

DM n° 1 : Révisions et logique

Correction du problème 1 – (d'après Bac C 1990)

Question préliminaire

On forme le taux d'accroissement de f en x_0 . Pour tout $h \neq 0$, tel que $ax_0 + b$ soit dans le domaine de f , on a

$$\frac{g(x_0 + h) - g(x_0)}{h} = \frac{f(ax_0 + b + ah) - f(ax_0 + b)}{h} = a \frac{f(ax_0 + b + ah) - f(ax_0 + b)}{ah}.$$

En supposant f dérivable en $ax_0 + b$, lorsque h tend vers 0, ah également, donc la fraction du terme de droite tend vers $f'(ax_0 + b)$. Par conséquent, g est dérivable en x_0 , et

$$\boxed{g'(x_0) = af'(ax_0 + b)}.$$

On procède de même pour la composition par la fonction $x \mapsto x^2$. On note cette fois $g : x \mapsto f(x^2)$. Le taux d'accroissement s'écrit cette fois, pour tout h en lequel il est défini :

$$\frac{g(x_0 + h) - g(x_0)}{h} = \frac{f(x_0^2 + 2x_0h + h^2) - f(x_0^2)}{h} = (2x_0 + h) \frac{f(x_0^2 + 2x_0h + h^2) - f(x_0^2)}{2x_0h + h^2}.$$

Lorsque h tend vers 0, $2x_0h + h^2$ aussi. Donc, en supposant f dérivable en x_0^2 , la fraction de droite tend vers $f'(x_0^2)$. De plus, $2x_0 + h$ tend vers $2x_0$. Ainsi, g est dérivable en x_0 , et

$$\boxed{g'(x_0) = 2x_0f'(x_0^2)}.$$

Partie I – Étude de f

1. (a) Puisque $\ln(t)$ tend vers $-\infty$ en 0,

$$\lim_{t \rightarrow 0^+} f(t) = \lim_{t \rightarrow 0^+} \frac{t-1}{\ln(t)} = 0 = f(0).$$

Ainsi, $\boxed{f \text{ est continue en } 0}$.

Par changement de variable,

$$\lim_{t \rightarrow 1^-} f(t) = \lim_{u \rightarrow 0} \frac{u}{\ln(1+u)} = 1 = f(1)$$

En effet, il s'agit d'une limite remarquable, traduisant ici la dérivabilité en 1 du logarithme.

Ainsi, $\boxed{f \text{ est continue en } 1}$.

- (b) La fonction $\boxed{f \text{ est dérivable sur }]0, 1[}$ en tant que quotient de fonctions dérivables, le dénominateur ne s'annulant pas sur cet intervalle.

- (c) Dans un premier temps, on exprime f' :

$$\forall t \in]0, 1[, \quad f'(t) = \frac{\ln(t) - \frac{t-1}{t}}{\ln(t)^2}.$$

Comme $\ln(t)^2$ est positif pour tout t de $]0, 1[$, f' est du signe de $\ln(t) - \frac{t-1}{t}$. Ce choix de fonction auxiliaire (plutôt que $t \ln(t) - (t-1)$ par exemple) s'impose du fait que sa dérivée s'exprime facilement, sans faire intervenir le logarithme.

Soit donc

$$g : t \mapsto \ln(t) - \frac{t-1}{t} = \ln(t) - 1 + \frac{1}{t}.$$

La fonction g est dérivable sur $]0, 1[$, de dérivée définie par :

$$\forall t \in]0, 1[, \quad g'(t) = \frac{1}{t} - \frac{1}{t^2} = \frac{t-1}{t^2}.$$

Ainsi, g' est négative sur $]0, 1[$, donc g est décroissante sur $]0, 1[$. Comme la limite de g en 1 est nulle, on en déduit que g est positive sur $]0, 1[$.

Ainsi, f' est positive sur $]0, 1[$.

- (d) Pour étudier la dérivabilité en 0, on forme le taux d'accroissement : pour tout $h \in]0, 1[$,

$$\frac{f(h) - f(0)}{h} = \frac{h-1}{h \ln(h)}.$$

Puisque $h \ln(h) \rightarrow 0^-$ lorsque $h \rightarrow 0$, et $h-1 \rightarrow -1$, on en déduit que ce taux d'accroissement tend vers $+\infty$.

