12th International Congress on Mathematical Education
Regular Lectures 6-12
8 July – 15 July, 2012, COEX, Seoul, Korea

LEARNING MATHEMATICS IN SECONDARY SCHOOL: THE CASE OF MATHEMATICAL MODELLING ENABLED BY TECHNOLOGY

Jonaki B Ghosh
Lady Shri Ram College for Women, University of Delhi, New Delhi, India
jonakibghosh@gmail.com

This paper describes a study which was undertaken to investigate the impact of teaching mathematics using mathematical modelling and applications at senior secondary school level in India. While traditionally the emphasis in mathematics teaching has been on the development of procedural skills, the study shows that the use of modelling and applications enabled by technology enhanced student's understanding of concepts and led them to explore mathematical ideas beyond their level. Using this approach, a balanced use of technology and paper pencil skills led to a deeper understanding of the subject.
Keywords: Mathematical Modelling, Technology, Visualization, Exploration, Paper pencil skills

INTRODUCTION

Increasingly, many countries across the world have witnessed a growing collection of didactical research on including mathematical applications and modelling in secondary school and this has impacted the mathematics curricula in these countries. The benefits of integrating applications and modelling in the curriculum are manifold. They help to motivate students and create a context for applying mathematical theory. They help students to learn new mathematical content and see that mathematics can be fruitfully applied to solve real problems. Above all they help to highlight the relevance of mathematics as a discipline and thus contribute to sustaining the student's interest in the subject.

In didactical research on mathematical modeling, *it is possible to identify a number of different approaches and perspectives in mathematics education research on the teaching and learning of modelling. Kaiser & Sriraman (2006) report about the historical development of different research perspectives and identify seven main perspectives describing the current trends in the research field*. (Blomhøj, 2008, p.2)

One of the perspectives among them is the Educational Perspective. *The main idea of the educational perspective is to integrate models and modelling in the teaching of mathematics both as means for learning mathematics and as an important competency in its own right*. (Blomhøj, 2008, p.5)

Blomhøj (2004), identifies the two main arguments for teaching mathematical modelling at the secondary level. These are

(1) *Mathematical modelling bridges the gap between students' real life experiences and mathematics…*

(2) *In the development of highly technological societies, competences for setting up, analysing, and criticising mathematical models are of crucial importance*. (Blomhøj, 2008, p.6)

This paper attempts to investigate the impact of integrating mathematical modelling and applications into a topic of the senior secondary mathematics curriculum of India. As suggested by the educational perspective, it aims to use modelling to provide the student with the opportunity to learn new mathematics. Research has also shown that the use of technology tools can greatly enhance student's explorations and investigations. Herwaarden (2001) gives a detailed description of a course in calculus and linear algebra for first year university students where integration of computer algebra with paper and pencil methods helped to enhance conceptual understanding. Arnold (2004) describes CAS (computer algebra system) as "the ultimate mathematical investigative assistant" (p. 19) which allows the student to engage in "purposeful and strategic investigation of problems" (p. 21). Heid (2001) describes CAS as a cognitive technology which makes higher level mathematical processes accessible to students. According to her, CAS plays a dual role: that of an amplifier and a reorganizer. On one hand, CAS plays the role of an 'amplifier' by making it possible to generate a larger number and greater range of examples and thus can be used to extend the curriculum. On the other hand it serves the role of a 'reorganizer' by changing the fundamental nature and arrangement of the curriculum. Lagrange (1999) also suggests that CAS helps to set a balance between skills and understanding. It lightens the technical work thus allowing students to focus on concepts and applications. These pedagogical affordances of the use of CAS can also be extended to other technology tools available for mathematics instruction.

The Senior Secondary Mathematics Curriculum in India

In the Indian school curriculum, mathematics is largely taught as an abstract subject in the traditional 'chalk and board' manner. Topics are often taught without any substantial reference to their applications to real life problems, thus making the subject pedantic. Traditionally, the emphasis has been on the development of manipulative skills and the school assessment also tests the same. The teaching and learning of mathematics at the senior secondary school is driven by preparation for the school leaving examinations (at the end of year 12) which often determine a student's future. It is at this stage that the student has to make a choice as to whether she will opt for the science, commerce or humanities stream and her performance in the school leaving examination holds the key to her future in terms of career opportunities. In this regard the school leaving examination at the end of year 12 is indeed a high stakes examination and its impact looms large over the curriculum at the senior secondary stage.

The National Curriculum Framework (NCF, 2005) of India, in its position paper on teaching of mathematics, begins by stating that the primary goal of mathematics education is the

mathematisation of the child's thought processes. It recommends that mathematics teaching at all levels be made more 'activity oriented'. While this has been the primary driving force for revisiting and revamping the elementary school mathematics curriculum, it has had little impact on the senior secondary curriculum. At this level, the textbooks, which happen to be the only resource for teachers and students, are usually examination oriented. Every chapter begins with a brief introductory note which sometimes includes a historical background of the development of the field, and then introduces the basic concepts of the topic. The chapter is further divided into sections and sub-sections which deal with definitions, theorems, results, examples and exercises. The mathematics curriculum in grade 12 is dominated by differential and integral calculus accounting for almost half of the content. Other topics include Matrices and Determinants, Vector Algebra, Three Dimensional Geometry, Linear Programming and Probability. Manipulative and computational aspects of these topics, rather than visualization and exploration of concepts and ideas, dominate mathematics at this stage. Topics like sets, relations, logic, sequences and series, linear inequalities and combinatorics are introduced in grade 11, but only at a superficial level. The syllabus of grade 12 does not include these topics and hence there is no room for delving deeper into these areas. The NCF 2005 recommends that curriculum designers reconsider the distribution of content between grades 11 and 12.

