utilized in tomography and tomographic reconstruction. Each projection, resulting from tomography under a specific angle, is made up of the set of line integrals through the object.

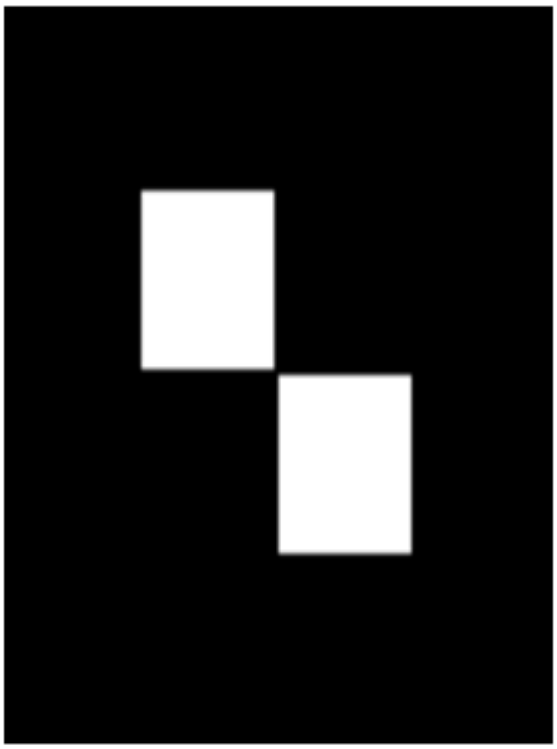

Fig. 2: Phantom object, two kitty-corner squares.

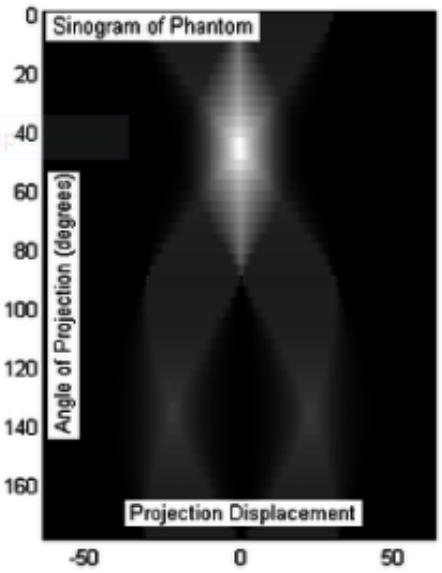

Fig. 3: Sinogram of the phantom object (Fig.2) resulting from tomography. 50 projection slices were taken over 180 degree angle, equidistantly sampled (only by coincidence the x-axis marks displacement at -50/50 units).

2.3.Transport Networks:

Everyday, on an average there are 93,000 flights originating from about 9,000 airports around the world. All planes, all luggages, every crew and all passengers have to be at the right place at the right time, and the planes need to be serviced and re-fueled. At the same time, planes should not crash when arriving at any busy airport. In addition to this, airlines want to save money by creating more efficient networks in which the planes take the best possible routes. So, the problem becomes an incredibly complex logistic challenge, solved with the help of Operation Research and Graph Theory. Each city-to-city flight is known as "leg". The airline fleets consist of different types of planes with varying seating capacities. The airlines' job is to assign the right plane to each flight leg while simultaneously determining the daily route of each plane – and minimizing its cost of operation. When assigning planes to flight legs, one model, known as the "fleet assignment model," matches the demand for each leg with the planes' seating capacities. When planes and flight legs have been matched, the airlines then take pairs of consecutive flight legs (such as, City X to City Y, and City Y

to City Z) and make them "through" flights using the "through assignment model." Through flights show up on the airline's schedule (such as, City X to City Z) as flights with one stopover at City Y. A technique known as "Very Large-Scale Neighborhood Search", in Mathematical optimization is a method that tries to find near optimal solutions to a combinatorial optimization problem by repeatedly transforming a solution into a different solution in the neighborhood of the current solution. The algorithm works as:

We define "A-B swaps" for two specified fleet types, A and B. An A-B swap consists of changing some legs flown by fleet type A to fleet type B, changing some legs flown by fleet type B to fleet type A, and then changing through connections as needed so that all constraints remain same. Illustration in Fig 4.

