**BIG IDEA** Most $2 \times 2$ and most $3 \times 3$ matrices $A$ have an inverse, $A^{-1}$, of the same dimensions, that satisfies $A^{-1}A = AA^{-1} = I$, where $I$ is the identity matrix for their dimensions.

Are there ever times when you want to send a friend a note, but you want only your friend to be able to read it? To do this, you could use cryptography. Cryptography, which comes from the Greek words κρυπτός (hidden) and γραφία (writing), is the study of encoding and decoding messages. In this lesson you will see how to use the **inverses of matrices** in cryptography.

### What Are Inverse Matrices?

The idea of an inverse of an operation runs throughout mathematics. Recall that two real numbers $a$ and $b$ are **additive inverses** (or **opposites**) if and only if $a + b = 0$. For example, $7.3$ and $-7.3$ are additive inverses. The sum of two additive inverses is 0, the additive identity. Two real numbers $a$ and $b$ are **multiplicative inverses** (or **reciprocals**) if and only if $ab = 1$. For example, $\pi$ and $\frac{1}{\pi}$ are multiplicative inverses. The product of two multiplicative inverses is 1, the multiplicative identity.

The definition of **inverse matrices** under multiplication follows the same idea as the inverses mentioned above. The $2 \times 2$ matrices $A$ and $B$ are called **inverse matrices** if and only if their product is the $2 \times 2$ identity matrix for multiplication, that is, if and only if

$$AB = BA = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$ 

Because matrix multiplication is not commutative, the definition of **inverse matrices** requires that the product in both orders of multiplication be the identity. To be multiplied in both directions, the matrices must be **square matrices**, those with the same number of rows and columns.

So there can be inverse $3 \times 3$ matrices, inverse $4 \times 4$ matrices, and so on. But there cannot be inverse $2 \times 3$ matrices. Furthermore, as you will see, not all square matrices are **invertible** (have inverses).

---

**Mental Math**

Sheila tosses a fair 6-sided die. What is the probability that the die shows

a. a 4?

b. an even number?

c. a prime number?

d. a rational number?
Notation for Inverse Matrices

The real number $x^{-1}$ is equal to $\frac{1}{x}$, the multiplicative inverse of $x$, for all $x \neq 0$. Similarly, the symbol $M^{-1}$ stands for the inverse of the square matrix $M$, if $M$ has an inverse. Many graphing calculators and all CAS can display matrices and their inverses. To verify that two matrices are inverses, multiply.

Activity 1

**MATERIALS** CAS or graphing calculator

**Step 1** Clear the variable $a$ on your calculator. Store $\begin{bmatrix} -3 & 5 \\ 7 & -11 \end{bmatrix}$ in your calculator as variable $a$.

**Step 2** Calculate $a^{-1}$ by using the inverse key on your calculator, or by entering $a^{-1}$.

**Step 3** Find the product $aa^{-1}$.

**Step 4** Find the product $a^{-1}a$.

A Formula for the Inverse of a $2 \times 2$ Matrix

You do not need a calculator to obtain the inverse of a $2 \times 2$ matrix. There is a formula.

**Inverse Matrix Theorem**

If $ad - bc \neq 0$ and $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, then $M^{-1} = \begin{bmatrix} \frac{d}{ad-bc} & -\frac{b}{ad-bc} \\ -\frac{c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$.

**Proof** We need to show that the product of the two matrices in either order is the identity matrix. Below, we show one order. In Question 9, you are asked to verify the multiplication in the reverse order.

\[
\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} d & -b \\ \frac{ad-bc}{ad-bc} & \frac{ad-bc}{ad-bc} \\ -\frac{c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix} = \begin{bmatrix} \frac{ad}{ad-bc} + \frac{-bc}{ad-bc} & \frac{-ab}{ad-bc} + \frac{ab}{ad-bc} \\ \frac{cd}{ad-bc} + \frac{-cd}{ad-bc} & \frac{-bc}{ad-bc} + \frac{ad}{ad-bc} \end{bmatrix}
\]

Matrix multiplication

\[
= \begin{bmatrix} \frac{ad-bc}{ad-bc} & 0 \\ 0 & \frac{ad-bc}{ad-bc} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}
\]

Addition of fractions, definition of subtraction
Not only does the Inverse Matrix Theorem tell you how to find an inverse without a calculator, it gives you a quick test for whether an inverse exists. Note that \( ad - bc \) cannot be zero because it is in the denominator of all the fractions. The inverse of a \( 2 \times 2 \) matrix \( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \) exists only if \( ad - bc \neq 0 \).

