ISM MP, Mathématiques
Année 2023/2024

# Préparation à l'oral python - Feuille n°1

## Exercice 1 (Centrale 2022)

On pose $$\forall n \in \mathbb{N} \qquad \mathrm{I}_n = \int_{-1}^{1} (1+t)^n \mathrm{e}^{-nt}\,\mathrm{d}t$$

1. Représenter les termes de la suite $(\sqrt{n}\mathrm{I}_n)_{n\in[\![ 100\,;\,500 ]\!]}$. Qu'observe-t-on ?
   On pose
   $$\forall t \in \mathbb{R} \qquad f(t) = (1+t)\mathrm{e}^{-t} \quad \text{et} \quad \forall t \in \,]-1\,;0\,[\, \cup \,]\,0\,;+\infty\,[ \qquad \varphi(t) = -\frac{1}{t^2}\ln f(t)$$
2. Montrer que la fonction $\varphi$ se prolonge par continuité en zéro. Que peut-on dire de $\varphi(t)$ lorsque $t \to -1$ ?
3. À l'aide de l'outil informatique, établir l'existence de $a > 0$ tel que
   $$\forall t \in \,]-1\,;1\,[ \qquad \varphi(t) \geqslant a$$
   On pose $$\forall (n,t) \in \mathbb{N}^* \times \mathbb{R} \qquad f_n(t) = f\left(\frac{t}{\sqrt{n}}\right)^n$$
4. Établir $$\forall t \in \mathbb{R} \qquad f_n(t) \xrightarrow[n\to\infty]{} \mathrm{e}^{-\frac{t^2}{2}}$$
5. En déduire $$\mathrm{I}_n \underset{n\to+\infty}{\sim} \sqrt{\frac{2\pi}{n}}$$
   On pose $$\forall n \in \mathbb{N}^* \qquad \mathrm{J}_n = \int_{1}^{+\infty} (1+t)^n \mathrm{e}^{-nt}\,\mathrm{d}t$$
6. Montrer $$\forall n \in \mathbb{N}^* \qquad n! = \mathrm{e}^{-n} n^{n+1}(\mathrm{I}_n + \mathrm{J}_n)$$
7. Établir $$\mathrm{J}_n \underset{n\to+\infty}{=} \mathrm{o}(\mathrm{I}_n)$$
   Retrouver la formule de Stirling.

**Corrigé :** 1. On saisit :

```
def I(n):
    return integr.quad(lambda t:np.exp(-n*t)*(1+t)**n,-1,1)[0]

tn=range(100,501)
trI=[np.sqrt(n)*I(n) for n in tn]
plt.plot(tn,trI)
plt.show()
```

On observe :

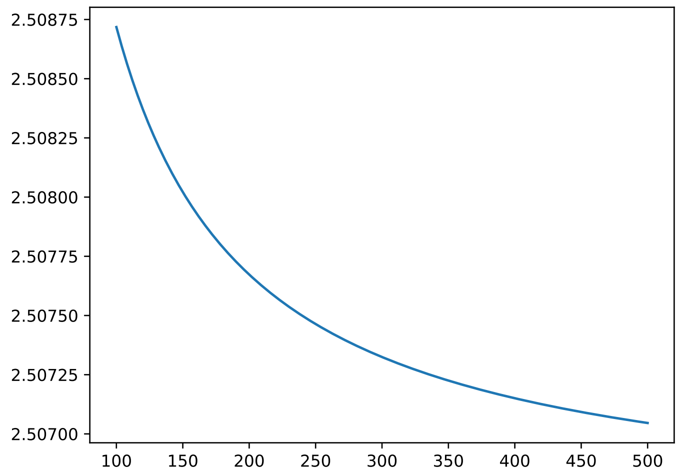


FIGURE 1 – Tracé de la suite $(\sqrt{n}\mathrm{I}_n)_n$

On peut conjecturer $\boxed{\text{La suite } (\sqrt{n}\mathrm{I}_n)_n \text{ converge.}}$

2. Soit $t > -1$ avec $t \neq 0$. On a

$$\varphi(t) = -\frac{1}{t^2}\left(\ln(1+t) - t\right) \underset{t\to 0}{=} -\frac{1}{t^2}\left(t - \frac{t^2}{2} + \mathrm{o}(t^2) - t\right) \xrightarrow[t\to 0]{} \frac{1}{2}$$

et
$$\varphi(t) \underset{t\to -1}{\sim} -\ln(1+t)$$

Ainsi $\boxed{\text{La fonction } \varphi \text{ se prolonge par continuité en zéro et } \varphi(t) \xrightarrow[t\to -1]{} +\infty.}$

Dans toute la suite, on confond $\varphi$ avec son prolongement par continuité en zéro.

