CH IX : Arithmétique

I. Relation de divisibilité dans $\mathbb{Z}$

I.1. Définition

Définition (Divisibilité dans $\mathbb{Z}$)
Soient $(p, q) \in \mathbb{Z}^2$.

- On dit que p *divise* q s'il existe $k \in Z$ tel que : $q = k \times p$. On note : $p \mid q$.
- On dit alors que p est un *diviseur de* q ou que q est un *multiple* de p.

Exemple

- L'entier 3 divise 36 car : $36 = 3 \times 12$. On écrit : $3 \mid 36$.
- Soit $n \in \mathbb{N}$.
  L'entier $n-2$ divise n^2+n-6. En effet : $n^2+n-6 = (n+3) \times (n-2)$.
  On écrit : $n-2 \mid n^2+n-6$.

Exercice 1
Déterminer tous les diviseurs de 36.

Démonstration.
On remarque :

$$\begin{aligned} 36 &= 2 \times 18 \\ &= 2 \times 2 \times 9 \\ &= 2 \times 2 \times 3 \times 3 \end{aligned}$$

Les diviseurs de 36 sont donc : 1, 2, 4, 6, 9, 12, 18 et 36. □

Remarque

- L'ensemble des multiples de p, noté $p\mathbb{Z}$ est donc l'ensemble :

$$\{p\,k \mid k \in \mathbb{Z}\} \;=\; \{\ldots, -3p, -2p, -p, 0, p, 2p, 3p, \ldots\}$$

- On peut remarquer : $0\,\mathbb{Z} = \{0\}$. Ainsi :
  - × 0 est le seul multiple de 0.
  - × 0 est multiple de tout entier : $\forall p \in \mathbb{Z}$, $0 \in p\,\mathbb{Z}$. En effet, pout tout $p \in \mathbb{Z}$:

$$0 \;=\; 0 \times p$$

I.2. Propriétés

Proposition 1. *Soit $(p, q) \in \mathbb{Z}^2$.*
Les propositions suivantes sont équivalentes :

1) *$p \mid q$*

2) *q est un multiple de p*

3) *$q \in p\,\mathbb{Z}$*

4) *$q\,\mathbb{Z} \subset p\,\mathbb{Z}$ (i.e. tous les multiples de q sont des multiples de p)*

Démonstration.

- D'après les définitions de la partie précédente, les propositions ***1)***, ***2)*** et ***3)*** sont équivalentes.
- Démontrons ***4) ⇒ 3)***.
  Supposons : $q\,\mathbb{Z} \subset p\,\mathbb{Z}$.
  Alors, pour tout $n \in q\,\mathbb{Z}$, on a : $n \in p\,\mathbb{Z}$.
  Or : $q \in q\,\mathbb{Z}$. On en déduit : $q \in p\,\mathbb{Z}$.
- Démontrons ***1) ⇒ 4)***.
  Supposons : $p \mid q$.
  Soit $n \in q\,\mathbb{Z}$.
  - × Comme $n \in a\,\mathbb{Z}$, alors il existe $k_1 \in \mathbb{Z}$ tel que : $n = k_1\,q$.
  - × De plus : $p \mid q$. Ainsi, il existe $k_2 \in \mathbb{Z}$ tel que : $q = k_2\,p$.

On en déduit : $n = k_1\, k_2\, p$.
En notant $k_3 = k_1\, k_2 \in \mathbb{Z}$, on obtient donc : $n = k_3\, p$. D'où : $n \in p\,\mathbb{Z}$.
On a bien démontré : $q\,\mathbb{Z} \subset p\,\mathbb{Z}$.

□

Proposition 2.

1) *Soit $n \in \mathbb{Z}^*$. L'entier n possède un nombre fini de diviseurs (au plus $2\,|n|$).*

2) *Soit $(a, b) \in \mathbb{Z}^2$. On a les équivalences suivantes :*

$$\boxed{a \mid b \quad \Leftrightarrow \quad -a \mid b \quad \Leftrightarrow \quad a \mid -b \quad \Leftrightarrow \quad -a \mid -b}$$

Démonstration.

1) Soit $n \in \mathbb{Z}^*$. On note $\mathcal{D}_n$ l'ensemble des diviseurs de n.

- On commence par démontrer :

$$\begin{array}{rcl} \mathcal{D}_n & \subset & \{-|n|, -(|n|-1), \ldots, -1, 0, 1, \ldots, |n|-1, |n|\} \\ & & \shortparallel \\ & & [\![-|n|, |n|]\!] \end{array}$$

  Soit $p \in \mathcal{D}_n$. Alors $p \in \mathbb{Z}$ et il existe $k \in \mathbb{Z}$ tel que : $n = k\, p$.
  - × Tout d'abord : $|n| = |k\, p| = |k|\,|p|$.
  - × De plus, comme $n \neq 0$, on en déduit : $k \neq 0$. Comme $k \in \mathbb{Z}$, on a alors : $k \leqslant -1$ ou $k \geqslant 1$. Ainsi :

$$\begin{array}{lll} & 1 \leqslant |k| & \\ \text{donc} & |p| \leqslant |k|\,|p| & \textit{(car : } |p| \geqslant 0\textit{)} \\ \text{d'où} & |p| \leqslant |n| & \\ \text{ainsi} & -|n| \leqslant p \leqslant |n| & \end{array}$$

  Or $p \in \mathbb{Z}$. On en déduit : $p \in [\![-|n|, |n|]\!]$.

  Finalement : $\mathcal{D}_n \subset [\![-|n|, |n|]\!]$.

- On en conclut :

$$\begin{array}{rcl} \text{Card}(\mathcal{D}_n) & \leqslant & \text{Card}\left([\![-|n|, |n|]\!]\right) \\ & & \shortparallel \\ & & |n| - (-|n|) + 1 \quad = \quad 2\,|n| + 1 \end{array}$$

  Finalement n n'admet qu'un nombre fini de diviseurs (au plus $2\,|n|+1$).
  Remarquons que 0 *ne peut être un diviseur de* n*, donc* n *admet au plus* $2\,|n|$ *diviseurs.*

2) Soit $(a, b) \in \mathbb{Z}^2$.

- Démontrons ***1) ⇒ 2)***.
  Supposons : $a \mid b$. Alors il existe $k \in \mathbb{Z}$ tel que : $b = k\, a$.
  On en déduit : $b = (-k) \times (-a)$. Or $-k \in \mathbb{Z}$. D'où : $-a \mid b$.
- Démontrons ***2) ⇒ 3)***.
  Supposons : $-a \mid b$. Alors il existe $k \in \mathbb{Z}$ tel que : $b = k \times (-a)$.
  On en déduit : $-b = k \times a$. Or $k \in \mathbb{Z}$. D'où : $a \mid -b$.
- Démontrons ***3) ⇒ 4)***.
  Supposons : $a \mid -b$. Alors il existe $k \in \mathbb{Z}$ tel que : $-b = k\, a$.
  On en déduit : $-b = (-k) \times (-a)$. Or $-k \in \mathbb{Z}$. D'où : $-a \mid -b$.
- Démontrons ***4) ⇒ 1)***.
  Supposons : $-a \mid -b$. Alors il existe $k \in \mathbb{Z}$ tel que : $-b = k \times (-a)$.
  On en déduit : $b = k \times a$. Or $k \in \mathbb{Z}$. D'où : $a \mid b$.

□

Remarque
Ce nombre maximal de diviseurs ($2\,|n|$) est en fait optimal. En effet, le nombre 2 admet exactement $2 \times |2| = 4$ diviseurs : -2, -1, 1 et 2.

