

DM n° 1 : Révisions et logique

Problème 1 – (d’après Bac C 1990)

On considère la fonction f définie sur $[0, 1]$ par :

$$f(0) = 0, \quad f(1) = 1 \quad \text{et} \quad f(t) = \frac{t-1}{\ln(t)} \text{ si } t \in]0, 1[.$$

On appelle \mathcal{C} la courbe représentative de f dans un repère orthonormé $(0, \vec{i}, \vec{j})$. Le but du problème est d’étudier f et de calculer $I = \int_0^1 f(t) \, dt$.

Question préliminaire

En revenant à la définition de la dérivabilité, et sans utiliser le théorème de dérivation des composées, exprimer la dérivée en x_0 de $g : x \mapsto f(ax + b)$ en fonction de $f'(ax_0 + b)$, sous l’hypothèse adéquate de dérivabilité de f . Établir une règle similaire pour la dérivation de $x \mapsto f(x^2)$.

Partie I – Étude de f

1. (a) Montrer que f est continue en 0 et en 1.
(b) Montrer que f est dérivable sur $]0, 1[$.
(c) Étudier le signe de f' sur $]0, 1[$ (on pourra introduire et étudier une fonction auxiliaire bien choisie).
(d) Étudier la dérivabilité et la tangente en 0.
2. (a) Prouver que pour tout $u \in [0, \frac{1}{2}]$,

$$0 \leq -\ln(1-u) - \left(u + \frac{u^2}{2}\right) \leq \frac{2u^3}{3}.$$

- (b) En déduire la dérivabilité en 1 de $g : x \mapsto \frac{1}{f(x)}$, et déterminer $g'(1)$.
 - (c) Montrer que f est dérivable en 1 et calculer $f'(1)$. Déterminer l’équation de la tangente en 1 à la courbe \mathcal{C} .
 - (d) Déterminer la position de la tangente en 1 par rapport à la courbe \mathcal{C} au voisinage du point 1.
3. À l’aide des informations précédentes, et sans calculer d’autre valeur, tracer l’allure de la courbe \mathcal{C} .

Partie II – Calcul de l’intégrale I

Pour tout élément x de $]0, 1]$, on pose

$$I(x) = \int_x^1 f(t) \, dt \quad \text{et} \quad J(x) = \int_x^1 \frac{f(t)}{t} \, dt.$$

On ne cherchera pas à calculer ces intégrales.

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

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

- (a) Montrer que K est dérivable sur $]0, 1]$ et que

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

(b) En réexprimant $x \mapsto f(x) - 2f(x^2)$, en déduire que

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

2. Calculer, pour tout $x \in]0, 1[$, l'intégrale $\int_{x^2}^x \frac{-1}{t \ln(t)} dt$.

3. Montrer que pour tout $x \in]0, 1[$,

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

4. En déduire la limite lorsque x tend vers 0 de $I(x)$.

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

Problème 2 – Logarithme discret, méthode d'Adleman (d'après CG)

Si m_1 et m_2 sont deux entiers tels que $m_1 \leq m_2$, on désigne par $\llbracket m_1, m_2 \rrbracket$ l'ensemble des entiers k tels que $m_1 \leq k \leq m_2$.

Si a , b et n sont trois entiers, on note $a \equiv b \pmod{n}$ 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 $(A \bmod p)$ le reste de la division euclidienne de A par p . C'est l'unique entier de $\llbracket 0, p-1 \rrbracket$ congru à A modulo p .

Un entier $x \in \llbracket 1, p-1 \rrbracket$ est appelé une racine primitive modulo p lorsque l'ensemble des $(x^k \bmod p)$ pour $k \in \mathbb{N}$ est l'ensemble $\llbracket 1, p-1 \rrbracket$, c'est-à-dire lorsque les puissances de x , calculées modulo p , décrivent $\llbracket 1, p-1 \rrbracket$ 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 :

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

- 3 est racine primitive modulo 5 puisque :

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

- 4 n'est pas racine primitive modulo 5 puisque $(4^k \bmod 5)$, $k \in \mathbb{N}$, 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 $(g^k \bmod p)$, pour $k \in \llbracket 0, p-2 \rrbracket$, est $\llbracket 1, p-1 \rrbracket$.

(b) Soit $A \in \llbracket 1, p-1 \rrbracket$. Justifier l'existence et l'unicité d'un entier $a \in \llbracket 0, p-2 \rrbracket$ 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. 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, \dots, p_n strictement inférieurs à p et des entiers a_1, \dots, a_n tels que, pour tout $i \in \llbracket 1, n \rrbracket$, les facteurs premiers de $(g^{a_i} \bmod p)$ appartiennent à $\{p_1, \dots, p_n\}$. Pour chaque $i \in \llbracket 1, n \rrbracket$, 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 $(i, j) \in \llbracket 1, n \rrbracket^2$, sont des entiers naturels.

2. Montrer que, pour tout $i \in \llbracket 1, n \rrbracket$:

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

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

(a) À l'aide de g et g^3 , déterminer $\ell(2)$ et $\ell(5)$.

(b) En déduire $\ell(40)$.

(c) Combien d'entiers de $\llbracket 1, 52 \rrbracket$ peuvent-ils s'écrire sous la forme $2^\alpha 5^\beta$, avec α et β , entiers naturels ?

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

(a) Montrer que : $\{(g^s A \bmod p) \mid s \in \llbracket 0, p-2 \rrbracket\} = \llbracket 1, p-1 \rrbracket$.

(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 $\llbracket 1, p-1 \rrbracket$ qui sont une puissance de p_1 ?

(b) En déduire la probabilité pour qu'un entier $s \in \llbracket 0, p-2 \rrbracket$ soit tel que $(g^s A \bmod p)$ soit une puissance de p_1 .

(c) Montrer que la probabilité P pour qu'un entier $s \in \llbracket 0, p-2 \rrbracket$ 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 de la question précédente au cas de n nombres premiers p_1, \dots, p_n .