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

Pour le 10/09/2018

DM n° 1 : Révisions et logique

Le problème 3 est facultatif

Problème 1 – (Extrait de : *Le livre qui rend fou* de Raymond Smullyan)
Un roi cherche à vider ses cachots de ses ennemis prisonniers. Comme il ne veut pas les tuer purement et simplement, il leur laisse une chance : chaque prisonnier aura à choisir entre deux portes. Derrière chaque porte se trouve un cachot contenant soit une princesse, soit un tigre. Si le prisonnier ouvre la porte d'une princesse, il ira filer le parfait amour avec elle, s'il ouvre la porte d'un tigre, il se fera dévorer. D'autre part, les deux cellules peuvent contenir un tigre, de même que les deux cellules peuvent contenir une princesse. Enfin, comme le roi n'aime pas le hasard bête et méchant, il met des affiches sur chaque porte, censées aider le prisonnier. Ces affiches peuvent être vraies ou fausses. Le roi peut donner des indications sur la véracité de ces affiches. Aider le prisonnier à s'en sortir. Pour chaque situation, on présentera d'abord une explication intuitive, en s'efforçant à produire une rédaction claire, concise et limpide, puis une démonstration formelle résultant de manipulations logiques sur des formules traduisant les différentes informations. On pourra appeler 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 exemple, dans l'exemple 1, si la deuxième affiche est vraie, on obtient la formule logique $(P_1 \wedge T_2) \vee (T_1 \wedge P_2)$.

1. **Premier prisonnier** : une seule des deux affiches est vraie, mais on ne sait pas laquelle :
   Porte 1 : Il y a une princesse dans cette cellule, et un tigre dans l'autre.
   Porte 2 : Il y a une princesse dans une cellule et un tigre dans une cellule.
2. **Deuxième prisonnier** : les affiches sont soit toutes les deux vraies, soit toutes les deux fausses.
   Porte 1 : Une au moins des deux cellules contient une princesse.
   Porte 2 : Il y a un tigre dans l'autre cellule.
3. **Troisième prisonnier** : mêmes règles.
   Porte 1 : Il y a un tigre dans cette cellule ou il y a une princesse dans l'autre.
   Porte 2 : Il y a une princesse dans l'autre cellule.
4. **Quatrième prisonnier** : sur la porte 1, l'affiche est vraie si la cellule contient une princesse, et fausse si la cellule contient un tigre ; sur la porte 2, c'est l'inverse.
   Porte 1 : Les deux cellules contiennent des princesses.
   Porte 2 : Les deux cellules contiennent des princesses.
5. **Cinquième prisonnier** : mêmes règles.
   Porte 1 : Choisis n'importe quelle cellule, ça n'a pas d'importance.
   Porte 2 : Il y a une princesse dans l'autre cellule.
6. **Sixième prisonnier** : mêmes règles.
   Porte 1 : Choisis bien ta cellule, ça a de l'importance.
   Porte 2 : Tu ferais mieux de choisir l'autre cellule !

On peut trouver d'autres énigmes de ce type faisant intervenir plus de deux portes dans le livre de Smullyan, ainsi que des énigmes sur d'autres thèmes. Du même auteur, on pourra consulter également Quel est le titre de ce livre ?

Problème 2 – **(d'après Bac des années 90)**
L'objet du problème est l'étude de quelques propriétés de la fonction f définie sur $\mathbb{R}$ par :

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

Partie I –

Dans cette partie, on cherche à représenter f.

1. (a) Déterminer une fonction g telle que pour tout $x \in \mathbb{R}$,

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

   (b) Étudier les variations de f sur $[0, 2\pi]$, et préciser les tangentes en 0 et 2π.

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) Quels sont les points d'intersection des deux courbes C et C_1 ? Comparer les tangentes aux deux courbes en ces points.

   (b) Même question pour C et C_2.

   (c) Donner l'allure, sur un même graphe, des courbes C, C_1 et C_2 (pour une meilleure clarté, il conviendra de bien choisir ses unités, le repère n'étant pas nécessairement choisi orthonormal).

   (d) Soit Φ l'application de $\mathbb{R}^2$ dans $\mathbb{R}^2$ définie par :

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

   Déterminer l'image de C par Φ, c'est-à-dire :

$$\{\Phi(x, y) \mid (x, y) \in C\}.$$

Partie II –

Dans cette partie, on étudie une primitive de f.

1. Exprimer une relation entre f, f' et f''.

2. En déduire une primitive de f, puis l'expression, pour tout $x \in \mathbb{R}$, de

$$F(x) = \int_0^x \mathrm{e}^{-t}\sin(t)\ \mathrm{d}t$$

   En déduire l'existence et la valeur de l'intégrale « impropre »

$$\int_0^{+\infty} \mathrm{e}^{-t}\sin(t)\ \mathrm{d}t = \lim_{x\to+\infty} \int_0^x \mathrm{e}^{-t}\sin(t)\ \mathrm{d}t.$$

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) Étudier la limite de (S_n).