Proposition 3.
Soit $(p,q,r) \in \mathbb{Z}^3$.

1) *Réflexivité :*

$$\boxed{p \mid p}$$

2) *Transitivité :*

$$\boxed{\left.\begin{array}{l} p \mid q \\ q \mid r \end{array}\right\} \quad \Rightarrow \quad p \mid r}$$

3)
$$\boxed{\left.\begin{array}{l} p \mid q \\ p \mid r \end{array}\right\} \quad \Rightarrow \quad \forall (\lambda,\mu) \in \mathbb{Z}^2,\ p \mid (\lambda q + \mu r)}$$

En particulier :

a)
$$\boxed{\left.\begin{array}{l} p \mid q \\ p \mid r \end{array}\right\} \quad \Rightarrow \quad p \mid (q+r)}$$

b)
$$\boxed{\left.\begin{array}{l} p \mid q \\ p \mid r \end{array}\right\} \quad \Rightarrow \quad p \mid (q-r)}$$

4) *Compatibilité avec l'exponentiation entière :*

$$\boxed{p \mid q \quad \Rightarrow \quad \forall n \in \mathbb{N},\ p^n \mid q^n}$$

5) $p \mid q \ \Rightarrow\ p\,r \mid q\,r$.

Démonstration.

1) On note : $p = 1 \times p$ (et $1 \in \mathbb{Z}$). On en déduit bien : $p \mid p$.

2) Supposons : $p \mid q$ et $q \mid r$. Alors :

- $\times$ il existe $k_1 \in \mathbb{Z}$ tel que : $q = k_1\,p$,
- $\times$ il existe $k_2 \in \mathbb{Z}$ tel que : $r = k_2\,q$.

On en déduit :

$$r \ = \ k_2\,q \ = \ k_2\,(k_1\,p) \ = \ k_2\,k_1\,p$$

Ainsi, en notant $k_3 = k_2\,k_1 \in \mathbb{Z}$, on obtient : $r = k_3\,p$.
On a bien démontré : $p \mid r$.

3) Soit $(\lambda,\mu) \in \mathbb{Z}^2$. Supposons : $(p \mid q)$ `ET` $(p \mid r)$. Alors :

- $\times$ il existe $k_1 \in \mathbb{Z}$ tel que : $q = k_1\,p$,
- $\times$ il existe $k_2 \in \mathbb{Z}$ tel que : $r = k_2\,p$.

Ainsi :

$$\lambda\,q + \mu\,r \ = \ \lambda\,k_1\,p + \mu\,k_2\,p \ = \ (\lambda\,k_1 + \mu\,k_2)\,p$$

En notant $k_3 = \lambda\,k_1 + \mu\,k_2 \in \mathbb{Z}$ (car $(\lambda,\mu) \in \mathbb{Z}^2$), on obtient : $\lambda\,q + \mu\,r = k_3\,p$.
On en déduit : $p \mid (\lambda\,q + \mu\,r)$.

4) Soit $n \in \mathbb{N}^*$. Supposons : $p \mid q$.
Alors il existe $k \in \mathbb{Z}$ tel que : $q = k\,p$. Ainsi :

$$q^n \ = \ (k\,p)^n \ = \ k^n\,p^n$$

En notant $k' = k^n \in \mathbb{Z}$, on obtient :$q^n = k'\,p^n$. On en déduit : $p^n \mid q^n$.

5) Supposons : $p \mid q$.
Alors il existe $k \in \mathbb{Z}$ tel que : $q = k\,p$. Ainsi :

$$q\,r \ = \ (k\,p)\,r \ = \ k\,(p\,r)$$

On en déduit : $p\,r \mid q\,r$.

□

On pourrait penser (dans un moment d'égarement) que la relation de divisibilité est *antisymétrique*.

- On dit qu'une relation R est antisymétrique si elle vérifie la propriété suivante : pour tout $(x, y) \in E^2$,

$$(xRy \texttt{ ET } yRx) \Leftrightarrow (x = y)$$

- La relation de divisibilité dans $\mathbb{Z}$ vérifie seulement une propriété approchant : pour tout $(p, q) \in \mathbb{Z}^2$,

$$\big((p \mid q) \texttt{ ET } (q \mid p)\big) \Leftrightarrow \big((p = q) \texttt{ OU } (p = -q)\big)$$

Démontrons la.

Démonstration.
Soit $(p, q) \in \mathbb{Z}^2$. On procède par double implication.

($\Rightarrow$) Supposons : $(p \mid q)$ ET $(q \mid p)$. Alors :

× il existe $k_1 \in \mathbb{Z}$ tel que : $q = k_1\, p$,

× il existe $k_2 \in \mathbb{Z}$ tel que : $p = k_2\, q$.

Ainsi :

$$q = k_1\, p = k_1\, (k_2\, q) = k_1\, k_2\, q$$

On en déduit : $k_1\, k_2 = 1$.
Or $(k_1, k_2) \in \mathbb{Z}^2$ (ce sont des entiers), donc :

$$(k_1 = 1 \texttt{ ET } k_2 = 1) \texttt{ OU } (k_1 = -1 \texttt{ ET } k_2 = -1)$$

On en déduit :

$$p = q \texttt{ OU } p = -q$$

($\Leftarrow$) Supposons : $p = q$ OU $p = -q$. Deux cas se présentent :

× si $p = q$, alors : $p = 1 \times q$ et $q = 1 \times p$.
Ainsi, comme $1 \in \mathbb{Z}$: $q \mid p$ et $p \mid q$.

× si $p = -q$, alors : $p = -1 \times q$ et $q = -1 \times p$.
Ainsi, comme $-1 \in \mathbb{Z}$: $q \mid p$ et $p \mid q$.

Finalement, dans tous les cas : $(p \mid q)$ ET $(q \mid p)$. □

Remarque

- Soit $(p, q) \in \mathbb{Z}^2$. On a la propriété suivante :

$$(p \mid q) \Leftrightarrow (|p| \mid |q|)$$

(on laisse la démonstration au lecteur)

- Comme $(p, q) \in \mathbb{Z}^2$, alors : $(|p|, |q|) \in \mathbb{N}^2$.
Grâce à l'équivalence précédente, on établit un lien entre la divisibilité sur $\mathbb{Z}$ et la divisibilité sur $\mathbb{N}$. Mieux que cela, on peut limiter l'étude de la divisibilité à $\mathbb{N}$ (plutôt que $\mathbb{Z}$).

Exercice 2
Déterminer les entiers relatifs n tels que : $2n - 3 \mid n + 9$.

Démonstration.
On procède par analyse-synthèse.

- **Analyse**.
Supposons : $2n - 2 \mid n + 9$.
  - 1ère étape : on cherche un multiple de $2n - 3$ qui ne dépend pas de n.
  On sait :
  × d'une part : $2n - 3 \mid n + 9$,
  × d'autre part : $2n - 3 \mid 2n - 3$.
  Donc $2n - 3$ divise toute combinaison linéaire de $n + 9$ et $2n - 3$. En particulier :
  $$2n - 3 \mid \big(2 \times (n + 9) - 1 \times (2n - 3)\big)$$
  D'où : $2n - 3 \mid 21$.

- 2ème étape : on en déduit les valeurs possibles de n.
  - × On a obtenu : $2n-3 \mid 21$.
  - × Or : $21 = 3 \times 7$.

