Chapitre 6

Somme, produit, petits systèmes linéaires, arithmétique

Dans ce chapitre, nous allons voir les sommes et les produits, les petits systèmes linéaires et des bases d'arithmétique.

Table des matières

1 Sommes et Produits

1.1 Définitions et propriétés

Définition d'une famille

Soit I un ensemble fini. Si pour tout $i \in I$, on dispose d'un élément a_i, alors, la collection de tous ces a_i est appelée **famille finie indexée** par I et est notée $(a_i)_{i\in I}$.

Définition de la somme et du produit d'une famille

Soit I un ensemble fini $(a_i)_{i\in I}$ une famille de complexes. On note, $\sum\limits_{i\in I} a_i$ la somme des éléments de la famille $(a_i)_{i\in I}$ et $\prod\limits_{i\in I} a_i$ le produit des éléments de la famille $(a_i)_{i\in I}$. Par **convention**, si $I = \varnothing$, $\sum\limits_{i\in I} a_i = 0$ et $\prod\limits_{i\in I} a_i = 1$.

Exemple 1. Si $I = \{3; 5; 7; 11\}$, $a_3 = 5$, $a_5 = 6$, $a_7 = 7$ et $a_{11} = 7$, alors $\sum\limits_{i\in I} a_i =$ et $\prod\limits_{i\in I} a_i =$.

Remarque 1. Si $I = [\![m\,;n]\!] = \{m; m+1; \dots; n-1; n\}$ avec $m \leqslant n$, on note aussi

$$\sum_{i=m}^{n} a_i = a_m + a_{m+1} + \cdots + a_n \qquad \text{et} \qquad \prod_{i=m}^{n} a_i = a_m \times a_{m+1} \times \cdots \times a_n \qquad (n-m+1 \text{ termes})$$

Remarque 2. L'indice i est un indice «muet» : on peut le remplacer par n'importe quel autre symbole non encore utilisé :

$$\sum_{i=m}^{n} a_i = \sum_{j=m}^{n} a_j = \sum_{k=m}^{n} a_k \quad \text{et} \quad \prod_{i=m}^{n} a_i = \prod_{j=m}^{n} a_j = \prod_{k=m}^{n} a_k$$

Proposition n° 1 : règles de calculs pour la somme (linéarité de la somme) et le produit

Soient I un ensemble fini à p éléments $(a_i)_{i\in I}$, $(b_i)_{i\in I}$ deux familles de nombres de $\mathbb{C}$ et $\lambda \in \mathbb{C}$:

$$\sum_{i\in I}(a_i + b_i) = \sum_{i\in I} a_i + \sum_{i\in I} b_i \qquad \text{et} \qquad \sum_{i\in I}(\lambda a_i) = \lambda \sum_{i\in I} a_i$$

$$\prod_{i\in I}(a_i b_i) = \left(\prod_{i\in I} a_i\right) \times \left(\prod_{i\in I} b_i\right) \qquad \text{et} \qquad \prod_{i\in I}(\lambda a_i) = \lambda^p \prod_{i\in I} a_i$$

Exemple 2. Calculer la somme $\sum\limits_{k=0}^{n} 1$ et le produit $\prod\limits_{k=0}^{n} 2$.

Exemple 3. $\sum\limits_{k=1}^{n} k^2 = \dfrac{n(n+1)(2n+1)}{6}$.

1.2 Méthodes de calculs

Changement d'indice

Pour effectuer un changement d'indice, on définit le nouvel indice (entier) en fonction de l'ancien indice. Puis on exprime la somme avec ce nouvel indice en veillant à changer les bornes de la somme et le terme sous la somme en fonction du nouvel indice.
Formellement, si $\varphi \colon J \to I$ est une bijection entre deux ensembles finis, $\sum\limits_{j\in J} a_{\varphi(j)} = \sum\limits_{i\in I} a_i$.

Exemple 4. Faites un changement d'indice dans $\sum_{k=0}^{n-1} u_{k+1}$ et $\sum_{k=0}^{n} u_{n-k}$.

