Problème de Mathématiques

Référence pp2110 — Version du 31 décembre 2025

On considère deux variables aléatoires X et Y définies sur un même espace probabilisé $(\Omega, \mathcal{A}, \mathbf{P})$. On suppose que ces deux variables aléatoires sont indépendantes et suivent toutes deux la loi uniforme sur $\mathbb{Z}/n\mathbb{Z}$:

$$\forall\, 0 \leqslant k < n, \quad \mathbf{P}\big(X = \mathscr{C}(k)\big) = \frac{1}{n}$$

où $\mathscr{C}(k)$ est la classe de k dans $\mathbb{Z}/n\mathbb{Z}$.

On rappelle que la série des inverses des nombres premiers est divergente : si $(p_k)_{k\geqslant 1}$ est la suite croissante des nombres premiers, alors la série $\sum {}^1/_{p_k}$ est divergente.

1. On note A, le fait que X soit inversible dans $\mathbb{Z}/n\mathbb{Z}$.

1. a. Vérifier que A est bien un événement.

1. b. Calculer la probabilité de A.

1. c. Comment choisir n pour que la probabilité de A soit supérieure à 99% ?

1. d. Comment choisir n pour que la probabilité de A soit inférieure à 1% ?

2. Calculer la loi de $X + Y$.

3. On admet que l'espérance et la variance conservent leurs propriétés habituelles avec les variables aléatoires à valeurs dans $\mathbb{Z}/n\mathbb{Z}$.

3. a. Déduire de la question précédente que

$$\mathbf{E}(X) = \mathbf{V}(X) = 0.$$

3. b. Commenter le résultat précédent.

3. c. Proposer une manière de décrire la valeur moyenne et la dispersion des valeurs d'une variable aléatoire à valeurs dans $\mathbb{Z}/n\mathbb{Z}$.

Solution ❀ Lois de probabilité sur $\mathbb{Z}/n\mathbb{Z}$

1. a. Comme X est une variable aléatoire définie sur l'espace probabilisé

$$(\Omega, \mathcal{A}, \mathbf{P})$$

à valeurs dans $\mathbb{Z}/n\mathbb{Z}$ (ensemble fini, donc naturellement muni de la tribu discrète $\mathcal{E} = \mathfrak{P}(\mathbb{Z}/n\mathbb{Z})$),

$$\forall\, 0 \leqslant k < n, \quad [X = \mathscr{C}_n(k)] \in \mathcal{A}.$$

D'après le cours, la valeur $X(\omega) \in \mathbb{Z}/n\mathbb{Z}$ est inversible si, et seulement si, il existe $1 \leqslant k < n$ premier à n tel que $X(\omega) = \mathscr{C}_n(k)$. Autrement dit :

$$A = [X \text{ est inversible}] = \bigcup_{\substack{1 \leqslant k < n \\ k \wedge n = 1}} [X = \mathscr{C}_n(k)].$$

Comme $\mathcal{A}$ est stable par union, on en déduit que

$$A \in \mathcal{A},$$

c'est-à-dire que A est bien un événement.

1. b. Comme

$$\big([X = \mathscr{C}_n(k)]\big)_{0 \leqslant k < n}$$

est un système complet d'événements, on a en fait décomposé A en une union d'événements deux à deux disjoints :

$$A = [X \text{ est inversible}] = \bigsqcup_{\substack{1 \leqslant k < n \\ k \wedge n = 1}} [X = \mathscr{C}_n(k)].$$

Par additivité de la mesure $\mathbf{P}$, on en déduit que

$$\mathbf{P}(A) = \sum_{\substack{1 \leqslant k < n \\ k \wedge n = 1}} \mathbf{P}(X = \mathscr{C}_n(k)).$$