3. On saisit :

```
def phi(t):
    if t!=0:
        return -(np.log(1+t)-t)/t**2
    else:
        return .5

tt=np.linspace(-1,1,100)
tphi=[phi(t) for t in tt]
plt.plot(tt,tphi)
plt.show()
```

On observe :

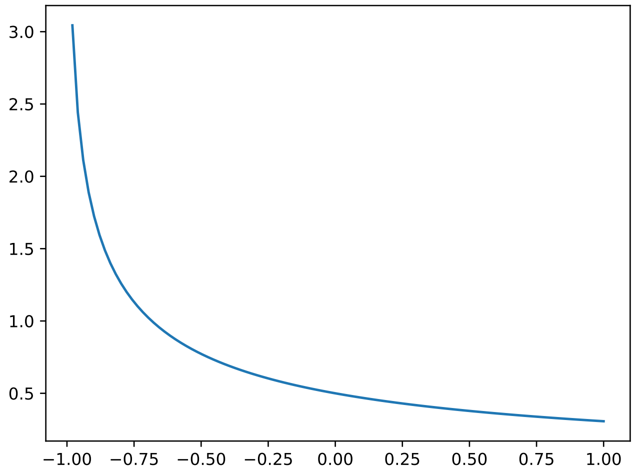


FIGURE 2 – Graphe de $y = \varphi(x)$

On conjecture que $\boxed{\text{La fonction } \varphi \text{ décroît sur } ]-1\,;1\,[.}$

Par dérivation, il vient pour $t > -1$ et $t \neq 0$

$$\varphi'(t) = \frac{\mathrm{N}(t)}{(1+t)t^3} \quad \text{avec} \quad \mathrm{N}(t) = 2(1+t)\ln(1+t) - 2t - t^2$$

puis
$$\mathrm{N}'(t) = 2(\ln(1+t) - t)$$

On a $\mathrm{N}'(t) \leqslant 0$ par concavité de ln et $\mathrm{N}(0) = 0$. La fonction N prend des valeurs positives sur $]-1\,;0\,[$ et négatives sur $]\,0\,;1\,[$. Par conséquent, la fonction $\varphi'$ est négative sur $]-1\,;1\,[\setminus\{0\}$ et on en déduit la décroissance de $\varphi$ sur $]-1\,;1\,[$ et comme $\varphi(t) \xrightarrow[t\to 1]{} 1 - \ln 2 > 0$, on conclut

$$\boxed{\forall t \in\, ]-1\,;1\,[ \qquad \varphi(t) \geqslant a \quad \text{avec} \quad a = 1 - \ln 2 > 0}$$

4. Soit $(n,t) \in \mathbb{N}^* \times\, ]-1\,;1\,[$. On a $1 + \dfrac{t}{\sqrt{n}} > 0$ pour $n$ assez grand et

$$\begin{aligned} f_n(t) &= \exp\left(n\ln\left(1+\frac{t}{\sqrt{n}}\right) - \sqrt{n}t\right) \\ &= \exp\left(n\left(\frac{t}{\sqrt{n}} - \frac{t^2}{2n} + \mathrm{o}\left(\frac{1}{n}\right)\right) - \sqrt{n}t\right) \\ f_n(t) &= \exp\left(-\frac{t^2}{2} + \mathrm{o}(1)\right) \end{aligned}$$

Ainsi
$$\boxed{\forall t \in \mathbb{R} \qquad f_n(t) \xrightarrow[n\to\infty]{} \mathrm{e}^{-\frac{t^2}{2}}}$$

5. Soit $n$ entier non nul. Avec le changement de variables $t = \dfrac{u}{\sqrt{n}}$, on obtient

$$\mathrm{I}_n = \frac{1}{\sqrt{n}}\int_{-\sqrt{n}}^{\sqrt{n}} \left(1+\frac{u}{\sqrt{n}}\right)^n \mathrm{e}^{-u\sqrt{n}}\,\mathrm{d}u$$

On pose
$$\forall (n,u) \in \mathbb{N}^* \times \mathbb{R} \qquad g_n(u) = \begin{cases} \left(1+\dfrac{u}{\sqrt{n}}\right)^n \mathrm{e}^{-u\sqrt{n}} & \text{si } |u| < \sqrt{n} \\ 0 & \text{sinon} \end{cases}$$

Ainsi $$\forall n \in \mathbb{N}^* \qquad \sqrt{n}\mathrm{I}_n = \int_{-\infty}^{+\infty} g_n(u)\,\mathrm{d}u$$

Soit $n$ entier non nul et $u \in \,]-\sqrt{n}\,;\sqrt{n}\,[$. On a
$$g_n(u) = \exp\left(-u^2\varphi\left(\frac{u}{\sqrt{n}}\right)\right) \leqslant \exp\left(-au^2\right)$$

et la majoration vaut aussi pour $|u| \geqslant \sqrt{n}$. La fonction $u \mapsto \mathrm{e}^{-au^2}$ est intégrable sur $\mathbb{R}$ et on conclut par convergence dominée
$$\sqrt{n}\mathrm{I}_n \xrightarrow[n\to\infty]{} \int_{-\infty}^{+\infty} \mathrm{e}^{-\frac{u^2}{2}}\,\mathrm{d}u = \sqrt{2\pi}$$

