Exercice 1

① ⓐ $P = \left(\begin{array}{ccc|ccc} 1 & 0 & -1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right) \underset{L_3 \leftarrow L_3 - L_1}{\sim} \left(\begin{array}{ccc|ccc} 1 & 0 & -1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 \end{array}\right) \underset{L_3 \leftarrow L_3 - L_2}{\sim} \left(\begin{array}{ccc|ccc} 1 & 0 & -1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & -1 & -1 & 1 \end{array}\right)$

$\underset{L_2 \leftarrow L_2 - L_3}{\sim} \left(\begin{array}{ccc|ccc} 1 & 0 & -1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 2 & -1 \\ 0 & 0 & 1 & -1 & -1 & 1 \end{array}\right) \underset{L_1 \leftarrow L_1 + L_3}{\sim} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & -1 & 1 \\ 0 & 1 & 0 & 1 & 2 & -1 \\ 0 & 0 & 1 & -1 & -1 & 1 \end{array}\right)$

Donc P est inversible d'inverse $P^{-1} = \begin{pmatrix} 0 & -1 & 1 \\ 1 & 2 & -1 \\ -1 & -1 & 1 \end{pmatrix}$

ⓑ

$$\begin{array}{cc} & \begin{pmatrix} 3 & 4 & -4 \\ -2 & -1 & 2 \\ -2 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & -1 & 1 \\ 1 & 2 & -1 \\ -1 & -1 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 1 & -1 \\ 1 & 2 & -1 \\ -3 & -3 & 3 \end{pmatrix} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix} = D \end{array}$$

On a mq $P^{-1}AP = D$
donc $P(P^{-1}AP)P^{-1} = PDP^{-1}$
donc $(PP^{-1})A(PP^{-1}) = PDP^{-1}$
donc $A = PDP^{-1}$
(ou calcul direct)

Comme D est diagonale, $\forall n \in \mathbb{N}$ $D^n = \begin{pmatrix} (-1)^n & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3^n \end{pmatrix}$

ⓒ Soit $\mathcal{P}(n)$ " $A^n = PD^nP^{-1}$ "

Initialisation si $n=0$, $A^0 = I_3$ et $PD^0P^{-1} = PI_3P^{-1} = PP^{-1} = I_3$

hérédité supposons qu'il existe $n \in \mathbb{N}$ tq $\mathcal{P}(n)$ est vraie

$A^{n+1} = A^n A = (PD^nP^{-1})(PDP^{-1}) = PD^n(P^{-1}P)DP^{-1} = PD^n I_3 D P^{-1} = PD^{n+1}P^{-1}$

Concl $\forall n \in \mathbb{N}$ $\mathcal{P}(n)$ vraie

② ⓐ Soit $n \in \mathbb{N}$. $U_{n+1} = \begin{pmatrix} a_{n+1} \\ b_{n+1} \\ c_{n+1} \end{pmatrix}$ et $AU_n = \begin{pmatrix} 3 & 4 & -4 \\ -2 & -1 & 2 \\ -2 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_n \\ b_n \\ c_n \end{pmatrix} = \begin{pmatrix} 3a_n + 4b_n - 4c_n \\ -2a_n - b_n + 2c_n \\ -2a_n + c_n \end{pmatrix}$

D'après la définition des suites (a_n), (b_n) et (c_n), on a donc $U_{n+1} = AU_n$.

