

DM6 - Évaluations asymptotiques en arithmétique et sur les permutations

L. TINTINAGLIA

Le problème comporte deux parties qui sont indépendantes.

Notations

On note \mathbb{N} l'ensemble des entiers naturels et \mathbb{N}^* l'ensemble des entiers naturels non nuls.

Soit n un entier naturel non nul. On note \mathfrak{S}_n le groupe des permutations de $\{1, \dots, n\}$ et $\varepsilon(\sigma)$ la signature d'une permutation $\sigma \in \mathfrak{S}_n$.

Si $\sigma \in \mathfrak{S}_n$, on appelle point fixe de σ un élément $i \in \{1, \dots, n\}$ tel que $\sigma(i) = i$. On note $\nu(\sigma)$ le nombre de points fixes de σ . On appelle dérangement une permutation $\sigma \in \mathfrak{S}_n$ n'ayant aucun point fixe. On note \mathfrak{D}_n l'ensemble des dérangements de \mathfrak{S}_n et D_n son cardinal.

Si k est un entier naturel tel que $k \leq n$, on note $\binom{n}{k}$ le coefficient binomial correspondant au nombre de parties à k éléments d'un ensemble à n éléments. Par convention, on pose $\binom{n}{k} = 0$ pour un entier naturel $k > n$.

On note $\mathbb{R}[X]$ l'ensemble des polynômes à une indéterminée et à coefficients réels. Si de plus $n \geq 0$ est un entier naturel, on note $\mathbb{R}_n[X]$ l'ensemble des éléments $P \in \mathbb{R}[X]$ de degré inférieur ou égal à n .

Si $n \geq 0$ et $d \geq 1$ sont deux entiers naturels, on note $d \mid n$ la relation « d divise n ».

Si x est un réel, on note $E(x)$ sa partie entière, c'est-à-dire l'unique entier $E(x)$ tel que $E(x) \leq x < E(x) + 1$.

Si p est un nombre premier et n un entier naturel non nul, on note

$$\nu_p(n) = \max \{ \nu \in \mathbb{N} : p^\nu \mid n \}$$

Soit n un entier naturel non nul. On note $\mathcal{M}_n(\mathbb{R})$ l'ensemble des matrices carrées de taille n à coefficients réels.

Pour tout ensemble E , on note $\mathcal{P}(E)$ l'ensemble des parties de E .

On note \ln_2 la fonction de $]1, +\infty[$ dans \mathbb{R} définie par $\ln_2(x) = \ln(\ln(x))$.

Si $(a_n)_{n \in \mathbb{N}}$ désigne une suite de nombres réels, on note, pour tout nombre réel $x \in \mathbb{R}$,

$$\sum_{n \leq x} a_n = \sum_{n=1}^{E(x)} a_n, \quad \sum_{\substack{p \leq x \\ p \text{ premier}}} a_p = \sum_{p=1}^{E(x)} a_p, \quad \prod_{\substack{p \leq x \\ p \text{ premier}}} a_p = \prod_{p=1}^{E(x)} a_p$$

avec la convention que la somme indexée par l'ensemble vide vaut 0 et le produit indexé par l'ensemble vide vaut 1.

On pourra utiliser sans démonstration le fait qu'il existe un réel γ tel que

$$\sum_{k=1}^n \frac{1}{k} \underset{n \rightarrow +\infty}{=} \ln(n) + \gamma + O\left(\frac{1}{n}\right)$$

Première partie

Soit un entier naturel $n \geq 2$. Pour tout nombre réel x , on considère la matrice de $\mathcal{M}_n(\mathbb{R})$ suivante

$$M_x = \begin{pmatrix} x & 1 & \cdots & 1 & 1 \\ 1 & x & \cdots & 1 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & \cdots & x & 1 \\ 1 & 1 & \cdots & 1 & x \end{pmatrix}$$

1a. Montrer que la matrice $-M_0$ est diagonalisable et déterminer ses valeurs propres et ses sous-espaces propres.

