CAPES EXTERNE

MATHÉMATIQUES 2

Problème 1

Partie A - Un chiffrement monographique

I. 1. Soit d un entier naturel non nul qui est un diviseur commun à a et b. Alors, d divise $au+bv$ ou encore d divise 1. On en déduit que $d=1$. Ainsi, 1 est le seul diviseur commun à a et b et donc a et b sont premiers entre eux.

I. 2. a. Si $a>0$, $a=a\times 1+b\times 0$ est un entier naturel non nul qui est un élément de $\mathscr{E}$. Si $a<0$, $-a=a\times(-1)+b\times 0$ est un entier naturel non nul qui est un élément de $\mathscr{E}$.
Dans tous les cas, $\mathscr{E}\cap\mathbb{N}^*$ est une partie non vide de $\mathbb{N}$ (et même de $\mathbb{N}^*$). On sait alors que $\mathscr{E}\cap\mathbb{N}^*$ admet un plus petit élément n_0. De plus, $n_0\in\mathbb{N}^*$.

I. 2. b. La division euclidienne de a par n_0 s'écrit $a=q\times n_0+r$ où $q\in\mathbb{Z}$ et $0\leqslant r\leqslant n_0-1$. De plus, puisque $n_0\in\mathscr{E}$, il existe $(u_0,v_0)\in\mathbb{Z}^2$ tel que $n_0=au_0+bv_0$. Mais alors,

$$r=a-qn_0=a-q\,(au_0+bv_0)=(1-qu_0)\,a+(-qv_0)\,b.$$

Puisque $1-qu_0$ et $-qv_0$ sont des entiers relatifs, on en déduit que $r\in\mathscr{E}$. Finalement, $r\in\mathscr{E}\cap[\![0,n-1]\!]=\{0\}$ (par définition de n_0). Donc, $r=0$.

I. 2. c. Ainsi, n_0 divise a et de même, en échangeant les rôles de a et b, n_0 divise b. Finalement, n_0 est un diviseur commun à a et à b et donc un diviseur du PGCD de a et b à savoir 1. Puisque n_0 est un entier naturel non nul, on en déduit que $n_0=1$.

On a montré que $1\in\mathscr{E}$ ou encore, il existe deux entiers relatifs u et v tels que $au+bv=1$.

I. 3. On a démontré le 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. Soient a, b et c trois entiers relatifs non nuls. On suppose que a divise bc et que a et b sont premiers entre eux. Donc, il existe $k\in\mathbb{Z}$ tel que $bc=ka$ et il existe $(u,v)\in\mathbb{Z}^2$ tel que $au+bv=1$.

On multiplie les deux membres de l'égalité $au+bv=1$ par c. On obtient

$$c=acu+bcv=acu+kav=a(cu+kv).$$

Puisqaue $cu+kv$ est un entier relatif, ceci montre que a divise c. On a démontré le théorème de Gauss.

III. Chiffrement lettre par lettre

III. 1. a. • G a pour rang $x=6$. $58x=348\equiv 348\ [369]$ avec $0\leqslant 348\leqslant 368$.
• A a pour rang $x=0$. $58x=0\equiv 0\ [369]$ avec $0\leqslant 0\leqslant 368$.
• U a pour rang $x=20$. $58x=1160\equiv 53\ [369]$ avec $0\leqslant 53\leqslant 368$.
• S a pour rang $x=18$. $58x=1044\equiv 306\ [369]$ avec $0\leqslant 306\leqslant 368$.

Le mot GAUSS est codé par

$$348\quad 0\quad 53\quad 306\quad 306.$$

III. 1. b. On peut proposer de faire recopier en ligne 1 d'un tableau Excel les 26 lettres de l'alphabet (cases A1 à A26). Puis de faire écrire leurs rangs respectifs en ligne 2 (on écrit 0 en case A2 puis la formule =A2+1 dans la case B2, formule que l'on recopie ensuite vers la droite). On propose ensuite de donner les codes associés en ligne 3 : en case A3, on rentre la formule =MOD(58*A2 ;369) qui donne le reste de la division euclidienne de 58 fois le rang de la lettre A par 369 puis on recopie cette formule vers la droite.

Il n'y a plus qu'à chercher en première ligne les lettres correspondant aux nombres 290 232 248 327 0 364 inscrits quant eux en ligne 3.

III. 2. a. Puisque e et n sont non nuls et premiers entre eux, d'après le théorème de BÉZOUT, il existe deux entiers relatifs u et v tels que $eu + nv = 1$. Mais alors, u est un entier relatif tel que $eu \equiv 1\ [n]$. Soit f le reste de la division euclidienne de u par n. f est un entier naturel tel que $u \equiv f\ [n]$ et donc tel que $ef \equiv eu\ [n]$ ou encore tel que $ef \equiv 1\ [n]$.

III. 2. b. Soient α une lettre de l'alphabet de rang $x \in [\![0, 25]\!]$ puis y le reste de la division euclidienne de ex par n. On suppose y connu et on veut retrouver x.

$$ex \equiv y\ [n] \Rightarrow fex \equiv fy\ [n] \Rightarrow x \equiv fy\ [n].$$

Donc, il existe $K \in \mathbb{Z}$ tel que $x = fy + Kn$. Enfin,

$$0 \leqslant x \leqslant 25 \Leftrightarrow 0 \leqslant fy + Kn \leqslant 25 \Leftrightarrow -\frac{fy}{n} \leqslant K \leqslant -\frac{fy}{n} + \frac{25}{n}.$$

Puisque $n \geqslant 26$, on a $0 \leqslant \dfrac{25}{n} < 1$ et donc il existe au plus un entier relatif dans l'intervalle $\left[-\dfrac{fy}{n}, -\dfrac{fy}{n} + \dfrac{25}{n}\right]$. Comme d'autre part x existe puisque x a été codé en y, il existe exactement un entier relatif dans l'intervalle $\left[-\dfrac{fy}{n}, -\dfrac{fy}{n} + \dfrac{25}{n}\right]$ ce qui détermine x de manière unique.

