Exercice 1

I-1. s et s' sont des similitudes indirectes, donc leur composée $r = s' \circ s$ est une similitude directe. C'est de plus une isométrie comme composée d'isométries.

Par ailleurs, I est un point fixe de r, donc r est une rotation de centre I. Soit θ son angle.

Pour un point M de D, différent de I, D' est bissectrice de l'angle $\left(\overrightarrow{IM}, \overrightarrow{Ir(M)}\right)$ donc θ est le double de l'angle $(\overrightarrow{u_D}, \overrightarrow{u_{D'}})$ de vecteurs directeurs $\overrightarrow{u_D}$ et $\overrightarrow{u_{D'}}$ des droites D et D'.

I-2. (a) D'après la question précédente : $s_2 \circ s_1 = r^2$ et $s_3 \circ s_1 = r$.

Toute symétrie axiale est sa propre réciproque. Ainsi :

$$\begin{cases} M_2 = s_2(M) = s_2 \circ s_1(M_1) = r^2(M_1) \\ M_3 = s_3(M) = s_3 \circ s_1(M_1) = r(M_1) \end{cases}$$

(b) $M_1M_2M_3$ est donc un triangle équilatéral indirect de centre O.

II-1. M_1 est le symétrique de M par rapport à l'axe des abscisses, donc d'affixe $\overline{z} = \rho e^{-\mathrm{i}\theta}$.

$M_2 = r^2(M_1)$ donc M_2 est d'affixe $e^{4\mathrm{i}\pi/3}\overline{z} = j^2\overline{z}$.

$M_3 = r(M_1)$ donc M_3 est d'affixe $e^{2\mathrm{i}\pi/3}\overline{z} = j\overline{z}$.

II-2. Notons s la symétrie axiale d'axe (BC). J est l'intersection de (OA) et (BC), et ces deux droites sont orthogonales donc $\quad s \circ s_1 = s_J$

où s_J la symétrie de centre J (qui est aussi la rotation de centre J d'angle de mesure π).

Ainsi $s = s_J \circ s_1$ donc $M_4 = s_J(s_1(M)) = s_J(M_1)$: J est le milieu du segment $[M_1, M_4]$.

M_4 a pour d'affixe $-1 - \overline{z} = -1 - \rho e^{-\mathrm{i}\theta}$.

II-3. (a) On prend $z \neq 0$ i.e. $M \neq O$.

M_2, M_3 et M_4 sont alignés si et seulement si $S = \dfrac{(-1-\overline{z}) - j\overline{z}}{j^2\overline{z} - j\overline{z}}$ est réel.

Or : $S = \dfrac{-1 + j^2\overline{z}}{-\mathrm{i}\sqrt{3}\overline{z}}$ donc M_2, M_3 et M_4 sont alignés si et seulement si :

$$\frac{-1 + j^2\overline{z}}{-\mathrm{i}\overline{z}} = \frac{-1 + jz}{\mathrm{i}z}.$$

Ceci est équivalent à : $z + \overline{z} = (j^2 + j)\,|z|^2$ et en posant $z = x + \mathrm{i}y$, $(x, y) \in \mathbb{R}^2$, on obtient la condition équivalente : $\quad 2x = -x^2 - y^2$ soit $(x+1)^2 + y^2 = 1$.

L'ensemble des points M tels que M_2, M_3 et M_4 soient alignés est donc le cercle de centre ω d'affixe -1 et de rayon 1 (O y compris, car dans ce cas particulier, M_2 et M_3 sont confondus).

(b) Ω doit être sur la médiatrice de $[M_2, M_3]$. Le triangle $M_1M_2M_3$ est équilatéral de centre O donc celle-ci est la droite (OM_1).

(c) λ est déterminé par le fait que $\Omega M_3 = \Omega M_4$, i.e. $\left|\rho j e^{-\mathrm{i}\theta} - \lambda e^{-\mathrm{i}\theta}\right| = \left|-1 - \rho e^{-\mathrm{i}\theta} - \lambda e^{-\mathrm{i}\theta}\right|$.

