

Correction CAPE 2015: 2^{ème} épreuve

Problème n°1

Partie A

I. 1. Supposons $\exists u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

Soit $d \in \mathbb{Z}$ tel que d/a et d/b
/ ne soit "divisor"

alors $d/a + b/v = 1$ donc $d = \pm 1$.

Donc les seuls diviseurs communs de a et de b sont 1 et -1

c-à-d a et b sont premiers entre eux.

2 a) Comme $a \neq 0$ a ou $-a \in \mathbb{N}^*$
Or $a = a \times 1 + b \times 0 \in \mathcal{E}$
 $-a = a \times -1 + b \times 0 \in \mathcal{E}$ } donc a ou $-a \in \mathcal{E} \cap \mathbb{N}^*$

$\mathcal{E} \cap \mathbb{N}^*$ est une partie non vide de $\mathbb{N}^*$ donc
admet un plus petit élément m_0 .

b) Soient $q \in \mathbb{Z}$, $r \in \mathbb{N}$ tel que $a = m_0 q + r$ $r < m_0$

Montrons $\mathcal{E}$ est un idéal de $\mathbb{Z}$

- $0 = a \times 0 + b \times 0 \in \mathcal{E}$

- Soient $x, y \in \mathcal{E}$ $x = au + bv$, $y = aw + bt$

alors $x + y = a(u+w) + b(v+t) \in \mathcal{E}$

- Soient $x \in \mathcal{E}$. Soit $q \in \mathbb{Z}$.

$x = au + bv$ donc $qx = a(qu) + b(qv) \in \mathcal{E}$

Comme $a \in \mathcal{E}$ et $m_0 \in \mathcal{E}$

$r = a + (-q)m_0 \in \mathcal{E}$ car $\mathcal{E}$ est un idéal

Supposons $r \neq 0$. Alors $r \in \mathcal{E} \cap \mathbb{N}^*$ $r < m_0$ qui est

le plus petit élément de $\mathbb{N}^*$. Contradiction donc $z = 0$ (2)
 De même avec b

e) Supposons maintenant que a et b sont premiers entre eux.

d'après b) m_0 est un diviseur commun de a et de b

donc $m_0 = 1$.

Par définition, $m_0 \in \mathbb{Z}$. Donc $\exists u, v \in \mathbb{Z}$ tel que

$$au + bv = m_0 = 1.$$

3) Théorème

a et b sont premiers entre eux (i.e. les seuls diviseurs communs de a et de b sont 1 et -1)

soi il existe $u, v \in \mathbb{Z}$ tel que $au + bv = 1$.

II Supposons que $a \nmid bc$ et que a et b sont premiers entre eux.

d'après I, il existe $u, v \in \mathbb{Z}$ tel que $au + bv = 1$

donc $c = acu + bcv$

$a \nmid bc$ donc $a \nmid (bcv + acu) = c$.

$a \nmid ac$

III

1.

lettre	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
rang	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

lettre	v	w	x	y	z
rang	21	22	23	24	25

a)	G	A	V	S	S
rang	6	0	20	18	18
codeage	348	0	53	306	306

$$\begin{array}{r} 58 \\ \times 6 \\ \hline 348 \end{array}$$

$$\begin{array}{r} 58 \\ \times 20 \\ \hline 1160 \\ - 1107 \\ \hline 53 \end{array}$$

$$\begin{array}{r} 369 \\ / 3 \\ \hline 123 \end{array}$$

$$\begin{array}{r} 369 \\ \times 3 \\ \hline 1107 \end{array}$$

$$\begin{array}{r} 58 \\ \times 18 \\ \hline 464 \\ 58 \\ \hline 1044 \\ - 738 \\ \hline 306 \end{array}$$

$$\begin{array}{r} 369 \\ \times 2 \\ \hline 738 \end{array}$$

b) A l'aide d'un tableau, faire un tableau

- 1^{re} ligne Les 26 lettres de l'alphabet
 2^{ème} ligne Les rangs $\times$
 3^{ème} ligne Le reste y de la division euclidienne de 58 et par 369.