III. 3. a. M est un entier naturel et $M \geqslant 3 \times 3 - 1 = 8$.
$n = \dfrac{(cM + a)(dM + b) - 1}{M} = \dfrac{cdM^2 + (a + d)M + ab - 1}{M} = cdM + a + d + \dfrac{ab - 1}{M} = cdM + a + d + 1$. Donc, n est un entier naturel. De plus, $n \geqslant 3 \times 3 \times 8 + 3 + 3 + 1 \geqslant 26$.
$e = cM + a$ est un entier naturel non nul tel que $fe + (-M)n = 1$. D'après le théorème de BÉZOUT, les entiers n et e sont premiers entre eux. Donc, (n, e) est une clé de codage.
$n = \dfrac{ef - 1}{M}$ fournit $ef = 1 + nM$ puis $ef \equiv 1\ [n]$. Donc, f est une clé de décodage associée.

III. 3. b. $M = ab - 1 = 11$. $e = cM + a = 5 \times 11 + 3 = 58$. $f = dM + b = 6 \times 11 + 4 = 70$. $n = \dfrac{58 \times 70 - 1}{11} = 369$.

III. 3. c. • $58x \equiv 290\ [369] \Rightarrow 70 \times 58x \equiv 70 \times 290\ [369] \Rightarrow x \equiv 20300\ [369] \Rightarrow x \equiv 5\ [369]$. Puisque $0 \leqslant 5 \leqslant 25$, on a donc $x = 5$ qui le rang de la lettre F.
• $58x \equiv 232\ [369] \Rightarrow x \equiv 70 \times 232\ [369] \Rightarrow x \equiv 16240\ [369] \Rightarrow x \equiv 4\ [369]$. Puisque $0 \leqslant 4 \leqslant 25$, on a donc $x = 4$ qui le rang de la lettre E.
• $58x \equiv 248\ [369] \Rightarrow x \equiv 70 \times 248\ [369] \Rightarrow x \equiv 17360\ [369] \Rightarrow x \equiv 17\ [369]$. Puisque $0 \leqslant 17 \leqslant 25$, on a donc $x = 17$ qui le rang de la lettre R.
• $58x \equiv 327\ [369] \Rightarrow x \equiv 70 \times 327\ [369] \Rightarrow x \equiv 22890\ [369] \Rightarrow x \equiv 12\ [369]$. Puisque $0 \leqslant 12 \leqslant 25$, on a donc $x = 12$ qui le rang de la lettre M.
• $58x \equiv 0\ [369] \Rightarrow x \equiv 0\ [369]$. Puisque $0 \leqslant 0 \leqslant 25$, on a donc $x = 0$ qui le rang de la lettre A.
• $58x \equiv 364\ [369] \Rightarrow x \equiv 70 \times 364\ [369] \Rightarrow x \equiv 25480\ [369] \Rightarrow x \equiv 12\ [369]$. Puisque $0 \leqslant 12 \leqslant 25$, on a donc $x = 19$ qui le rang de la lettre T.

Le mot qui a été codé est FERMAT.

III. 4. a. r_N est le dernier reste non nul dans l'algorithme d'EUCLIDE (puisque $r_N > r_{N+1} = 0$). Donc, r_N est le PGCD de n et e ou encore $r_N = 1$.

III. 4. b. Montrons par récurrence que $\forall k \in [\![0, N]\!]$, $\exists\, (u_k, v_k) \in \mathbb{Z}^2 / \ r_k = nu_k + ev_k$.

• $r_0 = n = 1 \times n + 0 \times e$ et $r_1 = e = 0 \times n + 1 \times e$. Donc, la propriété à démontrer est vraie pour $k = 0$ et $k = 1$.
• Soit $k \in [\![1, N]\!]$. Supposons la propriété vraie pour $k - 1$ et k. Alors

$$r_{k+1} = r_{k-1} - r_k q_k = (nu_{k-1} + ev_{k-1}) - q_k (nu_k + ev_k) = n(u_{k-1} - q_k u_k) + e(v_{k-1} - q_k v_k).$$

$u_{k+1} = u_{k-1} - q_k u_k$ et $v_{k+1} = v_{k-1} - q_k v_k$ sont des entiers relatifs tels que $r_{k+1} = nu_{k+1} + ev_{k+1}$.

Le résultat est démontré par récurrence.

III. 4. c. En particulier, $nu_N + ev_N = r_N = 1$ et donc $ev_N \equiv 1\ [n]$. Une clé de décodage associée à la clé de codage (n, e) est le reste de la division euclidienne de v_N par n.

