• Ex: [basis for column space of a matrix]

$$A = \begin{pmatrix} 1 & 0 & 2 \\ 1 & 1 & 2 \\ 1 & 1 & 2 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$\vec{a}_1$, $\vec{a}_2$; $\vec{r}_1$, $\vec{r}_2$

↳ $R = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ (row echelon form)

↳ $\{\vec{r}_1, \vec{r}_2\}$ are l.i and form basis for col. space of R

⇒ $\{\vec{a}_1, \vec{a}_2\}$ basis for column space of A.

• Ex: [basis for row space formed by the row vectors of A (not R)]

$$A = \begin{pmatrix} 0 & 2 & 0 & 1 \\ 1 & 4 & -1 & 2 \\ 1 & 6 & -1 & 3 \\ 6 & 8 & 0 & 4 \end{pmatrix} \quad \vec{a}_1', \vec{a}_2'$$

(row space → column space)

$$A^T = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 2 & 4 & 6 & 8 \\ 0 & -1 & -1 & 6 \\ 1 & 2 & 3 & 4 \end{pmatrix} \quad \vec{a}_1, \vec{a}_2$$

Now use method from previous example

rearrange A^T →

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 1 & 0 \\ 0 & -1 & -1 & 0 \\ 2 & 4 & 6 & 8 \end{pmatrix}$$

→

$$R = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \vec{v}_1, \vec{v}_2$$

↳ $\{\vec{v}_1, \vec{v}_2\}$ basis for column space of R

↳ $\{\vec{a}_1, \vec{a}_2\}$ basis for column space of A^T

↳ $\{\vec{a}_1', \vec{a}_2'\}$ basis for row space of A.

• Ex: [Basis for space spanned by a set of vectors]

Consider $S = \{\vec{v}_1, \vec{v}_2, \vec{v}_3\}$ where

$\vec{v}_1 = (2, -2, 2)$

$\vec{v}_2 = (0, 3/2, 3)$

$\vec{v}_3 = (2, -1, 4)$

a) Find subset in S that forms basis

b) Express vectors not in the basis as a l.c. of vectors in basis.

a) $\begin{pmatrix} \vec{v}_1 & \vec{v}_2 & \vec{v}_3 \\ 2 & 0 & 2 \\ -2 & 3/2 & -1 \\ 2 & 3 & 4 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 1 \\ -2 & 3/2 & -1 \\ 2 & 3 & 4 \end{pmatrix}$

$\to \begin{pmatrix} 1 & 0 & 1 \\ 0 & 3/2 & 1 \\ 0 & 3 & 2 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 1 \\ 0 & 3/2 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ →

$$\rightarrow \quad R = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2/3 \\ 0 & 0 & 0 \end{pmatrix} \qquad \vec{r}_1 \; \vec{r}_2 \; \vec{r}_3$$

$\Rightarrow \{\vec{r}_1, \vec{r}_2\}$ basis for R

$\Rightarrow \{\vec{v}_1, \vec{v}_2\}$ subset of S which is basis

b) Express $\vec{v}_3$ as l.c. of $\{\vec{v}_1, \vec{v}_2\}$

By inspection:

$$\vec{v}_3 = 1 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \frac{2}{3} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

$$= \vec{v}_1 + \frac{2}{3}\vec{v}_2$$

$$\boxed{\vec{v}_3 = \vec{v}_1 + \frac{2}{3}\vec{v}_2}$$

Check:

$$\begin{pmatrix} 2 \\ -2 \\ 2 \end{pmatrix} + \frac{2}{3}\begin{pmatrix} 0 \\ 3/2 \\ 3 \end{pmatrix} = \begin{pmatrix} 2 \\ -2+1 \\ 2+2 \end{pmatrix} = \begin{pmatrix} 2 \\ -1 \\ 4 \end{pmatrix} \quad =$$

• Ex: [plaintext → ciphertext]

$A = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$, encipher the word TANK using A.