The NCF 2005 strongly recommends the inclusion of modeling activities in the curriculum. The document suggests that this can be done in the form of investigatory exercises or projects which will enable the student to see the relevance of the mathematics taught at school. Such projects need to be designed in a manner so as to cover the depth and breadth of the topics taught while at the same time provide the student with ample scope to explore and apply important mathematical concepts and ideas in solving problems. Another important recommendation made by the NCF is the setting up of mathematics laboratories in schools. A mathematics laboratory can provide students with the opportunity to 'discover' mathematics through exploration and visualization of concepts and ideas and mathematical modelling activities can be integrated into the curriculum through the mathematics laboratory.

THE STUDY

The study described in this paper is based on the recommendations of the National Curriculum Framework 2005. It aims at exploring how learning is impacted by integrating mathematical modelling and applications into the senior secondary mathematics curriculum. In this study, a module titled *Learning Mathematics through Mathematical Modelling and Applications* was developed by the author and 30 students of grade12, selected from two schools of Delhi, participated in the study. The module was based on the topic *Matrices and Solutions of Systems of Equations* which is a part of the grade 12 syllabus. The module was spread over 16 hours, that is, eight sessions of two hours each, conducted on four consecutive school days. Graphics calculators and Mathematica were used as the primary vehicles of exploration. Throughout the module student's paper pencil work was recorded. At the end of the module students were required to respond to a short questionnaire and give a written

feedback describing their learning experience in the module. The objective of the study was to reflect upon the following research questions

- How does the integration of applications and modelling activities impact student's understanding of mathematical concepts?
- Does introducing mathematical modelling activities, enabled by technology, help students access higher level mathematical concepts?
- How does technology driven mathematical modelling activities affect student's perception of paper and pencil tasks?
- Does the integration of modelling and applications help to sustain and enhance student's interest in the subject?

Educational Setting

All 30 students who were a part of the study were from two Delhi schools which follow the curriculum prescribed by the Central Board of Secondary Education (CBSE), a national board for school education in India. The CBSE (CBSE, 2009) does not prescribe the use of technology for teaching mathematics or permit its use in examinations. Individual schools however have the freedom to integrate technology in their classrooms. The topic, Matrices and Determinants comprises of the subtopics on types of matrices, matrix operations, inverse of a matrix, computing determinants and their properties and solutions of systems of equations. The emphasis is on manipulation and on developing computational skills in dealing with matrices and determinants. The exercises at the end of a chapter also test computational skills. Two sample questions from the textbook exercises are

If $A = \begin{bmatrix} 3 & 1 \\ -1 & 2 \end{bmatrix}$, show that $A^2 - 5A + 7I = O$

Using properties of determinants prove that

$$\begin{vmatrix} a^2+1 & b^2 & c^2 \\ a^2 & b^2+1 & c^2 \\ a^2 & b^2 & c^2+1 \end{vmatrix} = 1 + a^2 + b^2 + c^2$$

The 30 students who were a part of the study had been taught matrices in a traditional manner in their regular class. However the manner in which the content was presented did not focus on the need and use of matrices in solving or modelling practical problems. In the module designed by the author, the emphasis was on integrating applications and mathematical models based on matrices to introduce concepts and procedures thereby highlighting the relevance of matrices as a tool for solving problems.

This section includes a detailed description of the laboratory module in which 30 grade 12 students explored the topic of Matrices and Determinants through applications and mathematical models enabled by technology. In some of the sessions students were given worksheets which required them to explore a problem or a mathematical model and record their solutions or observations. During the module students were given access to graphics

calculators for computational work. While solving systems of equations in three unknowns, Mathematica was used to plot the planes to help visualize the solution. Throughout the module students were encouraged to do certain procedures, such as, multiplying 2 by 2 matrices, finding determinants of 3 by 3 matrices or solving a system of equations in matrix form, by hand. The objective was to maintain a balance between technology enabled explorations and procedural skills. The graphics calculator helped to trivialize tedious calculations thus enabling students to focus on exploring the models and interpreting the solutions. The applications or mathematical models discussed in the module were taken from Genetics, Cryptography and the Pagerank Algorithm. Before transacting the module a short workshop session on the graphics calculator (Casio FX 9860) was conducted to familiarize the students with some of the basic features of the calculator.

Session 1: Introduction to Matrices

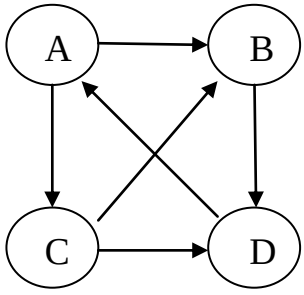
Students were introduced to the concept of a matrix using the following two examples

Example 1

The results of a chess championship between four players A, B, C, D are as follows

A defeated B and C; B defeated D; D defeated A; C defeated B and D.

This information may be represented in the form of the network diagram shown in Figure 1. The arrows point from winners to losers. The information regarding wins and losses can also be arranged in the form of a matrix using 0's and 1's.



$$M = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

Figure 1. Network diagram and incidence matrix representing the results of a tournament

In the matrix M, rows 1,2,3 and 4 as well as columns 1,2,3 and 4 denote the players A,B,C and D respectively. This is a first order dominance matrix where 1's denote the victories and 0's the losses. Thus, 1 in position (1,2) i.e in row 1 and column 2, represents the fact that player A has defeated player B.

Example 2

In this example students were introduced to Autosomal inheritance, where the inherited trait under consideration (say petal color in a certain plant) is assumed to be governed by a set of

two genes, denoted by **A** (red color) and **a** (white color). The three possible genotypes are **AA**, **Aa** and **aa** where **AA** produces red flowers, **Aa** produces pink flowers and **aa** produces white flowers. Every individual inherits one gene from each parent plant with equal probability. Thus, if the parent pairing is **AA-Aa** , the offspring will inherit an '**A**' gene from the first parent and either an '**A**' or an '**a**' (with equal probability) from the second parent. Thus the offspring is likely to inherit a genotype of **AA** or **Aa** with probability $\frac{1}{2}$ each.