III. 4. d. Dans la case C4, on a écrit =C2-B3*C3 (et dans la case D4, on a écrit =D2-B3*D3 ou aussi =(A4-369*C4)/58).

III. 4. e. $369 = 6 \times 58 + 21$, $58 = 2 \times 21 + 16$, $21 = 1 \times 16 + 5$, $16 = 3 \times 5 + 1$ puis

$$\begin{aligned}1 &= 16 - 3\times 5\\ &= 16 - 3(21-16) = 4\times 16 - 3\times 21\\ &= 4\times(58 - 2\times 21) - 3\times 21 = 4\times 58 - 11\times 21\\ &= 4\times 58 - 11\times(369 - 6\times 58) = -11\times 369 + 70\times 58.\end{aligned}$$

Le couple $(u_0, v_0) = (-11, 70)$ est un couple d'entiers relatifs tel que $369u_0 + 58v_0 = 1$.

On en déduit que $70\times 58 \equiv 1\ [369]$ et donc une clé de décodage est $f = 70$.

III. 4. f. Soit $(u, v) \in \mathbb{Z}^2$.

$$369u + 58v = 1 \Leftrightarrow 369u + 58v = 369u_0 + 58v_0 \Leftrightarrow 369\,(u - u_0) = 58\,(v_0 - v)\,.$$

Si $369u + 58v = 1$, alors nécessairement l'entier 58 divise l'entier $369\,(u - u_0)$. Puisque les entiers 58 et 369 sont premiers entre eux, on en déduit que nécessairement l'entier 58 divise l'entier $u - u_0$ et donc il existe un relatif k tel que $u - u_0 = 58k$ ou encore $u = u_0 + 58k$. De même, il existe un entier relatif k' tel que $v_0 - v = 369k'$ ou encore $v = v_0 - 369k'$.

Soient alors $(k, k') \in \mathbb{Z}^2$ puis $u = u_0 + 58k$ et $v = v_0 - 369k'$.

$$369u + 58v = 369\,(u_0 + 58k) + 58\,(v_0 - 369k') = 369u_0 + 58v_0 + 58\times 369\times(k - k') = 1 + 58\times 369\times(k - k').$$

Donc, $369u + 58v = 1 \Leftrightarrow k = k'$. Les couples $(u, v) \in \mathbb{Z}^2$ tels que $369u + 58v = 1$ sont les couples de la forme $(-11 + 58k, 70 - 369k)$, $k \in \mathbb{Z}$.

Posons $f_0 = 70$. Une clé de décodage est un entier naturel f tel que $58f \equiv 1\ [369]$. Donc,

$$\begin{aligned}f \text{ est une clé de décodage} &\Leftrightarrow f \in \mathbb{N} \text{ et } 58f \equiv 58f_0\ [369] \Leftrightarrow f \in \mathbb{N} \text{ et } 58\,(f - f_0) \equiv 0\ [369]\\ &\Leftrightarrow f \in \mathbb{N} \text{ et } f - f_0 \equiv 0\ [369] \text{ (car 58 et 369 sont premiers entre eux)}\\ &\Leftrightarrow f \in \mathbb{N} \text{ et } \exists k \in \mathbb{Z}/\ f = 70 + 369k\\ &\Leftrightarrow \exists k \in \mathbb{N}/\ f = 70 + 369k.\end{aligned}$$

Les clés de décodage associées à la clé de codage $(369, 58)$ sont les entiers naturels de la forme $f = 70 + 369k$, $k \in \mathbb{N}$.

Partie B - Chiffrement de Hill

I. Question de cours.

I. 1. Soit A une matrice carrée d'ordre 2 à coefficients réels. A est inversible si et seulement si il existe $B \in \mathcal{M}_2(\mathbb{R}$ telle que $AB = BA = I_2$.

Soit A une matrice inversible. Soient B et C deux matrices telles que $AB = BA = I_2$ et $AC = CA = I_2$. Alors,

$$B = BI_2 = B(AC) = (BA)C = I_2C = C.$$

Ceci montre que la matrice B est unique en cas d'existence.

I. 2. $A^2 = \begin{pmatrix} a & b\\ c & d\end{pmatrix}\begin{pmatrix} a & b\\ c & d\end{pmatrix} = \begin{pmatrix} a^2+bc & b(a+d)\\ c(a+d) & bc+d^2\end{pmatrix}$ puis

$$\begin{aligned}A^2 - (a+d)A + (ad-bc)I_2 &= \begin{pmatrix} a^2+bc & b(a+d)\\ c(a+d) & bc+d^2\end{pmatrix} - (a+d)\begin{pmatrix} a & b\\ c & d\end{pmatrix} + (ad-bc)\begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix}\\ &= \begin{pmatrix} a^2+bc-(a+d)a+(ad-bc) & b(a+d)-b(a+d)\\ c(a+d)-c(a+d) & bc+d^2-(a+d)d+(ad-bc)\end{pmatrix}\\ &= \begin{pmatrix} 0 & 0\\ 0 & 0\end{pmatrix} = 0_2.\end{aligned}$$

I. 3. • Si $ad - bc \neq 0$, d'après la question I.1.,

$$I_2 = A\times\frac{1}{ad-bc}\,(-A + (a+d)I_2) = \frac{1}{ad-bc}\,(-A + (a+d)I_2)\times A.$$

Dans ce cas, A est inversible d'inverse $A^{-1} = \dfrac{1}{ad-bc}(-A+(a+d)I_2) = \dfrac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

• Si $ad-bc=0$, on a $A^2-(a+d)A = 0_2$ puis $A(A-(a+d)I_2) = 0_2$. Supposons par l'absurde que A soit inversible. En multipliant les deux membres de la dernière égalité par A^{-1}, on obtient $A-(a+d)I_2 = 0$. Donc, il existe $\lambda \in \mathbb{R}$ tel que $A = \lambda I_2$. L'égalité $ad-bc=0$ fournit $\lambda^2 = 0$ puis $\lambda = 0$ puis $A = 0_2$.
Mais, pour toute matrice carrée B d'ordre 2, $B \times 0_2 = 0_2 \neq I_2$. Donc, $A = 0_2$ n'est pas inversible ce qui est une contradiction avec l'hypothèse initiale.

