Exemple de corrigé du CAPES de mathématiques

épreuve 2, session 2015

Nathalie DAVAL
ESPE-IREM Réunion

Problème 1

Partie A

I. On considère deux entiers relatifs a et b non nuls.

1. On suppose qu'il existe des entiers relatifs u et v tels que $au + bv = 1$.
Soit d un diviseur de a et de b, alors d divise n'importe quelle combinaison linéaire de a et b, en particulier d divise $au + bv$, donc d divise 1. On obtient $d = 1$ ou $d = -1$.
Les seuls diviseurs communs à a et à b sont 1 et -1, donc :

S'il existe des entiers relatifs u et v tels que $au + bv = 1$, alors a et b sont premiers entre eux.

2. On suppose cette fois que a et b sont premiers entre eux et on considère l'ensemble $\mathcal{E}$ suivant :

$$\mathscr{E} = \{z \in \mathbb{Z},\ z = au + bv,\ (u, v) \in \mathbb{Z}^2\}$$

a. L'ensemble $\mathscr{E} \cap \mathbb{N}^*$ est une partie non vide (il contient a si a est positif ou $-a$ si a est négatif) de $\mathbb{N}^*$, donc il admet un minimum n_0.

L'ensemble $\mathscr{E} \cap \mathbb{N}^*$ admet un plus petit élément n_0.

b. D'après la question **A.I.2.a.**, $\exists (u_0, v_0) \in \mathbb{Z}^2,\ n_0 = au_0 + bv_0$.
Soit $(q, r) \in \mathbb{Z}^2$ respectivement le quotient et le reste de la division euclidienne de a par n_0, on a : $a = n_0 q + r$ avec $0 \leqslant r < n_0$. d'où :

$$\begin{aligned} r &= a - n_0 q \\ &= a - (au_0 + bv_0)q \\ r &= a(1 - u_0 q) + b(-v_0 q) \end{aligned}$$

Donc, r est un élément de l'ensemble $\mathscr{E} \cap \mathbb{N}$ inférieur à n_0 ce qui n'est pas possible s'il n'est pas nul en vertu du statut de n_0 comme le plus petit élément de $\mathscr{E} \cap \mathbb{N}^*$. On en déduit alors que $r = 0$.
Un raisonnement analogue pour b nous donne également un reste nul.

Le reste de la division euclidienne de a (respectivement de b) par n_0 vaut 0.

c. D'après la question **A.I.2.b.**, n_0 divise à la fois a et b. Or, a et b sont premiers entre eux, ce qui signifie que $n_0 = \pm 1$.
Soit $au_0 + bv_0 = 1$ ou $au_0 + bv_0 = -1 \iff a(-u_0) + b(-v_0) = 1$.

Si a et b premiers entre eux, alors : $\exists (u, v) \in \mathbb{Z}^2,\ au + bv = 1$.

3. Il s'agit du théorème de Bézout :

Soient a et b deux entiers relatifs non nuls. a et b sont premiers entre eux si, et seulement si, il existe deux entiers relatifs u et v tels que $au + bv = 1$.

II. On considère trois entiers relatifs non nuls a, b et c. Si a divise bc, alors : $\exists\, k \in \mathbb{Z}^*$, $ak = bc$; de plus, si a et b sont premiers entre eux, d'après la question **A.I.3**, $\exists\,(u, v) \in \mathbb{Z}^2$, $au + bv = 1$,

soit : $acu + bcv = c$

$acu + akv = c$ car $bc = ak$

$a(cu + kv) = c$

a divise c

On obtient le théorème de Gauss :

Soit a, b et c trois entiers relatifs non nuls, si a divise bc et si a et b sont premiers entre eux, alors a divise c.

III. 1. a. On a respectivement :

lettre claire	rang x	$58x$	division euclidienne	reste y
G	$x = 6$	348	$348 = 369 \times 0 + 348$	$y = 348$
A	$x = 0$	0	$0 = 369 \times 0 + 0$	$y = 0$
U	$x = 20$	1160	$1160 = 369 \times 3 + 53$	$y = 53$
S	$x = 18$	1044	$1044 = 369 \times 2 + 306$	$y = 306$

Le codage de GAUSS donne 348 ; 0 ; 53 ; 306 ; 306.

b.
- Dans la ligne 1, on indique les 26 lettres de l'alphabet.
- Dans la ligne 2, on indique le rang x.
  Pour cela, on pourra expliquer la fonction CODE(caractère) qui renvoie le code ANSI d'un caractère. Celui-ci étant compris entre 65 (pour A) et 90 (pour Z), pour obtenir le rang des lettres, il faudra donc entrer dans la cellule B2 la formule : =CODE(B1)-65 puis la recopier vers la droite.
- Dans la ligne 3, on introduira la formule MOD(n ; p) qui renvoie le reste de la division euclidienne de n par p. Il faudra donc entrer dans la cellule B3 la formule : =MOD(58*B2 ; 369) puis la recopier vers la droite.
- Il suffira ensuite de repérer dans la ligne 3 le nombre codé puis de lire dans la même colonne et sur la ligne 1 la lettre recherchée.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA
1	Lettre claire	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	Rang x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
3	Reste y	0	58	116	174	232	290	348	37	95	153	211	269	327	16	74	132	190	248	306	364	53	111	169	227	285	343

2. a. n et e sont premiers entre eux et ce sont des entiers naturels non nuls ;
d'après le **théorème de Bézout**, il existe deux entiers relatifs u et v tels que $ue + vn = 1$, soit, modulo n : $ue \equiv 1\,(\text{mod } n)$. Il suffit de prendre pour f, par exemple, le reste de la division euclidienne de u par n pour obtenir un entier naturel.

Pour tout couple donné (n, e), il existe un entier naturel f tel que $fe \equiv 1\,(mod\ n)$.

b. Si x est la lettre à coder, y est le reste de la division euclidienne de ex par n, donc :

$$\begin{aligned}\exists q \in \mathbb{N},\ ex = nq + y &\Longrightarrow fex = fnq + fy \\ &\Longrightarrow x \equiv fy \,(\text{mod } n) \qquad \text{d'après la question } \textbf{A.III.2.a}.\end{aligned}$$

La connaissance de f permet de retrouver x à partir de y.

3. a. On a $a \geqslant 3, b \geqslant 3, c \geqslant 3$ et $d \geqslant 3$. donc :
   - $M = ab - 1 \geqslant 3 \times 3 - 1 = 8$;
   - $e = cM + a \geqslant 3 \times 8 + 3 = 27$;
   - $f = dM + b \geqslant 3 \times 8 + 3 = 27$;
   - $n = \dfrac{ef-1}{M} = \dfrac{(cM+a)(dM+b)-1}{M}$
     $= \dfrac{cdM^2 + cMb + adM + ab - 1}{M}$
     $= cdM + cb + ad + 1 \qquad \text{car } ab - 1 = M$
     $\geqslant 3 \times 3 \times 8 + 3 \times 3 + 3 \times 3 + 1$
     $n \geqslant 91.$ Donc, n est un entier supérieur à 26.