  Ainsi : $2n-3 \in \{-21,-7,-3,-1,1,3,7,21\}$. Enfin :

$$2n-3 = -21 \quad \Leftrightarrow \quad 2n = -18 \quad \Leftrightarrow \quad n = -9$$

  De même :

$$2n-3=-7 \Leftrightarrow n=-2 \qquad 2n-3=-3 \Leftrightarrow n=0$$
$$2n-3=-1 \Leftrightarrow n=1 \qquad 2n-3=1 \Leftrightarrow n=2$$
$$2n-3=3 \Leftrightarrow n=3 \qquad 2n-3=7 \Leftrightarrow n=5$$
$$2n-3=21 \Leftrightarrow n=12$$

  Finalement : $n \in \{-9,-2,0,1,2,3,5,12\}$.

- **Synthèse**.
  Vérifions maintenant que chacun des entiers de $\{-9,-2,0,1,2,3,5,12\}$ convient.
  - × si $n=-9$, alors : $2n-3=-21$ et $n+9=0$.
    On a bien : $2n-3 \mid n+9$.
  - × si $n=-2$, alors : $2n-3=-7$ et $n+9=7$.
    On a bien : $2n-3 \mid n+9$.
  - × ...
  - × si $n=5$, alors : $2n-3=7$ et $n+9=14$.
    On a bien : $2n-3 \mid n+9$.
  - × si $n=12$, alors : $2n-3=21$ et $n+9=21$.
    On a bien : $2n-3 \mid n+9$.

Finalement, l'ensemble des entiers $n \in \mathbb{Z}$ tels que $2n-3 \mid n+9$ est $\{-9,-2,0,1,2,3,5,12\}$. □

Remarque
Détaillons le principe d'un raisonnement par analyse-synthèse.

- Dans la première partie du raisonnement, on suppose que l'entier $n \in \mathbb{Z}$ vérifie : $2n-3 \mid n+9$. En se basant sur cette hypothèse, on obtient une caractérisation des entiers n :

$$n \in \{-9,-2,0,1,2,3,5,12\}$$

  Il faut bien comprendre que dans cette première partie du raisonnement, on a **supposé** (et non démontré !) : $2n-3 \mid n+9$. C'est pourquoi il faut, dans la deuxième partie du raisonnement, démontrer que les entiers n obtenus véfient bien la relation : $2n-3 \mid n+9$.
  L'idée est alors de trouver des entiers n tel que caractérisé dans la partie **analyse** et de **démontrer** que l'on obtient ainsi des entiers qui satisfont les exigences de la question.

- En résumé, un raisonnement par **analyse-synthèse** se déroule en deux temps :
  - × **analyse** : on suppose qu'un objet vérifie certains critères (ici, on suppose que l'entier n vérifie $2n-3 \mid n+9$). Si cet objet vérifie ces critères, il est alors d'une certaine forme ($n \in \{-9,-2,0,1,2,3,5,12\}$).
  - × **synthèse** : on vérifie que l'objet obtenu lors de la phase d'analyse répond bien aux critères initiaux (les entiers $-9,-2,0,1,2,3,5,12$ ainsi obtenus vérifient bien $2n-3 \mid n+9$).

  Ce schéma de démonstration permet non seulement de conclure :

$$\text{l'objet répond à certains critères} \quad \Leftrightarrow \quad \text{l'objet s'écrit sous une forme particulière}$$

  mais aussi de démontrer que chacune des deux propositions de l'équivalence est vérifiée.

Exercice 3
Démontrer que pour tout $n \in \mathbb{N}$: $11 \mid 3^{3n} - 4^{2n}$.

Démonstration.
Soit $n \in \mathbb{N}$.

$$\begin{aligned} 3^{3n} - 4^{2n} &= (3^3)^n - (4^2)^n = 27^n - 16^n \\ &= (27-16) \sum_{k=0}^{n-1} 27^k \, 16^{n-1-k} \\ &= 11 \times \sum_{k=0}^{n-1} 27^k \, 16^{n-1-k} \end{aligned}$$

Or : $\sum_{k=0}^{n-1} 27^k \, 16^{n-1-k} \in \mathbb{Z}$. On en déduit : $11 \mid 3^{3n} - 4^{2n}$. □

Exercice 4
Soit $p \in \mathbb{N}$. On suppose que p n'est divisible ni par 2, ni par 3. Démontrer : $24 \mid p^2 - 1$.

Démonstration.

- On commence par remarquer : $p^2 - 1 = (p-1)(p+1)$.
- Les entiers $p-1$, p et $p+1$ sont consécutifs. On en déduit :
  - × comme $2 \nmid p$, alors : $2 \mid p-1$ **et** $2 \mid p+1$.
    De plus : $4 \mid p-1$ **ou** $4 \mid p+1$. D'où : $2 \times 4 \mid (p-1)(p+1)$.
  - × comme $3 \nmid p$, alors : $3 \mid p-1$ **ou** $3 \mid p+1$. D'où : $3 \mid (p-1)(p+1)$.

  Finalement : $2 \times 4 \times 3 \mid (p-1)(p+1)$.

Ainsi : $24 \mid p^2 - 1$. □

II. Division euclidienne

II.1. Théorème et exemples

Théorème 1. (Division euclidienne dans $\mathbb{Z}$)
Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$.

Alors il existe un unique $(q,r) \in \mathbb{Z}^2$ tels que : $\begin{cases} a = bq + r \\ 0 \leqslant r < |b| \end{cases}$

On dit que :

× *l'entier q est le* quotient de la division euvlidienne de a par b.

× *l'entier r est le* reste de la division euvlidienne de a par b.

Démonstration.
Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$.

***a)* Existence**.
Deux cas se présentent.

- si $b > 0$, alors on note A l'ensemble défini par : $A = \{n \in \mathbb{Z} \mid nb > a\}$.
  - × Démontrons : $A \neq \varnothing$. Pour cela, on montre : $|a| + 1 \in A$.
    - Tout d'abord : $|a| + 1 \in \mathbb{Z}$.
    - De plus : $|a| + 1 > |a|$ et $b > 0$. D'où : $\big(|a| + 1\big) b > |a| \, b$.
      Or $b > 0$ et $b \in \mathbb{Z}$. Donc : $b \geqslant 1$. Ainsi : $|a| \, b \geqslant |a|$. Alors :

$$\big(|a| + 1\big) \, b \; > \; |a| \, b \; \geqslant \; |a| \; \geqslant \; a$$

    Finalement : $|a| + 1 \in A$.
  - × Démontrons que A est minorée (par $-|a|$). Autrement dit, démontrons : $\forall n \in A$, $n \geqslant -A$.
    Raisonnons par l'absurde.
    Supposons qu'il existe $m_0 \in A$ tel que : $m_0 < -|a|$.
    Alors, comme $b > 0$: $m_0 \, b < -|a| \, b$.

Or $b \geqslant 1$, donc : $-|a|\,b \leqslant -|a|$. Ainsi :

$$m_0\,b \;<\; -|a|\,b \;\leqslant\; -|a| \;\leqslant\; a$$

Finalement : $m_0\,b < a$. Donc : $m_0 \notin A$.
Absurde !

L'ensemble A vérifie :

1) $A \subset \mathbb{Z}$,

2) $A \neq \varnothing$,

3) A est minoré.

On en déduit que l'ensemble A possède un plus petit élément que l'on note n_0.

