Caroline Adkisson Wake Forest University

TOPIC: Navajo Codes in World War II

NCTM STANDARDS: Number and Operations, Communication, Connections, Representation

GOALS:

Students will connect algebraic matrices with the concept of cryptography and its use in Native American culture. They will review basic algebraic concepts of matrices, inverse matrices, and matrix multiplication in the context of coding.

INTRODUCTION:

Navajo code talkers were a vital part of the Allies victory in the battle of Iwo Jima. The complicated language of the Navajo tribe could not be broken by the Japanese. Their unwritten language was used to transmit information on movement on the troops and military tactics. The messages were conveyed as a string of Navajo words that were not correlated. The Navajo code talkers would translate the Navajo word into a comparable English word. Then they used the first letter of the English words to represent the coded word. The code talkers could complete this process for three-line English messages in twenty seconds, but it would take a machine thirty minutes.

ACTIVITIES:

- Part 1. Introduction. Teacher reviews how to construct matrices, how to find the inverse of a matrix, and how to multiply matrices. Then the teacher describes how to convert the letters of the alphabet into numbers. These numbers will be grouped into 2x2 matrices and multiplied by the cipher matrix. This creates the encoded matrices, which are used to construct the encoded message.
- Part 2. Decode a Short Encoded Message. Students will use their knowledge to decode a given matrix as practice.
- Part 3. Create Your Own Encoded Message. Students will create their own cipher matrix, encode a message, and then decode the message.

ASSESSMENT: At the end of the introduction activity, the students will decode a message. They will have to use their knowledge of matrices, inverses of matrices, and matrix multiplication to complete this activity.

Profaca, Mario. (1995). The Navajo Code Talkers. Retrieved September 22, 2006, from: http://mprofaca.cro.net/navajo.html.

Part 1: Introduction

Navajo code talkers were a vital part of the Allies victory in the battle of Iwo Jima. The complicated language of the Navajo tribe could not be broken by the Japanese. Their unwritten language was used to transmit information on movement on the troops and military tactics. One way to create a code is to use matrices. We will use 2x2 matrices for this project.

It is vital to be able to find the inverse of a matrix to use this type of coding technique. To use a graphing calculator for this function, simply enter the values into the 2x2 matrix. These values need to be entered clockwise, starting at the top left corner. Then call up the matrix onto the screen and hit the inverse key ($^{-1}$). This will give you the inverse of the given matrix.

In addition, you must be able to multiply matrices to use this type of coding. To use a graphing calculator for this function, simply enter the values of the two different matrices into two 2X2 matrices. Then multiply the first one by the second one. This will give the matrix product.

To use matrices for cryptography, you have to convert the letters of the alphabet into numbers. The following table tells which letter corresponds to which number:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Once you have the original message that you want to encode, you must translate it into a series of numbers. Then you will group every set of four numbers into a 2x2 matrix, like so: 1 2 3 4 = [1 2] [3 4] The numbers are inserted into the matrix starting at top left, top right, bottom left, and bottom right.

After creating a 2x2 matrix for every group of four letters (now numbers), you must create a cipher matrix. This is what you will use to encode your message! The numbers do not have to have any sort of significance, other than the fact that the matrix must have a nonzero determinant (so there is an inverse). To find the determinant for the matrix given above, do the following calculation: (1*4) – (2*3). Because this does not equal zero, this could be used as a cipher matrix.

Finally, to encode the message, multiply the cipher matrix by each individual matrix. It is vital that the cipher matrix is the first matrix being multiplied: (cipher) * (group of 4). To decode a message, you must find the inverse of the cipher matrix. Then you will multiply that by each individual encoded matrix. Once again, the inverse of the cipher matrix must be the first matrix being multiplied: (inverse of cipher)*(encoded group of 4).

Part 2: Decode a Short Encoded Message

With the knowledge that you received from the introduction, decode the following message. The cipher matrix for this message is [3 2] [4 3].

A E I O M T T F A O P B G Q N A

Part 3: Create Your Own Encoded Message

Now it is your turn. Create your own message that you wish to encode. Make sure to use a cipher matrix that has a determinant of one, because then you can find its inverse. It will be easier for you if you choose a message where the number of letters in it is a multiple of four. To earn full credit for this part, show your original message, your cipher matrix, how you used the cipher matrix to encode your matrix, the inverse of your cipher matrix, and how you used the inverse of the cipher matrix to convert the encoded message back to the original message.