2. a) m et e sont premiers entre eux. Donc d'après I,

(4)

$$\exists f, m \in \mathbb{Z} \text{ tel que } ef + m = 1$$

$$\text{donc } \exists f \in \mathbb{Z} \text{ tel que } ef \equiv 1 \pmod{m}.$$

En prenant le assez grand $f + km \in \mathbb{N}$ et vérifie aussi $e(f + km) \equiv 1 \pmod{m}$

b) $ex \equiv y \pmod{m}$

$$\text{donc } ef x \equiv f y \pmod{m}$$

$$\text{Car } ef \equiv 1 \pmod{m} \quad x \equiv ef x \equiv f y \pmod{m}$$

$$\text{Donc } x \text{ est la reste de } f y = qm + x$$

$$\text{car } 0 \leq x < 25 < m$$

x est la reste de la division euclidienne de $f y$

3. a) $e \equiv a \pmod{M}, f \equiv b \pmod{M}$ donc $ef - 1 \equiv ab - 1 \equiv 0 \pmod{M}$ donc $m \in \mathbb{N}$
 $ef + n(-M) = 1$ donc e et m premiers entre eux
 et $ef \equiv 1 \pmod{m}$

$$a, b, c \geq 3 \text{ donc } M \geq 3 \times 3 - 1 = 8$$

$$\text{donc } e \geq 3 \times 8 + 3 = 27 \quad f = dM + b \geq 3M$$

$$\text{donc } m = \frac{ab-1}{M} \geq \frac{e \cdot 3M - 1}{M} \geq e - \frac{1}{M} \geq 27 - 1 = 26$$

donc (m, e) est une clé de codage

et f est une clé de décodage aussi

2) $M = 11 \quad e = 5 \times 11 + 3 = 58$

$$f = 6 \times 11 + 4 = 70$$

$$m = \frac{58 \times 70 - 1}{11} = \frac{4059}{11} = 369$$

$$\begin{array}{r} 58 \\ 70 \\ \hline 4060 \end{array}$$

$$\begin{array}{r} 4059 \\ - 33 \\ \hline 75 \\ - 66 \\ \hline 9 \end{array}$$

$$\begin{array}{r} 11 \\ \hline 369 \end{array}$$

(5)

y	290 70 ⁶	232 70 ^{1/2}	248 70 ^{3/8}	327 70 ^{1/4}	0	364 70 ²
by	20300	16240	17360	22890	0	25480
x	5	4	17	12	0	19
	F	E	R	M	A	T

$$\begin{array}{r} 20300 \\ - 1845 \\ \hline 1850 \\ - 1845 \\ \hline 5 \end{array} \quad \begin{array}{r} 369 \\ \hline 55 \end{array}$$

$$\begin{array}{r} 16240 \\ - 1476 \\ \hline 01480 \\ - 1476 \\ \hline 4 \end{array} \quad \begin{array}{r} 369 \\ \hline 44 \end{array}$$

$$\begin{array}{r} 17360 \\ - 1476 \\ \hline 02600 \\ - 2583 \\ \hline 17 \end{array} \quad \begin{array}{r} 369 \\ \hline 47 \end{array}$$

$$\begin{array}{r} 22890 \\ - 2214 \\ \hline 750 \\ - 739 \\ \hline 11 \end{array} \quad \begin{array}{r} 369 \\ \hline 62 \end{array}$$

x	1	2	3	4	5	6	7	8	9
	369	738	1476	1845	2214	2583			3321

$$\begin{array}{r} 25480 \\ - 2214 \\ \hline 03340 \\ - 3321 \\ \hline 19 \end{array} \quad \begin{array}{r} 369 \\ \hline 64 \end{array}$$

Le mot est FERMAT

4 a) $\forall k \in [1, n] \quad r_{k-1} = r_k q_k + r_{k+1}$

donc $\text{pgcd}(r_{k-1}, r_k) = \text{pgcd}(r_k, r_{k+1})$

donc $\text{pgcd}(r_0, r_1) = \text{pgcd}(r_N, r_{N+1})$
 $k=1$ $k=N$

(6)

Comme $r_{N+1} = 0$ $\text{pgcd}(r_N, r_{N+1}) = r_N$

donc $r_N = \text{pgcd}(m, e) = 1$.

