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 $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}, +\right)$.

Solution Dire que $\overline{a}$ est inversible dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ équivaut à dire qu'il existe $\overline{b}$ dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ tel que $\overline{a}\overline{b} = \overline{1}$, ce qui est encore équivalent à dire qu'il existe b, q dans $\mathbb{Z}$ tels que $ab + qn = 1$ et revient à dire que a et n sont premiers entre eux (théorème de Bézout).

En traduisant le fait que $\overline{a}$ est inversible dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ par l'existence d'un entier relatif b tel que $\overline{a}\overline{b} = b\overline{a} = \overline{1}$, on déduit que cela équivaut à dire que $\overline{1}$ est dans le groupe engendré par $\overline{a}$ et donc que ce groupe est $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.

La fonction indicatrice d'Euler est la fonction φ qui associe à tout entier naturel non nul n, le nombre $\varphi(n)$ d'entiers compris entre 1 et n qui sont premiers avec n (pour $n = 1$, on a $\varphi(1) = 1$).

$\varphi(n)$ est aussi le nombre de générateurs du groupe cyclique $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}, +\right)$ (ou de n'importe quel groupe cyclique d'ordre n) ou encore le nombre d'éléments inversibles de l'anneau $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.

2. Quel est le nombre de diviseurs de $\overline{0}$ dans l'anneau $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$?

Solution

(a) On vérifie qu'un élément de $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$ est soit inversible, soit un diviseur de $\overline{0}$.

En effet, pour $\overline{a} \in \left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$ avec a compris entre 1 et $n-1$, il y a deux possibilités :
- soit a est premier avec n et dans ce cas, $\overline{a}$ est inversible :
- soit le pgcd δ de a et n est supérieur ou égal à 2 et dans ce cas, on a $\overline{a}\dfrac{\overline{n}}{\delta} = \dfrac{\overline{a}}{\delta}\overline{n} = \overline{0}$ avec $\dfrac{\overline{n}}{\delta} \neq \overline{0}$ puisque $1 \leq \dfrac{n}{\delta} \leq n-1$, ce qui signifie que $\overline{a}$ est un diviseur de $\overline{0}$ dans l'anneau $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.

(b) Il en résulte qu'il y a $\text{card}\left(\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^*\right) - \varphi(n) = n - 1 - \varphi(n)$ diviseurs de $\overline{0}$ dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.

(c) En fait, de manière plus générale, on peut vérifier que si $\mathbb{A}$ est un anneau commutatif unitaire et fini, alors un élément de $\mathbb{A}^*$ est soit inversible, soit un diviseur de 0.
En effet, pour $a \in \mathbb{A}^*$, l'application $\mu_a : x \mapsto ax$ est un morphisme du groupe additif $(\mathbb{A}, +)$ et on a deux possibilités :
- soit μ_a est surjectif et dans ce cas le neutre 1 pour le produit a un antécédent a', donc $aa' = 1$ et a est inversible dans $\mathbb{A}$;
- Soit μ_a est non surjectif et dans ce cas il est non injectif puisque $\mathbb{A}$ est fini, donc $\ker(\mu_a) \neq \{0\}$ et il existe $b \in \mathbb{A}^*$ tel que $ab = 0$, ce qui signifie que a est un diviseur de 0.

On en déduit qu'un anneau commutatif, unitaire et fini est intègre si, et seulement si, c'est un corps.
En effet, un corps est toujours intègre et réciproquement si $\mathbb{A}$ est fini et intègre, il est alors sans diviseurs de zéro, donc tous ses éléments non nuls sont inversibles et c'est un corps.

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.

Solution Il suffit de montrer que si $(A_k)_{1\leq k\leq n}$ est une suite d'événements mutuellement indépendants, alors les événements $\Omega \setminus A_1, A_2, \cdots, A_n$ sont mutuellement indépendants (récurrence finie).
On note $A'_1 = \Omega \setminus A_1$, $A'_k = A_k$ pour k compris entre 2 et n et on se donne une partie J non vide de $\{1, 2, \cdots, n\}$.
Si $1 \notin J$, on a alors :

$$\mathbb{P}\left(\bigcap_{j\in J} A'_j\right) = \mathbb{P}\left(\bigcap_{j\in J} A_j\right) = \prod_{j\in J} \mathbb{P}(A_j) = \prod_{j\in J} \mathbb{P}\left(A'_j\right)$$

Si J a plus de 2 éléments et $1 \in J$ (pour $J = \{1\}$, il n'y a rien à montrer), on a alors :

$$\bigcap_{j\in J} A'_j = (\Omega \setminus A_1) \cap \left(\bigcap_{j\in J\setminus\{1\}} A_j\right) = \bigcap_{j\in J\setminus\{1\}} A_j \setminus \bigcap_{j\in J} A_j$$

avec $\bigcap\limits_{j\in J} A_j \subset \bigcap\limits_{j\in J\setminus\{1\}} A_j$, donc :

$$\begin{aligned}\mathbb{P}\left(\bigcap_{j\in J} A'_j\right) &= \mathbb{P}\left(\bigcap_{j\in J\setminus\{1\}} A_j\right) - \mathbb{P}\left(\bigcap_{j\in J} A_j\right)\\ &= \prod_{j\in J\setminus\{1\}} \mathbb{P}(A_j) - \prod_{j\in J} \mathbb{P}(A_j)\\ &= (1 - \mathbb{P}(A_1)) \prod_{j\in J\setminus\{1\}} \mathbb{P}(A_j) = \prod_{j\in J} \mathbb{P}\left(A'_j\right)\end{aligned}$$

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 :

$$\varphi(n) = n\prod_{k=1}^{r}\left(1 - \frac{1}{q_k}\right) \tag{1}$$

Solution

(a) Pour d compris entre 1 et n, on a :

$$A_d = \left\{a \in \Omega_n \mid \exists q \in \left\{1, \cdots, \left[\frac{n}{d}\right]\right\} \ ; \ a = qd\right\}$$

donc :

$$\mathbb{P}(A_d) = \frac{\operatorname{card}(A_d)}{\operatorname{card}(\Omega)} = \frac{1}{n}\left[\frac{n}{d}\right]$$

Dans le cas où d est un diviseur de n, on a $\left[\dfrac{n}{d}\right] = \dfrac{n}{d}$ et $\mathbb{P}(A_d) = \dfrac{1}{d}$.