Exemple 5. À l'aide du changement d'indice $j = n - k$, retrouver la valeur de la somme $S_n = \sum_{k=0}^{n} k$.

Exemple 6. $(a_3 - a_2) + (a_4 - a_3) + (a_5 - a_4) =$ si a_2, a_3 et a_4 sont non nuls, $\frac{a_3}{a_2} \times \frac{a_4}{a_3} \times \frac{a_5}{a_4} =$

Proposition n° 2 : somme et produit télescopiques

Soit $(a_k)_{m \leqslant k \leqslant n+1}$ une famille de nombres, $\sum_{k=m}^{n} (a_{k+1} - a_k) = a_{n+1} - a_m$, si tous a_i sont non nuls, $\prod_{i=m}^{n} \frac{a_{i+1}}{a_i} = \frac{a_{n+1}}{a_m}$.

Exemple 7. Calculer la somme $S_n = \sum_{k=1}^{n} \frac{1}{k(k+1)}$. En déduire la limite de la suite $(S_n)_n$.

Exemple 8. Calculer le produit $P_n = \prod_{k=2}^{n} \left(1 - \frac{1}{k}\right)$.

Regroupement de termes

On décompose la somme de départ en plusieurs sommes plus simples à calculer.
Formellement, si $I = J \cup K$ avec J et K disjoints, alors $\sum_{i \in I} a_i = \sum_{j \in J} a_j + \sum_{k \in K} a_k$.

Exemple 9. Couper la somme $\sum_{k=1}^{2n} u_k$ en deux sommes contenant le même nombres de termes. Couper la somme $\sum_{k=1}^{2n+1} u_k$ en isolant le terme au milieu.

Exemple 10. Calculer la somme $S_n = \sum_{k=0}^{2n} \min(k, n)$, où $\min(k, n)$ est le minimum des entiers k et n.

Remarque 3. Soit $(z_k)_{k \in I}$ une famille finie de complexes, alors $\mathrm{Re}(\sum_{k \in I} z_k) = \sum_{k \in I} \mathrm{Re}(z_k)$ et $\mathrm{Im}(\sum_{k \in I} z_k) = \sum_{k \in I} \mathrm{Im}(z_k)$

Proposition n° 3 : somme de termes d'une suite arithmétique

Si $(u_n)_{n \in \mathbb{N}}$ est une suite arithmétique, alors pour $n \geqslant m$:

$$\sum_{k=m}^{n} u_k = \frac{u_m + u_n}{2} \times (n - m + 1) = \frac{\text{premier terme} + \text{dernier terme}}{2} \times (\text{nombre de termes})$$

Exemple 11. Calculer $\sum_{k=0}^{n} k$.

Proposition n° 4 : somme de termes d'une suite géométrique

Si $(u_n)_{n \in \mathbb{N}}$ est une suite géométrique de raison $q \neq 1$, alors :

$$\sum_{k=m}^{n} u_k = u_m \times \frac{1 - q^{n-m+1}}{1 - q} = \text{premier terme} \times \frac{1 - \text{raison}^{\text{nombre de termes}}}{1 - \text{raison}}$$

Dans le cas où $q = 1$ (suite constante), $\sum_{k=m}^{n} u_k = (n - m + 1) u_m$.

Exemple 12. Calculer $S_n = \sum\limits_{k=0}^{n} 2^{-k}$, en déduire la limite de la suite $(S_n)_n$.

Exemple 13. Pour $x \in \mathbb{C}$, calculer $S_n = \sum\limits_{i=1}^{n} x^i$.

Exemple 14. Soit $n \in \mathbb{N}^*$, calculer la somme des racines n-ièmes de l'unité.

