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

TP1 page 170 le modèle des urnes d'Ehrenfest

Le monde est-il irréversible ?

On fait les hypothèses suivantes :

* $n = 0$ Toutes les particules sont dans le même compartiment.
* À une date n, une et une seule particule change de compartiment.
* La probabilité qu'une particule donnée change de compartiment est la même en tout temps.

Le modèle mathématique :
On dispose de deux urnes A et B.

Les particules sont représentées par N boules numérotées de 1 à N.

Les tirages d'une boule sont équiprobables.

On tire une boule numérotée i et on la change d'urne.

A – Simulation (Voir exercice 49 page 184)

B – Étude du cas où N = 4

X_n est la variable aléatoire égale au nombre de particules dans A après le transfert numéro n.

$X_0 = 4$

1 a) X_n peut prendre l'une des cinq valeurs entières de 0 à 4 inclus.

b) **Un arbre.**

La probabilité de tirer un numéro entre 1 et 4 est $\frac{1}{4}$.

Si la boule est dans A, le nombre de boules dans A diminue de 1 et celui de B augmente de 1.

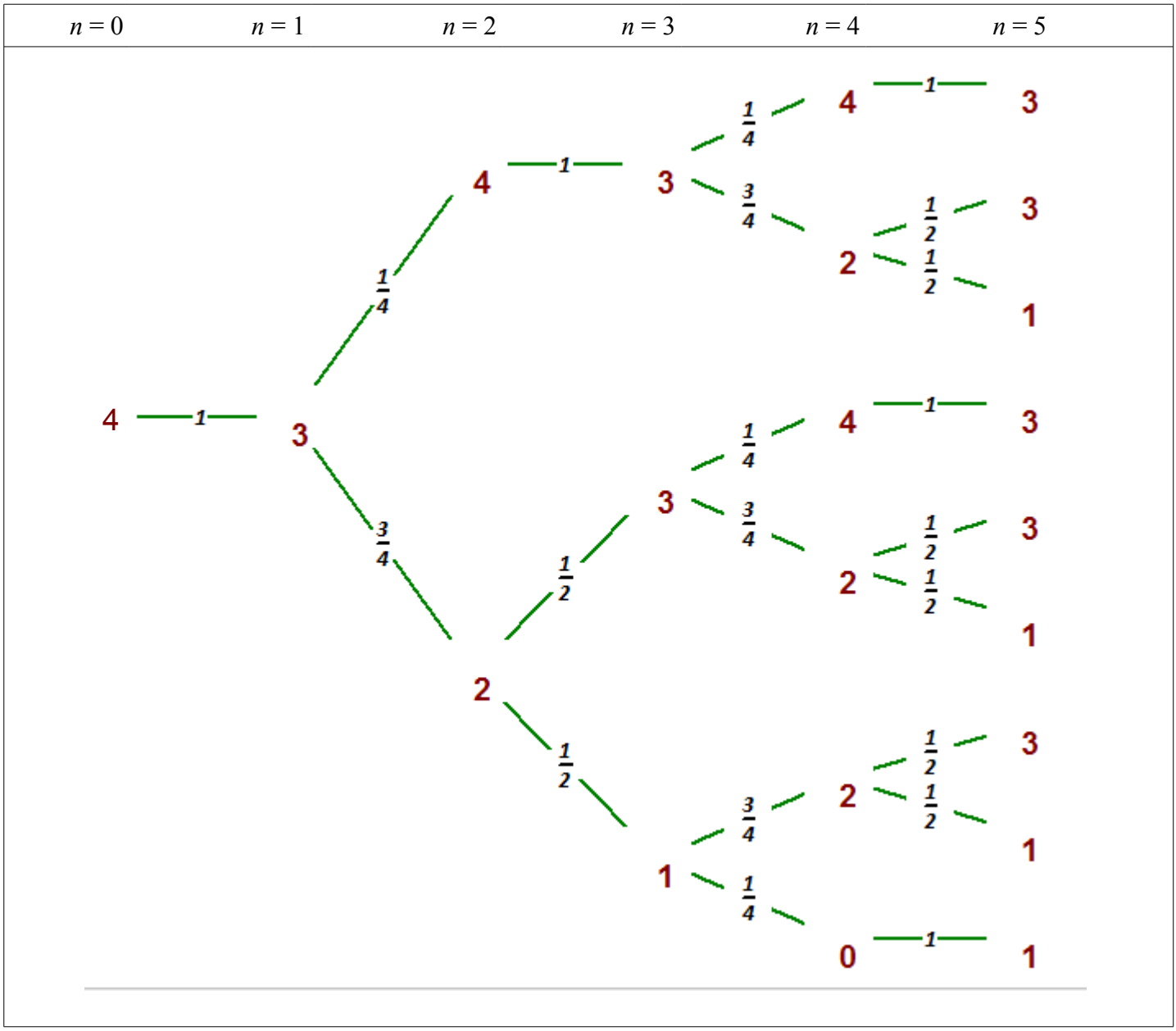
Si la boule est dans B, le nombre de boules dans A augmente de 1 et celui de B diminue de 1.

