Agrégation Interne

Probabilités et théorie des nombres

– I – Fonction indicatrice d'Euler

Pour tout entier naturel $n \geq 2$, $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est l'anneau des classes résiduelles modulo n.

On note $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^* = \left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right) \setminus \{\overline{0}\}$ et $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$ est le groupe multiplicatif des éléments inversibles de l'anneau $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.

1. Soit a un entier relatif. Montrer que les propriétés suivantes sont équivalentes :
   (a) $\overline{a}$ est inversible dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$;
   (b) a est premier avec n ;
   (c) $\overline{a}$ est un générateur du groupe additif $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}, +\right)$.
2. Quel est le nombre de diviseurs de $\overline{0}$ dans l'anneau $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$?
3. Soient $(\Omega, \mathcal{B}, \mathbb{P})$ un espace probabilisé et $(A_k)_{1\leq k\leq n}$ une suite finie de $n \geq 2$ événements. Montrer que $A_1, \cdots, A_n$ sont mutuellement indépendants si, et seulement si, pour tout entier k compris entre 1 et n, les événements $\Omega \setminus A_1, \cdots, \Omega \setminus A_k, A_{k+1}, \cdots, A_n$ sont mutuellement indépendants.
4. Soit $n \geq 2$ un entier naturel.
   On se place sur l'espace probabilisé $(\Omega_n, \mathcal{P}(\Omega_n), \mathbb{P})$, où $\Omega_n = \{1, \cdots, n\}$ et :
   $$\forall k \in \Omega_n,\ \mathbb{P}(\{k\}) = \frac{1}{n}$$
   ce qui revient à considérer l'expérience aléatoire qui consiste à choisir de manière équiprobable un entier k compris entre 1 et n.
   Pour tout entier d compris entre 1 et n, on désigne par A_d l'événement : « l'entier k choisi dans Ω_n est divisible par d ».
   Pour tout réel x, on note $[x]$ la partie entière de x.
   (a) Montrer que pour tout entier d compris entre 1 et n, on a $\mathbb{P}(A_d) = \dfrac{1}{n}\left[\dfrac{n}{d}\right]$.
   (b) Montrer que si $2 \leq q_1 < q_2 < \cdots < q_r \leq n$ sont tous les diviseurs premiers de n, les événements $A_{q_1}, \cdots, A_{q_r}$ sont alors mutuellement indépendants.
   (c) On désigne par B_1 l'événement : « l'entier k choisi dans Ω_n est premier avec n ».
   En calculant $\mathbb{P}(B_1)$ de deux manières différentes, montrer que :
   $$\varphi(n) = n\prod_{k=1}^{r}\left(1 - \frac{1}{q_k}\right) \tag{1}$$
5. Donner une démonstration « non probabiliste » de l'égalité (1).
6. Montrer que, pour tout entier $n \geq 3$ l'entier $\varphi(n)$ est pair.

7. Pour tout diviseur positif d de n, on désigne par B_d l'événement : « l'entier k choisi dans Ω_n est tel que $a \wedge n = d$ ».
   En calculant $\mathbb{P}(B_d)$, pour tout diviseur positif d de n, montrer que :

$$n = \sum_{d/n} \varphi\left(\frac{n}{d}\right) = \sum_{d/n} \varphi(d) \tag{2}$$

   (la notation d/n signifie que d est un diviseur positif de n).

8. Pour tout entier $m \geq 1$, on désigne par Φ_m le m-ème polynôme cyclotomique défini par :

$$\Phi_m(X) = \prod_{\substack{1 \leq k \leq m \\ k \wedge m = 1}} \left(X - e^{\frac{2ik\pi}{m}}\right)$$

   en notant $a \wedge b$ le pgcd de deux entiers a et b.
   En utilisant l'égalité (2), montrer que :

$$X^n - 1 = \prod_{d/n} \Phi_d(X)$$

– II – Un théorème de Cesàro

Pour tout entier $n \geq 2$, on se place sur l'espace probabilisé $(\Omega_n^2, \mathcal{P}(\Omega_n^2), \mathbb{P})$, où $\Omega_n = \{1, \cdots, n\}$, avec la mesure de probabilité $\mathbb{P}$ définie par :

$$\forall (a,b) \in \Omega_n^2,\ \mathbb{P}(\{(a,b)\}) = \frac{1}{n^2}$$

et on s'intéresse à l'événement :

$$C_n = \left\{(a,b) \in \Omega_n^2 \mid a \wedge b = 1\right\}$$

Précisément, on se propose de calculer $\mathbb{P}(C_n)$ de deux manières différentes, puis de montrer que $\lim\limits_{n \to +\infty} \mathbb{P}(C_n) = \dfrac{6}{\pi^2}$.