Ainsi, f n'est pas dérivable en 0, mais admet une tangente verticale.

2. (a) Le plus naturel est d'étudier les deux inégalités par étude de fonctions.

- On pose h_1 la fonction qui à x associe $-\ln(1-x) - \left(x + \frac{x^2}{2}\right)$. La fonction h_1 est dérivable sur $[0, \frac{1}{2}]$, et pour tout x de $[0, \frac{1}{2}]$,

$$h'_1(x) = \frac{1}{1-x} - 1 - x = \frac{x^2}{1-x} \geq 0.$$

Remarquez que cette dérivation composée est une conséquence de la question préliminaire. Ainsi, h_1 est croissante, et comme $h_1(0) = 0$, pour tout $x \in [0, \frac{1}{2}]$,

$$h_1(x) = -\ln(1-x) - \left(x + \frac{x^2}{2}\right) \geq 0.$$

- On pose h_2 la fonction qui à x associe $-\ln(1-x) - \left(x + \frac{x^2}{2} + \frac{2x^3}{3}\right)$. Cette fonction est dérivable sur $[0, \frac{1}{2}]$, et pour tout x de $[0, \frac{1}{2}]$,

$$h'_2(x) = \frac{1}{1-x} - 1 - x - 2x^2 = -\frac{x^2 - 2x^3}{1-x} = -\frac{x^2(1-2x)}{1-x}.$$

Ainsi, h'_2 est négative sur $[0, \frac{1}{2}]$, donc h_2 est décroissante sur cet intervalle. Puisque $h_2(0) = 0$, on a bien alors, pour tout $x \in [0, \frac{1}{2}]$,

$$h_2(x) = -\ln(1-x) - \left(x + \frac{x^2}{2}\right) \leq 0.$$

Les deux inégalités obtenues amènent bien l'encadrement :

$$\forall u \in [0, \frac{1}{2}], \quad 0 \leq -\ln(1-u) - \left(u + \frac{u^2}{2}\right) \leq \frac{2u^3}{3}$$

- (b) On forme le taux d'accroissement de g en 1. Pour tout h dans $] -\frac{1}{2}, 0[$,

$$\frac{g(1+h) - g(1)}{h} = \frac{\ln(1+h) - h}{h^2}.$$

On fait le changement de variable $u = -h$. On a donc $u \in [0, \frac{1}{2}]$, et $u \rightarrow 0$ lorsque $h \rightarrow 0$. On étudie donc la limite lorsque u tend vers 0 de $\frac{\ln(1-u) + u}{u^2}$.

Or, d'après la question précédente, pour tout $u \in [0, \frac{1}{2}]$,

$$-\frac{1}{2} - \frac{2u}{3} \leq \frac{\ln(1-u) + u}{u^2} \leq -\frac{1}{2}.$$

Les deux termes encadrants tendent vers $-\frac{1}{2}$ lorsque u tend vers 0, donc d'après le théorème d'encadrement, le terme du milieu admet la même limite. Ainsi g est dérivable en 1, et $g'(1) = -\frac{1}{2}$.

(c) Comme g ne s'annule pas en 1, la dérivabilité de g en 1 entraîne celle de $f = \frac{1}{g}$, et

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

La courbe de f admet donc en 1 une tangente (ou plutôt une demi-tangente à gauche), d'équation

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

(d) « Au voisinage » signifie ici qu'on n'est pas intéressé par les positions relatives sur tout l'intervalle $[0, 1]$, mais seulement sur un intervalle $[a, 1]$, avec a qu'on pourra choisir aussi grand qu'on veut, vérifiant $a < 1$. Cela dit, ici, l'étude peut se faire tout aussi facilement sur tout l'intervalle $[0, 1]$.