Il était donc absurde de supposer la matrice A inversible et finalement la matrice A n'est pas inversible.

On a montré que A est inversible si et seulement si $ad-bc \neq 0$.

II. 1. Soit $A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$. A est une matrice carrée à coefficients dans $\mathbb{Z}$. $2\times 1 - 0\times 0 = 2 \neq 0$ et donc la matrice A est inversible. De plus, $A^{-1} = \begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix}$ et les coefficients de A^{-1} ne sont pas tous dans $\mathbb{Z}$.

II. 2. Si $ad-bc \in \{-1,1\}$, alors $A^{-1} = \pm\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ et en particulier, A^{-1} est à coefficients dans $\mathbb{Z}$. Donc, ($ad-bc=1$ ou $ad-bc=-1$) est une condition suffisante pour que A^{-1} soit à coefficients dans $\mathbb{Z}$.

II. 3. Soit A une matrice carrée d'ordre 2, à coefficients entiers relatifs, inversible d'inverse A^{-1} à coefficients entiers relatifs. On sait que $ad-bc = \det(A) \neq 0$ et que $\det(A)$ est un entier relatif.
De même, $\det\left(A^{-1}\right)$ est un entier relatif non nul. Mais $\det\left(A^{-1}\right) = \dfrac{1}{\det(A)}$. Donc, nécessairement, $\det(A)$ est un entier relatif non nul dont l'inverse est aussi un entier relatif non nul. On en déduit que $\det(A) \in \{-1,1\}$ (car dans le cas contraire, $|\det(A)| \geqslant 2$ puis $0 < \left|\dfrac{1}{\det(A)}\right| \leqslant \dfrac{1}{2}$ ce qui contredit le fait que $\dfrac{1}{\det(A)}$ est un entier).

En résumé, A est inversible, d'inverse à coefficients dans $\mathbb{Z}$ si et seulement si $ad-bc \in \{-1,1\}$.

III. 1. $(S) \Leftrightarrow \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$.

III. 2. a. • Le rang de B est $x=1$ et le rang de E est $y=4$.

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 4 & 3 \\ 5 & 4 \end{pmatrix}\begin{pmatrix} 1 \\ 4 \end{pmatrix} = \begin{pmatrix} 16 \\ 21 \end{pmatrix}.$$

Ainsi, $x' \equiv 16\ [26]$ avec $0 \leqslant 16 \leqslant 25$ et $y' \equiv 21\ [26]$ avec $0 \leqslant 21 \leqslant 25$. Donc $x'=16$ et $y'=21$. La lettre de rang $x'=16$ est Q et la lettre de rang 21 est V. Donc BE est codé par QV.

• Le rang de Z est $x=25$ et le rang de O est $y=14$.

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 4 & 3 \\ 5 & 4 \end{pmatrix}\begin{pmatrix} 25 \\ 14 \end{pmatrix} = \begin{pmatrix} 142 \\ 181 \end{pmatrix}.$$

Ainsi, $x' \equiv 12\ [26]$ avec $0 \leqslant 12 \leqslant 25$ et $y' \equiv 25\ [26]$ avec $0 \leqslant 25 \leqslant 25$. Donc $x'=12$ et $y'=25$. La lettre de rang $x'=12$ est M et la lettre de rang 25 est Z. Donc ZO est codé par MZ.

• Le rang de U est $x=20$ et le rang de T est $y=19$.

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 4 & 3 \\ 5 & 4 \end{pmatrix}\begin{pmatrix} 20 \\ 19 \end{pmatrix} = \begin{pmatrix} 137 \\ 176 \end{pmatrix}.$$

Ainsi, $x' \equiv 7\ [26]$ avec $0 \leqslant 7 \leqslant 25$ et $y' \equiv 20\ [26]$ avec $0 \leqslant 20 \leqslant 25$. Donc $x'=7$ et $y'=20$. La lettre de rang $x'=7$ est H et la lettre de rang 20 est U. Donc UT est codé par HU.

Finalement, le mot BEZOUT est codé par QVMZHU.

III. 2. b. A est inversible d'inverse $A^{-1} = \dfrac{1}{4\times 4 - 3\times 5}\begin{pmatrix} 4 & -3 \\ -5 & 4 \end{pmatrix} = \begin{pmatrix} 4 & -3 \\ -5 & 4 \end{pmatrix}$.
Les lettres S F X M O J ont pour rangs respectifs

$$18 \quad 5 \quad 23 \quad 12 \quad 14 \quad 9$$

• Les lettres S et F ont pour rangs respectifs $x'=18$ et $y'=5$.

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 4 & -3 \\ -5 & 4 \end{pmatrix}\begin{pmatrix} 18 \\ 5 \end{pmatrix} = \begin{pmatrix} 57 \\ -70 \end{pmatrix}.$$

Ainsi, $x \equiv 5\ [26]$ avec $0 \leqslant 5 \leqslant 25$ et $y \equiv 8\ [26]$ avec $0 \leqslant 8 \leqslant 25$. Donc $x = 5$ et $y = 8$. La lettre de rang $x = 5$ est F et la lettre de rang 8 est I. Donc SF code FI.