En notant $m = \prod\limits_{i=1}^{r} q_i^{\alpha_i}$ la décomposition en facteurs premiers d'un entier $m \geq 2$ où $r \geq 1$, les q_i étant premiers deux à deux distincts et les α_i entiers naturels non nuls, on définit la fonction μ de Möbius par :

$$\forall m \in \mathbb{N}^*,\ \mu(m) = \begin{cases} 1 \text{ si } m = 1 \\ (-1)^r \text{ si } m = \prod\limits_{i=1}^{r} q_i \text{ (i. e. } m \text{ est sans facteurs carrés)} \\ 0 \text{ sinon} \end{cases}$$

Pour tout réel x, on note $[x]$ la partie réelle de x.

1. Montrer que :

$$\forall n \geq 2,\ \mathbb{P}(C_n) = \frac{1}{n^2}\left(2\sum_{k=1}^{n} \varphi(k) - 1\right)$$

2. Pour $n \geq 2$, on note $q_1 < q_2 < \cdots < q_r$ tous les nombres premiers compris entre 1 et n et pour tout entier k compris entre 1 et r, on note :

$$D_k = \left\{(a,b) \in \Omega_n^2 \mid q_k \text{ divise } a \text{ et } b\right\}$$

   (a) Montrer que :

$$\mathbb{P}(C_n) = 1 - \mathbb{P}\left(\bigcup_{k=1}^{r} D_k\right)$$

   (b) Montrer que pour $1 \leq k \leq r$ et $1 \leq i_1 < \cdots < i_k \leq r$, on a :

$$\mathbb{P}(D_{i_1} \cap \cdots \cap D_{i_k}) = \frac{1}{n^2}\left[\frac{n}{q_{i_1} \cdots q_{i_r}}\right]^2$$

   (c) En déduire que :

$$\mathbb{P}(C_n) = \frac{1}{n^2}\sum_{d=1}^{n} \mu(d)\left[\frac{n}{d}\right]^2$$

3. Montrer que :

$$\forall n \geq 2,\ \sum_{d/n} \mu(d) = 0$$

4. Déduire de ce qui précède que :

$$\forall n \geq 1,\ \sum_{k=1}^{n} \varphi(k) = \frac{1}{2}\left(\sum_{d=1}^{n} \mu(d)\left[\frac{n}{d}\right]^2 + 1\right)$$

   puis que :

$$\forall n \geq 1,\ \varphi(n) = \sum_{d/n} \mu(d)\frac{n}{d}$$

5. Justifier la convergence de la série numérique $\sum \dfrac{\mu(n)}{n^2}$, puis montrer que :

$$\lim_{n\to+\infty} \mathbb{P}(C_n) = \sum_{n=1}^{+\infty} \frac{\mu(n)}{n^2}$$

6. Le produit de convolution (ou le produit de Dirichlet) de deux suites réelles $(u_n)_{n\in\mathbb{N}^*}$ et $(v_n)_{n\in\mathbb{N}^*}$ est la suite $(w_n)_{n\in\mathbb{N}^*}$ définie par :

$$\forall n \in \mathbb{N}^*,\ w_n = \sum_{d/n} u_d v_{\frac{n}{d}}$$

   (a) Soient $(u_n)_{n\in\mathbb{N}^*}$ et $(v_n)_{n\in\mathbb{N}^*}$ deux suites à valeurs réelles positives et $(w_n)_{n\in\mathbb{N}^*}$ leur produit de convolution.
   Montrer si les séries $\sum u_n$ et $\sum v_n$ sont convergentes, il en est alors de même de la série $\sum w_n$ et on a :

$$\sum_{n=1}^{+\infty} w_n = \left(\sum_{n=1}^{+\infty} u_n\right)\left(\sum_{n=1}^{+\infty} v_n\right)$$

(b) Soient $(u_n)_{n\in\mathbb{N}^*}$ et $(v_n)_{n\in\mathbb{N}^*}$ deux suites à valeurs réelles et $(w_n)_{n\in\mathbb{N}^*}$ leur produit de convolution.
Montrer si les séries $\sum u_n$ et $\sum v_n$ sont absolument convergentes, il en est alors de même de la série $\sum w_n$ et on a :

$$\sum_{n=1}^{+\infty} w_n = \left(\sum_{n=1}^{+\infty} u_n\right)\left(\sum_{n=1}^{+\infty} v_n\right)$$

7. Montrer que pour tout réel $\alpha > 1$, on a

$$\left(\sum_{n=1}^{+\infty} \frac{\mu(n)}{n^\alpha}\right)\left(\sum_{n=1}^{+\infty} \frac{1}{n^\alpha}\right) = 1$$

et en déduire que :

$$\lim_{n\to+\infty} \mathbb{P}(C_n) = \frac{6}{\pi^2} \text{ (théorème de Cesàro).}$$

– II – Fonction zêta de Riemann

On note $(p_n)_{n\in\mathbb{N}^*}$ la suite strictement croissante des nombres premiers.
La fonction zêta de Riemann est définie par :

$$\forall \alpha > 1,\ \zeta(\alpha) = \sum_{n=1}^{+\infty} \frac{1}{n^\alpha}$$

On se propose de montrer, en utilisant des arguments « probabilistes » la formule d'Euler suivante :

$$\forall \alpha > 1,\ \zeta(\alpha) = \prod_{n=1}^{+\infty} \frac{1}{1-\frac{1}{p_n^\alpha}}$$

puis d'en déduire la divergence de la série $\sum \frac{1}{p_n}$.