   De plus :

$$\begin{aligned}n = \frac{ef-1}{M} &\Longleftrightarrow nM = ef - 1 \\ &\Longleftrightarrow e(f) + n(-M) = 1\end{aligned}$$

   D'après le théorème de Bézout, les entiers n et e sont premiers entre eux.

   Enfin, on a $e(f) + n(-M) = 1$, donc $fe \equiv 1 \,(\text{mod } n)$, et f est une clé de décodage associée.

Le couple d'entiers (n, e) est une clé de codage dont f est une clé de décodage associé.

b. Pour $a = 3, b = 4, c = 5$ et $d = 6$, on a :
   - $M = 3 \times 4 - 1 = 11$;
   - $e = 5 \times 11 + 3 = 58$;
   - $f = 6 \times 11 + 4 = 70$;
   - $n = \dfrac{58 \times 70 - 1}{11} = 369.$

Avec $a = 3, b = 4, c = 5$ et $d = 6$, la clé de codage est $(n, e) = (369, 58)$ et une clé de décodage est $f = 70$.

c. D'après la question **A.III.2.b.**, on a $x \equiv fy \,(\text{mod } n)$:

y	fy	rang x	lettre claire
290	20 300	5	F
232	16 240	4	E
248	17 360	17	R
327	22 890	12	M
0	0	0	A
364	25 480	19	T

4. a. r_N est le dernier reste non nul dans l'algorithme d'Euclide, il s'agit du PGCD de n et e. Or, n et e sont premiers entre eux, leur PGCD vaut 1.

$r_N = 1$.

b. Soit $(\mathcal{H}_k)$ l'hypothèse : il existe des entiers relatifs u_k et v_k tels que $r_k = nu_k + ev_k$.

- **Initialisation :** $r_0 = n = n \times 1 + e \times 0$, soit $u_0 = 1$ et $v_0 = 0$.
  $r_1 = e = n \times 0 + e \times 1$, soit $u_1 = 0$ et $v_1 = 1$.
- **Hérédité :** Supposons l'hypothèse vraie aux rangs k et $k-1$, avec $k < N$.

$$\begin{aligned} r_{k+1} &= r_{k-1} - r_k q_k \\ &= nu_{k-1} + ev_{k-1} - (nu_k + ev_k)q_k \\ &= n(u_{k-1} - u_k q_k) + e(v_{k-1} - v_k q_k) \end{aligned}$$

En choisissant $u_{k+1} = u_{k-1} - u_k q_k$ et $v_{k+1} = v_{k-1} - v_k q_k$, on a bien $r_{k+1} = nu_{k+1} + ev_{k+1}$. L'hypothèse est donc encore vraie aux rangs k et $k+1$.

Il existe deux suites d'entiers relatifs $(u_k)_{k\in[\![0,N]\!]}$ *et* $(v_k)_{k\in[\![0,N]\!]}$ *vérifiant, pour tout* $k \in [\![0, N]\!]$: $r_k = nu_k + ev_k$.

c. D'après les questions **A.III.4.a et b.**, $r_N = 1$ et $r_N = nu_N + ev_N$, soit $nu_N + ev_N = 1$. Donc, $ev_N \equiv 1 \,(\text{mod } n)$. Comme dans la question **A.III.2.a.**, il suffit de prendre comme clé de décodage le reste de la division euclidienne de v_N par n.

Une clé de décodage associée à la clé de codage (n, e) *est l'entier* f *défini comme le reste de la division euclidienne de* v_N *par* n.

d. D'après la question **A.III.4.b.**, les suites $(u_k)_{k\in[\![0,N]\!]}$ et $(v_k)_{k\in[\![0,N]\!]}$ sont définies pour tout $k \in [\![0, N]\!]$ par $u_{k+1} = u_{k-1} - u_k q_k$ et $v_{k+1} = v_{k-1} - v_k q_k$. Donc :

La formule à entrer dans la cellule C4 puis à tirer vers le bas et vers la droite est : =C2-C3*$B3.

e. On obtient le tableau suivant :

	A	B	C	D
1	r	q	u	v
2	369		1	0
3	58	6	0	1
4	21	2	1	-6
5	16	1	-2	13
6	5	3	3	-19
7	1	5	-11	70
8	0	#DIV/0!	58	-369
9	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!

Avec, par exemple, dans les cellules :
A4, la formule =MOD(A2 ;A3)
B4, la formule =ENT(A3/A4)

Le calcul à la main se fait de la même manière, en utilisant les formules définies auparavant.

On a alors $N = 5$, et $r_5 = 1 = 369 \times (-11) + 58 \times 70$, soit $u = -11$ et $v = 70$.
$v_5 = 70 \equiv 70 \pmod{369}$, soit $f = 70$.

On trouve $(u, v) = (-11, 70)$ *et une clé de décodage associée à* $(369, 58)$ *est* $f = 70$.

f. On a, d'après la question précédente :
$\begin{cases} 369 \times (-11) + 58 \times 70 = 1 \\ 369 \times u + 58 \times v = 1 \end{cases}$ soit $369(u+11) + 58(v-70) = 0$.
$369(u+11) = 58(70-v)$. Donc, 369 divise $58(70-v)$ et 369 est premier avec 58.
D'après le théorème de Gauss, 369 divise $70-v$: $\exists\, k \in \mathbb{Z}$, $70-v = 369k$, soit $v = 70-369k$.
Mais alors $369(u+11) = 58 \times 369k \iff u+11 = 58k$, soit $u = -11+58k$.

De plus, $369u + 58v = 1$ donc, $v \times 58 \equiv 1 \pmod{369}$.
L'ensemble des clés de décodage est donc l'ensemble des entiers v déterminés par $v = 70 - 369k$ avec $v > 0$, soit $k \leqslant 0$.

L'ensemble des couples d'entiers relatifs (u, v) tels que $369u+58v = 1$ est l'ensemble des couples de la forme $(-11+58k, 70-369k)$ où k est un entier relatif.
L'ensemble des clés de décodage est l'ensemble $\{70+369\ell,\ \ell \in \mathbb{N}\}$.

Partie B

I. 1. Une matrice carrée M d'ordre n est inversible si, et seulement si, il existe une matrice carrée N d'ordre n telle que $MN = NM = I_n$. Son inverse se note M^{-1}.
Supposons que P soit une autre matrice inverse de M, alors $MP = PM = I_n$, et :

$$N = NI_n = NMP = I_nP = P$$

L'inverse d'une matrice inversible est unique.

