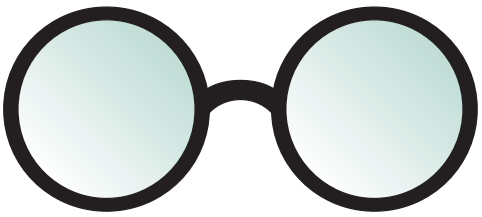
Title	Harry Potter and the cryptography with matrices
Author(s)	Chua Boon Liang
Source	*The Australian Mathematics Teacher, 62*(3), 25-27
Published by	The Australian Association of Mathemetics Teachers Inc

Document extract

Title of chapter/article	Harry Potter and the Cryptography with Matrices
Author(s)	Boon Liang Chua
Copyright owner	The Australian Association of Mathematics Teachers (AAMT) Inc.
Published in	The Australian Mathematics Teacher vol. 62 no. 3
Year of publication	2006
Page range	25–27
ISBN/ISSN	0045-0685

BOON LIANG CHUA

Harry Potter AND THE CRYPTOGRAPHY WITH MATRICES



Introduction

Cryptography, the science of encrypting and deciphering messages written in secret codes, has played a vital role in securing information since ancient times. Julius Caesar employed what has become known as the *Caesar Shift Cipher* when encoding messages to communicate with his generals. Under this form of encryption technique, each letter in a message is substituted with the letter that was a certain number of places further down the alphabet. Caesar used a shift of three places, and so A is replaced by D, B is replaced by E, and so on. In modern history, the Nazis continued to use the presumably highly sophisticated Engima machine to encrypt their messages when they communicated, still unaware that three Polish mathematicians had already cracked the unbreakable codes of the Engima machine and had provided the Allied Forces with the means to gain access to their top secrets. More recently, with millions of financial transactions conducted over the Internet daily, cryptography has become more important than ever. Companies have begun to make online transactions more secure by installing encryption software to prevent sensitive information such as credit card numbers from falling into the wrong hands.

There are several cryptographic techniques and many make extensive use of mathematics to secure information. This article describes an activity built around one of the techniques that illustrates an application of matrices. Secondary school teachers may use this activity to consolidate their students' learning of certain concepts of matrices such as the algorithm for matrix multiplication and the concept of the multiplicative inverse of a matrix.

The activity

To capitalise on the popularity of the Harry Potter series by J. K. Rowling, the entire activity is framed in the context of the Harry Potter story with the aim of stimulating and heightening students' interest. The activity begins with the following scenario:

> Harry Potter is in deep trouble. He is being pursued by Lord Voldemort and is presently hiding in a secret location to escape from being captured by him. He needs to send messages to his two good friends, Ron and Hermione, to tell them about his situation and whereabouts. Of course, he has to send the messages in code, just in case they are intercepted and cracked by Lord Voldemort along the way. So he composes his first message "Please save me!" by replacing each letter in the message by a number according to the code in Table 1.

Table 1. Coding system.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
O	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	29

Then students are asked to translate Harry's plain message into code, which appears as follows when completed:

P	L	E	A	S	E		S	A	V	E		M	E	!
16	12	5	1	19	5	0	19	1	22	5	0	13	5	27

The activity continues with the story of the clever, but devious, Harry using a super hi-tech LOCK to encrypt his message to make it

unbreakable by others, except for Ron and Hermione. The super hi-tech LOCK used is

$$\begin{pmatrix} 1 & 0 & 1 \\ -1 & 1 & 0 \\ 0 & 1 & 2 \end{pmatrix}$$

Here, students are told that the LOCK is a rectangular array of numbers in rows and columns, and are asked to write down the special name of such an array of numbers, as well as its order.

Next, the story proceeds to describe the encryption technique that Harry uses. First, he writes his encoded message in groups of three numbers as shown below:

$$\begin{pmatrix} 16 \\ 12 \\ 5 \end{pmatrix}\begin{pmatrix} 1 \\ 19 \\ 5 \end{pmatrix}\begin{pmatrix} 0 \\ 19 \\ 1 \end{pmatrix}\begin{pmatrix} 22 \\ 5 \\ 0 \end{pmatrix}\begin{pmatrix} 13 \\ 5 \\ 27 \end{pmatrix}$$

Second, he pre-multiplies each group of numbers by his super hi-tech LOCK. To reinforce the students' learning of matrix multiplication, they are instructed to apply the second step to the five groups of numbers. For instance, the first group,

$$\begin{pmatrix} 16 \\ 12 \\ 5 \end{pmatrix}$$

yields the result:

$$\begin{pmatrix} 1 & 0 & 1 \\ -1 & 1 & 0 \\ 0 & 1 & 2 \end{pmatrix}\begin{pmatrix} 16 \\ 12 \\ 5 \end{pmatrix} = \begin{pmatrix} 1\times16+0\times12+1\times5 \\ -1\times16+1\times12+0\times5 \\ 0\times16+1\times12+2\times5 \end{pmatrix} = \begin{pmatrix} 21 \\ -4 \\ 22 \end{pmatrix}$$

Now what has happened is that the letters P, L and E, which are originally given the codes 16, 12 and 5 respectively, have now ended up being correspondingly represented by the codes 21, –4 and 22. So numbers 21 and 22 can be converted directly into the codes U and V respectively based on the coding system given in Table 1. That is to say, the letters U and V become the corresponding encrypted codes for P and E. However, there is a problem here in such a technique. The number –4 cannot be converted because none of the codes in Table 1 corresponds to it. So Harry resolves this problem by reducing –4 modulo 30 to obtain 26. That is,

$$\begin{pmatrix} 21 \\ -4 \\ 22 \end{pmatrix} \equiv \begin{pmatrix} 21 \\ 26 \\ 22 \end{pmatrix} \bmod 30$$

In other words,

$$\begin{pmatrix} P \\ L \\ E \end{pmatrix}$$

which is represented by

$$\begin{pmatrix} 16 \\ 12 \\ 5 \end{pmatrix}$$

in the beginning, is now encrypted and translated into

$$\begin{pmatrix} U \\ Z \\ V \end{pmatrix}$$

Harry is ingenious, is he not?