1b. En déduire que pour tout $x \in \mathbb{R}$, on a

$$\sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) x^{\nu(\sigma)} = (x-1)^{n-1} (x+n-1)$$

2. Calculer

$$\sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma), \quad \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \nu(\sigma) \text{ et } \sum_{\sigma \in \mathfrak{S}_n} \frac{\varepsilon(\sigma)}{\nu(\sigma) + 1}$$

3. Établir que

$$\text{Card} \{ \sigma \in \mathfrak{S}_n : \varepsilon(\sigma) = 1 \} = \text{Card} \{ \sigma \in \mathfrak{S}_n : \varepsilon(\sigma) = -1 \}$$

et en déduire la probabilité qu'une permutation de \mathfrak{S}_n tirée uniformément au hasard soit de signature prescrite.

4. Pour $\sigma \in \mathfrak{S}_n$, préciser à quelle condition sur $\nu(\sigma)$, on a $\sigma \in \mathfrak{D}_n$. En déduire que

$$\text{Card} \{ \sigma \in \mathfrak{D}_n : \varepsilon(\sigma) = 1 \} = \text{Card} \{ \sigma \in \mathfrak{D}_n : \varepsilon(\sigma) = -1 \} + (-1)^{n-1} (n-1)$$

Soit $m \in \mathbb{N}$. On considère la matrice

$$M = \begin{pmatrix} \binom{0}{0} & 0 & \cdots & \cdots & \cdots & 0 \\ \binom{1}{0} & \binom{1}{1} & 0 & & & \vdots \\ \vdots & & \ddots & \ddots & & \vdots \\ \vdots & & & \ddots & \ddots & \vdots \\ \binom{m-1}{0} & & & & \binom{m-1}{m-1} & 0 \\ \binom{m}{0} & \cdots & \cdots & \cdots & \cdots & \binom{m}{m} \end{pmatrix} \in \mathcal{M}_{m+1}(\mathbb{R})$$

5a. Justifier que les familles $(1, X, \dots, X^m)$ et $(1, (X - 1), \dots, (X - 1)^m)$ sont des bases de $\mathbb{R}_m[X]$.

5b. Montrer que la transposée de M est la matrice de l'application linéaire identité

$$\begin{array}{ccc} \mathbb{R}_m[X] & \longrightarrow & \mathbb{R}_m[X] \\ P & \longmapsto & P \end{array}$$

dans les bases $(1, X, \dots, X^m)$ au départ et $(1, (X - 1), \dots, (X - 1)^m)$ à l'arrivée.

5c. Établir que M est inversible et expliciter son inverse.

5d. En déduire que pour tous $(u_0, \dots, u_m), (v_0, \dots, v_m) \in \mathbb{R}^{m+1}$,

$$\text{si } \forall k \leq m, \quad u_k = \sum_{\ell=0}^k \binom{k}{\ell} v_\ell, \quad \text{alors } \forall k \leq m, \quad v_k = \sum_{\ell=0}^k (-1)^{k-\ell} \binom{k}{\ell} u_\ell$$

6. Montrer que pour tout entier naturel n non nul,

$$D_n = n! \sum_{k=0}^n \frac{(-1)^k}{k!}$$

Pour n un entier naturel supérieur ou égal à 2, on considère l'espace probabilisé $(\mathfrak{D}_n, \mathcal{P}(\mathfrak{D}_n))$ muni de la probabilité uniforme. On définit une variable aléatoire Y_n par $Y_n(\sigma) = \varepsilon(\sigma)$.

7a. Expliciter la loi de Y_n .

7b. Calculer, pour tout $\varepsilon \in \{-1, 1\}$, $\lim_{n \rightarrow +\infty} \mathbb{P}(Y_n = \varepsilon)$.