**GUIDED Example**

Use the Inverse Matrix Theorem to find the inverse of each matrix, if it exists.

a. \( \begin{bmatrix} -2 & 4 \\ -1 & 6 \end{bmatrix} \)  
   b. \( \begin{bmatrix} 5 & 10 \\ 3 & 6 \end{bmatrix} \)

**Solution**

a. In \( \begin{bmatrix} -2 & 4 \\ -1 & 6 \end{bmatrix} \), \( a = \) \( \_ \), \( b = \) \( \_ \), \( c = \) \( \_ \), and \( d = \) \( \_ \).

So, \( ad - bc = ( \_ \cdot \_ - \_ \cdot \_ ) = \_ \), and the matrix has an inverse.

Now substitute into the formula. The inverse is \( \begin{bmatrix} \_ & \_ \\ \_ & \_ \end{bmatrix} \), which simplifies to \( \begin{bmatrix} \_ & \_ \\ \_ & \_ \end{bmatrix} \).

b. In \( \begin{bmatrix} 5 & 10 \\ 3 & 6 \end{bmatrix} \), \( a = \) \( \_ \), \( b = \) \( \_ \), \( c = \) \( \_ \), and \( d = \) \( \_ \).

So \( ad - bc = ( \_ \cdot \_ - \_ \cdot \_ ) = \_ \).

Because \( ad - bc = \_ \), \( \begin{bmatrix} 5 & 10 \\ 3 & 6 \end{bmatrix} \) has \( \_ \).

If a matrix has no inverse, trying to find it on a calculator leads to an error message. Some calculators say the inverse is undefined, while others say the original matrix is a **singular matrix**, meaning that its inverse does not exist.
Determinants and Inverses

The formula in the Inverse Matrix Theorem can be simplified using scalar multiplication. When $ad - bc \neq 0$,

$$\begin{bmatrix} \frac{d}{ad-bc} & -\frac{b}{ad-bc} \\ -\frac{c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Because the number $ad - bc$ determines whether or not a matrix has an inverse, it is called the determinant of the matrix. We abbreviate the word determinant as $det$. Thus, the Inverse Matrix Theorem can be written:

If $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, then $M^{-1} = \frac{1}{\text{det}M} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ if and only if $\text{det} M \neq 0$.

Calculators that handle matrices have a determinant function, usually called $\text{det}$.

Using Matrices to Encode and Decode

How can matrices and their inverses help in cryptography? At the right is a picture of a decoder ring, created as part of a promotional offer in May, 2000. On the outside circle are the letters of the alphabet and on the inside circle are the numbers 1 through 26. You are able to turn the inside dial so the number 1 can correspond to any of the letters in the alphabet. In the configuration in the photo at the right, 1 corresponds to C. This is the key to the code. A message gets encoded as a set of numbers. To decode the message, the recipient sets the dial according to the key and reads the letters corresponding to the numbers. For example, the code 9, 16, 4, 4, 15 in this configuration decodes as HELLO.

While encoding phrases using the ring is easy to do, it is also relatively easy to decode them. For one thing, each number always stands for the same letter. For example, each E is encoded as 16. Also, it is easy to tell the length of a word. For these reasons it would not be too difficult to break the code. Businesses and governments need a more powerful method of encryption. One such method is to use matrices.

QY

a. Use a calculator to find the determinant of $\begin{bmatrix} -3 & 5 \\ 7 & -11 \end{bmatrix}$.

b. Check by hand.
Activity 2

MATERIALS CAS or graphing calculator

Step 1 To encode a phrase using matrices, first make a key by assigning a number to each letter like the ring does on the previous page. For this Activity, let \( A = 1 \), \( B = 2 \), and so on, and assign the number 27 to spaces between words. Use this method to make a key for MEET ME IN THE PARK in the table below. It has been started for you.

