# 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.

**Attention : utiliser un lecteur de pdf adapté**

Ce polycopié contient plusieurs animations, il est donc conseillé d'utiliser un lecteur de pdf capable de lire les animations (comme Adobe Reader, Foxit PDF Reader, Okular ou autres).

## 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 et $(a_i)_{i\in I}$ une famille de complexes. On note, $\sum_{i\in I} a_i$ la somme des éléments de la famille $(a_i)_{i\in I}$ et $\prod_{i\in I} a_i$ le produit des éléments de la famille $(a_i)_{i\in I}$. Par **convention**, si $I = \varnothing$, $\sum_{i\in I} a_i = 0$ et $\prod_{i\in I} a_i = 1$.

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

**Remarques 1.**

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

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

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

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

- Le nombre $\sum_{i=m}^{n} a_i$ dépend de $m$ et de $n$ mais pas de $i$. Écrire cette $\sum_{i=m}^{n} a_i$ en fonction de $i$ est une erreur.

**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 $\lambda \in \mathbb{C}$ :

1. $\sum_{i\in I}(a_i + b_i) = \sum_{i\in I} a_i + \sum_{i\in I} b_i$
2. $\sum_{i\in I}(\lambda a_i) = \lambda \sum_{i\in I} a_i$
3. $\prod_{i\in I}(a_i b_i) = \left(\prod_{i\in I} a_i\right) \times \left(\prod_{i\in I} b_i\right)$
4. $\prod_{i\in I}(\lambda a_i) = \lambda^p \prod_{i\in I} a_i$

**Exemple 2.**

1. Calculer $\sum_{k=0}^{n} 1$
2. Calculer $\prod_{k=0}^{n} 2$
3. Prouver $\sum_{k=1}^{n} k^2 = \dfrac{n(n+1)(2n+1)}{6}$

## 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, $\sum_{j\in J} a_{\varphi(j)} = \sum_{i\in I} a_i$.

**Exemple 3.** Faites un changement d'indice dans $\sum_{k=0}^{n-1} u_{k+1}$ et dans $\sum_{k=0}^{n} u_{n-k}$.

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

**Séparation/regroupement de termes**

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

**Exemples 4.**

1. Couper $\sum_{k=1}^{2n} u_k$ en deux sommes ayant le même nombres de termes.
2. Couper $\sum_{k=1}^{2n+1} u_k$ en isolant le terme au milieu.
3. Calculer $S_n = \sum_{k=0}^{2n} \min(k,n)$, où $\min(k,n)$ est le minimum des entiers $k$ et $n$.
4. Couper $\sum_{k=0}^{n} u_k$ en deux sommes, l'une avec des indices pairs et l'autre avec des indices impairs.

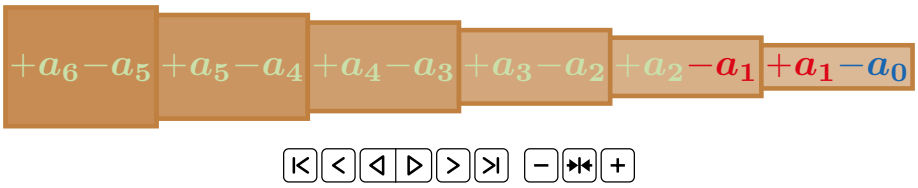
**Exemple 5.** $(a_3-a_2)+(a_4-a_3)+(a_5-a_4) = a_5-a_2$ et si $a_2$, $a_3$ et $a_4$ sont non nuls, $\frac{a_3}{a_2}\times\frac{a_4}{a_3}\times\frac{a_5}{a_4} = \frac{a_5}{a_2}$

**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, $\prod_{i=m}^{n}\frac{a_{i+1}}{a_i} = \frac{a_{n+1}}{a_m}$.

**Démonstration de la proposition n° 2 :** Par linéarité de la somme, puis par changement d'indice puis par séparation de somme :

$$\sum_{k=m}^{n}(a_{k+1}-a_k) = \sum_{k=m}^{n} a_{k+1} - \sum_{k=m}^{n} a_k = \sum_{j=m+1}^{n+1} a_j - \sum_{k=m}^{n} a_k = \sum_{j=m+1}^{n} a_j + a_{n+1} - \left(\sum_{k=m+1}^{n} a_k + a_m\right) = a_{n+1}-a_m \quad \blacksquare$$




**Exemple 6.**

1. Calculer la somme $S_n = \sum_{k=1}^{n} \frac{1}{k(k+1)}$.
2. En déduire la limite de la suite $(S_n)_n$.
3. Calculer le produit $P_n = \prod_{k=2}^{n}\left(1-\frac{1}{k}\right)$.

