

Feuille X : Raisins dans Kougelhof ?¹

Exercice 1. Pour $n \in \mathbb{N}^*$, posons $a_n = \sum_{k=1}^n \frac{(-1)^{n-1}}{n}$. Cette exercice est composé de 2 parties.

1. Ici, nous allons calculer la limite $\lim_{n \rightarrow \infty} a_n$.

(i) Pour tout $x \in [0; +\infty[$ et $n \in \mathbb{N}$, montrer l'identité $\sum_{k=1}^n (-x)^{k-1} = \frac{1 - (-x)^n}{1 + x}$.

(ii) En déduire l'identité suivante: $\sum_{k=1}^n \frac{(-1)^{k-1}}{k} = \ln 2 + (-1)^{n-1} \int_0^1 \frac{x^n}{1+x} dx$.

(iii) Montrer que $0 \leq \frac{x^n}{1+x} \leq x^n$ pour tout $x \in [0; 1]$. En déduire la limite $\lim_{n \rightarrow \infty} \int_0^1 \frac{x^n}{1+x} dx$.

(iv) Conclure.

2. Fixons $p, q \in \mathbb{N}^*$, et on pose $b_n = \sum_{k=1}^{pn} \frac{1}{2k-1} - \sum_{k=1}^{qn} \frac{1}{2k}$. Dans cette partie, on admet que la suite

$c_n = \sum_{k=1}^n \frac{1}{k} - \ln n$ converge à la constante appelée la **constante d'Euler-Mascheroni**, notons la par C .

(i) Montrer que $b_n = c_{2pn} - \frac{1}{2}c_{pn} - \frac{1}{2}c_{qn} + \ln 2 + \frac{1}{2}(\ln p - \ln q)$ pour tout $n \in \mathbb{N}^*$.

(ii) En déduire la limite $\lim_{n \rightarrow \infty} b_n$.

(iii) Que peut-on observer ?

Exercice 2. (Une suite logistique) Soit μ un nombre réel tel que $0 < \mu \leq 4$. Une suite réelle $\{x_n\}_{n \in \mathbb{N}}$ définie par

$$x_{n+1} = \mu x_n(1 - x_n), \quad x_0 \in [0; 1]$$

est appelée une **suite logistique**.

1. Montrer que pour tout $n \in \mathbb{N}$, x_n appartient à l'intervalle $[0; 1]$.

2. Montrer que pour $0 < \mu < 1$, $\lim_{n \rightarrow \infty} x_n = 0$.

3. Supposons que $\mu = 4$. Soit $a \in \mathbb{R}$ un nombre réel vérifiant $x_0 = \sin^2(a\pi)$.

(i) Déterminer x_n pour tout $n \in \mathbb{N}$.

(ii) Peut-on déterminer les valeurs de a vérifiant $\lim_{n \rightarrow \infty} x_n = 0$?

4. Que peut-on observer dans des cas $1 \leq \mu < 4$? On pourra programmer pour faire une expérience... à vous de voir !

Exercice 3. (Principe d'inclusion-exclusion) Soit E un ensemble et soient $A_1, A_2, \dots, A_n$ ($n \in \mathbb{N}^*$) des ensembles finis.

1. Ici, on va exprimer $\text{Card} \left(\bigcup_{i=1}^n A_i \right)$ en fonction des intersections de A_i ($1 \leq i \leq n$).

(i) Montrer la formule $\text{Card}(A_1 \cup A_2) = \text{Card}(A_1) + \text{Card}(A_2) - \text{Card}(A_1 \cap A_2)$.