Students were asked to list all possible parent pairings along with the probabilities of the resulting offspring combinations which led to the *genotype probability matrix* as shown in Table 1. This example was an interesting way of recalling the concept of probability and highlighting the fact that the entries of a matrix could also be probabilities.

Table 1. The Genotype Probability Matrix

		Parent pairings					
		AA - AA	AA - Aa	AA - aa	Aa - Aa	Aa - aa	aa-aa
Offspring outcomes	AA	1	1/2	0	1/4	0	0
	Aa	0	1/2	1	1/2	1/2	0
	aa	0	0	0	1/4	1/2	1

By the end of this session students were introduced to a matrix as a mathematical model for organising information in rows and columns. They were also acquainted with different practical situations in which matrices were used to represent information.

Session 2: Matrix operations

The second session began with the definition of a matrix, the notion of order of a matrix, symbolic representation in the form $A = \lfloor a_{ij} \rfloor_{m \times n}$ and different types of matrices (square matrix, row and column matrices, zero and identity matrices) examples of which were taken from the above matrix models as well as other examples. The operations of matrices were also introduced with the help of the above models. For example, matrix multiplication was introduced using a garment manufacturing example where the cost incurred by each of three factories for manufacturing three types of garments was obtained by multiplying the production matrix P to the cost matrix C.

$$PC = \begin{bmatrix} 3000 & 1000 & 1500 \\ 5000 & 1650 & 2000 \\ 3500 & 1450 & 1000 \end{bmatrix} \begin{bmatrix} 1500 \\ 800 \\ 500 \end{bmatrix} = \begin{bmatrix} 3000\times1500+1000\times800+1500\times500 \\ 5000\times1500+1650\times800+2000\times500 \\ 3500\times1500+1450\times800+1000\times500 \end{bmatrix}$$

This example helped to highlight the necessity of multiplying the matrices row by column. Students were then made to explore and observe the properties of matrix multiplication by working out products of matrices of different orders. By doing this they realized that matrices of different orders could be multiplied *if and only if the number of columns of the matrix on the left is equal to the number of rows of the matrix on the right*. Students used the graphics calculator for computing products of matrices of larger orders.

For squaring a matrix they revisited the chess tournament example and calculated M^2. The author asked them to find the relationship between M^2 and the results of the tournament. After some facilitation students figured out that each row of M^2 denotes the second order victories of each player over the others. E.g the number 1 in row 1 of M^2 indicates that player A has had one second order victory over B (i.e A defeated C and C defeated B). After this, students were required to combine the results of the first order victories and the second order victories by evaluating the expression $M + \frac{1}{2}M^2$. This exercise was a way to get them to use the operations of addition, multiplication as well as scalar multiplication. The row sums of the resultant matrix were used to rank the teams.

By the end of this session students were comfortable with performing matrix operations by hand as well as on the graphics calculator. There was no compromise on procedural skills as most students preferred to solve the exercises by hand and then verify their solutions using the graphics calculator.

Sessions 3 and 4: Investigations based on Matrix Operations

In this session the transpose of a matrix and its properties was introduced. To verify the property that the transpose of the product of two matrices is the product of the transposes taken in the reverse order, students were made to revisit the garment manufacturing example in which they worked out $(PC)^T$ and verified that it is equal to $C^T P^T$.

Having completed the above exercise, students explored the example on Autosomal inheritance. The problem was to create a model which could predict the genotype distribution of a plant population after any number of generations under specific breeding programs. For formulating the problem it was assumed that a_n, b_n and c_n are the fraction of plants of genotypes **AA**, **Aa** and **aa** in the nth generation of the plant population where n = 0,1,2……and $a_n + b_n + c_n = 1 \ \forall \ n$. a_0, b_0, c_0 were to denote the initial distribution of genotypes **AA**, **Aa** and **aa** respectively in the population. Students were first introduced to the case when all the plants are fertilized with type **AA**. The genotype distributions a_n, b_n and c_n were represented by the equations

$$a_n = a_{n-1} + \frac{1}{2}b_{n-1}, \qquad b_n = \frac{1}{2}b_{n-1} + c_{n-1}, \qquad c_n = 0. \qquad (1)$$

Students were then introduced to write the above equations in matrix notation as $x^{(n)} = Mx^{(n-1)}$,where $n = 1,2,\ldots\ldots$ and

$$\mathrm{x}^{(\mathrm{n})} = \begin{bmatrix} a_n \\ b_n \\ c_n \end{bmatrix} \text{ and } \mathrm{x}^{(\mathrm{n-1})} = \begin{bmatrix} a_{n-1} \\ b_{n-1} \\ c_{n-1} \end{bmatrix} \text{ and } M = \begin{bmatrix} 1 & 1/2 & 0 \\ 0 & 1/2 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

They verified using matrix multiplication that $x^{(n)}$ when equated to the product $Mx^{(n-1)}$ actually led to the equations (1). They used the equation $x^{(n)} = Mx^{(n-1)}$ to arrive at $x^{(n)} = M^n x^{(0)}$ where $\mathrm{x}^{(0)}$ is the matrix of the initial population distributions. Students were able to do this easily by repeatedly putting n as 1,2,3 etc. This matrix equation was used to predict the distribution of genotypes in the *n*th generation for a given initial distribution $x^{(0)}$.

The next exercise required them to use graphics calculators and the equation $x^{(n)} = M^n x^{(0)}$ to find the genotype distribution of a plant population in the first, second, third, fourth and fifth generations when the initial distributions $x^{(0)}$ were given as

$$\begin{bmatrix} 0.5 \\ 0.3 \\ 0.2 \end{bmatrix}, \quad \begin{bmatrix} 0 \\ 0.5 \\ 0.5 \end{bmatrix}, \quad \begin{bmatrix} 0.2 \\ 0.25 \\ 0.55 \end{bmatrix}$$

Figure 2 gives the screen shots of their calculations.