Pour n un entier naturel supérieur ou égal à 2, on considère l'espace probabilisé $(\mathfrak{S}_n, \mathcal{P}(\mathfrak{S}_n))$ muni de la probabilité uniforme. On définit une variable aléatoire Z_n par $Z_n(\sigma) = \nu(\sigma)$.

8a. Expliciter la loi de Z_n .

8b. Calculer, pour tout entier naturel $k \leq n$, $\lim_{n \rightarrow +\infty} \mathbb{P}(Z_n = k)$.

8c. Déterminer le nombre moyen de points fixes d'une permutation aléatoire ainsi que sa limite quand n tend vers $+\infty$.

Soit n un entier naturel non nul. Pour toute permutation $\sigma \in \mathfrak{S}_n$, on rappelle qu'il existe, à l'ordre près, une unique décomposition $\sigma = c_1 c_2 \cdots c_{\omega(\sigma)}$, où $\omega(\sigma) \in \mathbb{N}^*$ où $c_1, \dots, c_{\omega(\sigma)}$ sont des cycles à supports disjoints de longueurs respectives $\ell_1 \leq \ell_2 \leq \dots \leq \ell_{\omega(\sigma)}$ et $\ell_1 + \ell_2 + \dots + \ell_{\omega(\sigma)} = n$. En particulier, on prendra garde au fait que l'on prend ici en compte les cycles c_i de longueur 1, qui correspondent aux points fixes de σ , auquel cas c_i est l'identité.

Par exemple, si σ est la permutation identité de $\{1, \dots, n\}$, on a $\omega(\sigma) = n$ et $\ell_{\omega(\sigma)} = 1$. Et si σ est la permutation $(1, 2)$ de $\{1, 2, 3\}$, on a $\sigma = c_1 \circ c_2$ où c_1 est l'identité et $c_2 = (1, 2)$ de sorte que $\omega(\sigma) = 2$.

On obtient ainsi une application $\omega : \mathfrak{S}_n \rightarrow \mathbb{N}$. On se propose de montrer qu'en moyenne, $\omega(\sigma)$ est de l'ordre de $\ln(n)$ dans un sens que l'on précisera.

Pour un entier k inférieur ou égal à n , on note $s(n, k)$ le nombre de permutations de \mathfrak{S}_n telles que $\omega(\sigma) = k$. On considère alors, sur l'espace probabilisé $(\mathfrak{S}_n, \mathcal{P}(\mathfrak{S}_n))$ muni de la probabilité uniforme, la variable aléatoire X_n définie par $X_n(\sigma) = \omega(\sigma)$.

9. Calculer, pour $n \in \{2, 3, 4\}$, la quantité $\frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} \omega(\sigma)$.

10. Préciser $s(n, n)$ et $s(n, 1)$ puis montrer que, pour $2 \leq k \leq n - 1$, on a

$$s(n, k) = s(n - 1, k - 1) + (n - 1)s(n - 1, k)$$

Pour $\sigma \in \mathfrak{S}_n$, on pourra distinguer les cas $\sigma(1) = 1$ et $\sigma(1) \neq 1$.

11. Établir que, pour tout réel x , $\prod_{i=0}^{n-1} (x + i) = \sum_{k=1}^n s(n, k)x^k$.

12 Démontrer que $\mathbb{E}[X_n] \underset{n \rightarrow +\infty}{=} \ln(n) + \gamma + O\left(\frac{1}{n}\right)$.

13a. Montrer que

$$\frac{1}{n!} \sum_{k=1}^n k(k-1)s(n, k) = \sum_{i=1}^n \sum_{j=1}^n \frac{1}{ij} - \sum_{i=1}^n \frac{1}{i^2}$$

13b. En déduire que

$$\frac{1}{n!} \sum_{k=1}^n k^2 s(n, k) = \mathbb{E}[X_n] + \left(\sum_{i=1}^n \sum_{j=1}^n \frac{1}{ij} - \sum_{i=1}^n \frac{1}{i^2} \right)$$

14a. Montrer que

$$\frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} \omega(\sigma)^2 \underset{n \rightarrow +\infty}{=} (2\gamma + 1) \ln(n) + c + \ln(n)^2 + O\left(\frac{\ln(n)}{n}\right)$$

pour un réel c à préciser.