Part 4: Assessment

Decode the following message. Its cipher matrix is [7 4] [5 3]

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

Show all of your work.

TEACHER NOTES/SOLUTIONS

Part 1: The teacher should use the notes provided in the students' introduction to review that material.

Part 2: The teacher should guide the students through this example.
To find the answer to this problem, first find the inverse of the cipher matrix. The inverse of this matrix is: [3 -2]
[-4 3]
Then, they should find which numbers correspond to the given letters in the encoded message.

A	**E**	**I**	**O**	**M**	**T**	**T**	**F**
1	5	9	15	13	20	20	6

A	**O**	**P**	**B**	**G**	**Q**	**N**	**A**
1	15	16	2	7	17	14	1

Next, they should create four 2x2 matrices.
[1 5] [13 20] [1 15] [7 17]
[9 15] [20 6] [16 2] [14 1]

Finally, they should multiply the inverse of the cipher matrix by each of these new four matrices.
[3 -2] * [1 5] = [21 19] ***
[-4 3] [9 15] [5 13]

[3 -2] * [1 5] = [1 20] ***
[-4 3] [9 15] [8 20]

[3 -2] * [1 5] = [15 23] ***
[-4 3] [9 15] [9 14]

[3 -2] * [1 5] = [23 1] ***
[-4 3] [9 15] [18 19]

***(once converted to a 1-26 number-do this by adding or subtracting 26 until the number falls between 1-16)

21	19	5	13	1	20	8	20
U	**S**	**E**	**M**	**A**	**T**	**H**	**T**

15	23	9	14	23	1	18	19
O	**W**	**I**	**N**	**W**	**A**	**R**	**S**

Use math to win wars.

Part 3: In order to review this part, the teacher should follow each student's process. This will not be for a grade, but rather for extra practice. The teacher will check to see if the following procedures have been completed accurately:

1) The student should use a cipher matrix that has an inverse.
2) The original message correctly has been converted into numbers 1-26 and divided up into 2x2 matrices.
3) These matrices have been multiplied by the cipher matrix to find the encoded message.
4) The encoded matrix has been multiplied by the inverse of the cipher matrix to find the original message.

If the teacher prefers, the students can work in pairs and try to encode and decipher their partner's work. Either way, this is for more practice and not a grade.

Part 4:

The students should first create the corresponding 2x2 matrices for the given encoded message.

[6 25]	[18 11]	[14 11]	[22 17]
[6 2]	[3 4]	[9 8]	[5 4]
[9 22]	[14 2]	[23 5]	[17 15]
[18 2]	[13 5]	[11 10]	[8 11]
[13 8]	[21 22]	[1 14]	[19 2]
[12 9]	[16 23]	[5 19]	[20 23]
[19 5]	[5 5]		
[9 12]	[5 24]		

Then the students should multiply each of these matrices by the inverse of the cipher matrix.

[3 -4] * (each of the matrices listed above)
[-5 7]

This will create the following matrices, which correspond to letters in the original message.

[14 1]	[10 15]	[4 5]	[18 5]
[22 1]	[3 15]	[19 1]	[21 19]
[5 6]	[20 8]	[23 5]	[21 19]
[21 12]	[5 25]	[18 5]	[5 4]
[9 14]	[18 12]	[1 18]	[5 2]
[23 15]	[4 23]	[20 23]	[25 1]
[13 5]	[3 1]		
[18 9]	[14 19]		

Finally, the students should have determined which letters these numbers corresponded to in order to find the original message.

14	1	22	1	10	15	3	15	4	5	19	1	18	5
N	A	V	A	J	O	C	O	D	E	S	A	R	E

21	19	5	6	21	12	20	8	5	25	23	5	18	5
U	S	E	F	U	L	T	H	E	Y	W	E	R	E

21	19	5	4	9	14	23	15	18	12	4	23	1	18
U	S	E	D	I	N	W	O	R	L	D	W	A	R

20	23	15	2	25	1	13	5	18	9	3	1	14	19
T	W	O	B	Y	A	M	E	R	I	C	A	N	S

Navajo codes are useful. They were used in World War Two by Americans.

Rubric for Assessment:

It is possible to receive 50 points for this assignment.

Number of Points	
15	Correct matrices for the original message.**
5	Correct inverse of cipher matrix
15	Correct matrices received from multiplying the cipher matrix by the original message.**
15	Correct final message.**

**Give partial credit if so desired. Give one point for each correct matrix, as well as one point for attempting the problem.