Lycée Louis-Le-Grand, Paris
MPSI 4 – Mathématiques
A. Troesch

Pour le 10/09/2018

DM n° 1 : Révisions et logique

Correction du problème 1 – Pour toutes les formalisations, on notera P_1 le fait que la porte 1 cache une princesse, P_2 de même avec la porte 2, et T_1, T_2 de même avec des tigres. Par ailleurs, on désigne par τ une tautologie. On pourra remarquer que, puisque la cellule ne peut pas contenir à la fois une princesse et un tigre, et puisqu'elle ne peut pas être vide, P_1 et T_1 sont contraires l'un de l'autre et de même pour P_2 et T_2.

1. • Raisonnement intuitif : Si la première affiche est vraie, la deuxième l'est également, ce qui est impossible. Donc la première affiche est fausse, et la seconde vraie. Il y a donc une princesse et un tigre, et la princesse n'est pas derrière la porte 1, donc elle est derrière la porte 2.
   • Formalisation :
   ∗ L'affiche 1 affirme : $F_1 : P_1 \wedge P_2$
   ∗ L'affiche 2 affirme : $F_2 : (P_1 \wedge F_2) \vee (T_1 \wedge P_2)$.
   ∗ Par ailleurs, la propriété $A = (F_1 \wedge \neg F_2) \vee (\neg F_1 \wedge F_2)$ est vraie. Puisque $F_1 \implies F_2$ (du fait de la tautologie $B \implies B \cup C$), on en déduit que

   $$A \equiv \neg F_1 \wedge F_2 \equiv \neg(P_1 \wedge T_2) \wedge ((P_1 \wedge T_2) \vee (T_1 \wedge T_2) \equiv (\neg(P_1 \wedge T_2) \wedge (P_1 \wedge T_2)) \vee (\neg(P_1 \wedge T_2) \wedge (T_1 \wedge P_2)).$$

   Le premier facteur de cette dernière formule étant impossible, il vient :

   $$A \equiv ((T_1 \vee P_2) \wedge (T_1 \wedge P2) \equiv (T_1 \wedge T_1 \wedge P2) \vee (P_2 \wedge T_1 \wedge P_2) \equiv (T_1 \wedge P_2) \vee (T_1 \wedge P_2) \equiv (T_1 \wedge P_2).$$

   On a ici abondamment précisé les simplifications s'opérant dans la formule logique, par distributivité et utilisation des équivalents $B \wedge B \equiv B$ et $B \vee B \equiv B$. Dans les questions suivantes, ces étapes seront passées plus rapidement.

   Conclusion : le prisonnier doit choisir la porte 2.

2. • Raisonnement intuitif : Les affiches ne peuvent pas être toutes les deux fausses, sinon, on déduirait de l'affiche 1 que les deux portes cachent un tigre, et l'affiche 2 serait alors vraie. Ainsi, les affiches sont toutes les deux vraies. L'affiche 2 permet d'affirmer qu'il vaut mieux ne pas choisir la porte 1, et comme d'après l'affiche 1, l'une des deux portes cache une princesse, c'est la porte 2.
   • Formalisation :
   ∗ L'affiche 1 affirme : $F_1 : P_1 \vee P_2$
   ∗ L'affiche 2 affirme : $F_2 : T_1$.
   ∗ Par ailleurs, l'indication du roi permet d'affirmer que la propriété $A = (F_1 \wedge F_2) \vee (\neg F_1 \wedge \neg F_2)$ est vraie. Or :

   $$A \equiv ((P_1 \vee P_2) \wedge T_1) \vee ((T_1 \wedge T_2) \wedge P_1) \equiv (\neg\tau \vee (P_2 \wedge T_1)) \vee \neg\tau \equiv T_1 \wedge P_2.$$

   Conclusion : le prisonnier doit choisir la porte 2.

3. • Raisonnement intuitif : Les deux affiches ne peuvent pas être toutes les deux fausses. En effet, sinon, il y aurait un tigre dans la cellule 1, et l'affiche 1 serait vraie. Ainsi, les deux affiches sont vraies, et il y a une princesse dans la cellule 1 (d'après l'affiche 1), ainsi que dans la cellule 2 (d'après l'affiche 2).
   • Formalisation :
   ∗ L'affiche 1 affirme : $F_1 : T_1 \vee P_2$
   ∗ L'affiche 2 affirme : $F_2 : P_1$.
   ∗ Par ailleurs, l'indication du roi permet d'affirmer que la propriété $A = (F_1 \wedge F_2) \vee (\neg F_1 \wedge \neg F_2)$ est vraie. Or :

   $$A \equiv ((T_1 \vee P_2) \wedge P_1) \vee (P_1 \wedge P_2 \wedge T_1) \equiv (P_1 \wedge P_2) \vee \neg\tau \wedge P_1 \vee P_2.$$

- Conclusion : le prisonnier peut choisir l'une ou l'autre des deux portes.
  Le roi a été clément, et s'est contenté d'infliger une grosse frayeur...

4. - Raisonnement intuitif : La cellule 2 ne peut pas contenir un tigre, car sinon l'affiche 2 serait vraie et amènerait une contradiction. Ainsi, elle contient une princesse, et l'affiche 2 étant fausse, la cellule 1 contient un tigre. On vérifie alors la cohérence du résultat en remarquant que l'affiche 1 est fausse.
   - Formalisation :
     * L'affiche 1 affirme : $F_1 : P_1 \wedge P_2$
     * L'affiche 2 affirme : $F_2 : P_1 \wedge P_2$.
     * Par ailleurs, l'indication du roi permet d'affirmer que la propriété

       $$A = ((P_1 \wedge F_1) \vee (T_1 \wedge \neg F_1)) \wedge ((P_2 \wedge \neg F_2) \vee (T_2 \wedge F_2))$$

       est vraie. En développant et simplifiant cette expression, il vient :

       $$A \equiv ((P_1 \wedge P_2) \vee T_1) \wedge (P_2 \wedge (T_1 \vee T_2)) \equiv ((P_1 \wedge P_2) \vee T_1) \wedge (T_1 \wedge P_2) \equiv T_1 \wedge P_2,$$

       puisque $T_1 \wedge P_2$ et $P_1 \wedge P_2$ sont contradictoires.
   - Conclusion : le prisonnier doit choisir la porte 2.

