Index

Problème 5 page 98 Le système RSA

RSA : du nom des inventeurs Rivest, Shamir, Adleman en 1977

Principe : La clé publique consiste en la donnée d'un entier pq obtenu par le produit de deux nombres premiers p et q, et, d'un exposant c qui est un entier naturel premier avec l'entier $n = (p - 1)(q - 1)$.

Le chiffrement est obtenu en calculant $b \equiv a^c \pmod{pq}$ et $0 \leqslant a < pq$.

Pour déchiffrer b, on cherche l'entier d tel que $cd \equiv 1 \pmod{n}$, et, on sait que $a = b^d \pmod{pq}$.

Le déchiffrement est rendu difficile, car on ne connaît pas p et q, et on ne connaît donc pas l'entier n permettant de calculer d.

A- Un exemple

$p = 5$, $q = 19$ et $c = 61$ (La clé publique est : (95, 61)

1) le nombre $n = 4\times18 = 72$ est premier avec 61.

2) Codage de $a = 3$

$b \equiv 3^{61} \pmod{95}$ et $0 \leqslant b < 95$
***b* = 78** (Pour déterminer ce nombre à la main, on cherche les congruences modulo 95 des premières puissances ….)
$3^5 = 243$ et $243 = 2\times95 + 53$
$3^6 \equiv 53\times3\ (95)$ $159 = 95 + 64$
$3^7 \equiv 64\times3\ (95)$ $192 = 2\times95 + 2$
Comme $61 = 7\times8 + 5$, on a : $3^{61} = (3^7)^8 \times 3^5$, d'où, $3^{61} \equiv 2^8 \times53\ (95)$
$2^8 \times53 = 256\times53\ (95)$ $256 = 2\times95 + 66$
$66\times53 = 3\,498$ $3\,498 = 36\times95 + 78$
D'où, $3^{61} \equiv 78\ (95)$

3a) Résolution de l'équation diophantienne $61x - ny = 1$.
($n = 72$) L'existence de solutions est assurée par le ***théorème de Bézout***.
Algorithme d'Euclide
$72 = 1\times61 + 11$
$61 = 5\times11 + 6$
$11 = 1\times6 + 5$
$6 = 1\times5 + 1$
d 'où : $1 = 6 - 5 = (61 - 5\times11) - (11 - 1\times(61 - 5\times11)) = 2\times61 - 11\times11 = 2\times61 - 11\times(72 - 1\times61)$
$1 = 13\times61 - 11\times72$
$x = 13$ et $y = 11$ conviennent.
Théorème de Gauss
$61x - 72y = 61\times13 - 11\times72$ équivaut à $61(x - 13) = 72(y - 11)$
Comme 61 divise le produit $72(y - 11)$ et que 61 est premier avec 72 , 61 divise $y - 11$.
On a alors : $y = 11 + 61k$, $k \in \mathbb{Z}$, puis : $61(x - 13) = 72\times61k$: soit : $x = 13 + 72k$
Comme : $61(13 + 72k) - 72(11 + 61k) = 61\times13 - 72\times11 = 1$,
les solutions de l'équation $61x - 72y = 1$ sont les couples $(13 + 72k\ ;\ 11 + 61k)$ avec $k \in \mathbb{Z}$.

b) $61x - ny = 1$ mène à $61x \equiv 1 \pmod{n}$,
d'où, $61 \times 13 \equiv 1 \pmod{72}$.
Comme $0 \leqslant 13 < 72$, le nombre d permettant le décodage est 13.

c) $b = 78$ et $d = 13$,
on cherche 78^{13} modulo 95.
$78^2 = 6084$ et $6084 = 64 \times 95 + 4$
Comme $13 = 2 \times 6 + 1$, on a : $78^{13} = (78^2)^6 \times 78$
$78^{13} \equiv 4^6 \times 78 \pmod{95}$ $\quad 4^6 = 4096$ et $4096 = 43 \times 95 + 11$
$78^{13} \equiv 11 \times 78 \pmod{95}$ $\quad 11 \times 78 = 858$ et $858 = 9 \times 95 + 3$
$78^{13} \equiv 3 \pmod{95}$
On retrouve le nombre a.

B- Une justification

p et q sont ***deux nombres premiers*** et c est un entier naturel ***premier avec*** $n = (p - 1)(q - 1)$.
$a \in \mathbb{N}$ et $b \equiv a^c \pmod{pq}$.
1 a) Soit l'équation diophantienne $cx - ny = 1$.
L'existence de solutions est assurée par le ***théorème de Bézout***.
Notons $(x_0 ; y_0)$ l'une des solutions.