TANK → TA NK

$\vec{p} = \begin{pmatrix} 20 \\ 1 \end{pmatrix}$ $\vec{p} = \begin{pmatrix} 14 \\ 11 \end{pmatrix}$

$\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} 20 \\ 1 \end{pmatrix} = \begin{pmatrix} 22 \\ 3 \end{pmatrix}$

$\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} 14 \\ 11 \end{pmatrix} = \begin{pmatrix} 36 \\ 33 \end{pmatrix}$

VC

$36 = 1 \cdot 26 + 10$

$33 = 1 \cdot 26 + 7$

remainders

$\begin{pmatrix} 10 \\ 7 \end{pmatrix}$

JG

⇒ TANK → VCJG

- **Ex**: [residues]

R = remainder of $\frac{|a|}{m}$

$$r = \begin{cases} R & \text{if } a \geq 0 \\ m - R & \text{if } a < 0 \ \& \ R \neq 0 \\ 0 & \text{if } a < 0 \ \& \ R = 0 \end{cases}$$

We will deal with modulo 26 (mod 26) ($m = 26$)

- $a = 55$: $|a| = 55 = 2 \cdot 26 + 3$

$\Rightarrow R = 3$

because $a > 0 \Rightarrow r = R = 3$

- $a = -10$: $|a| = 10 = 0 \cdot 26 + 10$

$\Rightarrow R = 10$

because $a < 0$ and $R \neq 0 \Rightarrow r = m - R =$

$= 26 - 10 = 16$

- $a = -52$:

$|a| = 52 = 2 \cdot 26 + 0 \Rightarrow R = 0$

because $a < 0$ & $R = 0 \Rightarrow r = 0$

• Ex: [reciprocal] → mod 26

$1x = 1 \longrightarrow 1 \cdot 1 = 1 \pmod{26}$

Z_{26}

$3x = 1 \longrightarrow 3 \cdot 9 = 27 = 1 \pmod{26}$

$(27 - 1) = 1 \cdot 26$

$5x = 1 \longrightarrow 5 \cdot 21 = 105 = 1 \pmod{26}$

$(105 - 1) = 4 \cdot 26$

⋮

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

• Ex: [INVERTIBLE MATRIX MODULO 26]

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \rightarrow \det(A) = 3 \pmod{26}$$

COMMENT:

If, for instance,

$\det(A) = 28 = 2 \pmod{26}$

$\Rightarrow |a| = 29 = 1 \cdot 26 + 2$

$\Rightarrow R = 2$

$\Rightarrow r = R = 2$

(in this case, matrix not invertible mod 26.)

$\Rightarrow a = 3 \rightarrow \bar{a}^{-1} = 9$ ✓

$\Rightarrow$ $\det(A)$ has reciprocal mod 26 $\Rightarrow$ A is invertible modulo 26

· Ex: [DECIPHERING]

$A = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$ $\quad 9 \equiv 3^{-1} \pmod{26}$

$\hookrightarrow A^{-1} = (ad-bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \pmod{26}$

$\Rightarrow A^{-1} = 9 \begin{pmatrix} 3 & -2 \\ 0 & 1 \end{pmatrix} = \pmod{26}$

$= \begin{pmatrix} 27 & -18 \\ 0 & 9 \end{pmatrix} \equiv \begin{pmatrix} 1 & 8 \\ 0 & 9 \end{pmatrix}$

$|27| = 27 = 1 \cdot 26 + 1 \Rightarrow R = 1 \Rightarrow r = 1$

$|-18| = 18 = 0 \cdot 26 + 18 \Rightarrow R = 18$

$\hookrightarrow r = 26 - 18 = 8$

$|0| \Rightarrow r = 0, \; |9| \Rightarrow r = 9$

TANK $\xrightarrow{A}$ VCJG $\xrightarrow{A^{-1}}$ TANK

$VC \rightarrow \vec{c}_1 = \begin{pmatrix} 22 \\ 3 \end{pmatrix}$

$JG \rightarrow \vec{c}_2 = \begin{pmatrix} 10 \\ 7 \end{pmatrix}$

$$A \cdot \vec{c_1} = \begin{pmatrix} 1 & 8 \\ 0 & 9 \end{pmatrix} \begin{pmatrix} 22 \\ 3 \end{pmatrix} = \begin{pmatrix} 46 \\ 27 \end{pmatrix} =$$

$$= \begin{pmatrix} 20 \\ 1 \end{pmatrix} \pmod{26}$$

$$\Rightarrow |46| = 1 \cdot 26 + 20 \Rightarrow r = 20$$

$$|27| = 1 \cdot 26 + 0 \Rightarrow r = 1$$

$$A \cdot \vec{c_2} = \begin{pmatrix} 1 & 8 \\ 0 & 9 \end{pmatrix} \begin{pmatrix} 10 \\ 7 \end{pmatrix} = \begin{pmatrix} 66 \\ 63 \end{pmatrix} =$$

$$= \begin{pmatrix} 14 \\ 11 \end{pmatrix} \pmod{26}$$

$$\vec{p_1} = \begin{pmatrix} 20 \\ 1 \end{pmatrix}, \quad \vec{p_2} = \begin{pmatrix} 14 \\ 11 \end{pmatrix}$$

TA

NK

TANK