The inverse of a matrix

A matrix that has an inverse is called **invertible**. A matrix that does not have an inverse is called **singular**. Most matrices don't have an inverse. The only kind of matrix that has an inverse is a square matrix, and even most square matrices don't have inverses. For the purposes of this exercise, I'll make sure to give you matrices that are invertible. If you have to come up with an invertible matrix of your own, guess and check.

There are a couple of ways to find the inverse. Right now, we'll use the property that any matrix times its inverse equals the **identity matrix** (a matrix with 1s on it's upper left to bottom right diagonal and 0s everywhere else).

Example:

If your matrix is $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$, then you know that $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ times its inverse = $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Since we don't know what the inverse is, let's just fill in a 2x2 matrix with a bunch of variables: $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$

Then $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

But $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1a+2c & 1b+2d \\ 3a+4c & 3b+4d \end{bmatrix}$

So $\begin{bmatrix} 1a+2c & 1b+2d \\ 3a+4c & 3b+4d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Since corresponding elements of equal matrices are equal, you can make a couple of systems, one for *a* and *c*, and one for *b* and *d*.

$\begin{cases} 1a+2c=1 \\ 3a+4c=0 \end{cases}$ and $\begin{cases} 1b+2d=0 \\ 3b+4d=1 \end{cases}$

Solving these systems gives us a = -2, b = 1, c = 3/2, and d = -1/2. So our inverse matrix is $\begin{bmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{bmatrix}$

Use this method to find the inverse of $\begin{bmatrix} 5 & 4 \\ 3 & 2 \end{bmatrix}$

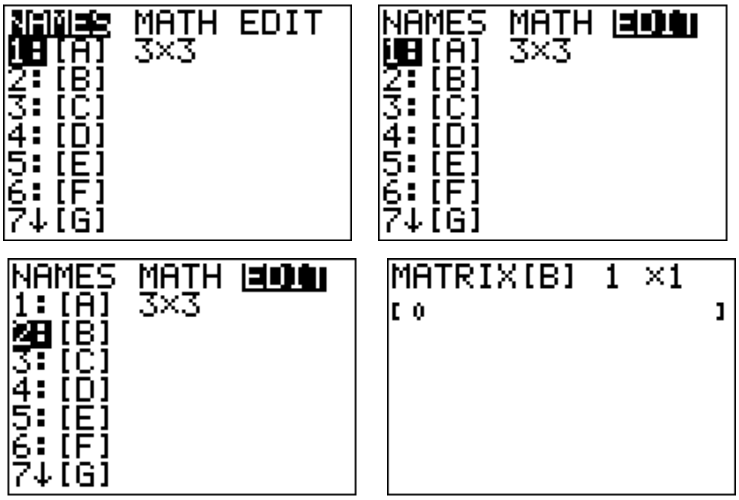
Use this method to find the inverse of $\begin{bmatrix} -2 & 3 \\ 1 & -1 \end{bmatrix}$

There's got to be a better way!!! Why yes. Now that you can do this by hand, it's time to let your graphing calculator do the drudgery.

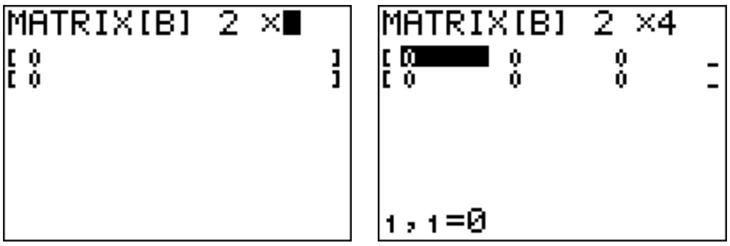
Before we can operate on a matrix, we must first enter the matrix into the TI83/84 calculator. Enter the following matrix into the calculator as matrix [B].