**Remarque 2.** Soit $(z_k)_{k\in I}$ une famille finie de complexes, alors $\mathrm{Re}\left(\sum_{k\in I} z_k\right) = \sum_{k\in I}\mathrm{Re}(z_k)$ et $\mathrm{Im}\left(\sum_{k\in I} z_k\right) = \sum_{k\in I}\mathrm{Im}(z_k)$

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

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

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

**Démonstration de la proposition n° 3 :** Notons $r$ la raison de cette suite. Calculons le double cette somme en effectuant un changement d'indice $j = n + m - k$ dans la seconde somme :

$$\begin{aligned} 2\sum_{k=m}^{n} u_k &= \sum_{k=m}^{n} u_k + \sum_{k=m}^{n} u_k = \sum_{k=m}^{n} u_k + \sum_{j=m}^{n} u_{n+m-j} = \sum_{k=m}^{n} u_k + \sum_{k=m}^{n} u_{n+m-k} = \sum_{k=m}^{n} (u_k + u_{n+m-k}) \\ &= \sum_{k=m}^{n} ([u_m + (k-m)r] + [u_n + (m-k)r]) = \sum_{k=m}^{n} (u_m + u_n) = (u_m + u_n)(n - m + 1) \end{aligned}$$

En divisant par 2, on obtient le résultat. ■

**Exemple 7.** 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 pour $n \geqslant m$ :

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

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

**Démonstration de la proposition n° 4 :** Si $q \neq 1$, alors :

$$(1-q)\sum_{k=m}^{n} u_k = \sum_{q=m}^{n} (1-q)u_k = \sum_{q=m}^{n} (u_k - u_{k+1}) = u_m - u_{n+1} = u_m - u_m q^{n+1-m} = u_m(1 - q^{n+1-m})$$

En divisant par $1 - q$, on obtient le résultat. Si $q = 1$, alors

$$\sum_{k=m}^{n} u_k = \sum_{k=m}^{n} u_m = u_m(n - m + 1)$$ ■

**Exemple 8.**

1. Calculer $S_n = \sum_{k=0}^{n} 2^{-k}$.
2. En déduire la limite de $(S_n)_{n\in\mathbb{N}}$
3. Soit $x \in \mathbb{C}$, calculer $S_n = \sum_{i=1}^{n} x^i$
4. 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 $\sum_{k=0}^{n} \cos(k\theta)$ et $\sum_{k=0}^{n} \sin(k\theta)$

**Exemple 9.** $(a-b)(a+b) =$ $(a-b)(a^2+ab+b^2) =$ $(a-b)(a^3+a^2b+ab^2+b^3) =$

**Proposition n° 5 : identité remarquable**

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

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

**Démonstration de la proposition n° 5 :** En partant du membre de gauche et en utilisant la linéarité, on reconnaît une somme télescopique :

$$(a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k} = \sum_{k=0}^{n-1}(a-b)a^k b^{n-1-k} = \sum_{k=0}^{n-1} \underbrace{a^{k+1}b^{n-1-k}}_{=u_{k+1}} - \underbrace{a^k b^{n-k}}_{=u_k} = \underbrace{a^n}_{u_n} - \underbrace{b^n}_{u_0}$$

■

**Exemple 10.** Soit $n \in \mathbb{N}^*$, étudier la dérivabilité de $p_n : x \mapsto x^n$ sur $\mathbb{R}$.

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

| | $p$ | $p+1$ | $\dots$ | $j$ | $\dots$ | $q$ | Totaux par ligne |
|---|---|---|---|---|---|---|---|
| $m$ | $a_{m,p}$ | $a_{m,p+1}$ | $\dots$ | $a_{m,j}$ | $\dots$ | $a_{m,q}$ | $\sum_{j=p}^{q} a_{m,j}$ |
| $m+1$ | $a_{m+1,p}$ | $a_{m+1,p+1}$ | $\dots$ | $a_{m+1,j}$ | $\dots$ | $a_{m+1,q}$ | $\sum_{j=p}^{q} a_{m+1,j}$ |
| $\vdots$ | $\vdots$ | $\vdots$ | | $\vdots$ | | $\vdots$ | |
| $i$ | $a_{i,p}$ | $a_{i,p+1}$ | $\dots$ | $a_{i,j}$ | $\dots$ | $a_{i,q}$ | $\sum_{j=p}^{q} a_{i,j}$ |
| $\vdots$ | $\vdots$ | $\vdots$ | | $\vdots$ | | $\vdots$ | |
| $n$ | $a_{n,p}$ | $a_{n,p+1}$ | $\dots$ | $a_{n,j}$ | $\dots$ | $a_{n,q}$ | $\sum_{j=p}^{q} a_{n,j}$ |
| Totaux par colonne | $\sum_{i=m}^{n} a_{i,p}$ | $\sum_{i=m}^{n} a_{i,p+1}$ | | $\sum_{i=m}^{n} a_{i,j}$ | | $\sum_{i=m}^{n} a_{i,q}$ | |