Given that modulo arithmetic is probably a new concept to most — if not all — students, it is advisable for teachers to illustrate sufficient examples to demonstrate how a number, not within the range of 0 to 29, is reduced modulo 30. Once students are familiar with the procedure, they can then be asked to encrypt the original message, which, if correctly done, should read as shown below:

Original	P	L	E	A	S	E		S	A	V	E		M	E	!
Encrypted	U	Z	V	F	R	.	A	S	U	V	M	E	J	V	.

This message is subsequently transmitted as a string of letters to Ron and Hermione. Ron and Hermione successfully receive this string of letters from Harry and immediately reconstruct the five groups of numbers. They use the following super sophisticated KEY to unlock and unscramble the message:

$$\begin{pmatrix} 2 & 1 & -1 \\ 2 & 2 & -1 \\ -1 & -1 & 1 \end{pmatrix}$$

To promote thinking, students are encouraged to predict the relationship between the LOCK used for encoding and the KEY used for deciphering. This should be an easy task for the students, with most of them expected to point out that the LOCK and the KEY are the multiplicative inverses of each other. To further probe their understanding of some properties of inverse matrices, students can be led to explain how the relationship is arrived at. When this activity was carried out with a group of Singapore secondary school students, many reached the conclusion by showing that the pre-multiplication of the KEY by the LOCK produced the identity matrix. However, when asked whether or not it was also necessary to check that the pre-multiplication of the LOCK

by the KEY also yielded the identity matrix, not many students seemed to know how to respond to this question. Therefore, this provided the teacher with an opportunity to engage the students in a constructive classroom discussion to consolidate some important properties of inverses.

The story progresses with an illustration of how Ron and Hermione decipher Harry's encrypted message. They pre-multiply a coded group of numbers,

$$\begin{pmatrix} 21 \\ 26 \\ 22 \end{pmatrix}$$

by their super sophisticated KEY, followed by reducing all the values, which fall outside the range of 0 to 29, modulo 30:

$$\begin{pmatrix} 2 & 1 & -1 \\ 2 & 2 & -1 \\ -1 & -1 & 1 \end{pmatrix}\begin{pmatrix} 21 \\ 26 \\ 22 \end{pmatrix} = \begin{pmatrix} 46 \\ 72 \\ -25 \end{pmatrix} \equiv \begin{pmatrix} 16 \\ 12 \\ 5 \end{pmatrix} \bmod 30$$

Not surprisingly, they obtain the result

$$\begin{pmatrix} 16 \\ 12 \\ 5 \end{pmatrix}$$

which should be instantly recognised by many students as the representative coded numbers for the group of letters

$$\begin{pmatrix} \mathrm{P} \\ \mathrm{L} \\ \mathrm{E} \end{pmatrix}$$

To verify that the original message can indeed be unveiled in such a manner, students can apply the process to the other coded groups of numbers to check. Having completely described how the entire encryption and decryption process works, students are given time to communicate with each other in encoded messages.

Subsequently, they are informed that this secret process is very unfortunately discovered and broken by the evil Lord Voldemort, and therefore, a new system has to be developed. So students are asked to explore and create a new LOCK and KEY for transmitting coded messages. They are also given the freedom to modify the existing coding system.

To help students in their exploration of this task, the use of computer or calculator technology can be integrated into this part of the activity. For instance, teachers can teach students to make use of the functions such as MMULT, MDETER and MINVERSE in Microsoft Excel to perform matrix multiplication, as well as to find the determinant and inverse of a matrix. Such use of technology not only reduces the drudgery of performing matrix multiplication manually and therefore leaves students with more time for exploration, it also adds a more challenging dimension to learning by enabling them to work with concepts that are beyond the syllabus. To illustrate this point, take finding the determinant and inverse of a 3 × 3 matrix as examples. These topics are not included in the Singapore secondary mathematics syllabus, but through the use of EXCEL, local students are able to generate them quickly. As a result, the new LOCK and KEY that they devise are not simply restricted to only 2 × 2 matrices. Additionally, it would seem logical to think that any arbitrary non-singular, square matrix can be chosen to represent the LOCK, but with the help of technology, Singapore students found that this was not exactly the case. They discovered that the determinant of the LOCK has to be 1 in order for the encryption technique previously described to work.

Conclusion

Secondary school students often ask their teachers why it is important to learn mathematics, and thus teachers are usually faced with the challenge of explaining its importance and relevance to real life situations to convince them. However, this may not always be an easy task. Therefore, it is hoped that this activity on cryptography not only offers teachers with great opportunities to either introduce or consolidate certain mathematical concepts and algorithms, but also to convince their students that mathematics plays an important role in various walks of life and hence is a useful and meaningful field of study.

References

Camp, D. R. (1985). Secret codes with matrices. *Mathematics Teacher, 78*(9), 676–680.

Lee, P. Y. (2005). *Teaching Secondary School Mathematics: A Resource Book.* Singapore: McGraw Hill.

Singh, S. (1999). *The Code Book: The Secret History of Codes and Code-Breaking.* London: Fourth Estate.

Boon Liang Chua
National Institute of Education
Nanyang Technological University, Singapore
blchua@nie.edu.sg