Comme la loi de X est uniforme sur $\mathbb{Z}/n\mathbb{Z}$, ensemble fini de cardinal n, on en déduit que

$$\mathbf{P}(A) = \sum_{\substack{1 \leqslant k < n \\ k \wedge n = 1}} \frac{1}{n} = \frac{\#\big((\mathbb{Z}/n\mathbb{Z})^\times\big)}{n}$$

et donc, par définition de l'indicatrice d'Euler, que

$$\mathbf{P}(A) = \frac{\varphi(n)}{n}.$$

1. c. Si l'entier n est premier, alors on sait que

$$\varphi(n) = n - 1$$

et donc que

$$\mathbf{P}(A) = 1 - \frac{1}{n}.$$

Il suffit de choisir n premier supérieur à 100, par exemple $n = 101$, pour que $\mathbf{P}(A) \geqslant 99\%$.

1. d. La suite $(p_k)_{k \geqslant 1}$ entiers premiers énumérés par ordre croissant tend vers $+\infty$, donc

$$\ell n\Big(1 - \frac{1}{p_k}\Big) \underset{k \to +\infty}{\sim} \frac{-1}{p_k}.$$

Comme la série $\sum {}^1/_{p_k}$ est une série divergente de terme général positif, on en déduit que la série

$$\sum \ell n\Big(1 - \frac{1}{p_k}\Big)$$

est une série divergente de terme général négatif et donc que ses sommes partielles tendent vers $-\infty$.

Par conséquent, la suite de terme général

$$\ell n \prod_{k=1}^{N}\Big(1-\frac{1}{p_k}\Big)=\sum_{k=1}^{N}\ell n\Big(1-\frac{1}{p_k}\Big)$$

tend vers $-\infty$ et la suite de terme général

$$\prod_{k=1}^{N}\Big(1-\frac{1}{p_k}\Big)$$

tend vers 0.

Il est donc possible de choisir N assez grand pour que

$$\prod_{k=1}^{N}\Big(1-\frac{1}{p_k}\Big)\leqslant\frac{1}{100}.$$

Pour

$$n=\prod_{k=1}^{N}p_k,$$

on a donc

$$\mathbf{P}(A)=\frac{1}{n}\cdot\prod_{k=1}^{N}(p_k-1)=\prod_{k=1}^{N}\Big(1-\frac{1}{p_k}\Big)\leqslant\frac{1}{100}.$$

> *On peut démontrer que*
>
> $$\sum_{k=1}^{N}\frac{1}{p_k}\underset{N\to+\infty}{\sim}\ell n\,\ell n\,N$$
>
> *ce qui suggère que*
>
> $$\prod_{k=1}^{N}\Big(1-\frac{1}{p_k}\Big)\approx\exp(-\ell n\,\ell n\,N)=\frac{1}{\ell n\,N}$$
>
> *et donc que* $\mathbf{P}(A)\leqslant 10^{-2}$ *pour* $N\geqslant e^{100}\approx 2.10^{43}$*...*

2. Nous allons décomposer l'événement

$$[X+Y=\mathscr{C}_n(k)]$$

au moyen du système complet d'événements

$$\big([X=\mathscr{C}_n(i)]\big)_{0\leqslant i<n}.$$

Pour tout $0\leqslant k<n$, on a :

$$\begin{aligned}[X+Y=\mathscr{C}_n(k)]&=\bigsqcup_{i=0}^{n-1}[X+Y=\mathscr{C}_n(k)]\cap[X=\mathscr{C}_n(i)]\\&=\bigsqcup_{i=0}^{n-1}[X=\mathscr{C}_n(i)]\cap[Y=\mathscr{C}_n(k-i)].\end{aligned}$$

On a obtenu une union d'événements deux à deux disjoints. Par additivité de $\mathbf{P}$, on en déduit que

$$\begin{aligned}\mathbf{P}(X+Y=\mathscr{C}_n(k))&=\sum_{i=0}^{n-1}\mathbf{P}\big([X=\mathscr{C}_n(i)]\cap[Y=\mathscr{C}_n(k-i)]\big)\\&=\sum_{i=0}^{n-1}\mathbf{P}(X=\mathscr{C}_n(i)).\,\mathbf{P}(Y=\mathscr{C}_n(k-i))\\&=n\times\frac{1}{n^2}=\frac{1}{n}\end{aligned}$$

puisque les variables aléatoires X et Y sont indépendantes et suivent la loi uniforme sur $\mathbb{Z}/n\mathbb{Z}$.