(a) Somme indexée par un rectangle

| | $m$ | $m+1$ | $\cdots$ | $j$ | $\cdots$ | $n$ | Totaux par ligne |
|---|---|---|---|---|---|---|---|
| $m$ | $a_{m,m}$ | $a_{m,m+1}$ | $\cdots$ | $a_{m,j}$ | $\cdots$ | $a_{m,n}$ | $\sum_{j=m}^{n} a_{m,j}$ |
| $m+1$ | | $a_{m+1,m+1}$ | $\cdots$ | $a_{m+1,j}$ | $\cdots$ | $a_{m+1,n}$ | $\sum_{j=m+1}^{n} a_{m+1,j}$ |
| $\vdots$ | | | $\ddots$ | | | $\vdots$ | |
| $i$ | | | | $\ddots$ | | $a_{i,n}$ | $\sum_{j=i}^{n} a_{i,j}$ |
| $\vdots$ | | | | | $\ddots$ | $\vdots$ | |
| $n$ | | | | | | $a_{n,n}$ | $\sum_{j=n}^{n} a_{n,j}$ |
| Totaux par colonne | $\sum_{i=m}^{m} a_{i,m}$ | $\sum_{i=m}^{m+1} a_{i,m+1}$ | | $\sum_{i=m}^{j} a_{i,j}$ | | $\sum_{i=m}^{n} a_{i,n}$ | |

(b) Somme indexée par un triangle

**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 $(m, n) \in \mathbb{N}$ 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 11.** Calculer $S_n = \sum_{1\leqslant i\leqslant j\leqslant n} \frac{i}{j}$.

**Remarque 3.** 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 : $\sum_{i=1}^{n} a_i \times \sum_{j=1}^{p} b_j = \sum_{i=1}^{n}\sum_{j=1}^{p} a_i b_j = \sum_{j=1}^{p}\sum_{i=1}^{n} a_i b_j$

**Remarque 4.** 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** de $n$ l'entier $n! = \prod_{k=1}^{n} k$.

**Exemple 12.** Donner les valeurs de $1! =$ $2! =$ $3! =$ $4! =$ $5! =$ $0! =$

**Remarque 5.** 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 13.** 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 6.** 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 $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$

**Démonstration du théorème n° 2 :** Posons l'hypothèse de récurrence $\mathscr{P}(n)$ : «$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$».

- Pour $n=0$, $\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} = \binom{0}{0} a^0 b^0 = 1$, tandis que $(a+b)^n = (a+b)^0 = 1$. Ainsi, $\mathscr{P}(0)$ est vraie.
- Soit $n \in \mathbb{N}$. Supposons $\mathscr{P}(n)$ vraie, alors :

$$
\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n = (a+b)\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k} = \sum_{k=0}^{n}\binom{n}{k}(a+b)a^k b^{n-k} \\
&= \sum_{k=0}^{n}\binom{n}{k}\left(a^{k+1}b^{n-k} + a^k b^{n+1-k}\right) = \sum_{k=0}^{n}\left(\binom{n}{k}a^{k+1}b^{n-k} + \binom{n}{k}a^k b^{n+1-k}\right) \\
&= \sum_{k=0}^{n}\binom{n}{k}a^{k+1}b^{n-k} + \sum_{k=0}^{n}\binom{n}{k}a^k b^{n+1-k} = \sum_{j=1}^{n+1}\binom{n}{j-1}a^j b^{n+1-j} + \sum_{k=0}^{n}\binom{n}{k}a^k b^{n+1-k} \\
&= \sum_{j=1}^{n}\binom{n}{j-1}a^j b^{n+1-j} + \binom{n}{n}a^{n+1}b^0 + \sum_{k=1}^{n}\binom{n}{k}a^k b^{n+1-k} + \binom{n}{0}a^0 b^{n+1} \\
&= \sum_{k=1}^{n}\left(\binom{n}{k-1}a^k b^{n+1-k} + \binom{n}{k}a^k b^{n+1-k}\right) + a^{n+1} + b^{n+1} \\
&= \sum_{k=1}^{n}\binom{n+1}{k}a^k b^{n+1} + \binom{n+1}{n+1}a^{n+1}b^{n+1-(n+1)} + \binom{n+1}{0}a^{n+1-(n+1)b^{n+1}} = \sum_{k=0}^{n+1}\binom{n+1}{k}a^k b^{n+1-k}
\end{aligned}
$$