Ceci est équivalent à : $\lambda^2 + \rho^2 + \lambda\rho = (\lambda + \rho)^2 + 1 + 2(\lambda + \rho)\cos\theta$

soit à $\lambda\rho + 1 + 2(\lambda + \rho)\cos\theta = 0$ ou à $\lambda = \dfrac{-1 - 2\rho\cos\theta}{\rho + 2\cos\theta}$.

(L'ensemble des points tels que $\rho = -2\cos\theta$ est le cercle de centre -1 de rayon 1).

(d) Ainsi $R = \Omega M_2 = \sqrt{\lambda^2 + \rho^2 + \lambda\rho}$ avec λ ci-dessus.

(e) $R^2 = 1$ si et seulement si $\lambda^2 + \rho^2 + \lambda\rho = 1$ ce qui est équivalent à

$(1 + 2\rho\cos\theta)^2 + \rho^2(\rho + 2\cos\theta)^2 - \rho(1 + 2\rho\cos\theta)(\rho + 2\cos\theta) = (\rho + 2\cos\theta)^2$

soit à $1 + 4\rho^2\cos^2\theta + 2\rho\cos\theta + \rho^4 + 2\rho^3\cos\theta - \rho^2 = \rho^2 + 4\cos^2\theta + 4\rho\cos\theta$

ou à $\rho^4 - 2\rho^2 + 1 + 2\rho\left(\rho^2 - 1\right)\cos\theta + 4\left(\rho^2 - 1\right)\cos^2\theta = 0$,

équivalent à : $\left(\rho^2 - 1\right)\left(\rho^2 + 2\rho\cos\theta + 4\cos^2\theta - 1\right) = 0$.

Comme ρ est positif, ceci est équivalent $\rho = 1$ ou $(\rho + \cos\theta)^2 + 3\cos^2\theta - 1 = 0$

ce qui donne la relation demandée.

II-4. La condition demandée s'écrit $R = \rho$, équivalent à :

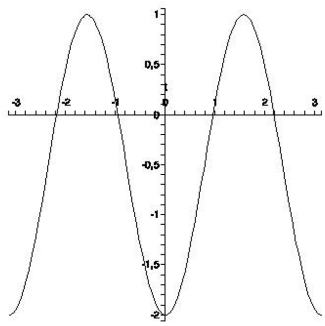
$$1 + 4\rho^2\cos^2\theta + 2\rho\cos\theta + \rho^4 + 2\rho^3\cos\theta - \rho^2 = \rho^4 + 4\rho^2\cos^2\theta + 4\rho^3\cos\theta$$

soit à $\left(1 - \rho^2\right)(1 + 2\rho\cos\theta) = 0$.

On obtient donc la réunion du cercle de centre O de rayon 1 et de la droite d'équation $x = -\dfrac{1}{2}$ qui est la droite (BC). Lorsque M est sur la droite, les cercles circonscrits à $M_1M_2M_3$ et $M_2M_3M_4$ sont confondus, de centre O de rayon OM, et lorsque M est sur le cercle trigonométrique, les deux cercles sont symétriques par rapport à (M_2M_3).

III-1. Par parité, il suffit de faire l'étude sur $[0, \pi]$.

a) s est dérivable sur $[0, \pi]$ et $s'(\theta) = 6\cos\theta\sin\theta = 3\sin(2\theta)$ donc s est croissante sur $\left[0, \dfrac{\pi}{2}\right]$ et décroissante sur $\left[\dfrac{\pi}{2}, \pi\right]$ (ce que l'on pourrait voir directement avec les variations de cos).



$s(\theta)$ s'annule lorsque $\cos\theta$ vaut $-\dfrac{1}{\sqrt{3}}$ ou $\dfrac{1}{\sqrt{3}}$, est positif lorsque $\cos\theta$ est dans $\left[-\dfrac{1}{\sqrt{3}}, \dfrac{1}{\sqrt{3}}\right]$, négatif sinon.

