

### Exercice 1

Dans cet exercice, on se place dans un plan  $\mathcal{P}$  muni d'un repère orthonormal direct  $(O; \vec{u}, \vec{v})$ .

#### I- Préliminaires de géométrie élémentaire

- Soit  $D$  et  $D'$  deux droites sécantes en un point  $I$ ,  $s$  et  $s'$  les symétries axiales respectivement d'axes  $D$  et  $D'$ .  
Montrer que  $s' \circ s$  est une rotation, et déterminer ses éléments caractéristiques.
- Soit  $ABC$  un triangle équilatéral direct,  $O$  le centre du cercle circonscrit à  $AC$ .  
On désigne par  $s_1$ ,  $s_2$  et  $s_3$  les symétries axiales respectivement par rapport aux droites  $(OA)$ ,  $(OB)$  et  $(OC)$ . et par  $r$  la rotation de centre  $O$  d'angle  $\frac{2\pi}{3}$ .  
Soit  $M$  un point de plan,  $M_1 = s_1(M)$ ,  $M_2 = s_2(M)$ ,  $M_3 = s_3(M)$ .
  - Montrer que  $M_2 = r^2(M_1)$  et  $M_3 = r(M_1)$  où  $r^2$  désigne  $r \circ r$
  - Quelle est la nature du triangle  $M_1M_2M_3$  ?

#### II- Nombres complexes

L'affixe du vecteur  $\vec{u}$  étant 1 et celle du vecteur  $\vec{v}$  étant  $i$  (avec  $i^2 = -1$ ), comme il est d'usage,

on pose  $j = e^{2i\pi/3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$

On considère, dans le plan  $\mathcal{P}$ , les points  $O$ ,  $A$ ,  $B$  et  $C$  d'affixes respectives  $0$ ,  $1$ ,  $j$  et  $j^2$ .

On désigne par  $s_1$ ,  $s_2$  et  $s_3$  les symétries axiales respectivement par rapport aux droites  $(OA)$ ,  $(OB)$  et  $(OC)$ .

Soit enfin  $M$  un point quelconque du plan  $\mathcal{P}$ , d'affixe  $z = \rho e^{i\theta}$ ,  $\rho \in \mathbb{R}^+$ ,  $\theta \in \mathbb{R}$ .

- Soit  $M_1 = s_1(M)$ ,  $M_2 = s_2(M)$ ,  $M_3 = s_3(M)$ .  
Montrer que les points  $M_1$ ,  $M_2$  et  $M_3$  ont pour affixes respectives  $\bar{z}$ ,  $j^2\bar{z}$  et  $j\bar{z}$ .
- Soit  $M_4$  la symétrique de  $M$  par rapport à la droite  $(BC)$ .  
Montrer le point  $J$  d'affixe  $-\frac{1}{2}$  est le milieu du segment  $[M_1M_4]$ .  
En déduire l'affixe de  $M_4$ .
- A quelle condition les points  $M_2$ ,  $M_3$  et  $M_4$  sont alignés?  
*On suppose désormais que  $M_2$ ,  $M_3$  et  $M_4$  ne sont pas alignés.*  
*On note  $\Omega$  le centre du cercle circonscrit au triangle  $M_2M_3M_4$*
  - Justifier le fait que  $\Omega$  appartient à la droite  $(OM_1)$ .  
Dans la suite, on note son affixe  $\lambda e^{-i\theta}$  avec  $\lambda$  réel.
  - Montrer que  $\lambda = -\frac{1 + 2\rho \cos(\theta)}{\rho + 2 \cos(\theta)}$
  - En déduire une expression du rayon  $R$  du cercle circonscrit au triangle  $M_2M_3M_4$ .
  - Montrer que ce rayon est égal à 1 si et seulement si :  $\rho = 1$  ou  $(\rho + \cos(\theta))^2 = 1 - 3 \cos^2(\theta)$ .
- Montrer que le cercle circonscrit au triangle  $M_2M_3M_4$  est de même rayon que le cercle circonscrit au triangle  $M_1M_2M_3$  si et seulement si  $M$  appartient à un ensemble  $\Gamma$  que l'on précisera géométriquement.  
Que peut-on dire dans ce cas des deux cercles circonscrits ?