  Ainsi, $\mathscr{P}(n+1)$ est vraie.
- Par récurrence, pour tout $n \in \mathbb{N}$, $\mathscr{P}(n)$ est vraie. ■

**Exemple 14.** 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.

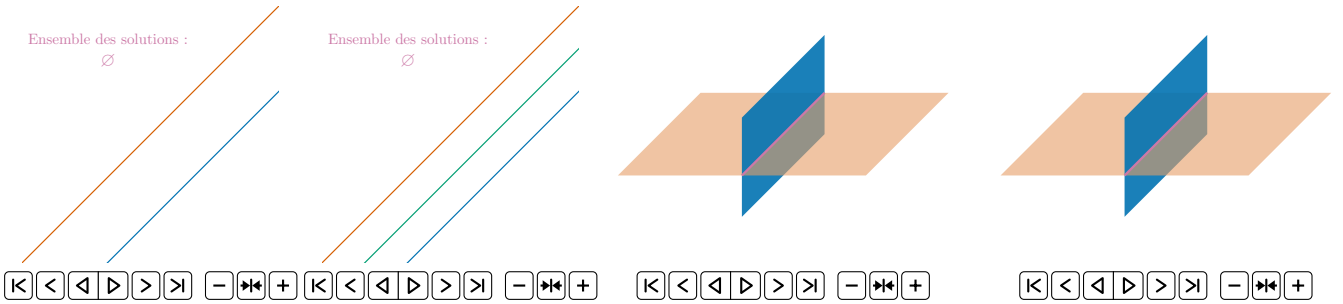
**Exemple 15.** $\begin{cases} 2x + 3y &= 2 \\ 2x + 3y &= 3 \end{cases}$ est un système linéaire de 2 équations et 2 inconnues. $\begin{cases} 2x + 3yx &= 2 \\ 2x + 3y &= 3 \end{cases}$ n'est pas un système linéaire.

**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.




(a) Système linéaire de deux équations à deux inconnues

(b) Système linéaire de trois équations à deux inconnues

(c) Système linéaire de deux équations à trois inconnues

(d) Système linéaire de trois équations à trois inconnues (coming soon)

FIGURE 1 – Interprétation graphique des solutions d'un système linéaire de deux/trois équations à deux/trois inconnues.

## 2.3 Algorithme de résolution des systèmes linéaires

**Remarque 7.** 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 les **opérations élémentaires** sur ce système pour obtenir un nouveau système :

1. Échanger deux lignes : $L_i \leftrightarrow L_j$ avec $i \neq j$
2. Multiplier une ligne par un nombre non nul : $L_i \leftarrow \lambda L_i$ avec $\lambda \neq 0$
3. Ajouter 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 8.** Si le système n'a aucune solution, on dit qu'il est incompatible.

**Exemple 16.** Résoudre les systèmes suivants :

1. $\begin{cases} x & +5y & = & 12 \\ 2x & +3y & = & 5 \end{cases}$
2. $\begin{cases} 3x & +2y & = & 10 \\ 2x & +2y & = & 1 \end{cases}$
3. $\begin{cases} x & +3y & -z & = & -1 \\ 2x & +5y & +z & = & 0 \end{cases}$
4. $\begin{cases} x & +3y & -z & = & -1 \\ 2x & +5y & +z & = & 0 \\ 3x & & +2z & = & 0 \end{cases}$
5. $\begin{cases} x & +3y & -z & = & -1 \\ 2x & +5y & +z & = & 0 \\ 3x & +7y & +3z & = & 1 \end{cases}$
6. $\begin{cases} x & +3y & -z & = & -1 \\ 2x & +5y & +z & = & 0 \\ 3x & +7y & +3z & = & 2 \end{cases}$

**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. Raisonner par équivalence et pas avec des «donc».
3. Indiquer les opérations effectuées en dessous de $\iff$.
4. Ne remontez le système que s'il est bien échelonné c'est à dire si les inconnues qui sont les plus à gauche dans chaque ligne s'expriment en fonction des autres inconnues.
5. Ne pas faire $L_i \leftarrow \lambda L_i + L_j$ avec $\lambda = 0$ car vous allez perdre $L_i$.
6. 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 17.**