5. - Raisonnement intuitif : Il y a nécessairement une princesse dans la cellule 2. En effet, l'affiche 1 permet d'affirmer que si la cellule 1 contient une princesse, la cellule 2 aussi (l'affiche 1 étant vraie), et si la cellule 1 contient un tigre, la cellule 2 non (l'affiche 1 étant fausse). On en déduit alors que l'affiche 2 est fausse et que la porte 1 cache un tigre.
   - Formalisation :
     * L'affiche 1 affirme : $F_1 : (P_1 \wedge P_2) \vee (T_1 \wedge T_2)$
     * L'affiche 2 affirme : $F_2 : P_1$.
     * Par ailleurs, l'indication du roi permet d'affirmer que la propriété

       $$A = ((P_1 \wedge F_1) \vee (T_1 \wedge \neg F_1)) \wedge ((P_2 \wedge \neg F_2) \vee (T_2 \wedge F_2))$$

       est vraie. Or, on peut remarquer que

       $$(P_2 \wedge \neg F_2) \vee (T_2 \wedge F_2) \equiv (P_2 \wedge T_1) \vee (P_1 \wedge T_2) \equiv \neg F_1.$$

       On a donc :

       $$A \equiv A \equiv (P_1 \wedge F_1 \wedge \neq F_1) \vee (T_1 \wedge F_1) \equiv T_1 \wedge \neg F_1 \equiv T_1 \wedge P_2.$$
   - Conclusion : le prisonnier doit choisir la porte 2.

6. On interprète l'affiche 2 au sens strict : si elle est vraie, cela signifie qu'il y a un tigre derrière cette porte et une princesse derrière l'autre.
   - Raisonnement intuitif : si la porte 1 cache un tigre, alors l'affiche 1 est fausse, donc la porte 2 cache aussi un tigre. Mais l'affiche 2 est alors fausse d'où une contradition. Ainsi, la porte 1 cache une princesse, et l'affiche 1 étant alors vraie, la porte 2 cache un tigre. On vérifie bien alors la cohérence (véracité de l'affiche 2).
   - Formalisation :
     * L'affiche 1 affirme : $F_1 : (P_1 \wedge T_2) \vee (T_1 \wedge P_2)$
     * L'affiche 2 affirme : $F_2 : P_1 \wedge T_2$.
     * Par ailleurs, l'indication du roi permet d'affirmer que la propriété

       $$A = ((P_1 \wedge F_1) \vee (T_1 \wedge \neg F_1)) \wedge ((P_2 \wedge \neg F_2) \vee (T_2 \wedge F_2))$$

       est vraie. Or :

       $$(P_1 \wedge F_1) \vee (T_1 \wedge \neg F_1) \equiv (P_1 \wedge T_2) \vee (T_1 \wedge (T_2 \vee P_1)) \equiv (P_1 \wedge T_2) \vee (T_1 \wedge T_2) \equiv T_2 \wedge (P_1 \vee T_1) \equiv T_2.$$

       De plus,

       $$(P_2 \wedge \neg F_2) \vee (T_2 \wedge F_2) \equiv (P_2 \wedge (T_1 \vee T_2)) \vee (T_2 \wedge P_1) \equiv (P_2 \wedge T_1) \vee (P_1 \wedge T_2).$$

       On obtient alors :

       $$A \equiv T_2 \wedge ((P_2 \wedge T_1) \vee (P_1 \wedge T_2)) \equiv P_1 \wedge T_2.$$

- Conclusion : $\boxed{\text{le prisionnier doit choisir la porte 1}}$.

Correction du problème 2 – (d'après Bac des années 90)

Partie I –

1. (a) La fonction f est dérivable sur $\mathbb{R}$ en tant que produit de fonctions dérivables, et :

$$\begin{aligned}\forall x \in \mathbb{R}, \quad f'(x) &= \mathrm{e}^{-x}(-\sin(x) + \cos(x)) \\ &= \frac{2}{\sqrt{2}} \cdot \mathrm{e}^{-x}\left(\cos\left(\frac{\pi}{4}\right)\cos(x) - \sin\left(\frac{\pi}{4}\right)\sin(x)\right) \\ &= \sqrt{2} \cdot \mathrm{e}^{-x}\cos\left(x + \frac{\pi}{4}\right)\end{aligned}$$

Ainsi,

$$\forall x \in \mathbb{R}, \quad \boxed{f'(x) = g(x)\cos\left(x + \frac{\pi}{4}\right) \text{ où } g(x) = \sqrt{2} \cdot \mathrm{e}^{-x}.}$$

Déterminer une fonction g telle que pour tout $x \in \mathbb{R}$,

$$f'(x) = g(x)\cos\left(x + \frac{\pi}{4}\right).$$

(b) La fonction g est strictement positive. Le signe de f est donc celui de $x \mapsto \cos\left(x + \frac{\pi}{4}\right)$, ce qui donne le tableau de variations suivant sur $[0, \frac{2}{\pi}]$:

x	0		$\frac{\pi}{4}$		$\frac{5\pi}{4}$		2π
$f'(x)$		$+$	0	$-$	0	$+$	
$f(x)$	0	↗	$\mathrm{e}^{-\frac{\pi}{4}}$	↘	$-\mathrm{e}^{-\frac{5\pi}{4}}$	↗	0

La droite (T_0) tangente à la courbe en 0 est d'équation $y = f'(0)x + f(0)$, soit :

$$\boxed{T_0 : \ y = x.}$$

La droite $(T_{2\pi})$ tangente à la courbe en 2π est d'équation $y = f'(2\pi)(x - 2\pi) + f(2\pi)$, soit :

$$\boxed{T_\pi : \mathrm{e}^{-2\pi}(x - 2\pi).}$$

2. Soit C la courbe représentative de f dans un repère orthogonal $(O, \vec{i}, \vec{j})$. On note également C_1 et C_2 les courbes représentatives de $x \mapsto \mathrm{e}^{-x}$ et $x \mapsto -\mathrm{e}^{-x}$ respectivement.

(a) Soit $A = (x, y)$. A est un point d'intersection de C et C_1 si et seulement si

$$\mathrm{e}^{-x} = \sin(x)\mathrm{e}^{-x},$$

donc si et seulement si $\sin(x) = 1$, si et seulement si $x \in \{\frac{\pi}{2} + 2k\pi, \quad k \in \mathbb{Z}\}$.
Ainsi, les points d'intersection des deux courbes C et C_1 sont les $\boxed{\text{points d'abscisse } \frac{\pi}{2} + 2k\pi, \text{ pour } k \in \mathbb{Z}.}$

(b) De même, x est l'abscisse d'un point d'intersection de C et C_2 si et seulement si $\sin(x) = -1$. Les points d'intersections de C et C_2 sont donc les $\boxed{\text{points d'abscisse } -\frac{\pi}{2} + 2k\pi, \text{ pour } k \in \mathbb{Z}.}$

(c) Comme par ailleurs, le sinus est toujours compris entre 0 et 1, la courbe C va rester comprise entre les deux courbes C_1 et C_2, en oscillant de l'une à l'autre. On obtient le graphe de la figure 1. Sur ce graphe, on a représenté en traits interrompus les courbes des deux fonctions $x \mapsto \mathrm{e}^{-x}$ et $x \mapsto -\mathrm{e}^{-x}$. La fonction exponentielle croisant vite en $+\infty$ et décroissant vite en $-\infty$, il est assez difficile de représenter la courbe de f sur un intervalle plus grand que $[0, 2\pi]$ (trop fortes variations pour $x < 0$, trop faibles pour $x > 2\pi$)