#### III- Etude de fonctions

On considère l'application  $s$  définie pour tout  $\theta \in [-\pi; \pi]$  par  $s(\theta) = 1 - 3 \cos^2(\theta)$ .

- Etudier les variations de  $s$ .  
Préciser ses extrema, les valeurs de  $\theta$  pour lesquelles  $s(\theta)$  est nul, l'ensemble  $E$  des  $\theta \in [-\pi; \pi]$  tels que  $s(\theta) \geq 0$ .
  - En déduire l'allure de la courbe décrite par le point d'affixe  $s(\theta)e^{i\theta}$  lorsque  $\theta$  varie.  
On précisera les points d'intersection avec les axes et éventuellement quelques points particuliers (pour  $\theta = \frac{\pi}{6}$ ,  $\frac{\pi}{4}$ ,  $\frac{\pi}{3}$  par exemple)  
On pourra aussi justifier les symétries de la courbe.
- Soit la fonction  $r_1$  définie pour tout  $\theta \in E$  par  $r_1(\theta) = \sqrt{1 - 3 \cos^2(\theta)} - \cos(\theta)$ .



2. (a) Montrer que l'ensemble des  $(g^k \bmod p)$  pour  $k \in [0; p-2]$  est  $[1; p-1]$ .  
 (b) Soit  $A \in [1; p-1]$ .  
 Justifier l'existence et l'unicité d'un entier  $a \in [0; p-2]$  tel que  $A = (g^a \bmod p)$ .  
*a est appelé logarithme de base g modulo p de A. On le note  $\ell(A)$*   
 (c) Soit  $b$  un entier naturel congru à  $a$  modulo  $p-1$ . Calculer  $g^b \bmod p$ .
3. Une solution élémentaire pour déterminer  $\ell(A)$  consiste à calculer les entiers  $(g^k \bmod p)$ , pour  $k = 0, 1, \dots$  jusqu'à trouver  $A$ .
- (a) Décrire un algorithme qui réalise ce travail.  
 (b) Dans cette question, on prend :  $p = 53$ ,  $A = 40$ ,  $g = 20$ .  
 On admettra que 20 est bien une racine primitive modulo 53.  
 En programmant l'algorithme précédent sur une calculatrice, déterminer  $\ell(A)$ .

## II - Calcul du logarithme discret par la méthode d'Adleman

Cette partie exploite le fait que la connaissance des logarithmes de quelques entiers permet de déterminer rapidement le logarithme de tout entier

1. On se place dans le cas  $p = 113$ ,  $g = 55$  et on donne  $\ell(2) = 60$ ,  $\ell(3) = 5$ . Trouver  $\ell(54)$ .

On suppose choisis, pour la suite de cette partie, des nombres premiers distincts  $p_1, \dots, p_n$  strictement inférieurs à  $p$  et des entiers  $a_1, \dots, a_n$  tels que, pour tout  $i \in [1; n]$ , les facteurs premiers de  $(g^{a_i} \bmod p)$  appartiennent à  $\{p_1; \dots; p_n\}$

Pour chaque  $i \in [1; n]$ , on a ainsi une relation  $(g^{a_i} \bmod p) = p_1^{e_{i,1}} p_2^{e_{i,2}} \dots p_n^{e_{i,n}}$  où les  $e_{i,j}$  pour  $(i, j) \in [1; n]^2$ , sont des entiers naturels.

2. Montrer que, pour tout  $i \in [1; n]$ ,

$$a_i = e_{i,1}\ell(p_1) + e_{i,2}\ell(p_2) + \dots + e_{i,n}\ell(p_n) \quad (\text{modulo } (p-1))$$

3. On prend dans cette question  $p = 53$ ,  $g = 20$ ,  $n = 2$ ,  $p_1 = 2$ ,  $p_2 = 5$ .

- (a) A l'aide de  $g$  et  $g^3$ , déterminer  $\ell(2)$  et  $\ell(5)$ .  
 (b) En déduire  $\ell(40)$ .  
 (c) Combien d'entiers de  $[1; 52]$  peuvent s'écrire sous la forme  $2^\alpha 5^\beta$ , avec  $\alpha$  et  $\beta$  entiers naturels?