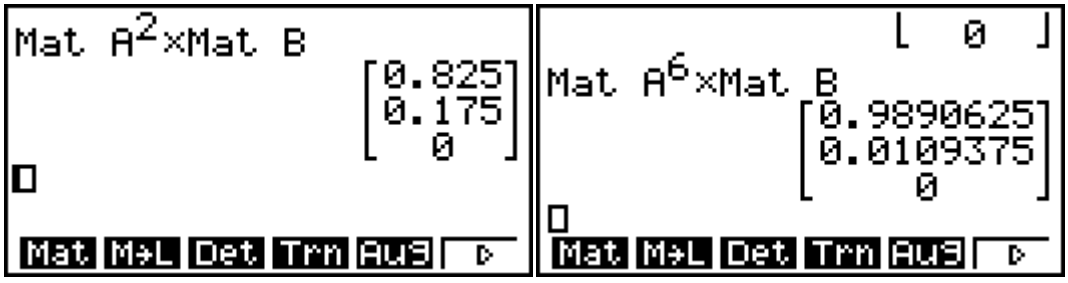


Figure 2. Graphics calculator screenshots showing matrix calculations for finding the steady state genotype distribution

After completing the calculations the students interpreted the solutions in terms of the proportion of the three genotypes in the population after 5 generations. Some students began to calculate for the 6th and 7th generations and then calculated for the 10th generation. They concluded that in the long run after a certain number of generations, the proportions of the

three genotypes steady out to the matrix $\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$ and that this is independent of the initial distribution. They then changed matrix M to explore the case when each plant is fertilised with type **Aa**. Here the steady state distribution was obtained as $\begin{bmatrix} 0.25 \\ 0.5 \\ 0.25 \end{bmatrix}$. Thus the calculator took over the computational part of the modelling process and enabled students to extend their investigations. They explored the steady state distribution in other breeding situations such as

- If each plant was fertilised with a plant of its own genotype.
- If alternate generations of plants were fertilised with genotypes AA and Aa respectively.

Sessions 5 and 6: Solutions of Systems of Equations

In this session of the module, students used Mathematica to visualize the solutions of systems of equations in three unknowns by plotting the planes representing the equations in three unknowns. They used the graphics calculator for solving the equations. They were encouraged to work in pairs or in groups of three and each group was given a worksheet with five systems of equations in the unknowns *x*, *y* and *z* as follows.

$$\begin{array}{lll} x+y+z=2 & x+y+z=1 & x+y+z=1 \\ x+3y-z=1 & x+4y+9z=3 & x+y+z=7 \\ -x+4y+9z=3 & 2x-y-6z=0 & 2x+2y+2z=25 \end{array}$$

(i) (ii) (iii)

$$\begin{array}{ll} x-2y+3z=2 & x+y+z=1 \\ 2x-y+2z=3 & x+y+z=12 \\ x+y-z=4 & 8x+y-6z=0 \end{array}$$

(iv) (v)

Students were introduced to the method of solving systems of equations by reducing them to triangular form using elementary row operations. The process of reducing the system (i) to triangular form was demonstrated on the graphics calculator. The system (i) had a *unique solution* $x=\frac{3}{2}$, $y=0$ and $z=\frac{1}{2}$. Figure 3 shows the screen shots of the row operations performed on their graphics calculator.

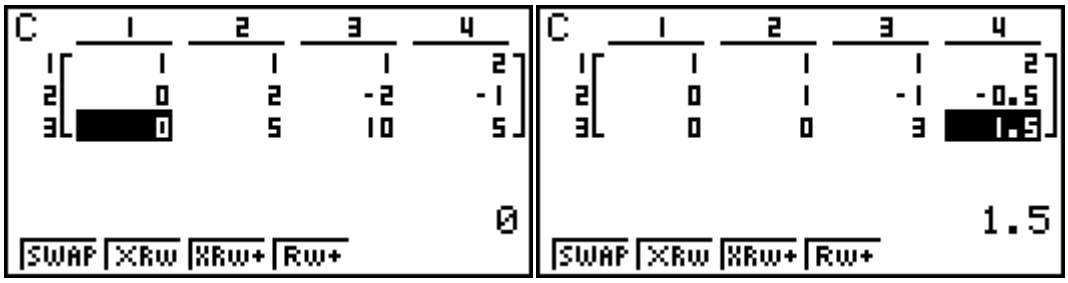


Figure 3. Graphics calculator screenshots for solving a system of equations using elementary row operations

The students also verified their solution using Mathematica's **Solve** command. This was repeated for all five systems of equations. After solving the system of equations (ii) the last equation was read as 0.z = 0. This was interpreted as a case of *infinitely many solutions* where z may be treated as a free variable. For the systems of equations (iii), (iv) and (v) row reduction led to an equation of the form 0.z = k which was interpreted as inconsistency. Students then used Mathematica's **Plot3D** command to plot the planes for all five systems. The plot for (i) showed three planes meeting at a point. The output for (ii) revealed three planes meeting in a line. See Figure 4. For (i) students interpreted that the point where the three planes meet must be the unique solution having the coordinates $x = \frac{3}{2}$, $y = 0$ and $z = \frac{1}{2}$. For (ii) they made the guess that since any point on the line (where the three planes meet) is a solution of the system, this was identified as a case of infinitely many solutions.