B) Démonstration par récurrence double

$\forall k \in [0, N] \quad r_k = m u_k + e v_k$

$k=0 \quad r_0 = m \times 1 + e \times 0$

$k=1 \quad r_1 = m \times 0 + e \times 1$

Supposons $\left\{ \begin{array}{l} r_{k-1} = m u_{k-1} + e v_{k-1} \text{ pour un } k \text{ quelconque} \\ r_k = m u_k + e v_k \quad k \in [1, N] \end{array} \right.$

Alors

$r_{k+1} = r_{k-1} - r_k q_k = m u_{k-1} + e v_{k-1} - m u_k q_k - e v_k q_k$

$= m (u_{k-1} - u_k q_k) + e (v_{k-1} - v_k q_k)$

donc $u_{k+1} = u_{k-1} - u_k q_k$ et $v_{k+1} = v_{k-1} - v_k q_k$

C) D'après B) pour $k=N$

$r_N = m u_N + e v_N$ donc $e v_N = 1 \pmod{N}$

D'après a) $r_N = 1$

v_N est une des décomposées

d) La formule est

$$u_{k+1} = u_{k-1} - u_k q_k, \quad v_{k+1} = v_{k-1} - v_k q_k$$

Verifions

$$u_2 = u_0 - u_1 q_1$$

$$u_0 = 1 \quad u_1 = 0 \quad \text{donc} \quad u_2 = 1$$

$$v_2 = v_0 - v_1 q_1$$

$$v_0 = 0 \quad v_1 = 1$$

$$n = 369 \quad e = 58$$

$$369 = 58 \times 6 + 21$$

$$q_2 = 6 \quad r_2 = 21$$

$$\text{donc } v_2 = -6$$

$$21 = 16 \times 1 + 5$$

$$16 = 5 \times 3 + 1$$

$$5 = 1 \times 5 + 0$$

e)	Je complete le tableau			
6	5	3	$1 - (-2) \times 1$ $= 3$	$-6 - 13 \times 1$ $= -19$
7	1	5	$-2 - 3 \times 3$ $= -11$	$13 - (-19) \times 3$ $= 70$
8	0			

$$\text{On trouve } 369 \times (-11) + 58 \times 70 = -6273$$

Autre methode

$$\text{au 3 a) on a un que } e f + n (-M) = 1$$

$$\text{c a d } 58 \times 70 + 369 \times (-11) = 1$$

f) Soient $(u, v) \in \mathbb{Z}^2$

$$369u + 58v = 1 \Leftrightarrow 369u + 58v = 369 \times (-11) + 58 \times 70 \quad (8)$$

$$\Leftrightarrow 369(u+11) + 58(v-70) = 0$$

$$\Rightarrow \left. \begin{array}{l} 369 \mid 58(v-70) \\ 369 \wedge 58 = 1 \end{array} \right\} \begin{array}{l} \text{D'après Gauss} \\ 369 \mid v-70 \end{array}$$

$$\text{donc } v-70 = k \cdot 369$$

$$\text{donc } \cancel{369}(u+11) + 58 \times \cancel{369}k = 0$$

$$\text{donc } 369u + 58v = 1 \Leftrightarrow \begin{cases} u+11 = -58k \\ v-70 = 369k \end{cases}$$

L'ensemble des couples (u, v) tel que $369u + 58v = 1$

est l'ensemble des couples de la forme

$$(-11 - 58k, 70 + 369k) \text{ où } k \in \mathbb{Z}.$$

I. 1. Soit A une matrice.

B est l'inverse de A si $BA = AB = I_2$

et A est inversible si A possède une inverse.

Units de l'inverse Soient B, C tel que $AB = I_2$ et $CA = I_2$

$$\left. \begin{array}{l} CAB = C(AB) = CI_2 = C \\ CAB = (CA)B = I_2B = B \end{array} \right\} \text{donc } B = C$$

2.

$$A^2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2+bc & ab+bd \\ ca+dc & cb+d^2 \end{pmatrix}$$

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

C'est le Théorème de Cayley-Hamilton

$$\begin{aligned} \text{car } \det(A - XI_2) &= X^2 - (a+d)X + \det A \\ &= X^2 - (a+d)X + (ad-bc) \end{aligned}$$