(b) La décomposition en facteurs premiers de n s'écrit $n = \prod_{k=1}^{r} q_k^{\alpha_k}$, les exposants α_k étant tous non nuls.
Soit J une partie non vide de $\{1, 2, \cdots, r\}$.
Les entiers q_j pour $j \in J$ sont premiers et distincts, donc premiers entre eux et un entier a compris entre 1 et n, est divisible par tous les q_j si, et seulement si, il est divisible par leur produit. On a donc :

$$\bigcap_{j\in J} A_{q_j} = A_{\prod\limits_{j\in J} q_j}$$

et :

$$\mathbb{P}\left(\bigcap_{j\in J} A_{q_j}\right) = \mathbb{P}(A_{\prod\limits_{j\in J} q_j}) = \frac{1}{\prod\limits_{j\in J} q_j} = \prod_{j\in J}\frac{1}{q_j} = \prod_{j\in J}\mathbb{P}\left(A_{q_j}\right)$$

(l'entier $\prod_{j\in J} q_j$ est un diviseur de n).
Les événements $A_{q_1}, \cdots, A_{q_r}$ sont donc mutuellement indépendants.

(c) On a :

$$\mathbb{P}(B_1) = \frac{\operatorname{card}(B_1)}{\operatorname{card}(\Omega_n)} = \frac{\varphi(n)}{n}$$

D'autre part, un entier est dans B_1 si, et seulement si, il n'est divisible par aucun des q_k, donc :

$$B_1 = \bigcap_{k=1}^{r}(\Omega_n \setminus A_{q_k})$$

Les événements $A_{q_1}, \cdots, A_{q_r}$ étant mutuellement indépendants, il en est de même des événements $\Omega_n \setminus A_{q_1}, \cdots, \Omega_n \setminus A_{q_r}$, donc :

$$\mathbb{P}(B_1) = \prod_{k=1}^{r} \mathbb{P}(\Omega_n \setminus A_{q_k}) = \prod_{k=1}^{r} \left(1 - \frac{1}{q_k}\right)$$

et :

$$\varphi(n) = n \prod_{k=1}^{r} \left(1 - \frac{1}{q_k}\right) = \prod_{k=1}^{r} q_k^{\alpha_k - 1}(q_k - 1)$$

5. Donner une démonstration « non probabiliste » de l'égalité (1).

Solution En utilisant la décomposition en facteurs premiers $n = \prod_{k=1}^{r} q_k^{\alpha_k}$, le théorème chinois nous dit qu'on a un isomorphisme d'anneaux :

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \overset{\sim}{\to} \prod_{k=1}^{r} \frac{\mathbb{Z}}{q_k^{\alpha_k}\mathbb{Z}}$$

qui induit un isomorphisme de groupes multiplicatifs :

$$\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times} \overset{\sim}{\to} \left(\prod_{k=1}^{r} \frac{\mathbb{Z}}{q_k^{\alpha_k}\mathbb{Z}}\right)^{\times} = \prod_{k=1}^{r} \left(\frac{\mathbb{Z}}{q_k^{\alpha_k}\mathbb{Z}}\right)^{\times}$$

ce qui nous donne :

$$\varphi(n) = \operatorname{card}\left(\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times}\right) = \operatorname{card}\left(\prod_{k=1}^{r} \left(\frac{\mathbb{Z}}{q_k^{\alpha_k}\mathbb{Z}}\right)^{\times}\right) = \prod_{i=1}^{r} \varphi(q_k^{\alpha_k})$$

Le calcul de $\varphi(n)$ est alors ramené à celui de $\varphi(p^{\alpha})$ où p est un nombre premier et α un entier naturel non nul.
Pour p premier, un entier k compris entre 1 et p^{α} n'est pas premier avec p^{α} si, et seulement si, il est divisible par p, ce qui équivaut à $k = mp$ avec $1 \leq m \leq p^{\alpha-1}$, soit $p^{\alpha-1}$ possibilités. On a donc :

$$\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1} = (p-1)\,p^{\alpha-1}$$

et $\varphi(n) = \prod_{k=1}^{r} q_k^{\alpha_k - 1}(q_k - 1) = n \prod_{k=1}^{r} \left(1 - \frac{1}{q_k}\right)$.

6. Montrer que, pour tout entier $n \geq 3$ l'entier $\varphi(n)$ est pair.

Solution Pour $n = 2^{\alpha_1}$ avec $\alpha_1 \geq 2$, on a $\varphi(n) = 2^{\alpha_1 - 1}$ qui est pair et pour $n = 2^{\alpha_1} \prod_{k=2}^{r} q_k^{\alpha_k}$ avec $\alpha_1 \geq 0$, $r \geq 1$, tous les q_k étant premiers impairs distincts, on a $\varphi(n) = \varphi(2^{\alpha_1}) \prod_{k=2}^{r} q_k^{\alpha_k - 1}(q_k - 1)$ qui 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).