Calcul de somme de cosinus/sinus

Soit $\theta \in \mathbb{R}$, calculer $\sum\limits_{k=0}^{n} \cos(k\theta)$ et $\sum\limits_{k=0}^{n} \sin(k\theta)$

Exemple 15. $(a-b)(a+b) =$ $\qquad$ $(a-b)(a^2+ab+b^2) =$ $\qquad$ $(a-b)(a^3+a^2b+ab^2+b^3) =$

Proposition n° 5 : identité remarquable

Soit $n \in \mathbb{N}$, a et b deux nombres réels ou complexes. Alors :

$$a^n - b^n = (a-b)\left(\sum_{k=0}^{n-1} a^k b^{n-1-k}\right)$$

1.3 Sommes doubles

Définition

Soient I et J deux ensembles finis et $(a_{i,j})_{(i,j)\in I\times J}$ une famille finie de nombres complexes. On note $\sum\limits_{(i,j)\in I\times J} a_{i,j}$ la **somme double des éléments** de la famille $(a_{i,j})_{(i,j)\in I\times J}$.

Si $I = [\![m\,;n]\!]$ et $J = [\![p\,;q]\!]$, on note $\sum\limits_{\substack{m\leqslant i\leqslant n\\ p\leqslant j\leqslant q}} a_{i,j}$ au lieu de $\sum\limits_{(i,j)\in I\times J} a_{i,j}$. Si $I = J = [\![m\,;n]\!]$, on note $\sum\limits_{m\leqslant i,j\leqslant n} a_{i,j}$.

Proposition n° 6 : somme double indexée par un rectangle

Soient m, n, p, q des entiers et $(a_{i,j})_{i,j}$ une famille de complexes indexée par le rectangle $[\![m\,;n]\!] \times [\![p\,;q]\!]$. Alors :

$$\sum_{\substack{m\leqslant i\leqslant n\\ p\leqslant j\leqslant q}} a_{i,j} = \sum_{i=m}^{n}\left(\sum_{j=p}^{q} a_{i,j}\right) = \sum_{j=p}^{q}\left(\sum_{i=m}^{n} a_{i,j}\right)$$

Proposition n° 7 : somme double indexée par un triangle

Soient m et n des entiers et $(a_{i,j})_{i,j}$ une famille de complexes indexée par le triangle $\{(i,j) \mid m \leqslant i \leqslant j \leqslant n\}$. Alors :

$$\sum_{m\leqslant i\leqslant j\leqslant n} a_{i,j} = \sum_{i=m}^{n}\left(\sum_{j=i}^{n} a_{i,j}\right) = \sum_{j=m}^{n}\left(\sum_{i=m}^{j} a_{i,j}\right)$$

Exemple 16. Calculer $S_n = \sum\limits_{1\leqslant i\leqslant j\leqslant n} \dfrac{i}{j}$.

Remarque 4. Les résultats précédents s'étendent si on remplace somme double par produit double.

Théorème n° 1 : produit de deux sommes

Soient $(a_i)_{1\leqslant i\leqslant n}$ et $(b_j)_{1\leqslant j\leqslant p}$ deux familles de nombres complexes : $\sum\limits_{i=1}^{n} a_i \times \sum\limits_{j=1}^{p} b_j = \sum\limits_{i=1}^{n}\sum\limits_{j=1}^{p} a_i b_j = \sum\limits_{j=1}^{p}\sum\limits_{i=1}^{n} a_i b_j$

Remarque 5. Calculer $(a+b+c)^2$, puis développer $(a_1+\ldots+a_n)^2$

1.4 Factorielle, coefficient binomial, binôme de Newton

Définition de la factorielle

Soit $n\in\mathbb{N}$. On appelle **factorielle n** et on note $n!$ l'entier $n! = \prod_{k=1}^{n} k$.

Exemple 17. Donner les valeurs de $1! =$ $2! =$ $3! =$ $4! =$ $5! =$ $0! =$

Remarque 6. Pour tout $n\in\mathbb{N}$, $(n+1)! = (n+1)\times n!$

Définition du coefficient binomial

Soit $(n,p)\in\mathbb{N}\times\mathbb{Z}$. On pose $\binom{n}{p} = \begin{cases} \dfrac{n!}{p!(n-p)!} & \text{si } p\in[\![0\,;n]\!] \\ 0 & \text{sinon}\end{cases}$ le **coefficient binomial** et se lit «p parmi n».