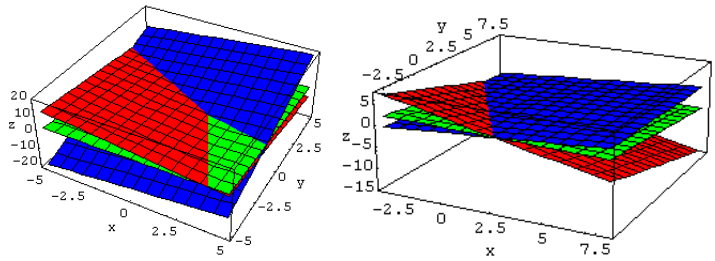


Figure 4. Mathematica plots of the planes representing systems of equations (i) and (ii)

The Mathematica outputs for (iii), (iv) and (v) revealed three different situations of inconsistency. In (iii) the planes were parallel. Since the planes do not meet, students concluded that the system was inconsistent. The plot of (iv) revealed that the *three planes intersected pair wise in three non-planar parallel lines*. Since all three planes do not intersect in a single point or line, students concluded that the three equations are inconsistent. For (v) students concluded that *two parallel planes were intersected in two parallel lines by a third*

non-parallel plane. Since all three planes do not intersect in a single point or line the three equations are inconsistent. Visualizing the systems of equations in the form of planes in three dimensions led to a graphical insight which would not have been possible without the 3- D graphing feature of Mathematica.

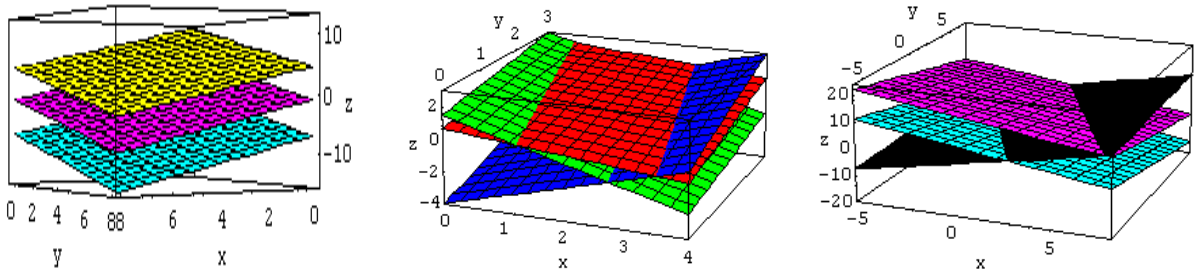


Figure 5. Mathematica plots of systems of equations (iii), (iv) and (v) showing three different situations of inconsistency.

The Pagerank Algorithm

As a practical example of arriving at systems of equations in more than two unknowns students were introduced to the Google Pagerank Algorithm. The pagerank of a webpage is calculated using the following

$$PR(A) = 1 - d + d\left(\frac{PR(T_1)}{C(T_1)} + \frac{PR(T_2)}{C(T_2)} + ... + \frac{PR(T_n)}{C(T_n)}\right) \qquad (2)$$

where PR denotes the page rank of a page, T_i are pages which link to A, $C(T_i)$ are the outbound links from page T_i, and d is the damping factor (usually taken as 0.85)

Students were asked to apply the formula to a simple website comprising of two pages A and B as shown in Figure 3. The arrows indicate that there is a link from page A to page B and vice versa.

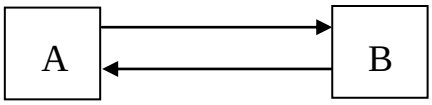


Figure 6. A diagram representing a website consisting of two pages.

Considering d = 0.5 and using (2) they obtained the following equations.

PR(A) – 0.5 PR(B) = 0.5

-0.5 PR(A) + PR(B) = 0.5 (3)

In matrix form, (3) can be written as MX = B, where

$$M = \begin{bmatrix} 1 & -0.5 \\ -0.5 & 1 \end{bmatrix},\ X = \begin{bmatrix} PR(A) \\ PR(B) \end{bmatrix},\ B = \begin{bmatrix} 0.5 \\ 0.5 \end{bmatrix}$$

To obtain the page ranks of pages A and B it was required to solve the matrix equation MX = B. At this point the idea of an inverse of a matrix was introduced. Students were told that if they could find a matrix N such that NM = I, the identity matrix, then by multiplying both sides of the equation MX = B by N one could obtain

N(MX) = NB leading to (NM)X = NB or IX = NB.

Thus X = NB. Since N is the inverse of M we can write N as M^{-1}. Hence $X = M^{-1}B$.

The process of finding the inverse of M was however not discussed here. Students used the graphics calculator for solving the equation $X = M^{-1}B$ (Figure 7) and arrived at the solution of the matrix equation as the pagerank vector $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$, which implied that PR(A) = PR(B) = 1.

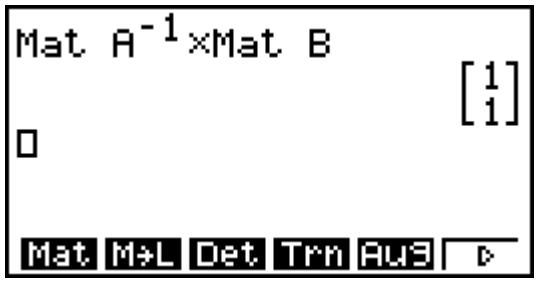


Figure 7. Graphics calculator screenshot for computing the pagerank vector

The next exercise required the students to consider the website in Figure 8, comprising of the four pages A,B,C and D and to find the pageranks of the pages using d = 0.85 as the damping factor

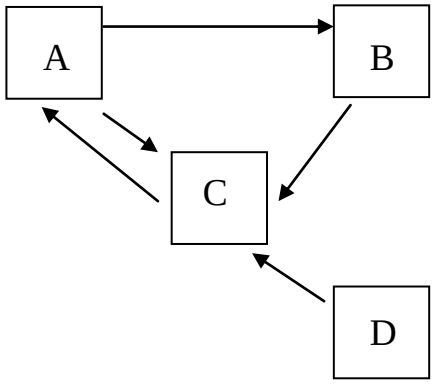


Figure 8. A website consisting of four pages

Considering PR(A) = x, PR(B) = y, PR(C) = z and PR(D) = w, students used (2) and obtained four equations in four unknowns x,y,z and w.