Ainsi $$\boxed{\mathrm{I}_n \underset{n\to+\infty}{\sim} \sqrt{\frac{2\pi}{n}}}$$

6. Soit $n$ entier non nul. Par relation de Chasles puis changement de variables, il vient
$$\mathrm{I}_n + \mathrm{J}_n = \int_{-1}^{+\infty} (1+t)^n\mathrm{e}^{-nt}\,\mathrm{d}t = \int_0^{+\infty} u^n\mathrm{e}^{-nu+n}\,\mathrm{d}u = \mathrm{e}^n\int_0^{+\infty} u^n\mathrm{e}^{-nu}\,\mathrm{d}u$$

Avec le changement de variables $v = nu$ et des intégrations parties, on obtient
$$\mathrm{I}_n + \mathrm{J}_n = \frac{\mathrm{e}^n}{n^{n+1}}\int_0^{+\infty} v^n\mathrm{e}^{-v}\,\mathrm{d}v = \frac{\mathrm{e}^n}{n^{n+1}}n!$$

Ainsi $$\boxed{\forall n \in \mathbb{N}^* \qquad n! = \mathrm{e}^{-n}n^{n+1}(\mathrm{I}_n + \mathrm{J}_n)}$$

7. Soit $n$ entier non nul. Avec le changement de variables $t = \dfrac{u}{\sqrt{n}}$, on obtient
$$\mathrm{J}_n = \frac{1}{\sqrt{n}}\int_{\sqrt{n}}^{+\infty} \left(1+\frac{u}{\sqrt{n}}\right)^n \mathrm{e}^{-u\sqrt{n}}\,\mathrm{d}u$$

On pose $$\forall (n,u) \in \mathbb{N}^* \times \mathbb{R}_+ \qquad h_n(u) = \begin{cases} \left(1+\dfrac{u}{\sqrt{n}}\right)^n \mathrm{e}^{-u\sqrt{n}} & \text{si } u \geqslant \sqrt{n} \\ 0 & \text{sinon} \end{cases}$$

Sans difficulté, on trouve $$\forall u \geqslant 0 \qquad h_n(u) \xrightarrow[n\to\infty]{} 0$$

Soit $u \geqslant 0$. On pose $$\forall x > 0 \qquad \psi(x) = x^2\ln\left(1+\frac{u}{x}\right) - ux$$

La fonction $\psi$ est dérivable et il vient
$$\begin{aligned} \forall x > 0 \qquad \psi'(x) &= 2x\ln\left(1+\frac{u}{x}\right) - \frac{t}{1+u/x} - u \\ &= \frac{2x}{1+u/x}\left[\left(1+\frac{u}{x}\right)\ln\left(1+\frac{u}{x}\right) - \frac{u}{x} - \frac{1}{2}\left(\frac{u}{x}\right)^2\right] \end{aligned}$$

On pose enfin $$\forall s \geqslant 0 \qquad \chi(s) = (1+s)\ln(1+s) - s - \frac{s^2}{2}$$

La fonction $\chi$ est dérivable et on trouve par concavité du ln
$$\forall s \geqslant 0 \qquad \chi'(s) = \ln(1+s) + 1 - 1 - s \leqslant 0$$

Avec $\chi(0) = 0$, il s'ensuit que $\chi(s) \leqslant 0$ pour $s \geqslant 0$ d'où

$$\forall x > 0 \qquad \psi'(x) = \frac{2x}{1+u/x}\chi\left(\frac{u}{x}\right) \leqslant 0$$

Par conséquent $$\forall n \in \mathbb{N}^* \qquad \psi(\sqrt{n}) \leqslant \psi(1)$$

c'est-à-dire $$\forall n \in \mathbb{N}^* \qquad n \ln\left(1+\frac{u}{\sqrt{n}}\right) - u\sqrt{n} \leqslant \ln(1+u) - u$$

et passant à l'exponentielle qui est croissante, on obtient

$$\forall (n,u) \in \mathbb{N}^* \times \mathbb{R}_+ \qquad h_n(u) \leqslant (1+u)\mathrm{e}^{-u}$$

Cette dominante est intégrable et par convergence dominée, il vient

$$\sqrt{n}\mathrm{J}_n \xrightarrow[n\to\infty]{} 0$$

D'où $$\boxed{\mathrm{J}_n \underset{n\to+\infty}{=} \mathrm{o}(\mathrm{I}_n)}$$

Il s'ensuit $$n! = \mathrm{e}^{-n}n^{n+1}\left(\sqrt{\frac{2\pi}{n}} + \mathrm{o}\left(\frac{1}{\sqrt{n}}\right)\right)$$

Et on conclut $$\boxed{n! \underset{n\to+\infty}{\sim} \sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^n}$$

