4.5. The Inverse of a Square Matrix

Wednesday, February 14, 2018 12:29 PM

Goals: ① Find the inverse of a square matrix

② Application in Cryptography.

Identity Matrix.

1 → Multiplicative Identity.

What matrices play the role of 1 in matrix multiplication?

$$\begin{pmatrix}1&2\\3&4\end{pmatrix}\cdot\boxed{\begin{pmatrix}1&0\\0&1\end{pmatrix}}=\begin{pmatrix}1&2\\3&4\end{pmatrix}$$

$$\boxed{\begin{pmatrix}1&0\\0&1\end{pmatrix}}\cdot\begin{pmatrix}1&2\\3&4\end{pmatrix}=\begin{pmatrix}1&2\\3&4\end{pmatrix}$$

The matrix $\underbrace{\begin{pmatrix}1&0\\0&1\end{pmatrix}}_{I_2}$ is called the 2-by-2 identity matrix.

Wednesday, February 14, 2018 12:37 PM

$$\underbrace{\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}}_{I_3} \; ; \; \underbrace{\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}}_{I_4}$$

$$2\cdot\boxed{\frac{1}{2}} = 1 \qquad \longrightarrow \qquad 2^{-1}$$

Definition of the inverse matrix:

The inverse of a matrix A is a matrix, denoted by A^{-1} (read as A inverse) such that

$$A^{-1}\cdot A = I$$

and

$$A\cdot A^{-1} = I$$

E.g. $A = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$

Consider the matrix $B = \begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix}$

$$AB = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$BA = \begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix}\begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

B is the inverse of A. $B = A^{-1}$.

$$\boxed{A^{-1} = \begin{pmatrix} 2 & -3 \\ 1 & 2 \end{pmatrix}}$$

Wednesday, February 14, 2018 12:45 PM

Formula to find the inverse of a 2-by-2 matrix:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

The inverse of A (if exists) is given by the formula:

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

(provided that $ad-bc \neq 0$)

E.g.

$$A = \begin{pmatrix} \overset{a}{2} & \overset{b}{3} \\ \underset{c}{1} & \underset{d}{2} \end{pmatrix} ; \quad A^{-1} = \frac{1}{2 \cdot 2 - 1 \cdot 3} \begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix}$$

$$A^{-1} = \begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix}$$

E.g. $A = \begin{pmatrix} 1 & 4 \\ 3 & 5 \end{pmatrix}$. Find A^{-1}?

$$A^{-1} = \frac{1}{1\cdot5-4\cdot3}\begin{pmatrix}5 & -4 \\ -3 & 1\end{pmatrix} = \frac{1}{-7}\cdot\begin{pmatrix}5 & -4 \\ -3 & 1\end{pmatrix}$$

$$A^{-1} = \begin{pmatrix}-\frac{5}{7} & \frac{4}{7} \\ \frac{3}{7} & -\frac{1}{7}\end{pmatrix}$$

Wednesday, February 14, 2018 12:56 PM

* Ex. Use TI-Cal to find the inverse matrix of

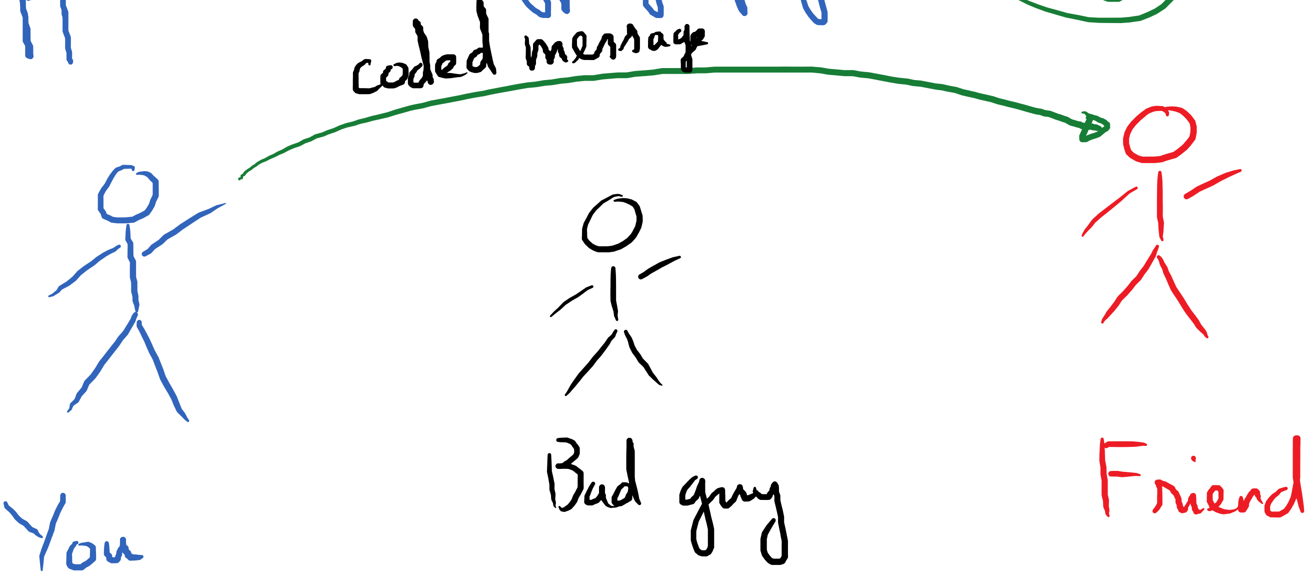
$$A = \begin{pmatrix} 1 & -1 & 3 \\ 2 & 1 & 2 \\ -2 & -2 & 1 \end{pmatrix}.$$

Check that the answer is correct

$$A^{-1} = \begin{pmatrix} 1 & -1 & -1 \\ -\frac{6}{5} & \frac{7}{5} & \frac{4}{5} \\ -\frac{2}{5} & \frac{4}{5} & \frac{3}{5} \end{pmatrix}$$

Application in Cryptography

Key → decode



"I am hungry."

A	B	C	. . . .	Z	Blank
1	2	3		26	0

$\to$ 9 0 1 13 0 8 20 14 7 18 25

$$M = \begin{pmatrix} 9 & 0 & 1 & 13 & 0 & 8 \\ 20 & 14 & 7 & 18 & 25 & 0 \end{pmatrix}$$

Key (encode)

$$E = \begin{pmatrix} 3 & 7 \\ 2 & 1 \end{pmatrix}$$

Encode message:

$$E \cdot M = \boxed{\begin{pmatrix} 167 & 98 & 52 & 165 & 175 & 24 \\ 38 & 14 & 9 & 44 & 25 & 16 \end{pmatrix}}$$

E^{-1}