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 2 ssi 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 $b|a \iff b = \pm a$
6. $a|b$ et $b|c \implies a|c$

**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 $0 \leqslant r < |b|$.

**Démonstration du théorème n° 4 :** Montrons d'abord l'existence de la division euclidienne. Posons l'hypothèse de récurrence $\mathscr{P}(n)$ : «il existe $(q,r) \in \mathbb{Z}^2$ tel que $n = bq + r$ avec $0 \leqslant r < |b|$». Pour $n = 0$, il suffit de poser $q = r = 0$. Ainsi, $\mathscr{P}(0)$ est vraie. Soit $n \in \mathbb{N}$, supposons $\mathscr{P}(n)$ vraie. Ainsi, il existe $(\tilde{q},\tilde{r}) \in \mathbb{Z}^2$ tel que $n = b\tilde{q} + \tilde{r}$ avec $0 \leqslant r < |b|$. Dès lors, $n+1 = b\tilde{q} + \tilde{r} + 1$, il y a donc deux cas :

- Si $\tilde{r} < |b| - 1$, alors $\tilde{r} + 1 < |b|$, on pose alors $q = \tilde{q}$ et $r = \tilde{r} + 1$ et on a bien $n + 1 = bq + r$ avec $0 \leqslant r < |b|$.
- Si $\tilde{r} = |b| - 1$, alors $n + 1 = b\tilde{q} + |b| = b(\tilde{q} \pm 1)$, (en effet $|b| = \pm b$), ainsi en posant $q = \tilde{q} \pm 1$ et $r = 0$ on a bien $n + 1 = bq + r$ avec $0 \leqslant r < b$.

On a donc montré que $\mathscr{P}(n)$ est vraie. Ainsi, si $a \in \mathbb{N}$, en appliquant $\mathscr{P}(a)$ on a démontré l'existence de la division euclidienne de $a$ par $b$. Si $a < 0$, alors $-a > 0$ et il existe $(\tilde{q},\tilde{r}) \in \mathbb{Z}^2$ tel que $-a = b\tilde{q} + \tilde{r}$ avec $0 \leqslant \tilde{r} < |b|$. Donc $a = b(-\tilde{q}) - \tilde{r}$, observons que si $\tilde{r} = 0$, alors $a = bq + r$ avec $q = -\tilde{q}$ et $r = 0$. Si $\tilde{r} > 0$, alors $a = b(-\tilde{q}) - |b| + (|b| - \tilde{r})$ posons $r = |b| - \tilde{r}$ de sorte que $0 \leqslant r < |b|$ et $q = (-\tilde{q}) + \pm 1$ de sorte que $a = bq + r$. Montrons l'unicité, si $a = bq + r = bq' + r'$ avec $(q,q',r,r') \in \mathbb{Z}^4$ et $0 \leqslant r < |b|$ et $0 \leqslant r < |b'|$, alors $r - r' = b(q' - q)$ avec $-|b| < r - r' < |b|$, donc $-|b| < b(q - q') < |b|$ donc $-1 \leqslant \pm(q' - q) < 1$ on en déduit que $q' - q = 0$ donc que $q = q'$ puis que $r = r'$.

■

```
q,r = a//b, a%b#Commande python à connaître et fonctionne aussi si a ou b sont négatifs

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
```

**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 $0 \leqslant r < |b|$.
Cependant, la proposition 10 fait 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.

**Démonstration de la proposition n° 10 :** Si le reste de la division euclidienne de $a$ par $b$ vaut 0, alors en notant $q \in \mathbb{Z}$ le quotient de cette division euclidienne $a = bq + 0$ et donc $b$ divise $a$. Réciproquement, si $a$ divise $b$, alors il existe $q \in \mathbb{Z}$ tel que $a = bq$, alors $a = bq + r$ avec $r = 0$ vérifiant $0 \leqslant r < |b|$. Par unicité de la division euclidienne, $q$ est le quotient et $r = 0$ le reste de la division euclidienne de $a$ par $b$. ■

## 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 $\text{PGCD}(a,b)$.

**Exemples 18.** $\text{PGCD}(9,12) =$ pour tout $b \in \mathbb{Z}^*$, $\text{PGCD}(0,b) =$

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

**Démonstration du lemme 1 :** Soit $d$ un diviseur commun de $a$ et $b$, alors $d$ divise $bq - a = d$, donc $d$ est un diviseur comme de $b$ et de $r$. Soit $d$ un diviseur comme de $b$ et de $r$, alors $d$ divise $bq + r = d$, donc $d$ est un diviseur commun de $a$ et de $b$. Ainsi, comme les diviseurs commun de $a$ et de $b$ sont exactement les mêmes que les diviseurs communs de $b$ et de $r$, en particuliers, ils ont le même plus grand diviseur commun. On a donc bien démontré que $\text{PGCD}(a,b) = \text{PGCD}(b,r)$.