## Exercice 2 (Centrale 2022)

Un *nombre de Carmichael* est un entier $n \geqslant 2$ non premier tel que

$$\forall a \in \mathbb{Z} \qquad a^n \equiv a\ [n]$$

1. Soit $n \geqslant 2$ non premier tel que

   $$\forall a \in [\![ 0\,;\, n-1 ]\!] \qquad a^n \equiv a\ [n]$$

   Montrer que $n$ est un nombre de Carmichael.
2. Écrire une fonction `carmichael(n)` d'argument `n` entier qui renvoie `True` si $n$ est un nombre de Carmichael et `False` sinon.
3. Déterminer à l'aide de l'outil informatique le plus petit nombre de Carmichael.
4. Soit $n = \prod_{i=1}^{r} p_i$ avec $r \geqslant 2$ et les $p_i$ des nombres premiers deux à deux distincts vérifiant $p_i - 1 | n-1$ pour tout $i \in [\![ 1\,;\, r ]\!]$.

   (a) Montrer $\quad \forall i \in [\![ 1\,;\, r ]\!] \qquad \forall a \in \mathbb{Z} \qquad a^n \equiv a\ [p_i]$

   (b) Montrer que $n$ est un nombre de Carmichael.
5. Soit $n$ un nombre de Carmichael. Montrer que $n$ est un produit de nombres premiers deux à deux distincts.
6. Soit $(\mathrm{G}, \times)$ un groupe abélien fini.

   (a) Soient $x$, $y$ dans G avec $o(x) \wedge o(y) = 1$. Montrer que $o(xy) = o(x)o(y)$.

   (b) Soit $x \in \mathrm{G}$. Pour $d$ diviseur de $o(x)$, montrer qu'il existe un élément de G d'ordre $d$.

   (c) Soit $m$ l'ordre maximal des éléments de G. Montrer que l'ordre de tout élément de G divise $m$.

(d) En déduire $\qquad \forall p \in \mathcal{P} \qquad \mathrm{U}(\mathbb{Z}/p\mathbb{Z}) \simeq \mathbb{Z}/(p-1)\mathbb{Z}$

7. Soit $n$ un nombre de Carmichael et $p$ un diviseur premier de $n$. Montrer que $p-1|n-1$.

**Corrigé :** 1. Soit $n$ entier $\geqslant 2$ vérifiant la condition annoncée et soit $a \in \mathbb{Z}$. D'après le théorème de la division euclidienne, on dispose d'un unique couple $(q,r) \in \mathbb{Z} \times [\![ 0\,; n-1 ]\!]$ tel que $a = qn+r$. Dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$, on a

$$\bar{a}^n = \bar{r}^n = \bar{r} = \bar{a}$$

Ainsi $\boxed{\text{L'entier } n \text{ est un nombre de Carminchael.}}$

2. Pour tester si un entier $n \geqslant 2$ est un nombre de Carmichael, on commence par tester sa non primalité. S'il existe $d$ un diviseur strict de $n$, alors on a $d \leqslant \sqrt{n}$ ou $\dfrac{n}{d} \leqslant n$. Sinon, on aurait $d > \sqrt{n}$ et $\dfrac{n}{d} > \sqrt{n}$ d'où $n > n$ ce qui est absurde. On saisit :

```
def carmichael(n):
    d=2
    diviseur_trouve=False
    while d**2<=n and not diviseur_trouve:
        if n%d==0:
            diviseur_trouve=True
        d+=1
    if not diviseur_trouve:
        return False
    for k in range(n):
        if (k**n)%n!=k:
            return False
    return True
```

3. On saisit :

```
n=2
while not carmichael(n):
    n+=1
print("Premier nombre de Carmichael=",n)
```

On obtient :

```
Premier nombre de Carmichael= 561
```

On peut améliorer la performance de cette fonction en procédant différemment et en gardant la mémoire des nombres premiers rencontrés au cours des itérations :

```
P=[2]

def carmichael(n):
    global P
    est_premier=True
    for p in P:
        if n%p==0:
```

```
            est_premier=False
    if est_premier:
        P.append(n)
        return False
    for k in range(n):
        if (k**n)%n!=k:
            return False
    return True
```

Puis, on saisit en démarrant à $n = 3$ (on sait que 2 n'est pas de Carmichael puisqu'il n'est pas premier) :

```
n=3
while not carmichael(n):
    n+=1
print("Premier nombre de Carmichael=",n)
```

La liste `P` est enrichie à chaque appel de la fonction `carmichael` des nouveaux nombres premiers rencontrés ce qui permet d'accélérer le test de non primalité.