<table>
<thead>
<tr>
<th>M</th>
<th>E</th>
<th>E</th>
<th>T</th>
<th>M</th>
<th>E</th>
<th>I</th>
<th>N</th>
<th>T</th>
<th>H</th>
<th>E</th>
<th>P</th>
<th>A</th>
<th>R</th>
<th>K</th>
</tr>
</thead>
</table>

Step 2 Create a \( 2 \times 2 \) encoder matrix \( e \) that has an inverse, for example, \( e = \begin{bmatrix} -3 & 8 \\ 2 & 5 \end{bmatrix} \).

Store this matrix in variable \( e \) in a calculator.

Although we are using a \( 2 \times 2 \) matrix for an encoder, any size square matrix with an inverse could be used.

Step 3 Turn the message into a matrix. Because you are using a \( 2 \times 2 \) matrix as an encoder, use a matrix with 2 rows. Enter your numerical message from Step 2 starting at the left of the matrix and filling the columns from top to bottom, left to right. Fill in the empty element at the end with a 27, like the other spaces.

\[
\begin{bmatrix}
\end{bmatrix}
\]

Step 4 Store your matrix from Step 3 as \( m \). Multiply the encoder matrix \( e \) by \( m \) and store the product as \( v \).

Step 5 To send the encoded message, record it as 1, 51, 145, 110, and so on, reading down the columns of \( v \). Notice that with this encoding method, each E (or any other letter) does not get encoded to the same number, making it a more difficult code to break.

Step 6 Imagine that you gave your encoded message to a friend. The friend is a receiver. The receiver first needs to rewrite the message as a \( 2 \times 10 \) matrix (the one you named \( v \)). Your friend then needs a decoder matrix to undo the multiplication by your encoder matrix \( e \). This matrix is \( e^{-1} \). Multiply the inverse matrix by matrix \( v \). This is how the receiver would get your keyed message. He or she could then use the key to read the message.
Step 7  If you want to send encoded messages this way, the receiver needs to know only the encoding matrix and the key. The receiver can then find the inverse matrix and apply it. Use the encoding matrix \[
\begin{pmatrix}
-89 & 120 \\
35 & 6 
\end{pmatrix}
\] and the key from this Activity \((A = 1, B = 2, \ldots)\) to decode the following message: \(-1304, 566, 589, 779, -843, 1023, 2311, 155, 2528, 442\)

Questions

**COVERING THE IDEAS**

1. Identify the identity for each operation.
   a. real-number multiplication
   b. real-number addition
   c. \(2 \times 2\) matrix multiplication

2. Explain why only square matrices can have inverses.

3. If \(N\) is a \(2 \times 2\) matrix and \(N^{-1}\) exists, find each product.
   a. \(NN^{-1}\)
   b. \(N^{-1}N\)

4. Verify that \[
\begin{pmatrix}
\frac{3}{4} & \frac{1}{2} \\
\frac{1}{8} & \frac{1}{4} 
\end{pmatrix}
\] is the inverse of \[
\begin{pmatrix}
-2 & 4 \\
-1 & 6 
\end{pmatrix}
\] using matrix multiplication.

5. a. When does the matrix \[
\begin{pmatrix}
a & b \\
c & d 
\end{pmatrix}
\] have an inverse?
   b. What is that inverse?

6. Determine whether each matrix has an inverse.
   a. \[
\begin{pmatrix}
3 & 2 \\
3 & 2 
\end{pmatrix}
\]
   b. \[
\begin{pmatrix}
3 & -2 \\
-3 & 2 
\end{pmatrix}
\]
   c. \[
\begin{pmatrix}
3 & -2 \\
3 & 2 
\end{pmatrix}
\]

In 7 and 8, give the determinant of the matrix. Give the inverse of the matrix if it exists.