• Les lettres X et M ont pour rangs respectifs $x' = 23$ et $y' = 12$.

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 4 & -3 \\ -5 & 4 \end{pmatrix} \begin{pmatrix} 23 \\ 12 \end{pmatrix} = \begin{pmatrix} 56 \\ -67 \end{pmatrix}.$$

Ainsi, $x \equiv 4\ [26]$ avec $0 \leqslant 4 \leqslant 25$ et $y \equiv 11\ [26]$ avec $0 \leqslant 8 \leqslant 25$. Donc $x = 4$ et $y = 11$. La lettre de rang $x = 4$ est E et la lettre de rang 11 est L. Donc XM code EL.

• Les lettres O et J ont pour rangs respectifs $x' = 14$ et $y' = 9$.

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 4 & -3 \\ -5 & 4 \end{pmatrix} \begin{pmatrix} 14 \\ 9 \end{pmatrix} = \begin{pmatrix} 29 \\ -34 \end{pmatrix}.$$

Ainsi, $x \equiv 3\ [26]$ avec $0 \leqslant 3 \leqslant 25$ et $y \equiv 18\ [26]$ avec $0 \leqslant 18 \leqslant 25$. Donc $x = 3$ et $y = 18$. La lettre de rang $x = 3$ est D et la lettre de rang 18 est S. Donc OJ code DS.

Finalement, SFXMOJ code le mot FIELDS.

III. 3. Ici, $A = \begin{pmatrix} 3 & 2 \\ 1 & 3 \end{pmatrix}$ puis $A^{-1} = \frac{1}{7}\begin{pmatrix} 3 & -2 \\ -1 & 3 \end{pmatrix}$.

III. 3. a. Les entiers 7 et $26 = 2 \times 13$ sont premiers entre eux car sans facteur premier commun. $15 \times 7 = 105 = 4 \times 26 + 1$ et donc $15 \times 7 \equiv 1\ [26]$. Donc $u = 15$ est un entier compris au sens large entre 0 et 25 tel que $7u \equiv 1\ [26]$.
D'autre part, d'après la question A-III.4.f., les entiers relatifs f tels que $7f \equiv 1\ [26]$ sont les entiers de la forme $f = 15 + 26k$, $k \in \mathbb{Z}$.

$$0 \leqslant 15 + 26k \leqslant 25 \Leftrightarrow -\frac{15}{26} \leqslant k \leqslant -\frac{15}{26} + \frac{25}{26} \Leftrightarrow k = 0.$$

Ceci montre l'unicité de l'entier u.

III. 3. b. Soit $B = 7A^{-1} = \begin{pmatrix} 3 & -2 \\ -1 & 3 \end{pmatrix}$. On a

$$uBA = 7uA^{-1}A = 7uI_2 \equiv I_2\ [26].$$

Donc la matrice B convient.

III. 3. c. Le décodage se mène alors de la façon suivante

$$\begin{aligned} A\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x' \\ y' \end{pmatrix} &\Rightarrow uBA\begin{pmatrix} x \\ y \end{pmatrix} = uB\begin{pmatrix} x' \\ y' \end{pmatrix} \Rightarrow I_2\begin{pmatrix} x \\ y \end{pmatrix} \equiv uB\begin{pmatrix} x' \\ y' \end{pmatrix}\ [26] \\ &\Rightarrow \begin{pmatrix} x \\ y \end{pmatrix} \equiv 15\begin{pmatrix} 3 & -2 \\ -1 & 3 \end{pmatrix}\begin{pmatrix} x' \\ y' \end{pmatrix}\ [26] \Rightarrow \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 45x' - 30y' \\ -15x' + 45y' \end{pmatrix}\ [26] \\ &\Rightarrow \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} -7x' - 4y' \\ 11x' - 7y' \end{pmatrix}\ [26]. \end{aligned}$$

• Les lettres A et K ont pour rang respectifs $x' = 0$ et $y' = 10$. $\begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} -40 \\ -70 \end{pmatrix}\ [26]$ puis $\begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 12 \\ 8 \end{pmatrix}\ [26]$. AK code MI

• Les lettres X et O ont pour rang respectifs $x' = 23$ et $y' = 14$. $\begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} -217 \\ 155 \end{pmatrix}\ [26]$ puis $\begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 17 \\ 25 \end{pmatrix}\ [26]$. XO code RZ

• Les lettres U et E ont pour rang respectifs $x' = 20$ et $y' = 4$. $\begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} -156 \\ 192 \end{pmatrix}\ [26]$ puis $\begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 10 \end{pmatrix}\ [26]$. UE code AK

• Les lettres V et H ont pour rang respectifs $x' = 21$ et $y' = 7$. $\begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} -175 \\ 182 \end{pmatrix}\ [26]$ puis $\begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 0 \end{pmatrix}\ [26]$. VH code HA

• Les lettres D et L ont pour rang respectifs $x' = 3$ et $y' = 11$. $\begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} -65 \\ -44 \end{pmatrix}\ [26]$ puis $\begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 13 \\ 8 \end{pmatrix}\ [26]$. DL code NI

Finalement, AKXOUEVHDL code MIRZAKHANI (première femme à avoir reçu la médaille Fields (2014)).

III. 4. Dans le cas général, posons $B = \det(A)A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. La matrice B est inversible d'inverse $\frac{1}{\det(A)}A$.

