Probabilités I

Table des matières

Introduction

La théorie des probabilités s'appelle ainsi car on est pas sur qu'elle existe...

Les mathématiques sont très pratiques pour étudier le monde réel, et beaucoup de concepts mathématiques sont utilisés en physique et en chimie. Cependant, les systèmes physiques et chimiques, entre autres, sont parfois trop complexes pour être appréhendés tels quels. On peut alors utiliser les probabilités comme une "approximation" de leurs comportements.

Par ailleurs, certains systèmes montrent des caracétistiques purement aléatoires, et là encore, l'étude des probabilités permet de faire des prédictions et des observations sur ces systèmes. Les probabilités sont également une partie intégrante des statistiques, dont l'usage est à la base de toute théorie scientifique moderne et rigoureuse.

Enfin, l'étude des probabilités en tant que telles, sans considérations pour le monde réel, a aussi été, et demeure, un moteur d'avancée dans les mathématiques modernes. Faisant appel à l'intuition et à la rigueur, l'étude des probabilités fait partie du bagage essentiel de tout scientifique, quelque soit la discipline.

Dans ce chapitre, nous allons nous concentrer sur les bases des probabilités : les cas d'univers finis, où les résultats de nos expériences ne peuvent prendre qu'un certain nombre, fini, de valeurs. Cependant, apporter à ces concepts une définition rigoureuse et un cadre d'étude bien défini nous permettra, d'une part, de développer des outils efficaces, et d'autre part, de généraliser ensuite nos résultats à des théories plus générales.

I - Entiers naturels et dénombrement

Faire des probabilités dans des ensembles finis nécessitera de savoir compter, de plusieurs manières souvent, les objets dont on parle. Pour cela, un peu de rappel de dénombrement, et donc d'arithmétique, sont d'usage.

1- Arithmétique élémentaire des entiers

1.a) Divisibilité dans $\mathbb{Z}$

Définition 1. Soient $a, b \in \mathbb{Z}^2$, on dit que a **divise** b (ou que b est *un multiple* de a), que l'on note $a \mid b$ sitôt que :

$$\exists n \in \mathbb{Z} \ / \ b = a \times n$$

Dans le cas contraire, si a ne divise pas b, on note $a \nmid b$.

Remarque 1.
- Quand $a|b$, on dit aussi que a est *un diviseur* de b.
- L'ensemble des multiples de a est noté $a\mathbb{Z} = \{b \in \mathbb{Z} \ / \ a \mid b\} = \{a.m \,,\ m \in \mathbb{Z}\}$

Exemple 1.
- $7 \mid 14$, $-6 \mid 24$, $2 \nmid 5$, ...
- 1 et -1 divisent tous les entiers : $\forall m \in \mathbb{Z},\ -1 \mid m$ et $1 \mid m$.
- 0 est multiple de tous les entiers.
- Les diviseurs de 18 sont : $\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18$

Proposition 1. Quelques résultats élémentaires :
- $a \mid b$ et $b \mid a \implies |a| = |b|$ (avec égalité si on prend $(a, b) \in \mathbb{N}$.
- $d \mid a$ et $d \mid b \implies \forall (u, v) \in \mathbb{Z}^2,\ d \mid au + bv$.
- $a \mid b$ et $b \mid c \implies a \mid c$
- $a \mid b \implies \forall k \in \mathbb{Z}^*,\ ak \mid bk$

Théorème 1. *Division Euclidienne*
*Soient $a \in \mathbb{Z}, b \in \mathbb{N}^*$. Il existe un **unique** couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :*

$$a = bq + r \text{ avec } 0 \leqslant r \leqslant b - 1$$

Définition 2. Appliquer le théorème précédent au couple d'entier (a, b) s'appelle *faire la division euclidienne* de a par b.
- On appelle q le **quotient** de la division euclidienne ;
- On appelle r le **reste** de la division euclidienne.