$x - 0.85\,z = 0.15,\ -0.425\,x + y = 0.15,\ -0.425\,x - 0.85\,y - 0.85\,w = 0.15,\ w = 0.15$ (4)

They solved the equations by reducing the augmented matrix of (4) to triangular form.

The primary objective of this session was to help students visualize solutions of equations in three unknowns and interpret them graphically. An attempt was made to ensure that there was no compromise on the 'by hand' skills as students were also required to work out the solutions manually by reducing the system of equations to triangular form. The Mathematica plots gave a physical meaning to their by-hand solutions. Introducing them to the Pagerank algorithm aroused their interest since all students are Google surfers and importance of webpages was something they were interested in. It also led to the need for solving a system of equations.

Sessions 7 and 8: Exploring the Inverse of a Matrix

In the last session of the module students were introduced to the idea of the inverse of a matrix and were made to find the inverse of any 2 by 2 matrix $A=\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ by solving the matrix equation $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} x & y \\ z & w \end{bmatrix}=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Many students asked whether there was a practical use of the inverse of a matrix.

Secret Codes Using Matrices: The Hill Cipher Method

At this point they were introduced to the Hill Cipher method (Eisenberg, 1999), an application of matrices to cryptography, the science of making and breaking codes. Ciphers are methods for transforming a given message, the plaintext, into a new form that is unintelligible to anyone who does not know the key (the transformation used to convert the plain text). In a cipher the key transforms the plaintext letters to other characters. The secret rule, that is, the inverse key, is required to reverse the transformation in order to recover the original message. The students were given 29 characters and their numerical values as shown in Table 2.

Table 2. The substitution table for the Hill Cipher Method

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

P	Q	R	S	T	U	V	W	X	Y	Z	.	_	?
15	16	17	18	19	20	21	22	23	24	25	26	27	28

The encoding matrix was chosen as $\begin{bmatrix} 1 & 4 \\ 2 & 9 \end{bmatrix}$. Students were then introduced to the encoding process (converting the plaintext to the ciphertext) as follows

Step 1. Let the plaintext message be **MATH_IS_FUN.**

Step 2. Convert it to its substitution values from the substitution table and group them in pairs

12 0 19 7 27 8 18 27 5 20 13 26

Each pair will form a column of the message matrix M.

Step 3. Compute the product EM

$$EM = \begin{bmatrix} 1 & 4 \\ 2 & 9 \end{bmatrix} \begin{bmatrix} 12 & 19 & 27 & 18 & 5 & 13 \\ 0 & 7 & 8 & 27 & 20 & 26 \end{bmatrix} = \begin{bmatrix} 12 & 47 & 59 & 126 & 85 & 117 \\ 24 & 101 & 126 & 279 & 190 & 260 \end{bmatrix}$$

Step 4. Reduce the product modulo 29 to obtain the Hill – 2 – cipher values. This is called a Hill – 2 – cipher since the encoding matrix is a 2 by 2 matrix. Students required help in understanding the concept of reducing a number modulo 29. The meaning of the congruence relation a ≡ b (mod c) was explained using various examples.

$$EM = \begin{bmatrix} 12 & 47 & 59 & 126 & 85 & 117 \\ 24 & 101 & 126 & 279 & 190 & 260 \end{bmatrix} = \begin{bmatrix} 12 & 18 & 1 & 10 & 27 & 1 \\ 24 & 14 & 10 & 18 & 16 & 28 \end{bmatrix} (\text{mod } 29)$$

Step 5. The encrypted message is **MYSOBKS_QB?**

Some screenshots of the encoding process is shown in Figure 9.

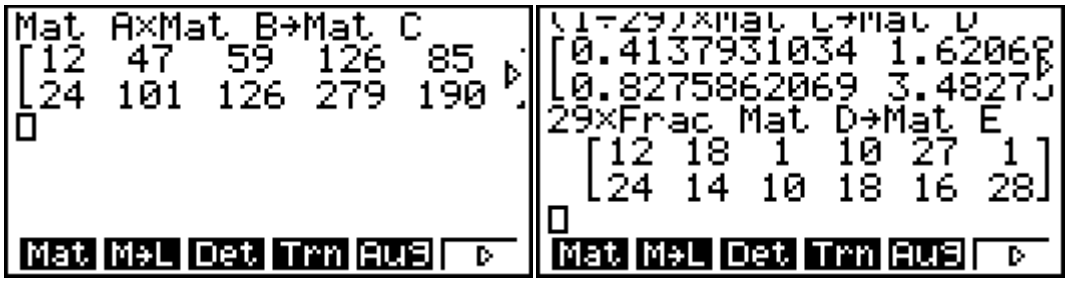


Figure 9. Graphics calculator screenshots for the encoding process of the Hill Cipher Method

The decoding process was introduced as follows

Step 1. The ciphertext message reaches the receiver as **MYSOBKS_QB?**

Step 2. Convert the characters to their respective Hill-2-cipher values and make pairs.

12 24 18 14 1 10 10 18 27 16 1 28

Each pair will form a column of a matrix N.

Step 3. Compute the product E^{-1} N

$$E^{-1}N = \begin{bmatrix} 9 & -4 \\ -2 & 1 \end{bmatrix} \begin{bmatrix} 12 & 18 & 1 & 10 & 27 & 1 \\ 24 & 14 & 10 & 18 & 16 & 28 \end{bmatrix} = \begin{bmatrix} 12 & 106 & -31 & 18 & 179 & -103 \\ 0 & -22 & 8 & -2 & -38 & 26 \end{bmatrix}$$

Step 4. Reduce the product modulo 29 to obtain the substitution values.

$$E^{-1}M = \begin{bmatrix} 12 & 106 & -31 & 18 & 179 & -103 \\ 0 & -22 & 8 & -2 & -38 & 26 \end{bmatrix} = \begin{bmatrix} 12 & 19 & 27 & 18 & 5 & 13 \\ 0 & 7 & 8 & 27 & 20 & 26 \end{bmatrix}$$

When the values are written column wise they become

12 0 19 7 27 8 18 27 5 20 13 26

which translates to **MATH_IS_FUN.**

Students found this technique very exciting. They wanted to try out the more examples and were divided into groups. Each group had to encode a message and post it on the whiteboard after declaring the encoding matrix. The 'receivers' had to use the inverse matrix to decode the message. Students were asked to choose encoding matrices with determinant equal to 1. Though it was a challenge, students were able to come up with 3 by 3 matrices with determinant 1. Two groups used 3 by 3 matrices as encoding matrices while the other three groups chose 2 by 2 matrices.