Théorème de Gauss
On a : $cx - ny = 1$ et $cx_0 - ny_0 = 1$
$cx - ny = cx_0 - ny_0$ équivaut à $c(x - x_0) = n(y - y_0)$
Comme c divise le produit $n(y - y_0)$ et que c est premier avec n , c divise $y - y_0$.
On a alors : $y = y_0 + ck$, $k \in \mathbb{Z}$, puis : $c(x - x_0) = n \times ck$: soit : $x = x_0 + nk$
Comme : $c(x_0 + nk) - n(y_0 + ck) = cx_0 - ny_0 = 1$,
les solutions de l'équation $cx - ny = 1$ sont les couples $(x_0 + nk ; y_0 + ck)$ avec $k \in \mathbb{Z}$.
b) On cherche parmi les solutions de la forme $x_0 + nk$ celle qui vérifie $0 \leqslant x_0 + nk < n$.
on a successivement : $-x_0 \leqslant nk < -x_0 + n$, puis : $\dfrac{-x_0}{n} \leqslant k < \dfrac{-x_0}{n} + 1$

Soit $\alpha = -\dfrac{x_0}{n}$, le seul entier k_d vérifiant $\alpha \leqslant k_d < \alpha + 1$ (intervalle de longueur 1)
permet de déterminer l'unique entier d tel que $0 \leqslant d < n$. En ce cas, $y_d = y_0 + ck_d$
Puis, comme $cd - ny_d = 1$, on a : $cd \equiv 1 \pmod{n}$.

2) **petit théorème de Fermat** :
Énoncé :
Si p est premier et a n'est pas divisible par p, alors $a^{p-1} \equiv 1 \pmod{p}$.

En prenant a non divisible par p et par q, le petit théorème de Fermat s'applique, d'où,
$a^{p-1} \equiv 1 \pmod{p}$.
En élevant à la puissance $q - 1$ les deux membres de la congruence : $(a^{p-1})^{q-1} \equiv 1^{q-1} \ (p)$
soit : $a^{(p-1)(q-1)} \equiv 1 \ (p)$
et,
$a^{q-1} \equiv 1 \pmod{q}$.
En élevant à la puissance $p - 1$ les deux membres de la congruence : $(a^{q-1})^{p-1} \equiv 1^{p-1} \ (q)$
soit : $a^{(p-1)(q-1)} \equiv 1 \ (q)$.

$a^{(p-1)(q-1)} \equiv 1 \ (p)$ implique qu'il existe un entier k tel que $a^{(p-1)(q-1)} = 1 + kp$.

$a^{(p-1)(q-1)} \equiv 1\ (q)$ implique qu'il existe un entier k' tel que $a^{(p-1)(q-1)} = 1 + k'q$.
Par différence (ou par comparaison des deux égalités), il vient : $kp = k'q$.
Comme q divise $k'p$ et que q est premier avec p, d'après le ***théorème de Gauss***, q divise k.
Il existe donc un entier k'' tel que $qk'' = k$.
On obtient : $a^{(p-1)(q-1)} = 1 + kp = 1 + k''pq$.
Conclusion : $(a^{p-1})^{q-1} \equiv 1^{q-1}\ (pq)$ Comme $n = (p-1)(q-1)$, on a : $a^n \equiv 1\ (pq)$