Définition 3. Congruence modulo n.
Soit $n \in \mathbb{N}^*$, et soient $(x, y) \in \mathbb{Z}$. On dit que x est **congru à** y **modulo** n, que l'on note $x \equiv y[n]$, sitôt que :

$$n \mid (x - y)$$

Proposition 2. La relation "être congru modulo n" est une *relation d'équivalence* sur $\mathbb{Z}$ (reflexive, symétrique, transitive), et elle est *compatible* avec $+$ et $\times$:

$$\left\{ \begin{array}{l} a \equiv b[n] \\ c \equiv d[n] \end{array} \right. \implies \left\{ \begin{array}{rcll} a + c & \equiv & b + d & [n] \\ ac & \equiv & bd & [n] \end{array} \right.$$

(L'ensemble des classes d'équivalences pour cette relation est noté $\mathbb{Z}/n\mathbb{Z}$, objet mathématique dont l'étude est fondamentale, mais en dehors du cadre de ce cours.

Exemple 2. $n \in \mathbb{Z}$ est pair $\Leftrightarrow n \equiv 0[2]$, et impair $\Leftrightarrow n \equiv 1[2]$.

1.b) PCGD, PPCM

Définition 4. Soit $(a_i)_{i\in[\![1;n]\!]} \in (\mathbb{N}^*)^n$ n entiers. Il existe alors un *plus grand entier naturel* d qui soit un diviseur de tous ces nombres à la fois. On dit que c'est le **plus grand diviseur commun** des $(a_i)_{i\in[\![1;n]\!]}$. On le note des manières suivantes :

$$d = \text{pgcd}((a_i)_{i\in[\![1;n]\!]}) = \text{pgcd}(a_1, \dots, a_n) = a_1 \wedge a_2 \wedge \cdots \wedge a_n = \bigwedge_{i=1}^{n} a_i$$

Remarque 2.

- Quand $a_1 \wedge a_2 = 1$, on dit que a_1 et a_2 sont **premier entre eux**.
- Quand $a_1 \wedge a_2 \wedge \cdots \wedge a_n = 1$, on dit que les a_i sont *premiers entre eux* **dans leur ensemble**.
- Quand $\forall (i,j) \in [\![1;n]\!],\ i \neq j \implies a_i \wedge a_j = 1$, on dit que les a_i sont *premiers entre eux* **deux à deux**.

Exemple 3.

$$4 \wedge 14 = 2 \qquad 13 \wedge 25 = 1 \qquad 6 \wedge 24 = 6$$

Proposition 3. Si une famille d'entiers naturels sont premiers deux à deux, alors ils sont premiers dans leur ensemble. (La réciproque n'est pas vraie).

Proposition 4. Soit $(a_i)_{i\in[\![1;n]\!]} \in (\mathbb{N}^*)^n$ n entiers et $d = \text{pgcd}((a_i)_{i\in[\![1;n]\!]})$.

- $m \mid d \Leftrightarrow \forall i \in [\![1;n]\!],\ m \mid a_i$
- $\forall m \in \mathbb{Z},\ \text{pgcd}((m \times a_i)_{i\in[\![1;n]\!]}) = |m|d$
- Si $a_1 = a_2 q + r$ est la division euclidienne de a_2 par a_1, alors $a_1 \wedge a_2 = a_2 \wedge r$.

Méthode 1. *Calcul du PGCD de deux nombres entiers par l'algorithme d'Euclide.*
On utilise le dernier point de la proposition précédente successivement, jusqu'à obtenir $r = 0$. Le PGCD est alors le dernier reste non nul.

Théorème 2. *de Bezout.*
Soit $(a_i)_{i\in[\![1;n]\!]} \in (\mathbb{N}^*)^n$ n entiers. Alors

$$\text{pgcd}((a_i)_{i\in[\![1;n]\!]}) = 1 \Leftrightarrow \exists (u_i)_{i\in[\![1;n]\!]}) \in \mathbb{Z}^n \ / \ u_1 a_1 + \cdots + u_n a_n = 1$$

Remarque 3. Lorsque deux entiers a et b sont premiers entre eux, on peut trouver les coefficient u, v tels que $au + bv = 1$ au moyen de l'algorithme d'Euclide :

Théorème 3. *de Gauss.*
Soient $a, b,$ et $c \in \mathbb{N}$,

$$a \mid bc \text{ et } a \wedge b = 1 \implies a \mid c$$

Proposition 5. Soient $a \in \mathbb{N}, (b_i)_{i\in[\![1;n]\!]} \in (\mathbb{N}^*)^n$ $n+1$ entiers.