3. Si $ad-bc \neq 0$

$$\frac{A^2 - (a+d)A}{-ad+bc} = I_2$$

$$\text{donc } \frac{A^2 - (a+d)A}{-ad+bc} = A \frac{A - (a+d)I_2}{-ad+bc} = \frac{A - (a+d)I_2}{-ad+bc} A = I_2$$

$$\text{donc } A \text{ est inversible d'inverse } \frac{1}{-ad+bc} \begin{pmatrix} A - (a+d)I_2 \end{pmatrix} = \frac{1}{ad-bc} \begin{pmatrix} +d-b & -c+a \\ -c+a & +d-b \end{pmatrix}$$

Réciproquement Soit A inversible, Notons A^{-1} son inverse

(11)

Supposons que $ad-bc = 0$

alors $A^2 - (a+d)A = 0$

donc $A(A - (a+d)I_2) = 0$

donc $A^{-1}A(A - (a+d)I_2) = 0$

c.a.d. $I_2(A - (a+d)I_2) = 0$

donc $A = (a+d)I_2 = \begin{pmatrix} a+d & 0 \\ 0 & a+d \end{pmatrix}$

donc $a = a+d = d$ donc $a=0$ et $d=0$

donc $A = 0$ la matrice nulle donc $0 = A^{-1}A = I_2$

contradiction donc $ad-bc \neq 0$. On

Remarque: On a démontré A inversible $\Leftrightarrow \det A \neq 0$ les valeurs

II.1 Soit $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ alors $ad-bc = 4 - 2 \times 3 = -2$

donc d'après I.3 $A^{-1} = -\frac{1}{-2} \begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & +1 \\ +\frac{3}{2} & -\frac{1}{4} \end{pmatrix}$

2. Si $ad-bc = 1$ ou -1

alors d'après 3, A est inversible

et $A^{-1} = \frac{1}{ad-bc} \begin{pmatrix} -d & b \\ c & a \end{pmatrix}$ a tous ses coefficients dans $\mathbb{Z}$

3.

Soit déterminant d'une matrice $\det A = ad-bc$

Supposons que A est inversible d'inverse A^{-1}

avec tous ses coefficients dans $\mathbb{Z}$

Alors $\det A^{-1}$ et $\det A$ sont des entiers relatifs

$AA^{-1} = I_2$ donc $\det A \det A^{-1} = \det I_2 = 1$

donc $\det A$ est une unité relatif à $\mathbb{Z}$ donc $\mathbb{Z}$

(11)

donc $\det A = \pm 1$.

III

1.

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix}$$

2. a)
$$\begin{cases} x' = 4x + 3y \\ y' = 5x + 4y \end{cases}$$

BE

Z O

$(x, y) (1, 4)$

$(25, 14)$

$(20, 19)$

$(x', y') (16, 21)$

$(142, \underline{125+56})$
 181

$(137, 176)$

mod 26

$(16, 21)$

$(12, 25)$

$(7, 20)$

Q V

M I

H U

137

26

176

26

130

156

5

5

20

6

B)

$$A = \begin{pmatrix} 4 & 3 \\ 5 & 4 \end{pmatrix}$$

$\det A = 4 \times 4 - 3 \times 5 = 1$

donc

$$A^{-1} = \begin{pmatrix} +4 & -3 \\ -5 & +4 \end{pmatrix}$$

$\in M_2(\mathbb{Z})$

$$b) \begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix} \text{ donc } \begin{pmatrix} x \\ y \end{pmatrix} = A A^{-1} \begin{pmatrix} x' \\ y' \end{pmatrix} = A^{-1} \begin{pmatrix} x' \\ y' \end{pmatrix} \quad (12)$$

donc

$$\begin{pmatrix} x \\ y \end{pmatrix} \equiv \left[A^{-1} \begin{pmatrix} x' \\ y' \end{pmatrix} \right] \text{ modulo } 26$$

$$\equiv \left(A^{-1} \text{ modulo } 26 \right) \times \begin{pmatrix} x' \\ y' \end{pmatrix} \text{ modulo } 26$$

$$\text{Car si } \begin{pmatrix} x'_1 \\ y'_1 \end{pmatrix} \equiv \begin{pmatrix} x'_2 \\ y'_2 \end{pmatrix} \text{ (modulo } 26)$$