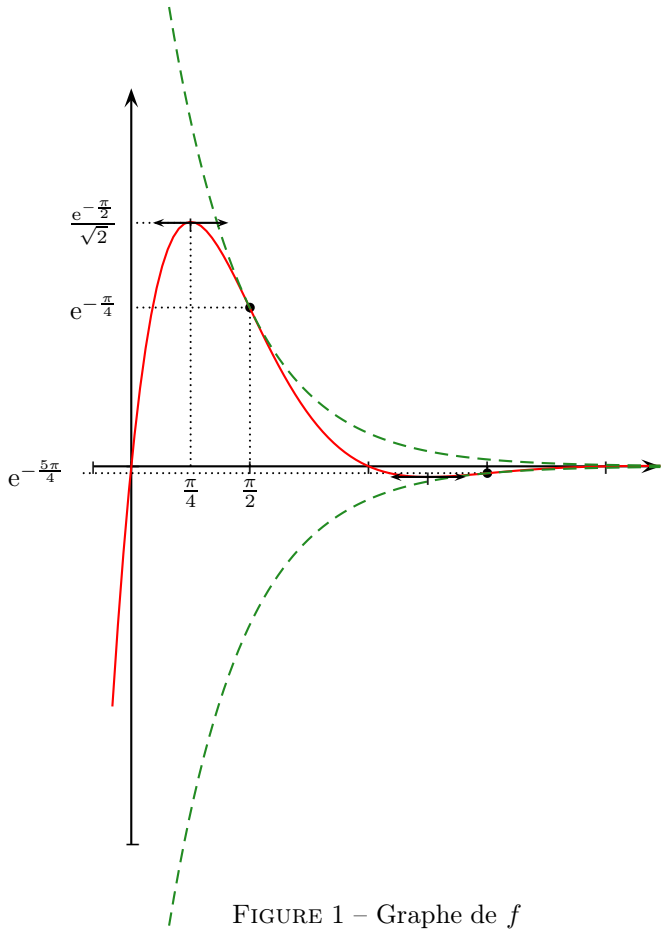

FIGURE 1 – Graphe de f

(d) • Soit $(x, y) \in C$, donc $y = \sin(x)e^{-x}$. On a alors :

$$\Phi(x, y) = (x + 2\pi, e^{-2\pi}\sin(x)e^{-x}) = (x + 2\pi, \sin(x + 2\pi)e^{-(x+2\pi)}).$$

Ainsi, en notant $A(x)$ le point de C d'abscisse x, on a :

$$\Phi(A(x)) = A(x + 2\pi).$$

En particulier $\Phi(A(x)) \in C$, donc $\Phi(C) \subset C$

• Réciproquement, pour tout $A(x) \in C$, $A(x) = \Phi(A(x - 2\pi))$, donc $A(x) \in \Phi(C)$. Ainsi $C \subset \Phi(C)$.

On en déduit que $\boxed{\Phi(C) = C.}$

Dans cet argument, n'oubliez pas de justifier les deux inclusions !

Partie II –

Dans cette partie, on étudie une primitive de f.

1. En redérivant f', on trouve :

$$\forall x \in \mathbb{R}, \quad f''(x) = -2e^{-x}\cos(x) = -2f'(x) - 2f(x).$$

Ainsi, f satisfait l'équation différentielle $\boxed{f'' + 2f' + 2f = 0}$.

2. De la relation précédente, on déduit :

$$(-\frac{1}{2}f' - f)' = f.$$

Ainsi, $\boxed{G = -\frac{1}{2}f' - f}$ est une primitive de f, à savoir :

$$G : \boxed{x \mapsto -\frac{1}{2}(\cos(x) + \sin(x))e^{-x}}.$$

Cela ne fait pas de mal de vérifier le résultat en dérivant l'expression obtenue.

On déduit de la pritive trouvée que pour tout $x \in \mathbb{R}$:

$$\boxed{F(x) = \int_0^x \mathrm{e}^{-t}\sin(t) = G(x) - G(0) = \frac{1}{2}\left(1 - (\cos(x) + \sin(x))\mathrm{e}^{-x}\right)}.$$

Cette expression admet une limite lorsque x tend vers $+\infty$, car $\mathrm{e}^{-x} \to 0$, et on obtient :

$$\boxed{\int_0^{+\infty} \mathrm{e}^{-t}\sin(t)\ \mathrm{d}t = \frac{1}{2}}.$$

3. On pose pour tout $k \in \mathbb{N}$, $B_k = \displaystyle\int_{k\pi}^{(k+1)\pi} f(t)\ \mathrm{d}t$, et pour tout $n \in \mathbb{N}$:

$$S_n = \sum_{k=0}^{n} B_k = B_0 + \cdots + B_n \qquad \text{et} \qquad T_n = \sum_{k=0}^{n} |B_k| = |B_0| + \cdots + |B_n|.$$

(a) D'après la relation de Chasles,

$$S_n = \int_0^{(n+1)\pi} \mathrm{e}^{-t}\sin(t)\ \mathrm{d}t.$$

Ainsi, d'après la question précédente, lorsque n tend vers $+\infty$, on obtient :

$$\lim_{n\to+\infty} S_n = \frac{1}{2}.$$

(b) C'est de (B_k) qu'il faut étudier les variations ((S_n) oscille autour de sa limite comme on le verra ci-dessous) Le sinus étant positif sur les intervalles $[k\pi, (k+1)\pi]$ si k est pair, et négatif si k est impair, la propriété de positivité de l'intégrale permet de conclure que $\boxed{\text{le signe de } B_k \text{ est celui de } (-1)^k.}$

Par ailleurs, on étudie les variations de la valeur absolue $(|B_k|)_{k\in\mathbb{N}}$. Pour cela, on se rend compte que pour tout $x \in \mathbb{R}$,

$$|\sin(x+\pi)\mathrm{e}^{-(x+\pi)}| = |\sin(x)\mathrm{e}^{-(x+\pi)}| \leqslant |\sin(x)\mathrm{e}^{-x}|.$$

Ainsi, la courbe de $|f|$ sur l'intervalle $[(k+1)\pi, (k+2)\pi]$ reste sous le translaté de π de la courbe de $|f|$ sur l'intervalle $[k\pi, (k+1)\pi]$, donc, en interprétant l'intégrale comme l'aire sous la courbe, et par propriété de croissance de l'intégrale, on obtient $|B_{k+1}| \leqslant |B_k|$ (cet argument de translation peut se formaliser par un changement de variables $y = x + \pi$ dans l'intégrale définissant $|B_k|$, mais en l'absence de ce procédé, l'interprétation géométrique convient).

On en déduit que $(|B_k|)_{k\in\mathbb{N}}$ est décroissante.

(c) Cela provient de la décroissance de $(|B_k|)$ et de l'alternance du signe de (B_k). En effet, lorsqu'on effectue la somme, en ajoutant un terme positif, on ne remonte pas autant que ce qu'on était descendu auparavant, et de même dans l'autre sens. Ainsi, les deux suites (S_{2n}) et (S_{2n+1}) vont être l'une croissante, l'autre décroissante, et vont donc encadrer la limite. Cette limite sera donc toujours comprise entre deux termes successifs de la somme partielle (S_n).