$$\begin{bmatrix} 5 & 14 & 7 & 1 \\ 2 & 3 & 10 & 4 \end{bmatrix}$$

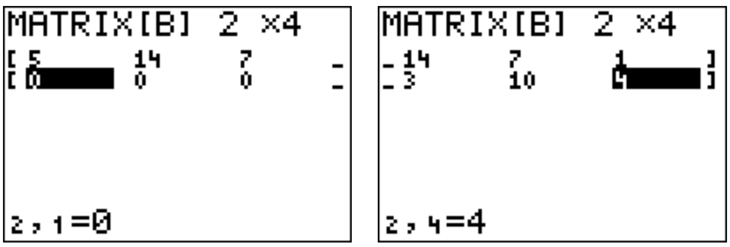
Press the 2^{nd} x^{-1} to get the matrix menu. Right arrow twice to highlight the EDIT menu. Select [B] and then press ENTER .



Next we enter the dimension of the matrix which is 2 X 4. Press 2 ENTER. The 2 appears and the cursor advances to the next position. Now press 4 ENTER. The size in now determined. We enter the numbers across the rows beginning with row one. The bottom of the screen lists the entry's position in the matrix.



Now press 5 ENTER 14 ENTER 7 ENTER 1 ENTER. This completes the first row. Press 2 ENTER 3 ENTER 10 ENTER 4 ENTER.

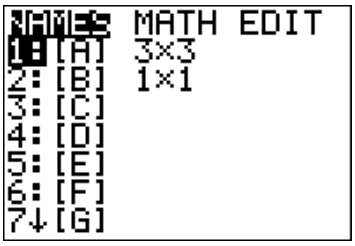


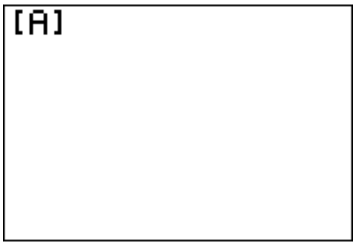
To exit the matrix editor, press 2^{nd} MODE [QUIT]. That returns you to the home screen.

Find the inverse of the following matrix.

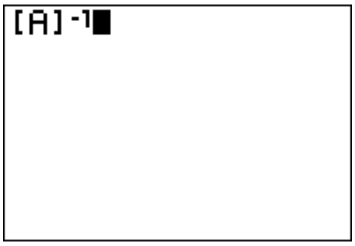
$$\begin{bmatrix} 1 & 2 & 0 \\ 3 & -1 & 2 \\ 2 & 0 & 1 \end{bmatrix}$$

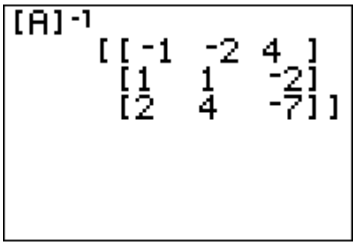
Press the matrix button or combination of buttons to get the matrix menu. Next,enter the matrix using the matrix editor under one of the letters. This time we will use[A]. From the home screen, re-enter the matrix menu. Select1: [A], then press ENTER.





Press the x^{-1} key, and then press ENTER. The inverse matrix is displayed.

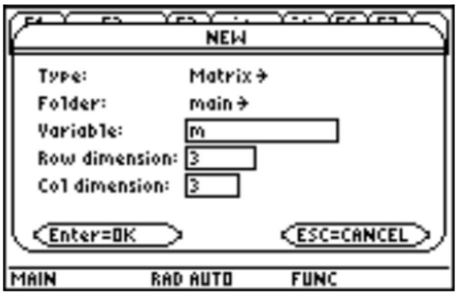




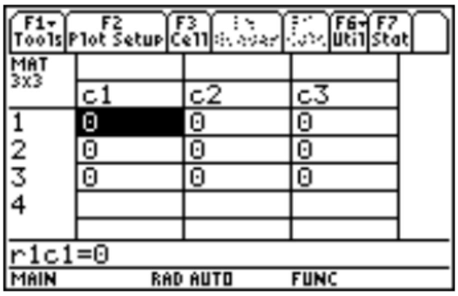
There's got to be a better way!!! Why yes. Now that you can do this by hand, it's time to let your graphing calculator do the drudgery.

