MPSI 3 - Fermat Le 31.03.18
2017-2018

Devoir surveillé n°8

Durée de l'épreuve : 4 heures
La calculatrice est interdite

Le devoir est composé d'un exercice et d'un problème.
Lorsqu'une question est jugée, a priori, plus difficile, elle est précédée du symbole $(*)$ voire $(**)$.
La notation tiendra particulièrement compte de **la qualité de la rédaction, la précision des raisonnements et l'énoncé des formules utilisées**.

BON COURAGE

Exercice. Symbole de Zolotarev $\approx$ **90 min.**

On considère pour tout entier n, $E_n = \{1, 2, \dots n\}$ et S_n l'ensemble des permutation de E_n.
Pour toute permutation $\sigma \in S_n$, on note $\epsilon(\sigma)$ la signature de σ.
On note $E_n \uplus E_m = \{(1,i), i \in E_n\} \cup \{(2,j), j \in E_m\} = \{(1,1), (1,2), \dots (1,n), (2,1) \dots (2,m)\}$.
Dans la seconde question, on voit comment définir la signature d'une bijection d'un ensemble fini quelconque. Puis on exploite celle dans des cas particuliers de F_n afin de démontrer le théorème de réciprocité quadratique (dans un prochain devoir...).

1. Autour de la signature.
   (a) Donner, sans démonstration, trois façons de calculer la signature d'une permutation $\sigma \in S_n$.
   (b) Si σ est un cycle de longueur p, que vaut $\epsilon(\sigma)$?
2. Signature sur un ensemble fini quelconque.
   (a) On considère F_n de cardinal n et τ, une bijection de F_n sur lui-même.
   Pour toute bijection φ de E_n sur F_n on note $\tau_\varphi = \varphi^{-1} \circ \tau \circ \varphi$.
   Montrer que, pour toute bijection φ de E_n sur F_n, $\tau_\varphi \in S_n$.
   (b) Montrer que pour toutes bijections φ et ψ de E_n sur F_n, $\epsilon(\tau_\varphi) = \epsilon(\tau_\psi)$.

   > Ainsi, $\epsilon(\tau_\varphi)$ st indépendante de la fonction d'énumération φ choisie.
   > On la note donc $\epsilon(\tau)$, et on définit ainsi la signature de toute bijection d'un ensemble fini.
   > On démontrerait, sans difficulté, que pour toute bijection τ_1, τ_2 de F_n, $\epsilon(\tau_1 \circ \tau_2) = \epsilon(\tau_1) \times \epsilon(\tau_2)$.

   (c) On note, pour tout $x \in \mathbb{Z}$, $\overline{x}$, la classe de x pour la relation $\equiv [n]$.
   Soient $c_{+a} : \frac{\mathbb{Z}}{n\mathbb{Z}} \to \frac{\mathbb{Z}}{n\mathbb{Z}}$, $\overline{x} \mapsto \overline{x+a}$ et $\varphi : E_n \to \frac{\mathbb{Z}}{n\mathbb{Z}}$, $k \mapsto \overline{k}$.
   Montrer que $\varphi^{-1} \circ c_{+1} \circ \varphi$ est une permutation bien connue de E_n. Quelle est sa signature ?
   (d) Soit $k \in \mathbb{N}$ et $k \leqslant n$. Quelle relation simple existe-t-il entre les applications c_{+k} et c_{+1} ?
   En déduire que c_{+k} a une signature égale à $(-1)^{k(n-1)}$.
3. On note $\text{inv}_{n,m} : E_n \times E_m \to E_n \times E_m$ la permutation qui consiste à passer de l'ordre lexico-graphique de gauche à droite à l'ordre lexico-graphique de droite à gauche.
   Ainsi pour $n = 2, m = 3$, on a

$$\text{inv}_{2,3} = \begin{pmatrix} (1,1) & (1,2) & (1,3) & (2,1) & (2,2) & (2,3) \\ (1,1) & (2,1) & (1,2) & (2,2) & (1,3) & (2,3) \end{pmatrix}$$