**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 définit $r_{k+1}$ comme 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, $\text{PGCD}(a,b) = r_N$.

**Démonstration du théorème n° 5 :** Supposons que pour tout $n \in \mathbb{N}$, $r_n \neq 0$. Soit un entier $n \geqslant 2$, alors on fait la division euclidienne de $r_{n-1}$ par $r_n$ et on trouve un reste $r_{n+1}$ qui vérifie $r_{n+1} < |r_n| = r_n$. Ainsi, $r_{n+1} \leqslant r_n - 1$. Par récurrence, on montre donc que pour tout entier $n \geqslant 2$, $0 < r_n \leqslant r_2 - n + 2$, Ainsi, pour $m = r_2 - 2 \in \mathbb{N}$, on obtient $0 < r_m \leqslant 0$ ce qui est absurde. Ainsi, il existe $m \in \mathbb{N}$ tel que $r_m = 0$. Notons alors $N = \max k \in [\![ 0\,;m-1 ]\!] \mid r_k \neq 0$, alors $r_N \neq 0$ et $r_{N+1} = 0$. De plus, d'après le lemme 1, pour tout $k \in [\![ 1\,;N-1 ]\!]$,

$$\text{PGCD}(r_{k-1}, r_k) = \text{PGCD}(r_k, r_{k+1})$$

On en déduit donc que la suite finie $(\text{PGCD}(r_k, r_{k+1}))_{0 \leqslant k \leqslant N}$ est constante. Il s'ensuit que $\text{PGCD}(r_0, r_1) = \text{PGCD}(r_N, r_{N+1})$. Par conséquent, $\text{PGCD}(a,b) = r_N$. ■

**Exemple 19.** Calculer le PGCD de 75 et 24.

```
def AlgoEuclide(a,b):
    """Pour a et b deux entiers, renvoie leur PGCD"""
    L = [a,b]#Va contenir les restes successifs
    while L[len(L)-1] != 0:#Tant que le dernier reste est non nul
        L.append(L[len(L)-2]%L[len(L)-1])# On calcule le reste et on le rajoute
    return L[len(L)-2]#On renvoie l'avant dernier reste, car le dernier reste est nul
```

**Définition du PPCM**

Soit $(a,b)$, 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 $\text{PPCM}(a,b)$.

**Exemple 20.** $\text{PPCM}(a,0) =$ $\text{PPCM}(-3,-5) =$ $\text{PPCM}(12,40) =$

**Remarque 9.** 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 un entier $n \geqslant 2$, on dit que $n$ est **premier** si les seuls diviseurs positifs de $n$ sont 1 et $n$.

**Exemple 21.** Les nombres 2,5,7,11,13,17 sont premiers, 0, 1, 4, 9, 15 et 21 ne le sont pas.

**Remarque 10.** Un nombre entier $n$ est premier ssi il n'admet pas de diviseurs entre 2 et $\sqrt{n}$, ce qui mène à l'algorithme suivant.

**Justification de la remarque 10 :** Si $n$ est premier, alors $\sqrt{n} < n$ et $n$ n'admet aucun diviseur entre 2 et $\sqrt{n}$. Si $n$ n'est pas premier, alors il existe $d$ et $d'$ tel que $n = dd'$ avec $2 \leqslant d < n$ et $2 \leqslant d' < n$. Remarquons que si $d > \sqrt{n}$ et $d' > \sqrt{n}$, alors par produit $n > n$ ce qui est impossible donc $d \leqslant \sqrt{n}$ ou $d' \leqslant sqrtn$. On a donc démontré que si $n$ n'est pas premier il admet un diviseur entre 2 et $\sqrt{n}$. Par contraposée, on a donc montré que si un nombre n'admet pas de diviseur entre 2 et $\sqrt{n}$ alors il est premier.