7. \[
\begin{pmatrix}
2 & 9 \\
-7 & 6 
\end{pmatrix}
\]

8. \[
\begin{pmatrix}
12 & -2 \\
25 & 5 
\end{pmatrix}
\]

9. Complete the second part of the proof of the Inverse Matrix Theorem. That is, show that the identity matrix is the product of the two matrices in the reverse order.
10. Refer to Activity 2. A message has the encoder matrix \[\begin{bmatrix} 4 & -8 \\ 10 & -10 \end{bmatrix}\]. Find its decoder matrix.

In 11 and 12, use the following key.

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

11. Encode the message MATRICES DO CODES using the matrix \[\begin{bmatrix} 2 & 1 \\ 7 & 4 \end{bmatrix}\]. Use 27 to represent a space.

12. Kendra got the message 378, -202, 294, -56, 504, -162, 343, -7, 273, -51, 203, 73, the encoder matrix \[\begin{bmatrix} 14 & 7 \\ -8 & 3 \end{bmatrix}\], and the key above.

a. What is the decoding matrix?
b. Decode the message.

**APPLYING THE MATHEMATICS**

13. Give an example of a 2 × 2 matrix not mentioned in this lesson that does not have an inverse.

14. If it has one, the inverse of a 2 × 2 matrix can be found by solving a pair of systems of linear equations. For example, if the inverse of \[\begin{bmatrix} 1 & 4 \\ 2 & -2 \end{bmatrix}\] is \[\begin{bmatrix} a & b \\ c & d \end{bmatrix}\], then \[\begin{bmatrix} 1 & 4 \\ 2 & -2 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\].

This yields the systems \[\begin{cases} a + 4c = 1 \\ 2a - 2c = 0 \end{cases}\] and \[\begin{cases} b + 4d = 0 \\ 2b - 2d = 1 \end{cases}\].

a. Solve these two systems and determine the inverse matrix.
b. Check your answer to Part a using matrix multiplication.

15. a. Multiply the matrix for \(R_{90}\) by the matrix for \(R_{270}\) in both orders.
b. Based on your answer to Part a, what can you say about the two matrices? Why do you think this is so?
c. Based on your answer to Part b, find the inverse of the matrix for \(R_{180}\). Try to get the answer *without* doing any calculations.
**REVIEW**

In 16 and 17, a situation is presented and a question is asked.

a. Set up a system of equations to represent the situation.

b. Solve the system using any method and answer the question.

c. Explain why you chose the method you did in Part b.

(Lessons 5-4, 5-3, 5-2)

16. Javier is making mango-and-banana fruit salad to take to a party. Mangos cost $2.19/pound and bananas cost $0.89/pound. Javier decides to buy 5 pounds of fruit for $7.50. How many pounds of each fruit does he buy?

17. Trevon is going on a long mountain bike ride. During the ride, he wants to make sure he consumes 160 g of carbohydrates, 20 g of protein, and 3 liters of fluids. An energy bar contains 50 g of carbohydrates, 10 g of protein, and no fluids. An energy drink bottle contains 30 g of carbohydrates, no protein, and 750 mL of fluid. A water bottle contains no carbohydrates, no protein, and 750 mL of fluid. How many energy bars, energy drink bottles, and water bottles should Trevon pack for his ride?

18. Translate into a single formula: \( P \) varies directly as \( w \) and inversely as \( m \) and \( r^2 \). (Lesson 2-9)

19. A car is traveling at 60 miles per hour. (Lessons 2-4, 2-1)

a. Write a variation equation to describe the distance \( d \) in miles the car travels in \( t \) hours.

b. Graph your equation from Part a.

**EXPLORATION**

20. Let \( A = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \) and \( B = \begin{bmatrix} 0 & -1 \\ 3 & 0 \end{bmatrix} \).

a. Calculate \( \det A \), \( \det B \), and \( \det AB \). What do you notice about these values?

b. Make a conjecture about the determinant of the product of two \( 2 \times 2 \) matrices. Check it for two pairs of \( 2 \times 2 \) matrices of your choosing.

**QY ANSWER**

a. \(-2\)

\[
\text{det}\begin{bmatrix} 3 & 5 \\ 7 & 11 \end{bmatrix} = -2
\]

b. \(-3 \cdot -11 - 5 \cdot 7 = 33 - 35 = -2\)

Inverses of Matrices 335