   (a) Calculer la signature de $\text{inv}_{2,3}$
   (b) Ecrire $\text{inv}_{4,3}$ et calculer $\epsilon(\text{inv}_{4,3})$.
   (c) Montrer que pour tout $n, m \in \mathbb{N}$, $\epsilon(\text{inv}_{n,m}) = (-1)^{\frac{n(n-1)}{2}\frac{m(m-1)}{2}}$
4. Pour la suite de l'exercice, on suppose que <u>n est un nombre premier impair</u>.
   On considère m, non divisible par n et $v_m : \frac{\mathbb{Z}}{n\mathbb{Z}} \mapsto \frac{\mathbb{Z}}{n\mathbb{Z}}$, $\overline{h} \mapsto \overline{m \times h}$.
   (a) Montrer que v_m est une bijection de $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

   > On note $\left(\frac{m}{n}\right) = \epsilon(v_m)$, et on l'appelle cette notation le symbole de ZOLOTAREV.

   (b) Montrer que pour tout m, m', $\left(\frac{mm'}{n}\right) = \left(\frac{m}{n}\right)\left(\frac{m'}{n}\right)$

(c) On note p la longueur de l'orbite de 1 sous l'action de la bijection v_m (appelé *ordre* de 1). Montrer que $m^p \equiv 1[n]$, que $m^h \not\equiv 1[n]$ pour tout $h \in [\![1, p-1]\!]$.

(d) Montrer que v_m se décompose en un produit de $\frac{n-1}{p}$ cycles de longueur p et d'un point fixe. En déduire le petit théorème de Fermat, *au passage*.

(e) (*) Montrer que $\left(\frac{m}{n}\right) \equiv m^{\frac{n-1}{2}}\ [n]$

(f) (*) On dit que m est un *résidu quadratique modulo* n si il existe $r \in E_n$ tel que $r^2 \equiv m[n]$. Montrer que

$$\left(\frac{m}{n}\right) = \begin{cases} 1 & \text{si } m \text{ est un résidu quadratique modulo } n \\ -1 & \text{sinon} \end{cases}$$

La suite au DM 12

Problème. Compléter la suite logique : 1, 2, 16, 272...

Dans l'ensemble de ce problème, on admet le résultat suivant :

> Soit $(a_n)_{n\in\mathbb{N}}$, une suite de termes positifs et $\rho > 0$ tels que $\sum_{n\geqslant 0} a_n \rho^n$ converge
>
> Alors $f : x \mapsto \sum_{n=0}^{+\infty} a_n x^n$ est de classe $\mathcal{C}^\infty$ sur $]-\rho, \rho[$,
>
> et pour tout $k \in \mathbb{N}$, pour tout $x \in]-\rho, \rho[$, $f^{(k)}(x) = \sum_{m=0}^{+\infty} \frac{(m+k)!}{m!} a_{m+k} x^m$

Ce résultat servira en partie B et C.

A. Interprétation combinatoire et algorithme ≈ 60 min.

On dit que $\sigma \in S_m$ **est une permutation alternante** si

$$\forall\, i \in \mathbb{N}_{\lfloor \frac{m}{2} \rfloor}, \qquad \sigma(2i-1) < \sigma(2i) \text{ et } \sigma(2i) > \sigma(2i+1)$$

Par exemple, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix}$ est alternante car $1 < 3$, $3 > 2$, $2 < 5$, $5 > 4$.

En revanche, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix}$ n'est pas une permutation alternante : $\sigma(4) < \sigma(5)$.

Dans cette partie on considère un entier $n \in \mathbb{N}^*$ puis $m = 2n+1$. Enfin, on note T_n, le nombre de permutation alternante (impaire) de $S_{2n+1} = S_m$. Par convention, on choisit $T_0 = 1$.

1. Quelques cas particuliers
   (a) Montrer que $T_1 = 2$.
   (b) Montrer que $T_2 = 16$.
2. Relation de récurrence.
   (a) On considère une permutation alternante de S_m.
   Quelle position peut occuper le nombre $m = 2n+1$, maximum de l'ensemble ?
   Que peut-on des dire « des nombres placés à sa gauche » et « ceux à sa droite » ?
   (b) En déduire que $T_n = \sum_{k=0}^{n-1} \binom{2n}{2k+1} T_k \times T_{n-k-1}$
   (c) En exploitant cette relation de récurrence, vérifier que $T_2 = 16$.
   Que vaut T_3 ?
3. Triangle d'Euler-Bernoulli (de Kempner ?). Construction.
   On construit, par récurrence, un triangle de nombres de la façon suivante :
   1/ la première ligne (notée ligne 0) est un 1
   2/ les lignes 0 à $i-1$ étant obtenues,
   — si i est pair, on commence à gauche par un zéro ; puis de gauche à droite,
   on additionne le terme de gauche avec celui du dessus afin d'obtenir celui de droite...
   — si i est impair, on commence à droite par un zéro ; puis de droite à gauche,
   on additionne le terme de droite avec celui du dessus afin d'obtenir celui de gauche...