14b. Montrer que

$$\frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} (\omega(\sigma) - \ln(n))^2 \underset{n \rightarrow +\infty}{=} \ln(n) + c + O\left(\frac{\ln(n)}{n}\right)$$

15. Justifier qu'il existe un nombre réel $C > 0$ tel que, pour tout réel $\varepsilon > 0$ et tout entier $n \geq 1$, on a

$$\mathbb{P}(|X_n - \ln(n)| > \varepsilon \ln(n)) \leq \frac{C}{\varepsilon^2 \ln(n)}$$

Deuxième partie

Pour tout entier naturel n non nul, on pose

$$\omega(n) = \text{Card}\{p \text{ premier} : p \mid n\} = \sum_{\substack{p \mid n \\ p \text{ premier}}} 1$$

Par exemple, $\omega(6) = \omega(12) = 2$.

16. Soit $(a_n)_{n \geq 2}$ une suite de nombres réels. Pour $t \in \mathbb{R}$, on pose $A(t) = \sum_{2 \leq k \leq t} a_k$.

Soit $b : [2, +\infty[\rightarrow \mathbb{R}$ une fonction de classe \mathcal{C}^1 . Montrer que pour tout entier $n \geq 2$,

$$\sum_{k=2}^n a_k b(k) = A(n)b(n) - \int_2^n b'(t)A(t)dt$$

17. L'objectif de cette question est de démontrer que si n est un entier naturel non nul, alors

$$\prod_{\substack{p \leq n \\ p \text{ premier}}} p \leq 4^n.$$

17a. Traiter les cas $n \in \{1, 2, 3\}$.

On suppose à présent $n \geq 4$ et le résultat connu au rang k pour tout entier k compris entre 1 et $n - 1$.

17b. Établir le résultat au rang n si n est pair.

17c. Soit $n = 2m + 1$ avec $m \in \mathbb{N}$. Justifier que $\prod_{\substack{m+1 < p \leq 2m+1 \\ p \text{ premier}}} p$ divise $\binom{2m+1}{m}$ et montrer

$$\text{que } \binom{2m+1}{m} \leq 4^m.$$

17d. Conclure.

18. Soit n un entier naturel non nul et soit p un nombre premier. Justifier la formule $\nu_p(n!) = \sum_{k=1}^{+\infty} E\left(\frac{n}{p^k}\right)$ et montrer que

$$\frac{n}{p} - 1 < \nu_p(n!) \leq \frac{n}{p} + \frac{n}{p(p-1)}$$

19a. Par comparaison avec une intégrale, établir que

$$\sum_{k=1}^n \ln(k) \underset{n \rightarrow +\infty}{=} n \ln(n) - n + O(\ln(n))$$

19b. Justifier que $n! = \prod_{\substack{p \leq n \\ p \text{ premier}}} p^{\nu_p(n!)}$ et en déduire que

$$n \sum_{\substack{p \leq n \\ p \text{ premier}}} \frac{\ln(p)}{p} - n \ln(4) < \ln(n!) \leq n \sum_{\substack{p \leq n \\ p \text{ premier}}} \frac{\ln(p)}{p} + n \sum_{\substack{p \leq n \\ p \text{ premier}}} \frac{\ln(p)}{p(p-1)}$$

19c. Justifier que la série $\sum_{k \geq 2} \frac{\ln(k)}{k(k-1)}$ converge.

19d. Conclure que $\sum_{\substack{p \leq n \\ p \text{ premier}}} \frac{\ln(p)}{p} \underset{n \rightarrow +\infty}{=} \ln(n) + O(1)$.