$A\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x' \\ y' \end{pmatrix} \Leftrightarrow BA\begin{pmatrix} x \\ y \end{pmatrix} = B\begin{pmatrix} x' \\ y' \end{pmatrix} \Leftrightarrow \begin{cases} (\det(A))x = dx' - by' \\ (\det(A))y = -cx' + ay' \end{cases}$.

Si $\det(A)$ est premier à 26, $\det(A)$ possède un inverse u modulo 26 et dans ce cas, on peut décoder : $\begin{cases} x \equiv u(dx' - by') \ [26] \\ y \equiv u(-cx' + ay') \ [26] \end{cases}$.

On peut décoder si $\det(A)$ est premier à 26.

Problème 2

Partie A

I. 1. Les 16 chemins sont
$(1,1,1,1)$
$(1,1,1,0)$
$(1,1,0,1)$
$(1,1,0,0)$
$(1,0,1,1)$
$(1,0,1,0)$
$(1,0,0,1)$
$(1,0,0,0)$
$(0,1,1,1)$
$(0,1,1,0)$
$(0,1,0,1)$
$(0,1,0,0)$
$(0,0,1,1)$
$(0,0,1,0)$
$(0,0,0,1)$
$(0,0,0,0)$

I. 2. Il y a 6 chemins qui contiennent deux fois l'élément 1 :
$(1,1,0,0)$
$(1,0,1,0)$
$(1,0,0,1)$
$(0,1,1,0)$
$(0,1,0,1)$
$(0,0,1,1)$

I. 3. Parmi les 6 chemins contenant deux fois l'élément 1,
il y en a 3 avec un 1 en première place,
$(1,1,0,0)$
$(1,0,1,0)$
$(1,0,0,1)$
il y en a 3 avec un 1 en deuxième place,
$(1,1,0,0)$
$(0,1,1,0)$
$(0,1,0,1)$
il y en a 3 avec un 1 en troisième place,
$(1,0,1,0)$
$(0,1,1,0)$
$(0,0,1,1)$
il y en a 3 avec un 1 en quatrième place,
$(1,0,0,1)$
$(0,1,0,1)$
$(0,0,1,1)$

II. 1. Soit $k \in [\![0, n]\!]$. Un chemin contient k fois l'élément 1 si et seulement si il contient $n-k$ fois l'élément 0. $\binom{n}{k}$ est donc le nombre de chemins contenant $n-k$ fois l'élément 0. En remplaçant les 0 par des 1 et les 1 par des 0 dans ces chemins, on ne change pas le nombre de ces chemins. Donc, $\binom{n}{k}$ est donc le nombre de chemins contenant $n-k$ fois l'élément 1 c'est-à-dire $\binom{n}{n-k}$. Ainsi,

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

II. 2. Soit $k \in [\![1, n]\!]$. Le nombre de $(n+1)$-uplets contenant k fois l'élément 1 est $\binom{n+1}{k}$. Ces $(n+1)$-uplets sont de deux types disjoints.

- Type I : les $(n+1)$-uplets contenant k fois l'élément 1, le dernier élément étant un 0,
- Type II : les $(n+1)$-uplets contenant k fois l'élément 1, le dernier élément étant un 1.

Un $(n+1)$-uplet du type I est constitué d'un n-uplet contenant k fois l'élément 1 puis de l'élément 0. Il y a $\binom{n}{k}$ tels $(n+1)$-uplets.

Un $(n+1)$-uplet du type II est constitué d'un n-uplet contenant $k-1$ fois l'élément 1 puis de l'élément 1. Il y a $\binom{n}{k-1}$ tels $(n+1)$-uplets.

Puisque les types I et II sont disjoints, on a montré que

$$\boxed{\forall k \in [\![1, n]\!],\ \binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}.}$$

II. 3. a. Une ligne est un chemin contenant k fois l'élément 1 et $n-k$ fois l'élément 0. Donc la somme des éléments d'une ligne est égale à k.

II. 3. b. La somme des éléments de la j-ème colonne est le nombre de 1 dans cette colonne ou encore le nombre de chemins à k succès et $n-k$ échecs comportant un 1 à la j-ème position.

II. 3. c. La somme des éléments d'une ligne est égale à k et il y a $\binom{n}{k}$ lignes. Donc, la somme de tous les coefficients de la matrice est égale à $k\binom{n}{k}$ (somme obtenue en additionnant en ligne).

Soit $j \in \mathbb{N}$. L'application qui, à un n-uplet comportant k fois l'élément 1 avec un 1 en j-ème position associe le $n-1$-uplet obtenu en effaçant le 1 en j-ème position est bien sûr une bijection de l'ensemble des n-uplets comportant comportant k fois l'élément 1 avec un 1 en j-ème position sur l'ensemble des $n-1$-uplets comportant $k-1$ fois l'élément 1. Le nombre de ces n-uplets est donc $\binom{n-1}{k-1}$.

Ainsi, la somme des éléments de la colonne j est $\binom{n-1}{k-1}$. Puisqu'il y a n colonnes, la somme de tous les coefficients de la matrice est aussi égale à $n\binom{n-1}{k-1}$ (somme obtenue en additionnant en colonne). Finalement,

$$\boxed{\forall k \in [\![1, n]\!],\ k\binom{n}{k} = n\binom{n-1}{k-1}.}$$

II. 4. a. Soit E un ensemble à n éléments. Les éléments de E peuvent se noter de manière ordonnée $x_1, \dots, x_n$. Chaque partie F de E est alors uniquement défini par un chemin dans l'arbre du début de la partie A : à la p-ème étape, on va vers 1 si x_p est dans F (succès) et vers 0 si x_p n'est pas dans F. Le nombre de parties à p éléments de E est alors aussi le nombre de chemins à p succès (et $n-p$ échecs).