Comme cos est continue strictement décroissante sur $I = [0, \pi]$ et puisque $\cos(I) = [-1, 1]$ contient $\dfrac{1}{\sqrt{3}}$, il existe un unique réel $\alpha \in [0, \pi]$ tel que $\cos\alpha = \dfrac{1}{\sqrt{3}}$.

Alors $\cos(\pi - \alpha)$ est l'unique réel de $[0, \pi]$ pour lequel cos prend la valeur $\dfrac{-1}{\sqrt{3}}$.

s est donc négatif sur $[0, \alpha]$ et $[\pi - \alpha, \pi]$, positif sur $E' = [\alpha, \pi - \alpha]$.

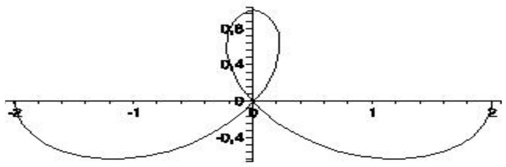
Par parité, on en déduit : $E = [-\pi + \alpha, -\alpha] \cup [\alpha, \pi - \alpha]$

(b) L'étude précédente conduit au tableau de valeurs :

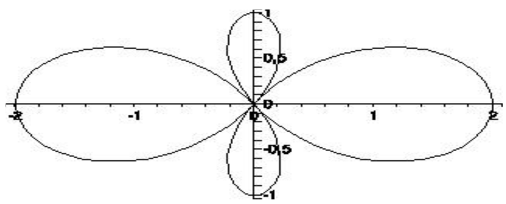
θ	0	$\pi/6$	$\pi/4$	α	$\pi/3$	$\pi/2$		$\pi - \alpha$		π
$s(\theta)$	-2	$-7/2$	$-1/2$	0	$1/4$	1		0		-2

La propriété $s(\theta) = s(-\theta)$ assure que la courbe est symétrique par rapport à l'axe des abscisses.

La propriété $s(\theta) = s(\pi - \theta)$ assure que la courbe est symétrique par rapport à l'axe des ordonnées.



Tracé sur $[0, \pi]$



Tracé sur $[-\pi, \pi]$

III-2. (a) Par parité, on étudie r_1 sur $[\alpha, \pi - \alpha]$.

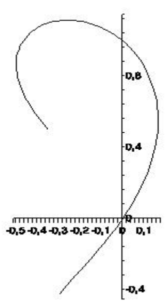
$r_1(\theta)$ est nul si et seulement si $\begin{cases} 1 - 3\cos^2\theta = \cos^2\theta \\ \cos\theta \geqslant 0 \end{cases}$ soit en $\dfrac{\pi}{3}$.

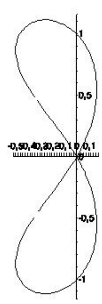
(b) On obtient le tableau :

θ	α	$\pi/3$	$\pi/2$	$\pi - \alpha$
$r_1(\theta)$	$-1/\sqrt{3}$	0	1	$1/\sqrt{3}$

et $r_1(\theta) = r_1(-\theta)$ assure que la courbe est symétrique par rapport à l'axe des abscisses.

Ceci donne le tracé, successivement sur $[\alpha, \pi - \alpha]$ puis sur E :



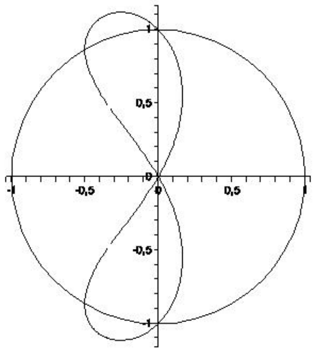


III-3. Dans la partie II, prendre le point M d'affixe $z = \rho' e^{i\theta'}$ avec $\rho' < 0$ revient à travailler avec $z = \rho e^{i\theta}$ où $\rho = -\rho'$ et $\theta = \pi + \theta'$.
La condition $(\rho + \cos\theta)^2 = 1 - 3\cos^2\theta$ est alors équivalente à $(\rho' + \cos\theta')^2 = 1 - 3\cos^2\theta'$.
$\rho = 1$ ou $\rho = -1$ est toujours une équation du cercle trigonométrique.