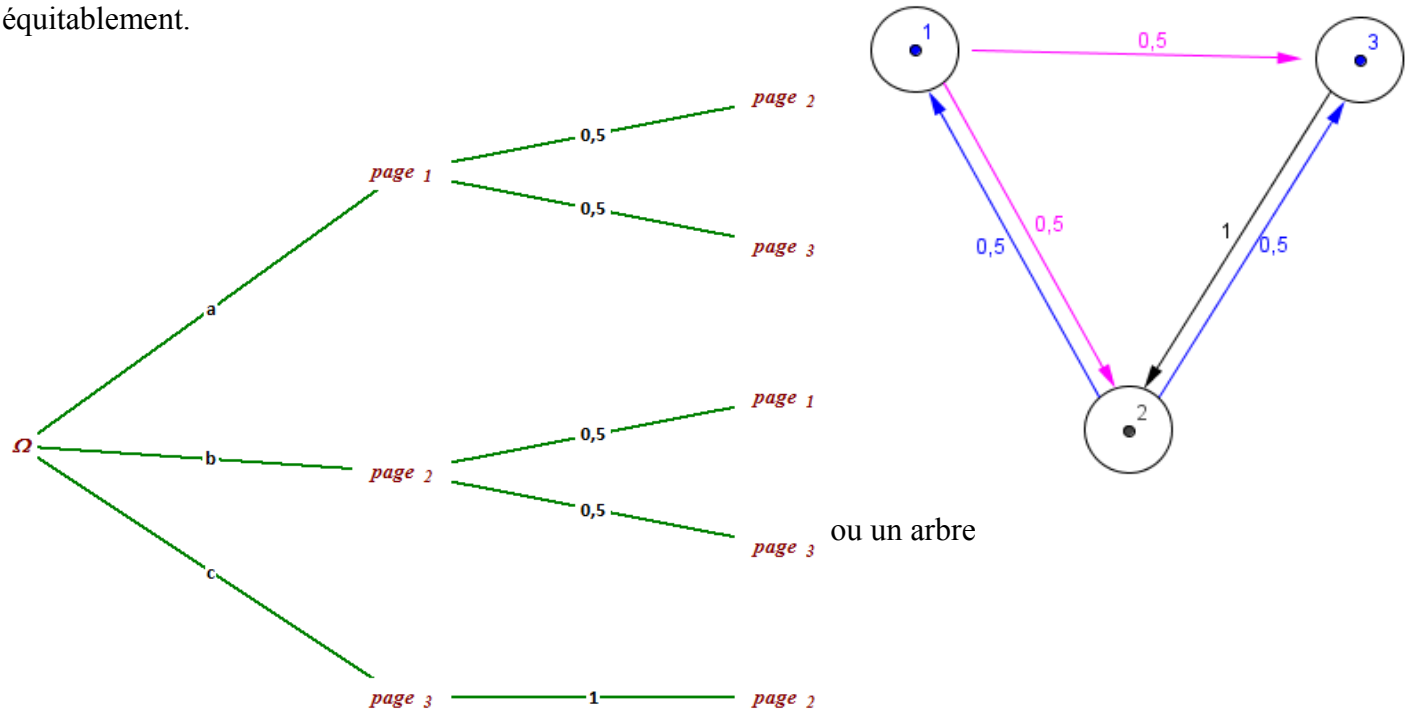
b) Soit un entier $k = 1 + mn$.
$a^k = a^{1+mn} = a \times (a^n)^m$ Or, $a^n \equiv 1\ (pq)$, d'où, par produit des congruences, $a^k \equiv a\ (pq)$.

3) On cherche $b^d \pmod{pq}$.
Par définition : $b \equiv a^c \pmod{pq}$ En élevant à la puissance d,
$b^d \equiv (a^c)^d \pmod{pq}$
$b^d \equiv a^{cd} \pmod{pq}$
D'après 1b), $cd = 1 + mn$ avec m entier.
$b^d \equiv a^{1+mn} \pmod{pq}$
D'après 2b), $a^{1+mn} \equiv a \pmod{pq}$
Par transitivité de la congruence : $b^d \equiv a \pmod{pq}$

---

objectif bac page 168 Étude asymptotique d'une marche aléatoire

Un graphe probabiliste : Étant sur une page, le lien est choisi équitablement.



ou un arbre

1) La matrice $(p_{i,j})$ où les coefficients $p_{i,j}$ désigne la probabilité, étant à la page *i,* d'aller à la page *j*. (*i* et *j* sont les entiers 1 ou 2 ou 3).

Remarque : $p_{i,j}$ est la probabilité conditionnelle qui pourrait être notée $p_i(j)$ avec les notations utilisées en probabilités dans le programme obligatoire.

$M = (p_{i,j}) = \begin{pmatrix} 0 & 0,5 & 0,5 \\ 0,5 & 0 & 0,5 \\ 0 & 1 & 0 \end{pmatrix}$.

2) P_n en fonction de M et de P_0.

X_n est la variable aléatoire donnant la page sur laquelle se trouve le surfeur au *n*-ième clic.

P_n est la matrice ligne donnant dans cet ordre : le surfeur est à la page 1, à la page 2, à la page 3 ;

$P_n = (P(X_n = 1) \quad P(X_n = 2) \quad P(X_n = 3))$

$P_0 = (a \quad b \quad c)$ avec $0 \leqslant a \leqslant 1$; $0 \leqslant b \leqslant 1$; $0 \leqslant c \leqslant 1$ et $a + b + c = 1$. État probabiliste initial.

