|  |
| --- |
|  |

Lesson 13: Using Matrix Operations for Encryption

Student Outcomes

* Students study and practice the properties of matrix multiplication.
* Students understand the role of the multiplicative identity matrix.

Lesson Notes

Data encryption has become a necessity with the rise of sensitive data being stored and transmitted via computers. The methods included in this section are not secure enough to use for applications such as Internet banking, but they result in codes that are not easy to break and provide a good introduction to the ideas of encryption. Interested students can research RSA public-key encryption, which relies on the fact that factoring extremely large numbers is a very difficult and slow process. Students interested in the history of data encryption can research the Cherokee and Choctaw Code Talkers from World War I and the Navajo Code Talkers from World War II.

This lesson reinforces concepts of matrix multiplication, matrix inverses, and the identity matrix in the context of encoding and decoding strings of characters using multiplication by either an encoding matrix or its inverse decoding matrix. This lesson aligns with **N-VM.C.6** (Use matrices to represent and manipulate data), **N-VM.C.8** (Add, subtract, and multiply matrices of appropriate dimensions), and **N-VM.C.10** (Understand that the zero and identity matrices play a role in matrix addition and multiplication similar to the role of 0 and 1 in the real numbers. The determinant of a square matrix is nonzero if and only if the matrix has a multiplicative inverse.)

The activity in Exercise 2 requires that six stations be set up in advance around the classroom as the messages have been encoded four times. At each station, post the specified decoding matrix:

|  |  |  |
| --- | --- | --- |
| Station 1: | Station 2: | Station 3: |
| Station 4: | Station 5: | Station 6: |

Divide students into at least six groups numbered 1–6, assign each group their coded message, and start them at their numbered station. Groups will apply the decoding matrix to their message and then move to the next station. After applying four decoding matrices, the original message will be revealed. Each group will decode 20 characters of the original message, combining the results into the full quote from the entire class.

Classwork

Opening (7 minutes)

The phrase “The crow flies at midnight” appears to have first occurred in Ian Fleming’s James Bond novel *From Russia with Love*. It has since become a coded message in spy movies and television shows.

Opening

A common way to send coded messages is to assign each letter of the alphabet to a number – and send the message as a string of integers. For example, if we encode the message “THE CROW FLIES AT MIDNIGHT” according to the chart below, we get the string of numbers

,,,,,,,,,,,,,,,,,, ,,, ,,, ,.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | SPACE |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |

However, codes such as these are easily broken using an analysis of the frequency of numbers that appear in the coded messages.

We can instead encode a message using matrix multiplication. If a matrix has an inverse, then we can encode a message as follows.

* + **First, convert the characters of the message to integers between and using the chart above.**
  + **If the encoding matrix is an matrix, then break up the numerical message into rows of the same length. If needed, add extra zeros to make the rows the same length.**
  + **Place the rows into a matrix .**
  + **Compute the product to encode the message.**
  + **The message is sent as the numbers in the rows of the matrix .**

**Example (10 minutes)**

* A common way to send coded messages is to assign each letter of the alphabet to a number – and send the message as a string of integers. For example, if we encode the message “THE CROW FLIES AT MIDNIGHT” according to the chart below, we get the string of numbers

,,,,,,,,,,,,,,,,,,,,,,,,,.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | SPACE |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |

However, codes such as these are easily broken using an analysis of the frequency of numbers that appear in the coded messages. For example if the coded phrase is , ,, ,,,,,,,,,,,,,,,,,,,,,,, we can see that there are three of the letters assigned to the integer , so we may want to try putting a common letter in for the number like S, T, or E. If we assume the word *the* is used to start the phrase since we have three letters then a space, that would lead us to think that maybe the number is E, and so on.

* We can instead encode a message using matrix multiplication. If a matrix has an inverse, then we can encode a message as follows.
* First, convert the characters of the message to integers between and using the chart above.
* If the encoding matrix is an matrix, then break up the numerical message into rows of the same length. If needed, add extra zeros to make the rows the same length. For example if we want to use an encoding matrix that is , we would write the message in two rows of equal length, filling in zero for the last number if the number of letters was odd. If the encoding matrix is , the message would be written in three equal rows adding zeros as necessary.
* Place the rows into a matrix .