Exemple 18. Pour n dans $\mathbb{N}$ avec $n\geqslant 2$, donner les valeurs de $\binom{n}{0}$, $\binom{n}{1}$, $\binom{n}{2}$, $\binom{n}{n-1}$ et $\binom{n}{n}$.

Proposition n° 8 : propriétés des coefficients binomiaux

Soit n un entier naturel non nul.

1. Pour tout $p\in[\![0\,;n]\!]$, $\binom{n}{p}=\binom{n}{n-p}$ (symétrie des coefficients binomiaux)
2. Pour tout $p\in[\![1\,;n]\!]$, $p\times\binom{n}{p} = n\times\binom{n-1}{p-1}$ (formule du maire)
3. Pour tout $p\in[\![1\,;n-1]\!]$, $\binom{n}{p}=\binom{n-1}{p-1}+\binom{n-1}{p}$ (formule du triangle de Pascal)

Remarque 7. La formule du triangle de Pascal permet le calcul des coefficients binomiaux et montre que $\binom{n}{p}\in\mathbb{N}$.

Théorème n° 2 : formule du binôme de Newton

Soient $(a,b)\in\mathbb{C}^2$ et n un entier naturel, alors $$(a+b)^n = \sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}$$

Exemple 19. Développer l'expression $(x-1)^5$.

Sommes de coefficients binomiaux

Soit $n\in\mathbb{N}$. Calculer $\sum_{k=0}^{n}\binom{n}{k}$ et $\sum_{k=0}^{n}(-1)^k\binom{n}{k}$. En déduire $\sum_{\substack{k=0\\ k \text{ pair}}}^{n}\binom{n}{k}$.

Exprimer $\cos(n\theta)$ **en fonction de** $\cos(\theta)$

Linéariser $\cos(\theta)^n$

2 Petits systèmes linéaires

2.1 Définition

Définition d'un système linéaire à deux inconnues

Soient $(a_1, a_2, a_3, b_1, b_2, b_3, c_1, c_2, c_3) \in \mathbb{K}^9$. On dit que $\begin{cases} a_1x + b_1y = c_1 \\ a_2x + b_2y = c_2 \end{cases}$ est un système de deux équations à deux inconnues (x, y). On dit que $\begin{cases} a_1x + b_1y = c_1 \\ a_2x + b_2y = c_2 \\ a_3x + b_3y = c_3 \end{cases}$ est un système de trois équations à deux inconnues. Les nombres x et y dans $\mathbb{K}$ sont les inconnues du système, les a_i, b_i sont les coefficients du système, les c_i sont les seconds membres du système.
Résoudre un tel système c'est trouver tous les couples $(x, y) \in \mathbb{K}^2$ qui vérifient ces deux ou trois équations.

Exemple 20. $\begin{cases} 2x + 3y &= 2 \\ 2x + 3y &= 3 \end{cases}$ est un système linéaire de 2 équations et 2 inconnues. $\begin{cases} 2x + 3yx &= 2 \\ 2x + 3y &= 3 \end{cases}$ n'est pas un système linéaire.

Définition d'un système linéaire à trois inconnues

Soient $(a_1, a_2, a_3, b_1, b_2, b_3, c_1, c_2, c_3, d_1, d_2, d_3) \in \mathbb{K}^{12}$. On dit que $\begin{cases} a_1x + b_1y + c_1z = d_1 \\ a_2x + b_2y + c_2z = d_2 \end{cases}$ est un système de deux équations à trois inconnues. On dit que $\begin{cases} a_1x + b_1y + c_1z = d_1 \\ a_2x + b_2y + c_2z = d_2 \\ a_3x + b_3y + c_3z = d_3 \end{cases}$ est un système de trois équations à trois inconnues.
Les nombres x et y, z dans $\mathbb{K}$ sont les inconnues du système, les a_i, b_i et c_i sont les coefficients du système, les d_i sont les seconds membres du système.
Résoudre un tel système c'est trouver tous les triplets $(x, y, z) \in \mathbb{K}^3$ qui vérifient ces deux ou trois équations.