Les quatre premières lignes sont donc les suivantes :

$$\begin{array}{c|ccccccc|c|}
\ell_0 & & & & 1 & & & & \\
\ell_1 & & & 1 & & 0 & & & \leftarrow \\
\ell_2 & & 0 & & 1 & & 1 & & \rightarrow \\
\ell_3 & 2 & & 2 & & 1 & & 0 & \leftarrow
\end{array}$$

(a) Compléter le triangle jusqu'à la ligne ℓ_7. Celle-ci se termine par : $\ldots 122\ \ 61\ \ 0$

(b) Pour $k, r \in \mathbb{N}$, avec $0 \leqslant k \leqslant r$, on note $\left\langle \begin{array}{c} r \\ k \end{array} \right\rangle$, le $(k+1)^{\text{e}}$ nombre obtenu en ligne ℓ_r.

Ainsi $\left\langle \begin{array}{c} 3 \\ 0 \end{array} \right\rangle = 2$ et $\left\langle \begin{array}{c} 2 \\ 1 \end{array} \right\rangle = 1$.

Quelle relation observe-t-on entre T_0, T_1, T_2 et T_3 respectivement et des nombres $\left\langle \begin{array}{c} r \\ 0 \end{array} \right\rangle$?

4. Triangle d'Euler-Bernoulli (de Kempner ?). Relations combinatoires.
   (a) Quelle relation lie, par construction, les nombres $\left\langle \begin{array}{c} r+1 \\ k \end{array} \right\rangle$, $\left\langle \begin{array}{c} r+1 \\ k+1 \end{array} \right\rangle$ et $\left\langle \begin{array}{c} r \\ k \end{array} \right\rangle$?
   On fera attention à la parité de r et on exploitera le nombre $(-1)^r$.
   (b) On note $P_{r,k}$, le nombre de permutation alternantes de S_r telle que $\sigma(r) = k$.
   Attention, dans ce cas, r peut être pair ou impair !
   Exprimer T_n en fonction des $P_{2n+1,k}$.
   (c) On suppose que r est pair. Que vaut $P_{r,1}$?
   Montrer que, pour tout $k \in [\![1, n-1]\!]$: $P_{r,k+1} = P_{r,k} + P_{r-1,k}$.
   (d) On suppose que r est impair. Que vaut $P_{r,r}$?
   Montrer que, pour tout $k \in [\![1, n-1]\!]$: $P_{r,k} = P_{r,k+1} + P_{r-1,k}$.
   (e) En déduire, que pour tout entiers non nuls r et k tels que $k \leqslant r$,
   $$P_{r,k} = \left\langle \begin{array}{c} r-1 \\ r-k \end{array} \right\rangle$$
   (f) Vérifier alors que $T_n = \left\langle \begin{array}{c} m \\ 0 \end{array} \right\rangle$ où $m = 2n+1$

B. Série $\displaystyle\sum_{n \geqslant 0} \frac{T_n}{(2n+1)!} x^{2n+1}$ **≈ 40 min.**

On note $P_n(x)$, la polynôme $\displaystyle\sum_{k=0}^{n} \frac{T_k}{(2k+1)!} x^{2k+1}$.

On rappelle que la suite (T_n) vérifie la relation : $T_n = \displaystyle\sum_{k=0}^{n-1} \binom{2n}{2k+1} T_k \times T_{n-k-1}$.