Prendre ρ dans $\mathbb{R}^+$ ou dans $\mathbb{R}$ ne change donc rien à la partie II, et l'ensemble trouvé en II.3.e est la réunion du cercle de centre O et de rayon 1, de la courbe précédente et de la courbe définie par

$$r_2(\theta) = -\sqrt{1 - 3\cos^2(\theta)} - \cos\theta.$$

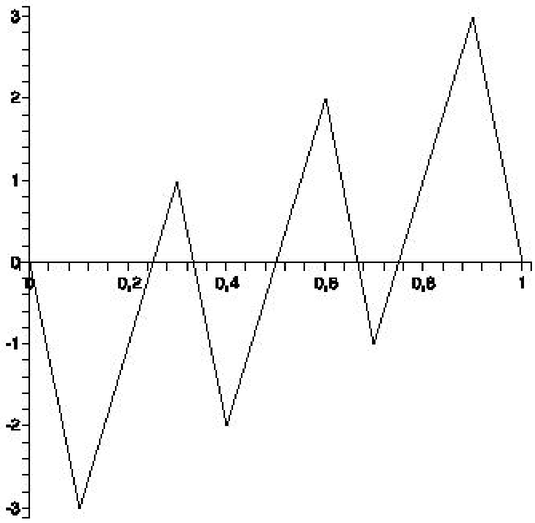
Mais comme $r_2(\theta) = -r_1(\pi - \theta)$, les courbes définies par r_1 et r_2 sont symétriques par rapport à l'axe des abscisses.
La courbe définie par r_2 est donc celle définie par r_1.



Exercice 2

1. La fonction $g : x \mapsto f\left(x + \frac{3}{10}\right) - f(x)$ est continue sur $\left[0, \frac{7}{10}\right]$ et jamais nulle, donc de signe constant sinon elle s'annulerait d'après le théorème des valeurs intermédiaires. Supposons par exemple que :
$$\forall x \in \left[0, \frac{7}{10}\right], f\left(x + \frac{3}{10}\right) - f(x) > 0.$$
Alors : $\begin{cases} 0 = f(0) < f\left(\frac{3}{10}\right) < f\left(\frac{6}{10}\right) < f\left(\frac{9}{10}\right) \\ f\left(\frac{1}{10}\right) < f\left(\frac{4}{10}\right) < f\left(\frac{7}{10}\right) < f(1) = 0 \end{cases}$
D'après le théorème des valeurs intermédiaires, f s'annule donc sur $\left]\frac{1}{10}, \frac{3}{10}\right[$, sur $\left]\frac{3}{10}, \frac{4}{10}\right[$, sur $\left]\frac{4}{10}, \frac{6}{10}\right[$, sur $\left]\frac{6}{10}, \frac{7}{10}\right[$ et sur $\left]\frac{7}{10}, \frac{9}{10}\right[$. En rajoutant 0 et 1, cela donne au moins 7 annulations.
2. Comme exemple d'une telle fonction, il suffit de prendre l'application continue affine par morceaux définie par :

$f(0) = 0,\ f\left(\frac{1}{10}\right) = -3,\ f\left(\frac{3}{10}\right) = 1,\ f\left(\frac{4}{10}\right) = -2,$
$f\left(\frac{6}{10}\right) = 2,\ f\left(\frac{7}{10}\right) = -1,\ f\left(\frac{9}{10}\right) = 3,\ f(1) = 0$
qui vérifie $f\left(x + \frac{3}{10}\right) - f(x) = 1$
pour tout $x \in \left[0, \frac{7}{10}\right]$.