Au premier tirage, toutes les boules sont dans A.

On tire une boule qui est mise dans B. Le nombre de boules dans A est 3 (et B contient une boule).

Quand A contient k boules ($k \geqslant 1$) (et B contient $4 - k$ boules), la probabilité de tirer une boule de A est $\frac{k}{4}$ et en ce cas, le nombre de boules de A est $k - 1$.

Si $k = 0$, la probabilité d'avoir 1 boule de B mise dans A est 1.



c) Soit $0 \leqslant k \leqslant 3$.

À l'étape n, l'urne A contient k boules, et, à l'étape n + 1, l'urne A contient k +1 boules.
$P_{(X_n=k)}(X_{n+1}=k+1)$ est la probabilité de tirer une boule de B et de la mettre dans A sachant que A contient k boules.

Le nombre de boules dans B est $4-k$, d'où $P_{(X_n=k)}(X_{n+1}=k+1) = \frac{4-k}{4}$.

À l'étape n, l'urne A contient k +1 boules, et, à l'étape n + 1, l'urne A contient k boules.
$P_{(X_n=k+1)}(X_{n+1}=k)$ est la probabilité de tirer une boule de A et de la mettre dans B sachant que A contient $k+1$ boules.

Le nombre de boules dans A est $k+1$, d'où $P_{(X_n=k+1)}(X_{n+1}=k) = \frac{k+1}{4}$.

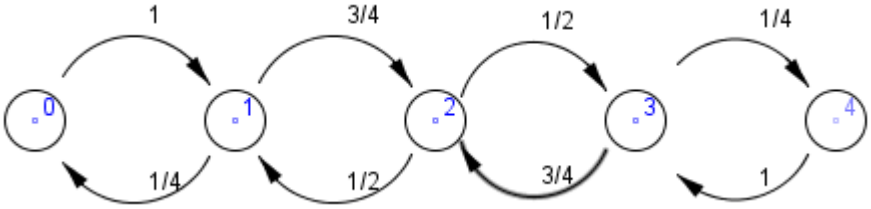
Ces probabilités sont indépendantes du n° n du tirage.

À l'étape n + 1, l'urne A contient k boules, et, à l'étape précédente n, l'urne A contient k + 1 boules.

$$P_{(X_{n+1}=k)}(X_n=k+1) = \frac{P((X_n=k+1)\cap(X_{n+1}=k))}{P(X_{n+1}=k)} = \frac{P_{(X_n=k+1)}(X_{n+1}=k)\times P(X_n=k)}{P(X_{n+1}=k+1)}$$

$$= \frac{k+1}{4}\times\frac{P(X_n=k+1)}{P(X_{n+1}=k)}$$ cette probabilité dépend de n.