4. Soit  $A \in [1; p-1]$ .

- (a) Montrer que l'ensemble des  $(g^s A \bmod p)$  pour  $s \in [0; p-2]$  est  $[1; p-1]$ .  
 (b) On suppose connu  $s \in \mathbb{N}$  tel que  $(g^s A \bmod p)$  se factorise à l'aide de  $p_1, \dots, p_n$  uniquement.  
 Si on suppose connus  $\ell(p_1), \dots, \ell(p_n)$ , en déduire  $\ell(A)$ .  
 (c) Avec  $p = 53$  et  $g = 20$ , déterminer  $\ell(30)$ .

5. On revient au cas général.

- (a) Quel est le nombre d'entiers de  $[1; p-1]$  qui sont une puissance de  $p_1$  ?  
 (b) En déduire la probabilité pour qu'un entier  $s \in [0; p-2]$  soit tel que  $(g^s A \bmod p)$  soit une puissance de  $p_1$ .  
 (c) Montrer que la probabilité  $P$  pour qu'un entier  $s \in [0; p-2]$  soit tel que  $(g^s A \bmod p)$  se factorise à l'aide de  $p_1$  et  $p_2$  uniquement vérifie:

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

- (d) Généraliser le résultat au cas de  $n$  nombres premiers  $p_1, \dots, p_n$ .

Si vous voulez mettre ce document en ligne sur votre site, ayez la politesse de citer son origine .....

<http://www.maths-express.com>

Merci .....

## 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  $\theta$  son angle.

Pour un point  $M$  de  $D$ , différent de  $I$ ,  $D'$  est bissectrice de l'angle  $(\overrightarrow{IM}, \overrightarrow{Ir(M)})$  donc  $\theta$  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  $\bar{z} = \rho e^{-i\theta}$ .

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

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

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  $s \circ s_1 = s_J$

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

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  $-1 - \bar{z} = -1 - \rho e^{-i\theta}$ .

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  $S = \frac{(-1 - \bar{z}) - j\bar{z}}{j^2\bar{z} - j\bar{z}}$  est réel.

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

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

Ceci est équivalent à :  $z + \bar{z} = (j^2 + j)|z|^2$  et en posant  $z = x + iy$ ,  $(x, y) \in \mathbb{R}^2$ , on obtient la condition équivalente :  $2x = -x^2 - y^2$  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  $\omega$  d'affixe  $-1$  et de rayon 1 ( $O$  y compris, car dans ce cas particulier,  $M_2$  et  $M_3$  sont confondus).

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

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  $\lambda = \frac{-1 - 2\rho\cos\theta}{\rho + 2\cos\theta}$ .

(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  $\lambda$  ci-dessus.

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

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

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

$$\text{ou à } \rho^4 - 2\rho^2 + 1 + 2\rho(\rho^2 - 1)\cos\theta + 4(\rho^2 - 1)\cos^2\theta = 0,$$

$$\text{équivalent à : } (\rho^2 - 1)(\rho^2 + 2\rho\cos\theta + 4\cos^2\theta - 1) = 0.$$

Comme  $\rho$  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 :

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

$$\text{soit à } (1 - \rho^2)(1 + 2\rho\cos\theta) = 0.$$

On obtient donc la réunion du cercle de centre  $O$  de rayon 1 et de la droite d'équation  $x = -\frac{1}{2}$  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  $\left[0, \frac{\pi}{2}\right]$  et décroissante sur  $\left[\frac{\pi}{2}, \pi\right]$  (ce que l'on pourrait voir directement avec les variations de  $\cos$ ).

$s(\theta)$  s'annule lorsque  $\cos \theta$  vaut  $-\frac{1}{\sqrt{3}}$  ou  $\frac{1}{\sqrt{3}}$ , est positif

lorsque  $\cos \theta$  est dans  $\left[-\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}\right]$ , négatif sinon.