II. 4. b. Soit $k \in [\![1, n]\!]$.

$$\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1} = \frac{n}{k} \times \frac{n-1}{k-1} \times \dots \times \frac{n-k+1}{1}\binom{n-k}{0}.$$

$\binom{n-k}{0}$ est le nombre de parties à 0 élément d'un ensemble à $n-k$ éléments. Il n'y en a qu'une à savoir $\varnothing$. Donc, $\binom{n-k}{0} = 1$ puis

$$\binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k!} = \frac{n(n-1)\dots(n-k+1)(n-k)(n-k-1)\dots 1}{k!(n-k)(n-k-1)\dots 1} = \frac{n!}{k!(n-k)!}.$$

Cette égalité reste vraie quand $k = 0$ car $0! = 1$.

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

II. 4. c. Soit $k \in [\![1,n]\!]$.

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

et

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n}{k}\frac{(n-1)!}{(k-1)!((n-1)-(k-1))!} = \frac{n}{k}\binom{n-1}{k-1}$$

et donc $k\binom{n}{k} = n\binom{n-1}{k-1}$.

III. X suit la loi binomiale de paramètres n et θ puis

$$\begin{aligned}E(X) &= \sum_{k=0}^{n} kP(X=k) = \sum_{k=1}^{n} k\binom{n}{k}\theta^k(1-\theta)^{n-k} = \sum_{k=1}^{n} n\binom{n-1}{k-1}\theta^k(1-\theta)^{n-k} \\ &= np\sum_{k=1}^{n}\binom{n-1}{k-1}\theta^{k-1}(1-\theta)^{(n-1)-(k-1)} = n\theta\sum_{l=0}^{n-1}\binom{n-1}{l}\theta^l(1-\theta)^{(n-1)-l} \\ &= n\theta,\end{aligned}$$

car si Y est une variable aléatoire suivant une loi binomiale de paramètres $n-1$ et θ (ce qui permet de ne pas utiliser la formule du binôme de Newton : $\sum_{l=0}^{n-1}\binom{n-1}{l}\theta^l(1-\theta)^{(n-1)-l} = (\theta+(1-\theta))^{n-1} = 1$),

$$\sum_{l=0}^{n-1}\binom{n-1}{l}\theta^l(1-\theta)^{(n-1)-l} = \sum_{l=0}^{n-1} P(Y=l) = 1.$$

Partie B

I. 1. D_4 prend les valeurs 0, 1, 2, 3, 4 et D_4 suit une loi binomiale de paramètres $n=4$ et $p=\frac{1}{2}$.
X_4 prend les valeurs 4 (si on a obtenu 4 fois pile), 2 si on a obtenu 3 fois pile, 0 (si on a obtenu 2 fois pile), -2 (si on a obtenu 1 fois pile), -4 (si on a obtenu 0 fois pile).

En fait, $X_4 = 1\times D_4 + (-1)\times(4-D_4) = 2D_4 - 4$ puis pour $k \in [\![0,4]\!]$,

$$D_4 = k \Leftrightarrow 2D_4 - 4 = 2k-4 \Leftrightarrow X_4 = 2k-4.$$

Donc, pour tout $k \in [\![0,4]\!]$, les événements $(D_4 = k)$ et $(X_4 = 2k-4)$ sont égaux. On en déduit que pour tout $k \in [\![0,4]\!]$,

$$P(X_4 = 2k-4) = \binom{4}{k}\left(\frac{1}{2}\right)^k\left(\frac{1}{2}\right)^{4-k} = \frac{\binom{4}{k}}{16}.$$

I. 2. D_n suit la loi binomiale de paramètres n et $p=\frac{1}{2}$.

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

I. 4. $E(X_n) = 2E(D_n) - n = 2\times n\times\frac{1}{2} - n = 0$. Ceci signifie qu'au bout d'un grand nombre de déplacements, en moyenne, le point mobile est en l'origine.

$$\boxed{E(X_n) = 0.}$$

II. 1. La parité de l'abscisse du point mobile change à chaque déplacement. Puisque qu'au départ, le point mobile a pour abscisse 0 qui est un nombre pair, l'abscisse du point mobile est un nombre impair au bout d'un nombre impair de déplacement et en particulier, l'abscisse du point mobile n'est pas nulle. Donc,

$$\boxed{\text{si } n \text{ est impair, } P(X_n = 0) = 0.}$$

II. 2. $X_{2n} = 0 \Leftrightarrow 2D_{2n} - 2n = 0 \Leftrightarrow D_{2n} = n$. Donc,

$$P(X_{2n} = 0) = P(D_{2n} = n) = \frac{\binom{2n}{n}}{2^{2n}}.$$

$$\boxed{\forall n \in \mathbb{N}^*,\ P(X_{2n} = 0) = \frac{\binom{2n}{n}}{2^{2n}}.}$$

III. 1. Dans l'algorithme proposé, on part de 0 et à chaque étape, on ajoute 1 avec une chance sur deux et on retranche 1 avec une chance sur deux. Cet algorithme simule donc la marche aléatoire de cette partie B et renvoie l'abscisse du point mobile au bout de n étapes.