*Scaffolding:*

* Students who are struggling can be given a simpler phrase such as “Be Happy” or “Dream Big.”
* Have advanced learners find their own phrase of 30 characters or more and encode using a matrix.
* Compute the product to encode the message.
* The message is sent as the numbers in the rows of the matrix
* Using the matrix*,* we encode our message as follows:
* Since is a matrix, we need to break up our message into two rows.
* Then we place the rows into a matrix
* Explain how matrix represents “THE CROW FLIES AT MIDNIGHT.”

**MP.2**

* + *Each letter and space in the phrase was assigned an integer value, and these numbers represent the letters in the phrase.*
* We encode the message into matrix by multiplying
* Thus, the coded message that we send is

,,,,,,,,,,,,,,,,,,,,,,,,,

If this coded message is intercepted, then it cannot easily be decoded unless the recipient knows how it was originally encoded.

Be sure to work through this discussion and emphasize that the way to decode a message is to multiply by the inverse of the encoding message.

* Using what you know about how the message was encoded, as well as matrix multiplication, describe how you would decode this message.

**MP.4**

* + *We need to know a decoding matrix*
* How can we find that matrix?
  + *The decoding matrix is the inverse of the encoding matrix, so*
* What is the decoding matrix?
* Decode this message!

As expected, this is the matrix that stored our original message “THE CROW FLIES AT MIDNIGHT.”

* Why does this process work?
  + *The coded message stored in matrix is the product of matrices and , so. We then decode the message stored in matrix by multiplying by matrix Since matrices and are inverses, we have*

*So, encoding and then decoding will return the original message in matrix*

* Explain to your neighbor what you learned about how to encode and decode messages. Teachers should use this as an informal way to check for understanding.

Exercise 1 (7 minutes)

The encoded phrase in this exercise is “ARCHIMEDES.” Archimedes (c. 287–212 BCE, Greece) is regarded as the greatest mathematician of his age and one of the greatest of all time. He developed and applied an early form of integral calculus to derive correct formulas for the area of a circle, volume of a sphere, and area under a parabola. He also found accurate approximations of irrational numbers such as and. However, during his lifetime he was known more for his inventions such as the Archimedean screw, compound pulleys, and weapons such as the Claw of Archimedes used to protect Syracuse in times of war.

The original message is stored in matrix , and the matrix used to encode the message is  
 This exercise introduces students to using a larger matrix to perform the encoding and decoding and requires that students practice matrix multiplication with non-integer matrix entries. Additionally, because students have not learned a method for finding the inverse of a matrixthey must demonstrate understanding of the meaning of a matrix inverse in order to decode this matrix.

Exercises

*Scaffolding:*

* Students may need to be reminded that the matrices we use to encode and decode a message are inverses.
* Students may also need to be reminded of the property that defines inverse matrices: and are inverse matrices if

1. You have received an encoded message: ,,,,,,,,,,, You know that the message was encoded using matrix .
   1. Store your message in a matrix . What are the dimensions of ?

There are numbers in the coded message, and it was encoded using a   
matrix. Thus, the matrix needs to have three rows. That means hasfour columns, so is a matrix.

* 1. You have forgotten whether the proper decoding matrix is matrix ,, or as shown below. Determine which of these is the correct matrix to use to decode this message.

Matrices used to encode and decode messages must be inverses of each other. Thus, the correct decoding matrix is the matrix so that We can find the correct decoding matrix by multiplying   
, and

Since , we know that is the decoding matrix we need.

* 1. Decode the message.

Using matrix to decode, we have

The decoded message is “ARCHIMEDES.”

Exercises 2–3 (15 minutes)

In this exercise, groups of students decode separate parts of a message that have been encoded four times; as groups complete the decoding of their portion of the message, have them record it in a location that all students can see—either on the white board or projected through a document camera, for example. The decoded messages will together spell out a famous quote by Albert Einstein: “Do not worry about your difficulties in mathematics. I can assure you that mine are still greater.” You may substitute a different quote if you would like, perhaps a school motto. Carefully encode each of six portions of a quote stored in matrices to using encoding matrices to as follows.