Pour faire cette étude, on considère la fonction h définie par

$$h(x) = f(x) - \frac{x}{2} - \frac{1}{2} = \frac{x-1}{\ln(x)} - \frac{x}{2} - \frac{1}{2}.$$

Il faut étudier le signe de h sur $]0, 1[$, qui est l'opposé du signe de

$$k(x) = x - 1 - \frac{x}{2} \ln(x) - \frac{1}{2} \ln(x),$$

expression qui se dérive plus facilement. La fonction k étant dérivable, on obtient, pour $x \in]0, 1[$,

$$k'(x) = 1 - \frac{x}{2} \cdot \frac{1}{x} - \frac{1}{2} \ln(x) - \frac{1}{2x} = \frac{1}{2} - \frac{1}{2x} - \frac{1}{2} \ln(x).$$

On peut redériver une nouvelle fois :

$$\forall x \in]0, 1[, \quad k''(x) = \frac{1}{2x^2} - \frac{1}{2x} = \frac{1-x}{2x^2} \geq 0.$$

Ainsi, k' est croissante sur $]0, 1]$, et $k(1) = 0$, donc k' est négative sur $]0, 1]$. On en déduit que k est décroissante sur $]0, 1]$, et $k(1) = 0$. Ainsi, k est positive sur $]0, 1]$, donc h est négative sur $]0, 1]$.

Ainsi, la courbe \mathcal{C} est sous la tangente en 1, sur tout l'intervalle $]0, 1[$.

3. On obtient le graphe de la figure 1

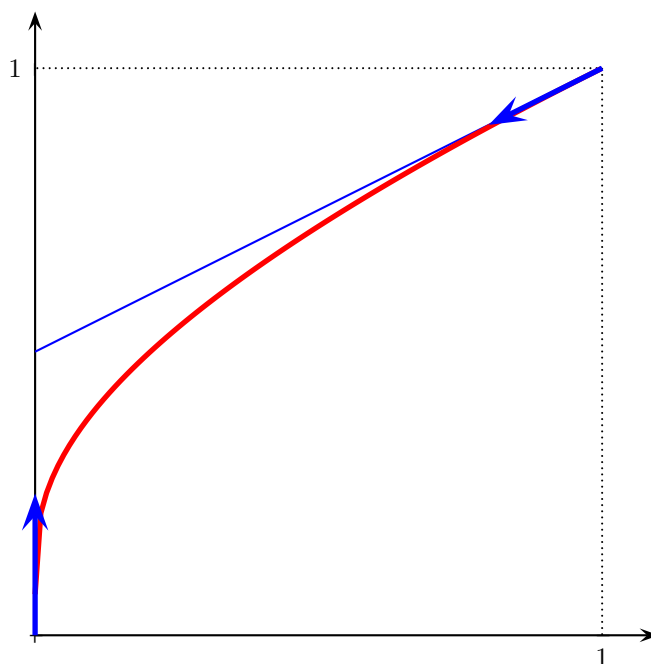


FIGURE 1 – Graphe de f

Partie II – Calcul de l'intégrale I

Pour commencer, remarquons qu'on n'a pas de problème de définition des intégrales, toutes les fonctions considérées étant continues sur leur intervalle fermé borné d'intégration.

1. Soit K la fonction définie sur $]0, 1]$ par :

$$K(x) = J(x^2) - J(x).$$

- (a) La fonction $g : t \mapsto \frac{f(t)}{t}$ est continue sur $]0, 1]$, donc admet une primitive. Soit G une primitive de g . On a alors, pour tout $x \in]0, 1]$,

$$J(x) = G(1) - G(x) \quad \text{et} \quad J(x^2) = G(1) - G(x^2).$$

La fonction G est dérivable sur $]0, 1]$ (une primitive est toujours dérivable, par définition !), donc d'après la question préliminaire, $x \mapsto G(x^2)$ également sur $]0, 1]$ (puisque si x est dans $]0, 1]$, x^2 aussi). De plus, toujours d'après la question préliminaire, la dérivée de $x \mapsto G(x^2)$ est $x \mapsto 2xG'(x^2) = 2xg(x^2)$. On en déduit que K est dérivable sur $]0, 1]$, et

$$\forall x \in]0, 1], \quad K'(x) = -2xg(x^2) + g(x) = \frac{-2f(x^2) + f(x)}{x}.$$

- (b) Pour tout x de $]0, 1]$,

$$f(x) - 2f(x^2) = \frac{x-1}{\ln(x)} - 2\frac{(x^2-1)}{2\ln(x)} = \frac{(x-1) - (x-1)(x+1)}{\ln(x)} = -xf(x).$$