$P_1 = P_0 M$ et $P_{n+1} = P_n M$ Par récurrence, on montre que : $P_n = P_0 M^n$.

3) Soit la matrice $P = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 1 & -4 \\ 1 & -2 & 4 \end{pmatrix}$. On admet que P est inversible et que $P^{-1} = \frac{1}{18} \begin{pmatrix} 4 & 8 & 6 \\ 8 & -2 & -6 \\ 3 & -3 & 0 \end{pmatrix}$.

a) $Q = P^{-1}MP$.

$$Q = \frac{1}{18} \begin{pmatrix} 4 & 8 & 6 \\ 8 & -2 & -6 \\ 3 & -3 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0,5 & 0,5 \\ 0,5 & 0 & 0,5 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 2 \\ 1 & 1 & -4 \\ 1 & -2 & 4 \end{pmatrix} = \frac{1}{18} \begin{pmatrix} 4 & 8 & 6 \\ -1 & -2 & 3 \\ -1,5 & 1,5 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 2 \\ 1 & 1 & -4 \\ 1 & -2 & 4 \end{pmatrix}$$

$$= \frac{1}{18} \begin{pmatrix} 18 & 0 & 0 \\ 0 & -9 & 18 \\ 0 & 0 & -9 \end{pmatrix}.$$

$$Q = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -0,5 & 1 \\ 0 & 0 & -0,5 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -0,5 & 0 \\ 0 & 0 & -0,5 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

On pose : $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -0,5 & 0 \\ 0 & 0 & -0,5 \end{pmatrix}$ et $T = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$, d'où, $Q = D + T$.

3 b) $T^2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = 0_3$.

$$DT = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -0,5 & 0 \\ 0 & 0 & -0,5 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -05 \\ 0 & 0 & 0 \end{pmatrix} = -0,5 \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} = -0,5T$$

$$TD = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -0,5 & 0 \\ 0 & 0 & -0,5 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -05 \\ 0 & 0 & 0 \end{pmatrix} = -0,5T$$

Remarquer :

Lorsqu'une ligne *i* de la matrice à gauche est nulle, la ligne *i* de la matrice produit est nulle.

Lorsqu'une colonne *j* de la matrice à droite est nulle, la colonne *j* de la matrice produit est nulle.

Montrons l'égalité : Pour tout $n \in \mathbb{N}^*$, $D^n T = (-0,5)^n T$.

Par récurrence :

Initialisation : $n = 1$. Le calcul précédent initialise la proposition.

Hérédité : Soit un entier $n \geqslant 1$ tel que $D^n T = (-0,5)^n T$.

$D^{n+1} T = D.\ D^n T = D((-0,5)^n T) = (-0,5)^n DT = (-0,5)^n (-0,5T) = (-0,5)^{n+1} T$.

Conclusion : D'après l'axiome de récurrence, pour tout $n \in \mathbb{N}^*$, $D^n T = (-0,5)^n T$.

3c) Proposition à démontrer par récurrence: Pour tout $n \in \mathbb{N}^*$, $Q^n = D^n + n(-0,5)^{n-1} T$.

Initialisation : $n = 1$.

$Q = D + T$ et $D + 1 \times (-0,5)^0 T = D + T$ L'égalité est vérifiée.

Hérédité : Soit un entier $n \geqslant 1$ tel que $Q^n = D^n + n(-0,5)^{n-1} T$.

$Q^{n+1} = Q^n Q = (D^n + n(-0,5)^{n-1} T)(D + T)$

$= D^{n+1} + n(-0,5)^{n-1} TD + D^n T + n(-0,5)^{n-1} T^2$

Or, $T^2 = 0_3$, $TD = -0,5T$ et $D^n T = (-0,5)^n T$.

On a donc : $Q^{n+1} = D^{n+1} + n(-0,5)^{n-1} (-0,5T) + (-0,5)^n T$

$= D^{n+1} + n(-0,5)^n T + (-0,5)^n T$

$= D^{n+1} + (n+1)(-0,5)^n T$.

Conclusion : D'après l'axiome de récurrence, pour tout $n \in \mathbb{N}^*$, $Q^n = D^n + n(-0,5)^{n-1} T$.

d) On sait : $Q = P^{-1} MP$.