Remarque

- On admet ce résultat.
- Notons que ces trois hypothèses sont minimales pour qu'un ensemble possède un plus petit élément. En effet :
  - × l'ensemble $\{\frac{1}{n} \mid n \in \mathbb{N}^*\}$ est bien non vide et minorée (par 0), mais n'admet pas de plus petit élément.
    *Cet ensemble vérifie les propriétés **2)** et **3)** mais pas **1)**.*
  - × l'ensemble $\{-n \mid n \in \mathbb{N}\}$ est inclus dans $\mathbb{Z}$ et non vide, mais n'admet pas de plus petit élément.
    *Cet ensemble vérifie les propriétés **1)** et **2)** mais pas **3)**.*
  - × l'ensemble $\varnothing$ est inclus dans $\mathbb{Z}$ et minoré, mais n'admet pas de plus petit élément.
    *Cet ensemble vérifie les propriétés **2)** et **3)** mais pas **2)**.*

Comme $n_0 - 1 < n_0$ et $b > 0$, alors : $(n_0 - 1)\,b < n_0\,b$.
Ainsi, par définition de n_0 :

$$(n_0 - 1)\,b \;\leqslant\; a \;<\; n_0\,b$$

× On pose alors : $q = n_0 - 1 \in \mathbb{Z}$. On obtient :

$$\begin{array}{ccccc} q\,b & \leqslant & a & < & (q+1)\,b \\ & & & & \shortparallel \\ & & & & q\,b + b \end{array}$$

D'où : $0 \leqslant a - q\,b < b \quad (*)$.

× On pose alors : $r = a - q\,b \in \mathbb{Z}$. On obtient :

$$\begin{cases} (q, r) \in \mathbb{Z}^2 \\ a \;=\; b\,q + r \quad \textit{(par définition de } r\textit{)} \\ 0 \;\leqslant\; r \;<\; b = |b| \quad \textit{(d'après } (*)\textit{)} \end{cases}$$

- si $b \leq 0$, alors : $-b > 0$.
  Ainsi, d'après le cas précédent, il existe $(q, r) \in \mathbb{Z}^2$ tel que :

$$\begin{cases} a \;=\; (-b) \times q + r \\ 0 \leqslant r < -b \end{cases}$$

  D'où :

$$\begin{cases} a \;=\; b \times (-q) + r \\ 0 \leqslant r < |b| \end{cases}$$

  Le couple $(-q, r)$ convient donc.

b) **Unicité**.
Soit $(q_1, q_2, r_1, r_2) \in \mathbb{Z}^4$ tel que :

$$\begin{cases} a \;=\; b\,q_1 + r_1 \\ 0 \leqslant r_1 < |b| \end{cases} \qquad \begin{cases} a \;=\; b\,q_2 + r_2 \\ 0 \leqslant r_2 < |b| \end{cases}$$

- Alors : $b\,q_1 + r_1 = b\,q_2 + r_2$. D'où ;

$$r_1 - r_2 \;=\; b\,q_2 - b\,q_1 \;=\; b\,(q_2 - q_1)$$

- De plus, comme $0 \leqslant r_1 < |b|$ et $-|b| < r_2 \leqslant 0$:

$$\begin{array}{ll} & -|b| < r_1 - r_2 < |b| \\ \text{donc} & -|b| < b\,(q_2 - q_1) < |b| \\ \text{d'où} & |b\,(q_2 - q_1)| < |b| \\ \text{ainsi} & |b|\,|q_2 - q_1| < |b| \end{array}$$

  Or : $|b| > 0$. D'où : $0 \leqslant |q_2 - q_1| < 1$.
  Or $|q_2 - q_1| \in \mathbb{N}$. On en déduit : $|q_2 - q_1| = 0$. Donc : $q_2 - q_1 = 0$, *i.e.* $q_2 = q_1$.
- Enfin :

$$r_1 - r_2 \;=\; b\,(q_2 - q_1) \;=\; b \times 0 \;=\; 0$$

  D'où : $r_1 = r_2$.

□

Remarque
C'est l'unicité du quotient et du reste qui implique l'utilisation d'articles définis : **LE** quotient, **LE** reste d'une division euclidienne.

Corollaire 1. (Division euclidienne dans $\mathbb{N}$)
Soit $(a, b) \in \mathbb{N} \times \mathbb{N}^*$.
Alors il existe un unique $(q, r) \in \mathbb{N}^2$ *tels que :* $\begin{cases} a = b\,q + r \\ 0 \leqslant r < b \end{cases}$

Démonstration.
L'unicité du couple (q, r) pour la division euclidienne dans $\mathbb{N}$ provient de l'unicité de la division euclidienne dans $\mathbb{Z}$. On s'intéresse donc maintenant à l'existence d'un couple (q, r) tel que décrit dans le Corollaire.

a) **Méthode 1** : Descente de Fermat.
Soit $(a, b) \in \mathbb{N} \times \mathbb{N}^*$.

- Deux cas se présentent :
  × si $b > a$, alors le couple $(q, r) = (0, a)$ convient. En effet :

$$\begin{cases} (q, r) \in \mathbb{N}^2 \\ a \;=\; b \times 0 + a \;=\; b\,q + r \\ 0 \leqslant r < b \quad \textit{(car } a < b\textit{)} \end{cases}$$

  × si $0 < b \leqslant a$, alors il existe $q_1 \in \mathbb{N}^*$ tel que : $q_1\,b \leqslant a$.
  (en effet, l'ensemble $A = \{n \in \mathbb{N}^* \mid n\,b \leqslant a\}$ *est non vide : il contient au moins le nombre* 1*)*

  On note alors : $r_1 = a - b\,q_1$. On a bien : $r_1 \in \mathbb{N}$. En effet : $r_1 = a - b\,q_1 \in \mathbb{Z}$. De plus, par définition de q_1 : $b\,q_1 \leqslant a$. D'où : $0 \leqslant a - b\,q_1 = r_1$.
  Deux nouveaux cas se présentent :

  - si $r_1 < b$, alors le couple (q_1, r_1) convient. En effet :

$$\begin{cases} (q_1, r_1) \in \mathbb{N}^2 \\ a \;=\; b\,q_1 + r_1 \qquad \textit{(par définition de } r_1\textit{)} \\ 0 \leqslant r_1 < b \qquad \textit{(on rappelle : } r_1 \in \mathbb{N}\textit{)} \end{cases}$$

  - si $b \leqslant r_1$, alors il existe $q_2 \in \mathbb{N}^*$ tel que : $b\,q_2 \leqslant r_1$.
    On note alors $r_2 = r_1 - b\,q_2 \in \mathbb{N}$. Deux nouveaux cas se présentent :

    ▸ si $r_2 < b$, alors le couple $(q_1 + q_2, r_2) \in \mathbb{N}^2$ convient. En effet :

$$\begin{array}{rcll} a & = & b\,q_1 + r_1 & \textit{(par définition de } r_1\textit{)} \\ & = & b\,q_1 + (b\,q_2 + r_2) & \textit{(par définition de } r_2\textit{)} \\ & = & b\,(q_1 + q_2) + r_2 & \end{array}$$

    De plus : $0 \leqslant r_2 < b$.

▸ si $b \leqslant r_2$, alors il existe $q_3 \in \mathbb{N}^*$ tel que : $b\,q_3 \leqslant r_2$.
On note alors $r_3 = r_2 - b\,q_3 \in \mathbb{N}$. On itère alors le processus...