1. Montrer que $\lim\limits_{\alpha\to1^+} \zeta(\alpha) = +\infty$.
Pour ce qui suit, on munit l'ensemble $\mathbb{N}^*$ de la tribu $\mathcal{P}(\mathbb{N}^*)$.
2. Soient $\alpha > 1$ un réel fixé et $\mathbb{P}$ une mesure de probabilité sur $(\mathbb{N}^*, \mathcal{P}(\mathbb{N}^*))$ telle que :

$$\forall n \in \mathbb{N}^*,\ \mathbb{P}(n\mathbb{N}^*) = \frac{1}{n^\alpha}$$

Montrer que, pour toute suite $(n_k)_{k\in\mathbb{N}^*}$ d'entiers deux à deux premiers entre eux, la suite $(n_k\mathbb{N}^*)_{k\in\mathbb{N}^*}$ est formée d'événements mutuellement indépendants.
3. Soient $\alpha > 1$ un réel fixé.
(a) Montrer que l'on définit une mesure probabilité sur $(\mathbb{N}^*, \mathcal{P}(\mathbb{N}^*))$ qui vérifie l'hypothèse de la question précédente en posant :

$$\forall n \in \mathbb{N}^*,\ \mathbb{P}(\{n\}) = \frac{1}{\zeta(\alpha)}\frac{1}{n^\alpha}$$

(b) En utilisant cette mesure probabilité, montrer que :

$$\frac{1}{\zeta(\alpha)} = \prod_{n=1}^{+\infty} \left(1 - \frac{1}{p_n^\alpha}\right) \tag{3}$$

(c) Calculer $\mathbb{P}(A)$ où A est l'ensemble des entiers naturels non nuls sans facteurs carrés. Que vaut la limite de $\mathbb{P}(A)$ quand α tend vers 1^+ ?

4. En utilisant l'égalité (3) , montrer que $\sum_{n=1}^{+\infty} \frac{1}{p_n} = +\infty$.

5. Soient $(\Omega, \mathcal{A}, \mathbb{P})$ un espace probabilisé et $(A_n)_{n\in\mathbb{N}}$ une suite d'événements.
On note :

$$\limsup_{n\to+\infty} A_n = \bigcap_{n\in\mathbb{N}} \bigcup_{k\geq n} A_k \text{ et } \liminf_{n\to+\infty} A_n = \bigcup_{n\in\mathbb{N}} \bigcap_{k\geq n} A_k$$

$\limsup_{n\to+\infty} A_n$ est l'ensemble des $x \in \Omega$ qui appartiennent à une infinité de A_n et $\liminf_{n\to+\infty} A_n$ est l'ensemble des $x \in \Omega$ qui appartiennent à tous les A_n sauf au plus un nombre fini.
Montrer que :

(a) si la série $\sum \mathbb{P}(A_n)$ converge, on a alors $\mathbb{P}\left(\limsup_{n\to+\infty} A_n\right) = 0$;

(b) si les événements A_n sont mutuellement indépendants et la série $\sum \mathbb{P}(A_n)$ diverge, on a alors $\mathbb{P}\left(\limsup_{n\to+\infty} A_n\right) = 1$ (loi du zéro-un de Kolmogorov ou lemme de Borel-Cantelli).

6. Montrer que, pour $0 < \alpha \leq 1$, il n'existe pas de mesure de probabilité sur $(\mathbb{N}^*, \mathcal{P}(\mathbb{N}^*))$ telle que :

$$\forall n \in \mathbb{N}^*,\ \mathbb{P}(n\mathbb{N}^*) = \frac{1}{n^\alpha}$$

7. Montrer que l'on définit une mesure probabilité sur $(\mathbb{N}^* \times \mathbb{N}^*, \mathcal{P}(\mathbb{N}^* \times \mathbb{N}^*))$ en posant :

$$\forall (n,m) \in \mathbb{N}^* \times \mathbb{N}^*,\ \mathbb{P}((n,m)) = \frac{1}{\zeta^2(\alpha)} \frac{1}{(nm)^\alpha}$$

Calculer $\mathbb{P}(A)$ où A est l'ensemble des couples d'entiers naturels non nuls qui sont premiers entre eux. Que vaut la limite de $\mathbb{P}(A)$ quand α tend vers 1^+ ?