2.2 Interprétation graphique

- Si $(a, b) \neq (0, 0)$, l'équation $ax + by = c$ est l'équation d'une droite. Résoudre un système linéaire à deux inconnues revient donc à chercher l'intersection de deux ou trois droites.
- Si $(a, b, c) \neq (0, 0, 0)$ l'équation $ax + by + cz = d$ est l'équation d'un plan. Résoudre un système linéaire à trois inconnues revient donc à chercher l'intersection de deux ou trois plans.
- Ainsi, on peut déterminer quels sont les différents cas possibles dans la résolution des systèmes linéaires.

2.3 Algorithme de résolution des systèmes linéaires

Remarque 8. Le système $\begin{cases} 3x + 2y + z &= 4 \\ y + z &= 2 \\ z &= 3 \end{cases}$ est facile à résoudre, $z = 3$, $y = -1$, $x = 1$.

Définition des opérations élémentaires

Soit un système avec 2/3 équations et 2/3 inconnues. Notons L_1, L_2 (et éventuellement L_3) les lignes du système. Alors on peut faire des opérations, dites élémentaires, sur ce système pour obtenir un nouveau système :

1. échangeant deux lignes : $L_i \leftrightarrow L_j$ avec $i \neq j$
2. en multipliant une ligne par un nombre non nul : $L_i \leftarrow \lambda L_i$ avec $\lambda \neq 0$
3. en ajoutant à une ligne une autre ligne multipliée par un nombre : $L_i \leftarrow L_i + \lambda L_j$ avec $i \neq j$

Théorème n° 3 : invariance des solutions par opérations élémentaires

Soit (S) un système linéaire et (S') un système obtenu à partir de (S) après une ou plusieurs opérations élémentaires. Alors (S) et (S') ont exactement les mêmes solutions.

Comment résoudre un système linéaire ?

1. Éliminer les inconnues de façon à «trigonaliser» le système en effectuant des opérations élémentaires.
2. Trouver les inconnues en «remontant»

Remarque 9. Si le système n'a aucune solution, on dit qu'il est incompatible.

Exemple 21. Résoudre $\left\{\begin{array}{lcl} 2x+3y & = & 5 \\ x+5y & = & 12 \end{array}\right.$, $\left\{\begin{array}{lcl} 3x+2y & = & 10 \\ 2x+2y & = & 1 \end{array}\right.$, $\left\{\begin{array}{lcl} x+3y-z & = & -1 \\ 2x+5y+z & = & 0 \end{array}\right.$, $\left\{\begin{array}{lcl} x+3y-z & = & -1 \\ 2x+5y+z & = & 0 \\ 3x+2z & = & 0 \end{array}\right.$, $\left\{\begin{array}{lcl} x+3y-z & = & -1 \\ 2x+5y+z & = & 0 \\ 3x+7y+3z & = & 1 \end{array}\right.$, $\left\{\begin{array}{lcl} x+3y-z & = & -1 \\ 2x+5y+z & = & 0 \\ 3x+7y+3z & = & 2 \end{array}\right.$,

Attention : à plusieurs choses

1. Si vous utilisez L_1 pour modifier L_2, alors n'utilisez en même temps pas L_2 pour modifier L_1 ou L_3.
2. Toujours raisonner par équivalence et non de «donc».
3. Toujours indiquer les opérations effectuées en dessous de $\iff$.
4. N'exprimez pas x en fonction de y sur une ligne et en même temps, exprimer y en fonction de x.
5. Ne remontez le système que quand il est bien triangulé.
6. Ne pas faire $L_i \leftarrow \lambda L_i + L_j$ avec $\lambda = 0$ car vous allez perdre L_i.
7. Vous avez le droit d'utiliser deux lignes pour modifier une autre : $L_1 \leftarrow L_1 - 2L_3 + 5L_2$.