ⓑ Montrons que $\mathcal{P}'(n)$ " $U_n = A^nU_0$ " est vraie par réc

Initialisation si $n=0$, $U_0 = A^0U_0$ car $A^0 = I_3$

hérédité supposons qu'il existe $n \in \mathbb{N}$ tq $\mathcal{P}'(n)$ est vraie

$U_{n+1} = AU_n = AA^nU_0 = A^{n+1}U_0$

Concl $\forall n \in \mathbb{N}$ $\mathcal{P}'(n)$ vraie

$\begin{pmatrix} (-1)^n & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3^n \end{pmatrix} \begin{pmatrix} 0 & -1 & 1 \\ 1 & 2 & -1 \\ -1 & -1 & 1 \end{pmatrix}$

ⓒ Ainsi $U_n = A^nU_0 = PD^nP^{-1}U_0$ or $\begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} (-1)^n & 0 & -3^n \\ 0 & 1 & -3^n \\ (-1)^n & 1 & 3^n \end{pmatrix} \begin{pmatrix} 3^n & (-1)^{n+1}+3^n & (-1)^n-3^n \\ 1-3^n & 2-3^n & -1+3^n \\ 1-3^n & (-1)^{n+1}+2-3^n & (-1)^n-1+3^n \end{pmatrix} = PD^nP^{-1}$

Donc $U_n = \begin{pmatrix} 3^n a_0 + ((-1)^{n+1}+3^n) b_0 + ((-1)^n - 3^n) c_0 \\ (1-3^n) a_0 + (2-3^n) b_0 + (-1+3^n) c_0 \\ (1-3^n) a_0 + ((-1)^{n+1}+2-3^n) b_0 + ((-1)^n - 1 + 3^n) c_0 \end{pmatrix}$

Ainsi $\forall n \in \mathbb{N}$ $\begin{cases} a_n = 3^n a_0 + ((-1)^{n+1}+3^n) b_0 + ((-1)^n - 3^n) c_0 \\ b_n = (1-3^n) a_0 + (2-3^n) b_0 + (3^n-1) c_0 \\ c_n = (1-3^n) a_0 + ((-1)^{n+1}+2-3^n) b_0 + ((-1)^n - 1 + 3^n) c_0 \end{cases}$

3- Deuxième application

ⓐ. Soit $M \in \mathcal{M}_3(\mathbb{C})$ tq $M^2 = A$.

$(P^{-1}MP)^2 = (P^{-1}MP)(P^{-1}MP) = P^{-1}M(PP^{-1})MP = P^{-1}M^2P = P^{-1}AP =$

(× est associatif dans $\mathcal{M}_3(\mathbb{C})$, ①ⓑ)

$= P^{-1}(PDP^{-1})P = (P^{-1}P)D(P^{-1}P) = D.$

Ainsi $N^2 = D$

Mq $ND = DN$:

$ND = NN^2 = N^3 = N^2N = DN$ donc N et D commutent

ⓑ Soit $N = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \in \mathcal{M}_3(\mathbb{C})$

$ND = DN$ ssi $\begin{pmatrix} -a & b & 3c \\ -d & e & 3f \\ -g & h & 3i \end{pmatrix} = \begin{pmatrix} -a & -b & -c \\ d & e & f \\ 3g & 3h & 3i \end{pmatrix}$

ssi $\begin{cases} b = -b \\ 3c = -c \\ -d = d \\ 3f = f \\ -g = 3g \\ h = 3h \end{cases}$ ssi $b = c = d = f = g = h = 0$ ssi $N = \begin{pmatrix} a & 0 & 0 \\ 0 & e & 0 \\ 0 & 0 & i \end{pmatrix}$

ssi N est une matrice diagonale.

ⓒ On a donc $N^2 = D$ d'après ⓐ et $N^2 \in \mathcal{D}_3(\mathbb{C})$ d'après ⓑ

Ainsi si on pose $N = \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}$ où $(a,b,c) \in \mathbb{C}^3$, on a :

$N^2 = \begin{pmatrix} a^2 & 0 & 0 \\ 0 & b^2 & 0 \\ 0 & 0 & c^2 \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}$ ssi $\begin{cases} a^2 = -1 \\ b^2 = 1 \\ c^2 = 3 \end{cases}$ ssi $\begin{cases} a = \pm i \\ b = \pm 1 \\ c = \pm\sqrt{3} \end{cases}$

et donc comme $N = P^{-1}MP$, $PNP^{-1} = P(P^{-1}MP)P^{-1} = (PP^{-1})M(PP^{-1}) = M$

on a donc $M = P\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}P^{-1}$ avec $\begin{cases} a = \pm i \\ b = \pm 1 \\ c = \pm\sqrt{3} \end{cases}$

ⓓ Le nombre de solution de l'équation $N^2 = A$ dans $\mathcal{M}_3(\mathbb{C})$ est : $2^3 = 8$ (2 valeurs possibles pour chacun des 3 coefficients de N qui sont non nuls).