On en déduit que pour tout $x \in]0, 1]$,

$$K'(x) = -f(x).$$

Ainsi, K et I admettent même dérivée, donc diffèrent uniquement d'une constante additive. Or, $I(1) = K(1) = 0$, donc cette constante est nulle. Ainsi, pour tout $x \in]0, 1]$,

$$I(x) = K(x) = \int_{x^2}^1 \frac{f(t)}{t} dt - \int_x^1 \frac{f(t)}{t} dt.$$

La relation de Chasles amène alors :

$$I(x) = \int_{x^2}^x \frac{t-1}{t \ln(t)} dt.$$

2. Cette question nécessite de savoir dériver une composée. Il s'agit donc d'une généralisation de la question préliminaire. Vous êtes nombreux à connaître cette formule de dérivation, même si elle n'est plus au programme du lycée. Pour les autres, admettez-là. Sous réserve de dérivabilité des fonctions considérées aux points d'évaluation, on a

$$(g \circ f)' = f' \times g' \circ f.$$

En particulier, si u est une fonction strictement positive, et dérivable, $\ln \circ u$ aussi, et sa dérivée est $\frac{u'}{u}$. Or, la fonction qu'on cherche à intégrer ici est de cette forme, au signe près, avec $u = \ln$. On obtient donc :

$$\int_{x^2}^x \frac{-1}{t \ln(t)} dt = \left[-\ln(\ln(x)) \right]_{x^2}^x = \ln(\ln(x)) - \ln(\ln(x^2)) = \ln(\ln(x)) - \ln(2 \ln(x)) = \ln \left(\frac{\ln(x)}{2 \ln(x)} \right),$$

d'où finalement,

$$\int_{x^2}^x \frac{-1}{t \ln(t)} dt = \ln(2).$$

3. La fonction \ln est négative sur $[x^2, x]$, donc

$$\left| \int_{x^2}^x \frac{dt}{\ln(t)} \right| = - \int_{x^2}^x \frac{dt}{\ln(t)}.$$

De plus, \ln est croissante sur $]0, 1]$, donc pour tout $t \in [x^2, x]$,

$$\ln(x^2) \leq \ln(t) \leq \ln(x) < 0,$$

donc

$$\frac{1}{\ln(x)} \leq \frac{1}{\ln(t)} < 0,$$

puis

$$0 < -\frac{1}{\ln(t)} \leq -\frac{1}{\ln(x)}.$$

En intégrant cette inégalité sur $[x^2, x]$, il vient donc :

$$0 < -\int_{x^2}^x \frac{-1}{t \ln(t)} dt \leq -\int_{x^2}^x \frac{1}{\ln(x)} dt = -(x - x^2) \frac{1}{\ln(x)}.$$

Puisque $x - x^2 \leq x$, et $-\frac{1}{\ln(x)} \geq 0$ sur $[x^2, x]$, on peut encore majorer ce dernier terme par $-\frac{x}{\ln(x)}$. Ainsi, pour tout $x \in [x^2, x]$,

$$0 < \left| \int_{x^2}^x \frac{-1}{t \ln(t)} dt \right| \leq -\frac{x}{\ln(x)}.$$

4. Ce majorant tendant vers 0 lorsque x tend vers 0, on en déduit, d'après le théorème d'encadrement, que

$$\lim_{x \rightarrow 0} \left| \int_{x^2}^x \frac{-1}{t \ln(t)} dt \right| = 0,$$

donc

$$\lim_{x \rightarrow 0} \int_{x^2}^x \frac{-1}{t \ln(t)} dt = 0$$

La question 1(b) et la question 2 permettent alors d'affirmer que

$$\lim_{x \rightarrow 0} I(x) = \ln(2).$$

5. Soit $x \in]0, 1]$. On a, par la relation de Chasles :

$$|I - I(x)| = \int_0^x f(x) dx.$$

D'après les variations de f , f est majorée par 1 sur $[0, 1]$, donc sur $[0, x]$. On a alors

$$|I - I(x)| \leq \int_0^x 1 dx = x.$$

Ceci est équivalent à l'encadrement $-x \leq I - I(x) \leq x$. Les deux termes encadrant admettent la même limite nulle, donc d'après le théorème d'encadrement (ici la convergence est déjà acquise, donc on peut se contenter de passer à la limite dans les inégalités) :

$$\lim_{x \rightarrow 0^+} I - I(x) = 0 \quad \text{donc:} \quad I = \lim_{x \rightarrow 0^+} I(x) = \ln(2).$$

Montrer que pour tout $x \in]0, 1]$, $|I - I(x)| \leq x$. En déduire que $I = \ln(2)$.