- On cherche alors à savoir si ce processus s'arrête. Autrement dit, on cherche à savoir s'il existe $i_0 \in \mathbb{N}^*$ tel que : $r_{i_0} < b$.
Raisonnons par l'absurde.
Supposons : $\forall i \in \mathbb{N}^*,\ r_i \geqslant b$.
  × Démontrons que la suite $(r_i)_{i\in\mathbb{N}^*}$ est strictement décroissante.
  Soit $i \in \mathbb{N}^*$.
  Comme $r_i \leqslant b$, il existe $q_{i+1} \in \mathbb{N}^*$ tel que : $b\,q_{i+1} \leqslant r_i$.
  On note alors : $r_{i+1} = r_i - b\,q_i$. Comme $b > 0$ et $q_{i+1} > 0$, on obtient :

$$\begin{array}{ll} & b\,q_{i+1} > 0 \\ \text{donc} & -b\,q_{i+1} < 0 \\ \text{d'où} & r_i - b\,q_{i+1} < r_i \\ \text{ainsi} & r_{i+1} < r_i \end{array}$$

  La suite $(r_i)_{i\in\mathbb{N}^*}$ est donc strictement décroissante.
  × Ainsi la suite $(r_i)_{i\in\mathbb{N}^*}$ est :
  - strictement décroissante,
  - minorée par b.
  Elle converge donc vers une limite ℓ, *i.e.* :

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N}^*,\ \forall i \geqslant N,\ |r_i - \ell| \leqslant \varepsilon$$

  En particulier, il existe $N \in \mathbb{N}^*$ tel que, pour tout $i \geqslant N$:

$$\begin{array}{ll} & |r_i - \ell| \leqslant \dfrac{1}{4} \\ \text{donc} & -\dfrac{1}{4} \leqslant r_i - \ell \leqslant \dfrac{1}{4} \\ \text{d'où} & \ell - \dfrac{1}{4} \leqslant r_i \leqslant \ell + \dfrac{1}{4} \\ \text{ainsi} & r_i \in [\ell - \frac{1}{4}\ ;\ \ell + \frac{1}{4}] \end{array}$$

  Or l'intervalle $[\ell - \frac{1}{4}\ ;\ \ell + \frac{1}{4}]$ est de longueur :

$$\left(\ell + \frac{1}{4}\right) - \left(\ell - \frac{1}{4}\right) = \frac{1}{2} < 1$$

  Il contient donc au plus un entier n_0.
  Deux cas se présentent donc :
  - si l'intervalle ne contient pas d'entier.
  Absurde ! (car $r_i \in \mathbb{N}$ appartient à cet intervalle)
  - si l'intervalle contient un entier n_0. Alors, comme : $\forall i \in \mathbb{N}^*,\ r_i \in \mathbb{N}^*$, on obtient :

$$\forall i \in \mathbb{N}^*,\ r_i = n_0$$

  Autrement dit, la suite $(r_i)_{i\in\mathbb{N}^*}$ est constante à partir d'un certain rang.
  Absurde ! (car cette suite est strictement décroissante)
  Il existe donc $i_0 \in \mathbb{N}^*$ tel que : $r_{i_0} < b$.
  × Le couple $(q_1 + \cdots + q_{i_0}, r_{i_0}) \in \mathbb{N}^2$ convient. En effet :

$$\begin{array}{rcll} a & = & b\,q_1 + r_1 & \\ & = & b\,q_1 + (b\,q_2 + r_2) & \\ & = & b\,(q_1 + q_2) + r_2 & \\ & = & b\,(q_1 + q_2) + (b\,q_3 + r_3) & \textit{(par définition de } r_3\textit{)} \\ & = & b\,(q_1 + q_2 + q_3) + r_3 & \\ & \cdots & & \\ & = & b\,(q_1 + \cdots + q_{i_0-1}) + r_{i_0-1} & \\ & = & b\,(q_1 + \cdots + q_{i_0-1}) + (b\,q_{i_0} + r_{i_0}) & \textit{(par définition de } r_{i_0}\textit{)} \\ & = & b\,(q_1 + \cdots + q_{i_0}) + r_{i_0} & \end{array}$$

  De plus : $0 \leqslant r_{i_0} < b$.

b) **Méthode 2** : Récurrence.
Soit $b \in \mathbb{N}^*$. Démontrons par récurrence : $\forall a \in \mathbb{N}$, $\mathscr{P}(a)$

où $\mathscr{P}(a)$: il existe $(q,r) \in \mathbb{N}^2$ tel que : $\begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases}$.

- **Initialisation** :
  Si $a = 0$, alors le couple $(q,r) = (0,0) \in \mathbb{N}^2$ convient. En effet :
  $$\begin{cases} a = 0 = b \times 0 + 0 = bq + r \\ 0 \leqslant r < b \end{cases}$$
  D'où $\mathscr{P}(0)$.
- **Hérédité** : soit $a \in \mathbb{N}$.
  Supposons $\mathscr{P}(a)$ et démontrons $\mathscr{P}(a+1)$ (*i.e.* il existe $(q,r) \in \mathbb{N}^2$ tel que : $\begin{cases} a+1 = bq + r \\ 0 \leqslant r < b \end{cases}$)
  Par hypothèse de récurrence, il existe $(q',r') \in \mathbb{N}^2$ tel que :
  $$\begin{cases} a = bq' + r' \\ 0 \leqslant r' < b \end{cases}$$
  Ainsi : $a + 1 = bq' + r' + 1$. Deux cas se présentent :
  - si $r' + 1 < b$, alors le couple $(q,r) = (q', r'+1) \in \mathbb{N}^2$ convient. En effet :
    - Tout d'abord :
      $$a + 1 = bq' + (r'+1) = bq + r$$
    - Ensuite : $0 \leqslant r' < r' + 1 < b$. D'où : $0 \leqslant r < b$.
  - si $r' + 1 \geqslant b$, alors :
    - d'une part : $r' + 1 \geqslant b$,
    - d'autre part : $r' + 1 < b + 1$ (car : $r' < b$).
      Or $r' + 1 \in \mathbb{N}$, donc : $r' + 1 \leqslant b$.

    Finalement : $r' + 1 = b$. D'où :
    $$a = bq' + r' + 1 = bq' + b = b(q'+1)$$
    Ainsi le couple $(q,r) = (q'+1, 0) \in \mathbb{N}^2$ convient. En effet :
    $$\begin{cases} a + 1 = b(q' + 1 + 0 = bq + r \\ 0 \leqslant r < b \qquad (car\ r = 0) \end{cases}$$
    D'où $\mathscr{P}(a+1)$.

Par principe de récurrence, pour tout $a \in \mathbb{N}$, il existe $(q,r) \in \mathbb{N}^2$ tel que :
$\begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases}$

□

Remarque
La 2ème démonstration a l'avantage d'être bien plus courte que la 1ère. Cependant, la descente de Fermat possède un réel atout : c'est une preuve constructive. C'est-à-dire elle fournit un moyen d'obtenir explicitement les entiers q et r. Elle ne se contente pas d'établir leur existence. On peut alors utiliser cette démonstration pour coder un algorithme de division euclidienne. On présente un code possible en section suivante.