Formalisons un peu ce raisonnement. Soit $n \in \mathbb{N}$, on a :

- $S_{2n+2} - S_{2n} = B_{2n+2} + B_{2n+1} = |B_{2n+2}| - |B_{2n+1}| \leqslant 0$, et :
- $S_{2n+3} - S_{2n+1} = B_{2n+3} + B_{2n+2} = -|B_{2n+3}| + |B_{2n+2}| \geqslant 0$.

Ainsi, (S_{2n}) est décroissante et converge vers la même limite que (S_n), donc $\frac{1}{2}$. En particulier, par décroissance, on obtient :

$$\forall n \in \mathbb{N}, \quad S_{2n} \geqslant \frac{1}{2}.$$

Pour la même raison, (S_{2n+1}) est croissante et :

$$\forall n \in \mathbb{N}, \quad S_{2n+1} \leqslant \frac{1}{2}.$$

Soit $n \in \mathbb{N}$. D'après ce qui précède, la limite $\frac{1}{2}$ de (S_n) est compris entre S_n et S_{n+1}, donc

$$\left|\frac{1}{2} - S_n\right| \leqslant |S_{n+1} - S_n| = |B_{n+1}|.$$

On a bien obtenu :

$$\boxed{\left|\int_0^{+\infty} \mathrm{e}^{-t}\sin(t)\ \mathrm{d}t - S_n\right| \leqslant |B_{n+1}|.}$$

Remarque : Cette méthode est valable dès lors qu'on cherche à estimer la somme d'une série alternée (ce qui, par définition, signifie que son terme général s'écrit sous la forme $(-1)^n a_n$, où (a_n) est décroissante de limite nulle). Dans ce cas, la différence entre la somme partielle au rang n et la somme totale est majorée par la valeur absolue du terme général a_{n+1}.

Pour que la différence entre S_n et l'intégrale soit inférieure à 10^{-10}, il suffit donc que $|B_{n+1}| \leqslant 10^{-10}$. Or, sin étant de signe constant sur l'intervalle d'intégration, on peut écrire :

$$|B_{n+1}| = \int_{(n+1)\pi}^{(n+2)\pi} |\sin(t)|\mathrm{e}^{-t}\ \mathrm{d}t \leqslant \int_{(n+1)\pi}^{(n+2)\pi} \mathrm{e}^{-t}\ \mathrm{d}t = \mathrm{e}^{-(n+1)\pi}(1-\mathrm{e}^{-\pi}).$$

Il suffit donc que $\mathrm{e}^{-(n+1)\pi}(1-\mathrm{e}^{-\pi}) \leqslant 10^{-10}$, soit

$$(n+1)\pi \geqslant -\ln\left(\frac{10^{-10}}{1-\mathrm{e}^{-\pi}}\right) \text{ soit: } \boxed{n \geqslant \tfrac{1}{\pi}\ln((1-\mathrm{e}^{-\pi})10^{10}) - 1}.$$

À l'aide d'une calculatrice, on obtient $n \geqslant 6.31$. Il suffit donc de prendre $\boxed{n=7}$ (la convergence de l'intégrale est très rapide, à cause de l'exponentielle qui écrase la courbe vers 0).

4. On utilise la majoration trouvée dans la question précédente :

$$\forall n \in \mathbb{N},\quad |B_n| \leqslant \mathrm{e}^{-n\pi}(1-\mathrm{e}^{-\pi})$$

Le théorème de comparaison des séries à termes positifs nous permettrait de conclure directement, du fait de la convergence de $\sum \mathrm{e}^{-n\pi}$ (en tant que série géométrique de raison inférieure à 1). En l'absence de ce résultat, on y va « à la main ».

Comme la somme (T_n) est constituée de termes positifs, (T_n) est croissante. De plus,

$$\forall n \in \mathbb{N},\quad T_n \leqslant \sum_{k=0}^{n} \mathrm{e}^{-k\pi}(1-\mathrm{e}^{-pi}) = 1-\mathrm{e}^{-(n+1)\pi} \leqslant 1,$$

cette somme se calculant comme somme de termes en progression géométrique de raison $\mathrm{e}^{-\pi}$. La suite (T_n) est donc majorée.

Le théorème de convergence monotone nous permet de conclure qu'étant croissante et majorée, $\boxed{\text{la suite } (T_n) \text{ converge}}$.

5. La limite T peut se calculer, en utilisant la primitive F (ou G) de f, qui amène :

$$\forall n \in \mathbb{N},\quad B_n = \frac{1}{2}\cos(n\pi)\mathrm{e}^{-n\pi} - \frac{1}{2}\cos((n+1)\pi)\mathrm{e}^{-(n+1)\pi}.$$

Cette quantité étant positive si n est paire, et négative sinon, il vient, pour tout $n \in \mathbb{N}$:

$$|B_{2n}| + |B_{2n+1}| = \frac{1}{2}\mathrm{e}^{-2n\pi} + \mathrm{e}^{-(2n+1)\pi} + \frac{1}{2}\mathrm{e}^{-2(n+1)\pi}.$$

En effectuant les sommes deux par deux, il vient donc, pour $n \in \mathbb{N}$:

$$T_{2n+1} = \sum_{k=0}^{n}\left(\frac{1}{2}\mathrm{e}^{-2k\pi} + \mathrm{e}^{-(2k+1)\pi} + \frac{1}{2}\mathrm{e}^{-2(k+1)\pi}\right).$$

Chaque terme $\mathrm{e}^{-(2k+1)\pi}$ apparaît une fois exactement, alors que chaque terme $\mathrm{e}^{-2k\pi}$ apparaît deux demi-fois (sauf les extrêmes). On obtient donc :

$$T_{2n+1} = \sum_{k=0}^{2n+1} \mathrm{e}^{-k\pi} - \frac{1}{2}\left(1+\mathrm{e}^{-(2n+2)\pi}\right) = \frac{1-\mathrm{e}^{-(2n+2)\pi}}{1-\mathrm{e}^{-\pi}} - \frac{1}{2}\left(1+\mathrm{e}^{-(2n+2)\pi}\right).$$

En prenant la limite en $+\infty$, il vient alors :

$$T = \frac{1}{1-\mathrm{e}^{-\pi}} - \frac{1}{2} = \frac{1+\mathrm{e}^{-\pi}}{2(1-\mathrm{e}^{-\pi})}.$$

On calcule alors :

$$\frac{1}{S}+\frac{1}{T}=2+\frac{2(1-\mathrm{e}^{-\pi})}{1+\mathrm{e}^{-\pi}}=\frac{4}{1+\mathrm{e}^{-\pi}}.$$

En utilisant l'expression de B_n trouvée plus haut, on se rend compte qu'on a bien obtenu :

$$\boxed{\frac{1}{S}+\frac{1}{T}=\frac{2}{|B_0|}}.$$

Je n'ai pas trouvé d'explication intuitive et logique de cette relation.