Solution On a la partition $\Omega_n = \bigcup_{d/n} B_d$ (les B_d forment un système complet d'événements), donc :

$$1 = \mathbb{P}(\Omega_n) = \sum_{d/n} \mathbb{P}(B_d)$$

Si d est un diviseur d de n, il existe alors un entier $q \geq 1$ tel que $n = qd$ et :

$$(k \in B_d) \Leftrightarrow \left(k = q_1 d \text{ où } 1 \leq q_1 = \frac{k}{d} \leq \frac{n}{q} = q \text{ et } q_1 \wedge q = 1\right)$$

donc :

$$\text{card}(B_d) = \text{card}\{q_1 \in \{1, \cdots, q\} \mid q_1 \wedge q = 1\} = \varphi(q) = \varphi\left(\frac{n}{d}\right)$$

ce qui nous donne :

$$\mathbb{P}(B_d) = \frac{1}{n}\varphi\left(\frac{n}{d}\right)$$

et les égalités :

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

(l'application $d \mapsto \dfrac{n}{d}$ est une permutation de l'ensemble des diviseurs positifs 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 :

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

Solution Chaque polynôme Φ_d est de degré $\varphi(d)$ et scindé à racines simples dans $\mathbb{C}[X]$.
Tenant compte de l'égalité des degrés :

$$\deg(X^n - 1) = n = \sum_{d/n} \varphi(d) = \sum_{d/n} \deg(\Phi_d)$$

tous les polynômes considérés étant unitaires, il nous suffit de montrer que pour tout diviseur d de n le polynôme Φ_d divise $X^n - 1$ et que les polynômes Φ_d sont deux à deux premiers entre eux.
Pour d divisant n, les racines de Φ_d sont les nombres complexes :

$$e^{\frac{2ik\pi}{d}} = \left(e^{\frac{2i\pi}{n}}\right)^{k\frac{n}{d}}$$

avec $j = k\dfrac{n}{d}$ compris entre 1 et n, ce sont donc des racines n-èmes de l'unité et Φ_d divise $X^n - 1$.
Chacun de ces entiers k étant premier avec d, on a :

$$j \wedge n = \left(k\frac{n}{d}\right) \wedge \left(d\frac{n}{d}\right) = \frac{n}{d}(k \wedge d) = \frac{n}{d}$$

les polynômes Φ_d, pour d divisant n, sont deux à deux premiers entre eux.

– II – Un théorème de Cesàro

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

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

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 :

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

Solution En notant $C_n^+ = \{(a,b) \in A_n \mid a < b\}$ et $C_n^- = \{(a,b) \in A_n \mid a > b\}$, on a la partition :

$$C_n = \{(1,1)\} \cup C_n^+ \cup C_n^-$$

et :

$$\begin{aligned} \mathbb{P}(C_n) &= \mathbb{P}\left(\{(1,1)\}\right) + \mathbb{P}\left(C_n^+\right) + \mathbb{P}\left(C_n^-\right) \\ &= \frac{1}{n^2}\left(1 + 2\,\mathrm{card}\left(C_n^+\right)\right) \end{aligned}$$

(par symétrie, on a $\mathrm{card}\left(C_n^-\right) = \mathrm{card}\left(C_n^+\right)$).
En utilisant la partition :

$$C_n^+ = \bigcup_{b=2}^{n} C_n^+(b)$$

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

on a :

$$\mathrm{card}\left(C_n^+(b)\right) = \mathrm{card}\left\{a \in \{1, \cdots, b-1\} \mid a \wedge b = 1\right\} = \varphi(b)$$

et :

$$\mathrm{card}\left(C_n^+\right) = \sum_{b=2}^{n} \varphi(b)$$

ce qui nous donne :

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

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 :

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

Solution

(a) On a :

$$\left((a,b) \in \Omega_n^2 \setminus C_n\right) \Leftrightarrow (a \wedge b \geq 2) \Leftrightarrow (\exists k \in \{1, \cdots, \} \mid q_k \text{ divise } a \text{ et } b)$$

donc :

$$\Omega_n^2 \setminus C_n = \bigcup_{k=1}^{r} D_k$$

et :

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

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

$$\begin{aligned}((a,b) \in D_{i_1} \cap \cdots \cap D_{i_k}) &\Leftrightarrow (a \text{ et } b \text{ sont multiples communs de } q_{i_1}, \cdots, q_{i_k}) \\ &\Leftrightarrow (a \text{ et } b \text{ sont multiples communs de } q_{i_1} \cdots q_{i_r})\end{aligned}$$

(tous les q_k sont premiers) et on a vu en **I.4a** qu'il y a $\left[\dfrac{n}{q_{i_1} \cdots q_{i_r}}\right]$ entiers compris entre 1 et n multiples de $q_{i_1} \cdots q_{i_r}$, donc :

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

et :

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

(c) En utilisant la formule de Poincaré (ou du crible), on a :

$$\begin{aligned}1 - \mathbb{P}(C_n) = \mathbb{P}\left(\bigcup_{k=1}^{r} D_k\right) &= \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \leq i_1 < \cdots < i_k \leq n} \mathbb{P}(D_{i_1} \cap \cdots \cap D_{i_k}) \\ &= -\frac{1}{n^2}\sum_{k=1}^{n} (-1)^k \sum_{1 \leq i_1 < \cdots < i_k \leq n} \left[\frac{n}{q_{i_1} \cdots q_{i_r}}\right]^2 \\ &= -\frac{1}{n^2}\sum_{k=1}^{n} \sum_{1 \leq i_1 < \cdots < i_k \leq n} \mu(q_{i_1} \cdots q_{i_r})\left[\frac{n}{q_{i_1} \cdots q_{i_r}}\right]^2\end{aligned}$$