1. Calculer, pour tout $x \in \mathbb{R}$, $P_n'(x)$ et $P_n^2(x)$.
   Montrer que $\forall\, x \in \mathbb{R}$, $P_n'(x) \leqslant 1 + P_n^2(x) \leqslant P_{2n+1}'(x)$
2. Montrer, par récurrence, que pour tout $n \in \mathbb{N}$, $0 \leqslant T_n \leqslant (2n+1)!$.
3. On considère $\rho \in]-1, 1[$. Montrer que la série $\sum_{n \geqslant 0} \frac{T_n}{(2n+1)!} \rho^{2n+1}$ est convergente.
   On note $T(\rho)$ sa limite.
4. Montrer que $T(0) = 0$.
5. Montrer que T est de classe $\mathcal{C}^\infty$ sur $]-1, 1[$ et que pour tout $x \in]-1, 1[$, $T'(x) = 1 + T^2(x)$.
6. Déduire des deux questions précédentes la valeur de $\displaystyle\sum_{n=0}^{+\infty} \frac{T_n}{(2n+1)!} x^{2n+1}$ à l'aide d'une fonction usuelle.

C. Calcul (originale) de $\displaystyle\sum_{k=1}^{+\infty} \frac{1}{k^s}$ **≈ 50 min.**

On note pour tout $s > 1$, $\zeta(s) = \displaystyle\sum_{n=1}^{+\infty} \frac{1}{n^s}$.

1. Convergence.
   Expliquer pourquoi $\zeta(s)$ est bien défini.

2. Expression de $\zeta(2s)$ en fonction de T_n

   (a) On note $I(s) = \displaystyle\sum_{k=0}^{+\infty} \frac{1}{(2k+1)^s}$.

   Montrer que pour tout $s > 1$, $I(s) = \dfrac{2^s - 1}{2^s}\zeta(s)$

   (b) Justifier « *à la Euler* » que

$$\forall\, x \in \mathbb{R}, \tan(x) = \sum_{k=0}^{+\infty} \frac{8x}{(2k+1)^2\pi^2 - 4x^2}$$

   On supposera (ademttra) que $\tan(x)$ *est une fraction rationnelle qui se décompose en éléments simples...*

   (c) Montrer alors que

$$\forall\, x \in]-\frac{\pi}{2}, \frac{\pi}{2}[, \qquad \tan(x) = 8x \sum_{k=0}^{+\infty} \left(\frac{1}{(2k+1)^2\pi^2} \sum_{n=0}^{+\infty} \left(\frac{2x}{(2k+1)\pi} \right)^{2n} \right)$$

   (d) Dans **ce** cas de double somme, on a : $\displaystyle\sum_{k=0}^{+\infty}\sum_{n=0}^{+\infty} a_{k,n} = \sum_{n=0}^{+\infty}\sum_{k=0}^{+\infty} a_{k,n}$.

   En déduire

$$\forall\, x \in]-\frac{\pi}{2}, \frac{\pi}{2}[, \qquad \tan(x) = \sum_{n=0}^{+\infty} 2 \times (2^{2n+2} - 1) \times \zeta(2n+2) \times \frac{1}{\pi^{2n+2}} x^{2n+1}$$

   (e) Montrer, en exploitant le résultat admis en début de problème, que

   si $\tan(x) = \displaystyle\sum_{n=0}^{+\infty} a_n x^n$, alors $a_n = \frac{\tan^{(n)}(0)}{n!}$.

   En déduire que pour tout $n \in \mathbb{N}$,

$$\zeta(2n+2) = \frac{T_n \times \pi^{2n+2}}{2(2^{2n+2} - 1)(2n+1)!}$$

   (f) Calculer $\zeta(2)$, $\zeta(4)$, $\zeta(6)$ et $\zeta(8)$.

3. Vitesse de convergence

   (a) Soit $s > 1$. Donner le développement limité à l'ordre 1 de $\dfrac{1}{n^{s-1}} - \dfrac{1}{(n+1)^{s-1}}$ pour $n \to +\infty$.

   (b) En déduire que :

$$\forall\, \epsilon > 0, \exists\, N \in \mathbb{N} \text{ tel que } \forall\, n \geqslant N, (1-\epsilon)\frac{s-1}{n^s} \leqslant \frac{1}{n^{s-1}} - \frac{1}{(n+1)^{s-1}} \leqslant (1+\epsilon)\frac{s-1}{n^s}$$

   (c) Montrer alors que

$$\zeta(s) - \sum_{n=1}^{m-1} \frac{1}{n^s} = \sum_{n=m}^{+\infty} \frac{1}{n^s} \underset{m \to +\infty}{\sim} \frac{1}{(s-1)m^{s-1}}$$

4. Ecrire un programme informatique qui calcule $\zeta(s)$ à ϵ près (donné en argument)