All groups were able to decode the messages successfully. But the natural question which arose was what happens in the decoding process if the encoding matrix had a determinant other than 1. Also the other question which arose was, is it possible for a person (other than receiver or sender) to crack the code, that is, figure out the encoding matrix if the plaintext and ciphertext are known. Both had to be addressed in a separate special class which was not a part of the module. Here students had to be introduced to the following ideas,

In Z_n , the set of integers modulo n, every element has an inverse in the set provided n is prime. Hence the technique required that the number of characters be prime. If each element in Z_n did not have an inverse within Z_n then decoding would not be possible when the encoding matrix had a determinant which did not have an inverse within the set.

The Cracking theorem

Suppose the length m of the alphabet is a prime. Let P and C be the plaintext matrix and ciphertext matrices respectively.

$$P = \begin{bmatrix} \vec{p}_1 & \vec{p}_2 & \vec{p}_3 & .. & .. & \vec{p}_n \end{bmatrix} \quad C = \begin{bmatrix} \vec{c}_1 & \vec{c}_2 & \vec{c}_3 & .. & .. & \vec{c}_n \end{bmatrix}$$

Then the elementary row transformations that reduce C^T to the identity matrix I also reduce the matrix P^T to $(A^{-1})^T$.

This project gave students a flavor of the practical use of manipulating matrices and their inverses. Also students had to be familiarized with some concepts in number theory which were beyond the scope of the curriculum. This application of matrix theory to a cryptographic technique gave students access to higher level mathematical concepts. The computational aspects of multiplying matrices of higher orders, inverting matrices as well as reducing them modulo 29, were performed on the graphics calculator. Since students were able to 'outsource' the computations to the calculator they were free to think about the mathematical aspects of the Hill cipher technique.

RESULTS OF THE STUDY

At the end of the module students were asked to respond to a short questionnaire of 12 items by entering a number from 1 to 5, where the numbers indicated the following.

1-Strongly disagree, 2-Disagree, 3- Not sure, 4- Agree, 5- Strongly agree

The data of student's responses are shown in Table 3. They were also asked to give a written feedback in terms of specific comments describing their impressions regarding how the module helped (or did not help) them.

Table 3. Responses of grade 12 students (N = 32) to questionnaire

Item no.	Item	SA	A	NS	D	SD
1.	I found this module on matrices and determinants more interesting than the traditional classroom teaching.	7	16	7	__	__
2.	This module has helped me to see the relevance of mathematics to real life.	12	16	2	__	__
3.	Such modules should become a part of regular school curriculum.	21	7	2	__	__
4.	Questions based on modelling and applications should be included in examinations.	2	5	16	7	__
5.	The inclusion of applications and modelling in this module played a key role in my understanding of the concepts.	9	18	3	__	__
6.	My interest in mathematics will increase if topics are taught by including modelling and applications.	21	7	2	__	__

7.	Mathematics as a subject will seem less abstract if topics are taught with the help of modelling and applications.	11	11	6	__	2
8.	I feel that in this module technology helped me to visualize and explore concepts and thus gain a deeper insight into the subject.	9	18	3	__	__
9.	I feel that technology played a key role in trivializing calculations so that more time could be spent on exploring the mathematical models.	6	14	7	3	__
10.	My confidence level in solving problems related to matrices has increased after going through this module.	5	16	7	2	__
11.	The inclusion of modelling and applications may have a detrimental (harmful) effect on my paper and pencil skills.	__	__	11	5	14
12.	I feel technology should be used to solve problems which cannot be done by hand.	18	5	2	5	__

Table 4 shows the sample means and standard deviations for agreement scores (1 to 5) for selected items of the questionnaire, shown in Table 3. These have been used to estimate the population mean scores by calculating 95% confidence intervals. A mean score of 3.75 and above indicates agreement with the statement given in a particular item. For items 1, 2, 3, 5, 6 and 8 the interval estimates indicate strong agreement and the interval estimate for item 4 indicates that respondents are not sure about the statement. These estimates show that majority of students agree that the module is more interesting than traditional classroom teaching (item 1) and that it helped them to see the relevance of mathematics to realistic problems (item 2). One student commented, "The way the concepts were taught with applications was the best part of this module" and another wrote, "I particularly found the Hill Cipher method very useful and interesting. Including such models based on matrices made the topic very interesting". Majority of students agreed that such modules should become a part of the regular curriculum (item 3) although they had reservations about including questions based on modelling and applications in the examinations (item 4). This was be probably due to the fact that they had been introduced to this approach for the first time and it would take them more time to be comfortable enough to be able to attempt problems based on applications in examinations. Students also agreed that the applications played a key role in

helping them understand concepts (item 5) and that their interest in mathematics would increase if such modules were included in other topics of the curriculum (item 6). A student commented, "The module helped to understand why we are using certain formulae and procedures. The regular classes do not deal with these things." Another reflected, "this module helped to clear my concepts and doubts." They disagreed that focus on modelling and applications can have a harmful effect on their manipulative skills (item 11) and also agreed that technology should be used to solve problems which are difficult to solve by hand.