4.(a) Soit $i \in [\![ 1\,;\, r ]\!]$ et $a \in \mathbb{Z}$. Si $p_i$ divise $a$, alors $p_i$ divise $a^n$ et l'égalité a lieu. Supposons que $p_i$ ne divise par $a$ ce qui éguivaut à $a \wedge p_i = 1$. D'après le petit théorème de Fermat, on a donc

$$a^{p_i-1} \equiv 1\ [p_i]$$

Comme $p_i - 1 | n - 1$, on dispose de $q_i$ entier non nul tel que $n - 1 = q_i(p_i - 1)$. Par suite, il vient

$$a^n \equiv \left(a^{p_i-1}\right)^{q_i} a \equiv a\ [p_i]$$

On conclut $\boxed{\forall i \in [\![ 1\,;\, r ]\!] \qquad \forall a \in \mathbb{Z} \qquad a^n \equiv a\ [p_i]}$

4.(b) Les $p_i$ sont des nombres premiers deux à deux distincts et sont donc deux à deux premiers entre eux. D'après le théorème chinois, l'application

$$\pi : \begin{cases} \mathbb{Z}/n\mathbb{Z} \longrightarrow \prod_{i=1}^{r} \mathbb{Z}/p_i\mathbb{Z} \\ \bar{a}^{[n]} \quad \longmapsto \left(\bar{a}^{[p_i]}\right)_{1 \leqslant i \leqslant r} \end{cases}$$

est un isomorphisme d'anneaux. Ainsi, pour $a \in \mathbb{Z}$, on a

$$\overline{a^n}^{[n]} = \bar{a}^{[n]} \iff \pi(\overline{a^n}^{[n]}) = \pi(\bar{a}^{[n]}) \iff \forall i \in [\![ 1\,;\, r ]\!] \qquad \overline{a^n}^{[p_i]} = \bar{a}^{[p_i]}$$

et comme la dernière assertion est vraie d'après le résultat de la question précédente, on conclut

$$\boxed{\text{L'entier } n \text{ est un nombre de Carmichael.}}$$

5. Supposons qu'il existe $p$ premier et $\alpha$ entier $\geqslant 2$ tel que $p^\alpha | n$. Comme le nombre $n$ est de Carmichael, on a $p^n \equiv p\ [n]$ d'où $p^n \equiv p\ [p^2]$ ce qui signifie qu'on dispose de $q \in \mathbb{Z}$ tel que $p^n = p + qp^2$ d'où

$$p(p^{n-2} - q) = 1$$

ce qui est absurde. Ainsi, les valuations des facteurs premiers dans la décomposition de $n$ sont égales à 1 et il n'y a pas qu'un facteur premier sans quoi l'entier $n$ serait premier. On conclut

$$\boxed{\text{Un nombre de Carmichael est produit de nombres premiers deux à deux distincts.}}$$