Comme  $\cos$  est continue strictement décroissante sur  $I = [0, \pi]$  et puisque  $\cos(I) = [-1, 1]$  contient  $\frac{1}{\sqrt{3}}$ , il existe

un unique réel  $\alpha \in [0, \pi]$  tel que  $\cos \alpha = \frac{1}{\sqrt{3}}$ .

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

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

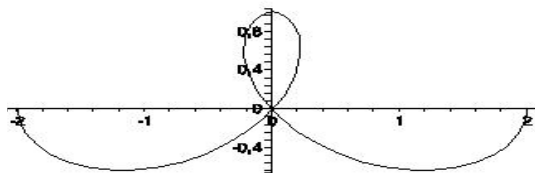
Par parité, on en déduit :  $E = [-\pi + \alpha, -\alpha] \cup [\alpha, \pi - \alpha]$

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

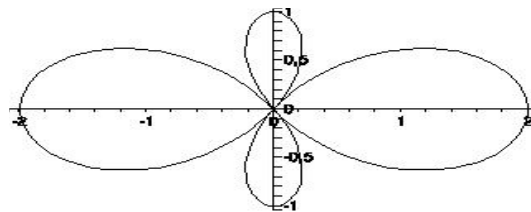
$\theta$	0	$\pi/6$	$\pi/4$	$\alpha$	$\pi/3$	$\pi/2$	$\pi - \alpha$	$\pi$
$s(\theta)$	-2	$-7/2$	$-1/2$	0	$1/4$	1	0	-2

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  $[\alpha, \pi - \alpha]$ .

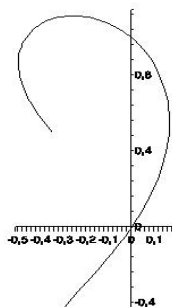
$r_1(\theta)$  est nul si et seulement si  $\begin{cases} 1 - 3 \cos^2 \theta = \cos^2 \theta \\ \cos \theta \geq 0 \end{cases}$  soit en  $\frac{\pi}{3}$ .

(b) On obtient le tableau :

$\theta$	$\alpha$	$\pi/3$	$\pi/2$	$\pi - \alpha$
$r_1(\theta)$	$-1/\sqrt{3}$	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  $(\rho' + \cos \theta')^2 = 1 - 3 \cos^2 \theta'$ .

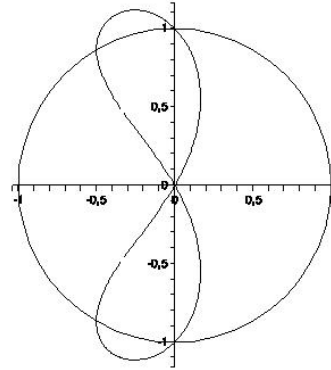
$\rho = 1$  ou  $\rho = -1$  est toujours une équation du cercle trigonométrique.

Prendre  $\rho$  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 :

$$\forall x \in \left[0, \frac{7}{10}\right], f\left(x + \frac{3}{10}\right) - f(x) > 0.$$

$$\text{Alors : } \begin{cases} 0 = f(0) < f\left(\frac{3}{10}\right) < f\left(\frac{6}{10}\right) < f\left(\frac{9}{10}\right) \\ f\left(\frac{1}{10}\right) < f\left(\frac{4}{10}\right) < f\left(\frac{7}{10}\right) < f(1) = 0 \end{cases}$$

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.