(ii) Montrer la formule suivante par récurrence :

$$\text{Card} \left(\bigcup_{i=1}^n A_i \right) = \sum_{r=1}^n (-1)^{r-1} \sum_{1 \leq i_1 < i_2 < \dots < i_r \leq n} \text{Card} \left(\bigcap_{k=1}^r A_{i_k} \right).$$

1. Une expression inspirée du mathématicien Jean-Pierre Serre.

2. Soit $n \in \mathbb{N}^*$ et soit $\mathfrak{S}_n$ l'ensemble des applications bijectives de $\llbracket 1, n \rrbracket := \{1, 2, \dots, n\}$ vers lui-même. Soit x_n le nombre des applications $f \in \mathfrak{S}_n$ pour laquelle il n'existe pas $i \in \llbracket 1, n \rrbracket$ tel que $f(i) = i$.
- (i) Pour $i \in \llbracket 1, n \rrbracket$, soit S_i l'ensemble des applications $f \in \mathfrak{S}_n$ vérifiant $f(i) = i$. Montrer que

$$x_n = \text{Card}(\mathfrak{S}_n) - \text{Card}\left(\bigcup_{i=1}^n S_i\right).$$

- (ii) Soit $r \in \llbracket 1, n \rrbracket$. Pour les entiers $1 \leq i_1 < i_2 < \dots < i_r \leq n$, Calculer $\text{Card}(S_{i_1} \cap S_{i_2} \cap \dots \cap S_{i_r})$.
- (iii) Conclure.

Exercice 4. ($\mathbb{N}$ et $\mathbb{R}$) Ici, on va comparer les cardinaux de $\mathbb{N}$ et $\mathbb{R}$.

- Donner un exemple d'une application bijective f entre l'intervalle $]0, 1[$ et $\mathbb{R}$.
- Soit $g :]0, 1[\rightarrow]0, 1[$ une fonction définie par

$$g(x) = \begin{cases} 2x & \text{si } \exists n \in \mathbb{N}^* \text{ t.q. } x = \frac{1}{2^n}, \\ x & \text{sinon.} \end{cases}$$

Montrer que g est une application bijective. En conclure que l'intervalle $]0, 1[$ et l'ensemble $\mathbb{R}$ ont la même cardinalité.

D'ici, on va montrer qu'il n'existe pas une application surjective de $\mathbb{N}^*$ vers $]0, 1[$. Pour cela, on exprime un nombre réel $x \in]0, 1[$:

$$x = \sum_{k=1}^{\infty} \frac{x_k}{10^k}, \quad x_k \in \mathbb{Z} \cap [0, 9].$$

Comme $1 = 0,99999999\dots$, pour un nombre x admettant un $N \in \mathbb{N}^*$ tel que $x_N \neq 0$ et $x_l = 0$ pour tout $l > N$, on adopte l'expression

$$x = \sum_{k=1}^{N-1} \frac{x_k}{10^k} + \frac{x_N - 1}{10^N} + \sum_{k=N+1}^{\infty} \frac{9}{10^k}.$$

Soit $F : \mathbb{N}^* \rightarrow]0, 1[$ une application. Pour $n \in \mathbb{N}^*$, notons le développement décimal de $F(n)$ par

$$\sum_{k=1}^{\infty} \frac{a_k^n}{10^k}.$$

- Définissons la suite des entiers positifs $\{b_k\}_{k \in \mathbb{N}^*}$ par

$$b_k = \begin{cases} 1 & \text{si } a_n^n \text{ est paire,} \\ 2 & \text{si } a_n^n \text{ est impaire.} \end{cases}$$

Vérifier qu'il n'existe pas $n \in \mathbb{N}^*$ tel que $F(n) = \sum_{k=1}^{\infty} \frac{b_k}{10^k}$.

- En déduire qu'il n'existe pas une application surjective entre $\mathbb{N}$ et $\mathbb{R}$.

Exercice 5. (Fraction continue) Fixons un nombre réel $x \in \mathbb{R}$.