En multipliant à gauche par P et à droite par P^{-1} , on a :

$PQ P^{-1} = P(P^{-1} MP) P^{-1}$ Par associativité :

$PQ P^{-1} = (P P^{-1})M(P P^{-1}) = M$ puisque $P P^{-1} = P P^{-1} = I_3$.

On a : $M^2 = PQ P^{-1} PQ P^{-1} = PQ^2 P^{-1}$ (et par récurrence ...)

$M^n = P Q^n P^{-1}$

3 e) **Étude de la limite en +∞ de la suite (Q^n) .**

On sait : pour tout $n \in \mathbb{N}^*$, $Q^n = D^n + n(-0,5)^{n-1} T$.

Étude de D^n ***en*** $+\infty$.

Comme $-1 < -0,5 < 1$, on sait : $\lim\limits_{n \to +\infty} (-0,5)^n = 0$

La matrice D étant une matrice diagonale, on a : $D^n = \begin{pmatrix} 1 & 0 & 0 \\ 0 & (-0,5)^n & 0 \\ 0 & 0 & (-0,5)^n \end{pmatrix}$ et quand n tend vers $+\infty$, (D^n)

tend vers la matrice $\begin{pmatrix}1&0&0\\0&0&0\\0&0&0\end{pmatrix}$.

Étude de la limite de $n(-0{,}5)^{n-1}$

$n(-0{,}5)^{n-1} = 2\ \frac{n}{2}\times(-1)^{n-1}\times\frac{1}{2^{n-1}} = (-1)^{n-1}\times 2\times\frac{n}{2^n}$

Il reste à étudier la limite de $\frac{n}{2^n}$

Comme $2^n = \mathrm{e}^{n\ln 2}$, posons $x = n\ln 2$, et, étudions la limite de $\frac{1}{\ln 2}\ \frac{x}{\mathrm{e}^x}$

D'autre part, on sait : $\lim\limits_{x\to+\infty}\frac{\mathrm{e}^x}{x} = +\infty$, d'où, $\lim\limits_{x\to+\infty}\frac{x}{\mathrm{e}^x} = 0$, (soit : $\lim\limits_{x\to+\infty} x\,\mathrm{e}^{-x} = 0$.)

La limite en $+\infty$ de $\frac{n}{2^n}$ est la limite en $+\infty$ (car $\ln 2 > 0$) de $\frac{1}{\ln 2}\ \frac{x}{\mathrm{e}^x}$, donc, $\lim\limits_{n\to+\infty}\ \frac{n}{2^n} = 0$.

Comme, pour tout $n\in\mathbb{N}^*$, $(-1)^{n-1} = -1$ ou 1, $\lim\limits_{n\to+\infty}\ (-1)^{n-1}\times 2\times\frac{n}{2^n} = 0$

la matrice Q^n a donc pour limite en $+\infty$, la matrice $\begin{pmatrix}1&0&0\\0&0&0\\0&0&0\end{pmatrix}$.

Étude de la limite en +∞ de la suite (M^n) .

Comme $\mathrm{M}^n = \mathrm{P}\,\mathrm{Q}^n\,\mathrm{P}^{-1}$, on a quand n tend vers $+\infty$, M^n tend vers $\mathrm{P}\begin{pmatrix}1&0&0\\0&0&0\\0&0&0\end{pmatrix}\mathrm{P}^{-1}$.

Calcul de : $\frac{1}{18}\begin{pmatrix}1&1&2\\1&1&-4\\1&-2&4\end{pmatrix}\begin{pmatrix}1&0&0\\0&0&0\\0&0&0\end{pmatrix}\begin{pmatrix}4&8&6\\8&-2&-6\\3&-3&0\end{pmatrix} = \frac{1}{18}\begin{pmatrix}1&0&0\\1&0&0\\1&0&0\end{pmatrix}\begin{pmatrix}4&8&6\\8&-2&-6\\3&-3&0\end{pmatrix}$

$= \frac{1}{18}\begin{pmatrix}4&8&6\\4&8&6\\4&8&6\end{pmatrix} = \begin{pmatrix}\frac{2}{9}&\frac{4}{9}&\frac{3}{9}\\\frac{2}{9}&\frac{4}{9}&\frac{3}{9}\\\frac{2}{9}&\frac{4}{9}&\frac{3}{9}\end{pmatrix}$.

On note M_∞ la matrice $\begin{pmatrix}\frac{2}{9}&\frac{4}{9}&\frac{3}{9}\\\frac{2}{9}&\frac{4}{9}&\frac{3}{9}\\\frac{2}{9}&\frac{4}{9}&\frac{3}{9}\end{pmatrix}$.

