4.6: Cryptography and Matrices

Inverse Matrices

Cryptography can be defined as the coding and decoding of messages sent, so that they may only be read by the sender and the recipient. The Egyptians, Greeks and Romans all used secret codes in military and politics. Caesar used a simple shift of three so that A meant D, B meant E and so on. Most people were illiterate so any type of substitution worked.

Modern day cryptography is dominated by computers and is still used in the military and government but also by business and private individuals (computer data transfer) and uses bigger "keys" (i.e. algorithms), to keep secure. No system is 100% unbreakable since the ideas are based on mathematics.

One of the most common secret codes is an Alpha-Numeric Substitution using a key like the one below.

Blank	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	15

P	Q	R	S	T	U	V	W	X	Y	Z	.	,	!	?
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

1. Let's send the message: **Math Rocks!**
   Map the letters to the corresponding numbers. What do you get?

2. How could you make this code more secure?

II. Cryptography and Matrices

We will use matrices to make a more secure key and encode our message before sending. First, we choose a **block size** (blocks of two numbers, three numbers, four numbers, etc) and divide up the message into blocks of this size – adding zeros at the end, if needed.

Let's use blocks of two for this example, so from our first message

13 1 20 8 0 18 15 3 11 19 29 0 (note the added zero)

Now, we form a Matrix B by placing the blocks as columns of the matrix.

3. The first two blocks have been filled in below. Fill in the remaining blocks.

$$B=\begin{bmatrix}13 & 20 & & \\ 1 & 8 & & \end{bmatrix}$$

Of course, we could use any arithmetic operation to encode the message further – addition, subtraction, or even scalar multiplication – but multiplying by another matrix A will give us the most secure code of all. And one more trick: the matrix has to be a square matrix. A **square matrix** is one that has the same number of rows as columns.

4. Multiply matrix B above by $\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$. Why would this not be a good encoding matrix?

This is known as an Identity Matrix.

IDENTITY MATRIX

The **identity matrix** I_n is the $n \times n$ matrix for which each main diagonal entry is a 1 and for which all other entries are 0.

Thus the 2 x 2, 3 x 3, and 4 x 4 identity matrices are

$$I_2=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \qquad I_3=\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix} \qquad I_4=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}$$

Identity matrices behave like the number 1 in the sense that $A \cdot I_n = A$ and $I_n \cdot B = B$ whenever these products are defined.

5. Multiply matrix B by $\begin{bmatrix} 1 & 4 \\ -1 & -3 \end{bmatrix}$. Why would this be a better encoding matrix?

6. Create your own message, but keep it under 40 characters (for now).
   a. Apply Key 1: the alpha-numeric substitution
   b. Apply Key 2: separate into blocks of two
   c. Apply Key 3: create your own square matrix with no zeros in it

III. Decoding with Inverse Matrices

Since we encoded B by multiplying by matrix A, then to decode the message, all one has to do is multiply by the inverse matrix A^{-1}.

INVERSE OF A MATRIX

Let A be a square $n \times n$ matrix. If there exists an $n \times n$ matrix A^{-1} with the property that

$$AA^{-1} = A^{-1}A = I_n$$

then we say that A^{-1} is the **inverse** of A.

$$C = \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix} \qquad D = \begin{bmatrix} 3 & -1 \\ -5 & 2 \end{bmatrix}$$

7. Perform matrix multiplication to prove that C and D are inverse matrices. (Remember that matrix multiplication is not always commutative, so check that both CD and DC equal I.

The following rule provides a simple way for finding the inverse of a 2 x 2 matrix, when it exists. For larger matrices there is a more general procedure for finding inverses, which we consider later.

INVERSE OF A 2 × 2 MATRIX

If $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, then

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

If $ad - bc = 0$, then A has no inverse.

The quantity $ad - bc$ that appears in the rule for calculating the inverse of a 2 x 2 matrix is called the **determinant** of the matrix. If the determinant is 0, then the matrix does not have an inverse (since we cannot divide by 0).

EXAMPLE 1 – The Inverse of a 2x2 Matrix

Find the inverse of $A = \begin{bmatrix} 1 & 4 \\ -1 & -3 \end{bmatrix}$ (this was Key 2 of our encoding process.)

- First, assign variables a-d, according to the rule above
  $a = 1$, $b = 4$, $c =$ -1 and $d =$ -3
- Then substitute in the formula

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

$$A^{-1} = \frac{1}{(1 \cdot -3) - (4 \cdot -1)}\begin{bmatrix} -3 & -(4) \\ -(-1) & 1 \end{bmatrix}$$

- Simplify

$$A^{-1} = \frac{1}{-3 + 4}\begin{bmatrix} -3 & -4 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} -3 & -4 \\ 1 & 1 \end{bmatrix}$$

So, this is our decoding matrix. Let's apply it to our coded message from Question 5.

$$A^{-1} = \begin{bmatrix} -3 & -4 \\ 1 & 1 \end{bmatrix} \quad B' = \begin{bmatrix} 17 & 52 & 72 & 69 & 81 & 29 \\ -16 & -44 & -54 & -57 & -62 & -29 \end{bmatrix}$$

8. Multiply $A^{-1} \cdot B'$.

9. Decode the message:
   a. Rewrite the 2 x 6 matrix as a single sequence of numbers. Remember to change the columns to blocks of two characters.

   b. Translate the numbers into words using Key 1. Write it BIG!