Exercice 3

1. On se place dans un repère orthonormal direct tel que B ait pour coordonnées $(0,0)$, C ait pour coordonnées $(a,0)$, $a>0$, et on note θ_1 (resp. θ_2) l'angle de vecteurs $\left(\overrightarrow{BC},\overrightarrow{BA_0}\right)$ (resp. $\left(\overrightarrow{CB},\overrightarrow{CA_0}\right)$).

   Alors A_k est le point tel que : $\begin{cases} \left(\overrightarrow{BC},\overrightarrow{BA_k}\right) = \theta_1/2^k \\ \left(\overrightarrow{CB},\overrightarrow{CA_k}\right) = \theta_2/2^k \end{cases}$

   donc A_k est le point d'intersection des droites d'équations $\begin{cases} y = \tan\left(\dfrac{\theta_1}{2^k}\right)x \\ y = \tan\left(\dfrac{\theta_2}{2^k}\right)(x-a) \end{cases}$.

   Ainsi, A_k a pour coordonnées : $\begin{cases} x_k = \dfrac{-\tan\left(\theta_2/2^k\right)a}{\tan\left(\theta_1/2^k\right)-\tan\left(\theta_2/2^k\right)} \xrightarrow{k\to+\infty} \dfrac{\theta_2 a}{\theta_2-\theta_1} \\ y_k = \tan\left(\dfrac{\theta_1}{2^k}\right)x_k \xrightarrow{k\to+\infty} 0 \end{cases}$

   ce qui donne le point A, de coordonnées $\left(\dfrac{\theta_2 a}{\theta_2-\theta_1},0\right)$.

2. Supposons A_1 différent de A_0.
   A_1 est l'intersection des hauteurs de A_0BC. Par définition, CA_1 est donc orthogonal à BA_0, ce qui signifie que BA_0 est une hauteur de BCA_1.
   Par ailleurs, A_0BC et A_1BC ont en commun la hauteur A_0A_1.
   BA_0 et A_0A_1 s'intersectent en A_0, donc A_0 est l'orthocentre de A_1BC : $A_0 = A_2$.
   Finalement, pour tout $k\in\mathbb{N}$: $A_{2k} = A_0$ et $A_{2k+1} = A_1$.
   Dans le cas particulier $A_0 = A_1$ (triangle rectangle en A_0), la suite est constante égale à A_0.

Exercice 4

I-1. 1 ne convient pas.
$\left(2^k \bmod 7\right)$, $k\in\mathbb{N}$, vaut alternativement 1, 2 et 4 donc 2 ne convient pas.
$\left(3^k \bmod 7\right)$, $k\in\mathbb{N}$, vaut successivement 1, 3, 2, 6, 4, 5 pour $k\in[\![0,5]\!]$ donc 3 est une racine primitive modulo 7.
$\left(4^k \bmod 7\right)$, $k\in\mathbb{N}$, vaut 1, 4 ou 2 donc 4 ne convient pas.
$\left(5^k \bmod 7\right)$, $k\in\mathbb{N}$, vaut successivement 1, 5, 4, 6, 2, 3 pour $k\in[\![0,5]\!]$ donc 5 est racine primitive modulo 7.
$\left(6^k \bmod 7\right)$, $k\in\mathbb{N}$, vaut alternativement 1 et 6 donc 7 ne convient pas.

I-2. (a) Soit $k \geqslant p-1$.
En faisant la division euclidienne de k par $p-1$, il existe $q\in\mathbb{N}$ et $r\in[\![0,p-2]\!]$ tels que :
$$k = q(p-1)+r.$$
D'après le petit théorème de Fermat : $g^{p-1} = 1 \pmod{p}$ donc $g^k = g^r \pmod{p}$.
Alors : $\left\{\left(g^k \bmod p\right) \mid k\in\mathbb{N}\right\} = \{(g^r \bmod p) \mid r\in[\![0,p-2]\!]\}$ et comme g est racine primitive modulo p, les $\left(g^i \bmod p\right)$, $i\in[\![0,p-2]\!]$, décrivent $[\![1,p-1]\!]$.