Partie III –

1. Soit $z=a+\mathrm{i}\,b$. On a :
$$\boxed{\mathrm{e}^{z}=\mathrm{e}^{a}\cos(b)+\mathrm{i}\,\mathrm{e}^{a}\sin(b)}.$$

2. On a donc, en écrivant $c=a+\mathrm{i}\,b$, pour tout $t\in\mathbb{R}$:
$$f(t)=\mathrm{e}^{at}\cos(bt)+\mathrm{i}\,\mathrm{e}^{at}\sin(bt),$$
et par dérivation de produits, après simplifications :
$$\forall t\in\mathbb{R}, f'(t)=(a+\mathrm{i}\,b)\mathrm{e}^{at}(\cos(bt)+\mathrm{i}\sin(bt)).$$
On a donc obtenu : $\boxed{\forall t\in\mathbb{R},\quad f'(x)=c\mathrm{e}^{ct},}$ ce qui ne nous étonne guère !
Si $c\neq 0$, une primitive de f est donc $t\mapsto\frac{1}{c}\mathrm{e}^{ct}$ (dérivez cette expression !)
Si $c=0$, la fonction f est constante égale à 1, tout le monde sait primitiver cela !

3. Soit $f:t\mapsto\mathrm{e}^{-t}\sin(t)$, et $g:t\mapsto\mathrm{e}^{(-1+i)t}$. On a donc $\forall t\in\mathbb{R},\quad f(t)=\mathrm{Im}(g(t))$. Par ailleurs, une primitive de g est $t\mapsto\frac{1}{-1+\mathrm{i}}\mathrm{e}^{(-1+\mathrm{i})t}$. Ainsi, une primitive de f est :
$$\begin{aligned}\forall t\in\mathbb{R},\quad G(t)&=\mathrm{Im}\left(\frac{1}{-1+\mathrm{i}}\mathrm{e}^{(-1+\mathrm{i})t}\right)\\&=\mathrm{Im}\left(\frac{-1-\mathrm{i}}{2}(\cos(t)+\mathrm{i}\sin(t))\mathrm{e}^{-t}\right)\\&=\boxed{-\frac{1}{2}\left(\sin(t)+\cos(t)\right)\mathrm{e}^{-t}}.\end{aligned}$$
On retrouve bien l'expression précédente. De même, en considérant la partie réelle, on obtient une primitive de $t\mapsto\mathrm{e}^{-t}\cos(t)$:
$$\boxed{t\mapsto\frac{1}{2}(\sin(t)-\cos(t))\mathrm{e}^{-t}}.$$

4. En s'inspirant de ce qui précède, on peut écrire :
$$\mathrm{e}^{\cos(t)}\cos(t+\sin(t))=\mathrm{Re}\left(\mathrm{e}^{\cos(t)+\mathrm{i}(t+\sin(t))}\right)=\mathrm{Re}(\mathrm{e}^{\mathrm{i}\,t+\mathrm{e}^{\mathrm{i}\,t}})=\mathrm{Re}(\mathrm{e}^{\mathrm{i}\,t}\mathrm{e}^{\mathrm{e}^{\mathrm{i}\,t}}).$$
Or, une primitive de $t\mapsto\mathrm{e}^{\mathrm{i}\,t}\mathrm{e}^{\mathrm{e}^{\mathrm{i}\,t}}$ est $t\mapsto\frac{1}{\mathrm{i}}\mathrm{e}^{\mathrm{e}^{\mathrm{i}\,t}}$, donc une primitive de $t\mapsto\mathrm{e}^{\cos(t)}\cos(t+\sin(t))$ est
$$t\mapsto\mathrm{Re}\left(\frac{1}{\mathrm{i}}\mathrm{e}^{\mathrm{e}^{\mathrm{i}\,t}}\right)=\mathrm{e}^{\cos(x)}\sin(\sin(t)).$$
On peut vérifier ce résultat par dérivation et utilisation des formules de trigonométrie. On obtient alors :
$$\boxed{\int_0^{\pi}\mathrm{e}^{\cos(t)}\cos(t+\sin(t))\,\mathrm{d}t=\left[\mathrm{e}^{\cos(t)}\sin(\sin(t))\right]_0^{\pi}=0.}$$
En considérant la partie imaginaire au lieu de la partie réelle, on trouve :
$$\boxed{\int_0^{\pi}\mathrm{e}^{\cos(t)}\sin(t+\sin(t))\,\mathrm{d}t=\left[-\mathrm{e}^{\cos(t)}\cos(\sin(t))\right]_0^{\pi}=\mathrm{e}-\frac{1}{\mathrm{e}}}.$$

Correction du problème 3 – Logarithme discret, méthode d'Adleman (d'après CG)

Partie I – Définition du logarithme discret

1. • 1 et 6 ne sont pas des racines primitives, puisque leurs puissances successives sont toujours 1, et $(-1)^n$ respectivement (modulo 7).
   • Le calcul des puissances de 2 modulo 7 donne :

   $$2^1 \equiv 2\ [7],\quad 2^2 \equiv 4\ [7],\quad 2^3 \equiv 1\ [7],\quad 2^4 \equiv 2\ [7],$$

   donc 2 n'est pas racine primitive. Le calcul des puissances de 3 modulo 7 donne :

   $$3^1 \equiv 3\ [7],\quad 3^2 \equiv 2\ [7],\quad 3^3 \equiv 6\ [7],\quad 3^4 \equiv 4\ [7],\quad 3^4 \equiv 5\ [7],\quad 3^5 \equiv 1\ [7]$$

   donc 3 est racine primitive. Comme $4 \equiv -3\ [7]$, on obtient la même suite que pour 3, en prenant l'opposé modulo 7 des puissances impaires. En particulier $4^4 \equiv 4\ [7]$, et donc 4 n'est pas racine primitive.
   Les puissances de 5 se ramènent aux puissances de 2, avec un signe qui alterne. 5 est une racine primitive.
   Ainsi, $\boxed{\text{3 et 5 sont les seules racines primitives modulo 7}}$.
2. (a) Si les ($g^k \mod p$) ne sont pas tous distincts pour $k \in [\![0, p-2]\!]$, il existe $i < j$ dans $[\![0, p-2]\!]$ tels que $g^i \mod p = g^j \mod p$. Notons A l'ensemble des restes modulo p des puissances $g^0, \dots, g^{j-1}$.
   Montrons alors, pour tout $n \in \mathbb{N}^*$, $g^n \mod p \in A$.
   Cette propriété est trivialement vraie pour $n \in [\![1, j-1]\!]$, ainsi que pour $n = j$ (car $g^j \mod p = g^i \mod p$).
   Soit $n \geqslant j$, et supposons la propriété vraie jusqu'au rang $n-1$. Alors, en écrivant

   $$g^n \equiv g^j g^{n-j} \equiv g^i g^{n-j} \equiv g^{n-(j-i)}\ [p],$$

   on peut utiliser l'hypothèse de récurrence au rang $n-(j-i) < n$, pour conclure que $g^n \mod p \in A$.
   Ainsi, A étant de cardinal strictement inférieur à $[\![1, p-1]\!]$, cela contredit le fait que g soit une racine primitive.
   Par conséquent, les ($g^k \mod p$), pour $k \in [\![0, p-2]\!]$, sont dexu à deux distincts et dans $[\![1, p-1]\!]$ (en effet, le reste ne peut pas être nul, car cela signifierait que p divise g^k, et p étant premier, cela impliquerait que p divise g, ce qui est incompatible avec la définition d'une racine primitive). Pour des raisons de cardinalité, on a alors :

   $$\boxed{\{g^k \mod p \mid k \in [\![0, p-2]\!]\} = [\![1, p-1]\!]}.$$

   On peut aussi se servir de la question c (en y répondant d'abord), qui implique une périodicité des puissances, de période $p-1$. Au bout d'une période, on a alors l'ensemble de toutes les valeurs possibles.