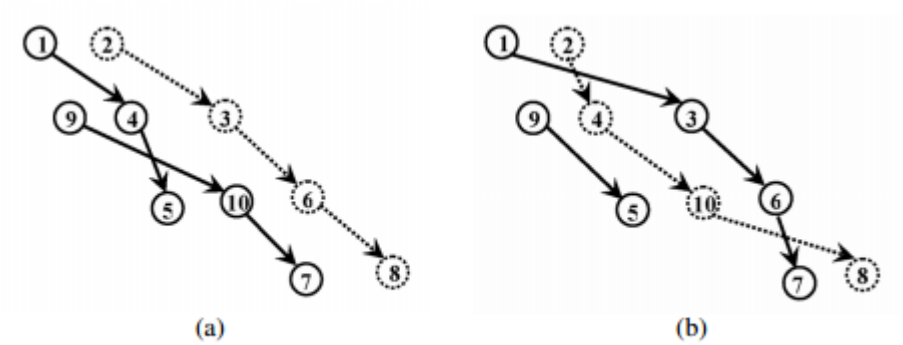

Figure 4. *Part of the solution (a) before and (b) after an A–B swap.*

Each flight is represented by a node and Connection between the fights by arcs. The nodes corresponding to the fleet type A are depicted by solid lines and that corresponding to the fleet type B by dotted lines. An A – B swap is said to be profitable if performing it decreases the fleet assignment costs and through benefits. The node set of the graph G^{AB} (x, y), for solution (x,y), denoted by N (G^{AB} (x, y)), is the set of flight legs that are assigned fleet type A or B in the solution (x'y), i.e., $N\left(G^{AB}(x,y)\right) = \{i \in N : y_i^A = 1 \text{ or } y_i^B = 1\}$. The improvement graph searches for a directed cycle

C in G^{AB} (x, y) satisfying some additional constraints. The presence of a node I in C indicates that flight I switches its flight type, either from A to B or from B to A. The cost c_{ij}^1 of the arc (i , j) is

equal to the increase in the fleeting and through contributions resulting from the "changes attributed to the arc (i , j)". Profitable A-B swaps are called valid cycles. If the A- B improvement graph contains a negative cost valid cycle, we perform the corresponding A-B swap and update the A-B improvement graph to reflect changes in the current solution. If there are no negative cost valid cycles, we choose another pair of fleet types. The algorithm terminates if a solution (x, y) is found

such that there are no cost improving A-B swaps possible for any pair A-B of fleet types. Since G^{AB} can contain an exponentially large number of valid cycles, the size of our neighborhood being very large. The identification of a valid cycle in G^{AB} is done through integer programming problem using CPLEX, a commercial integer programming solver. This technique allows testing trillions of neighbors and determining the best solution in a fraction of a second on a typical personal computer.

2.4.CROWD CONTROL:

There are countless examples of tragic accidents. As an instance, approximately 2400 people died in a crowd collapse during the annual Hajj pilgrimage at Mina, Mecca on 24 Sept., 2015. The general behavior analyzed in such situations is that movement of every human depends on the movement of all others in their immediate surroundings. The likelihood of accidents in future can be reduced, if we understand how local changes in human behavior and architecture affect the crowd as a whole.

Suppose there is a venue with crowd of people moving with constant velocity v_o, and constant density ρ_o such that the distance between the persons is also constant as shown in figure. If an observer measure the number of persons per unit time τ that pass him (i.e. traffic flow f). In τ time, each person has moved $v_0\tau$ distance, and so the number of persons that pass the observer in τ time is the number of cars in $v_0\tau$ distance.