2 a) un diagramme



Lorsque A contient k boules à la date n, alors, à la date $n+1$, A contient $k+1$ boules avec la probabilité $\frac{4-k}{4}$ et contient $k-1$ boules avec la probabilité $\frac{k}{4}$.

b) La matrice de transition $T = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ \frac{1}{4} & 0 & \frac{3}{4} & 0 & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & 0 & \frac{3}{4} & 0 & \frac{1}{4} \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$.

3) a) La matrice ligne L_n représente l'état probabiliste de l'urne A après le transfert n° n.

$L_0 = (0\ 0\ 0\ 0\ 1)$ $\quad P(X_0=4) = 1$ (Seule possibilité)

$L_1 = (0\ 0\ 0\ 1\ 0)$ $\quad P(X_1=3) = 1$ (Seule possibilité)

$L_2 = (0\ \ 0\ \ \frac{3}{4}\ \ 0\ \ \frac{1}{4})$ $P(X_2=4) = P(X_1=3)\times\frac{1}{4}$ L'urne A contient 4 boules, lorsqu'on a tiré la boule de B, et $P(X_2=2) = P_{(X_1=3)}\times\frac{3}{4}$ L'urne A contient 2 boules, lorsqu'on a tiré une des trois boules de A.

$L_3 = (0\ \ \frac{3}{8}\ \ 0\ \ \frac{5}{8}\ \ 0)$ $P(X_3=1) = P(X_2=2)\times\frac{1}{2}$ et $P(X_3=3) = P(X_2=2)\times\frac{1}{2} + P(X_2=4)\times 1$

b)

$L_n = L_0 T^n$ pour $n \geqslant 1$.

Démonstration évidente par récurrence.

Il semble que la position des 0 dépendent de la parité de n. (La preuve sera apportée au e/)

c) $A = T^2 = \begin{pmatrix} \frac{1}{4} & 0 & \frac{3}{4} & 0 & 0 \\ 0 & \frac{5}{8} & 0 & \frac{3}{8} & 0 \\ \frac{1}{8} & 0 & \frac{3}{4} & 0 & \frac{1}{8} \\ 0 & \frac{3}{8} & 0 & \frac{5}{8} & 0 \\ 0 & 0 & \frac{3}{4} & 0 & \frac{1}{4} \end{pmatrix}$

d) $L_{n+2} = L_n T^2 = L_n A$.

Soit $n \geqslant 4$.

premier cas : ***n* pair** (On peut poser $n = 2p$)

$L_0 = (0\ \ 0\ \ 0\ \ 0\ \ 1)$

$L_2 = (0\ \ 0\ \ \frac{3}{4}\ \ 0\ \ \frac{1}{4})$

Propriété à montrer : pour tout $n \geqslant 4$ et $n = 2p$, $b_{2p} = d_{2p} = 0$

Initialisation :

$n = 4$

$L_4 = L_2 A = (\frac{3}{32}\ \ 0\ \ \frac{3}{4}\ \ 0\ \ \frac{5}{32})$ On a bien : $b_4 = d_4 = 0$

Hérédité :

Soit un indice $p \geqslant 2$ tel que $b_{2p} = d_{2p} = 0$

$L_{2p} = (a_{2p}\ \ 0\ \ c_{2p}\ \ 0\ \ e_{2p})$

On a alors $L_{2(p+1)} = L_{2p+2} = L_{2p} A = (\frac{1}{4} a_{2p} + \frac{1}{8} c_{2p}\ \ 0\ \ \frac{3}{4}(a_{2p} + c_{2p} + e_{2p}\ \ 0\ \ \frac{1}{8} c_{2p} + \frac{1}{4} e_{2p})$

La propriété est vraie au rang $p + 1 = n + 2$

Conclusion :

pour tout $n \geqslant 4$ et $n = 2p$, $b_{2p} = d_{2p} = 0$

Interprétation : au bout d'un nombre pair d'étapes, on ne peut pas avoir 1 ou 3 boules dans A.