   (b) L'existence de A provient de l'égalité de la première question. L'unicité a été prouvée lors de cette question aussi (c'est le fait que les $g^k modp$ soient deux à deux distincts pour $k \in [\![0, p-2]\!]$).
   Ainsi, $\boxed{\text{il existe un unique } a \in [\![1, p-2]\!] \text{ tel que } A = (g^a \mod p)}$.

   (c) Écrivons $b = a + k(p-1)$. D'après le petit théorème de Fermat, $g^{p-1} \equiv 1[p]$, donc $g^b \equiv g^a\ [p]$. On en déduit que $\boxed{g^b \mod p = g^a \mod p}$.
   Si on ne connait pas le petit théorème de Fermat, on peut aussi utiliser le théorème de Bachet-Bézout : g et p étant premiers entre eux, il existe u et v tels que

   $$gu + pv = 1$$

   On en déduit que $gv \equiv 1\ [p]$ (donc g est inversible modulo p). Ainsi, en multipliant par v, on constate que $gx \equiv gy\ [p]$ équivaut à $x \equiv y\ [p]$.
   D'après les début du problème, on peut dire que $g^{p-1} \mod p$ est une valeur qu'on a déjà rencontrée avant, disons $g^{p-1} \equiv g^i\ [p]$, pour $i \in [\![0, p-2]\!]$. Si $i \neq 0$, on peut simplifier i fois par g, et on obtient :

   $$g^{p-i-1} \equiv g^0\ [p]$$

   L'argument donné dans la première question permet alors d'affirmer que les $g^n \mod p$ prennent leurs valeurs dans $\{g^k \mod p \mid k \in [\![0, p-i-2]\!]\}$, ce qui contredit le fait que g soit une racine primitive. On a donc $g^{p-1} \mod p = 1$. On conclut alors comme plus haut.

3. On calcule les puissances successives de g modulo p jusqu'à obtenir A. Écrit en Python, cela donne :

```
def logdiscret(A,p,g):
    x = 1
    a = 0
    while x != A:
        X *= g      # calcul de la puissance suivante
        X %= p      # réduction modulo p
        a += 1      # incrémentation de l'exposant
    return a
```

Partie II – Calcul du logarithme discret par la méthode d'Adleman

1. On a $54 = 2 \times 3^3$, donc
$$g^{\ell(2)+3\ell(3)} = g^2(g^3)^3 \equiv 2 \times 3^3 \equiv 54 \ [113].$$
Comme $\ell(2) + 3\ell(3) = 75 \in [\![0, p-2]\!]$, on en déduit que
$$\boxed{\ell(54) = 75}.$$

2. On a :
$$g^{a_i} \equiv p_1^{e_{i,1}} \dots p_n^{e_{i,n}} = g^{e_{i,1}\ell(p_1)} \dots g^{e_{i,n}\ell(p_n)} \ [p-1].$$
D'après la partie I, $g^i \equiv g^j \ [p]$ si et seulement si $i \equiv j \ [p-1]$ (en effet, les puissances de g forment une suite périodique de période $p-1$, les termes d'une période étant 2 à 2 distincts). Ainsi,
$$\boxed{a_i \equiv e_{i,1}\ell(p_1) + \dots + e_{i,n}\ell(p_n) \ [p-1].}$$

3. On prend dans cette question $p = 53$, $g = 20$ (racine primitive admise), $n = 2$, $p_1 = 2$, $p_2 = 5$.
   (a) On a $g^2 = 400 \equiv 29 \ [53]$ et $g^3 \equiv 580 \equiv 50 \ [53]$
   On a donc
   $$1 \equiv \ell(20) \equiv \ell(2^2 \times 5) \equiv 2\ell(2) + \ell(5) \ [p-1]$$
   et :
   $$3 \equiv \ell(50) \equiv \ell(2 \times 5^2) \equiv \ell(2) + 2\ell(5) \ [p-1].$$
   La résolution du système obtenu amène :
   $$3\ell(5) \equiv 5 \ [52] \qquad \text{et} \qquad 3\ell(2) \equiv -1 \ [52].$$
   Comme $\ell(2)$ et $\ell(5)$ sont dans $[\![0, p-2]\!]$, les seules valeurs possibles de $3\ell(5)$ sont 57 et 109. Seule la première est divisible par 3, donc $\boxed{\ell(5) = 19}$
   De même, les seules valeurs possibles de $\ell(2)$ sont 51 et 103. Seul 51 est divisible par 3, donc $\boxed{\ell(2) = 17}$
   (b) On obtient alors :
   $$\ell(40) = \ell(2^3 \times 5) \equiv 3\ell(2) + \ell(5) \equiv 70 \ [52].$$
   Comme $\ell(40)$ doit être dans $[\![0, 51]\!]$, on en déduit que $\boxed{\ell(40) = 18}$
   On aurait pu l'obtenir de façon plus directe, puisque $40 = 2 \times 20 = 2g$: cela implique que $\ell(40) = \ell(2) + 1$.
   (c) Ici, un comptage manuel est ce qu'il y a de plus rapide. Avec $\beta = 0$, on a les entiers 2^α, avec $\alpha \in [\![0, 5]\!]$, donc 6 possibilités. Avec $\beta = 1$, on a les entiers $5 \times 2^\alpha$, avec $2^\alpha < 11$, donc $\alpha \in [\![0, 3]\!]$. Avec $\beta = 2$, il reste les possibilités $\alpha \in [\![0, 1]\!]$. Les autres valeurs de β fournissent des entiers trop grands.
   Ainsi, il y a $\boxed{\text{12 entiers}}$ de $[\![1, 52]\!]$ s'écrivant sous la forme $2^\alpha 5^\beta$.

4. Soit $A \in [\![1, p-1]\!]$.
   (a) • Par définition du reste, et du fait que ni g^s ni A ne sont divisibles par l'entier premier p, $\{(g^s A \mod p) \mid s \in [\![0, p-2]\!]\} \subset [\![1, p-1]\!]$.