3 Arithmétique

3.1 Diviseur, multiples et division euclidienne

Définition d'un diviseur d'un entier

Soit $(a,b) \in \mathbb{Z}^2$, on dit que b **divise** a (ou que b **est un diviseur de** a ou que a **est un multiple de** b) s'il existe $k \in \mathbb{Z}$ tel que $a = kb$. On note alors $b|a$.

Exemple 22.

1. L'ensemble des diviseurs de 12 est $\{1,2,3,4,6,12,-1,-2,-3,-4,-6,-12\}$.
2. L'ensemble des diviseurs de 0 est $\mathbb{Z}$.
3. L'ensemble des diviseurs de 1 est $\{1,-1\}$.
4. L'ensemble des diviseurs de 5 est $\{1,5,-1,-5\}$
5. L'ensemble des multiples de 12 est $\{12k \mid k \in \mathbb{Z}\}$.
6. L'ensemble des multiples de 1 est $\mathbb{Z}$.
7. L'ensemble des multiples de 0 est $\{0\}$.
8. Un nombre est divisible par deux si et seulement s'il est pair.

Proposition n° 9 : propriétés de la divisibilité

Soient $(a,b,c,d) \in \mathbb{Z}^4$.

1. $a|b$ et $a|c \implies a|(b+c)$
2. $a|b \implies a|bc$
3. $a|b$ et $c|d \implies (ac)|(bd)$
4. $(ab)|c \implies a|c$ et $b|c$.
5. $a|b$ et $b|a \iff b = \pm a$

Théorème n° 4 : division euclidienne dans $\mathbb{Z}$

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$. Alors, il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ avec $0 \leqslant r < |b|$.

```
def DivisionEuclidienne(a,b):
    """À la main: si (a,b)€NxN*, renvoie le quotient et le reste de la division euclidienne de a par b"""
    r,q=a,0
    while
        r,q=r-b,q+1
    return q,r

a//b, r=a%b#Commande python
```

Attention à ne pas confondre la division euclidienne et la divisibilité

La phrase «b divise a» est une proposition à laquelle on répond par oui ou par non.
Effectuer la division euclidienne de a par b revient à trouver le quotient et le reste : $a = bq + r$ avec $0 \leqslant r < |b|$.
Il y a, cependant, un lien entre les deux :

Proposition n° 10 : lien entre divisibilité et division euclidienne

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$. Alors $b|a$ ssi le reste de la division euclidienne de a par b vaut 0.

3.2 PGCD et PPCM

Définition du PGCD de deux entiers

Soit $(a,b) \in \mathbb{Z}^2$ tel que $a \neq 0$ ou $b \neq 0$. Alors, l'ensemble des diviseurs commun à a et b est fini et admet donc un plus grand élément. On appelle cet élément plus grand diviseur commun à a et b et on le note $\mathrm{PGCD}(a,b)$.

Exemple 23. $\mathrm{PGCD}(9,12) =$ Pour tout $b \in \mathbb{Z}$, $\mathrm{PGCD}(0,b) =$

Lemme 1. Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$, et $a = bq + r$ la division euclidienne de a par b. Alors $\mathrm{PGCD}(a,b) = \mathrm{PGCD}(b,r)$

Théorème n° 5 : algorithme d'Euclide

Soient $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$, on pose $r_0 = a$, $r_1 = b$ et tant que $r_k \neq 0$, on pose r_{k+1} le reste de la division euclidienne de r_{k-1} par r_k. Alors, il existe $N \in \mathbb{N}$ tel que $r_N \neq 0$ et $r_{N+1} = 0$, de plus, $\mathrm{PGCD}(a,b) = r_N$.

Exemple 24. Calculer le PGCD de 75 et 24.

```
def AlgoEuclide(a,b):
  """Pour a et b deux entiers, renvoie leur PGCD"""
    L=[a,b]
    while L[len(L)-1]!=0:
      r=L[len(L)-2]%L[len(L)-1]
      L.append(r)
    return L[len(L)-2]
```

Définition du PPCM

Soit $(a,b) \in \mathbb{Z}^2$, l'ensemble des multiples communs positifs à a et b admet un plus petit élément, on l'appelle plus petit commun multiple de a et b, notée $\mathrm{PPCM}(a,b)$.