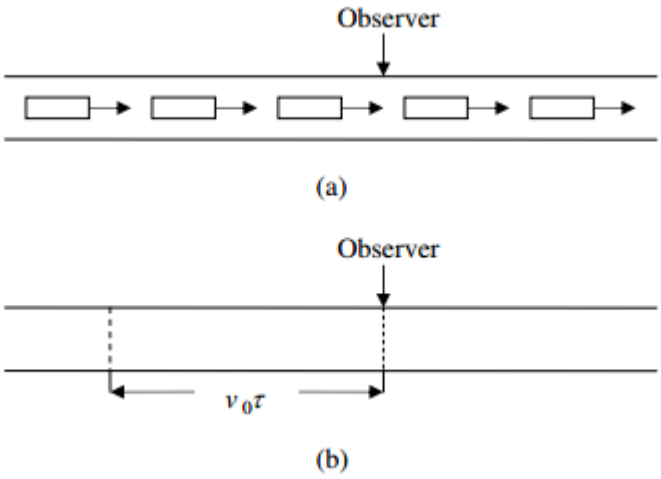

Fig 5: (a) Constant flow of persons, (b) Distance travelled in τ hours for a single person.

The crowd flow is given by $f = \rho_o v_0 \tau$; where ρ_o is the human density and there is $v_o\tau$ distance. The number of persons within $[x_1, x_2]$ at a given time t is the integral of human density given by

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 10, October 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

$N = \int_{x_1}^{x_2} \rho(x,t)dx$. N is maximum when human density is equal to jam densityρ_m.

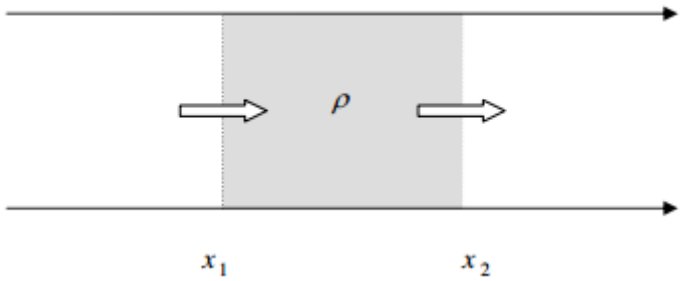

Fig 6: One dimensional flow

The rate of change of number of humans is given by $\frac{dN}{dt} = f_{in}(\rho,v) - f_{out}(\rho,v)$

$$\Rightarrow \quad \frac{d}{dt}\int_{x_1}^{x_2} \rho(x,t)dx = f_{in}(\rho,v) - f_{out}(\rho,v).$$

If the end points are independent variables (not fixed with time), then the full derivative is replaced by partial derivative to get

$$\frac{\partial}{\partial t}\int_{x_1}^{x_2} \rho(x,t)dx = f_{in}(\rho,v) - f_{out}(\rho,v) \qquad (a)$$

The number of persons with respect to distance is given by

$$f_{in}(\rho,v) - f_{out}(\rho,v) = -\int_{x_1}^{x_2} \frac{\partial f(\rho,v)}{\partial x}dx \qquad (b)$$

Equating (a) and (b) with each other, we get

$$\int_{x_1}^{x_2} \left[\frac{\rho(x,t)}{\partial t} + \frac{\partial f(\rho,v)}{\partial x}\right]dx = 0$$

This equation states that the definite integral of some quantity is always zero for all values of the independent varying limits of the integral. The only function with this feature is the zero function. Therefore assuming $\rho\,(x,t)$ and $f(\rho,v)$ are both smooth, the one dimensional conservation law is

$$\boldsymbol{\rho_t + f_x(\rho,v) = 0}$$

This equation is valid for crowd and many more physical quantities like traffic flow. This leads us to choose the velocity function for the crowd flow model to be dependent on density. The method of characteristics can be used to solve the initial value problem

$\rho_t(x,t) + f(\rho,v)_x = 0$ under the initial condition $\rho(x,0) = \rho_0(x)$; where $x\epsilon\,\mathbb{R}$ and time $t\epsilon\,\mathbb{R}^+$.

If the initial density and velocity field are know, the above equation can be used to predict future crowd density and the arrangements for the smooth flow can be made well in time to reduce crowd collapse accidents.

2.5Coding Theory - ISBN Code:

In the modern era, digital information has become a valuable commodity. It is extremely difficult, and often impossible to prevent errors when data is stored, retrieved, operated on and transmitted from a channel to another channel. To guarantee reliable transmission or to recover degraded data, techniques from coding theory are used. Coding theory includes both the error detection and the error correction. The simplest way to detect an error if a transmission channel is assumed to create a single error is to add a parity check bit at the end of the string. If a bit string contains an even number of 1's, we put a 0 at the end of string and put a 1 at the end if the string contains an odd number of 1's. This addition of a parity check bit is ensures the even number of 1's in every code. Whenever a transmission channel makes odd number of errors, the error can be detected. This method will not detect an even number of errors. To detect such errors, repetition codes can be used.