4) $\mathrm{P}_0 = (a\ \ b\ \ c)$ avec $0\leqslant a\leqslant 1$; $0\leqslant b\leqslant 1$; $0\leqslant c\leqslant 1$ et $a+b+c=1$. État probabiliste initial.

$\mathrm{P}_n = \mathrm{P}_0\,\mathrm{M}^n$ donc P_n tend vers la matrice

$$P_\infty = P_0\, M_\infty = (a \quad b \quad c)\begin{pmatrix} \frac{2}{9} & \frac{4}{9} & \frac{3}{9} \\ \frac{2}{9} & \frac{4}{9} & \frac{3}{9} \\ \frac{2}{9} & \frac{4}{9} & \frac{3}{9} \end{pmatrix} = \begin{pmatrix} \frac{2}{9}(a+b+c) & \frac{4}{9}(a+b+c) & \frac{3}{9}(a+b+c) \end{pmatrix}$$

Comme $a + b + c = 1$, la suite (P_n) converge vers $P_\infty = \begin{pmatrix} \frac{2}{9} & \frac{4}{9} & \frac{3}{9} \end{pmatrix}$.

la page 2 est celle qui est la plus probable après de nombreux clics.

---

objectif bac page 169 Étude d'une suite de matrices

$X_n = \begin{pmatrix} p_n \\ q_n \\ r_n \end{pmatrix}$ avec $X_0 = \begin{pmatrix} 12 \\ 16 \\ 10 \end{pmatrix}$ et $X_{n+1} = A\,X_n + C$ où $A = \begin{pmatrix} 0{,}5 & 0{,}25 & 0{,}25 \\ 0{,}25 & 0{,}5 & 0{,}25 \\ 0{,}25 & 0{,}25 & 0{,}5 \end{pmatrix}$ et $C = \begin{pmatrix} 0 \\ 3 \\ -3 \end{pmatrix}$.

1 a) Soit $X = \begin{pmatrix} 16 \\ 20 \\ 12 \end{pmatrix}$. $AX + C = \begin{pmatrix} 0{,}5 & 0{,}25 & 0{,}25 \\ 0{,}25 & 0{,}5 & 0{,}25 \\ 0{,}25 & 0{,}25 & 0{,}5 \end{pmatrix}\begin{pmatrix} 16 \\ 20 \\ 12 \end{pmatrix} + \begin{pmatrix} 0 \\ 3 \\ -3 \end{pmatrix} = \begin{pmatrix} 8+5+3 \\ 4+10+3 \\ 4+5+6 \end{pmatrix} + \begin{pmatrix} 0 \\ 3 \\ -3 \end{pmatrix} = \begin{pmatrix} 16 \\ 20 \\ 12 \end{pmatrix} = X$

Remarques et point-méthode :

1) recherche et existence de X

On cherche s'il existe une matrice constante X vérifiant AX + C = X.

Si cette matrice existe, elle vérifie $(I_3 - A)X = C$.

On pose $B = I_3 - A$.

Lorsque B est inversible $X = B^{-1} C$.

2) Dans l'étude des suites arithmético-géométriques, l'étude est semblable.

Soit $u_{n+1} = au_n + b$.

On résout : $ax + b = x$. si $a \neq 1$, il existe un réel $\alpha = \frac{b}{1-a}$ tel que $\alpha = a\alpha + b$.

par différence : $u_{n+1} - \alpha = a(u_n - \alpha)$, d'où, l'introduction de la suite (v_n) définie par $v_n = u_n - \alpha$.

(v_n) est une suite géométrique de raison a. *$v_n = a^n v_0$, puis : $u_n - \alpha = a^n (u_0 - \alpha)$*

$u_n = a^n (u_0 - \alpha) + \alpha$.

b) On pose $Y_n = X_n - X$.

Plusieurs méthodes pour disposer les calculs ….

On cherche Y_{n+1}, on pose donc par définition Y_{n+1}, et, on remplace X_{n+1} par $A\,X_n + C$ et X par $AX + C$.