Posons $q_0 = \lfloor x \rfloor$, la partie entière de x , i.e., le plus grand entier qui est inférieur ou égale à x . Par définition, on a $0 \leq x - \lfloor x \rfloor < 1$. Si ce dernier $x - \lfloor x \rfloor$ n'est pas nul, le nombre $x_1 := \frac{1}{x - \lfloor x \rfloor}$ est un réel plus grand que 1 et on a

$$x = \lfloor x \rfloor + (x - \lfloor x \rfloor) = q_0 + \frac{1}{\frac{1}{x - \lfloor x \rfloor}} = q_0 + \frac{1}{x_1}.$$

Posons $q_1 := \lfloor x_1 \rfloor$. Si $x_1 - q_1 = 0$, on s'arrête ici. Sinon, on répète la même chose. Comme $0 < x_1 - q_1 < 1$, le nombre $x_2 := \frac{1}{x_1 - q_1}$ est un réel plus grand que 1 et on a

$$x = q_0 + \frac{1}{x_1} = q_0 + \frac{1}{q_1 + (x_1 - q_1)} = q_0 + \frac{1}{q_1 + \frac{1}{x_2}}.$$

... Posons $q_n = \lfloor x_n \rfloor$ et $x_{n+1} = \frac{1}{x_n - q_n}$ si x_n n'est pas entier. On a

$$x = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\ddots \frac{1}{q_n + \frac{1}{x_{n+1}}}}}}.$$

On notera cette fraction monstrueuse comme $[q_0, q_1, q_2, \dots, q_n, x_{n+1}]$.

1. Ici, on montre que x est un nombre rationnel si et seulement si la procédure ci-dessus se termine en nombre fini d'étape.

(0) Vérifier que s'il existe $q_0, q_1, \dots, q_n \in \mathbb{Z}$ tels que $x = [q_0, q_1, \dots, q_n]$ et que $q_1, q_2, \dots, q_n$ soient strictement positifs, alors, x est un nombre rationnel.

(i) Soient $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ tels que $x = \frac{p}{q}$ et que p et q sont premiers entre eux, et soient $p_1, q_1 \in \mathbb{N}^*$ tels que $x_1 = \frac{p_1}{q_1}$ et que p_1 et q_1 sont premiers entre eux. Montrer que $0 < q_1 < q$.

(ii) En déduire que si x est un nombre rationnel, la procédure ci-dessus (pour définir les q_i) se termine en nombre fini d'étape.

2. Pour $x = \sqrt{2}, \sqrt{3}$ et $x = \frac{1 + \sqrt{5}}{2}$ (le nombre d'or), déterminer la suite $\{q_n\}_{n \in \mathbb{N}}$. Si cela vous plait, déterminer la suite $\{q_n\}_{n \in \mathbb{N}}$ pour $x = \sqrt{199}$.

3. Sont-ils rationnels ?

Exercice 6. (Projection stéréographique) Soit $\mathbb{S}$ la sphère d'unité $\{(x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 = 1\}$. Posons $N = (0, 0, 1) \in \mathbb{S}$. Pour un point $P \in \mathbb{S} \setminus \{N\}$, soit l_P la droite passant les deux points N et P . Nous allons étudier l'application

$$\pi : \mathbb{S} \setminus \{N\} \longrightarrow \Pi := \{(x, y, 0) \mid x, y \in \mathbb{R}\}; \quad P \longmapsto Q,$$

où $Q \in \Pi$ est le point vérifiant $\{Q\} = \Pi \cap l_P$, c'est-à-dire, l'intersection de la droite l_P et le plan Π . Une telle application s'appelle une **projection stéréographique**.²

1. Soit $l \subset \Pi$ une droite et soit Π_l le plan (dans $\mathbb{R}^3$) incluant le point N et la droite l .

2. On pourra définir une application similaire en prenant $S := (0, 0, -1)$ à la place du point N .

- i) Vérifier que l'image réciproque $\pi^{-1}(l)$ est égale à l'intersection de $\mathbb{S} \setminus \{N\}$ et le plan Π_l .
- ii) En déduire que $\pi^{-1}(l)$ est un cercle privé du point N .
2. Pour un point $Q = (x, y, 0)$, calculer son image réciproque $P = \pi^{-1}(Q)$.
(Indication: la droite passant les points N et Q est paramétrée comme suit : $(0, 0, 1) + t(-x, -y, 1)$.)
3. Soit $C \subset \Pi$ un cercle, i.e., $C = \{ (x, y, 0) \mid (x - a)^2 + (y - b)^2 = R^2 \}$ où $(a, b) \in \mathbb{R}^2$ et $R \in \mathbb{R}_+^*$.
- i) Pour $Q \in C$, vérifier que l'image réciproque $P = (X, Y, Z) \in \mathbb{S}$ du point Q par π vérifie l'équation suivante :
- $$-2aX - 2bY + (R^2 - a^2 - b^2)Z = R^2 - a^2 - b^2 - 1.$$
- ii) En déduire que l'image réciproque du cercle C par π est un cercle.