   (b) Étudier le signe de $(B_k)_{k\in\mathbb{N}}$ et les variations de la suite $(|B_k|)_{k\in\mathbb{N}}$.

   (c) Justifier que pour tout $n \in \mathbb{N}$,

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

   En déduire un entier n tel que S_n est une valeur approchée de $\displaystyle\int_0^{+\infty} \mathrm{e}^{-t}\sin(t)\ \mathrm{d}t$ à 10^{-10} près.

4. Justifier que (T_n) admet une limite en $+\infty$.

5. En notant S et T les limites de (S_n) et (T_n) respectivement, montrer que :

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

Partie III –

Soit $a < b$ deux réels. Soit f_1 et f_2 deux fonctions de $[a,b]$ dans $\mathbb{R}$, et f la fonction de $[a,b]$ dans $\mathbb{C}$ définie par $f = f_1 + \mathrm{i}\, f_2$. Si f_1 et f_2 sont continues, on définit l'intégrale de f par :

$$\int_a^b f(t)\ \mathrm{d}t = \int_a^b f_1(t)\ \mathrm{d}t + \mathrm{i}\int_a^b f_2(t)\ \mathrm{d}t.$$

Si f_1 et f_2 sont dérivables, on définit la dérivée de f par :

$$\forall t \in [a,b],\quad f'(t) = f_1(t) + \mathrm{i}\, f_2(t).$$

On rappelle que pour tout $\theta \in \mathbb{R}$,

$$\mathrm{e}^{\mathrm{i}\,\theta} = \cos(\theta) + \mathrm{i}\sin(\theta).$$

On pose alors, pour tout $z = a + \mathrm{i}\, b$ dans $\mathbb{C}$ (avec a, $b \in \mathbb{R}$), $\mathrm{e}^z = \mathrm{e}^a \mathrm{e}^{\mathrm{i}\, b}$, et on rappelle, ou admet, que pour tout z, z' dans $\mathbb{C}$,

$$\mathrm{e}^z \mathrm{e}^{z'} = \mathrm{e}^{z+z'}.$$

1. Soit $z = a + \mathrm{i}\, b$ comme plus haut. Exprimer e^z sous forme algébrique.
2. Soit $c \in \mathbb{C}$, et $f : t \mapsto \mathrm{e}^{ct}$. Exprimer la dérivée f'. Que dire d'une primitive de f ?
3. Retrouver, grâce à ces considérations, une expression d'une primitive de $t \mapsto \mathrm{e}^{-t}\sin(t)$, ainsi que de $t \mapsto \mathrm{e}^{-t}\cos(t)$.
4. Calculer sur la même méthode les intégrales :

$$\int_0^\pi \mathrm{e}^{\cos(t)}\cos(t + \sin(t))\ \mathrm{d}t \qquad \text{et} \qquad \int_0^\pi \mathrm{e}^{\cos(t)}\sin(t + \sin(t))\ \mathrm{d}t.$$

Problème 3 – Logarithme discret, méthode d'Adleman (d'après CG)

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 $a \equiv b\ [n]$ lorsque a et b sont congrus modulo n, c'est-à-dire lorsque $b - a$ est un multiple de n.
Dans tout le problème, p désigne un nombre premier.

Partie 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 $(x^k \mod p)$ 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 :*

$$(2^0 \mod 5) = 1,\quad (2^1 \mod 5) = 2,\quad (2^2 \mod 5) = 4,\quad (2^3 \mod 5) = 3.$$

- *3 est racine primitive modulo 5 puisque :*

$$(3^0 \mod 5) = 1,\quad (3^1 \mod 5) = 3,\quad (3^2 \mod 5) = 4,\quad (3^3 \mod 5) = 2.$$

- *4 n'est pas racine primitive modulo 5 puisque $(4^k \mod 5)$, $k \in \mathbb{N}$, 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 $(g^k \mod p)$, 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 $A = (g^a \mod p)$. *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 $(g^b \mod p)$.

3. Décrire un algorithme élémentaire permettant le calcul de $\ell(A)$.

Partie 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 $p = 113$, on admet que $g = 55$ est une racine primitive modulo p. On donne $\ell(2) = 60$ et $\ell(3) = 5$. Trouver $\ell(54)$.

On suppose choisis, pour 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 $(g^{a_i} \mod p)$ appartiennent à $\{p_1, \ldots, p_n\}$. Pour chaque $i \in [\![1, n]\!]$, on a ainsi une relation $(g^{a_i} \mod p) = p_1^{e_{i,1}} p_2^{e_{i,2}}, \ldots, p_n^{e_{i,n}}$, 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 $p = 53$, $g = 20$ (racine primitive admise), $n = 2$, $p_1 = 2$, $p_2 = 5$.

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

   (b) On suppose connu $s \in \mathbb{N}$ tel que $(g^s A \mod p)$ 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 $(g^s A \mod p)$ soit une puissance de p_1.

   (c) Montrer que la probabilité P pour qu'un entier $s \in [\![0, p-2]\!]$ soit tel que $(g^s A \mod p)$ 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 de la question précédente au cas de n nombres premiers $p_1, \ldots, p_n$.