$Y_{n+1} = X_{n+1} - X = A\,X_n + C - (AX + C) = A(X_n - X) = A\,Y_n$

ou bien on pose les deux égalités : $X_{n+1} = A\,X_n + C$ et $X = AX + C$, puis on fait la différence membre-à-

membre ,

$\begin{cases} X_{n+1} = A X_n + C \\ X = AX + C \end{cases}$ mène à $X_{n+1} - X = A\ X_n - AX = A(X_n - X) = A\ Y_n$, soit : $Y_{n+1} = A\ Y_n$

Une récurrence évidente permet alors de montrer : $Y_n = A^n\ Y_0$

Comme $Y_n = X_n - X$ et $Y_0 = X_0 - X$, il vient : $X_n - X = A^n (X_0 - X)$

Conclusion : $X_n = = A^n (X_0 - X) + X$

2 a) $4A - 2I_3 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} = B$

b) $B^2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} = 2I_3 + B.$

On pose $A^n = \alpha_n I_3 + \beta_n B$ avec $\begin{cases} \alpha_{n+1} = \frac{1}{2}\alpha_n + \frac{1}{2}\beta_n \\ \beta_{n+1} = \frac{1}{4}\alpha_n + \frac{3}{4}\beta_n \end{cases}$

initialisation :

$A^0 = I_3 = 1.I_3 + 0.B$ $\qquad \alpha_0 = 1$ et $\beta_0 = 0$

$A = \frac{1}{2} I_3 + \frac{1}{4} B$ $\qquad \alpha_1 = \frac{1}{2}$ et $\beta_1 = \frac{1}{4}$ $\qquad \alpha_1 = \frac{1}{2} \times \alpha_0 + \frac{1}{2} \times \beta_0$

$\beta_1 = \frac{1}{4} \times \alpha_0 + \frac{3}{4} \times \beta_0$

hérédité :

Soit un entier *n* tel que $A^n = \alpha_n I_3 + \beta_n B$.

$A^{n+1} = A^n A = (\alpha_n I_3 + \beta_n B)(\frac{1}{2} I_3 + \frac{1}{4} B)$

$= \frac{1}{2}\alpha_n I_3 + \frac{1}{4}\alpha_n B + \frac{1}{2}\beta_n B + \frac{1}{4}\beta_n B^2$ comme $B^2 = 2I_3 + B$,

on a : $A^{n+1} = (\frac{1}{2}\alpha_n + \frac{1}{2}\beta_n) I_3 + \frac{1}{4}\alpha_n B + \frac{1}{2}\beta_n B + \frac{1}{4}\beta_n B$

$= (\frac{1}{2}\alpha_n + \frac{1}{2}\beta_n) I_3 + (\frac{1}{4}\alpha_n + \frac{3}{4}\beta_n) B$

On obtient : $\alpha_{n+1} = \frac{1}{2}\alpha_n + \frac{1}{2}\beta_n$ et $\beta_{n+1} = \frac{1}{4}\alpha_n + \frac{3}{4}\beta_n$.

Conclusion : pour tout $n\in\mathbb{N}$, on a : $A^n = \alpha_n I_3 + \beta_n B$ avec $\begin{cases}\alpha_{n+1}=\frac{1}{2}\alpha_n+\frac{1}{2}\beta_n \\ \beta_{n+1}=\frac{1}{4}\alpha_n+\frac{3}{4}\beta_n\end{cases}$ et $\alpha_0 = 1$ et $\beta_0 = 0$.

3a) $U_n = \begin{pmatrix}\alpha_n\\ \beta_n\end{pmatrix}$ pour tout $n\in\mathbb{N}$.

a) Le système suivant se traduit par l'égalité matricielle $\begin{pmatrix}\alpha_{n+1}\\ \beta_{n+1}\end{pmatrix} = \begin{pmatrix}0,5 & 0,5\\ 0,25 & 0,75\end{pmatrix}\begin{pmatrix}\alpha_n\\ \beta_n\end{pmatrix}$.

En posant M = $\begin{pmatrix}0,5 & 0,5\\ 0,25 & 0,75\end{pmatrix}$, on a : $U_{n+1} = M\,U_n$.

Une récurrence évidente permet alors de montrer : $U_n = M^n\,U_0$ avec $U_0 = \begin{pmatrix}1\\ 0\end{pmatrix}$

b) On pose V = $\begin{pmatrix}1\\ 1\end{pmatrix}$ et W = $\begin{pmatrix}-2\\ 1\end{pmatrix}$.