Ainsi, une droite ou un cercle dans le plan $\mathbb{R}^2$, donc dans $\mathbb{C}$ via la correspondance $(a, b) \longleftrightarrow a + bi$, correspond à un cercle (privé à un point, au maximum) sur la sphère $\mathbb{S}$. Que dit-on le résultat (de cours) sur la transformation de Möbius, alors ?

Exercice 7. (Petit théorème de Fermat) On donne deux preuves du petite théorème de Fermat.

1. Soit p un nombre premier supérieur à 2.
- (i) Pour tout entier k entre 1 et $p - 1$, montrer que le coefficient binomial $\binom{p}{k}$ est divisible par p .
- (ii) Montrer, par récurrence, que $p \mid a^p - a$ pour tout entier naturel a .
- (iii) En déduire que si a et p sont premier entre eux, $a^{p-1} - 1$ est divisible par p .
2. Soient p un nombre premier et $a \in \mathbb{N}$ un entier qui n'est pas divisible par p . Posons $R_p = \{1, 2, \dots, p-1\}$. Soit $f : R_p \rightarrow R_p$ l'application définie par $f(i) = j$ où j est l'élément de R_p vérifiant $ai \equiv j \pmod{p}$.
- (i) Montrer que l'application f est bijective. Indication : Montrer que f est injective.
- (ii) Montrer que $a^{p-1}(p-1)!$ est congru à $(p-1)!$ modulo p .
Indication : Montrer que $a^{p-1}(p-1)! \equiv f(1) \cdot f(2) \cdots f(p-1) \pmod{p}$ et en déduire.
- (iii) En déduire que $a^{p-1} \equiv 1 \pmod{p}$.

Exercice 8. (Théorème de Wilson)

Soit p un nombre premier. Le but de cet exercice est de montrer le théorème de Wilson :

$$(p-1)! \equiv -1 \pmod{p}.$$

Pour $p = 2$, c'est immédiat, donc on suppose que $p > 2$ dans la suite. Posons

$$R_p = \{ n \in \mathbb{N} \mid 0 < n < p \} = \{1, 2, \dots, p-1\}.$$

1. Soit $i : R_p \longrightarrow R_p$ qui associe k à l vérifiant $kl \equiv 1 \pmod{p}$.
- i) Montrer que l'application i est bien-définie.
- ii) Montrer que l'application i est bijective.
2. Montrer qu'il existe deux éléments de R_p , disons x_+ et x_- , tels que $i(x_{\pm}) = x_{\pm}$. Préciser-les.
(Indication : $i(x) = x$ implique $x^2 - 1 = (x+1)(x-1) \equiv \cdots [p]$.)
3. Posons $S_p = R_p \setminus \{x_+, x_-\}$. On considère l'application $I : S_p \rightarrow S_p$ définie par $I(x) = i(x)$.
- i) Montrer que l'application I est bien-définie.
- ii) Montrer qu'il existe $\tilde{S}_p \subset S_p$ tel que $S_p = \tilde{S}_p \sqcup I(\tilde{S}_p)$.
4. En déduire que

$$(p-1)! = \prod_{x \in R_p} x = (x_+ x_-) \prod_{x \in \tilde{S}_p} (x I(x)).$$

5. Conclure.

- Exercice 9.** 1. Soit n un entier plus grand que 1. Montrer que l'entier n est un nombre premier si et seulement si tout nombre premier, qui ne dépasse pas $\sqrt{n}$, ne divise pas n .
2. (**L. Euler**) Vérifier que, pour tout entier $0 \leq n < 40$, l'entier $n^2 + n + 41$ est un nombre premier et que pour $n = 40$ et 41 , ils ne le sont pas.
3. Existe-t-il un entier K tel que $n^2 + n + K$ est un nombre premier pour tout $n \in \mathbb{N}$ sauf $n = K - 1$, K ? Justifier votre réponse.