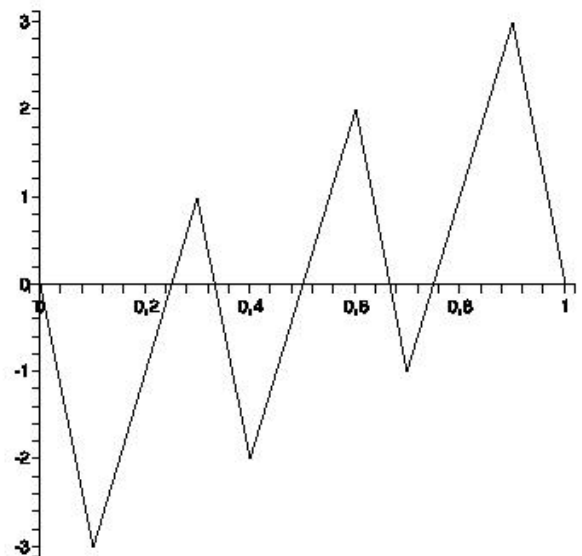
2. Comme exemple d'une telle fonction, il suffit de prendre l'application continue affine par morceaux définie par :

$$f(0) = 0, f\left(\frac{1}{10}\right) = -3, f\left(\frac{3}{10}\right) = 1, f\left(\frac{4}{10}\right) = -2,$$

$$f\left(\frac{6}{10}\right) = 2, f\left(\frac{7}{10}\right) = -1, f\left(\frac{9}{10}\right) = 3, f(1) = 0$$

$$\text{qui vérifie } f\left(x + \frac{3}{10}\right) - f(x) = 1$$

$$\text{pour tout } x \in \left[0, \frac{7}{10}\right].$$



### 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  $\theta_1$  (resp.  $\theta_2$ ) l'angle de vecteurs  $(\overrightarrow{BC}, \overrightarrow{BA_0})$  (resp.  $(\overrightarrow{CB}, \overrightarrow{CA_0})$ ).

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

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

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

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

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.

$(2^k \bmod 7)$ ,  $k \in \mathbb{N}$ , vaut alternativement 1, 2 et 4 donc 2 ne convient pas.

$(3^k \bmod 7)$ ,  $k \in \mathbb{N}$ , vaut successivement 1, 3, 2, 6, 4, 5 pour  $k \in \llbracket 0, 5 \rrbracket$  donc 3 est une racine primitive modulo 7.

$(4^k \bmod 7)$ ,  $k \in \mathbb{N}$ , vaut 1, 4 ou 2 donc 4 ne convient pas.

$(5^k \bmod 7)$ ,  $k \in \mathbb{N}$ , vaut successivement 1, 5, 4, 6, 2, 3 pour  $k \in \llbracket 0, 5 \rrbracket$  donc 5 est racine primitive modulo 7.

$(6^k \bmod 7)$ ,  $k \in \mathbb{N}$ , vaut alternativement 1 et 6 donc 6 ne convient pas.

I-2. (a) Soit  $k \geq p - 1$ .

En faisant la division euclidienne de  $k$  par  $p - 1$ , il existe  $q \in \mathbb{N}$  et  $r \in \llbracket 0, p - 2 \rrbracket$  tels que :

$$k = q(p - 1) + r.$$

D'après le petit théorème de Fermat :  $g^{p-1} = 1$  (modulo  $p$ ) donc  $g^k = g^r$  (modulo  $p$ ).

Alors :  $\{(g^k \bmod p) \mid k \in \mathbb{N}\} = \{(g^r \bmod p) \mid r \in \llbracket 0, p - 2 \rrbracket\}$  et comme  $g$  est racine primitive modulo  $p$ , les  $(g^i \bmod p)$ ,  $i \in \llbracket 0, p - 2 \rrbracket$ , décrivent  $\llbracket 1, p - 1 \rrbracket$ .

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

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  $g^{75} = g^{60}g^{15} = g^{60} (g^5)^3$  est égal, modulo 113, à 54.

Ainsi :  $\ell(54) = 75$ .

II-2. Posons  $q_j = \ell(p_j)$ . Alors  $p_j = g^{q_j}$  (modulo  $p$ ) donc  $g^{a_i} = g^{q_1 e_{i,1} + q_2 e_{i,2} + \dots + q_n e_{i,n}}$  (modulo  $p$ ).

Deux entiers  $k$  et  $l$ , avec par exemple  $k > l$ , sont tels que  $g^k = g^l$  (modulo  $p$ ) si et seulement si  $g^{k-l} = 1$  (modulo  $p$ ) puisque  $g^l$  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 :  $a_i = e_{i,1}\ell(p_1) + e_{i,2}\ell(p_2) + \dots + e_{i,n}\ell(p_n)$  (modulo  $(p-1)$ ).