MV = $\begin{pmatrix}0,5 & 0,5\\ 0,25 & 0,75\end{pmatrix}\begin{pmatrix}1\\ 1\end{pmatrix} = \begin{pmatrix}1\\ 1\end{pmatrix}$ = V et MW = $\begin{pmatrix}0,5 & 0,5\\ 0,25 & 0,75\end{pmatrix}\begin{pmatrix}-2\\ 1\end{pmatrix} = \begin{pmatrix}-0,5\\ 0,25\end{pmatrix} = \frac{1}{4}$ W.

c) d'après le 3b), les valeurs propres de la matrice M sont 1 et $\frac{1}{4}$ associées aux vecteurs V et W.

On a donc en posant P = $\begin{pmatrix}1 & -2\\ 1 & 1\end{pmatrix}$, $P^{-1} = \frac{1}{3}\begin{pmatrix}1 & 2\\ -1 & 1\end{pmatrix}$, D = $\begin{pmatrix}1 & 0\\ 0 & \frac{1}{4}\end{pmatrix}$, M = PD P^{-1}

et $M^n = P\,D^n\,P^{-1}$

3 d) Comme dét(P) = 3, $P^{-1} = \frac{1}{3}\begin{pmatrix}1 & 2\\ -1 & 1\end{pmatrix}$.

D étant une matrice diagonale, $D^n = \begin{pmatrix}1 & 0\\ 0 & 0,25^n\end{pmatrix}$.

$$M^n = \frac{1}{3}\begin{pmatrix}1 & -2\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 0,25^n\end{pmatrix}\begin{pmatrix}1 & 2\\ -1 & 1\end{pmatrix}$$

$$= \frac{1}{3}\begin{pmatrix}1 & -2\times 0,25^n\\ 1 & 0,25^n\end{pmatrix}\begin{pmatrix}1 & 2\\ -1 & 1\end{pmatrix} = \frac{1}{3}\begin{pmatrix}1+2\times 0,25^n & 2-2\times 0,25^n\\ 1-0,25^n & 2+0,25^n\end{pmatrix}$$

e) Comme $0 < 0,25 < 1$, $\lim\limits_{n\to+\infty} 0,25^n = 0$

La limite en $+\infty$ de M^n est donc la matrice $\begin{pmatrix}\frac{1}{3} & \frac{2}{3}\\ \frac{1}{3} & \frac{2}{3}\end{pmatrix}$

Or, $U_n = M^n U_0$ avec $U_0 = \begin{pmatrix}1\\0\end{pmatrix}$, d'où la matrice U_n converge vers $\begin{pmatrix}\frac{1}{3} & \frac{2}{3}\\ \frac{1}{3} & \frac{2}{3}\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}\frac{1}{3}\\ \frac{1}{3}\end{pmatrix}$.

Les deux suites (α_n) et (β_n) convergent vers $\frac{1}{3}$.

4) Comme $A^n = \alpha_n I_3 + \beta_n B$

la suite (A_n) converge vers $\frac{1}{3} I_3 + \frac{1}{3} B = \begin{pmatrix}\frac{1}{3} & 0 & 0\\ 0 & \frac{1}{3} & 0\\ 0 & 0 & \frac{1}{3}\end{pmatrix} + \frac{1}{3}\begin{pmatrix}0 & 1 & 1\\ 1 & 0 & 1\\ 1 & 1 & 0\end{pmatrix} = \begin{pmatrix}\frac{1}{3} & \frac{1}{3} & \frac{1}{3}\\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3}\\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3}\end{pmatrix}$

Comme $X_n == A^n (X_0 - X) + X$, avec $X_0 = \begin{pmatrix}12\\16\\10\end{pmatrix}$, $X = \begin{pmatrix}16\\20\\12\end{pmatrix}$, donc, $X_0 - X = \begin{pmatrix}-4\\-4\\-2\end{pmatrix}$

la suite (X_n) converge vers $\begin{pmatrix}\frac{1}{3} & \frac{1}{3} & \frac{1}{3}\\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3}\\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3}\end{pmatrix}\begin{pmatrix}-4\\-4\\-2\end{pmatrix} + \begin{pmatrix}16\\20\\12\end{pmatrix} = \begin{pmatrix}\frac{-10}{3}\\ \frac{-10}{3}\\ \frac{-10}{3}\end{pmatrix} + \begin{pmatrix}16\\20\\12\end{pmatrix}$

$$= \begin{pmatrix}\frac{38}{3}\\ \frac{50}{3}\\ \frac{26}{3}\end{pmatrix}.$$

Les suites (p_n), (q_n) et (r_n) convergent respectivement vers $\frac{38}{3}$, $\frac{50}{3}$ et $\frac{26}{3}$.