CONCOURS GÉNÉRAL DES LYCÉES

SESSION DE 2005

COMPOSITION DE MATHÉMATIQUES

(Classe terminale S)

Durée : 5 heures

La calculatrice de poche est autorisée, conformément à la réglementation.

La clarté et la précision de la rédaction seront prises en compte dans l'appréciation des copies.

Le sujet comporte quatre exercices indépendants.

Il n'est pas obligatoire de traiter systématiquement les questions dans l'ordre de l'énoncé, à condition d'indiquer clairement la question traitée en respectant l'indexation du texte.

Pour poursuivre, les candidats peuvent admettre les résultats d'une question, à condition de l'indiquer clairement sur la copie.

Exercice 1

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

I- Préliminaires de géométrie élémentaire

1. 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.
2. Soit ABC un triangle équilatéral direct, O le centre du cercle circonscrit à ABC.
   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 $\dfrac{2\pi}{3}$.
   Soit M un point du plan, $M_1 = s_1(M)$, $M_2 = s_2(M)$, $M_3 = s_3(M)$.
   (a) Montrer que : $M_2 = r^2(M_1)$ et $M_3 = r(M_1)$ (où r^2 désigne $r \circ r$).
   (b) Quelle est la nature du triangle $M_1M_2M_3$?

II- Nombres complexes

L'affixe du vecteur $\overrightarrow{u}$ étant 1 et celle du vecteur $\overrightarrow{v}$ étant notée i (avec $\mathrm{i}^2 = -1$), comme il est d'usage, on pose $j = \mathrm{e}^{2\mathrm{i}\pi/3} = -\dfrac{1}{2} + \mathrm{i}\dfrac{\sqrt{3}}{2}$.

On considère, dans le plan $\mathscr{P}$, 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 $\mathscr{P}$, d'affixe $z = \rho e^{\mathrm{i}\theta}$, $\rho \in \mathbb{R}^+$, $\theta \in \mathbb{R}$.

1. 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 $\overline{z}$, $j^2\overline{z}$ et $j\overline{z}$.
2. Soit M_4 le symétrique de M par rapport à la droite (BC).
   Montrer que le point J d'affixe $-\dfrac{1}{2}$ est le milieu du segment $[M_1M_4]$.
   En déduire l'affixe de M_4.
3. (a) À quelle condition les points M_2, M_3 et M_4 sont-ils alignés ?

On suppose désormais que M_2, M_3 et M_4 ne sont pas alignés ; on note Ω le centre du cercle circonscrit au triangle $M_2M_3M_4$.

   (b) Justifier le fait que Ω appartient à la droite (OM_1).
   Dans la suite, on note son affixe $\lambda e^{-\mathrm{i}\theta}$, avec λ réel.
   (c) Montrer que : $\lambda = -\dfrac{1 + 2\rho\cos\theta}{\rho + 2\cos\theta}$.
   (d) En déduire une expression du rayon R du cercle circonscrit au triangle $M_2M_3M_4$.
   (e) Montrer que ce rayon est égal à 1 si et seulement si : « $\rho = 1$ ou $(\rho + \cos\theta)^2 = 1 - 3\cos^2\theta$ ».
4. 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 Γ que l'on précisera géométriquement. Que peut-on dire dans ce cas des deux cercles circonscrits ?

III- Étude de fonctions

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

1. (a) Étudier les variations de s. Préciser ses extremums, les valeurs de θ pour lesquelles $s(\theta)$ est nul, l'ensemble E des $\theta \in [-\pi, \pi]$ tels que $s(\theta) \geqslant 0$.

(b) En déduire l'allure de la courbe décrite par le point d'affixe $s(\theta)e^{i\theta}$ lorsque θ 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.

2. Soit la fonction r_1 définie pour tout $\theta \in E$ par $r_1(\theta) = \sqrt{1 - 3\cos^2\theta} - \cos\theta$.
   (a) Déterminer les valeurs de θ pour lesquelles $r_1(\theta)$ est nul.
   (b) En déduire l'allure de la courbe décrite par le point d'affixe $r_1(\theta)e^{i\theta}$ lorsque θ varie.
3. Dessiner, sans chercher à être extrêmement précis, l'ensemble des points M tels que le triangle $M_2M_3M_4$ défini à la partie II ait un cercle circonscrit de rayon 1.

Exercice 2

Soit $f : [0,1] \to \mathbb{R}$ une fonction numérique définie et continue sur l'intervalle $[0,1]$.
On suppose que $f(0) = f(1) = 0$ et que pour tout x réel de l'intervalle $\left[0, \frac{7}{10}\right]$, $f\left(x + \frac{3}{10}\right) \neq f(x)$.

1. Démontrer que l'équation $f(x) = 0$ a au moins sept solutions sur $[0,1]$.
2. Donner un exemple de fonction f vérifiant les hypothèses ; on pourra se contenter d'une représentation graphique claire.

Exercice 3

On considère dans le plan trois points A_0, B, C non alignés.