2. $A^2 - (a+d)A + (ad-bc)I_2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^2 - (a+d)\begin{pmatrix} a & b \\ c & d \end{pmatrix} + (ad-bc)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
$= \begin{pmatrix} a^2+bc & ab+bd \\ ca+dc & cb+d^2 \end{pmatrix} - \begin{pmatrix} a^2+da & ab+db \\ ac+dc & ad+d^2 \end{pmatrix} + \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix}$
$A^2 - (a+d)A + (ad-bc)I_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

$A^2 - (a+d)A + (ad-bc)I_2 = O_2$.

3. $A^2 - (a+d)A + (ad-bc)I_2 = O_2 \iff A\left(A - (a+d)I_2\right) = -(ad-bc)I_2$
$\iff \left(A - (a+d)I_2\right)A = -(ad-bc)I_2$
- si $ad-bc$ est non nul, on a $A \times \dfrac{1}{ad-bc}\left[(a+d)I_2 - A\right] = \dfrac{1}{ad-bc}\left[(a+d)I_2 - A\right] \times A = I_2$.
- si $ad-bc = 0$, supposons A inversible, on a :

$$\begin{aligned} A^2 = (a+d)A &\iff A^2A^{-1} = (a+d)AA^{-1} \\ &\iff A = (a+d)I_2 \\ &\iff \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+d & 0 \\ 0 & a+d \end{pmatrix} \\ &\iff a = b = c = d = 0 \end{aligned}$$

$A = O_2$ n'est pas inversible, on aboutit à une contradiction.

La matrice A est inversible si, et seulement si, $ad-bc \neq 0$.
Dans ce cas, $A^{-1} = \dfrac{1}{ad-bc}\left[(a+d)I_2 - A\right]$.

II. 1. La matrice $M = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ est inversible car $ad - bc = 2 \times 1 - 0 \times 0 = 2$.

Son inverse est $M^{-1} = \frac{1}{2}\left[(2+1)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\right] = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{pmatrix}$.

La matrice $M = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ est une matrice inversible à coefficients dans $\mathbb{Z}$ dont l'inverse n'a pas tous ses coefficients dans $\mathbb{Z}$.

2. La condition $|ad - bc| = 1$ est une condition suffisante pour que A soit inversible dans $\mathbb{Z}$ car dans ce cas, $A^{-1} = \pm[(a+d)I_2 - A]$. Cette matrice est clairement à coefficients dans $\mathbb{Z}$.

Une condition suffisante pour que A soit inversible et d'inverse à coefficients dans $\mathbb{Z}$ est : $|ad - bc| = 1$.

3. Montrons que la condition est nécessaire : on suppose que A est inversible et que A et A^{-1} sont à coefficients dans $\mathbb{Z}$. On a alors $\det(A)$ et $\det(A^{-1})$ des éléments de $\mathbb{Z}$.

$$\begin{aligned} A \text{ inversible} &\iff A \times A^{-1} = A^{-1} \times A = I_2 \\ &\implies \det(A \times A^{-1}) = \det(A^{-1} \times A) = \det(I_2) \\ &\implies \det(A) \times \det\left(A^{-1}\right) = \det(A^{-1}) \times \det(A) = 1 \end{aligned}$$

Or, l'équation $XY = 1$, dans $\mathbb{Z}$ a comme solutions $X = Y = 1$ ou $X = Y = -1$. Donc :

$$\det(A) = \det\left(A^{-1}\right) = 1 \text{ ou } \det(A) = \det\left(A^{-1}\right) = -1$$

Le déterminant permet de montrer que la condition suffisante $|ad - bc| = 1$ est aussi une condition nécessaire.

III. 1. On a le système suivant : $\begin{cases} x' = ax + by \\ y' = cx + dy \end{cases}$, soit $\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$.

Compte tenu des notations du préambule de la **partie B** :

(S) se traduit par l'équation matricielle $X' = AX$.

2. a. Avec $a = 4, b = 3, c = 5$ et $d = 4$, on obtient : $\begin{cases} x' = 4x + 3y \\ y' = 5x + 4y \end{cases}$.

lettre claire	rang	codage	rang codé	lettre codée
B	1	$4 \times 1 + 3 \times 4 = 16$	16	Q
E	4	$5 \times 1 + 4 \times 4 = 21$	21	V
Z	25	$4 \times 25 + 3 \times 14 = 142$	12	M
O	14	$5 \times 25 + 4 \times 14 = 181$	25	Z
U	20	$4 \times 20 + 3 \times 19 = 137$	7	H
T	19	$5 \times 20 + 4 \times 19 = 176$	20	U

Avec ce chiffrement de Hill, le mot BEZOUT est codé QVMZHU.

b. Pour le décodage, nous avons x' et y' et il nous faut retrouver x et y.
Or, la matrice $A = \begin{pmatrix} 4 & 3 \\ 5 & 4 \end{pmatrix}$ est inversible puisque $ad - bc = 4 \times 4 - 3 \times 5 = 1$.
De plus, cette matrice est à coefficients dans $\mathbb{Z}$ d'après la question **B.II.2.**
On peut alors écrire $X' = AX \iff X = A^{-1}X'$ avec

$$\begin{aligned} A^{-1} &= \frac{1}{1}\left[(4+4)I_2 - A\right] \\ &= 8I - A \\ A^{-1} &= \begin{pmatrix} 4 & -3 \\ -5 & 4 \end{pmatrix} \end{aligned}$$

Soit $\begin{cases} x = 4x' - 3y' \\ y = -5x' + 4y' \end{cases}$. On obtient alors :

Lettre codée	rang	système	rang décodé	lettre claire
S	18	$4 \times 18 - 3 \times 5 = 57$	5	F
F	5	$-5 \times 18 + 4 \times 5 = -70$	8	I
X	23	$4 \times 23 - 3 \times 12 = 4$	4	E
M	12	$-5 \times 23 + 4 \times 12 = 11$	11	L
O	14	$4 \times 14 - 3 \times 9 = 3$	3	D
J	9	$-5 \times 14 + 4 \times 9 = 18$	18	S

Avec ce chiffrement de Hill, le mot SFXMOJ est décodé FIELDS.