En revanche il n'y a aucune solution dans $\mathcal{M}_3(\mathbb{R})$ puisque aucun réel a ne vérifie $a^2 = -1$.

Exercice 2

① @ $f(1\times 1) = f(1) + f(1)$ donc $f(1) = 2f(1)$ donc $\underline{f(1) = 0}$

Soit $x>0$ $\quad f\left(x\times\frac{1}{x}\right) = f(1) = 0$ et $f\left(x\times\frac{1}{x}\right) = f(x) + f\left(\frac{1}{x}\right)$ donc $\underline{f\left(\frac{1}{x}\right) = -f(x)}$

⑥ Soit $n\in\mathbb{N}$. On pose $\mathcal{P}(n)$: "$\forall x>0,\ f(x^n) = nf(x)$"

Mq $\forall n\in\mathbb{N}$, $\mathcal{P}(n)$ vraie par récurrence.

- initialisation : si $n=0$ alors $\forall x>0$, $f(x^0) = f(1) = 0\times f(x)$. donc $\mathcal{P}(0)$ vraie
- hérédité : supposons que $\mathcal{P}(n)$ vraie pour un certain $n\in\mathbb{N}$
  Mq $\mathcal{P}(n+1)$ vraie.
  Soit $x>0$ $\quad f(x^{n+1}) = f(x\times x^n) \overset{(*)}{=} f(x) + f(x^n) \overset{HR}{=} f(x) + nf(x) = (n+1)f(x)$
  donc $\mathcal{P}(n+1)$ vraie
- Conclusion : $\forall n\in\mathbb{N}$ $\mathcal{P}(n)$ vraie

Soit $n\in\mathbb{Z}\setminus\mathbb{N}$ alors $-n\in\mathbb{N}^*$.

Soit $x>0$. $\quad f(x^n) = f\left(\frac{1}{x^{-n}}\right) \overset{q①a}{=} -f(x^{-n}) \overset{\mathcal{P}(-n)\text{ vraie car } -n\in\mathbb{N}^*}{=} -(-n)f(x) = nf(x)$.

© Soit $r\in\mathbb{Q}$

Il existe $p\in\mathbb{Z}$ et $q\in\mathbb{N}^*$ tq $r = \frac{p}{q}$

D'une part on a :

$f\left(e^{\frac{p}{q}}\right) = f\left(\left(e^{\frac{1}{q}}\right)^p\right) = pf\left(e^{\frac{1}{q}}\right)$ d'après ①⑥ avec $x = e^{\frac{1}{q}} > 0$

D'autre part $f(e) = f\left(e^{q\times\frac{1}{q}}\right) = f\left(\left(e^{\frac{1}{q}}\right)^q\right) \overset{①⑥}{=} qf\left(e^{\frac{1}{q}}\right)$ donc $f\left(e^{\frac{1}{q}}\right) = \frac{1}{q}f(e)$.

Donc $f\left(e^{\frac{p}{q}}\right) = pf\left(e^{\frac{1}{q}}\right) = p\times\frac{1}{q}f(e) = \frac{p}{q}f(e)$

et $\underline{f(e^r) = rf(e)}$.

⑥ Soit $x\in\mathbb{R}$.