$$\text{alors } A^{-1} \begin{pmatrix} x'_1 \\ y'_1 \end{pmatrix} \equiv A^{-1} \begin{pmatrix} x'_2 \\ y'_2 \end{pmatrix} \text{ (modulo } 26)$$

$$\text{car que } A^{-1} \in \mathbb{Z}$$

	S	F	X	M	O	J
$\begin{pmatrix} x' \\ y' \end{pmatrix} \text{ modulo } 26$	18	5	23	12	14	9

$$A^{-1} \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 4x' - 3y' \\ -5x' + 6y' \end{pmatrix}$$

$$\begin{pmatrix} 72 - 15, -30 + 20 \end{pmatrix} \begin{pmatrix} 92 - 36, 115 + 48 \end{pmatrix} \begin{pmatrix} 56 - 27, -70 + 36 \end{pmatrix} \\ = \begin{pmatrix} +57, -10 \end{pmatrix} \begin{pmatrix} +56, -67 \end{pmatrix} \begin{pmatrix} +29, -34 \end{pmatrix}$$

modulo 26	$\begin{pmatrix} 5, 8 \end{pmatrix}$	$\begin{pmatrix} 4, 11 \end{pmatrix}$	$\begin{pmatrix} 3, 18 \end{pmatrix}$
	$\begin{pmatrix} F, I \end{pmatrix}$	$\begin{pmatrix} E, L \end{pmatrix}$	$\begin{pmatrix} D, S \end{pmatrix}$

3 a) 7 et 26 sont premiers entre eux

Donc d'après III.2. a,

il existe un entier naturel u tel que $7u \equiv 1 [26]$

Unicité Soient $u, v \in \mathbb{N}$ tel que

$$7u \equiv 1 [26]$$

$$7v \equiv 1 [26]$$

alors $7u \equiv 7v [26]$ donc $7(u-v) \equiv 0 [26]$

donc $26 \mid 7(u-v)$. Comme 26 est premier avec 7,

il s'ensuit d'après II.2. a) $26 \mid u-v$

$$\text{donc } u \equiv v [26]$$

Si u et v sont compris entre 0 et 25 alors $u = v$

b)

$$A = \begin{pmatrix} 3 & 2 \\ 1 & 3 \end{pmatrix}$$

$$\det A = ad - bc = 3 \times 3 - 2 \times 1 = 7$$

$$\text{Soit } B = -A + (a+d)I_2 = \begin{pmatrix} +d-b & \\ -c+a & \end{pmatrix} = \begin{pmatrix} 3 & -2 \\ -1 & 3 \end{pmatrix}$$

Il s'agit de B.I.2

$$BA = (ad-bc)I_2 = 7I_2$$

$$\text{donc } uBA = u7I_2$$

$$uBA \equiv I_2 \pmod{26}$$

$$\text{Comme } u7 \equiv 1 [26]$$

c)

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix} \text{ donc } A \begin{pmatrix} x' \\ y' \end{pmatrix} = BA \begin{pmatrix} x \\ y \end{pmatrix}$$

$$\text{donc } uBA \begin{pmatrix} x \\ y \end{pmatrix} = uB \begin{pmatrix} x' \\ y' \end{pmatrix}$$

$$\text{donc } \begin{pmatrix} x \\ y \end{pmatrix} = uB \begin{pmatrix} x' \\ y' \end{pmatrix} \pmod{26}$$

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

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

donc $-11 \times 7 \equiv 1 \pmod{26}$

donc $\begin{pmatrix} x \\ y \end{pmatrix} \equiv -11 \begin{pmatrix} 3 & -2 \\ -1 & 3 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \pmod{26}$

$$\begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} -33 & 22 \\ 11 & -33 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} -7 & -4 \\ 11 & -7 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \pmod{26}$$

A K X O U E V H D L

$$(x', y') \begin{pmatrix} 0, 10 \\ 23, 14 \\ 20, 4 \\ 21, 7 \\ 5, 11 \end{pmatrix}$$

$$(x, y) \begin{pmatrix} 40, 70 \\ 21+48, -33+84 \\ 26, -66-28 \\ 35-28, -55-49 \\ -21-44, 33-77 \end{pmatrix}$$