3. a. Solutions de l'équation $(E) : 7u \equiv 1 \,(\text{mod } 26)$ par l'algorithme d'Euclide étendu :

$$\begin{aligned} 26 &= 7 \times 3 + 5 \\ 7 &= 5 \times 1 + 2 \\ 5 &= 2 \times 2 + 1 \end{aligned}$$

$$\begin{aligned} 1 &= 5 - 2 \times (7 - 5 \times 1) \\ &= -2 \times 7 + 3 \times 5 \\ &= -2 \times 7 + 3 \times (26 - 7 \times 3) \\ 1 &= -11 \times 7 + 3 \times 26 \end{aligned}$$

-11 est une solution particulière de (E), déterminons toutes les solutions :

$$\begin{cases} 7 \times (-11) = 1 + 26 \times (-3) \\ 7 \times u = 1 + 26 \times k \end{cases} \implies 7(u+11) = 26(k+3)$$

26 divise $7(u+11)$ et 26 et 7 étant premiers entre eux, d'après le théorème de Gauss, 26 divise $u + 11$, donc $\exists\, n \in \mathbb{Z}$, $u + 11 = 26n \iff u = -11 + 26n$.

$$\begin{aligned} \text{Or, } 0 \leqslant u \leqslant 25 &\iff 0 \leqslant -11 + 26n \leqslant 25 \\ &\iff \frac{11}{26} \leqslant n \leqslant \frac{36}{26} \end{aligned}$$

n est un entier, il vaut donc 1 et $u = -11 + 26 \times 1 = 15$.
C'est la seule solution possible entre 0 et 25.

Il existe un unique entier u compris entre 0 *et* 25 *tel que* $7u \equiv 1\,(mod\ 26)$.

b. Dans cette question, on a $A = \begin{pmatrix} 3 & 2 \\ 1 & 3 \end{pmatrix}$, soit

$$\begin{aligned} A^{-1} &= \frac{1}{3\times 3 - 2\times 1}[(3+3)I_2 - A] \\ &= \frac{1}{7}\left[\begin{pmatrix} 6 & 0 \\ 0 & 6 \end{pmatrix} - \begin{pmatrix} 3 & 2 \\ 1 & 3 \end{pmatrix}\right] \\ A^{-1} &= \frac{1}{7}\begin{pmatrix} 3 & -2 \\ -1 & 3 \end{pmatrix} \end{aligned}$$

D'où :

$$\begin{aligned} uBA \equiv I_2 \,(\text{mod } 26) &\Longrightarrow 7uBA \equiv 7I_2 \,(\text{mod } 26) \\ &\Longrightarrow BA \equiv 7I_2 \,(\text{mod } 26) \qquad \text{d'après la question } \textbf{B.III.3.a.} \\ &\Longrightarrow B \equiv 7A^{-1} \,(\text{mod } 26) \\ &\Longrightarrow B \equiv 7 \times \frac{1}{7}\begin{pmatrix} 3 & -2 \\ -1 & 3 \end{pmatrix} \,(\text{mod } 26) \\ &\Longrightarrow B \equiv \begin{pmatrix} 3 & -2 \\ -1 & 3 \end{pmatrix} \,(\text{mod } 26) \end{aligned}$$

La matrice $B = \begin{pmatrix} 3 & -2 \\ -1 & 3 \end{pmatrix}$ *est une matrice à coefficients entiers relatifs telle que* $uBA \equiv I_2$ *(mod* 26*).*

c. Un bloc de deux lettres est codé par la formule $X' = AX$ et peut être décodé grâce à la formule $X = A^{-1}X'$.
Cependant, dans notre cas, la matrice A^{-1} n'est pas à coefficients dans $\mathbb{Z}$.
On a, d'après la question précédente :

$$\begin{aligned} X = A^{-1}X' &\Longrightarrow uBAX \equiv uBAA^{-1}X' \,(\text{mod } 26) \\ &\Longrightarrow I_2X \equiv uBX' \,(\text{mod } 26) \\ &\Longrightarrow X \equiv uBX' \,(\text{mod } 26) \\ &\Longrightarrow X \equiv 15\begin{pmatrix} 3 & -2 \\ -1 & 3 \end{pmatrix} X' \,(\text{mod } 26) \qquad \text{avec } u = 15 \\ &\Longrightarrow X \equiv \begin{pmatrix} 45 & -30 \\ -15 & 45 \end{pmatrix} X' \,(\text{mod } 26) \end{aligned}$$

Pour le premier bloc (A ; K), $X' = \begin{pmatrix} 0 \\ 10 \end{pmatrix}$, soit $X \equiv \begin{pmatrix} 45 & -30 \\ -15 & 45 \end{pmatrix}\begin{pmatrix} 0 \\ 10 \end{pmatrix} \,(\text{mod } 26)$

$$X \equiv \begin{pmatrix} -300 \\ 450 \end{pmatrix} \,(\text{mod } 26)$$

$$X \equiv \begin{pmatrix} 12 \\ 8 \end{pmatrix} \,(\text{mod } 26)$$

$x = 12$ correspond à la lettre M et $y = 8$ correspond à la lettre I.

Pour le bloc (X ; O), $X' = \begin{pmatrix} 23 \\ 14 \end{pmatrix}$, soit $X \equiv \begin{pmatrix} 45 & -30 \\ -15 & 45 \end{pmatrix}\begin{pmatrix} 23 \\ 14 \end{pmatrix} \,(\text{mod } 26)$

$$X \equiv \begin{pmatrix} 17 \\ 25 \end{pmatrix} \,(\text{mod } 26)$$

$x = 17$ correspond à la lettre R et $y = 21$ correspond à la lettre Z.

Pour le bloc (U ; E), $X' = \begin{pmatrix}20\\4\end{pmatrix}$, soit $X \equiv \begin{pmatrix}45 & -30\\-15 & 45\end{pmatrix}\begin{pmatrix}20\\4\end{pmatrix} \pmod{26}$

$$X \equiv \begin{pmatrix}0\\10\end{pmatrix} \pmod{26}$$

$x = 0$ correspond à la lettre A et $y = 10$ correspond à la lettre K.

Pour le bloc (V ; H), $X' = \begin{pmatrix}21\\7\end{pmatrix}$, soit $X \equiv \begin{pmatrix}45 & -30\\-15 & 45\end{pmatrix}\begin{pmatrix}21\\7\end{pmatrix} \pmod{26}$

$$X \equiv \begin{pmatrix}7\\0\end{pmatrix} \pmod{26}$$

$x = 7$ correspond à la lettre K et $y = 0$ correspond à la lettre A.

Pour le bloc (D ; L), $X' = \begin{pmatrix}3\\11\end{pmatrix}$, soit $X \equiv \begin{pmatrix}45 & -30\\-15 & 45\end{pmatrix}\begin{pmatrix}3\\11\end{pmatrix} \pmod{26}$

$$X \equiv \begin{pmatrix}13\\8\end{pmatrix} \pmod{26}$$

$x = 13$ correspond à la lettre N et $y = 8$ correspond à la lettre I.

Le décodage de AKXOUEVHDL donne MIRZAKHANI.[1]

4. Un bloc de deux lettres est codé par la formule $X' = AX$ et peut être décodé grâce à la formule $X = A^{-1}X'$.
Pour déchiffrer le message, il s'agit donc d'inverser la matrice A modulo 26.
Cela peut se faire si, et seulement si, le déterminant de cette matrice possède un inverse modulo 26, c'est-à-dire, d'après le théorème de Bézout, si $\det(A)$ est premier avec 26.