Tout entier d compris entre 2 et n s'écrit $d = q_{i_1}^{\alpha_{i_1}} \cdots q_{i_r}^{\alpha_{i_r}}$ où $1 \leq k \leq n$, $1 \leq i_1 < \cdots < i_k \leq n$, les exposants α_{i_j} étant positifs non nuls et on a $\mu(d) = 0$ si l'un des α_{i_j} est supérieur ou égal à 2 (i. e. si d a un facteur carré), donc la somme précédente s'écrit aussi :

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

ce qui nous donne :

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

3. Montrer que :

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

Solution Si $n = \prod_{i=1}^{r} q_i^{\alpha_i}$ est la décomposition en facteurs premiers de l'entier $n \geq 2$, tous les diviseurs de n sont alors de la forme $d = \prod_{i=1}^{r} q_i^{\beta_i}$ avec $0 \leq \beta_i \leq \alpha_i$ pour $1 \leq i \leq r$ et $\mu(d) = 0$ si l'un des β_i est supérieur ou égal à 2.
Ce qui nous donne :

$$\sum_{d/n} \mu(d) = \sum_{(\beta_1, \cdots, \beta_r) \in \{0,1\}^r} \mu\left(\prod_{i=1}^{r} q_i^{\beta_i}\right)$$

Pour k compris entre 0 et r, il y a $\binom{r}{k}$ façons de choisir un r-uplet $(\beta_1, \cdots, \beta_r)$ formé de k termes égaux à 1 et $r-k$ termes égaux à 0 et pour chacun de ces choix, on a $\mu\left(\prod_{i=1}^{r} q_i^{\beta_i}\right) = (-1)^k$, donc :

$$\sum_{d/n} \mu(d) = \sum_{k=0}^{r} \binom{r}{k} (-1)^k = (1-1)^r = 0$$

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 :

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

Solution Pour $n = 1$, on a par conventions $\varphi(1) = \mu(1) = 1$ et il n'y a rien à prouver.
Pour $n \geq 2$, des égalités :

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

on déduit que :

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

ce qui nous donne :

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

Pour $d \in \{1, \cdots, n-1\}$ divisant n, on a $n = qd$ avec $q = \dfrac{n}{d} \in \{2, \cdots, n\}$, donc $\left[\dfrac{n}{d}\right] = q$, $\left[\dfrac{n-1}{d}\right] = \left[q - \dfrac{1}{d}\right] = q - 1$ et :

$$\left[\frac{n}{d}\right]^2 - \left[\frac{n-1}{d}\right]^2 = q^2 - (q-1)^2 = 2q - 1 = 2\frac{n}{d} - 1$$

Pour $d \in \{2, \cdots, n-1\}$ ne divisant pas n, on a $n = qd + r$ avec $q = \left[\dfrac{n}{d}\right] \in \{1, \cdots, n-1\}$ et $r \in \{1, \cdots, d-1\}$, donc :

$$\left[\frac{n-1}{d}\right] = \left[q + \frac{r-1}{d}\right] = q$$

(on a $0 \leq \dfrac{r-1}{d} \leq \dfrac{d-2}{d} < 1$) et :

$$\left[\frac{n}{d}\right]^2 - \left[\frac{n-1}{d}\right]^2 = 0$$

On a donc :

$$\varphi(n) = \frac{1}{2}\left(\sum_{\substack{1 \leq d \leq n-1 \\ d/n}} \mu(d)\left(2\frac{n}{d} - 1\right) + \mu(n)\right) = \frac{1}{2}\sum_{\substack{1 \leq d \leq n \\ d/n}} \mu(d)\left(2\frac{n}{d} - 1\right)$$
$$= \sum_{\substack{1 \leq d \leq n \\ d/n}} \mu(d)\frac{n}{d} - \frac{1}{2}\sum_{\substack{1 \leq d \leq n \\ d/n}} \mu(d) = \sum_{\substack{1 \leq d \leq n \\ d/n}} \mu(d)\frac{n}{d}$$

Ce résultat peut aussi se montrer en utilisant un théorème d'inversion de Möbius qui nous dit que si $(u_n)_{n \in \mathbb{N}^*}$ et $(v_n)_{n \in \mathbb{N}^*}$ sont deux suites réelles telles que :

$$\forall n \in \mathbb{N}^*,\ u(n) = \sum_{d/n} v(d)$$

on a alors :

$$\forall n \in \mathbb{N}^*,\ v(n) = \sum_{d/n} \mu(d)\, u\left(\frac{n}{d}\right)$$

Des relations :

$$\forall n \in \mathbb{N}^*,\ n = \sum_{d/n} \varphi(d)$$

on en déduit alors que $\varphi(n) = \displaystyle\sum_{d/n} \mu(d)\frac{n}{d}$ pour tout $n \in \mathbb{N}^*$.