Exemples
- Les nombres $q = 7$ et $r = 2$ sont respectivement le quotient et le reste de la division euclidienne de 37 par 5. En effet :
  $$\begin{cases} 37 = 5 \times 7 + 2 \\ 0 \leqslant 2 < 5 \end{cases}$$
- Les nombres $q = -7$ et $r = 7$ sont respectivement le quotient et le reste de la division euclidienne de -63 par 10. En effet :
  $$\begin{cases} -63 = 10 \times (-7) + 7 \\ 0 \leqslant 7 < 10 \end{cases}$$

- Les nombres $q = 7$ et $r = 4$ sont respectivement le quotient et le reste de la division euclidienne de -45 par -7. En effet :

$$\begin{cases} -45 = (-7) \times 7 + 4 \\ 0 \leqslant 4 < |-7| \end{cases}$$

Le reste d'une division euclidienne est **toujours** positif.
Ainsi, l'assertion suivante est fausse :

~~Les nombres $q = -6$ et $r = -3$ sont respectivement le quotient et le reste de la division euclidienne de -63 par 10.~~

En effet, même si $-63 = 10 \times q + r$, on n'a pas : $r \geqslant 0$.

Proposition 4. (Lien entre divisibilité et division euclidienne)
Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$.
L'entier b divise a si et seulement si le reste de la division euclidienne de a par b est nul.

Démonstration.
On raisonne par équivalence.

$$\begin{aligned} & b \mid a \\ \Leftrightarrow\ & \exists k \in \mathbb{Z},\ a = b\,k \\ \Leftrightarrow\ & \text{le reste de la division euclidienne de } a \text{ par } b \text{ est } 0 \text{ (et le quotient est } k) \end{aligned}$$

(par unicité du quotient et du reste de la division euclidienne)

□

Proposition 5.
Soit $p \in \mathbb{N}$ tel que : $p \geqslant 2$.
Tout $n \in \mathbb{Z}$, il existe un unique $q \in \mathbb{Z}$ tel que n s'écrive sous l'une (et une seule) des formes suivantes :

$$q\,p, \quad q\,p + 1, \quad q\,p + 2, \quad \ldots, \quad q\,p + (p-1)$$

Démonstration.
Soit $n \in \mathbb{N}$.
On effectue la division euclidienne de n par p. Alors il existe un unique $(q, r) \in \mathbb{Z}^2$ tel que :

$$\begin{cases} n = p\,q + r \\ 0 \leqslant r < p \end{cases}$$

On vient de préciser que cette écriture est unique. De plus $r \in [\![0, p[\![= \{0, 1, \ldots, p-1\}$. □

Exemples

- Tout $n \in \mathbb{Z}$ s'écrit sous la forme $2k$ ou $2k+1$.
  Autrement dit, tout entier est soit pair, soit impair.
- Tout $n \in \mathbb{Z}$ s'écrit sous la forme $3k$, $3k+1$ ou $3k+2$.

Exercice 5 Soit $n \in \mathbb{Z}$. Démontrer que $n^2 - 2$ n'est jamais divisible par 3.

Démonstration.

- On commence par effectuer la division euclidienne de n par 3.
  Il existe $(k, r) \in \mathbb{Z}^2$ tel que : $\begin{cases} n = 3\,k + r \\ 0 \leqslant r < 3 \end{cases}$
- Trois cas se présentent alors :
  × si $r = 0$, alors : $n = 3k$. D'où :

$$n^2 - 2 = (3k)^2 - 2 = 9k^2 - 2 = 9k^2 - 3 + 1 = 3\,(3k^2 - 1) + 1$$

  Comme $q = 3k^2 - 1$ et $r = 1$ vérifient :

$$\begin{cases} n^2 - 2 = 3\,q + r \\ 0 \leqslant r < 3 \end{cases}$$

  alors, par unicité du quotient et du reste de la division euclidienne, r est le reste de la division euclidienne de $n^2 - 2$ par 3.
  Or : $r = 1 \neq 0$. Donc : $3 \nmid n^2 - 2$.

× si $r = 1$, alors : $n = 3k + 1$. D'où :

$$\begin{aligned} n^2 - 2 &= (3k+1)^2 - 2 \\ &= 9k^2 + 6k + 1 - 2 \\ &= 9k^2 + 6k - 3 + 2 \\ &= 3\left(3k^2 + 3k - 1\right) + 2 \end{aligned}$$

Comme $q = 3k^2 + 3k - 1$ et $r = 2$ vérifient :

$$\begin{cases} n^2 - 2 = 3q + r \\ 0 \leqslant r < 3 \end{cases}$$

alors r est le reste de la division euclidienne de $n^2 - 2$ par 3.
Or : $r = 2 \neq 0$. Donc : $3 \nmid n^2 - 2$.

× si $r = 2$, alors : $n = 3k + 2$. D'où :

$$\begin{aligned} n^2 - 2 &= (3k+2)^2 - 2 \\ &= 9k^2 + 12k + 4 - 2 \\ &= 9k^2 + 12k + 2 \\ &= 3\left(3k^2 + 4k\right) + 2 \end{aligned}$$

Comme $q = 3k^2 + 3k - 1$ et $r = 2$ vérifient :

$$\begin{cases} n^2 - 2 = 3q + r \\ 0 \leqslant r < 3 \end{cases}$$

alors r est le reste de la division euclidienne de $n^2 - 2$ par 3.
Or : $r = 2 \neq 0$. Donc : $3 \nmid n^2 - 2$.

Finalement, $n^2 - 2$ n'est jamais divisible par 3.

□

II.2. Algorithmique

On cherche dans cette partie à coder en **Python** la descente de Fermat présentée dans la démonstration de la division euclidienne dans $\mathbb{N}$. On propose la fonction suivante qui permet d'obtenir le quotient et le reste de la division euclidienne de `a` par `b` (où $(\texttt{a}, \texttt{b}) \in \mathbb{N} \times \mathbb{N}^*$) :

```
1  def Descente_Fermat(a, b)
2      q = 0
3      r = a
4      while r >= b:
5          q = q + 1
6          r = a - q * b
7      return q,r
```

Détaillons les éléments de ce script.

- **Début de la fonction**
  On commence par préciser la structure de la fonction :
  × cette fonction se nomme `Descente_Fermat`,
  × elle prend en entrée les paramètres `a` et `b`,
  × elle admet pour variables de sortie les variables `q` et `r`

```
1  def Descente_Fermat(a, b)
```

```
7      return q,r
```

  On initialise ensuite les variables de sortie `q` et `r` avec les valeurs fournies par le tout premier cas de la descente de Fermat.

```
2      q = 0
3      r = a
```

- **Structure itérative**
  Les lignes 4 à 6 consistent à déterminer le quotient q et le reste r de la division euclidienne de `a` par `b`. Pour cela, on doit augmenter la valeur de la variable `q` jusqu'à ce que la variable `r` ($r = a - q\,b$) vérifie : `r` $<$ `b`. Autrement dit, on doit augmenter la valeur de la variable `q` tant que la variable `r` vérifie : `r` $\geqslant$ `b`. Pour cela, on utilise une structure itérative (boucle while).

```
4        while r >= b:
```

  À chaque tour de boucle, on doit :

  1) incrémenter la variable `q` de 1.

```
5            q = q + 1
```

  2) mettre à jour la variable `r`.

```
6            r = a - q * b
```

  On est certain que le nombre d'itération de la boucle while est **fini**, puisqu'on a démontré que la descente de Fermat s'arrête toujours.
  À l'issue de cette boucle, la variable `r` vérifie :

$$\begin{cases} 0 \leqslant \texttt{r} < \texttt{b} \\ \texttt{r} = \texttt{a} - \texttt{q}\,\texttt{b} \end{cases}$$

  Ainsi :

$$\begin{cases} 0 \leqslant \texttt{r} < \texttt{b} \\ \texttt{a} = \texttt{q}\,\texttt{b} + \texttt{r} \end{cases}$$

  On a donc bien déterminé le quotient `q` et le reste `r` de la division euclidienne de `a` par `b`.