6.(a) On a $$(xy)^{o(x)o(y)} = (x^{o(x)})^{o(y)}(y^{o(y)})^{o(x)} = 1$$
d'où $o(xy)|o(x)o(y)$. Puis, on a $(xy)^{o(xy)} = 1$ d'où
$$(xy)^{o(xy)o(x)} = (x^{o(x)})^{o(xy)}y^{o(xy)o(x)} = y^{o(xy)o(y)} = 1$$
d'où $o(y)|o(xy)o(x)$ et comme $o(x) \wedge o(y) = 1$, il s'ensuit $o(y)|o(xy)$ d'après le lemme de Gauss. Par symétrie des rôles, on a également $o(x)|o(xy)$ d'où $o(x) \vee o(y)|o(xy)$. Or, on a
$$o(xy) = (o(x) \wedge o(y))(o(x) \vee o(y)) = o(x) \vee o(y)$$
Ceci prouve que $o(x)o(y)|o(x)o(y)$ et les entiers $o(xy)$ et $o(x)o(y)$ sont donc des entiers associés. On conclut
$$\boxed{o(xy) = o(x)o(y)}$$
**Variante :** On peut aussi observer
$$(xy)^{o(xy)} = 1 \iff \underbrace{x^{o(xy)}}_{\in\langle x\rangle} = \underbrace{y^{-o(xy)}}_{\in\langle y\rangle}$$
Or, l'intersection $\langle x\rangle \cap \langle y\rangle$ est sous-groupe de $\langle x\rangle$ et de $\langle y\rangle$ donc d'ordre divisant $o(x)$ et $o(y)$ d'où $\langle x\rangle \cap \langle y\rangle = 1$. On en déduit
$$x^{o(xy)} = 1 \quad \text{et} \quad y^{o(xy)} = 1$$
d'où $o(x)|o(xy)$ et $o(y)|o(xy)$ et on conclut comme précédemment.
6.(b) Soit $x \in \mathrm{G}$ et $d$ diviseur de $o(x)$. On dispose de $c$ entier non nul tel que $o(x) = dc$. On a $(x^c)^d = x^{dc} = 1$ d'où $d|o(x^c)$. Puis, on a $(x^c)^{o(x^c)} = 1 = x^{co(x^c)}$ d'où $o(x)|co(x^c)$, c'est-à-dire $dc|co(x^c)$ d'où $d|o(x^c)$. Les entiers $d$ et $o(x^c)$ sont associés donc égaux et par conséquent
$$\boxed{\text{Il existe un élément de G d'ordre } d.}$$
6.(c) La quantité $\max\{o(x), x \in \mathrm{G}\}$ est bien définie comme maximum d'une partie finie non vide. On note $m = \max\{o(x), x \in \mathrm{G}\}$ et $x \in \mathrm{G}$ tel que $o(x) = m$. Supposons qu'il existe $y \in \mathrm{G}$ tel que $o(y)$ ne divise pas $o(x)$. Ainsi, on dispose de $q \in \mathcal{P}$ tel que $v_q(o(y)) > v_q(o(x))$. D'après le résultat de la question précédente, on dispose de $x' \in \mathrm{G}$ d'ordre $\displaystyle\prod_{p\in\mathcal{P}\smallsetminus\{q\}} p^{v_p(o(x))}$ et de $y' \in \mathrm{G}$ d'ordre $p^{v_p(o(y))}$. Or, on a
$$q^{v_q(o(y)} \wedge \prod_{p\in\mathcal{P}\smallsetminus\{q\}} p^{v_p(o(x)} = 1$$
et d'après le résultat de la question 6.(a), on obtient
$$o(x'y') = o(x')o(y') = q^{v_q(o(y))} \prod_{p\in\mathcal{P}\smallsetminus\{q\}} p^{v_p(o(x))} > o(x)$$
ce qui est absurde par maximalité de $o(x)$. On conclut
$$\boxed{\text{L'ordre de tout élément de G divise } m.}$$
6.(d) Soit $p \in \mathcal{P}$. Le groupe $(\mathrm{U}(\mathbb{Z}/p\mathbb{Z}), \times)$ est d'ordre $p-1$. Notons $m$ l'ordre maximal des éléments de G. On a $\bar{x}^m = \bar{1}$ pour tout $\bar{x} \in \mathrm{U}(\mathbb{Z}/p\mathbb{Z})$ d'après le résultat de la question précédente. Comme l'anneau $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps, le polynôme $\mathrm{X}^m - \bar{1}$ de $\mathbb{Z}/p\mathbb{Z}[\mathrm{X}]$ admet au plus $m$ racines distinctes (résultat qui n'est pas officiellement au programme, à savoir redémontrer par récurrence sur le degré avec une factorisation de Bernoulli). Ainsi, on a $p - 1 \leqslant m$ et comme l'ordre d'un élément d'un groupe divise l'ordre du groupe, on a aussi $m|p-1$ d'où $m \leqslant p-1$ et par conséquent $m = p - 1$ ce qui prouve que le groupe $(\mathrm{U}(\mathbb{Z}/p\mathbb{Z}), \times)$ admet un générateur. On conclut

$$\boxed{\forall p \in \mathcal{P} \qquad \mathrm{U}(\mathbb{Z}/p\mathbb{Z}) \simeq \mathbb{Z}/(p-1)\mathbb{Z}}$$

7. Pour $a \in \mathbb{Z}$, on a $a^n \equiv a\ [n]$ d'où $a^n \equiv a\ [p]$. Pour $a[\![ 1\,;\, p-1 ]\!]$, on a $\bar{a} \in \mathrm{U}(\mathbb{Z}/p\mathbb{Z})$ et il vient

$$\bar{a}^{n-1} = \bar{a}^{-1}\bar{a}^n = \bar{a}^{-1}\bar{a} = \bar{1}$$

Comme le groupe $(\mathrm{U}(\mathbb{Z}/p\mathbb{Z}), \times)$ est cyclique, on choisit $a \in [\![ 1\,;\, p-1 ]\!]$ d'ordre égal à $p-1$. Ainsi, on trouve

$$\boxed{o(\bar{a}) = p - 1 | n - 1}$$

**Commentaire :** On a donc établi l'équivalence suivante :

$$\boxed{\begin{array}{l}\text{Le nombre } n \geqslant 2 \text{ est de Carmichael si et seulement si } n = \displaystyle\prod_{i=1}^{r} p_i \text{ avec } r \geqslant 2 \text{ et les } p_i \\ \text{des nombres premiers distincts vérifiant } p_i - 1 | n - 1 \text{ pour tout } i \in [\![ 1\,;\, r ]\!].\end{array}}$$

## Exercice 3 (Centrale 2019)

On effectue $n$ lancers de pièces indépendants et la probabilité d'obtenir pile au $k$-ième lancer est notée $p_k$. On note $\mathrm{X}_n$ le nombre de piles obtenus au cours de ces $n$ lancers et $\pi_n$ la probabilité que $\mathrm{X}_n$ soit pair.