III. 2. Dans l'algorithme ci-dessous, on ne compte pas la position initiale en l'origine.

```
entrer (n)
x ← 0
c ← 0
pour k allant de 1 à n
        si alea () > 0,5 alors
                x ← x + 1
        sinon
                x ← x − 1
        finsi
si x = 0 alors
                c ← c + 1
        finsi
finpour
retourner (c)
```

III. 3.

```
entrer (n)
C ← 0
pour i allant de 1 à 1000
        x ← 0
        c ← 0
        pour k allant de 1 à n
                si alea () > 0,5 alors
                        x ← x + 1
                sinon
                        x ← x − 1
                finsi
        si x = 0 alors
                c ← c + 1
                finsi
        finpour
        C ← C+c
finpour
retourner (C/1000)
```


III. 4. • Les deux premiers algorithmes sont peu utilisables en tant que tels. Le premier fournit une valeur possible de l'abscisse finale du point mobile mais ne pourrait permettre de conjecturer les valeurs prises par cette abscisse que si on le répétait un grand nombre de fois. Le deuxième algorithme fournit une valeur du nombre de passages en l'origine mais ne pourrait permettre de conjecturer le nombre de passage moyen par exemple (déterminé à la dernière question du problème) que si on le répétait un grand nombre de fois.

• En répétant 1000 séries de n lancers, la fréquence d'apparition de l'événement $X_n = 0$ devrait être environ sa probabilité (calculée aux questions II.1 et II.2.). Le professeur peut alors faire dégager l'idée qu'une probabilité est la limite d'une suite de fréquences (loi faible des grands nombres) à partir du troisième algorithme.

IV. 1. Notons x_{2n} l'abscisse du point mobile au bout de $2n$ lancers.

$$-2n = \underbrace{-1-1-\ldots-1}_{2n} \leqslant x_{2n} \leqslant \underbrace{1+1+\ldots+1}_{2n} = 2n.$$

De plus, comme on l'a déjà expliqué à la question II.1., x_{2n} est nécessairement un entier pair.

IV. 2. Réciproquement, pour $k \in [\![-n, n]\!]$, l'abscisse $2k$ est obtenue en se déplaçant $n+k$ fois vers la droite et $n-k$ fois vers la gauche. Donc, l'ensemble des valeurs prises par la variable X_{2n} est $\{2k,\ k \in [\![-n, n]\!]\}$.

Soit $k \in [\![0, n]\!]$. $X_{2n} = 2k \Leftrightarrow 2D_{2n} - 2n = 2k \Leftrightarrow D_{2n} = n + k$ puis

$$P(X_{2n} = 2k) = P(D_{2n} = n-k) = \frac{\binom{2n}{n+k}}{2^{2n}}.$$

IV. 3. Soit $k \in [\![0, 2n]\!]$. On note Ω_k la variable aléatoire égale à 1 si, à l'issue du k-ème lancer, l'abscisse du point est nulle et à 0 sinon. On a alors $C_n = \Omega_2 + \Omega_4 + \ldots + \Omega_{2n}$ puis, par linéarité de l'espérance

$$E(C_n) = \sum_{k=1}^{2n} E(\Omega_{2k}).$$

Ensuite, pour $k \in [\![1, n]\!]$, $\Omega_{2k} = 1 \Leftrightarrow X_{2k} = 0$ et donc

$$E(\Omega_k) = 0 \times P(\Omega_k = 0) + 1 \times P(\Omega_k = 1) = P(X_{2k} = 0) = \frac{\binom{2k}{k}}{2^{2k}}.$$

Donc,

$$E(C_n) = \sum_{k=1}^{n} \frac{\binom{2k}{k}}{2^{2k}} = \left(\sum_{k=0}^{n} \frac{\binom{2k}{k}}{4^k}\right) - 1.$$

Montrons par récurrence que $\forall n \in \mathbb{N}^*$, $\displaystyle\sum_{k=0}^{n} \frac{\binom{2k}{k}}{4^k} = \frac{2n+1}{4^n}\binom{2n}{n}$.

- $\displaystyle\sum_{k=0}^{1} \frac{\binom{2k}{k}}{2^{2k}} = 1 + \frac{2}{4} = \frac{3}{2}$ et $\displaystyle\frac{2\times 1+1}{4^1}\binom{2}{1} = \frac{3}{2}$. La formule à démontrer est donc vraie quand $n = 1$.

- Soit $n \geqslant 1$. Supposons que $\displaystyle\sum_{k=0}^{n} \frac{\binom{2k}{k}}{4^k} = \frac{2n+1}{4^n}\binom{2n}{n}$. Alors,

$$\begin{aligned}\sum_{k=0}^{n+1}\frac{\binom{2k}{k}}{4^k} &= \sum_{k=0}^{n}\frac{\binom{2k}{k}}{4^k}+\frac{\binom{2n+2}{n+1}}{4^{n+1}}\\ &= \frac{2n+1}{4^n}\binom{2n}{n}+\frac{\binom{2n+2}{n+1}}{4^{n+1}} \text{ (par hypothèse de récurrence)}\\ &= \frac{1}{4^{n+1}}\left(4(2n+1)\binom{2n}{n}+\binom{2n+2}{n+1}\right) = \frac{1}{4^{n+1}}\left(4(2n+1)\frac{(n+1)^2}{(2n+1)(2n+2)}+1\right)\binom{2n+2}{n+1}\\ &= \frac{2(n+1)+1}{4^{n+1}}\binom{2n+2}{n+1}.\end{aligned}$$

On a montré par récurrence que

$$\boxed{\forall n\in\mathbb{N}^*,\ E(C_n)=\frac{2n+1}{4^n}\binom{2n}{n}-1.}$$