III. Congruences

III.1. Définition et premières propriétés

Définition (Congruence)
Soit $(m, n, p) \in \mathbb{Z}^2 \times \mathbb{N}^*$.
On dit que m et n sont *congrus modulo* p si $m - n$ est un multiple de p.
On écrit : $m \equiv n\ [p]$ ou $m \equiv n \mod(p)$.

Remarque
D'après cette définition :

$$m \equiv n\ [p] \quad \Leftrightarrow \quad p \mid (m-n) \quad \Leftrightarrow \quad \exists k \in \mathbb{Z},\ m - n = k\,p$$

Exemples

- 1^{er} exemple : $9 \equiv 19\ [5]$. En effet : $9 - 19 = -10$ et $5 \mid -10$.
- 2^{nd} exemple : $-7 \equiv -1\ [3]$. En effet : $-7 - (-1) = -6$ et $3 \mid -6$.

Proposition 6.
Soit $(a, b, p) \in \mathbb{Z}^2 \times \mathbb{Z}^*$.

$$a \equiv b\ [p] \quad \Leftrightarrow \quad \begin{array}{l} a \text{ et } b \text{ ont même reste dans leur} \\ \text{division euclidienne par } p \end{array}$$

Démonstration.
On procède par double implication.
($\Rightarrow$) Supposons : $a \equiv b\ [p]$.

- Tout d'abord : $p \mid a - b$. Il existe donc $k \in \mathbb{Z}$ tel que : $a - b = k\,p$. D'où : $a = k\,p + b$.
- On effectue alors la division euclidienne de b par p. Il existe $(q_1, r_1) \in \mathbb{Z}^2$ tel que :

$$\begin{cases} b = p\,q_1 + r_1 \\ 0 \leqslant r_1 < |p| \end{cases}$$

On en déduit :

$$a \;=\; p\,k+b \;=\; p\,k+(p\,q_1+r_1) \;=\; p\,(k+q_1)+r_1$$

En posant $(q_2,r_2)=(k+q_1,r_1)$, on obtient :

$$\begin{cases} (q_2,r_2)\in\mathbb{Z}^2 \\ a \;=\; p\,q_2+r_2 \\ 0\leqslant r_2<|p| \end{cases}$$

On en déduit que r_2 est le reste (et q_2 le quotient) de la division euclidienne de a par p.
On obtient bien : $r_1=r_2$.

($\Leftarrow$) Supposons que a et b ont même reste dans leur division euclidienne par p.
Alors il existe $(q_1,q_2,r)\in\mathbb{Z}^3$ tel que :

$$\begin{cases} a \;=\; p\,q_1+r \\ 0\leqslant r<|p| \end{cases} \qquad \begin{cases} b \;=\; p\,q_2+r \\ 0\leqslant r<|p| \end{cases}$$

Ainsi :

$$a-b \;=\; (p\,q_1+r)-(p\,q_2+r) \;=\; p\,(q_1-q_2)$$

En notant $k=q_1-q_2$, on a : $k\in\mathbb{Z}$ et $a-b=k$. Ainsi : $p\mid a-b$.
On en déduit : $a\equiv b\ [p]$.

□

Exemples

- 1er exemple : $475\equiv 1\ [2]$. En effet : $475=2\times 237+1$ et $1=2\times 0+1$.
- 2nd exemple : $8\equiv -1\ [3]$. En effet : $8=3\times 2+2$ et $-1=3\times(-1)+2$.
  Et d'ailleurs on a aussi : $8\equiv 2\ [3]$ *et* $-1\equiv 2\ [3]$.

Proposition 7.
Soient $(n,p)\in\mathbb{Z}^2$.

$$\boxed{n\equiv 0\ [p] \quad\Leftrightarrow\quad p\mid n}$$

III.2. Propriétés de la congruence

Proposition 8.
Soit $p\in\mathbb{Z}$. *Soit* $(a,b,c,d)\in\mathbb{Z}^4$.

1) *Réflexivité :* $\boxed{a\equiv a\ [p]}$

2) *Symétrie :*

$$\boxed{a\equiv b\ [p] \quad\Leftrightarrow\quad b\equiv a\ [p]}$$

3) *Transitivité :*

$$\boxed{\left.\begin{array}{l} a\equiv b\ [p] \\ b\equiv c\ [p] \end{array}\right\} \quad\Leftrightarrow\quad a\equiv c\ [p]}$$

4) *Compatibilité avec l'addition :*

$$\boxed{\left.\begin{array}{l} a\equiv b\ [p] \\ c\equiv d\ [p] \end{array}\right\} \quad\Rightarrow\quad a+c\equiv b+d\ [p]}$$

5) *Compatibilité avec la multiplication :*

$$\boxed{\left.\begin{array}{l} a\equiv b\ [p] \\ c\equiv d\ [p] \end{array}\right\} \quad\Rightarrow\quad a\,c\equiv b\,d\ [p]}$$

6) *Compatibilité avec l'exponentiation entière :*

$$\boxed{a\equiv b\ [p] \quad\Leftrightarrow\quad \forall n\in\mathbb{N},\ a^n\equiv b^n\ [p]}$$

Démonstration.

1) On sait : $p \mid 0$. Donc : $p \mid a-a$. Ainsi : $a \equiv a\ [p]$.

2) On raisonne par équivalence.

$$\begin{aligned} a \equiv b\ [p] &\Leftrightarrow p \mid a-b \\ &\Leftrightarrow p \mid (-1)\times(a-b) \\ &\Leftrightarrow p \mid b-a \\ &\Leftrightarrow b \equiv a\ [p] \end{aligned}$$

3) Supposons : $a \equiv b\ [p]$ et $b \equiv c\ [p]$. Alors :

× d'une part : $p \mid a-b$,

× d'autre part : $p \mid b-c$.

On en déduit : $p \mid \big((a-\cancel{b})+(\cancel{b}-c)\big)$. D'où : $a \equiv c\ [p]$.

4) Supposons : $a \equiv b\ [p]$ et $c \equiv d\ [p]$. Alors :

× d'une part : $p \mid a-b$,

× d'autre part : $p \mid c-d$.

On en déduit : $p \mid \big((a-b)+(c-d)\big)$. D'où : $p \mid \big((a+c)-(b+d)\big)$.
Finalement : $a+c \equiv b+d\ [p]$.

5) Supposons : $a \equiv b\ [p]$ et $c \equiv d\ [p]$. Alors :

× d'une part : $p \mid a-b$. Comme $c \in \mathbb{Z}$: $p \mid c\,(a-b)$. Donc : $p \mid a\,c-b\,c$.

× d'autre part : $p \mid c-d$. Comme $b \in \mathbb{Z}$: $p \mid b\,(c-d)$. Donc : $p \mid b\,c-b\,d$.

On en déduit : $p \mid \big((a\,c-\cancel{b\,c})+(\cancel{b\,c}-b\,d)\big)$. D'où : $p \mid (a\,c-b\,d)$.
Finalement : $a\,c \equiv b\,d\ [p]$.

6) On procède par double implication.

($\Rightarrow$) Supposons : $a \equiv b\ [p]$.
Démontrons par récurrence : $\forall n \in \mathbb{N}$, $\mathscr{P}(n)$ où $\mathscr{P}(n) : a^n \equiv b^n\ [p]$.