Example: To encode a transmitted message, which may contain errors, triple repetition code can be used. In such codes, we repeat each string of the message three times before sending, i.e if the message is abc, we encode it abcdefghi, where a=d=g, b=e=h and c=f=i. All possible code-words are: 000000000, 001001001, 010010010, 011011011, 100100100, 101101101, 110110110 and 111111111. The message will be decoded using majority rule. If we receive 011111010, then the message sent was 011 for the first, fourth and seventh strings are 0, 1 and 0 will be decoded as 1 (by majority), second, fifth and eighth strings are 1, 1 and 1 will be decoded as 1, and third, sixth and ninth strings are 1, 1 and 0 will be decoded as 1.

An important code, The ISBN Code is a milestone in the history of Standard Numbering in the Book Trade. The ISBN was introduced in 1967 as the Standard Book Number (SBN) jointly by J. Whitaker (regarded as the "Father of the ISBN") and sons Ltd, the British National Bibliography and the publishers association who set up the Standard Book Numbering agency (SBNA) for British publications. The initial ISBN configuration of recognition was generated in 1965 based upon the 9- digit Standard Book Numbering code created by Gordon Foster, Emeritus Professor of Statistics at Trinity College, Dublin. The 10- digit ISBN format was developed by International Organisation for Standardization (ISO) and was published in 1970. Now a days, an ISBN containing 13 digits is also used for books pubished after January 2007.

The ISBN consists of a group of symbols which identify each book title as a unique product. An ISBN consisting of ten digits divided into four groups and an ISBN consisting of 13 digits is divided into five groups, usually seperated by dashes or spaces, each group having a specific function.

1. For a 13-digit ISBN, a prefix element, 977 for International Standard Serial Number, 978 for International Standard Book Number and 979 for International Standard Music Number have been made available by GS1.
2. The *registration group element*, (language-sharing country group, individual country or territory) e.g. 0 is group identifier for English Language, 3 for German, 4 for Japanese etc.

3. The Publisher Number, e.g. 07 for McGraw Hill, 19 for Oxford University Press, 333 for Macmillan etc.
4. The title number assigned by publisher, e.g. 853803
5. The check digit

Method to chose Check digit for ISBN -10: If the digits of the ISBN are denoted by $= x_1x_2x_3x_4x_5x_6x_7x_8x_9x_{10}$, then the check digit x_{10} is chosen as

$$x_{10} = \sum_{k=1}^{9} kx_k \ (mod\ 11)$$

The tenth digit is chosen to make the weighted check sum ($\sum_{k=1}^{10} kx_k \equiv 0\ (mod 10)$,

I, e., the weighted check sum of all the ten digits is a multiple of 11.

Example: Suppose we have an ISBN code 0-306-40615-*?* Then the last digit is evaluated as follows:

$$x_{10} \equiv [(1*0)+(2*3)+(3*0)+(4*6)+(5*4)+(6*0)+(7*6)+(8*1) + (9*5)](mod\ 11)$$

$$\equiv 0+6+0+24+20+0+42+8+45\ (mod\ 10) \quad \equiv 2(mod\ 11)$$

So the last digit of this ISBN is 2.

Method to convert ISBN-10 into ISBN -13 : The conversion is quite simple as one only needs to prefix "978" to the existing number and calculate the new checksum using the ISBN-13 algorithm given by:

If the digits of the ISBN-13 are denoted by $x = x_1x_2x_3x_4x_5x_6x_7x_8x_9x_{10}x_{11}x_{12}x_{13}$, then the check digit x_{13} ranging from 0 to 9 is chosen so that sum of all the thirteen digits, each multiplied by its weight, alternatively 1 and 3 from the first digit is a multiple of 10, i.e., 13th digit is calculated by the following formula;

$$(x_1+3x_2+x_3+3x_4+x_5+3x_6+x_7+3x_8+x_9+3x_{10}+x_{11}+3x_{12}+x_{13}) \equiv 0 \pmod{10}.$$

Allotment of ISBN for Authors, Publishers and Educational/Research Institutions for their upcoming publications including conferences/ seminars proceedings in India is done through Raja Rammohun Roy National Agency for ISBN, Govt. of India, Ministry of Human Resource Development, Department of Higher Education, New Delhi.