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

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

Solution Pour tout entier $n \geq 1$, on a $\mu(n) \in \{-1, 0, 1\}$, donc $\left|\frac{\mu(n)}{n^2}\right| \leq \frac{1}{n^2}$ et en conséquence la série $\sum \frac{\mu(n)}{n^2}$ est absolument convergente.
Pour tout entier $n \geq 1$, on a :

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

avec, pour tout entier k compris entre 1 et n :

$$\left[\frac{n}{k}\right] \leq \frac{n}{k} < \left[\frac{n}{k}\right] + 1$$

soit :

$$0 \leq \frac{n}{k} - 1 < \left[\frac{n}{k}\right] \leq \frac{n}{k}$$

donc :

$$\left(\frac{n}{k} - 1\right)^2 < \left[\frac{n}{k}\right]^2 \leq \left(\frac{n}{k}\right)^2$$

et :

$$0 \leq \left(\frac{n}{k}\right)^2 - \left[\frac{n}{k}\right]^2 < \left(\frac{n}{k}\right)^2 - \left(\frac{n}{k} - 1\right)^2 = 2\frac{n}{k} - 1$$

Ce qui nous donne :

$$|\varepsilon_n| \leq \frac{1}{n^2} \sum_{k=1}^{n} \left(\left(\frac{n}{k}\right)^2 - \left[\frac{n}{k}\right]^2 \right) < \frac{2}{n} \sum_{k=1}^{n} \frac{1}{k} - \frac{1}{n}$$

avec $\sum_{k=1}^{n} \frac{1}{k} \underset{n\to+\infty}{\backsim} \ln(n)$ et $\lim_{n\to+\infty} \frac{\ln(n)}{n} = 0$.
Il en résulte que $\lim_{n\to+\infty} \varepsilon_n = 0$, donc la suite $(\mathbb{P}(C_n))_{n\in\mathbb{N}^*}$ est convergente et :

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

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 :

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

Solution Pour tout entier $n \in \mathbb{N}^*$, on note U_n, V_n, W_n les sommes partielles des séries $\sum u_n$, $\sum v_n$ et $\sum w_n$.
Pour tout entier $n \in \mathbb{N}^*$, on a :

$$U_n V_n = \sum_{1\leq i,j\leq n} u_i v_j = \sum_{(i,j)\in\Omega_n^2} u_i v_j$$

et :

$$W_n = \sum_{k=1}^{n} \sum_{\substack{1\leq i\leq k \\ i/k}} u_i v_{\frac{k}{i}} = \sum_{\substack{1\leq i,j\leq n \\ ij\leq n}} u_i v_j = \sum_{(i,j)\in\Delta_n} u_i v_j$$

en notant $\Delta_n = \{(i,j) \in \Omega_n^2 \mid ij \leq n\}$.

(a) Comme $\Delta_n \subset \Omega_n^2 \subset \Delta_{n^2}$ et les séries considérées sont à termes positifs, on a :

$$W_n \leq U_n V_n \leq W_{n^2}$$

De la convergence des séries $\sum u_n$ et $\sum v_n$, on déduit que la suite croissante $(W_n)_{n\in\mathbb{N}^*}$ est majorée, donc convergente.
Faisant tendre n vers l'infini dans l'encadrement précédent, on aboutit à l'égalité :

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

(b) Dans le cas général, des inégalités :

$$|w_n| \leq \sum_{d/n} |u_d| \left|v_{\frac{n}{d}}\right| = t_n$$

la suite $(t_n)_{n\in\mathbb{N}^*}$ étant le produit de convolution des suites positives convergentes $(|u_n|)_{n\in\mathbb{N}^*}$ et $(|v_n|)_{n\in\mathbb{N}^*}$, on déduit que la série $\sum w_n$ est absolument convergente.
Puis avec :

$$\begin{aligned} |U_n V_n - W_n| &= \left|\sum_{(i,j)\in\Omega_n^2} u_i v_j - \sum_{(i,j)\in\Delta_n} u_i v_j\right| = \left|\sum_{(i,j)\in\Omega_n^2\setminus\Delta_n} u_i v_j\right| \\ &\leq \sum_{(i,j)\in\Omega_n^2\setminus\Delta_n} |u_i|\,|v_j| = U'_n V'_n - T_n \end{aligned}$$

où U'_n, V'_n et T_n sont les sommes partielles des séries $\sum |u_n|$, $\sum |v_n|$ et $\sum t_n$ avec $\lim\limits_{n\to+\infty} (U'_n V'_n - T_n) = 0$ puisque $\sum\limits_{n=1}^{+\infty} t_n = \left(\sum\limits_{n=1}^{+\infty} |u_n|\right)\left(\sum\limits_{n=1}^{+\infty} |v_n|\right)$, on déduit que $\lim\limits_{n\to+\infty} (U_n V_n - W_n) = 0$, ce qui signifie que :

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

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 :

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

Solution Les séries $\sum\frac{1}{n^\alpha}$ et $\sum\frac{\mu(n)}{n^\alpha}$ étant absolument convergentes, on a :

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

où :

$$w_1 = \mu(1) = 1$$

et :

$$\forall n \geq 2,\ w_n = \sum_{d/n}\frac{\mu(d)}{d^\alpha}\left(\frac{d}{n}\right)^\alpha = \frac{1}{n^\alpha}\sum_{d/n}\mu(d) = 0$$

ce qui nous donne $\left(\sum_{n=1}^{+\infty}\frac{\mu(n)}{n^\alpha}\right)\left(\sum_{n=1}^{+\infty}\frac{1}{n^\alpha}\right) = 1$, soit :

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

En particulier, on a :

$$\lim_{n\to+\infty}\mathbb{P}(C_n) = \sum_{n=1}^{+\infty}\frac{\mu(n)}{n^2} = \frac{1}{\zeta(\alpha)} = \frac{6}{\pi^2}$$

De manière analogue, en désignant par $\mathbb{P}(C_{n,r})$ la probabilité que $r \geq 2$ entiers compris entre 1 et r soient premiers entre eux, on a :

$$\lim_{n\to+\infty}\mathbb{P}(C_{n,r}) = \sum_{n=1}^{+\infty}\frac{\mu(n)}{n^r} = \frac{1}{\zeta(r)}$$

– 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 $\lim\limits_{\alpha\to 1^+}\zeta(\alpha)=+\infty$.