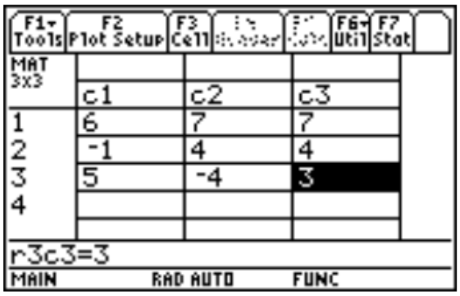
Entering Matrices

To enter a matrix on the TI-89 choose the Data/Matrix Editor. Indicate that you are entering a "New" matrix. On the next screen select 2:Matrix for type, enter a name for the matrix and the size of the matrix.



This will result in a screen showing a matrix of the appropriate size that is filled with zeros. Fill in the matrix with the values (either numerical or variable).





Remember to use the (-) key to the left of the enter key for negative numbers, not the subtraction key.

This matrix may also be entered and stored from the entry line of the HOME screen by typing [6, 7, 7; -1, 4, 4; 5, -4, 3] -> m.

Note that we are using a numerical example here, but we may also have symbolic entries in the matrix.

Matrix Functions

The TI-89 has many functions that allow you to manipulate matrices and vectors.
Go to the Home Screen. Use the MATH key (2nd, 5) to select 4:Matrix and then choose what operation to perform on your matrix. To find the inverse, m^{-1}, you don't even need the math menu; just use the alpha key to type m^ - 1. (This will find the inverse, rather than 1/m because matrix division doesn't exist.)

Application to Cryptography

Cryptography, to most people, is concerned with keeping communications private. Indeed, the protection of sensitive communications has been the emphasis of cryptography throughout much of its history. Encryption is the transformation of data into some unreadable form. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended, even those who can see the encrypted data. Decryption is the reverse of encryption; it is the transformation of encrypted data back into some intelligible form.

Encryption and decryption require the use of some secret information, usually referred to as a key. Depending on the encryption mechanism used, the same key might be used for both encryption and decryption, while for other mechanisms, the keys used for encryption and decryption might be different.

Today governments use sophisticated methods of coding and decoding messages. One type of code, which is extremely difficult to break, makes use of a large matrix to encode a message. The receiver of the message decodes it using the inverse of the matrix. This first matrix is called the **encoding matrix** and its inverse is called the **decoding matrix.**

Example Let the message be

PREPARE TO NEGOTIATE

and the encoding matrix be

$$\begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix}$$

We assign a number for each letter of the alphabet. For simplicity, let us associate each letter with its position in the alphabet: A is 1, B is 2, and so on. Also, we assign the number 27 (remember we have only 26 letters in the alphabet) to a space between two words. Thus the message becomes:

P	*R*	*E*	*P*	*A*	*R*	*E*	*	*T*	*O*	*	*N*	*E*	*G*	*O*	*T*	*I*	*A*	*T*	*E*
16	18	5	16	1	18	5	27	20	15	27	14	5	7	15	20	9	1	20	5

Since we are using a 3 by 3 matrix, we break the enumerated message above into a sequence of 3 by 1 vectors:

$$\begin{bmatrix} 16 \\ 18 \\ 5 \end{bmatrix} \begin{bmatrix} 16 \\ 1 \\ 18 \end{bmatrix} \begin{bmatrix} 5 \\ 27 \\ 20 \end{bmatrix} \begin{bmatrix} 15 \\ 27 \\ 14 \end{bmatrix} \begin{bmatrix} 5 \\ 7 \\ 15 \end{bmatrix} \begin{bmatrix} 20 \\ 9 \\ 1 \end{bmatrix} \begin{bmatrix} 20 \\ 5 \\ 27 \end{bmatrix}$$

Note that it was necessary to add a space at the end of the message to complete the last vector. We now encode the message by multiplying each of the above vectors by the encoding matrix. This can be done by writing the above vectors as columns of a matrix and perform the matrix multiplication of that matrix with the encoding matrix as follows:

$$\begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix} \begin{bmatrix} 16 & 16 & 5 & 15 & 5 & 20 & 20 \\ 18 & 1 & 27 & 27 & 7 & 9 & 5 \\ 5 & 18 & 20 & 14 & 15 & 1 & 27 \end{bmatrix}$$

which gives the matrix

$$\begin{bmatrix} -122 & -123 & -176 & -182 & -96 & -91 & -183 \\ 23 & 19 & 47 & 41 & 22 & 10 & 32 \\ 138 & 139 & 181 & 197 & 101 & 111 & 203 \end{bmatrix}$$