Exemple 25. $\text{PPCM}(a,0) =$ $\text{PPCM}(-3,-5) =$ $\text{PPCM}(12,40) =$

Remarque 10. Calculer le PPCM permet de remettre au même dénominateur deux fractions sans forcément effectuer le produit des dénominateurs.

3.3 Nombres premiers

Définition d'un nombre premier

Soit $n \in \mathbb{N}$ avec $n \geqslant 2$, on dit que n est premier si les seuls diviseurs positifs de n sont 1 et n.

Exemple 26. Les nombres 2,5,7,11,13,17 sont premiers, 4, 9 et 21 ne le sont pas.

Remarque 11. Un nombre n est premier ssi il n'admet pas de diviseurs entre 2 et $\sqrt{n}$, on peut donc faire un algorithme qui renvoie `True` si n est premier :

```
def EstPremier(n):
  """Pour un entier naturel, renvoie True ssi n est premier"""
  if n<2:
    return False
  for d in range(2,n**(1/2)+1):
    if n%d==0:#d divise n
      return False
  return True

ListePremiers=[k for k in range(2,1001) if EstPremier(k)==True]#Liste des nombres premiers
```

Lemme 2. Soit un entier $n \geqslant 2$, alors n est divisible par au moins un nombre premier.

Théorème n° 6 : ensemble des nombres premiers

Il existe une infinité de nombres premiers.

Théorème n° 7 : décomposition d'un entier naturel en facteurs premiers *(admis)*

Soit un entier $n \geqslant 2$. Il existe un unique $r \in \mathbb{N}^*$, un unique r-uplet de nombre premiers $p_1 < p_2 < \ldots < p_r$ et un unique r-uplet d'entiers naturels non nuls $(\alpha_1, \alpha_2, \ldots, \alpha_r)$ tels que $n = \prod_{i=1}^{r} {p_i}^{\alpha_i}$.

Exemple 27. $24 = 2^3 \times 3$ $245 =$

Remarque 12. Si on prend deux nombres a et b, ils ne sont pas forcément divisibles par les mêmes nombres premiers. Cependant, on peut rajouter dans la décomposition de a les nombres premiers de la décomposition de b avec un exposant 0 s'ils ne sont pas dans a idem pour b.

Proposition n° 11 : condition nécessaire et suffisante de divisibilité

Soit $a = \prod_{i=1}^{s} {p_i}^{\alpha_i}$ et $d = \prod_{i=1}^{s} {p_i}^{\beta_i}$ avec p_i des nombres premiers tels que $p_1 < p_2 < \ldots < p_s$ et α_i et β_i des entiers naturels. Alors, d divise a ssi pour tout $i \in [\![1\,;s]\!]$, $\beta_i \leqslant \alpha_i$.

Proposition n° 12 : expression du PGCD/PPCM à l'aide de la décomposition

Si $a = \prod_{i=1}^{s} {p_i}^{\alpha_i}$ et $b = \prod_{i=1}^{s} {p_i}^{\beta_i}$ avec p_i des nombres premiers tels que $p_1 < p_2 < \ldots < p_s$, α_i et β_i des entiers naturels, alors $\text{PGCD}(a,b) = \prod_{i=1}^{s} {p_i}^{\min(\alpha_i,\beta_i)}$ et $\text{PPCM}(a,b) = \prod_{i=1}^{s} {p_i}^{\max(\alpha_i,\beta_i)}$

Exemple 28. Calculer le PGCD et le PPCM de 84 et 48.

Proposition n° 13 : lien entre PGCD et PCCM

Soit $(a, b) \in (\mathbb{N}^*)^2$, alors $\mathrm{PGCD}(a, b)\mathrm{PPCM}(a, b) = ab$