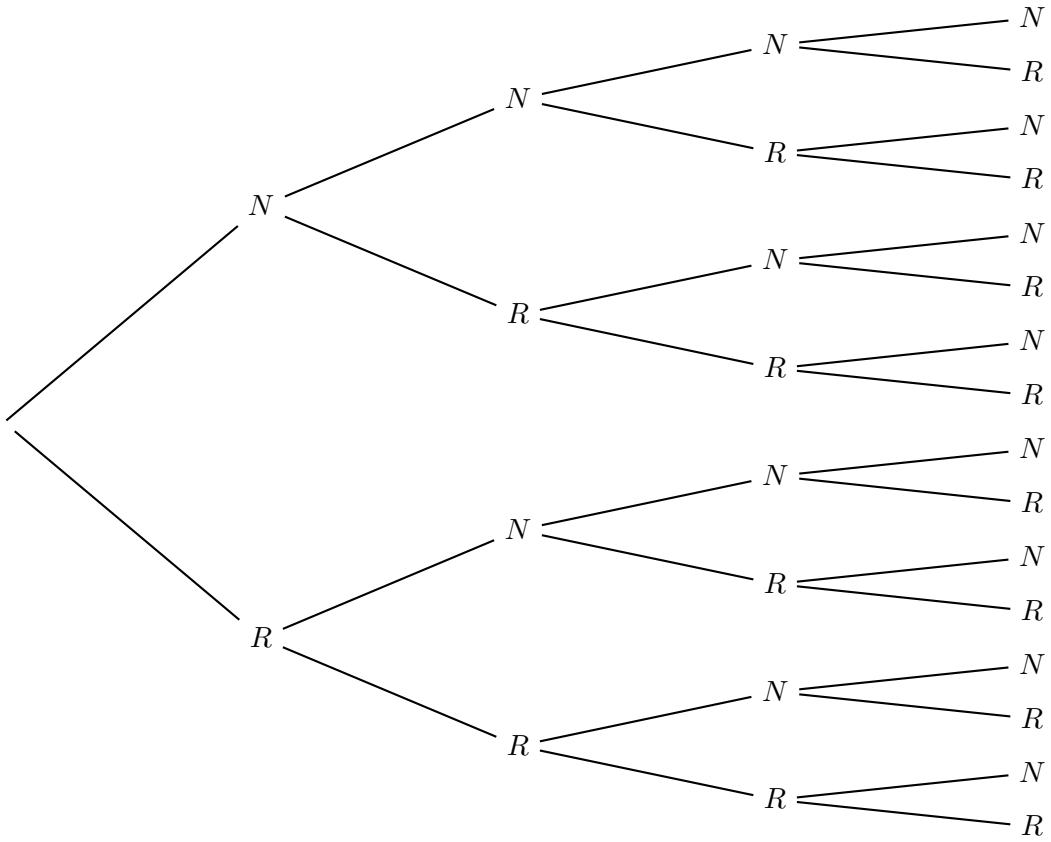
Tout mot comportant un nombre pair de lettres peut-être décodé par la méthode de Hill si, et seulement si, le déterminant $ad - bc$ est premier avec 26.

1. La médaille **Fields** est la plus prestigieuse récompense pour la reconnaissance de travaux en mathématiques, souvent considérée comme un équivalent du prix Nobel. Elle est attribuée tous les quatre ans.
Maryam Mirzakhani est une mathématicienne iranienne brillante, première femme à obtenir la médaille Fields en 2014.

Problème n°2

Partie A

I. 1. Construisons l'arbre correspondant à $n = 4$:



En suivant les branches de cet arbre de haut en bas, on obtient la liste des 16 chemins :

(0,0,0,0) - (0,0,0,1) - (0,0,1,0) - (0,0,1,1) - (0,1,0,0) - (0,1,0,1) - (0,1,1,0) - (0,1,1,1)
(1,0,0,0) -(1,0,0,1) - (1,0,1,0) - (1,0,1,1) - (1,1,0,0) - (1,1,0,1) - (1,1,1,0) - (1,1,1,1)

2. *Parmi ces 16 chemins, 6 contiennent exactement 2 fois l'élément 1.*

3. *Parmi ces 6 chemins, il y a à chaque fois 3 chemins contenant un 1 respectivement à la première, deuxième, troisième et quatrième place.*

II. 1. $\binom{n}{k}$ est le nombre de chemins de l'arbre correspondant à n tirages réalisant exactement k succès, et donc $n-k$ échecs. Par symétrie de l'arbre et le caractère binaire des événements (on a soit 0, soit 1), celui-ci correspond également au nombre de chemins réalisant $n-k$ succès et k échecs, c'est-à-dire $\binom{n}{n-k}$. Donc :

$$\forall\, n \in \mathbb{N}^*, \forall\, k \in [\![0, n]\!],\ \binom{n}{k} = \binom{n}{n-k}.$$

2. L'ensemble E des $(n+1)$-uplets contenant k fois l'élément 1 est de cardinal $\binom{n+1}{k}$.
   Il peut être partitionné en deux ensembles :
   - l'ensemble E_1 des $(n+1)$-uplets contenant l'élément 1 en première place. Cet élément étant fixé, le nombre de n-uplets contenant exactement $k-1$ fois l'élément 1 est de $\binom{n}{k-1}$;
   - l'ensemble E_2 des $(n+1)$-uplets contenant l'élément 0 en première place. Cet élément étant fixé, le nombre de n-uplets contenant exactement k fois l'élément 1 est de $\binom{n}{k}$.

   Les ensembles E_1 et E_2 étant complémentaires dans E, on a : $\text{card}(E) = \text{card}(E_1) + \text{card}(E_2)$:

$$\forall\, n \in \mathbb{N}^*, \forall\, k \in [\![1, n]\!],\ \binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}.$$

3. a. Chaque ligne de la matrice A est l'un des chemins conduisant à k succès et $n-k$ échecs. Cette ligne comporte donc k fois le nombre 1 et $n-k$ fois le nombre 0. La somme de ses éléments vaut $k \times 1 + (n-k) \times 0 = k$.