$\mathbb{Q}$ est dense dans $\mathbb{R}$ donc il existe une suite $(r_n)_{n\in\mathbb{N}}$ tq

(r_n) CV vers x et $\forall n\in\mathbb{N}$ $r_n\in\mathbb{Q}$

Comme exp est continue sur $\mathbb{R}$, $e^{r_n} = \exp(r_n) \underset{n\to+\infty}{\longrightarrow} \exp(x) = e^x$

or $\forall n\in\mathbb{N}$, $r_n\in\mathbb{Q}$ donc $f(e^{r_n}) = r_n f(e)$ (Δ)

Comme f est continue sur $\mathbb{R}_+^*$, $f(e^{r_n}) \underset{n\to+\infty}{\longrightarrow} f(e^x)$

Par passage à la limite dans (Δ) on obtient : $f(e^x) = xf(e)$.

Ainsi $\underline{\forall x\in\mathbb{R},\ f(e^x) = xf(e)}$

② D'après ①, si $f:\mathbb{R}_+^*\to\mathbb{R}$ est continue telle que $\forall x,y\in\mathbb{R}_+^*$, $f(xy) = f(x)+f(y)$ alors $\forall x\in\mathbb{R}$, $f(e^x) = xK$ et donc $\forall t>0$, $f(t) = K\ln(t)$, avec $K = f(e)$

Réciproquement, soit $f: t\mapsto K\ln t$ avec $K\in\mathbb{R}$. f est continue sur $\mathbb{R}_+^*$

$\forall x>0\ \forall y>0$, $f(xy) = K\ln(xy) = K(\ln x + \ln y) = K\ln x + K\ln y = f(x)+f(y)$

Donc les fonctions numériques continues définies sur $\mathbb{R}_+^*$ qui vérifient la relation $(*)$ sont les fonctions $x \mapsto Kln x$, $K \in \mathbb{R}$.

② ⓐ Soit $f : \mathbb{R}_+^* \to \mathbb{R}$ telle que $\forall x>0\ \forall y>0$ $f(xy) = xf(y)+yf(x)$ et f continue sur $\mathbb{R}_+^*$

Soit $g : \mathbb{R}_+^* \to \mathbb{R}$, $x \mapsto \frac{f(x)}{x}$.

Soit $x>0$, $y>0$

$g(xy) = \frac{f(xy)}{xy} = \frac{xf(y)+yf(x)}{xy} = \frac{f(y)}{y} + \frac{f(x)}{x} = g(y)+g(x) = g(x)+g(y)$

g est continue sur $\mathbb{R}_+^*$ en tant que quotient de fcts continues sur $\mathbb{R}_+^*$ dont le dénominateur ne s'annule pas.

Donc g vérifie la relation $(*)$.

ⓑ Donc si $f : \mathbb{R}_+^* \to \mathbb{R}$ continue et vérifie $(*)$ alors il existe $K \in \mathbb{R}$ tq $\forall x>0$ $\frac{f(x)}{x} = Kln x$, càd $\forall x>0$, $f(x) = xKln x$.

Réciproquement, si $f : x \mapsto xKln x$, $K \in \mathbb{R}$, alors f est continue sur $\mathbb{R}_+^*$.

De plus, $\forall x>0\ \forall y>0$, $f(xy) = xyK\ln(xy) = xyK[\ln(x)+\ln(y)]$
$= xyK\ln x + xyK\ln y$
$= y \times xK\ln x + x \times yK\ln y$
$= yf(x) + xf(y)$.

Concl : Les fonctions numériques continues définies sur $\mathbb{R}_+^*$ qui vérifient $(*)$ sont de la forme :

$x \mapsto xKln x$, $K \in \mathbb{R}$.

Exercice 3

0- Les seize premiers termes sont : u_{15}

0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610

Partie 1.

1-a- • Montrons que tout diviseur commun à a et à b est un diviseur de a-b et de b.

Soit d un diviseur commun à a et à b.

$\exists k_1 \in \mathbb{N}\ \exists k_2 \in \mathbb{N}$ / $a = k_1 d$ et $b = k_2 d$

Or $a - b = k_1 d - k_2 d = (k_1 - k_2) d$ et $k_1 - k_2 \in \mathbb{N}$ puisque $a \geq b$.