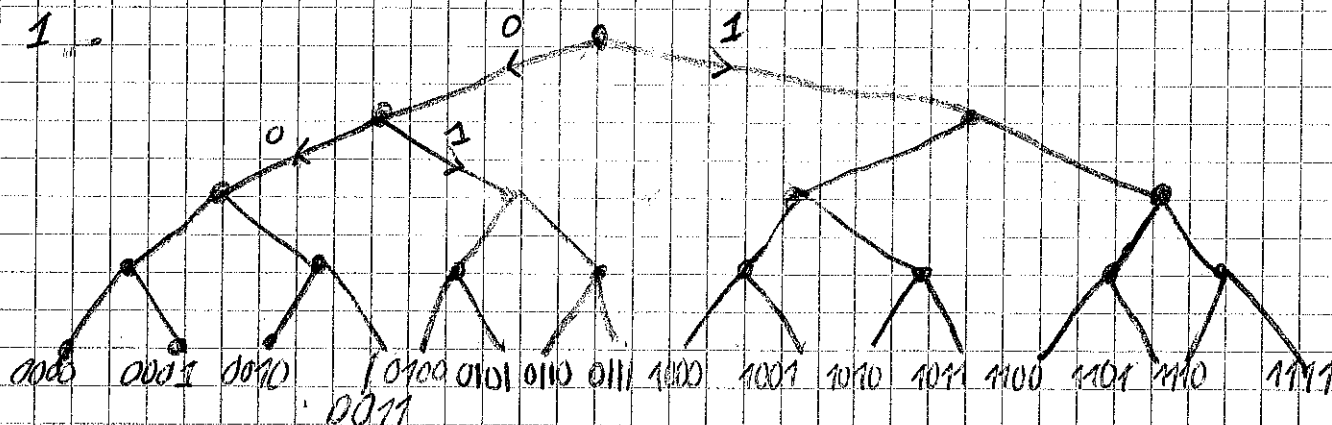
$$\pmod{26} \begin{pmatrix} 12, 8 \\ 17, 25 \\ 0, 8 \\ 7, 10 \\ 13, 8 \end{pmatrix}$$

M I R ~~M~~ A K H A N I

4) Si $ad-bc$ est premier avec 26

et $d \nmid \det A = ad-bc$ est inversible dans $\mathbb{Z}/26\mathbb{Z}$

1.



2. 6 chemins contenant exactement 2 fois 1

3. 1 à la première place, 3 chemins

----- deuxième -----, 3 chemins

----- troisième -----, 3 chemins

quatrième

3

II $\binom{n}{k} \stackrel{\text{def}}{=} \text{nombre de chemins contenant } k \text{ fois } 1$

1. nombre de chemins contenant k fois 0

= nombre de chemins contenant k fois 1 $\stackrel{\text{def}}{=} \binom{n}{k}$

Un chemin contenant k fois 0

si il contient $n-k$ fois 1

donc nombre de chemins contenant k fois 0 = $\binom{n}{n-k}$

2. Pour les chemins de longueur $n+1$ contenant k fois 1,

il y a

- ceux qui commencent par un 1. Ils sont
composés de ce 1 et d'un chemin de longueur n
avec $k-1$ fois 1. Il y en a donc $\binom{n}{k-1}$

- ceux qui commencent par un 0. Il y en a $\binom{n}{k}$

donc $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$

(16)

3.

$A = \begin{pmatrix} \text{une } n\text{-uplet contenant } k \text{ fois } 1 \\ \vdots \\ \text{une } n\text{-uplet contenant } k \text{ fois } 1 \end{pmatrix}$ $\binom{n}{k}$ lignes correspondant à tous les n -uplets contenant k fois 1 possible

a) ligne de $A = n$ -uplet avec k fois 1 et des 0
donc la somme est égal à k

b) soit $j \in \llbracket 1, n \rrbracket$

somme de la j ème colonne de A représente le nombre de n -uplets avec k fois 1 dont la j ème élément est 1 c.à.d. $\binom{n-1}{k-1}$

c) d'après a), la somme des éléments que A est égal à $k \binom{n}{k}$

d'après b), c'est $\sum_{j \in \llbracket 1, n \rrbracket} \binom{n-1}{k-1} = n \binom{n-1}{k-1}$

d'où $k \binom{n}{k} = n \binom{n-1}{k-1}$

4) a) Soit partie d'un ensemble à n éléments $\{1, 2, \dots, n\}$ sont en bijection avec les n -uplets $(b_1, \dots, b_n)$ composés de 0 et de 1 :
Soit $A \subset \{1, 2, \dots, n\}$ on lui associe le n -uplet $(b_1, \dots, b_n)$ tel que $b_i = 1$ si $i \in A$.