20a. On pose, pour tout réel $t \geq 2$,

$$R(t) = \sum_{\substack{p \leq t \\ p \text{ premier}}} \frac{\ln(p)}{p} - \ln(t)$$

Montrer, en utilisant le résultat de la question 16, que

$$\sum_{\substack{p \leq n \\ p \text{ premier}}} \frac{1}{p} = 1 + \ln_2(n) - \ln_2(2) + \frac{R(n)}{\ln(n)} + \int_2^n \frac{R(t)}{t(\ln(t))^2} dt$$

20b. Justifier que la fonction $t \mapsto \frac{R(t)}{t(\ln(t))^2}$ est intégrable sur $[2, +\infty[$.

20c. Établir que $\sum_{\substack{p \leq n \\ p \text{ premier}}} \frac{1}{p} \underset{n \rightarrow +\infty}{=} \ln_2(n) + c_1 + O\left(\frac{1}{\ln(n)}\right)$, pour un réel $c_1 \in \mathbb{R}$ à préciser.

21a. Soient x un réel positif supérieur ou égal à 1 et $q \in \mathbb{N}^*$. Justifier que la quantité

$$\text{Card} \{n \in \mathbb{N} \cap [1, x] : n \equiv 0(\text{mod } q)\} - \frac{x}{q}$$

est bornée en valeur absolue par un réel indépendant de x et de q .

21b. Démontrer, à l'aide d'une interversion de sommes, que $\frac{1}{x} \sum_{n \leq x} \omega(n) \underset{x \rightarrow +\infty}{=} \ln_2(x) + O(1)$.

22a. Montrer que

$$\frac{1}{x} \sum_{n \leq x} (\omega(n) - \ln_2(x))^2 \underset{x \rightarrow +\infty}{=} \frac{1}{x} \left(\sum_{n \leq x} \omega(n)^2 \right) - \ln_2(x)^2 + O(\ln_2(x))$$

22b. Montrer que

$$\sum_{n \leq x} \omega(n)^2 = \sum_{\substack{p_1 \leq x \\ p_1 \text{ premier}}} \sum_{\substack{p_2 \leq x \\ p_2 \text{ premier}}} \text{Card} \{n \in \mathbb{N}^* : n \leq x, p_1 \mid n \text{ et } p_2 \mid n\}$$

22c. Montrer que

$$\left(\sum_{\substack{p_1, p_2 \leq x \\ p_1 \neq p_2 \text{ premiers}}} \text{Card} \{n \in \mathbb{N}^* : n \leq x, p_1 \mid n \text{ et } p_2 \mid n\} \right) - x \ln_2(x)^2 \underset{x \rightarrow +\infty}{=} O(x \ln_2(x))$$

On pourra estimer le cardinal de l'ensemble des paires de nombres premiers (p_1, p_2) tels que $p_1 p_2 \leq x$ quand x tend vers $+\infty$.

22d. Conclure que $\frac{1}{x} \left(\sum_{n \leq x} (\omega(n) - \ln_2(x))^2 \right) \underset{x \rightarrow +\infty}{=} O(\ln_2(x))$.

23. On pose $\mathcal{S} = \left\{ n \geq 3 : \left| \frac{\omega(n) - \ln_2(n)}{\sqrt{\ln_2(n)}} \right| \geq (\ln_2(n))^{1/4} \right\}$. Montrer que

$$\lim_{x \rightarrow +\infty} \frac{1}{x} \text{Card}\{n \leq x : n \in \mathcal{S}\} = 0$$

On pourra commencer par écrire $\text{Card}(\mathcal{S} \cap [1, x]) \underset{x \rightarrow +\infty}{=} \text{Card}(\mathcal{S} \cap [\sqrt{x}, x]) + O(\sqrt{x})$ et remarquer que dans la somme du membre de droite, la différence $|\ln_2(n) - \ln_2(x)|$ reste bornée.

On dit alors que l'ensemble \mathcal{S} a densité 0. De même que pour les permutations, on obtient que, en dehors d'un ensemble de densité nulle, $\omega(n) = \ln(\ln(n))(1 + o(1))$.