Solution Pour tout réel $\alpha>1$ et tout entier $n\geq 1$, on a :

$$\zeta(\alpha)>\sum_{k=1}^{n}\frac{1}{k^\alpha}=\sum_{k=1}^{n}\frac{1}{k}-\sum_{k=1}^{n}\left(\frac{1}{k}-\frac{1}{k^\alpha}\right)$$

avec $\displaystyle\sum_{n=1}^{+\infty}\frac{1}{n}=+\infty$.

Pour tout réel $M>0$, il existe donc un entier n_M tel que $\displaystyle\sum_{k=1}^{n_M}\frac{1}{k}>2M$, ce qui nous donne :

$$\zeta(\alpha)>2M-\sum_{k=1}^{n_M}\left(\frac{1}{k}-\frac{1}{k^\alpha}\right)$$

avec $\lim\limits_{\alpha\to 1^+}\displaystyle\sum_{k=1}^{n_M}\left(\frac{1}{k}-\frac{1}{k^\alpha}\right)=0$.

Il existe donc un entier $\eta>0$ tel que $\displaystyle\sum_{k=1}^{n_M}\left(\frac{1}{k}-\frac{1}{k^\alpha}\right)<M$ pour tout réel $\alpha\in\,]1,1+\eta[$, ce qui nous donne :

$$\forall\alpha\in\,]1,1+\eta[\,,\ \zeta(\alpha)>2M-M=M$$

On a donc ainsi prouvé que $\lim\limits_{\alpha\to 1^+}\zeta(\alpha)=+\infty$.

On peut aussi écrire que, pour tout $n\geq 1$, on a :

$$\zeta(\alpha)>\sum_{k=1}^{n}\frac{1}{k^\alpha}>\sum_{k=1}^{n}\int_k^{k+1}\frac{dt}{t^\alpha}=\int_1^{n+1}\frac{dt}{t^\alpha}=\frac{1}{\alpha-1}\left(1-\frac{1}{(n+1)^{\alpha-1}}\right)$$

ce qui donne $\zeta(\alpha)\geq\dfrac{1}{\alpha-1}$ en faisant tendre n vers l'infini et en conséquence $\lim\limits_{\alpha\to 1^+}\zeta(\alpha)=+\infty$.

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.

Solution Pour toute partie I finie de $\mathbb{N}^*$, on a $\displaystyle\bigcap_{k\in I}n_k\mathbb{N}^*=\operatorname*{ppcm}_{k\in I}(n_k)\,\mathbb{N}^*$ par définition du ppcm, avec $\displaystyle\operatorname*{ppcm}_{k\in I}(n_k)=\prod_{k\in I}n_k$ puisque les n_k sont deux à deux premiers entre eux, donc

$$\mathbb{P}\left(\bigcap_{k\in I}n_k\mathbb{N}^*\right)=\mathbb{P}\left(\left(\prod_{k\in I}n_k\right)\mathbb{N}^*\right)=\frac{1}{\displaystyle\prod_{k\in I}n_k^\alpha}=\prod_{k\in I}\left(\frac{1}{n_k^\alpha}\right)$$

$$=\prod_{k\in I}\mathbb{P}(n_k\mathbb{N}^*)$$

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^+ ?

Solution

(a) Pour tout entier $n \in \mathbb{N}^*$, on a $\mathbb{P}(\{n\}) > 0$ et :

$$\sum_{n=1}^{+\infty} \mathbb{P}(\{n\}) = \frac{1}{\zeta(\alpha)} \sum_{n=1}^{\infty} \frac{1}{n^\alpha} = 1$$

donc $\mathbb{P}$ est bien une mesure de probabilité sur $(\mathbb{N}^*, \mathcal{P}(\mathbb{N}^*))$.
Pour tout entier $n \in \mathbb{N}^*$, on a :

$$\mathbb{P}(n\mathbb{N}^*) = \mathbb{P}\left(\bigcup_{q \in \mathbb{N}^*} \{qn\}\right) = \sum_{q=1}^{+\infty} \mathbb{P}(\{qn\}) = \frac{1}{\zeta(\alpha)} \sum_{q=1}^{+\infty} \frac{1}{q^\alpha n^\alpha} = \frac{1}{n^\alpha}$$

(b) On a :

$$\frac{1}{\zeta(\alpha)} = \mathbb{P}(\{1\})$$

avec :

$$\{1\} = \bigcap_{n=1}^{+\infty} (\mathbb{N}^* \setminus p_n\mathbb{N}^*)$$

(1 est l'unique entier naturel non nul qui n'a pas de diviseur premier).
En notant, pour tout entier $n \geq 1$:

$$A_n = \bigcap_{k=1}^{n} (\mathbb{N}^* \setminus p_k\mathbb{N}^*)$$

on définit une suite décroissante d'évènements (A_n est l'ensemble des entiers qui ne sont multiples d'aucun des nombres premier $p_1, \cdots, p_n$, donc $A_{n+1} \subset A_n$) et on a :

$$\{1\} = \bigcap_{n=1}^{+\infty} A_n$$

donc :

$$\mathbb{P}(\{1\}) = \lim_{n \to +\infty} \mathbb{P}(A_n)$$

avec, pour tout entier $n \geq 1$:

$$\mathbb{P}(A_n) = \prod_{k=1}^{n} \mathbb{P}(\mathbb{N}^* \setminus p_k\mathbb{N}^*) = \prod_{k=1}^{n} (1 - \mathbb{P}(p_k\mathbb{N}^*)) = \prod_{k=1}^{n} \left(1 - \frac{1}{p_k^\alpha}\right)$$