Une partie A a p éléments correspondant à un m -uplet avec p fois 1

donc nombre de parties a p éléments de $\{1, \dots, m\}$
 = nombre de m -uplets avec p fois 1

b) Soit $\psi: \begin{cases} \text{injection} \\ \text{de } \{1, \dots, k\} \text{ vers } \{1, \dots, m\} \end{cases} \rightarrow \begin{cases} \text{parties à k éléments} \\ \text{de } \{1, \dots, m\} \end{cases}$
 $\psi: \{1, \dots, k\} \rightarrow \{1, \dots, m\} \rightarrow \{f(1), \dots, f(k)\}$

ψ est surjective

Pour chaque partie $\{f(1), \dots, f(k)\}$, il y a

$k!$ injections $\phi: \{1, \dots, k\} \rightarrow \{1, \dots, m\}$ possibles

donc $\binom{m}{k} = \frac{\text{nombre d'injections de } \{1, \dots, k\} \text{ vers } \{1, \dots, m\}}{k!}$

$$= \frac{m \times (m-1) \times (m-2) \times \dots \times (m-k+1)}{k!}$$

donc de $f(1)$ de $f(k)$ a $f(k)$

$$= \frac{m!}{(m-k)!} \times \frac{1}{k!}$$

autre démonstration voir $k=2$ à partir du II.3

$$c) \binom{n+1}{k} = \frac{(n+1)n}{k!} \frac{(n-k+2)}{k!}$$

$$\binom{n}{k-1} + \binom{n}{k} = \frac{n}{(k-1)!} \frac{(n-k+2)}{k!} + \frac{n}{k!} \frac{(n-k+1)}{k!} =$$

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

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

III

Ω = ensemble des n -uplets de 0 et de 1

muni de la probabilité $P(\{E_1, \dots, E_m\}) = \theta^{E_1 + \dots + E_m} (1-\theta)^{n-E_1 - \dots - E_m}$
 $\{E_1, \dots, E_m\}$ = m -uplet de 0 et de 1

" $X = k$ " correspond à l'ensemble des m -uplets avec k fois 1

donc $P(X = k) = \text{card "X=k"} \times \theta^k (1-\theta)^{n-k}$

$$= \binom{n}{k} \theta^k (1-\theta)^{n-k}$$

loi binomiale de paramètres n et θ .

$$E(X) = \sum_{k=0}^n k P(X=k) = \sum_{k=1}^n k \binom{n}{k} \theta^k (1-\theta)^{n-k}$$

$$= \sum_{k=1}^n n \binom{n-1}{k-1} \theta^k (1-\theta)^{n-k}$$

posons $k' = k-1$

$$= n \sum_{k'=0}^{n-1} \binom{n-1}{k'} \theta \theta^{k'} (1-\theta)^{n-1-k'}$$

d'après le binôme de Newton $n \theta \left[\theta + (1-\theta) \right]^{n-1} = n \theta$

I. 1. 4 cases,

les 4-uplets sont équiprobables

$$P(X_4 = -4) = P(\{0000\}) = \frac{1}{16}$$

$$P(X_4 = -2) = P(1 \text{ fois } 1) = \frac{4}{16} \text{ d'après A.1.3}$$

$$P(X_4 = 0) = P(2 \text{ fois } 1) = \frac{6}{16}$$

$$P(X_4 = 2) = \frac{4}{16}$$

$$P(X_4 = 4) = \frac{1}{16}$$

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

$$P(D_n = k) = \binom{n}{k} \frac{1}{2^n}$$

$$3. X_n = -n + 2 D_n = 2 D_n - n$$

$$4. \text{ d'après A.III } E(D_n) = n \times \frac{1}{2}$$

$$\text{donc } E(X_n) = 2 \frac{n}{2} - n = 0$$

On a autant de chances de perdre que d'arriver à chaque lancer de pièce. Donc en moyenne on ne gagne pas.