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

L = [k for k in range(2,1001) if EstPremier(k)]#Liste des nombres premiers inférieurs ou égale à 1000
```

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

**Démonstration du lemme 2 :** Posons, pour $n \in \mathbb{N}$, $\mathscr{P}(n)$ : «$n$ est divisible par au moins un nombre premier».

- Comme 2 est premier et que 2 divise 2, $\mathscr{P}(2)$ est vraie.
- Soit un entier $n \geqslant 2$. Supposons que, pour tout $k \in [\![ 2\,;n ]\!]$, $\mathscr{P}(k)$ est vraie.
  - Si $n+1$ est premier, alors $n+1$ divise $n+1$, ainsi il existe un nombre premier divisant $n+1$.
  - Si $n+1$ n'est pas premier, il existe $d \in \mathbb{N}$ divisant $n+1$ avec $2 \leqslant d < n+1$. En particulier, $2 \leqslant d \leqslant n$. Comme $\mathscr{P}(d)$ est vraie, il existe $p$ un nombre premier tel que $p$ divise $d$ comme $d$ divise $n+1$, on en déduit que $p$ divise $n+1$.

  Dans tous les cas, on a montré que $\mathscr{P}(n+1)$ est vraie.
- Par récurrence forte, on a montré que tout entier $n \geqslant 2$ est divisible par au moins un nombre premier.

**Théorème n° 6 : ensemble des nombres premiers**
Il existe une infinité de nombres premiers.

**Démonstration du théorème n° 6 :** Supposons qu'il existe un nombre fini de nombres premiers, notons les $p_1, p_2, \ldots, p_n$. Posons $N = \prod_{i=1}^{n} p_i + 1$, alors d'après le lemme 2, il existe un nombre premier divisant $N$. Ainsi, il existe $k \in [\![ 1\,;n ]\!]$ tel que $p_k$ divise $N$. De plus, $p_k$ divise $\prod_{i=1}^{n} p_i$. Par différence, $p_k$ divise $N - \prod_{i=1}^{n} p_i = 1$. Comme $p_k \geqslant 2$ c'est absurde. Ainsi, il existe un nombre infini 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 22.** $24 = 2^3 \times 3$ $245 =$

**Remarque 11.** Si un nombre premier $p$ divise $a$ mais pas $b$, on peut toujours rajouter $p$ dans la décomposition de $b$ avec un exposant nul. De même pour les nombres premiers divisant $b$ mais pas $a$.

**Proposition n° 11 : condition nécessaire et suffisante de divisibilité**
Soit $a = \prod_{i=1}^{s} {p_i}^{\alpha_i}$ et $d = \prod_{i=1}^{s} {p_i}^{\delta_i}$ avec $p_i$ des nombres premiers tels que $p_1 < p_2 < \ldots < p_s$ et $\alpha_i$ et $\delta_i$ des entiers naturels. Alors, $d$ divise $a$ ssi pour tout $i \in [\![ 1\,;s ]\!]$, $\delta_i \leqslant \alpha_i$.

**Démonstration de la proposition n° 11 :** Supposons que pour tout $i \in [\![ 1\,;s ]\!]$, $\delta_i \leqslant \alpha_i$, alors

$$a = \prod_{i=1}^{s} {p_i}^{\alpha_i} = \prod_{i=1}^{s} \left( {p_i}^{\delta_i} \times {p_i}^{\alpha_i - \delta_i} \right) = \prod_{i=1}^{s} {p_i}^{\delta_i} \times \prod_{i=1}^{s} {p_i}^{\alpha_i - \delta_i} = d \times \prod_{i=1}^{s} {p_i}^{\alpha_i - \delta_i}$$

Comme $\alpha_i - \beta_i \in \mathbb{N}$, on en déduit que $a = dk$ avec $k \in \mathbb{N}$. Ainsi, $d$ divise $a$. Supposons que $d$ divise $a$, alors il existe $k \in \mathbb{N}$ tel que $a = dk$. Alors, on peut décomposer $k$ comme un produit en facteur premiers, ainsi, $k = \prod_{i=1}^{s} {p_i}^{\gamma_i} \times \prod_{i=s+1}^{r} {p_i}^{\gamma_i}$ où les nombres $p_i$ pour $i > s$ sont d'éventuels nombres premiers qui apparaissent dans la décomposition de $k$ sans apparaître dans celles de $a$ et de $d$, alors par produit