Correction du problème 2 – Logarithme discret, méthode d'Adleman (d'après CG)

Partie I – Définition du logarithme discret

- 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 :

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

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, 3 et 5 sont les seules racines primitives modulo 7.

2. (a) Si les $(g^k \bmod p)$ ne sont pas tous distincts pour $k \in \llbracket 0, p-2 \rrbracket$, il existe $i < j$ dans $\llbracket 0, p-2 \rrbracket$ tels que $g^i \bmod p = g^j \bmod p$. Notons A l'ensemble des restes modulo p des puissances g^0, \dots, g^{j-1} .

Montrons alors, pour tout $n \in \mathbb{N}^*$, $g^n \bmod p \in A$.

Cette propriété est trivialement vraie pour $n \in \llbracket 1, j-1 \rrbracket$, ainsi que pour $n = j$ (car $g^j \bmod p = g^i \bmod p$).

Soit $n \geq j$, 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 $g^n \bmod p \in A$.

Ainsi, A étant de cardinal strictement inférieur à $\llbracket 1, p-1 \rrbracket$, cela contredit le fait que g soit une racine primitive.

Par conséquent, les $(g^k \bmod p)$, pour $k \in \llbracket 0, p-2 \rrbracket$, sont deux à deux distincts et dans $\llbracket 1, p-1 \rrbracket$ (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 :

$$\{g^k \bmod p \mid k \in \llbracket 0, p-2 \rrbracket\} = \llbracket 1, p-1 \rrbracket.$$

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 $g^k \bmod p$ soient deux à deux distincts pour $k \in \llbracket 0, p-2 \rrbracket$).

Ainsi, $\boxed{\text{il existe un unique } a \in \llbracket 1, p-2 \rrbracket \text{ tel que } A = (g^a \bmod p)}$.

- (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 $\boxed{g^b \bmod p = g^a \bmod p}$.