2 x 2 Practice:

10. Find the inverse of the following 2 x 2 matrices. Verify that $AA^{-1} = A^{-1}A = I$. If there is no inverse, explain why.
    a. $\begin{bmatrix} 3 & 4 \\ 7 & 9 \end{bmatrix}$

    b. $\begin{bmatrix} -7 & 4 \\ 8 & -5 \end{bmatrix}$

    c. $\begin{bmatrix} 12 & -9 \\ 4 & -3 \end{bmatrix}$

    d. $\begin{bmatrix} \frac{1}{2} & \frac{1}{3} \\ 5 & 4 \end{bmatrix}$

11. Create your own message, but keep it under 40 characters (for now).
    d. Apply Key 1: the alpha-numeric substitution
    e. Apply Key 2: try using blocks of three this time
    f. Apply Key 3: create your own square matrix with no zeros in it.

IV. Finding the Inverse of a 3 x 3 (or Larger) Matrix

For 3 x 3 and larger square matrices the following technique provides the most efficient way to calculate their inverses. If A is an n x n matrix, we first construct the n x $2n$ matrix that has the entries of A on the left and of the identity matrix I_n on the right:

$$\left[\begin{array}{cccc|cccc} a_{11} & a_{12} & \cdots & a_{1n} & 1 & 0 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & a_{2n} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} & 0 & 0 & \cdots & 1 \end{array}\right]$$

We then use the elementary row operations on this new large matrix to change the left side into the identity matrix. (This means that we are changing the large matrix to reduced row-echelon form.) The right side is transformed automatically into A^{-1}.

EXAMPLE 2 – Finding the Inverse of a 3 x 3 Matrix

$$A = \begin{bmatrix} 1 & -2 & -4 \\ 2 & -3 & -6 \\ -3 & 6 & 15 \end{bmatrix}$$

We begin by creating a 3 x 6 matrix whose left half is A and whose right half is the identity matrix.

$$A = \left[\begin{array}{ccc|ccc} 1 & -2 & -4 & 1 & 0 & 0 \\ 2 & -3 & -6 & 0 & 1 & 0 \\ -3 & 6 & 15 & 0 & 0 & 1 \end{array}\right]$$

We then transform the left half of this new matrix into the identity matrix by performing the following sequence of elementary row operations on the *entire* new matrix.

$$\xrightarrow[R_3 + 3R_1 \to R_3]{R_2 - 2R_1 \to R_2} \left[\begin{array}{ccc|ccc} 1 & -2 & -4 & 1 & 0 & 0 \\ 0 & 1 & 2 & -2 & 1 & 0 \\ 0 & 0 & 3 & 3 & 0 & 1 \end{array}\right]$$

$$\xrightarrow{\frac{1}{3}R_3} \left[\begin{array}{ccc|ccc} 1 & -2 & -4 & 1 & 0 & 0 \\ 0 & 1 & 2 & -2 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & \frac{1}{3} \end{array}\right]$$

$$\xrightarrow{R_1 + 2R_2 \to R_1} \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & -3 & 2 & 0 \\ 0 & 1 & 2 & -2 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & \frac{1}{3} \end{array}\right]$$

$$\xrightarrow{R_2 - 2R_3 \to R_2} \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & -3 & 2 & 0 \\ 0 & 1 & 0 & -4 & 1 & -\frac{2}{3} \\ 0 & 0 & 1 & 1 & 0 & \frac{1}{3} \end{array}\right]$$

We have now transformed the left half of this matrix into an identity matrix. (This means that we have put the entire matrix in reduced row-echelon form.) Note that to do this in as systematic a fashion as possible, we first changed the elements below the main diagonal to zeros, just as we would if we were using Gaussian elimination. We then changed each main diagonal element to a 1 by multiplying by the appropriate constant(s). Finally, we completed the process by changing the remaining entries on the left side to zeros.

The right half is now A^{-1}.

$$A^{-1} = \begin{bmatrix} -3 & 2 & 0 \\ -4 & 1 & -\frac{2}{3} \\ 1 & 0 & \frac{1}{3} \end{bmatrix}$$

Your Turn:

12. Find the inverse of the following 3 x 3 matrices. Verify that $AA^{-1} = A^{-1}A = I$. If there is no inverse, explain why.

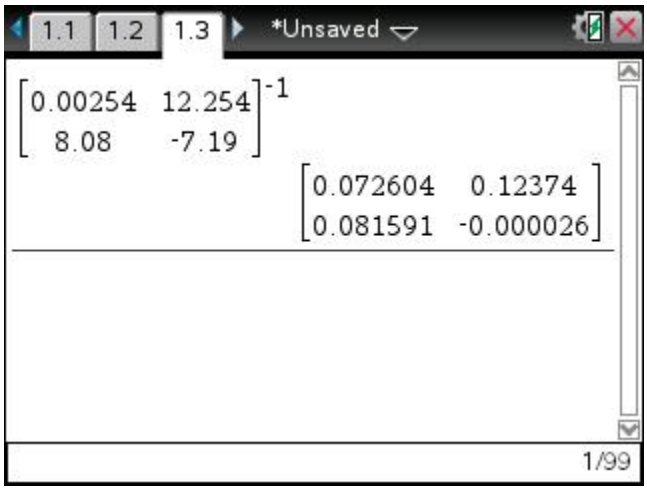
    a. $\begin{bmatrix} 4 & 2 & 3 \\ 3 & 3 & 2 \\ 1 & 0 & 1 \end{bmatrix}$

b. $\begin{bmatrix} 5 & 7 & 4 \\ 3 & -1 & 3 \\ 6 & 7 & 5 \end{bmatrix}$

c. $\begin{bmatrix} 2 & 1 & 0 \\ 1 & 1 & 4 \\ 2 & 1 & 2 \end{bmatrix}$

d. $\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$

Graphing calculators are also able to calculate matrix inverses. On the TI-nSpire raising a matrix to the -1 power will calculate the inverse.



On the TI-84 calculators, matrices are stored in memory using names such as [A], [B], [C]. To find the inverse of [A], we key in

[A] x^{-1} ENTER