Exercice 10. (Principe de RSA) Soient $p, q \in \mathbb{N}^*$ deux nombres premiers distincts > 2 . Posons

$$R = \{n \in \mathbb{N} \mid 0 < n < pq \text{ et } \text{PGCD}(n, pq) = 1 \exists m \in R \text{ t.q. } \text{PGCD}(mn, pq) = 1\}.$$

- Calculer le nombre M d'éléments de R .
- Soit $a \in R$. Pour $i \in R$, montrer qu'il existe $j \in R$ tel que $ai \equiv j \pmod{pq}$.
Dans la suite, on considère l'application $f : R \rightarrow R$ définie par $f(i) = j$.
- Montrer que f est injective. En déduire que f est bijective.
- En déduire qu'il existe $m \in \mathbb{N}^*$ tel que $m \leq M$ et que $f^m = \text{Id}_R$.
(Indication : Pour $i \in R$, étudier la partie $R_i = \{f^k(i) \mid k = 1, 2, \dots\}$ de R .)
- Montrer que l'entier m de la question précédent est un diviseur de M .
- En déduire que, pour tout $a \in R$, on a $a^M \equiv 1 \pmod{pq}$.

- Exercice 11.** 1. Soit $n \in \mathbb{N}$ un nombre impaire. Montrer qu'il existe un polynôme réel $F_n(y) \in \mathbb{R}[y]$ tel que $F_n(\sin x) = \sin nx$.
2. Posant $n = 2m + 1$. En analysant les zéros du polynôme F_n , vérifier que le polynôme $F_n(y)$ est un multiple de

$$y \prod_{j=1}^m \left(1 - \frac{y^2}{\sin^2\left(\frac{j}{n}\pi\right)}\right).$$

3. En déduire la formule suivante :

$$\sin nx = n \sin x \prod_{j=1}^m \left(1 - \frac{\sin^2 x}{\sin^2\left(\frac{j}{n}\pi\right)}\right).$$

Exercice 12. Soit $n \in \mathbb{N}^*$. Posons $\mathcal{P}_n := \{P \in \mathbb{R}[X] \mid P \text{ est unitaire de degré } n\}$. Le but de cet exercice est de montrer

$$\min_{P \in \mathcal{P}_n} \max_{x \in [-1, 1]} |P(x)| = \frac{1}{2^{n-1}}.$$

- On définit une suite de polynômes $T_n \in \mathbb{R}[X] : T_0 = 1, T_1 = X, T_{n+2} = 2XT_{n+1} - T_n$ pour $n \in \mathbb{N}$.
(i) Montrer que le polynôme T_n est un polynôme de degré n .
(ii) Montrer que $T_n(\cos \theta) = \cos(n\theta)$ pour tout $n \in \mathbb{N}^*$.
Le polynôme T_n est appelé **polynôme de Tchebyscheff** de degré n .

- Montrer que $Q_n := \frac{1}{2^{n-1}}T_n \in \mathcal{P}_n$.

- Montrer que $\max_{x \in [-1, 1]} |Q_n(x)| = \frac{1}{2^{n-1}}$ et que

$$\left\{x \in [-1, 1] \mid |Q_n(x)| = \frac{1}{2^{n-1}}\right\} = \left\{\cos\left(\frac{\pi k}{n}\right) \mid k = 0, 1, \dots, n\right\}.$$

- Conclure.

Indication : Montre par l'absurde, i.e., supposons qu'il existe $P \in \mathcal{P}_n$ tel que $\max_{x \in [-1, 1]} |P(x)| < \frac{1}{2^{n-1}}$.
Compter le nombre de zéros de $P - Q_n$ dans $[-1, 1]$ en appliquant le théorème des valeurs intermédiaires.