Si on ne connaît 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 le début du problème, on peut dire que $g^{p-1} \bmod p$ est une valeur qu'on a déjà rencontrée avant, disons $g^{p-1} \equiv g^i [p]$, pour $i \in \llbracket 0, p-2 \rrbracket$. 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 $g^n \bmod p$ prennent leurs valeurs dans $\{g^k \bmod p \mid k \in \llbracket 0, p-i-2 \rrbracket\}$, ce qui contredit le fait que g soit une racine primitive. On a donc $g^{p-1} \bmod p = 1$. 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
```

1. On a $54 = 2 \times 3^3$, donc

$$g^{\ell(2)+3\ell(3)} = g^2(g^3)^3 \equiv 2 \times 3^3 \equiv 54 \pmod{113}.$$

Comme $\ell(2) + 3\ell(3) = 75 \in \llbracket 0, p-2 \rrbracket$, on en déduit que

$$\boxed{\ell(54) = 75}.$$

2. On a :

$$g^{a_i} \equiv p_1^{e_{i,1}} \dots p_n^{e_{i,n}} = g^{e_{i,1}\ell(p_1)} \dots g^{e_{i,n}\ell(p_n)} \pmod{p-1}.$$

D'après la partie I, $g^i \equiv g^j \pmod{p}$ si et seulement si $i \equiv j \pmod{p-1}$ (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,

$$\boxed{a_i \equiv e_{i,1}\ell(p_1) + \dots + e_{i,n}\ell(p_n) \pmod{p-1}}.$$

3. On prend dans cette question $p = 53$, $g = 20$ (racine primitive admise), $n = 2$, $p_1 = 2$, $p_2 = 5$.

(a) On a $g^2 = 400 \equiv 29 \pmod{53}$ et $g^3 \equiv 580 \equiv 50 \pmod{53}$

On a donc

$$1 \equiv \ell(20) \equiv \ell(2^2 \times 5) \equiv 2\ell(2) + \ell(5) \pmod{p-1}$$

et :

$$3 \equiv \ell(50) \equiv \ell(2 \times 5^2) \equiv \ell(2) + 2\ell(5) \pmod{p-1}.$$

La résolution du système obtenu amène :

$$3\ell(5) \equiv 5 \pmod{52} \quad \text{et} \quad 3\ell(2) \equiv -1 \pmod{52}.$$

Comme $\ell(2)$ et $\ell(5)$ sont dans $\llbracket 0, p-2 \rrbracket$, 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 :

$$\ell(40) = \ell(2^3 \times 5) \equiv 3\ell(2) + \ell(5) \equiv 70 \pmod{52}.$$

Comme $\ell(40)$ doit être dans $\llbracket 0, 51 \rrbracket$, 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 $\alpha \in \llbracket 0, 5 \rrbracket$, donc 6 possibilités. Avec $\beta = 1$, on a les entiers $5 \times 2^\alpha$, avec $2^\alpha < 11$, donc $\alpha \in \llbracket 0, 3 \rrbracket$. Avec $\beta = 2$, il reste les possibilités $\alpha \in \llbracket 0, 1 \rrbracket$. Les autres valeurs de β fournissent des entiers trop grands.

Ainsi, il y a $\boxed{12 \text{ entiers}}$ de $\llbracket 1, 52 \rrbracket$ s'écrivant sous la forme $2^\alpha 5^\beta$.

4. Soit $A \in \llbracket 1, p-1 \rrbracket$.

- (a) • Par définition du reste, et du fait que ni g^s ni A ne sont divisibles par l'entier premier p , $\{(g^s A \pmod{p}) \mid s \in \llbracket 0, p-2 \rrbracket\} \subset \llbracket 1, p-1 \rrbracket$.
- Réciproquement, on peut trouver, comme plus haut, un entier u tel que $Au \equiv 1 \pmod{p}$ (par Bézout, A étant premier avec p). Soit alors $b \in \llbracket 1, p-1 \rrbracket$, et $c = ub \pmod{p}$. Par définition des racines primitives, il existe $s \in \llbracket 0, p-2 \rrbracket$ tel que $g^s = c$, d'où :

$$g^s A \equiv Ac \equiv Aub \equiv b \pmod{p}.$$

Ainsi, $b \in \{(g^s A \pmod{p}) \mid s \in \llbracket 0, p-2 \rrbracket\}$

Des deux inclusions, on déduit : $\boxed{\{(g^s A \pmod{p}) \mid s \in \llbracket 0, p-2 \rrbracket\} = \llbracket 1, p-1 \rrbracket}$.

(b) Soit

$$g^s A \pmod{p} = p_1^{e_1} \dots p_n^{e_n}.$$

On a alors

$$s + \ell(A) \equiv e_1\ell(p_1) + \dots + e_n\ell(p_n) \pmod{p-1},$$

et par conséquent

$$\boxed{\ell(A) = (e_1\ell(p_1) + \dots + e_n\ell(p_n) - s) \pmod{p-1}}.$$

(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 $1 \leq p_1^\alpha < p$, donc

$$0 \leq \alpha < \frac{\ln(p)}{\ln(p_1)}.$$

Ce dernier nombre n'étant pas entier (car p_1 ne divise pas p) Il y a donc $\left\lfloor \frac{\ln(p)}{\ln(p_1)} \right\rfloor$ entiers de $\llbracket 1, p-1 \rrbracket$ s'écrivant p_1^α . On peut exprimer cette quantité légèrement différemment, en résolvant $p_1^\alpha \leq p-1$ 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 $\left\lfloor \frac{\ln(p-1)}{\ln(p_1)} \right\rfloor + 1$.