*Scaffolding:*

For struggling students, select a shorter quote, or encode it in fewer than four steps.

;;;;;

Divide the class into at least six groups of two or three students, numbered 1–6, assigning multiple groups to the same number as needed. Set up six stations around the room in a circular arrangement. Have each group start at the station with the same number as the group—Group 1 starts at Station 1, Group 2 starts at Station 2, etc. At each station, the groups apply the posted decoding matrix to their encoded message shown below, and then they progress to the next station, with groups at Station 6 proceeding to Station 1. It will require four decoding steps with different matrices (such as , , and ) to uncover a group’s portion of the original message.

At each station, post the matrix listed below.

Station 1:

Station 2:

Station 3:

Station 4:

Station 5:

Station 6:

1. You have been assigned a group number. The message your group receives is listed below. This message is TOP SECRET! It is of such importance that it has been encoded four times.

Your group’s portion of the coded message is listed below.

Group 1:

, , , , , , , , , , , , , , , , , , ,

Group 2: ,,,,,,,,,,,,,,,,,,

Group 3:

,,,,,,,,,,,,,,,,,,,

Group 4:

,,,,,,,,,,,,,,,,,,,

Group 5:

,,,,,,,,,,,,,,,,,,,

Group 6:

,,,,,,,,,,,,,,,,,,,

* 1. Store your message in a matrix with two rows. How many columns does matrix have?

(Sample responses are provided for Group 1.) Our message is stored in a matrix with ten columns:  
.

* 1. Begin at the station of your group number, and apply the decoding matrix at this first station.
  2. Proceed to the next station in numerical order; if you are at Station 6, proceed to Station 1. Apply the decoding matrix at this second station.
  3. Proceed to the next station in numerical order; if you are at Station 6, proceed to Station 1. Apply the decoding matrix at this third station.
  4. Proceed to the next station in numerical order; if you are at Station 6, proceed to Station 1. Apply the decoding matrix at this fourth station.
  5. Decode your message.

The numerical message is ,,,,,,,,,,,,,,,,,,,, which represents the characters “DO NOT WORRY TOO MUCH.”

1. Sydnie was in Group 1 and tried to decode her message by calculating the matrix and then multiplying. This produced the matrix  
   1. How did she know that she made a mistake?

If Sydnie had properly decoded her message, all entries in the matrix would be integers betweenand

* 1. Matrix was encoded using matrices ,, and , where decodes a message encoded by , decodes a message encoded by and so on. What is the relationship between matrices and , between and , etc.?

Matrices and are inverse matrices, as are and , , and and so on.

* 1. The matrix that Sydnie received was encoded by . Explain to Sydnie how the decoding process works to recover the original matrix , and devise a correct method for decoding using multiplication by a single decoding matrix.

Since , we can recover the original matrix by multiplying both sides of this equation by the proper decoding matrix at each step, remembering that , , etc.

Since matrix multiplication is associative, this means that

* 1. Apply the method you devised in part (c) to your group’s message to verify that it works.

So,

This is the same decoded message that we found in Exercise 2, part (f).

Exercise 4 (optional, 8 minutes)

The encoded phrase in this exercise is “RAMANUJAN.” Srinivasa Ramanujan (1887–1920) was a self-taught mathematician from India who made significant contributions to many branches of mathematics, particularly analysis and number theory, compiling thousands of mathematical results. Although he died young, he is widely considered to be one of the greatest mathematicians of his time.

The original message is stored in matrix , and the matrix used to encode the message is  
 In this optional exercise, students need to reason through the process of encoding and decoding to recover a missing entry in the decoding matrix when the encoding matrix is unknown. Use this exercise as an extension for students who have finished the previous exercises quickly.

1. You received a coded message in the matrix . However, the matrix that will decode this message has been corrupted, and you do not know the value of entry . You know that all entries in matrix are integers. Using to represent this unknown entry, the decoding matrix is given by . Decode the message in matrix .

Decoding the message requires that we multiply :

Since we know all entries are integers and that the entries represent letters, we know that

Solving these inequalities gives

Because we know that is an integer, the third inequality becomes , so we know that Then the decoded message is

thus,

and the decoded message is “RAMANUJAN.”