La somme des éléments d'une ligne de la matrice A vaut k.

   b. À chaque 1 de la j-ième colonne de la matrice A, on associe le $(n-1)$-uplet contenant $k-1$ nombres 1 obtenu en prenant la i-ième ligne correspondante et en supprimant le j-ième coefficient. On a donc une bijection entre les $(n-1)$-uplets ayant exactement $k-1$ composantes égales à 1 et les lignes de la matrice ayant la j-ème composante égale à 1. D'où,

Pour j compris entre 1 et n, la somme des éléments de la j-ème colonne de la matrice A vaut $\binom{n-1}{k-1}$.

   c. On peut effectuer la somme S des coefficients de la matrice de deux manières différentes :
   - par ligne, il y a $\binom{n}{k}$ lignes dont la somme des coefficients vaut k, soit $S = \binom{n}{k} \times k$;
   - par colonne, il y a n colonnes dont la somme des coefficients vaut $\binom{n-1}{k-1}$, soit $S = n \times \binom{n-1}{k-1}$. Donc :

$$\forall\, n \in \mathbb{N}^*, \forall\, k \in [\![1, n]\!],\ k\binom{n}{k} = n\binom{n-1}{k-1}.$$

4. a. On considère $E = \{e_1, e_2, \ldots, e_n\}$ un ensemble ordonné à n éléments. À toute partie $\mathcal{P}$ de E, on associe un n-uplet $(p_1, p_2, \ldots p_n)$ tel que pour tout i allant de 1 à n, $p_i = 1$ si $e_i \in \mathcal{P}$ et $p_i = 0$ sinon. L'application ainsi construite définit une bijection de l'ensemble des parties de E vers l'ensemble des n-uplets définis comme ci-dessus. Donc, le nombre d'éléments d'une partie de E est égal au nombre de composantes égales à 1 du n-uplet correspondant.
   Ainsi, le nombre des parties à p éléments d'un ensemble à n éléments est égal au nombre des n-uplets ayant exactement p fois 1, donc au nombre de chemins de longueur n réalisant p succès.

Les définitions du coefficient binomial données dans le supérieur et au lycée sont cohérentes entre elles puisqu'elles définissent le même nombre.

b. Déterminons dans un premier temps le nombre d'ensembles ordonnés à k éléments d'un ensemble à n éléments : il y a $n!$ façon de choisir son premier élément. Cet élément étant choisi, il y a $(n-1)!$ façon de choisir son deuxième élément, ainsi de suite jusqu'au k-ième élément pour lequel il y a $(n-k+1)!$ façon de le choisir.
Donc, il y a $n! \times (n-1)! \times \cdots \times (n-k+1)! = \dfrac{n!}{(n-k)!}$ façons de choisir k éléments ordonnés parmi n.
Pour chacune de ces façons, il faut éliminer celles qui contiennent les mêmes éléments, mais dans un ordre différent. Il y a $k!$ manières d'ordonner les k éléments, d'où :

$$\forall\, k \in [\![0, n]\!],\ \binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

c. Résultat de la question **A.II.2** : $\forall\, n \in \mathbb{N}^*, \forall\, k \in [\![0, n]\!]$:

$$\begin{aligned}\binom{n}{k-1} + \binom{n}{k} &= \frac{n!}{(k-1)!(n-k+1)!} + \frac{n!}{k!(n-k)!} \\ &= \frac{n!(k + n - k + 1)}{k!(n+1-k)!} \\ \binom{n}{k-1} + \binom{n}{k} &= \frac{(n+1)!}{k!(n+1-k)!}\end{aligned}$$

$$\forall\, n \in \mathbb{N}^*, \forall\, k \in [\![0, n]\!] : \binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}.$$

Résultat de la question **A.II.3** : $\forall\, n \in \mathbb{N}^*, \forall\, k \in [\![1, n]\!]$:

$$\begin{aligned}n\binom{n-1}{k-1} &= n \times \frac{(n-1)!}{(k-1)!(n-1-k+1)!} \\ &= \frac{n!}{(k-1)!(n-k)!} \\ n\binom{n-1}{k-1} &= k \times \frac{n!}{k!(n-k)!}\end{aligned}$$

$$\forall\, n \in \mathbb{N}^*, \forall\, k \in [\![1, n]\!] : n\binom{n-1}{k-1} = k\binom{n}{k}.$$

III. On considère l'expérience suivante : on tire une boule dans une urne, on note sa couleur, puis on la remet dans l'urne. Un succès correspond à l'obtention d'une boule rouge, en proportion θ dans l'urne. Il s'agit d'une expérience de Bernoulli de paramètre $p = \theta$.
On réitère cette expérience n fois, de manière indépendante. On obtient donc la loi binomiale de paramètres (n, θ).

Le nombre de résultats menant à k boules rouges correspond au nombre de parties à k éléments parmi n, il y en a $\binom{n}{k}$.

La probabilité d'obtenir k boules rouges (et donc $n-k$ boules noires) dans un ordre donné est de $\theta^k \times (1-\theta)^{n-k}$.

On a alors $P(X = k) = \binom{n}{k}\, \theta^k \times (1-\theta)^{n-k}$.

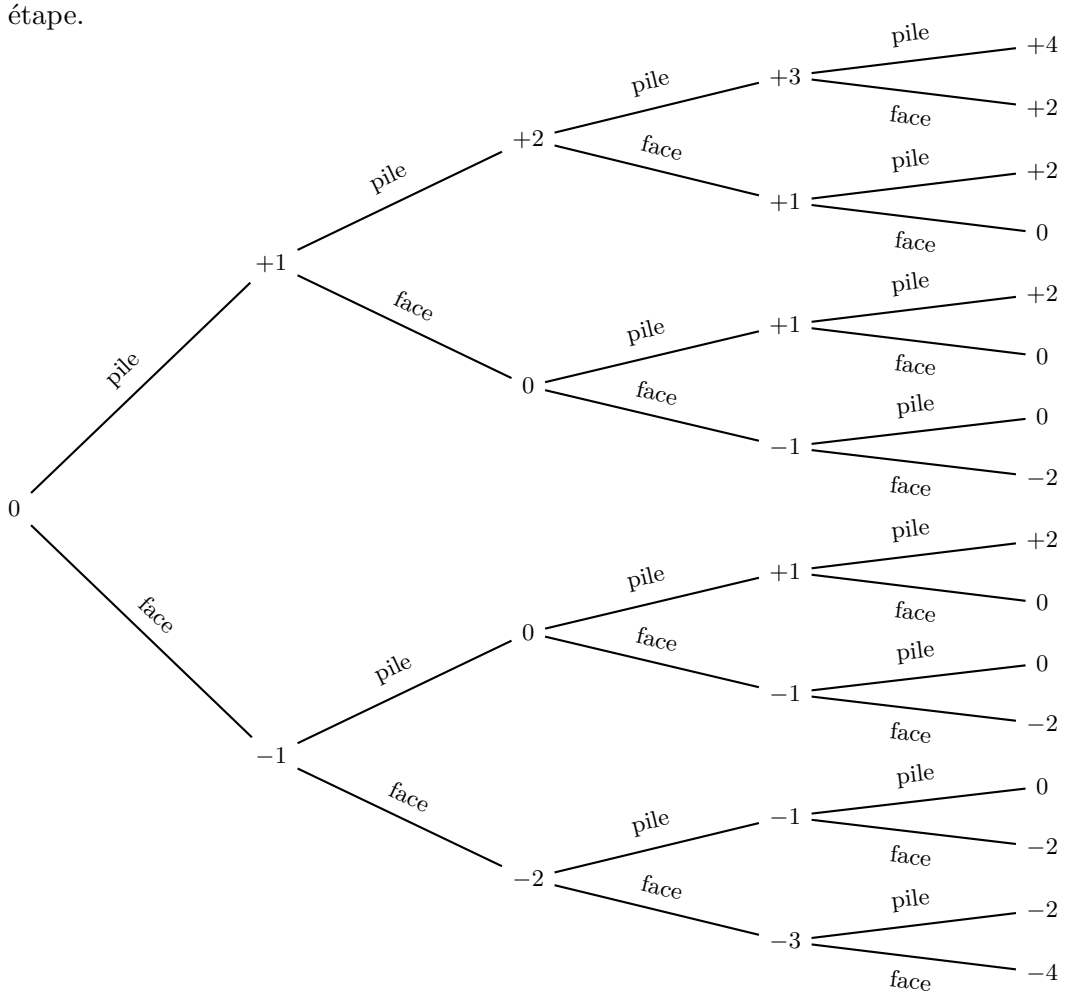
Calculons l'expérience mathématique de la loi de X pour tout $n \in \mathbb{N}^*$:

$$\begin{aligned}
E(X) &= \sum_{k=0}^{n} k \binom{n}{k} \theta^k \times (1-\theta)^{n-k} \\
&= \sum_{k=1}^{n} k \binom{n}{k} \theta^k \times (1-\theta)^{n-k} \\
&= n\,\theta \sum_{k=1}^{n} \binom{n-1}{k-1} \theta^{k-1} \times (1-\theta)^{n-k} && \text{d'après la question } \textbf{A.II.3.c.} \\
&= n\theta \sum_{k=0}^{n-1} \binom{n-1}{k} \theta^{k} \times (1-\theta)^{n-k-1} \\
&= n\theta\,(\theta + 1 - \theta)^{n-1} && \text{formule du binôme de Newton} \\
E(X) &= n\theta
\end{aligned}$$

X suit une loi binomiale $\mathcal{B}(n,\theta)$ avec $P(X=k) = \binom{n}{k} \theta^k \times (1-\theta)^{n-k}$ et $E(X) = n\theta$.

Partie B

I. 1. Représentons par un arbre la situation. Les nombres correspondent à l'abscisse du point à chaque étape.



La pièce étant équilibrée, nous sommes dans une situation d'équiprobabilité, donc chaque branche de l'arbre est équiprobable. Pour déterminer la loi de X_4, il suffit donc de compter, pour chaque élément de l'univers, le nombre de possibilités.
$\Omega = \{-4, -2, 0, 2, 4\}$ et on obtient la loi suivante :

k	-4	-2	0	2	4
$P(X_4 = k)$	$\frac{1}{16}$	$\frac{4}{16}$	$\frac{6}{16}$	$\frac{4}{16}$	$\frac{1}{16}$

2. D_n est le nombre de fois où la pièce est tombée sur pile au cours des n premiers lancers. C'est la somme de n expériences de Bernoulli indépendantes consistant à jeter une pièce de monnaie équilibrée dont le succès : « obtenir un pile » est de probabilité $\frac{1}{2}$. Donc :

D_n est la variable aléatoire suivant la loi binomiale de paramètres n et $\frac{1}{2}$.

3. $X_n = 0 + D_n \times 1 + (n - Dn) \times (-1) = D_n - n + D_n = 2D_n - n$.

$X_n = 2D_n - n$.

4. L'espérance mathématique étant linéaire, on a :

$$\begin{aligned} E(X_n) &= E(2D_n - n) \\ &= 2E(D_n) - E(n) \\ &= 2 \times \frac{1}{2}n - n \qquad \text{d'après la question } \textbf{A.III.} \\ E(X_n) &= 0 \end{aligned}$$

L'espérance de X_n est nulle, ce qui signifie que, en moyenne, au bout de n lancers, le point est revenu à l'origine.

II. 1. Pour $k \in [\![0, n]\!]$, on considère une issue correspondant à l'obtention de k « pile » et de $n - k$ « face ». On a alors $X_n = 0 + k \times 1 + (n - k) \times (-1) = 2k - n$.
Si n est impair, X_n est un nombre impair comme somme d'un nombre pair et d'un nombre impair, donc l'éventualité $\{X_n = 0\}$ est impossible.

Lorsque n est impair, $P(X_n = 0) = 0$.

2. $X_{2n} = 0$ lorsqu'on a obtenu autant de « pile » que de « face ». Il s'agit donc de déterminer le nombre de $2n$-uplets comportant exactement n « pile ». Il y en a $\binom{2n}{n}$.
Or, le nombre d'éléments de l'univers de cette expérience aléatoire est de 2^{2n}. Donc,

$$\begin{aligned} P(X_{2n} = 0) &= \frac{\binom{2n}{n}}{2^{2n}} \qquad \text{puisqu'il y a équiprobabilité} \\ P(X_{2n} = 0) &= \frac{2n!}{n!n!} \times \frac{1}{4^n} \end{aligned}$$

$P(X_{2n} = 0) = \dfrac{2n!}{4^n (n!)^2}$.

III. 1. L'algorithme donne, pour k allant de 1 à n, un nombre aléatoire compris entre 0 et 1. Pour chaque valeur de k, si ce nombre est supérieur à $0,5$ (qui correspond au tirage d'un pile) x est incrémenté de 1. Si le nombre est inférieur à $0,5$ (qui correspond au tirage d'un face) x est diminué de 1.

La valeur x retournée correspond à l'abscisse du point après n déplacements.

2. Voici, par exemple, un deuxième algorithme écrit en Python :

```
1  from random import *
2  n=int(input("Entrer le nombre de lancers : n = "))
3  x=0
4  i=0
5  for k in range(n):
6     if random()>0.5:
7        x=x+1
8     else:
9        x=x-1
10    if x==0:
11       i=i+1
12 print("À la fin, l'abscisse du point vaut x =",x)
13 print("Le point est passé",i,"fois par l'origine")
```

Cet algorithme introduit une compteur `i` qui compte le nombre de fois où `x` prend la valeur 0.

3. Voici, par exemple, un troisième algorithme écrit en Python :

```
1  from random import *
2  n=int(input("Entrer le nombre de lancers : n = "))
3  i=0
4  for j in range(1000):
5      x=0
6      for k in range(n):
7          if random()>0.5:
8              x=x+1
9          else:
10             x=x-1
11     if x==0:
12         i=i+1
13 f=i/1000
14 print("L'événement Xn=0 a une fréquence d'apparition
   de",f,"au cours de la répétition de 1000 séries
   de",n,"lancers.")
```

Cette fois, le compteur `i` compte le nombre de fois où `x` prend la valeur 0 à la fin des `n` lancers. La fréquence est calculée en effectuant le quotient de `i` par 1000, le nombre de séries.