On a : 0 ou 2 ou 4 boules.

deuxième cas : ***n* impair** (On peut poser $n = 2p + 1$)

$L_1 = (0 \ 0 \ 0 \ 1 \ 0)$

$L_3 = (0 \ \frac{3}{8} \ 0 \ \frac{5}{8} \ 0)$

Propriété à montrer : pour tout $n \geqslant 4$ et $n = 2p + 1$, $a_{2p+1} = c_{2p+1} = e_{2p+1} = 0$

Initialisation :

$n = 5$

$L_5 = L_3 A = (0 \ \frac{15}{32} \ 0 \ \frac{17}{32} \ 0)$ On a bien : $a_5 = c_5 = e_5 = 0$

Hérédité :

Soit un indice $p \geqslant 2$ tel que $a_{2p+1} = c_{2p+1} = e_{2p+1} = 0$

$L_{2p+1} = (0 \ b_{2p+1} \ 0 \ d_{2p+1} \ 0)$

On a alors $L_{2(p+1)+1} = L_{2p+1+2} = L_{2p+1} A = (0 \ \frac{5}{8} b_{2p+1} + \frac{3}{8} d_{2p+1} \ 0 \ \frac{3}{8} b_{2p+1} + \frac{5}{8} d_{2p+1} \ 0)$

La propriété est vraie au rang $p + 1 = n + 2$

Conclusion :

pour tout $n \geqslant 5$ et $n = 2p + 1$, $a_{2p+1} = c_{2p+1} = e_{2p+1} = 0$

Interprétation : au bout d'un nombre impair d'étapes, on ne peut pas avoir 0 ou 2 ou 4 boules dans A.

On a : 1 ou 3 boules.

Recherche d'une limite éventuelle :

Supposons que la suite (L_n) ait une limite L.

L'unicité de la limite implique : $\lim_{p \to +\infty} L_{2p} = \lim_{p \to +\infty} L_{2p+1} = L$

On a donc : L = (0 0 0 0 0). Comme L est un état probabiliste, la somme des coefficients est égale à 1.

Il y a contradiction.

La suite (L_n) ne possède pas de limite.

Interprétation physique :

A chaque étape, le nombre de boules dans A augmente ou diminue de 1.

Ce nombre change donc de parité.

Si à une étape n, A possède un nombre pair (resp. impair) de boules alors à l'étape $n + 1$, A possède un nombre impair (resp. pair) de boules et à l'étape $n + 2$, A possède un nombre pair (resp. impair) de boules

4) **Utilisation de Xcas (voir livre pages 9-10)**

La matrice T

T:=[[0,1,0,0,0],[1/4,0,3/4,0,0],[0,1/2,0,1/2,0],[0,0,3/4,0,1/4],[0,0,0,1,0]]

Diagonalisation de T :

P,D:=jordan(T) (On obtient la matrice P et la matrice diagonale D telle que $T = PD\,P^{-1}$

La matrice P

P:=egv(T) (matrice des vecteurs propres)

La matrice D

D:=egvl(T) (matrice diagonale des valeurs propres)

Puissance entière d'une matrice

assume(n,integer) (n est un entier naturel)

Tn:=matpow(T,n) afficher(matpow(T,n))