1. (a) Écrire une fonction `pi(n,p)` qui donne une estimation de $\pi_n$ pour la fonction $p$. Elle doit effectuer 1000 simulations.
   (b) Représenter $\pi_n$ en fonction de $n \in [\![ 0\,;\, 100 ]\!]$ pour $p_n = \dfrac{1}{2(n+1)}$ puis $p_n = \dfrac{1}{2(n+1)^2}$.
   (c) Représenter $\pi_{100}$ en fonction de $\alpha \in [\,0\,;6\,]$ pour $p_n = \dfrac{1}{2(n+1)^\alpha}$.
2. Exprimer $\pi_n$ en fonction des $p_k$. On pourra considérer la suite $u_n = \pi_n - \dfrac{1}{2}$.
3. Calculer $\displaystyle\lim_{n\to+\infty} \pi_n$ quand $p_n = \dfrac{1}{2(n+1)}$ puis $p_n = \dfrac{1}{2(n+1)^2}$. Que se passe-t-il quand la pièce est équilibrée ?
4. Montrer que si $p_k < \dfrac{1}{2}$ pour tout $k$ entier, alors $(\pi_n)_n$ tend vers une limite $\ell \in \left[\dfrac{1}{2}\,;1\right]$.
   Montrer que $\ell = \dfrac{1}{2}$ si et seulement si la série $\sum p_n$ diverge.

**Corrigé :** 1.(a) On saisit :

```
def pi(n,p):
    N=1000
    res=0
    for i in range(N):
        S=0
        for k in range(1,n+1):
            if rd.rand()<p(k):
                S+=1
        if S%2==0:
            res+=1
    return res/N
```

1.(b) On saisit :

```
def p1(n):
    return 1/(2*(n+1))

def p2(n):
    return 1/(2*(n+1)**2)

tn=range(101)
tpi1=[pi(n,p1) for n in tn]
plt.scatter(tn,tpi1)
plt.grid();plt.show()

tpi2=[pi(n,p2) for n in tn]
plt.scatter(tn,tpi2)
plt.grid();plt.show()
```

On observe :

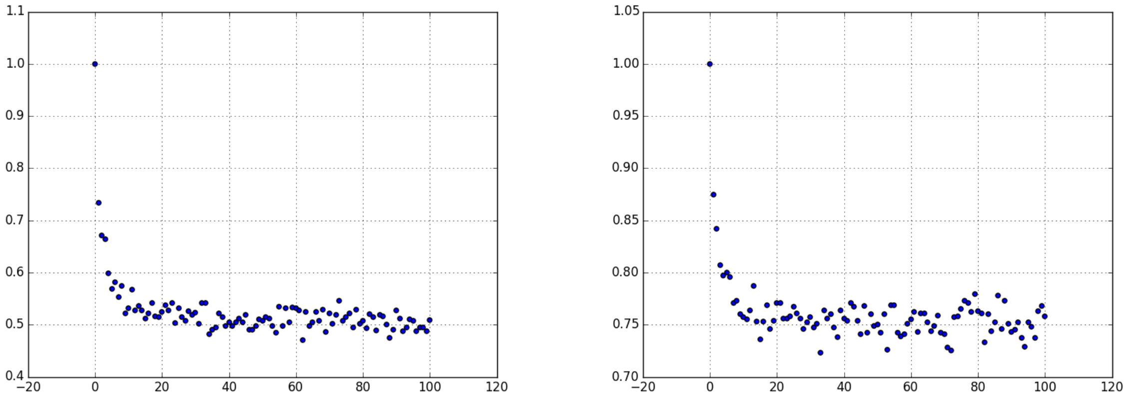


FIGURE 3 – Tracé de $(\pi_n)_n$

On conjecture que pour chacun des scénarios considérés

$$\boxed{\pi_n \xrightarrow[n\to\infty]{} \frac{1}{2} \quad \text{et} \quad \pi_n \xrightarrow[n\to\infty]{} \frac{3}{4}}$$

1.(c) On saisit :

```
ta=np.linspace(0,6,100)
tpi3=[pi(100,lambda n:1/(2*(n+1)**a)) for a in ta]
plt.plot(ta,tpi3)
plt.grid();plt.show()
```

On observe :

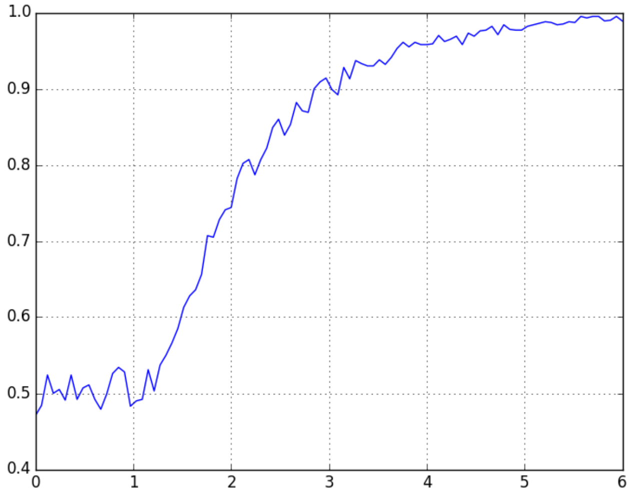


Figure 4 – Tracé du graphe $\alpha \mapsto \pi_{100}$

On conjecture $$\boxed{\forall \alpha \in [\,0\,;1\,] \qquad \lim_{n\to+\infty} \pi_n = \frac{1}{2}}$$