(b) Lorsque s parcourt $\llbracket 0, p-2 \rrbracket$, les $g^s A \bmod p$ parcourent une et une seule fois chaque entier de $\llbracket 1, p-1 \rrbracket$. Ainsi, si on suppose que l'entier s est choisi uniformément dans $\llbracket 0, p-2 \rrbracket$, $g^s A \bmod p$ se répartit aussi uniformément dans $\llbracket 1, p-1 \rrbracket$ (c'est-à-dire avec équiprobabilité). Ainsi, la probabilité que $g^s A \bmod p$ soit une puissance de p_1 s'obtient en formant le quotient du nombre de cas favorables par le nombre total de cas, donc :

$$P = \frac{1}{p-1} \left\lfloor \frac{\ln(p)}{\ln(p_1)} \right\rfloor = \frac{1}{p-1} \left(\left\lfloor \frac{\ln(p-1)}{\ln(p_1)} \right\rfloor + 1 \right)$$

(c) On compte le nombre N d'entiers q de $\llbracket 1, p_1 \rrbracket$ 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 :

$$N \leq \sum_{\alpha=0}^{\left\lfloor \frac{\ln(p-1)}{\ln(p_1)} \right\rfloor} \frac{\ln(p-1)}{\ln(p_2)} + 1 = \left(\left\lfloor \frac{\ln(p-1)}{\ln(p_1)} \right\rfloor + 1 \right) \left(\frac{\ln(p-1)}{\ln(p_2)} + 1 \right) \leq \left(\frac{\ln(p-1)}{\ln(p_1)} + 1 \right) \left(\frac{\ln(p-1)}{\ln(p_2)} + 1 \right).$$

Pour obtenir la minoration, il faut faire le calcul de façon un peu 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 :

$$N \geq \sum_{\alpha=0}^{\lfloor K \rfloor} \left\lfloor L - \alpha \frac{\ln(p_1)}{\ln(p_2)} + 1 \right\rfloor \geq \sum_{\alpha=0}^{\lfloor K \rfloor} \left(L - \alpha \frac{\ln(p_1)}{\ln(p_2)} \right).$$

Ainsi,

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

Or,

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

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

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

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 :

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

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

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

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

Notons $K_i = \frac{\ln(p-1)}{\ln(p_i)}$. Le n -uplet $(\alpha_1, \dots, \alpha_n)$ doit donc être choisi dans $\llbracket 0, [K_1] \rrbracket \times \cdots \times \llbracket 0, [K_n] \rrbracket$. 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 :

$$N \leq \prod_{i=1}^n ([K_i] + 1) \leq \prod_{i=1}^n (K_i + 1).$$

- 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, \dots, p_n vérifie

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

Les questions précédentes prouvent la propriété aux rangs 1 et 2. Soit $n \geq 3$, 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 $i \in \llbracket 1, n \rrbracket$, $K_i = \frac{\ln(x)}{\ln(p_i)}$:

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

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

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

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 $k \in \llbracket 0, [K_n] - 1 \rrbracket$ (cela n'est plus nécessairement le cas pour l'intervalle suivant) on a, pour une telle valeur de k , et pour tout $t \in [k, k+1]$:

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

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

$$(\ln(x) - k \ln(p_n))^{n-1} \leq \int_k^{k+1} (\ln(x) - t \ln(p_n))^{n-1} dt,$$

et en sommant pour k de 0 à $[K_n] - 1$:

$$\sum_{k=0}^{[K_n]-1} (\ln(x) - k \ln(p_n))^{n-1} \geq \sum_{k=0}^{[K_n]-1} \int_k^{k+1} (\ln(x) - t \ln(p_n))^{n-1} dt = \int_0^{[K_n]} (\ln(x) - t \ln(p_n))^{n-1} dt,$$

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

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

et donc, par intégration sur cet intervalle,

$$(\ln(x) - k \ln(p_n))^{n-1} \geq (K_n - [K_n])(\ln(x) - k \ln(p_n))^{n-1} \geq \int_{[K_n]}^{K_n} (\ln(x) - t \ln(p_n))^{n-1} dt,$$

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

$$\sum_{k=0}^{\lfloor K_n \rfloor} (\ln(x) - k \ln(p_n))^{n-1} \geq \int_0^{K_n} (\ln(x) - t \ln(p_n))^{n-1} dt = \left[-\frac{1}{n \ln(p_n)} (\ln(x) - t \ln(p_n))^n \right]_0^{K_n} = \frac{\ln(x)^n}{n \ln(p_n)}.$$

On peut donc enfin conclure que :

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

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 :

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