Inversion modulaire d'une matrice

1) $\begin{pmatrix} 3 & 2 \\ 4 & 6 \end{pmatrix}^{-1}$ mod 21 :

Rq : $\begin{vmatrix} 3 & 2 \\ 4 & 6 \end{vmatrix} = 10$, or pgcd$(10, 21) = 1$ donc 10 est inversible modulo 21.

En notant, A la matrice à inverser, on a :

$$\boxed{A^{-1} \equiv \det(A)^{-1} \, \mathrm{com}(A)^t \mod 21}$$

• Calcul de $\det(A)^{-1}$: L'algo d'Euclide étendu fournit :

k	r_k	u_k	v_k	q_k	div. euclid.
0	21		0		
1	10		1	2	$21 = 10 \times 2 + 1$
2	1		-2		

On vérifie :

$10 \times (-2) \equiv -20 \equiv 1 \mod 21$ ✓

$$\boxed{\det(A)^{-1} \equiv -2 \equiv 19 \mod 21.}$$

• Calcul de $\mathrm{com}(A)^t$:

$\det\begin{pmatrix} \cancel{3} & \cancel{2} \\ \cancel{4} & 6 \end{pmatrix}$

transposition (la i-ème ligne devient la i-ème colonne)

$\mathrm{com}(A) = \begin{pmatrix} +6 & -4 \\ -2 & +3 \end{pmatrix}$ donc $\boxed{\mathrm{com}(A)^t = \begin{pmatrix} 6 & -2 \\ -4 & 3 \end{pmatrix}}$

• <u>Conclusion</u>

$$\begin{pmatrix} 3 & 2 \\ 4 & 6 \end{pmatrix}^{-1} \equiv -2 \begin{pmatrix} 6 & -2 \\ -4 & 3 \end{pmatrix} \equiv \begin{pmatrix} -12 & 4 \\ 8 & -6 \end{pmatrix} \mod 21$$

<u>On vérifie</u> :

$$\begin{pmatrix} 3 & 2 \\ 4 & 6 \end{pmatrix} \begin{pmatrix} -12 & 4 \\ 8 & -6 \end{pmatrix} = \begin{pmatrix} -20 & 0 \\ 0 & -20 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod 21$$

2) <u>Calculer $A^{-1} \mod 35$</u> avec $A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ -1 & -4 & -1 \end{pmatrix}$

• <u>$\det(A)^{-1}$</u> :

on dévelope selon cette colonne

$$\begin{vmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ -1 & -4 & -1 \end{vmatrix} = 1 \times \begin{vmatrix} 1 & 2 \\ -4 & -1 \end{vmatrix} - 1 \times \begin{vmatrix} 2 & 3 \\ 1 & 2 \end{vmatrix} = 6$$

k	r_k	u_k	v_k	q_k	div. eucl.
0	35		0		
1	6		1	5	$35 = 6 \times 5 + 5$
2	5		-5	1	$6 = 5 \times 1 + 1$
3	1		6		

<u>On vérifie</u> :

$$6 \times 6 = 36 \equiv 1 \mod 35$$

$$\boxed{\det(A)^{-1} \equiv 6 \mod 35}$$

- $\underline{com(A)^t}$:

$$com(A) = \begin{pmatrix} +\begin{vmatrix} 1 & 2 \\ -4 & -1 \end{vmatrix} & -\begin{vmatrix} 0 & 2 \\ -1 & -1 \end{vmatrix} & +\begin{vmatrix} 0 & 1 \\ -1 & -4 \end{vmatrix} \\ -\begin{vmatrix} 2 & 3 \\ -4 & -1 \end{vmatrix} & +\begin{vmatrix} 1 & 3 \\ -1 & -1 \end{vmatrix} & -\begin{vmatrix} 1 & 2 \\ -1 & -4 \end{vmatrix} \\ +\begin{vmatrix} 2 & 3 \\ 1 & 2 \end{vmatrix} & -\begin{vmatrix} 1 & 3 \\ 0 & 2 \end{vmatrix} & +\begin{vmatrix} 1 & 2 \\ 0 & 1 \end{vmatrix} \end{pmatrix} = \begin{pmatrix} +7 & -2 & +1 \\ -10 & +2 & -(-2) \\ +1 & -2 & +1 \end{pmatrix}$$

donc $\boxed{com(A)^t = \begin{pmatrix} 7 & -10 & 1 \\ -2 & 2 & -2 \\ 1 & 2 & 1 \end{pmatrix}}$

- $\underline{\text{Conclusion}}$:

$$A^{-1} \equiv 6 \begin{pmatrix} 7 & -10 & 1 \\ -2 & 2 & -2 \\ 1 & 2 & 1 \end{pmatrix} \equiv \begin{pmatrix} 7 & 10 & 6 \\ -12 & 12 & -12 \\ 6 & 12 & 6 \end{pmatrix} \mod 35 .$$

$\underline{\underline{\text{On vérifie}}}$:

$$\begin{array}{cc} & \begin{pmatrix} 7 & 10 & 6 \\ -12 & 12 & -12 \\ 6 & 12 & 6 \end{pmatrix} \\ \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ -1 & -4 & -1 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{array} \mod 35$$