- $\forall i \in [\![1;n]\!],\ a \wedge b_i = 1 \implies a \wedge (b_1 \times \cdots \times b_n) = 1$
- Si les (b_i) sont premiers entre eux deux à deux, alors :

$$\forall i \in [\![1;n]\!],\ b_i \mid a \Leftrightarrow b_1 \times \cdots \times b_n \mid a$$

Définition 5. Soit $(a_i)_{i\in[\![1;n]\!]} \in (\mathbb{N}^*)^n$ n entiers. Il existe alors un *plus petit entier naturel* m qui soit un multiple de tous ces nombres à la fois. On dit que c'est le **plus petit multiple commun** des $(a_i)_{i\in[\![1;n]\!]}$. On le note des manières suivantes :

$$m = \text{ppcm}((a_i)_{i\in[\![1;n]\!]}) = \text{ppcm}(a_1, \ldots, a_n) = a_1 \vee a_2 \vee \cdots \vee a_n = \bigvee_{i=1}^{n} a_i$$

Proposition 6. Soit $(a_i)_{i\in[\![1;n]\!]} \in (\mathbb{N}^*)^n$ n entiers et $m = \text{ppcm}((a_i)_{i\in[\![1;n]\!]})$.

- $k \mid m \Leftrightarrow \forall i \in [\![1;n]\!],\ k \mid a_i$
- $\forall m \in \mathbb{Z},\ \text{ppcm}((m \times a_i)_{i\in[\![1;n]\!]}) = |m|d$
- Si $\text{pgcd}((a_i)_{i\in[\![1;n]\!]}) = 1$, alors $\text{ppcm}((a_i)_{i\in[\![1;n]\!]}) = a_1 \times \cdots \times a_n$.

Théorème 4. *Soient $(a, b) \in \mathbb{N}^2$. Alors :*

$$\text{pgcd}(a, b) \times \text{ppcm}(a, b) = a \times b$$

1.c) Nombres premiers

Définition 6. Soit p un entier supérieur ou égal à deux. p est dit **premier** sitôt que :

$$\forall n \in \mathbb{N}, n \mid p \implies n = 1 \text{ ou } n = p$$

Remarque 4.

- 1 n'est pas un nombre premier.
- Tout entier $n \geqslant 2$ est divisible par un nombre premier.
- Si p est premier et $p \nmid a$ alors $p \wedge a = 1$

Théorème 5. *L'ensemble des nombres premiers est infini.*

Théorème 6. *Théorème fondamental de l'arithmétique.*
Soit $n \geqslant 2$ un entier, soit $\mathcal{P}$ l'ensemble des nombres premiers. Alors, il existe des entiers naturels $(\alpha_p)_{p\in\mathcal{P}}$ tels que :

$$n = \prod_{p\in\mathcal{P}} p^{\alpha_p}$$

*Cette **décomposition en produit de facteurs premiers** est unique (à l'ordre des facteurs près).*

Proposition 7. Soient a et b deux entiers naturels $\geqslant 2$, et soient leurs décomposition en produit de facteur premier :

$$a = \prod_{p\in\mathcal{P}} p^{\alpha_p} \text{ et } b = \prod_{p\in\mathcal{P}} p^{\beta_p}$$

alors :

$$a \wedge b = \prod_{p\in\mathcal{P}} p^{\min(\alpha_p,\beta_p)} \text{ et } a \vee b = \prod_{p\in\mathcal{P}} p^{\max(\alpha_p,\beta_p)}$$

Exercice I-1. Soit p un nombre premier et $k \in [\![0; p]\!]$. Montrer que $p \mid \dfrac{p!}{k!(p-k)!}$.

Exercice I-2. Determiner les triplets d'entier (a, b, c) tels que :

$$\begin{cases} a \vee b &= 42 \\ a \wedge c &= 3 \\ a+b+c &= 29 \end{cases}$$

Exercice I-3. Montrer que $\forall n \in \mathbb{N}$, on a $5 \mid (2^{3n+5} + 3^{n+1})$

Exercice I-4. Montrer que si a est un entier et $a^n - 1$ est premier, alors $a = 2$ et n est un nombre premier.