(b) On remarque que $[\![1,p-1]\!]$ contient $p-1$ éléments, et que lorsque r parcourt $[\![0,p-2]\!]$, on a $p-1$ valeurs de g^r, donc il existe, pour chaque $A\in[\![1,p-1]\!]$, exactement un élément $r\in[\![0,p-2]\!]$ tel que :
$$A = (g^r \bmod p).$$

(c) Si b est congru à a modulo $p-1$, il existe k tel que $b = a+k(p-1)$.
Comme $g^{p-1} = 1 \pmod{p}$: $\left(g^b \bmod p\right) = (g^a \bmod p) = A$.

I-3. (a) Initialisations : $y \leftarrow 1$, $i \leftarrow 0$
Tant que $y \neq A$ faire
– $y \leftarrow g*y \pmod{p}$
– $i \leftarrow i+1$

fin Tant que
Renvoyer i

(b) $\ell(40) = 18$.

II-1. $54 = 2 \times 3^3$ donc $g^{75} = g^{60} g^{15} = g^{60}\left(g^5\right)^3$ est égal, modulo 113, à 54.
Ainsi : $\ell(54) = 75$.

II-2. Posons $q_j = \ell(p_j)$. Alors $p_j = g^{q_j} \pmod{p}$ donc $g^{a_i} = g^{q_1 e_{i,1} + q_2 e_{i,2} + \cdots + q_n e_{i,n}} \pmod{p}$.
Deux entiers k et l, avec par exemple $k > l$, sont tels que $g^k = g^l \pmod{p}$ si et seulement si $g^{k-l} = 1 \pmod{p}$ puique g^l est premier avec p.
Soit r le reste de la division euclidienne de $k - l$ par $p - 1$: g^{k-l} est égal à g^r modulo p, et g^r est égal à 1 si et seulement si $r = 0$ (cf. 2.b) donc g^k et g^l sont égaux modulo p si et seulement si :

$$k = l \pmod{(p-1)}.$$

Ainsi : $a_i = e_{i,1}\ell(p_1) + e_{i,2}\ell(p_2) + \cdots + e_{i,n}\ell(p_n) \pmod{(p-1)}$.

II-3. (a) $\begin{cases} g = 2^2 \times 5 \pmod{53} \\ g^3 = 2 \times 5^2 \pmod{53} \end{cases}$ donc $\begin{cases} 2\ell(2) + \ell(5) = 1 \pmod{52} \\ \ell(2) + 2\ell(5) = 3 \pmod{52} \end{cases}$
En soustrayant la deuxième ligne à deux fois la première : $3\ell(2) = -1 \pmod{52}$.
3 est premier avec 52 : il existe $(u, v) \in \mathbb{Z}^2$ tel que $3u + 52v = 1$ soit $3u = 1 \pmod{52}$.
On sait déterminer u par l'algorithme d'Euclide et on trouve -17 donc $\ell(2) = 17$.
On en déduit que : $\ell(5) = 1 - 2\ell(2) \pmod{52}$ donc $\ell(5) = 19$.

(b) $A = 2^3 \times 5$ donc $\ell(40) = 3\ell(2) + \ell(5) \pmod{52}$: $\ell(40) = 18$.

(c) Il s'agit de déterminer le nombre de couples $(\alpha, \beta) \in \mathbb{N}^2$ tels que $2^\alpha 5^\beta$ est inférieur à 52.
Pour $\beta = 0$, α peut varier entre 0 et 5 soit 6 couples.
Pour $\beta = 1$: α varie entre 0 et 3 d'où 4 couples.
Pour $\beta = 2$: α vaut 0 ou 1 d'où 2 couples.
Finalement, il y a 12 entiers dans $[\![1, 52]\!]$ qui se factorisent en fonction de 2 et 5.