La matrice L_0 *:*

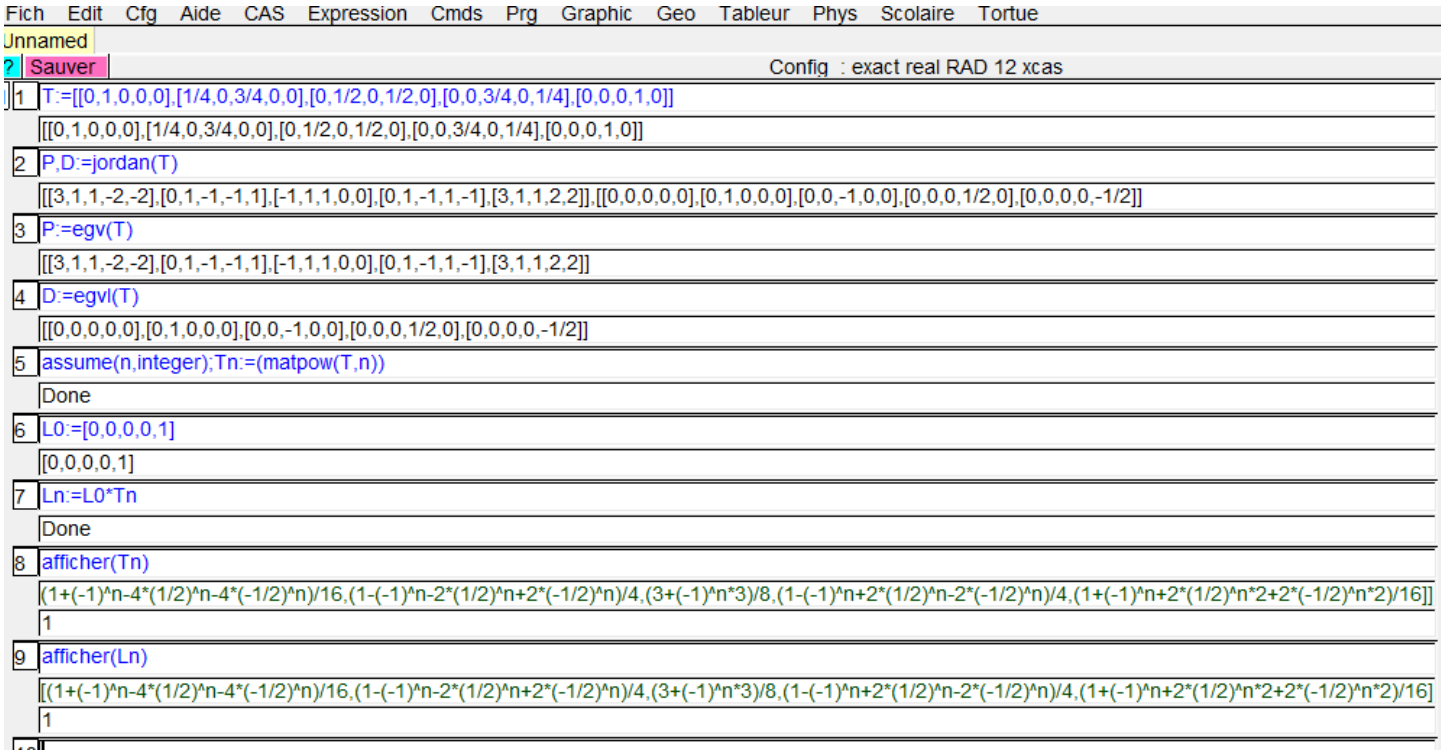
L0:=[0,0,0,0,1]

la matrice Ln

Ln:=L0*Tn

$[1/16-(1/4)(-1/2)^n+(-1/4)(1/2)^n+(-1^n)/16,1/4-(1/2)(1/2)^n+(1/2)(-1/2)^n+(-1)^n/(-4),$

$(-1)^n*3/8+3/8,1/4+(1/2)(1/2)^n-(1/2)(-1/2)^n+(-1)^n/(-4),1/16+(1/4)(1/2)^n+(1/4)(-1/2)^n+(-1)^n/16]$



a) **Si *n* est pair**, $(-1)^n = 1$ et $\left(\frac{-1}{2}\right)^n = \frac{1}{2^n}$.