- Réciproquement, on peut trouver, comme plus haut, un entier u tel que $Au \equiv 1\ [p]$ (par Bézout, A étant premier avec p). Soit alors $b \in [\![1, p-1]\!]$, et $c = ub \mod p$. Par définition des racines primitives, il existe $s \in [\![0, p-2]\!]$ tel que $g^s = c$, d'où :
$$g^s A \equiv Ac \equiv Aub \equiv b\ [p].$$
Ainsi, $b \in \{(g^s A \mod p) \mid s \in [\![0, p-2]\!]\}$

Des deux inclusions, on déduit : $\boxed{\{(g^s A \mod p) \mid s \in [\![0, p-2]\!]\} = [\![1, p-1]\!]}$.

(b) Soit
$$g^s A \mod p = p_1^{e_1} \cdots p_n^{e_n}.$$
On a alors
$$s + \ell(A) \equiv e_1\ell(p_1) + \cdots + e_n\ell(p_n)\ [p-1],$$
et par conséquent
$$\boxed{\ell(A) = (e_1\ell(p_1) + \cdots + e_n\ell(p_n) - s) \mod (p-1)}.$$

(c) On a $g \times 30 = 600 \equiv 17\ [53]$ puis $g^2 \times 30 \equiv 340 \equiv 22\ [53]$, et enfin $g^3 \times 30 \equiv 300 \equiv 16\ [53]$. Ainsi,
$$\ell(30) \equiv 4\ell(2) - 3 = 65\ [52].$$
Ainsi, $\boxed{\ell(30) = 13}$.

5. On revient au cas général.

(a) On compte les entiers p_1^α, tels que $1 \leqslant p_1^\alpha < p$, donc
$$0 \leqslant \alpha < \frac{\ln(p)}{\ln(p_1)}.$$
Ce dernier nombre n'étant pas entier (car p_1 ne divise pas Il y a donc $\boxed{\left\lceil \frac{\ln(p)}{\ln(p_1)} \right\rceil \text{ entiers}}$ de $[\![1, p-1]\!]$ s'écrivant p_1^α. On peut exprimer cette quantité légèrement différemment, en résolvant $p_1^\alpha \leqslant p-1$ plutôt que $p_1^\alpha < p$. La borne supérieure obtenue peut cette fois être un entier, on ne peut pas utiliser la partie entière par excès. En revanche, cela s'exprime bien avec la partie entière, et on trouve un nombre d'entiers égal à $\boxed{\left\lfloor \frac{\ln(p-1)}{\ln(p_1)} \right\rfloor + 1}$.

(b) Lorsque s parcourt $[\![0, p-2]\!]$, les $g^s A \mod p$ parcourent une et une seule fois chaque entier de $[\![1, p-1]\!]$. Ainsi, si on suppose que l'entier s est choisi uniformément dans $[\![0, p-2]\!]$, $g^s A \mod p$ se répartit aussi uniformément dans $[\![1, p-1]\!]$ (c'est-à-dire avec équiprobabilité). Ainsi, la probabilité que $g^s A \mod p$ soit une puissance de p_1 s'obtient en formant le quotient du nombre de cas favorables par le nombre total de cas, donc :
$$\boxed{P = \frac{1}{p-1}\left\lceil \frac{\ln(p)}{\ln(p_1)} \right\rceil = \frac{1}{p-1}\left(\left\lfloor \frac{\ln(p-1)}{\ln(p_1)} \right\rfloor + 1 \right)}$$

(c) On compte le nombre N d'entiers q de $[\![1, p_1]\!]$ s'écrivant sous la forme $p_1^\alpha p_2^\beta$. On commence comme dans la question (a), pour le facteur α, puis on compte les exposants β correspondants en divisant par p_1^α :
$$N = \sum_{\alpha=0}^{\left\lfloor \frac{\ln(p-1)}{\ln(p_1)} \right\rfloor} \left\lfloor \frac{\ln\left(\frac{p-1}{p_1^\alpha}\right)}{\ln(p_2)} \right\rfloor + 1 = \sum_{\alpha=0}^{\left\lfloor \frac{\ln(p-1)}{\ln(p_1)} \right\rfloor} \left\lfloor \frac{\ln(p-1)}{\ln(p_2)} - \alpha\frac{\ln(p_1)}{\ln(p_2)} \right\rfloor + 1$$
La majoration est facile à obtenir : il suffit de majorer $\left\lfloor \frac{\ln(p-1)}{\ln(p_2)} - \alpha\frac{\ln(p_1)}{\ln(p_2)} \right\rfloor + 1$ par $\frac{\ln(p-1)}{\ln(p_2)} + 1$, ce qui donne alors :
$$N \leqslant \sum_{\alpha=0}^{\left\lfloor \frac{\ln(p-1)}{\ln(p_1)} \right\rfloor} \frac{\ln(p-1)}{\ln(p_2)} + 1 = \left(\left\lfloor \frac{\ln(p-1)}{\ln(p_1)} \right\rfloor + 1 \right)\left(\frac{\ln(p-1)}{\ln(p_2)} + 1 \right) \leqslant \left(\frac{\ln(p-1)}{\ln(p_1)} + 1 \right)\left(\frac{\ln(p-1)}{\ln(p_2)} + 1 \right).$$
Pour obtenir la minoration, il faut faire le calcul de façon un peut plus fine. Pour simplifier l'expression, notons $K = \frac{\ln(p-1)}{\ln(p_1)}$ et $L = \frac{\ln(p-1)}{\ln(p_2)}$. On a alors :
$$N \geqslant \sum_{\alpha=0}^{\lfloor K \rfloor} \left\lfloor L - \alpha\frac{\ln(p_1)}{\ln(p_2)} + 1 \right\rfloor \geqslant \sum_{\alpha=0}^{\lfloor K \rfloor} \left(L - \alpha\frac{\ln(p_1)}{\ln(p_2)} \right).$$

Ainsi,

$$N \geqslant (\lfloor K \rfloor + 1)L - \frac{\lfloor K \rfloor(\lfloor K \rfloor + 1)}{2}\frac{\ln(p_1)}{\ln(p_2)} \geqslant (\lfloor K \rfloor + 1)\left(L - \frac{\lfloor K \rfloor}{2}\frac{\ln(p_1)}{\ln(p_2)}\right).$$

Or,

$$L - \frac{\lfloor K \rfloor}{2}\frac{\ln(p_1)}{\ln(p_2)} \geqslant L - \frac{K}{2}\frac{\ln(p_1)}{\ln(p_2)} = L - \frac{L}{2} = \frac{L}{2} \geqslant 0$$

Comme de plus $\lfloor K \rfloor + 1 \geqslant K$, on obtient :

$$N \geqslant \frac{KL}{2}.$$

La probabilité recherchée est obtenue en divisant par $p-1$, le nombre total de choix de l'entier (par équiprobabilité). Les deux inégalités trouvées précédemment amènent :

$$\boxed{\frac{(\ln(p-1))^2}{2(p-1)(\ln(p_1))(\ln(p_2))} \leqslant P \leqslant \frac{1}{p-1}\left(\frac{\ln(p-1)}{\ln(p_1)} + 1\right)\left(\frac{\ln(p-1)}{\ln(p_2)} + 1\right)}.$$

(d) Soient $p_1, \ldots, p_n$ des nombres premiers distincts inférieurs à p.