II-4. (a) A est inversible modulo p et les $(g^s \bmod p)$ décrivent $[\![1, p-1]\!]$ donc les $(g^s A \bmod p)$ aussi ; en particulier, il existe (au moins) un entier s tel que $(g^s A \bmod p)$ se factorise à l'aide de $p_1, \cdots, p_n$ uniquement.

(b) Si on a choisi un tel s : il existe des entiers $\alpha_1, \cdots, \alpha_n$ tels que $(g^s A \bmod p) = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$
donc $s + \ell(A) = \alpha_1 \ell(p_1) + \cdots + \alpha_n \ell(p_n) \pmod{(p-1)}$
d'où $\ell(A) = \alpha_1 \ell(p_1) + \cdots + \alpha_n \ell(p_n) - s \pmod{(p-1)}$.

(c) Pour $A = 30$, on peut prendre $s = 3$:

$$(g^s A \bmod 53) = 2^4 \text{ donc } s + \ell(A) = 4\ell(2) \pmod{52}.$$

Finalement : $\ell(30) = 13$.

II-5. (a) Les puissances de p_1 dans $[\![1, p-1]\!]$ sont $1, p_1, \cdots, p_1^{k_1}$ où $k_1 = \mathrm{E}\left(\dfrac{\ln(p-1)}{\ln p_1}\right)$.
Il y en a donc $\mathrm{E}\left(\dfrac{\ln(p-1)}{\ln p_1}\right) + 1$.

(b) Lorsque s décrit $[\![0, p-2]\!]$, $g^s A \pmod{p}$ décrit (exactement une fois) $[\![1, p-1]\!]$.
La probabilité demandée est le nombre d'entiers qui conviennent divisé par le nombre $p - 1$ de cas soit $\dfrac{1}{p-1}\left(\mathrm{E}\left(\dfrac{\ln(p-1)}{\ln p_1}\right) + 1\right)$.
Elle est supérieure à $\dfrac{\ln(p-1)}{(p-1)\ln p_1}$.

(c) Pour i fixé, le nombre d'entiers de la forme $p_1^i p_2^j$ est le nombre d'entiers j tels que $p_2^j \leqslant \dfrac{p-1}{p_1^i}$, soit le nombre d'entiers de $\left[0, \mathrm{E}\left(\dfrac{\ln \dfrac{(p-1)}{p_1^i}}{\ln p_2}\right)\right]$, qui est supérieur à $\dfrac{\ln \dfrac{(p-1)}{p_1^i}}{\ln p_2}$, donc le nombre d'entiers qui se factorisent en fonction de p_1 et p_2 est supérieur à

$$S=\frac{1}{\ln p_2}\sum_{i=0}^{k_1}\ln\frac{p-1}{p_1^i} \text{ où } k_1=\mathrm{E}\left(\frac{\ln(p-1)}{\ln p_1}\right).$$

Or $S=\dfrac{1}{\ln p_2}\ln\dfrac{(p-1)^{k_1+1}}{p_1^{k_1(k_1+1)/2}}\geqslant\dfrac{\ln\left[(p-1)^{(k_1+1)/2}\right]}{\ln p_2}=\dfrac{(k_1+1)\ln(p-1)}{2\ln p_2}\geqslant\dfrac{(\ln(p-1))^2}{2(\ln p_1)(\ln p_2)}$.

Ainsi : $P\geqslant\dfrac{S}{p-1}\geqslant\dfrac{(\ln(p-1))^2}{2(p-1)(\ln p_1)(\ln p_2)}$.

Majoration : il suffit de majorer le nombre d'entiers q de $[\![1,p-1]\!]$ qui s'écrivent sous la forme $p_1^\alpha p_2^\beta$ avec $(\alpha,\beta)\in\mathbb{N}^2$.