$L_n = [\frac{1}{16} - \frac{1}{4}\times\frac{1}{2^n} - \frac{1}{4}\times\frac{1}{2^n} + \frac{1}{16} \quad \frac{1}{4} - \frac{1}{2}\times\frac{1}{2^n} + \frac{1}{2}\times\frac{1}{2^n} - \frac{1}{4} \quad \frac{3}{8} + \frac{3}{8} \quad \frac{1}{4} + \frac{1}{2}\times\frac{1}{2^n} - \frac{1}{2}\times\frac{1}{2^n} - \frac{1}{4} \quad \frac{1}{16} + \frac{1}{4}\times\frac{1}{2^n} + \frac{1}{4}\times\frac{1}{2^n} + \frac{1}{16}]$

$L_n = [\frac{1}{8} - \frac{1}{2^{n+1}} \quad 0 \quad \frac{3}{4} \quad 0 \quad \frac{1}{8} + \frac{1}{2^{n+1}}]$

Si *n* est impair, $(-1)^n = -1$ et $\left(\frac{-1}{2}\right)^n = -\frac{1}{2^n}$.

$L_n = [\frac{1}{16} + \frac{1}{4}\times\frac{1}{2^n} - \frac{1}{4}\times\frac{1}{2^n} - \frac{1}{16} \quad \frac{1}{4} - \frac{1}{2}\times\frac{1}{2^n} - \frac{1}{2}\times\frac{1}{2^n} + \frac{1}{4} \quad \frac{-3}{8} + \frac{3}{8} \quad \frac{1}{4} + \frac{1}{2}\times\frac{1}{2^n} + \frac{1}{2}\times\frac{1}{2^n} + \frac{1}{4} \quad \frac{1}{16} + \frac{1}{4}\times\frac{1}{2^n} - \frac{1}{4}\times\frac{1}{2^n} - \frac{1}{16}]$

$L_n = [0 \quad \frac{1}{2} - \frac{1}{2^n} \quad 0 \quad \frac{1}{2} + \frac{1}{2^n} \quad 0]$

b) Comme $0 < \frac{1}{2} < 1$, on a : $\lim\limits_{n\to+\infty} \left(\frac{1}{2}\right)^{n+1} = 0$

Si *n* est pair, $\lim\limits_{n\to+\infty} L_n = [\frac{1}{8} \quad 0 \quad \frac{3}{4} \quad 0 \quad \frac{1}{8}]$ (ou encore $\lim\limits_{p\to+\infty} L_{2p} = [\frac{1}{8} \quad 0 \quad \frac{3}{4} \quad 0 \quad \frac{1}{8}]$)

Si *n* est impair, $\lim\limits_{n\to+\infty} L_n = [0 \quad \frac{1}{2} \quad 0 \quad \frac{1}{2} \quad 0]$ (ou encore : $\lim\limits_{p\to+\infty} L_{2p+1} = [0 \quad \frac{1}{2} \quad 0 \quad \frac{1}{2} \quad 0]$)

c) Calcul de l'espérance $E(X_n)$.

Si *n* est pair, $E(X_n) = 0\times(\frac{1}{8} - \frac{1}{2^{n+1}}) + 1\times0 + 2\times\frac{3}{4} + 3\times0 + 4\times(\frac{1}{8} + \frac{1}{2^{n+1}}) = 2 + \frac{1}{2^{n-1}}$.

Si *n* est impair, $E(X_n) = 0\times0 + 1\times(\frac{1}{2} - \frac{1}{2^n}) + 2\times0 + 3\times(\frac{1}{2} + \frac{1}{2^n} + 4\times0 = 2 + \frac{1}{2^{n-1}}$.

Interprétation : $E(X_n)$ est la moyenne du nombre de boules dans l'urne A

Cette moyenne tend vers 2 puisque $\frac{1}{2^{n-1}}$ tend vers 0 quand *n* tend vers $+\infty$.

5) retour à l'état initial .

a) b) On a calculé $L_2 = (0 \ 0 \ \frac{3}{4} \ 0 \ \frac{1}{4})$ $\qquad P(X_2=4) = \frac{1}{4}$.

Le retour à l'état initial en deux transferts est possible avec la probabilité $\frac{1}{4}$.