On constate donc que la variable aléatoire $X+Y$ suit, comme X et Y, la loi uniforme sur $\mathbb{Z}/n\mathbb{Z}$.

3. a. Comme $X+Y$ suit la même loi que X, on a donc

$$\mathbf{E}(X+Y) = \mathbf{E}(X) \quad \text{et} \quad \mathbf{V}(X+Y) = \mathbf{V}(X).$$

❧ Par linéarité de l'espérance, on a aussi

$$\mathbf{E}(X+Y) = \mathbf{E}(X) + \mathbf{E}(Y) = 2\,\mathbf{E}(X)$$

puisque X et Y suivent la même loi. On en déduit que

$$\mathbf{E}(X) = 0.$$

❧ Comme X et Y sont indépendantes et suivent la même loi, on a aussi

$$\mathbf{V}(X+Y) = \mathbf{V}(X) + \mathbf{V}(Y) = 2\,\mathbf{V}(X).$$

On en déduit également que

$$\mathbf{V}(X) = 0.$$

3. b. C'est très étrange ! La variable X n'est pas constante et pourtant sa variance est nulle...

En fait, ni l'espérance, ni la variance ne sont définies pour les variables aléatoires étudiées ici ! En effet, $\mathbb{Z}/n\mathbb{Z}$ est muni d'une structure d'anneau, mais pas d'espace vectoriel, donc la formule usuelle

$$\mathbf{E}(X) = \sum_{k=0}^{n-1} \mathbf{P}(X = \mathscr{C}_n(k)).\mathscr{C}_n(k) = \frac{1}{n}\sum_{k=0}^{n-1} \mathscr{C}_n(k)$$

n'a pas de sens : on ne peut pas diviser par n dans $\mathbb{Z}/n\mathbb{Z}$ (d'une part, parce qu'il n'y a pas de division dans un anneau et d'autre part, parce que la classe $\mathscr{C}_n(n)$ est aussi la classe de 0 et n'est donc inversible dans $\mathbb{Z}/n\mathbb{Z}$ pour aucune valeur de n !)

L'espérance n'étant pas définie, on ne peut pas non plus donner un sens à la variance...

3. c. On sait que l'application

$$\mathscr{C}_n(k) \longmapsto \exp\frac{2ik\pi}{n}$$

réalise une bijection de $\mathbb{Z}/n\mathbb{Z}$ sur l'ensemble $\mathbb{U}_n$ des racines n-ièmes de l'unité.

On peut ainsi en quelque sorte transporter une loi de probabilité sur $\mathbb{Z}/n\mathbb{Z}$ vers une loi de probabilité sur $\mathbb{U}_n$. Comme $\mathbb{U}_n \subset \mathbb{C}$, on peut sans difficulté définir l'espérance selon les méthodes usuelles :

$$\mathbf{E}(X) = \sum_{k=0}^{n-1} e^{2ik\pi/n}.\mathbf{P}[X = \mathscr{C}_n(k)] \in \mathbb{C}$$

(et si X suit la loi uniforme sur $\mathbb{Z}/n\mathbb{Z}$, cette espérance est nulle).

La variance mérite une attention plus soutenue : il faut veiller à ce qu'elle soit nulle seulement pour une variable aléatoire presque sûrement constante ! On pourra donc poser

$$\mathbf{V}(X) = \mathbf{E}\left[\left|X - \mathbf{E}(X)\right|^2\right] \in \mathbb{R}_+$$

et par linéarité de l'espérance, la relation de Koenig-Huyghens devient alors

$$\mathbf{V}(X) = \mathbf{E}\left[|X|^2\right] - \left|\,\mathbf{E}(X)\right|^2.$$