1. On désigne par A_1 le centre du cercle inscrit dans le triangle A_0BC (c'est-à-dire le point d'intersection des bissectrices intérieures du triangle A_0BC).
   On poursuit le processus en considérant A_2, centre du cercle inscrit dans le triangle A_1BC, etc. Ainsi, pour tout i entier naturel, A_{i+1} est le centre du cercle inscrit dans le triangle A_iBC.
   Démontrer qu'il existe un point A, limite de la suite (A_n), c'est-à-dire tel que AA_n tende vers 0 et préciser sa position.
2. Que devient le résultat précédent si, à chaque étape, pour $i = 0, 1, 2, \ldots$, on prend pour A_{i+1} l'orthocentre du triangle A_iBC au lieu du centre du cercle inscrit ?

Exercice 4

Si m_1 et m_2 sont deux entiers tels que $m_1 \leqslant m_2$, on désigne par $[\![m_1, m_2]\!]$ l'ensemble des entiers k tels que $m_1 \leqslant k \leqslant m_2$.
Si a, b et n sont trois entiers, on note $a = b$ (modulo n) lorsque a et b sont congrus modulo n, c'est-à-dire lorsque $b - a$ est multiple de n.
Dans tout cet exercice, p désigne un nombre premier.

I- Définition du logarithme discret

Pour tout $A \in \mathbb{N}$, on note (A mod p) le reste de la division euclidienne de A par p. C'est l'unique entier de $[\![0, p-1]\!]$ congru à A modulo p.
Un entier $x \in [\![1, p-1]\!]$ est appelé une racine primitive modulo p lorsque l'ensemble des $\left(x^k \bmod p\right)$ pour $k \in \mathbb{N}$ est l'ensemble $[\![1, p-1]\!]$, c'est-à-dire lorsque les puissances de x, calculées modulo p, décrivent $[\![1, p-1]\!]$ tout entier.

Ainsi pour $p = 5$:
- 1 n'est pas racine primitive modulo 5 puisque ses puissances valent toujours 1.
- 2 est racine primitive modulo 5 puisque :
  $\left(2^0 \bmod 5\right) = 1$, $\left(2^1 \bmod 5\right) = 2$, $\left(2^2 \bmod 5\right) = 4$, $\left(2^3 \bmod 5\right) = 3$.
- 3 est racine primitive modulo 5 puisque :
  $\left(3^0 \bmod 5\right) = 1$, $\left(3^1 \bmod 5\right) = 3$, $\left(3^2 \bmod 5\right) = 4$, $\left(3^3 \bmod 5\right) = 2$.

- 4 n'est pas racine primitive modulo 5 puisque $\big(4^k \bmod 5\big)$, $k \in \mathbb{N}$, vaut alternativement 1 ou 4.

1. On prend dans cette question $p = 7$. Déterminer les racines primitives modulo 7.

On admet désormais que, quel que soit le nombre premier p, il existe au moins une racine primitive modulo p. Dans la suite, on désigne par g une racine primitive modulo p.

2. (a) Montrer que l'ensemble des $\big(g^k \bmod p\big)$ 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 $\big(g^b \bmod p\big)$.

3. Une solution élémentaire pour déterminer $\ell(A)$ consiste à calculer les entiers $\big(g^k \bmod p\big)$, pour $k = 0, 1, \ldots$, 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 toute la suite de cette partie, des nombres premiers distincts $p_1, \ldots, p_n$ strictement inférieurs à p et des entiers $a_1, \ldots, a_n$ tels que, pour tout $i \in [\![1, n]\!]$, les facteurs premiers de $(g^{a_i} \bmod p)$ appartiennent à $\{p_1, \ldots, p_n\}$.
Pour chaque $i \in [\![1, n]\!]$, on a ainsi une relation $(g^{a_i} \bmod p) = p_1^{e_{i,1}} p_2^{e_{i,2}} \cdots p_n^{e_{i,n}}$ où les $e_{i,j}$, pour $(i, j) \in [\![1, n]\!]^2$, sont des entiers naturels.

2. Montrer que, pour tout $i \in [\![1, n]\!]$:
$$a_i = e_{i,1}\ell(p_1) + e_{i,2}\ell(p_2) + \cdots + e_{i,n}\ell(p_n) \ \text{(modulo } (p-1)).$$

3. On prend dans cette question $p = 53$, $g = 20$, $n = 2$, $p_1 = 2$, $p_2 = 5$.
   (a) À 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-ils s'écrire sous la forme $2^\alpha 5^\beta$, avec α et β 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 supppose connu $s \in \mathbb{N}$ tel que $(g^s A \bmod p)$ se factorise à l'aide de $p_1, \ldots, p_n$ uniquement. Si on suppose connus $\ell(p_1), \ldots, \ell(p_n)$, 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 :
$$\frac{(\ln(p-1))^2}{2(p-1)(\ln p_1)(\ln p_2)} \leqslant P \leqslant \frac{1}{p-1}\left(\frac{\ln(p-1)}{\ln p_1} + 1\right)\left(\frac{\ln(p-1)}{\ln p_2} + 1\right).$$
   (d) Généraliser le résultat au cas de n nombres premiers $p_1, \ldots, p_n$.