2.6.CONCLUSION

The mathematics is a two-stage process. Rather than studying the world directly, mathematicians create so-called models of the world, and study them. We study a model, a sort of idealized world that contains things that we do not come across in everyday life, such as infinitely thin lines that stretch away to infinity, or absolutely perfect circles, and do not contain untidy, worldly things like hamburgers, chairs or human beings. These models can explain the great complexities of sciences, as complexity arises from the simplicity

In the modern age, the intensely abstract nature of pure Mathematics has brought the science nearer to philosophy. One is the line taken by the famous Cambridge mathematician G. H. Hardy, who was perfectly content, indeed almost proud, that his chosen field, Number Theory, had no applications, either then or in the foreseeable future. For him, the main criterion of mathematical worth was beauty. On the other hand, there are mathematicians who work in areas such as theoretical computer science, financial mathematics or statistics, areas of acknowledged practical importance. Mathematicians in these areas can point to ideas that have had a big impact, such as the use of Radon transform and Line Integrals in recovering the original 3-D model from 2-D snapshots used in Tomography, the construction of ISBN code using concept of congruences in number theory and the public-key cryptosystem invented by Rivest, Shamir and Adelman, which is now the basis for security on the internet, and which, as has been pointed out many times, is an application of number theory that Hardy certainly did not expect. Taken as a whole, then, mathematics is undeniably important in all spheres of life.

REFERENCES

1. R.L. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM, Feb. 1978, 21(2): 120-126.
2. Ahuja, Ravindra K.; Orlin, James B.; Sharma, Dushyant (2000), "Very large-scale neighborhood search" ,*International Transactions in Operational Research* 7 (4–5): 301–317
3. C. Barnhart and K.T. Talluri, *Airlines operation research in Design and Operation of Civil and Environmental Engineering systems*, McGarity and C. Revelle, eds., Wiley Interscince, New York, 1997, 435-469.
4. R. Gopalan and K.T. Talluri, *Mathematical models in airline schedule planning: A survey*, in Ann. Oper. Res. 76 (1998), 155- 185.
5. K.T. Talluri, *Swapping Applications in a daily fleet assignment*, Transportation Sci., 31 (1996), 237-248
6. Al- Nasur, S. and Kachroo, P. (2006), *A microscopic to macroscopic crowd dynamic model. In 9th International IEEE Conference on ITSC, pages 606-611*
7. Al-nasur, Sadeq J. "New models for Crowd dynamics and control." (2006).
8. Shinohara, Kazunori, and Serban Georgescu. "Modelling adopter behaviour based on the Navier Stokes equation." *ISRN Mathematical Analysis* 2011 (2010).
9. Renardy, M. and Rogers, R. (2004). *Introduction to Partial differential Equations,* Springer, NY., 2nd edition

10. Hughes, R. L. (2002), *A continuum theory for the flow of pedestrians,* Transportation Research Part B, 36: 507-535
11. Bradley, Philip (1992). "Book numbering: The importance of the ISBN PDF (245KB). *The Indexer*. **18** (1): 25–26.
12. R. Hill, A First Course in Coding Theory, Oxford University Press, Oxford, 1997.
13. S. Ling & C. Xing, Coding Theory: A First Course, Cambridge Univ. Press, Cambridge, 2004.
14. Bradley, Philip. "Book numbering: the importance of the ISBN." *The Indexer*18.1 (1992): 25-26.
15. Öchsner, Andreas. "Types of Scientific Publications." *Introduction to Scientific Publishing*. Springer Berlin Heidelberg, 2013. 9-21.
16. Achalare, R. A., S. V. Patil, and S. S. Patil. "Significance of ISSN and ISBN in Publications." *Current Pharma Research* 5.1 (2014): 1378.
17. www.google.com