2. Soit $n$ entier. D'après la formule des probabilités totales, on obtient

$$\begin{aligned}\pi_{n+1} &= \mathbb{P}(\mathrm{X}_{n+1} \text{ pair}, \mathrm{X}_n \text{ pair}) + \mathbb{P}(\mathrm{X}_{n+1} \text{ pair}, \mathrm{X}_n \text{ impair})\\ &= \mathbb{P}(\mathrm{F}_{n+1}, \mathrm{X}_n \text{ pair}) + \mathbb{P}(\mathrm{P}_{n+1}, \mathrm{X}_n \text{ impair})\end{aligned}$$

Par indépendance des lancers, on trouve

$$\pi_{n+1} = (1 - p_{n+1})\pi_n + p_{n+1}(1 - \pi_n)$$

Puis $$u_{n+1} + \frac{1}{2} = (1 - p_{n+1})\left(u_n + \frac{1}{2}\right) + p_{n+1}\left(\frac{1}{2} - u_n\right)$$

d'où $$u_{n+1} = (1 - 2p_{n+1})u_n$$

On en déduit, par récurrence ou avec un produit téléscopique

$$\boxed{\forall n \in \mathbb{N} \qquad u_n = 2^{n-1}\prod_{k=1}^{n}\left(\frac{1}{2} - p_k\right)}$$

3. On suppose $p_n = \dfrac{1}{2(n+1)}$ pour $n$ entier. On a

$$u_n = 2^{n-1}\prod_{k=1}^{n}\left(\frac{1}{2} - \frac{1}{2(k+1)}\right) = \frac{1}{2}\prod_{k=1}^{n}\left(\frac{k}{k+1}\right) = \frac{1}{2(n+1)} \xrightarrow[n\to\infty]{} 0$$

et par conséquent $$\boxed{\text{Si } p_n = \frac{1}{2(n+1)} \text{ pour } n \text{ entier, alors } \pi_n \xrightarrow[n\to\infty]{} \frac{1}{2}.}$$

On suppose ensuite $p_n = \dfrac{1}{2(n+1)^2}$ pour $n$ entier. On a

$$u_n = 2^{n-1}\prod_{k=1}^{n}\left(\frac{1}{2} - \frac{1}{2(k+1)^2}\right) = \frac{1}{2}\prod_{k=1}^{n}\left(\frac{k}{k+1}\,\frac{k+2}{k+1}\right) = \frac{1}{2}\,\frac{1}{n+1}\,\frac{n+2}{2} \xrightarrow[n\to\infty]{} \frac{1}{4}$$

Ainsi $$\boxed{\text{Si } p_n = \frac{1}{2(n+1)^2} \text{ pour } n \text{ entier, alors } \pi_n \xrightarrow[n\to\infty]{} \frac{3}{4}.}$$

4. Soit $n$ entier. On a $$\ln u_n = -\ln 2 + \sum_{k=1}^{n} \ln(1-2p_k)$$

Supposons $p_k < \dfrac{1}{2}$ pour tout $k$ entier. Il s'ensuit $1 \geqslant 1 - 2p_k > 0$ pour tout $k$ entier. La série $\sum \ln(1-2p_k)$ est donc à terme négatifs. Si $(p_k)_k$ ne tend pas vers zéro, la série diverge grossièrement donc sa somme partielle tend vers $-\infty$. Si $(p_k)_k$ tend vers zéro, on a $\ln(1-2p_k) \underset{k\to+\infty}{\sim} -2p_k$ et les séries $\sum \ln(1-2p_k)$ et $\sum p_k$ sont donc de même nature. Si $\sum p_k$ diverge, la somme partielle de la série $\sum \ln(1-2p_k)$ tend vers $-\infty$ et sinon, elle tend vers une limite finie négative S d'où $\pi_n \xrightarrow[n\to\infty]{} \ell = \dfrac{1}{2}(1+\mathrm{e}^{\mathrm{S}})$. On conclut

$$\boxed{\text{Si } p_k < \frac{1}{2} \text{ pour } k \text{ entier, alors } \pi_n \xrightarrow[n\to\infty]{} \ell \in \left[\frac{1}{2}\,;1\right].}$$

Et l'étude précédente montrer que si $\sum p_n$ diverge, alors $\ell = \dfrac{1}{2}$ et si $\sum p_n$ converge, alors on a $\ell \in \left]\dfrac{1}{2}\,;1\right]$. Ainsi

$$\boxed{\ell = \frac{1}{2} \iff \sum p_n \text{ diverge}}$$