$L_4 = (\frac{3}{32} \quad 0 \quad \frac{3}{4} \quad 0 \quad \frac{5}{32})$ $\qquad P(X_4=4) = \frac{5}{32}$.

Le retour à l'état initial en quatre transferts est possible avec la probabilité $\frac{5}{32}$.

C – Cas général.

N > 2 est un entier quelconque et à $n = 0$ l'urne B est vide.

Les notations dans la partie C sont celles de la partie B en remplaçant 4 par N pour le nombres de boules.

1 a) la matrice T = (t_{ij}) où les coefficients t_{ij} sont les probabilités conditionnelles $P_{(X_n=i)}(X_{n+1}=j)$.

i et *j* sont deux entiers compris entre 0 et N inclus (N + 1 entiers entre 0 et N inclus)
T est une matrice carrée de format (N + 1)×(N + 1).

b) Soit un entier *i*.

À l'étape *n*, l'urne A contient *i* boules, l'urne B contient N – *i* boules.
L'état de l'urne A est modifié de plus ou moins une boule à l'étape *n* + 1.

Si on tire une boule de A, l'urne A contient *i* – 1 boule à l'étape *n* + 1, d'où, $P_{(X_n=i)}(X_{n+1}=i-1) = \frac{i}{N}$.

On a donc $t_{i,i-1} = \frac{i}{N}$

Si on tire une boule de B, l'urne A contient *i* + 1 boule à l'étape *n* + 1, d'où, $P_{(X_n=i)}(X_{n+1}=i+1) = \frac{N-i}{N}$.

On a donc $t_{i,i+1} = \frac{N-i}{N}$

Si $|j-i| > 1$ où si $i=j$, alors $P_{(X_n=i)}(X_{n+1}=i) = P_{(X_n=i)}(X_{n+1}=j) = 0$.
Tous les termes de la diagonale sont nuls : $t_{i,i} = 0$.
Si $j > i+1$ ou $j < i-1$, $t_{ij} = 0$.
Les termes t_{ij} sont indépendants de *n*.

$$T = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & \dots & \dots & 0 & 0 & 0 & 0 \\ \frac{1}{N} & 0 & \frac{N-1}{N} & 0 & \dots & \dots & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{2}{N} & 0 & \frac{N-2}{N} & 0 & \dots & \dots & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & \dots & \dots & 0 & \frac{N-2}{N} & 0 & \frac{2}{N} & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & \dots & \dots & 0 & \frac{N-1}{N} & 0 & \frac{1}{N} \\ 0 & 0 & 0 & 0 & \dots & \dots & \dots & 0 & 0 & 1 & 0 \end{pmatrix}$$

2) On admet que $E(X_n) = \frac{N}{2} + \left(1-\frac{2}{N}\right)^n \left(E(X_0)-\frac{N}{2}\right)$.

Si N > 2, alors $0 < 1 - \frac{2}{N} < 1$, d'où, $\left(1-\frac{2}{N}\right)^n$ tend vers 0 quand *n* tend vers $+\infty$.

La limite en $+\infty$ de $E(X_n)$ est $\frac{N}{2}$.

Le nombre de boules dans l'urne A tend vers $\frac{N}{2}$.

Avec le temps passe, le nombre de boules dans chaque urne est à peu près égal.

3) On admet que le temps moyen pour retrouver l'état initial est 2^N.

Si N est le nombre d'Avogadro ($N = 6{,}02\times 10^{23}$), le nombre 2^N est « inimaginable »

$2^6 = 64$, donc, $2^N > 64^{10^{23}}$

Le nombre $10^{10^{23}}$ est un nombre qui s'écrit avec 1 suivi de 10^{23} zéros ….

En supposant la terre avec 15 milliards d'année, soit : $15\times 10^9 \times 365\times 24\times 3600$ secondes

qu'on peut arrondir à 5×10^{16} secondes, on est encore très, très, …, très loin de $10^{10^{23}}$

et même en supposant un changement d'urne toutes les nanosecondes ou picosecondes …. ….