4. Ces trois algorithmes peuvent permettre de conjecturer certaines propriétés :
   - le premier algorithme permet de conjecturer les valeurs possibles pour X_n ;
   - le second le nombre de fois où le point est passé par l'origine ;
   - le troisième permet d'effectuer de multiples simulations. On pourra également modifier la valeur de n pour conjecturer le fait que, plus on effectue des lancers, plus le résultat obtenu (la fréquence d'apparition de l'événement $X_n = 0$, c'est à dire de l'espérance mathématique), se rapproche de la probabilité $P(X_n = 0)$.

IV. 1. Pour $n \in \mathbb{N}^*$ et $k \in [\![0, 2n]\!]$, on considère une issue correspondant à l'obtention de k fois « pile » et de $2n-k$ fois « face ». On a alors

$$\begin{aligned} X_{2n} &= 0 + k \times 1 + (2n-k) \times (-1) \\ &= 2k - 2n \\ X_{2n} &= 2(k-n) \qquad \text{qui est un entier relatif pair.} \end{aligned}$$

De plus, $0 \leqslant k \leqslant 2n \iff -2n \leqslant 2k - 2n \leqslant 2n$. D'où :

À l'issue de ces $2n$ lancers, l'abscisse du point est un entier relatif pair compris entre $-2n$ et $2n$.

2. Pour $n \in \mathbb{N}^*$, on a $X_{2n} = 2D_{2n} - 2n$ d'après la question **B.I.3.**

$$\begin{aligned} \text{Soit } k \in [\![0, n]\!],\ P(X_{2n} = 2k) &= P(2D_{2n} - 2n = 2k) \\ &= P\left(D_{2n} = \frac{2k+2n}{2}\right) \\ &= P(D_{2n} = k+n) \\ &= \binom{2n}{k+n}\left(\frac{1}{2}\right)^{k+n}\left(\frac{1}{2}\right)^{2n-k-n} \qquad D_{2n} \sim \mathcal{B}\left(2n, \frac{1}{2}\right) \\ P(X_{2n} = 2k) &= \binom{2n}{k+n}\left(\frac{1}{2}\right)^{2n} \end{aligned}$$

Soit $n \in \mathbb{N}^*$ et $k \in [\![0, n]\!]$, la probabilité qu'à l'issue de ces $2n$ lancers, l'abscisse du point soit égale à $2k$ est de $\binom{2n}{k+n} \times \frac{1}{4^n}$.

3. Soit C_n la valeur aléatoire égale au nombre de passages à l'origine entre le premier et le $2n$-ième lancer. C_n prend des valeurs entières entre 0 et n.
Soit Ω_k la variable aléatoire égale à 1 si l'abscisse du point à l'issue du k-ième lancer est nulle et égale à 0 sinon. On a :

$$\begin{aligned} C_n &= \sum_{k=1}^{2n} \Omega_k \\ &= \sum_{k=0}^{n-1} \Omega_{2k+1} + \sum_{k=1}^{n} \Omega_{2k} \\ C_n &= \sum_{k=1}^{n} \Omega_{2k} \end{aligned}$$

puisque l'abscisse du point ne peut être nulle lorsque le nombre de lancers est impair, d'après la question **B.II.1.** Donc, $\forall\, k \in [\![0, n-1]\!]$, $\Omega_{2k+1} = 0$.
On peut alors calculer l'espérance de C_n, par linéarité, sachant que la variable aléatoire Ω_k suit une loi de Bernoulli prenant les valeurs 1 et 0 :

$$\begin{aligned}
E(C_n) &= E\left(\sum_{k=1}^{n}\Omega_{2k}\right)\\
&= \sum_{k=1}^{n} E(\Omega_{2k})\\
&= \sum_{k=1}^{n} 1\times P(\Omega_{2k}=1)+0\times P(\Omega_{2k}=0)\\
&= \sum_{k=1}^{n} P(\Omega_{2k}=1)\\
&= \sum_{k=1}^{n} P(X_{2k}=0)\\
E(C_n) &= \sum_{k=1}^{n}\binom{2k}{0+k}\times\frac{1}{4^k}
\end{aligned}$$

L'espérance mathématique de C_n se calcule grâce à la formule $E(C_n)=\sum_{k=1}^{n}\binom{2k}{k}\times\frac{1}{4^k}$.

Soit $(\mathcal{H}_n)$ l'hypothèse : $\sum_{k=1}^{n}\frac{1}{4^k}\binom{2k}{k}=\frac{2n+1}{4^n}\binom{2n}{n}-1$.

- **Initialisation :** pour $n=1$, $\sum_{k=1}^{1}\frac{1}{4^k}\binom{2k}{k}=\frac{1}{4}\times 2=\frac{1}{2}$.
  D'autre part, $\frac{2\times 1+1}{4^1}\binom{2}{1}-1=\frac{3}{4}\times 2-1=\frac{1}{2}$.
  $\mathcal{H}_1$ est donc vraie.

- **Hérédité :** supposons l'hypothèse vraie au rang n.

$$\begin{aligned}
\sum_{k=1}^{n+1}\frac{1}{4^k}\binom{2k}{k} &= \sum_{k=1}^{n}\frac{1}{4^k}\binom{2k}{k}+\frac{1}{4^{n+1}}\binom{2n+2}{n+1}\\
&= \frac{2n+1}{4^n}\binom{2n}{n}-1+\frac{1}{4^{n+1}}\binom{2n+2}{n+1} \qquad (\mathcal{H}_n)\\
&= \frac{1}{4^{n+1}}\binom{2n+2}{n+1}\left[4\cancel{(2n+1)}\frac{(n+1)(n+1)}{\cancel{(2n+1)}(2n+2)}+1\right]-1\\
&= \frac{1}{4^{n+1}}\binom{2n+2}{n+1}\left[\frac{4(n+1)}{2}+1\right]-1\\
&= \frac{1}{4^{n+1}}\binom{2n+2}{n+1}\left[\frac{4n+4+2}{2}\right]-1\\
\sum_{k=1}^{n+1}\frac{1}{4^k}\binom{2k}{k} &= \frac{2n+3}{4^{n+1}}\binom{2n+2}{n+1}-1
\end{aligned}$$

  L'hypothèse est encore vraie au rang $n+1$.

L'hypothèse de récurrence $(\mathcal{H}_n)$ est donc vraie pour tout n supérieur ou égal à 1.

$\forall\, n\geqslant 1,\ E(C_n)=\frac{2n+1}{4^n}\binom{2n}{n}-1.$