$$\text{I. 1. } "X_n = 0" \Leftrightarrow "2 D_n = n"$$

donc si n est impair, l'événement " $X_n = 0$ "

est impossible donc $P(X_n = 0) = 0$

$$2/ X_{2n} = 0 \Leftrightarrow 2 D_{2n} = 2n \Leftrightarrow D_{2n} = n$$

$$\text{donc } P(X_{2n} = 0) = P(D_{2n} = n) = \binom{2n}{n} \frac{1}{2^{2n}}$$

III 1. L'algorithme remonte l'abscisse du point
au bout du n-ème lancer

(20)

2. entier (n)
x ← 0
no ← 0
Pour k allant de 1 à n
Si alea() > 0,5 alors
x ← x+1

fin pour

x ← x-1

fin

Si x = 0 alors

no ← no+1.

fin

fin pour

retourner / no /

3. entier (n)
b ← 0
Pour i allant de 1 à 1000 } ← ligne nouvelle
x ← 0

Pour k allant de 1 à n

⋮

programme du

fin pour

Si x = 0 alors b ← b+1

fin pour

} ligne nouvelle

$b = \frac{b}{1000}$ lignes nouvelles
retourner $\{b\}$

(21)

4) Le programme du 1. permet au professeur
de montrer tous les valeurs de X_m possibles
Pour un m donné.

Soit $C_{m/2}$, la variable aléatoire égale au
nombre de passage à l'origine entre le premier et
le m ème lancer.

Le programme du 2. permet au professeur de donner
toutes les valeurs possibles de C_m

Le programme du 3 permet de donner une valeur
appartenant de $P(X_m = 0)$

IV

1. D'après R.I.3,

$$X_{2n} = 2 D_{2n} - 2n$$

donc X_{2n} est pair.

Comme $0 \leq D_{2n} \leq 2n$ alors $0 - 2n \leq X_{2n} \leq 2 \times 2n - 2n$

2. Soit k compris entre $-n$ et $+n$.

$$X_{2n} = 2k \Leftrightarrow D_{2n} = k + n$$

$$\text{donc } P(X_{2n} = 2k) = P(D_{2n} = k + n) = \frac{\binom{2n}{k+n}}{\binom{2n}{n}} = \frac{1}{2n}$$

d'après R.I.2

3.

$$P(X_R = 1) = P(X_R = 0) = \begin{cases} 0 & \text{si } R \text{ impair} \\ \binom{2R-1}{R-1} \frac{1}{2^{2R-1}} & \text{si } R \text{ pair} \end{cases}$$

$$C_m = X_1 + \dots + X_{2m}$$

$$\text{donc } E(C_m) = \sum_{R=1}^{2m} E(X_R)$$

$$E(X_R) = 1 \times P(X_R = 1) + 0 \times P(X_R = 0) = 0 \text{ si } R \text{ impair}$$

$$\text{donc } E(C_m) = \sum_{R=1}^{2m} \binom{2R-1}{R-1} \frac{1}{2^{2R-1}}$$

$$\text{on particulier } E(C_1) = \binom{2}{1} \frac{1}{4} = \frac{1}{2}$$

$$\text{Démonstration par récurrence } \forall m \geq 1, E(C_m) = \frac{2m+1}{4^m} \binom{2m}{m} - 1$$

$$\bullet m=1 \quad \frac{2 \times 1 + 1}{4} \binom{2}{1} - 1 = \frac{3}{2} - 1 = \frac{1}{2} = E(C_1)$$

$$\bullet \frac{2m+1}{4^m} \binom{2m}{m} - \frac{2m-1}{4^{m-1}} \binom{2m-2}{m-1} - \frac{\binom{2m}{m}}{2^{2m}}$$

$$= \frac{1}{4^{m-1}} \left[\frac{2m}{4} \frac{2m \times (2m-1) \times \dots \times (m+1)}{m \times (m-1)!} - \frac{(2m-1)(2m-2) \times \dots \times m}{(m-1)!} \right] = 0$$

$$\text{donc si } E(C_{m-1}) = \frac{2m-1}{4^{m-1}} \binom{2m-2}{m-1} \text{ alors } E(C_m) = \frac{2m+1}{4^m} \binom{2m}{m}$$