(les $p_k\mathbb{N}^*$ étant indépendants, il en est de même des $\mathbb{N}^* \setminus p_k\mathbb{N}^*$), ce qui nous donne :

$$\frac{1}{\zeta(\alpha)} = \lim_{n \to +\infty} \prod_{k=1}^{n} \left(1 - \frac{1}{p_k^\alpha}\right) = \prod_{n=1}^{+\infty} \left(1 - \frac{1}{p_n^\alpha}\right)$$

(c) Dire qu'un entier n est sans facteur carré revient à dire qu'il n'est divisible par aucun des p_n^2, donc :

$$A = \bigcap_{n=1}^{+\infty} \left(\mathbb{N}^* \setminus p_n^2\mathbb{N}^*\right)$$

les $p_n^2\mathbb{N}^*$ étant indépendants, donc :

$$\begin{aligned}\mathbb{P}(A) &= \bigcap_{n=1}^{+\infty}\left(\bigcap_{k=1}^{n}\left(\mathbb{N}^* \setminus p_k^2\mathbb{N}^*\right)\right) = \lim_{n\to+\infty}\mathbb{P}\left(\bigcap_{k=1}^{n}\left(\mathbb{N}^* \setminus p_k^2\mathbb{N}^*\right)\right)\\ &= \lim_{n\to+\infty}\prod_{k=1}^{n}\mathbb{P}\left(\mathbb{N}^* \setminus p_k^2\mathbb{N}^*\right) = \lim_{n\to+\infty}\prod_{k=1}^{n}\left(1-\frac{1}{p_k^{2\alpha}}\right)\\ &= \prod_{n=1}^{+\infty}\left(1-\frac{1}{p_n^{2\alpha}}\right) = \frac{1}{\zeta(2\alpha)}\end{aligned}$$

et :

$$\lim_{\alpha\to1^+}\mathbb{P}(A) = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}$$

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

Solution Comme $\lim_{n\to+\infty} p_n = +\infty$ et $-\ln\left(1-\frac{1}{p_n}\right) \underset{n\to+\infty}{\backsim} \frac{1}{p_n}$, il nous suffit de prouver la divergence de $\sum \ln\left(1-\frac{1}{p_n}\right)$.
Par continuité de la fonction ln, on a pour tout réel $\alpha > 1$:

$$\ln(\zeta(\alpha)) = -\sum_{n=1}^{+\infty}\ln\left(1-\frac{1}{p_n^\alpha}\right)$$

Comme $\lim_{\alpha\to1^+}\ln(\zeta(\alpha)) = +\infty$, on peut trouver, pour tout réel $M > 0$, un réel $\alpha > 1$ tel que $\ln(\zeta(\alpha)) > 2M$ et pour tout entier $n \geq 1$, on a :

$$\begin{aligned}-\sum_{k=1}^{n}\ln\left(1-\frac{1}{p_k}\right) \geq -\sum_{k=1}^{n}\ln\left(1-\frac{1}{p_k^\alpha}\right) &= -\sum_{k=1}^{+\infty}\ln\left(1-\frac{1}{p_k^\alpha}\right) + \sum_{k=n+1}^{+\infty}\ln\left(1-\frac{1}{p_n^\alpha}\right)\\ &> 2M + \sum_{k=n+1}^{+\infty}\ln\left(1-\frac{1}{p_n^\alpha}\right)\end{aligned}$$

avec $\lim_{n\to+\infty}\sum_{k=n+1}^{+\infty}\ln\left(1-\frac{1}{p_n^\alpha}\right) = 0$.

On peut alors trouver un entier $n_M \geq 1$ tel que $\displaystyle\sum_{k=n+1}^{+\infty}\ln\left(1-\frac{1}{p_n^\alpha}\right) > -M$ pour tout $n \geq n_M$, ce qui nous donne :

$$\forall n \geq n_M,\ -\sum_{k=1}^{n}\ln\left(1-\frac{1}{p_k}\right) > M$$

On a donc prouvé que $-\displaystyle\sum_{n=1}^{+\infty}\ln\left(1-\frac{1}{p_n}\right) = +\infty$ et en conséquence $\displaystyle\sum_{n=1}^{+\infty}\frac{1}{p_n} = +\infty$.

5. Soient $(\Omega, \mathcal{A}, \mathbb{P})$ un espace probabilisé et $(A_n)_{n\in\mathbb{N}}$ une suite d'événements.
On note :
$$\limsup_{n\to+\infty} A_n = \bigcap_{n\in\mathbb{N}}\bigcup_{k\geq n} A_k$$
(c'est l'ensemble des $x \in \Omega$ qui appartiennent à une infinité de A_n).
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. Notons $A = \limsup_{n\to+\infty} A_n = \bigcap_{n\in\mathbb{N}}\bigcup_{k\geq n} A_k$ et, pour tout entier naturel n, $B_n = \bigcup_{k\geq n} A_k$.

   (a) La suite $(B_n)_{n\in\mathbb{N}}$ étant décroissante, on a $\mathbb{P}(A) = \lim_{n\to+\infty} \mathbb{P}(B_n)$ avec :
   $$\mathbb{P}(B_n) \leq R_n = \sum_{k\geq n} \mathbb{P}(A_k)$$
   Dans le cas où la série $\sum \mathbb{P}(A_n)$ converge, on a $\lim_{n\to+\infty} R_n = 0$ et en conséquence, $\mathbb{P}\left(\limsup_{n\to+\infty} A_n\right) = 0$.