The columns of this matrix give the encoded message. The message is transmitted in the following linear form

$$\begin{array}{ccccccccc} -122, & 23, & 138, & -123, & 19, & 139, & -176, & 47, & 181, \\ -182, & 41, & 197, & -96, & 22, & 101, & -91, & 10, & 111, \\ -183 & 32 & 203. & & & & & & \end{array}$$

To decode the message, the receiver writes this string as a sequence of 3 by 1 column matrices and repeats the technique using the inverse of the encoding matrix. The inverse of this encoding matrix, the decoding matrix, is:

$$\begin{bmatrix} 1 & 0 & 1 \\ 4 & 4 & 3 \\ -4 & -3 & -3 \end{bmatrix}$$

Thus, to decode the message, perform the matrix multiplication

$$\begin{bmatrix} 1 & 0 & 1 \\ 4 & 4 & 3 \\ -4 & -3 & -3 \end{bmatrix} \begin{bmatrix} -122 & -123 & -176 & -182 & -96 & -91 & -183 \\ 23 & 19 & 47 & 41 & 22 & 10 & 32 \\ 138 & 139 & 181 & 197 & 101 & 111 & 203 \end{bmatrix}$$

and get the matrix

$$\begin{bmatrix} 16 & 16 & 5 & 15 & 5 & 20 & 20 \\ 18 & 1 & 27 & 27 & 7 & 9 & 5 \\ 5 & 18 & 20 & 14 & 15 & 1 & 27 \end{bmatrix}$$

The columns of this matrix, written in linear form, give the original message:

$$\begin{array}{cccccccccccccccccccc} 16 & 18 & 5 & 16 & 1 & 18 & 5 & 27 & 20 & 15 & 27 & 14 & 5 & 7 & 15 & 20 & 9 & 1 & 20 & 5 \\ P & R & E & P & A & R & E & * & T & O & * & N & E & G & O & T & I & A & T & E \end{array}$$

Encoding Worksheet Name: ______________________________

Use the following table to compose a secret message to your friend. Write the letters of your message on the top line and the corresponding numbers below each letter. Use 27 for any spaces.

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	27

(more space, if you need it)

Now take the numbers and, starting in the upper left corner and moving down the column and then to the next column, fill in the 3 x whatever grid with your numerical message. You don't have to use all the columns, but every column you use needs to be full. Add a 27 to any empty blocks (max 2) to finish up the column.

Now choose your encrypting matrix. To encode a 3 x whatever matrix, your matrix needs to be 3 x 3. Check to be sure the matrix you picked is invertible, or no one will be able to decode your note!

Encoding Matrix:
(pick any matrix, as long as it's invertible)

Decoding Inverse:
(checking invertibility - don't give this to your friend!)

Use your calculator to multiply your encoding matrix and your message matrix.

Encoded message:

Now starting in the upper left corner and working down, copy the numbers into a long strip. This is what you will give your partner, along with the **encoding matrix** (make them find the decoding matrix for themselves!)

(more space, if you need it)

Decoding Worksheet Name: ______________________________

Encoded Message:

(more space, if you need it)

Encoding Matrix:
(Your friend should give this to you)

Decoding Inverse:
(You need to figure this out for yourself!)

Take the numbers in your friend's secret message and, starting in the upper left corner and moving down the column and then to the next column, fill in the 3 x whatever grid with your numerical message.

Use your calculator to multiply the inverse decoding matrix times the coded message matrix to get your decoded message matrix. Write it here:

Starting in the upper left corner and moving down the column and then to the next column, take the numbers from the secret message and write them along the top row of the grid. Below them, write the letter equivalents so you can read the secret message!

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	27