Closing (3 minutes)

Ask students to write a brief answer to the question, “How do matrix inverses make encoding and decoding messages possible?” Then, have students share responses with a partner before sharing responses as a class.

* How do matrix inverses make encoding and decoding messages possible?
  + *If an matrix is invertible, then it can be used to encode a message. We store the message in a matrix , where has rows, and then encode it by multiplying . To decode the message, we multiply*

Exit Ticket (4 minutes)

The message encoded in the problem in the Exit Ticket is “HYPATIA.” Hypatia (Hy-pay-shuh) of Alexandria (born between 350–370 CE, died 415 CE) is one of the earliest known female mathematicians. She was the head of the Neoplatonic School in Alexandria, Egypt, and the head of the Library of Alexandria. She was murdered in a religious conflict. None of her mathematical works have survived.

Name Date

Lesson 13: Using Matrix Operations for Encryption

Exit Ticket

Morgan used matrix to encode the name of her favorite mathematician in the message

,,,,,,,.

* 1. How can you tell whether or not her message can be decoded?
  2. Decode the message, or explain why the original message cannot be recovered.

Exit Ticket Sample Solutions

Morgan used matrix to encode the name of her favorite mathematician in the message

,,,,,,,.

* 1. How can you tell whether or not her message can be decoded?

*Since the matrix has determinant , we know that , so then a decoding matrix exists.*

* 1. Decode the message, or explain why the original message cannot be recovered.

First, we place the coded message into a matrix Using , we have

The decoded message is “HYPATIA.”

Problem Set Sample Solutions

Problems 1–4 are optional as they are practice on skills previously taught and assessed. Problems 6–9 allow students to practice the use of matrix multiplication for coding and decoding messages.

1. Let , ,, , and . Evaluate the following.

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

1. For any matrix and any real number , show that if , then or .

Let ; then . Suppose that .

Case 1: Suppose . Then and ; all imply that . Thus, if , then .

Case 2: Suppose that . Then at least one of and is not zero, so and imply that .

Thus, if , then either or .

1. Claire claims that she multiplied by another matrix and obtained as her result. What matrix did she multiply by? How do you know?

She multiplied by the multiplicative identity matrix. Since the product is a matrix, we know that is a matrix of the form . Multiplying gives Since  
 , we have the following system of equations:

The third and fourth equations give and , respectively, and substituting into the first two equations gives and . Thus, and , and the matrix must be .

1. Show that the only matrix such that is the zero matrix.

Let and ; then we have , , , , and . In each case, solving for the elements of , we find that .

1. A matrix of the form is a *diagonal* matrix. Daniel calculated

and concluded that if is a diagonal matrix and is any other matrix, then

* 1. Is there anything wrong with Daniel’s reasoning? Prove or disprove that if is adiagonal matrix, then for any other matrix

Yes, there is something wrong with Daniel’s reasoning. A single example does not establish that a statement is true, and the example he calculated used a special case of a diagonal matrix in which the entries on the main diagonal are equal.

If and , then and . Thus, it is not true that for all diagonal matrices and all other matrices

* 1. For matrices, Elda claims that only diagonal matrices of the form satisfy for any other matrix . Is her claim correct?

Elda is correct since . Then,  
for all matrices .

1. Calvin encoded a message using ,giving the coded message ,,,,,,,. Decode the message, or explain why the original message cannot be recovered.

Putting the message in a matrix, we have . We can decode the message with   
. Then the original message is found in message M:

The original message is “ALPHABET.”

1. Decode the message below using the matrix

,,,,-,,,,,,,.

The decoded message is found by multiplying . Then the message is “CRYPTOGRAPHY.”

1. Brandon encoded his name with the matrix , producing the matrix Decode the message, or explain why the original message cannot be recovered.

Brandon used a matrix that is not invertible. The original matrix cannot be recovered.

1. Janelle used the encoding matrix to encode the message “FROG” by multiplying  
   . When Taylor decoded it, she computed  
   . What went wrong?

Janelle multiplied her matrices in the wrong order. When Janelle tried to decode the matrix using the decoding matrix , she ended up calculating

Because matrix multiplication is not commutative, , Taylor was unable to recover the original message.