The responses based on the role of technology were also insightful. Students felt that technology contributed to a deeper understanding of concepts by aiding visualization and exploration (item 8) and that it helped to trivialize calculations thereby allowing more time for exploration (item 9). They also agreed that technology should be used to solve problems which cannot be solved by hand (item 12). One student observed, "The use of graphics calculators helped a lot. We focused on the concepts and problems but the calculator did all the lengthy calculations. The calculator made the sessions more interactive". Commenting on the use of Mathematica, one student wrote "Mathematica helped us to actually see the solutions of equations in three unknowns. The methods taught in class only helped us find the solutions but I could never understand what they looked like. Now I know, thanks to the 3-D graphing feature of Mathematica."

Table 4. 95% confidence interval estimates for population mean of students responses

Item no.	Sample mean (N = 30)	Sample Standard deviation	Population Mean (95% confidence interval)	
			Upper Bound	Lower Bound
1	4.00	0.69	4.25	3.75
2	4.33	0.61	4.55	4.12
3	4.63	0.61	4.84	4.41
4	3.07	0.83	3.36	2.77
5	4.20	0.61	4.42	3.98
6	4.63	0.61	4.85	4.41
8	4.20	0.61	4.42	3.98
11	1.90	0.92	2.23	1.57
12	4.20	1.16	4.61	3.70

CONCLUSION

This paper describes a module *Learning Mathematics through Mathematical Modelling and Applications* which was undertaken by 30 students of grade 12. The module was based on the topic *Matrices and Solutions of Systems of Equations* and was spread over 8 two hour sessions. In each session, students were introduced to concepts of the topic through mathematical models and applications. After an introduction to the mathematical theory on which the models were based, students were required to explore the models through tasks and problems which were posed to them in worksheets. Their explorations were facilitated by the researcher and they were given access to graphics calculators throughout the module. In many cases it was found that students preferred to do the calculations by hand and then verify their answer on the calculator. However in some explorations, such as finding the genotype distribution of a plant population after several generations, students were required to raise a matrix to higher powers. Here the calculator helped to trivialize the computations and enabled the students to focus on exploring the problem which led to a deeper insight. As Herwardeen's (2001) study suggests the integration of technology helped to create a connection between paper-pencil methods and calculator manipulations. In the Hill Cipher method, the lengthy calculations such as multiplying matrices of large orders and reducing matrices modulo 29, was 'outsourced' to the calculator. Throughout the module the graphics calculator served as a 'mathematical investigation assistant', as proposed by Arnold (2004), giving students control over what they were learning. While exploring the solutions of three equations in three unknowns, paper pencil methods helped students to compute the solutions while Mathematica gave a physical meaning to their computations. Thus, as suggested by Lagrange (1999), Mathematica helped to balance 'by hand' calculations and conceptual understanding. The exploration of the mathematical applications such as the pagerank algorithm and Hill cipher method provided the students with new contexts where they could apply the theory of matrices. They also learnt new mathematical content, some of which was far beyond the grade 12 level. For example, the Hill cipher method led to the discussion of the some ideas in number theory and the Cracking Theorem which was beyond the curriculum. The technology enabled explorations of the mathematical applications gave students access to higher level mathematical concepts and this supports Heid's (2001) theory that technology acts as an 'amplifier'.

It may be concluded that integrating mathematical modelling and applications for teaching the topic of Matrices led to a very satisfying combination of technology use and 'by-hand'skills. The study supports Lindsay (1995) that, when properly used, technology enabled explorations can augment learning and provide a rich and motivating environment to explore mathematics. It also supports the educational perspective of mathematics education research on teaching and learning of modelling which asserts that including modelling in the curriculum to helps to highlight the relevance of mathematics as a discipline. Through the module described in this paper students not only learnt new mathematical content but also obtained a glimpse of how mathematics can be applied to solve realistic problems.

References

Arnold, S. (2004). Classroom computer algebra: some issues and approaches. *The Australian Mathematics Teacher, 60(2)*, 17–21.

Blomhøj, M. (2008). Different perspectives in research on the teaching and learning mathematical modelling – Categorising the TSG21 papers. Proceedings from Topic Study Group 21 at the 11th International Congress on Mathematical Education in Monterrey, Mexico, July 6-13, 2008. 1 -17

Central Board for Secondary Education. (n.d.). Course structure of Mathematics (class XI and XII). Retrieved from http://cbseportal.com/exam/Syllabus/cbse-11th-12th-2011-mathematics

Eisenberg, M. (1999). Hill Ciphers and Modular Linear Algebra. Retrieved from http://www.apprendre-en-ligne.net/crypto/hill/Hillciph.pdf

Heid, M. K. (2001). Theories that inform the use of CAS in the teaching and learning of mathematics. Plenary paper presented at the Computer Algebra in Mathematics Education (CAME) 2001 symposium. Retrieved from http://www.lkl.ac.uk/research/came/events/freudenthal/3-Presentation-Heid.pdf

Herwaarden, O. & van Gielden, J. (2002). Linking computer algebra systems and paper-and pencil techniques to support the teaching of mathematics. *International Journal of Computer Algebra in Mathematics Education, 9(2)*, 139–154.

Lagrange J. B. (1999). A didactic approach of the use of computer algebra systems to learn mathematics. Paper presented at the Computer Algebra in Mathematics Education workshop, Weizmann Institute, Israel. Retrieved from http://www.lkl.ac.uk/research/came/events/Weizmann/CAME-Forum1.pdf

Lindsay, M. (1995, December). Computer algebra systems: sophisticated 'number crunchers' or an educational tool for learning to think mathematically? Paper presented at the annual conference of the Australasian Society for Computers in Learning in Tertiary Education (ASCILITE), Melbourne, Australia.

National Council for Educational Research and Training. (2005). Position paper of National Focus Group on Teaching of Mathematics. Retrieved from http://www.ncert.nic.in/rightside/links/pdf/framework/nf2005.pdf