$$\prod_{i=1}^{s} {p_i}^{\alpha_i} = a = dk = \prod_{i=1}^{s} {p_i}^{\beta_i + \gamma_i} \prod_{i=s+1}^{r} {p_i}^{\gamma_i}$$

mais par unicité de la décomposition d'un entier naturel en facteurs premiers, on en déduit que, pour tout $i \in [\![ 1\,;s ]\!]$, $\beta_i + \gamma_i = \alpha_i$ et donc que $\beta_i \leqslant \alpha_i$. ■

**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 $p_1 < p_2 < \ldots < p_s$, $\alpha_i$ et $\beta_i$ des entiers naturels, alors $\text{PGCD}(a,b) = \prod_{i=1}^{s} {p_i}^{\min(\alpha_i,\beta_i)}$ et $\text{PPCM}(a,b) = \prod_{i=1}^{s} {p_i}^{\max(\alpha_i,\beta_i)}$

**Démonstration de la proposition n° 12 :**

- Pour tout $i \in [\![ 1\,;s ]\!]$, $\min(\alpha_i,\beta_i) \leqslant \alpha_i$, ainsi, d'après la proposition 11, $D = \prod_{i=1}^{s} {p_i}^{\min(\alpha_i,\beta_i)}$ divise $a$, il divise de même $b$. Soit $d$ un diviseur quelconque de $a$ et de $b$, alors nécessairement, d'après la proposition 11, la décomposition en facteurs premiers de $d$ contient au plus les nombres premiers $p_1$, $p_2$, …, $p_r$, dès lors, $d = \prod_{i=1}^{s} {p_i}^{\gamma_i}$ avec $\gamma_i \in \mathbb{N}$, et $\gamma_i \leqslant \alpha_i$. De même, comme $d$ divise $b$, $\gamma_i \leqslant \beta_i$, par conséquent, $\gamma_i \leqslant \min(\alpha_i,\beta_i)$ et donc par produit d'inégalités, $d \leqslant D$. Ainsi, le plus grand diviseur commun de $a$ et $b$ est $D = \prod_{i=1}^{s} {p_i}^{\min(\alpha_i,\beta_i)}$.
- Comme pour tout $i \in [\![ 1\,;s ]\!]$, $\alpha_i \leqslant \max(\alpha_i,\beta_i)$, d'après la proposition 11, $a$ divise $M = \prod_{i=1}^{s} {p_i}^{\max(\alpha_i,\beta_i)}$, de même, $b$ divise $M$, ainsi $M$ est un multiple commun à $a$ et $b$. Soit $m$ un multiple commun de $a$ et $b$, alors $m = \prod_{i=1}^{s} {p_i}^{\gamma_i} \times \prod_{i=s+1}^{r} {p_i}^{\gamma_i}$ avec $\gamma_i \in \mathbb{N}$ et $p_{s+1}, \ldots, p_r$ d'éventuels autres nombres premiers intervenant dans la décomposition de $m$, comme $a$ divise $m$, pour tout $i \in [\![ 1\,;s ]\!]$, $\alpha_i \leqslant \gamma_i$, de même $\beta_i \leqslant \gamma_i$, ainsi, $\max(\alpha_i,\beta_i) \leqslant \gamma_i$, donc $M \leqslant m$. Ainsi, $M = \prod_{i=1}^{s} {p_i}^{\max(\alpha_i,\beta_i)}$ est le plus petit multiple commun à $a$ et à $b$. ■

**Exemple 23.** Calculer le PGCD et le PPCM de 84 et 48.

**Proposition n° 13 : lien entre PGCD et PCCM**

Soit deux entiers $a \geqslant 2$ et $b \geqslant 2$, alors $\text{PGCD}(a,b)\text{PPCM}(a,b) = ab$

**Démonstration de la proposition n° 13 :** Tout d'abord $a = \prod_{i=1}^{s} {p_i}^{\alpha_i}$ et $b = \prod_{i=1}^{s} {p_i}^{\beta_i}$ avec $p_1 < p_2 < \ldots < p_r$ des nombres premiers. Remarquons que, pour tout $i \in [\![ 1\,;s ]\!]$, $\max(\alpha_i,\beta_i) + \min(\alpha_i,\beta_i) = \alpha_i + \beta_i$ (en effet soit le maximum vaut $\alpha_i$ et dans ce cas le minimum vaut $\beta_i$, soit c'est l'inverse.). Ainsi, en utilisant la proposition 12 :

$$\text{PGCD}(a,b)\text{PPCM}(a,b) = \prod_{i=1}^{s} {p_i}^{\min(\alpha_i,\beta_i)} \times \prod_{i=1}^{s} {p_i}^{\max(\alpha_i,\beta_i)} = \prod_{i=1}^{s} {p_i}^{\min(\alpha_i,\beta_i)+\max(\alpha_i,\beta_i)} = \prod_{i=1}^{s} {p_i}^{\alpha_i+\beta_i} = \prod_{i=1}^{s} {p_i}^{\alpha_i} \times \prod_{i=1}^{s} {p_i}^{\beta_i} = ab$$ ■