Ainsi $d \mid (a-b)$ et d est un diviseur commun à a-b et à b.

• Réciproquement, montrons que tout diviseur commun à a-b et à b est un diviseur de a et de b.

Soit d un diviseur commun à a-b et à b.

$\exists k_3 \in \mathbb{N}\ \exists k_4 \in \mathbb{N}$ / $a - b = k_3 d$ et $b = k_4 d$.

Or $a = a - b + b = k_3 d + k_4 d = (k_3 + k_4) d$ et $k_3 + k_4 \in \mathbb{N}$

Donc $d \mid a$ et d est un diviseur commun à a et à b.

• Conclusion : les diviseurs communs à a et à b sont les diviseurs communs à a-b et à b. Le plus grand d'entre eux est donc le même et $\underline{a \wedge b = (a-b) \wedge b}$.

1-b- Soit $\mathcal{P}(n)$: " $u_{n+1} \wedge u_n = 1$ ". Montrons par récurrence que $\mathcal{P}(n)$ est vraie pour tout $n \in \mathbb{N}^*$.

• Initialisation : $u_2 = 1$ et $u_1 = 1$ donc $u_1 \wedge u_2 = 1$ et $\mathcal{P}(1)$ vraie

• Hérédité : Supposons la propriété $\mathcal{P}(n)$ vraie pour $n \in \mathbb{N}^*$. Montrons que $\mathcal{P}(n+1)$ vraie.

$u_{n+2} \wedge u_{n+1} = (u_{n+1} + u_n) \wedge u_{n+1}$

or d'après 1-a, $(u_{n+1} + u_n) \wedge u_{n+1} = u_n \wedge u_{n+1}$

donc $u_{n+2} \wedge u_{n+1} = u_n \wedge u_{n+1} = u_{n+1} \wedge u_n = 1$ et $\mathcal{P}(n+1)$ vraie

• Conclusion : $\underline{\forall n \in \mathbb{N}^*\ \mathcal{P}(n) \text{ vraie}}$

2-a- $8 \wedge 12 = 4$ et $u_4 = 3$

D'autre part $u_8 \wedge u_{12} = 21 \wedge 144 = 3$ donc $\underline{u_{8 \wedge 12} \mid u_8 \wedge u_{12}}$.

2-b- Soit $\mathcal{P}(p)$: "$\forall n \in \mathbb{N}$, $u_{n+p+1} = u_n u_p + u_{n+1} u_{p+1}$". Montrons que $\mathcal{P}(p)$ est vraie pour tout $p \in \mathbb{N}$ par récurrence double

• Initialisation : Soit $n \in \mathbb{N}$

$u_{n+1} = u_n \cdot u_0 + u_{n+1} u_1$ car $u_0 = 0$ et $u_1 = 1$.

donc $\mathcal{P}(0)$ vraie. De plus $u_n u_1 + u_{n+1} u_2 = u_n + u_{n+1} = u_{n+2}$

donc $\mathcal{P}(1)$ vraie.

• Hérédité : on suppose qu'il existe $p \in \mathbb{N}$ telle que $\mathcal{P}(p)$ et $\mathcal{P}(p+1)$ sont vraies. Montrons que $\mathcal{P}(p+2)$ est vraie

Soit $n \in \mathbb{N}$

On veut donc montrer que $u_{n+p+2+1} = u_n u_{p+2} + u_{n+1} u_{p+2+1}$

c&d $u_{n+p+3} = u_n u_{p+2} + u_{n+1} u_{p+3}$.

$u_{n+p+3} = u_{n+p+2} + u_{n+p+1}$ par définition de u

$= (u_n u_{p+1} + u_{n+1} u_{p+2}) + (u_n u_p + u_{n+1} u_{p+1})$

$= u_n (u_p + u_{p+1}) + u_{n+1} (u_{p+1} + u_{p+2})$

$= u_n u_{p+2} + u_{n+1} u_{p+3}$. donc $\mathcal{P}(p+2)$ est vraie.