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  $\beta = 0$ ,  $\alpha$  peut varier entre 0 et 5 soit 6 couples.

Pour  $\beta = 1$  :  $\alpha$  varie entre 0 et 3 d'où 4 couples.

Pour  $\beta = 2$  :  $\alpha$  vaut 0 ou 1 d'où 2 couples.

Finalement, il y a 12 entiers dans  $\llbracket 1, 52 \rrbracket$  qui se factorisent en fonction de 2 et 5.

II-4. (a)  $A$  est inversible modulo  $p$  et les  $(g^s \bmod p)$  décrivent  $\llbracket 1, p-1 \rrbracket$  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  $p_1, \dots, p_n$  uniquement.

(b) Si on a choisi un tel  $s$  : il existe des entiers  $\alpha_1, \dots, \alpha_n$  tels que  $(g^s A \bmod p) = p_1^{\alpha_1} \dots p_n^{\alpha_n}$

donc  $s + \ell(A) = \alpha_1 \ell(p_1) + \dots + \alpha_n \ell(p_n) \pmod{(p-1)}$

d'où  $\ell(A) = \alpha_1 \ell(p_1) + \dots + \alpha_n \ell(p_n) - s \pmod{(p-1)}$ .

(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  $\llbracket 1, p-1 \rrbracket$  sont  $1, p_1, \dots, p_1^{k_1}$  où  $k_1 = E\left(\frac{\ln(p-1)}{\ln p_1}\right)$ .

Il y en a donc  $E\left(\frac{\ln(p-1)}{\ln p_1}\right) + 1$ .

(b) Lorsque  $s$  décrit  $\llbracket 0, p-2 \rrbracket$ ,  $g^s A \pmod{p}$  décrit (exactement une fois)  $\llbracket 1, p-1 \rrbracket$ .

La probabilité demandée est le nombre d'entiers qui conviennent divisé par le nombre  $p-1$  de cas soit  $\frac{1}{p-1} \left( E\left(\frac{\ln(p-1)}{\ln p_1}\right) + 1 \right)$ .

Elle est supérieure à  $\frac{\ln(p-1)}{(p-1) \ln p_1}$ .

(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  $p_2^j \leq \frac{p-1}{p_1^i}$ ,

soit le nombre d'entiers de  $\left[ 0, E\left(\frac{\ln\left(\frac{p-1}{p_1^i}\right)}{\ln p_2}\right) \right]$ , qui est supérieur à  $\frac{\ln(p-1)}{\ln p_2}$ , donc le nombre

d'entiers qui se factorisent en fonction de  $p_1$  et  $p_2$  est supérieur à

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

$$\text{Or } S = \frac{1}{\ln p_2} \ln \frac{(p-1)^{k_1+1}}{p_1^{k_1(k_1+1)/2}} \geq \frac{\ln [(p-1)^{(k_1+1)/2}]}{\ln p_2} = \frac{(k_1+1) \ln(p-1)}{2 \ln p_2} \geq \frac{(\ln(p-1))^2}{2(\ln p_1)(\ln p_2)}.$$

$$\text{Ainsi : } P \geq \frac{S}{p-1} \geq \frac{(\ln(p-1))^2}{2(p-1)(\ln p_1)(\ln p_2)}.$$

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

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

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

(d) On généralise le travail fait précédemment.

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

*Minoration.*

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

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

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

avec  $k_1 = E\left(\frac{\ln x}{\ln p_1}\right)$ .

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

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

$$\text{donc } S \geq \left(\ln \frac{x}{p_1^{k_1}}\right)^{n-1} + \frac{1}{\ln p_1} \int_{\ln x - k_1 \ln p_1}^{\ln x} t^{n-1} dt \geq \frac{1}{\ln p_1} \int_0^{\ln x} t^{n-1} dt = \frac{(\ln x)^n}{n \ln p_1}$$

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

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