Dans ce cas : $\ln q=\alpha\ln p_1+\beta\ln p_2\leqslant\ln(p-1)$ donc $\begin{cases}0\leqslant\alpha\leqslant\dfrac{\ln(p-1)}{\ln p_1}\\ 0\leqslant\beta\leqslant\dfrac{\ln(p-1)}{\ln p_2}\end{cases}$.

Il y a donc au plus $\left(E\left(\dfrac{\ln(p-1)}{\ln p_1}\right)+1\right)\left(E\left(\dfrac{\ln(p-1)}{\ln p_2}\right)+1\right)\leqslant\left(\dfrac{\ln(p-1)}{\ln p_1}+1\right)\left(\dfrac{\ln(p-1)}{\ln p_2}+1\right)$ choix pour le couple (α,β), d'où le résultat.

(d) On généralise le travail fait précédemment.

Majoration : comme ci-dessus, la probabilité recherchée est majorée par $\dfrac{1}{p-1}\displaystyle\prod_{k=1}^{n}\left(\dfrac{\ln(p-1)}{\ln p_k}+1\right)$.

Minoration.

Montrons par récurrence sur n que, pour tout réel $x\geqslant 1$, le nombre d'entiers de $[1,x]$ qui se décomposent à l'aide de p_1, …, p_n uniquement est supérieur à $\dfrac{(\ln x)^n}{n!(\ln p_1)\cdots(\ln p_n)}$.

On l'a vu ci-dessus pour $n=1$ et $n=2$ (le fait que x était de la forme $p-1$ avec p premier n'intervenait pas).

Supposons le résultat vrai pour $n-1$ nombres premiers et passons à n.

Pour i_1 fixé, le nombre d'entiers inférieurs à x de la forme $p_1^{i_1}\left(p_2^{i_2}\cdots p_n^{i_n}\right)$ est le nombre d'entiers de la forme $p_2^{i_2}\cdots p_n^{i_n}$ inférieurs à $\dfrac{x}{p_1^{i_1}}$, donc est supérieur à $\dfrac{\left(\ln\left[x/p_1^{i_1}\right]\right)^{n-1}}{(n-1)!(\ln p_2)\cdots(\ln p_n)}$.

Le nombre d'entiers recherché dans $[1,x]$ est donc supérieur à $T=\displaystyle\sum_{i=0}^{k_1}\frac{\left(\ln\left[x/p_1^{i}\right]\right)^{n-1}}{(n-1)!(\ln p_2)\cdots(\ln p_n)}$ avec $k_1=\mathrm{E}\left(\dfrac{\ln x}{\ln p_1}\right)$.

Soit $S=\displaystyle\sum_{i=0}^{k_1}\left(\ln\frac{x}{p_1^i}\right)^{n-1}$.

On remarque que, pour $i\leqslant k_1-1$: $\forall t\in\left[\ln x-(i+1)\ln p_1,\ln x-i\ln p_1\right],\ t^{n-1}\leqslant\left(\ln\dfrac{x}{p_1^i}\right)^{n-1}$

donc $S\geqslant\left(\ln\dfrac{x}{p_1^{k_1}}\right)^{n-1}+\dfrac{1}{\ln p_1}\displaystyle\int_{\ln x-k_1\ln p_1}^{\ln x}t^{n-1}\,\mathrm{d}\,t\geqslant\frac{1}{\ln p_1}\int_0^{\ln x}t^{n-1}\,\mathrm{d}\,t=\frac{(\ln x)^n}{n\ln p_1}$

d'où $T\geqslant\dfrac{(\ln x)^n}{n!(\ln p_1)\cdots(\ln p_n)}$ et on a l'hérédité.

Finalement, la probabilité pour qu'un entier de $[\![1,p-1]\!]$ se décompose en fonction de $p_1,\ \cdots,\ p_n$ uniquement est supérieure à $\dfrac{(\ln(p-1))^n}{n!(p-1)(\ln p_1)\cdots(\ln p_n)}$.