- L'inégalité $p_1^{\alpha_1} \cdots p_n^{\alpha_n} \leqslant p-1$ implique (de façon grossière) $p_i^{\alpha_i}$, pour tout $i \in [\![1, n]\!]$. Ainsi,

$$\alpha_i \leqslant \frac{\ln(p-1)}{\ln(p_i)}.$$

  Notons $K_i = \dfrac{\ln(p-1)}{\ln(p_i)}$. Le n-uplet $(\alpha_1, \ldots, \alpha_n)$ doit donc être choisi dans $[\![0, \lfloor K_1 \rfloor]\!] \times \cdots \times [\![0, \lfloor K_n \rfloor]\!]$. Il s'agit d'une condition nécessaire, mais largement pas suffisante (la majoration effectuée est très lâche). Le nombre N de choix convenables des α_i est donc majoré par le cardinal de ce produit cartésien, à savoir :

$$N \leqslant \prod_{i=1}^{n}(\lfloor K_i \rfloor + 1) \leqslant \prod_{i=1}^{n}(K_i + 1).$$

- La minoration, comme précédemment, est nettement plus délicate à obtenir. Étant donnée une suite $(p_n)_{n\in\mathbb{N}}$ d'entiers premiers distincts, on prouve par récurrence sur $n \in \mathbb{N}^*$ que pour tout x (entier ou réel positif), le nombre d'entiers $N_n(x)$ dont la décomposition primaire n'utilise que les entiers $p_1, \ldots, p_n$ vérifie

$$N_n(x) \geqslant \frac{\ln(x)^n}{n!\ln(p_1)\ldots\ln(p_n)}.$$

  Les questions précédentes prouvent la propriété aux rangs 1 et 2. Soit $n \geqslant 3$, et supposons l'inégalité vraie pour tout $x > 0$ et tout entier $m < n$. Alors par un raisonnement similaire à celui de la question précédente, en notant comme plus haut pour tout $i \in [\![1, n]\!]$, $K_i = \dfrac{\ln(x)}{\ln(p_i)}$:

$$N_n(x) = \sum_{\alpha_n=0}^{\lfloor K_n \rfloor} N_{n-1}\left(\frac{x}{p_n^{\alpha_i}}\right).$$

  En utilisant l'hypothèse de récurrence, il vient alors :

$$N_n(x) \geqslant \sum_{\alpha_n=0}^{\lfloor K_n \rfloor} \frac{(\ln(x) - \alpha_n \ln(p_n))^n}{n!\ln(p_1)\cdots\ln(p_{n-1})} = \frac{1}{(n-1)!\ln(p_1)\cdots\ln(p_{n-1})}\sum_{\alpha_n=0}^{\lfloor K_n \rfloor}(\ln(x) - \alpha_n \ln(p_n))^{n-1}$$

  Nous utilisons ensuite un argument classique (comparaison somme / intégrale) pour ramener la minoration à un calcul d'intégrale simple. Cette comparaison consiste à comparer la fonction en escalier définie sur chaque intervalle $[k, k+1]$ par la constante $(\ln(x) - k\ln(p_n))^{n-1}$ à la fonction $(\ln(x) - t\ln(p_n))^{n-1}$. En effet, la fonction $t \mapsto (\ln(x) - t\ln(p_n))^{n-1}$ étant décroissante sur $[k, k+1]$ lorsque $k \in [\![0, \lfloor K_n \rfloor - 1]\!]$ (cela n'est plus nécessairement le cas pour l'intervalle suivant) on a, pour une telle valeur de k, et pour tout $t \in [k, k+1]$:

$$(\ln(x) - k\ln(p_n))^{n-1} \geqslant (\ln(x) - t\ln(p_n))^{n-1},$$

  d'où en intégrant par rapport à la variable t sur $[k, k+1]$:

$$(\ln(x) - k\ln(p_n))^{n-1} \leqslant \int_k^{k+1}(\ln(x) - t\ln(p_n))^{n-1}\,\mathrm{d}t,$$

et en sommant pour k de 0 à $\lfloor K_n \rfloor - 1$:

$$\sum_{k=0}^{\lfloor K_n \rfloor - 1} (\ln(x) - k\ln(p_n))^{n-1} \geqslant \sum_{k=0}^{\lfloor K_n \rfloor - 1} \int_k^{k+1} (\ln(x) - t\ln(p_n))^{n-1}\, \mathrm{d}t = \int_0^{\lfloor K_n \rfloor} (\ln(x) - t\ln(p_n))^{n-1}\, \mathrm{d}t,$$

d'après la relation de Chasles. Par ailleurs, on a aussi, pour $k = \lfloor K_n \rfloor$, et pour tout $t \in [\lfloor K_n \rfloor, K_n]$:

$$(\ln(x) - k\ln(p_n))^{n-1} \geqslant (\ln(x) - t\ln(p_n))^{n-1},$$

et donc, par intégration sur cet intervalle,

$$(\ln(x) - k\ln(p_n))^{n-1} \geqslant (K_n - \lfloor K_n \rfloor)(\ln(x) - k\ln(p_n))^{n-1} \geqslant \int_{\lfloor K_n \rfloor}^{K_n} (\ln(x) - t\ln(p_n))^{n-1}\, \mathrm{d}t,$$

la première inégalité découlant du fait que $(K_n - \lfloor K_n \rfloor) \leqslant 1$. Ainsi, en ajoutant ce dernier terme à la somme précédente, et toujours d'après la relation de Chasles,

$$\sum_{k=0}^{\lfloor K_n \rfloor} (\ln(x) - k\ln(p_n))^{n-1} \geqslant \int_0^{K_n} (\ln(x) - t\ln(p_n))^{n-1}\, \mathrm{d}t = \Big[-\frac{1}{n\ln(p_n)} (\ln(x) - t\ln(p_n))^n \Big]_0^{K_n} = \frac{\ln(x)^n}{n\ln(p_n)}.$$

On peut donc enfin conclure que :

$$N_n(x) \geqslant \frac{\ln(x)^n}{n!\ln(p_1)\dots\ln(p_n)},$$

ce qui prouve bien la propriété voulue au rang n.

Ainsi, d'après le principe de récurrence forte, la propriété est vraie pour tout n.

Pour obtenir la probabilité, on divise comme plus haut par $p-1$. Ainsi :

$$\boxed{\frac{\ln(p-1)^n}{n!(p-1)\ln(p_1)\dots\ln(p_n)} \leqslant P \leqslant \frac{1}{p-1} \prod_{i=1}^{n} \left(\frac{\ln(p-1)}{\ln(p_i)} + 1 \right)}.$$