   (b) On a :
   $$\Omega \setminus \limsup_{n\to+\infty} A_n = \bigcup_{n\in\mathbb{N}} (\Omega \setminus B_n)$$
   la suite $(\Omega \setminus B_n)_{n\in\mathbb{N}}$ étant croissante, donc :
   $$1 - \mathbb{P}\left(\limsup_{n\to+\infty} A_n\right) = \lim_{n\to+\infty} \mathbb{P}(\Omega \setminus B_n)$$
   Pour tout entier $n \in \mathbb{N}$ et tout entier $m > n$, on a :
   $$\Omega \setminus B_n = \bigcap_{k\geq n} (\Omega \setminus A_k) \subset \bigcap_{k=n}^{m} (\Omega \setminus A_k)$$
   Dans le cas où les événements A_k sont mutuellement indépendants, il en est de même des $\Omega \setminus A_k$ et on a :
   $$\mathbb{P}\left(\bigcap_{k=n}^{m} (\Omega \setminus A_k)\right) = \prod_{k=n}^{m} \mathbb{P}((\Omega \setminus A_k)) = \prod_{k=n}^{m} (1 - \mathbb{P}(A_k))$$
   En utilisant l'inégalité $1 - x \leq e^{-x}$ pour tout réel x, on en déduit que :
   $$\mathbb{P}(\Omega \setminus B_n) \leq \prod_{k=n}^{m} (1 - \mathbb{P}(A_k)) \leq \exp\left(-\sum_{k=n}^{m} \mathbb{P}(A_k)\right)$$
   Dans le cas où $\sum_{n=0}^{+\infty} \mathbb{P}(A_n) = +\infty$, faisant tendre $m > n$ vers l'infini, on en déduit que $\mathbb{P}(\Omega \setminus B_n) = 0$ pour tout entier $n \in \mathbb{N}$ et en conséquence, $\mathbb{P}\left(\limsup_{n\to+\infty} A_n\right) = 1$.

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

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

Solution Supposons qu'il existe une mesure de probabilité $\mathbb{P}$ sur $(\mathbb{N}^*, \mathcal{P}(\mathbb{N}^*))$ telle que :

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

On a :

$$A = \limsup_{n \to +\infty} p_n \cdot \mathbb{N}^* = \bigcap_{n \in \mathbb{N} k \geq n} \bigcup p_k \cdot \mathbb{N}^* = \emptyset$$

(sinon, on aurait un entier $a \in \mathbb{N}^*$ divisible par une infinité de nombres premiers), donc $\mathbb{P}(A) = 0$.
Mais de $\sum_{n=1}^{+\infty} \mathbb{P}(p_n \cdot \mathbb{N}^*) = \sum_{n=1}^{+\infty} \frac{1}{p_n^\alpha} = +\infty$, les $p_n \cdot \mathbb{N}^*$ étant indépendants (Borel-Cantelli), on déduit que $\mathbb{P}(A) = 1$, soit une impossibilité.

8. 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^+ ?

Solution Pour tout entier $(n,m) \in \mathbb{N}^* \times \mathbb{N}^*$, on a $\mathbb{P}(\{(n,m)\}) > 0$ et :

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

donc $\mathbb{P}$ est bien une mesure de probabilité sur $(\mathbb{N}^* \times \mathbb{N}^*, \mathcal{P}(\mathbb{N}^* \times \mathbb{N}^*))$.
Dire qu'un couple (n,m) est formé de deux entiers premiers entre eux revient à dire qu'ils n'ont aucun facteur premier en commun, donc :

$$A = \bigcap_{n=1}^{+\infty} (\mathbb{N}^* \times \mathbb{N}^* \setminus p_n\mathbb{N}^* \times p_n\mathbb{N}^*)$$

et en notant $A_n = \bigcap_{k=1}^{n} (\mathbb{N}^* \times \mathbb{N}^* \setminus p_k\mathbb{N}^* \times p_k\mathbb{N}^*)$, on a :

$$\mathbb{P}(A) = \mathbb{P}\left(\bigcap_{n=1}^{+\infty} A_n\right) = \lim_{n \to +\infty} \mathbb{P}(A_n)$$

(suite décroissante d'événements) avec :

$$\begin{aligned}\mathbb{P}(A_n) &= \prod_{k=1}^{n} \mathbb{P}(\mathbb{N}^* \times \mathbb{N}^* \setminus p_k\mathbb{N}^* \times p_k\mathbb{N}^*) \\ &= \prod_{k=1}^{n} (1 - \mathbb{P}(p_k\mathbb{N}^* \times p_k\mathbb{N}^*))\end{aligned}$$

(les $p_k\mathbb{N}^* \times p_k\mathbb{N}^*$ sont indépendants).
Pour $(n,m) \in \mathbb{N}^* \times \mathbb{N}^*$, on a :

$$\begin{aligned}\mathbb{P}\left(n\mathbb{N}^* \times m\mathbb{N}^*\right) &= \mathbb{P}\left(\bigcup_{(j,k)\in\mathbb{N}^*\times\mathbb{N}^*} \{(jn,km)\}\right) = \sum_{(j,k)\in\mathbb{N}^*\times\mathbb{N}^*} \mathbb{P}\left(\{(jn,km)\}\right) \\ &= \frac{1}{\zeta^2(\alpha)}\frac{1}{(nm)^\alpha}\sum_{(j,k)\in\mathbb{N}^*\times\mathbb{N}^*}\frac{1}{(jk)^\alpha} = \frac{1}{(nm)^\alpha}\end{aligned}$$

donc :

$$\mathbb{P}(A) = \lim_{n\to+\infty}\prod_{k=1}^{n}\left(1-\frac{1}{p_k^{2\alpha}}\right) = \frac{1}{\zeta(2\alpha)} \underset{\alpha\to1^+}{\to} \frac{6}{\pi^2}$$