- Conclusion: $\forall p \in \mathbb{N}$, $\mathcal{P}(p)$ est vraie.

2-c- Soit $\mathcal{P}(q)$: "$\forall n \in \mathbb{N}^*$, $u_n \mid u_{qn}$". Montrons par récurrence sur q que $\forall q \in \mathbb{N}^*$, $\mathcal{P}(q)$ est vraie.

- initialisation : Soit $n \in \mathbb{N}^*$ si $q=1$, $u_{qn} = u_n$ et $u_n \mid u_n$ donc $\mathcal{P}(1)$ vraie
- hérédité: supposons qu'il existe $q \in \mathbb{N}^*$ tq $\mathcal{P}(q)$ vraie. Montrons que $\mathcal{P}(q+1)$ vraie. Soit $n \in \mathbb{N}^*$

$u_{(q+1)n} = u_{qn+n} = u_{n+qn} = u_n u_{qn-1} + u_{n+1} u_{qn}$ d'après 2-b-

or $u_n \mid u_{qn}$ donc $\exists c \in \mathbb{N} / u_{qn} = c u_n$

d'où $u_{(q+1)n} = u_n u_{qn-1} + u_{n+1} \cdot c \cdot u_n = u_n \underbrace{(u_{qn-1} + u_{n+1} c)}_{\in \mathbb{N}}$

Ainsi $u_n \mid u_{(q+1)n}$ et $\mathcal{P}(q+1)$ vraie.

- Conclusion: $\forall q \in \mathbb{N}^*$, $\mathcal{P}(q)$ vraie.

2-d Soit $d = n \wedge m$.

$d \mid n$ et $d \mid m$

donc $\exists k_1 \in \mathbb{N} \exists k_2 \in \mathbb{N} /$ $n = k_1 d$ et $m = k_2 d$

D'après 2-c on a donc $u_d \mid u_{k_1 d}$ et $u_d \mid u_{k_2 d}$, soit $u_d \mid u_n$ et $u_d \mid u_m$ donc u_d est un diviseur commun à u_n et à u_m donc $u_d \mid (u_n \wedge u_m)$.

Conclusion : $u_{n \wedge m} \mid u_n \wedge u_m$.

Partie 2 :

1- Si $k=1$, le reste de la division euclidienne de $1 \times x$ par 26 est égal à x dans la mesure où $0 \leq x \leq 25$.

la lettre cryptée est la lettre donnée --- le cryptage est inopérant ...

2-a- $x = 8$

$11 \cdot x = 88$

$88 = 3 \times 26 + 10$

la lettre cryptée est K.

2-b- JKQS

3-a. $19 \times 11 = 209$

$209 = 26 \times 8 + 1$ et $0 \leq 1 < 26$

donc le reste de 19×11 dans la division euclidienne par 26 est 1.

3-b. i. c'est y par définition

ii. On a $11 \times x = 26 \times q + y$ avec $q \in \mathbb{N}$ et $0 \leq y < 26$

donc $19 \times y = 19(11x - 26q)$

$= 19 \times 11x - 26 \times 19q$

$= (26 \times 8 + 1)x - 26 \times 19q$

$= 26[8 - 19q] + x$, avec $0 \leq x < 26$

le reste de $19y$ dans la division euclidienne par 26 est x

3-c. LEO

4-a. 1 - 3 - 5 - 21

4-b. le reste de la division euclidienne de 1×1 par 26 est 1

le reste de la division euclidienne de 3×9 par 26 est 1

le reste de la division euclidienne de 5×21 par 26 est 1

($21 \times 5 = 105 = 26 \times 4 + 1$).

On en déduit que une clé de décryptage associée à

1	est 1
3	est 9
5	est 21
21	est 5