▸ **Initialisation** :
D'après ***1)*** : $1 \equiv 1\ [p]$. Ainsi : $a^0 \equiv b^0\ [p]$.
D'où $\mathscr{P}(0)$.

▸ **Hérédité** : soit $n \in \mathbb{N}$.
Supposons $\mathscr{P}(n)$ et démontrons $\mathscr{P}(n+1)$ (*i.e.* $a^{n+1} \equiv b^{n+1}\ [p]$).

× Par hypothèse de récurrence : $a^n \equiv b^n\ [p]$.

× Par hypothèse de ***6)*** : $a \equiv b\ [p]$.

D'après ***5)***, on en déduit : $a^{n+1} \equiv b^{n+1}\ [p]$.
D'où $\mathscr{P}(n+1)$.

Par principe de récurrence : $\forall n \in \mathbb{N}$, $a^n \equiv b^n\ [p]$.

($\Leftarrow$) Supposons : $\forall n \in \mathbb{N}$, $a^n \equiv b^n\ [p]$.
Alors, en particulier (pour $n=1$) : $a \equiv b\ [p]$.

□

Remarque
Soit E un ensemble.

- Une relation R réflexive, symétrique et transitive (c'est-à-dire vérifiant les propriétés ***1)***, ***2)*** et ***3)***) est appelée *relation d'équivalence*. Nous avons déjà à disposition plusieurs relations d'équivalence :

  × la relation d'égalité entre nombres ($=$),

  × la relation d'équivalence entre propositions ($\Leftrightarrow$),

  × la relation de parallélisme entre droites.

  × la relation de congruence entre entiers.

  Il en existe évidemment beaucoup d'autres.

- Toute relation d'équivalence permet de partitionner (de « découper ») l'ensemble sur lequel elle s'applique en plusieurs sous-ensembles. On appelle ces sous-ensembles des *classes d'équivalence*. Précisons.

  × Soient E un ensemble et R une relation d'équivalence sur E. Soit $x \in E$.

  - On appelle *classe d'équivalence de* x, et on note $\dot{x}$ l'ensemble : $\dot{x} = \{y \in E \mid xRy\}$.
  - On appelle *représentant de* $\dot{x}$ n'importe quel élément de $\dot{x}$.

× L'ensemble des classes d'équivalence de R forme une partition de E, c'est-à-dire :

1) les classes d'équivalence de R sont 2 à 2 disjointes.

2) l'union des classes d'équivalence de R est égale à E.

On peut faire l'analogie avec un puzzle. Les classes d'équivalence sont les pièces.

1) Deux pièces ne se chevauchent jamais.

2) Toutes les pièces mises côte à côte permettent de reconstituer le dessin (qui n'est rien d'autre que E).

× Tout l'intérêt des classes d'équivalence réside dans l'assertion suivante : *si une propriété est vraie pour un seul représentant d'une classe d'équivalence, elle est vraie sur toute cette classe d'équivalence*
On peut ainsi se limiter à des études sur un seul représentant par classe d'équivalence.

Remarque

- La relation de congruence modulo p possède exactement p classes d'équivalence :

$$\begin{array}{lcccl}
\dot{0} & = & \{\ldots,-2p,-p,0,p,2p,3p,\ldots\} & = & p\,\mathbb{Z} \\
\dot{1} & = & \{\ldots,1-2p,1-p,1,1+p,1+2p,1+3p,\ldots\} & = & \{1+k\,p \mid k\in\mathbb{Z}\} \\
\dot{2} & = & \{\ldots,2-2p,2-p,2,2+p,2+2p,2+3p,\ldots\} & = & \{2+k\,p \mid k\in\mathbb{Z}\} \\
\vdots & & & & \\
\dot{(p-1)} & = & \{p-1+k\,p \mid k\in\mathbb{Z}\} & &
\end{array}$$

  L'entier p est un représentant de la classe $\dot{0}$ (mais aussi 0, $-p$, $147\,p$...).
- On retrouve dans la Proposition 5 les p classes d'équivalence de la relation de divisibilité par p. Plus précisément, la proposition indique que tout entier $n\in\mathbb{Z}$ appartient à une unique classe d'équivalence pour la divisibilité par p.
  (ce que nous savons déjà puisque les classes d'équivalence forment une partition de $\mathbb{Z}$)

Exercice 6

a) Établir le critère de divisibilité par 9 suivant : pour tout $n\in\mathbb{N}$, la somme des chiffres du nombre n est divisible par 9 si et seulement si n est divisible par 9.

b) Le nombre 4783452 est-il divisible par 9 ?

Démonstration.

a) Soit $n\in\mathbb{N}$. Alors il existe $N\in N$ et $(a_0,\ldots,a_N)\in\mathbb{R}^{N+1}$ tel que : $n=\sum_{k=0}^{N} a_k\,10^k$.

On écrit ici la décomposition de n en base 10 : a_0, ..., a_N sont les chiffres constituant le nombre n (a_0 est le chiffre des unités, a_1 celui des dizaines...).

- Tout d'abord :

$$10\equiv 1\ [9]$$

$$\begin{array}{lll}
\text{donc} & \forall k\in\mathbb{N},\ 10^k\equiv 1^k\ [9] & \textit{(par compatibilité de la congruence avec l'exponentiation entière)} \\
\text{d'où} & \forall k\in\mathbb{N},\ 10^k\equiv 1\ [9] & \\
\text{puis} & \forall k\in\mathbb{N},\ a_k\,10^k\equiv a_k\ [9] & \textit{(par compatibilité de la congruence avec la multiplication)} \\
\text{ainsi} & \sum_{k=0}^{N} a_k\,10^k\equiv\sum_{k=0}^{N} a_k\ [9] & \textit{(par compatibilité de la congruence avec la somme)} \\
\text{enfin} & n\equiv\sum_{k=0}^{N} a_k\ [9] &
\end{array}$$

- On procède maintenant par double implication.

  ($\Rightarrow$) Supposons que la somme des chiffres du nombre n est divisible par 9, *i.e.* : $9 \mid \sum_{k=0}^{N} a_k$.
  Alors, on obtient :

  $$n \equiv \sum_{k=0}^{N} a_k \ [9] \quad \text{et} \quad \sum_{k=0}^{N} a_k \equiv 0 \ [9]$$

  Par transitivité de la relation de congruence, on en déduit :

  $$n \equiv 0 \ [9]$$

  D'où n est divisible par 9.

  ($\Leftarrow$) Supposons que n est divisible par 9, *i.e.* : $9 \mid n$.
  On a démontré : $n \equiv \sum_{k=0}^{N} a_k \ [9]$. Par symétrie de la relation de congruence, on en déduit : $\sum_{k=0}^{N} a_k \equiv n \ [9]$. Ainsi :

  $$\sum_{k=0}^{N} a_k \equiv n \ [9] \quad \text{et} \quad n \equiv 0 \ [9]$$

  Par transitivité de la relation de congruence, on en conclut :

  $$\sum_{k=0}^{N} a_k \equiv 0 \ [9]$$

  D'où la somme des chiffres du nombre n est divisible par 9.

b) On utilise le critère de divisibilité démontré en question précédente :

$$4 + 7 + 8 + 3 + 4 + 5 + 2 \ = \ 33$$

Or $33 = 2 \times 11$ n'est pas divisible par 9. D'où 4783452 n'est pas divisible par 9.

□

Définition (Inverse modulo p)
Soit $(a, p) \in \mathbb{Z} \times \mathbb{N}^*$.
On dit que a est *inversible modulo* p s'il existe $b \in \mathbb{Z}$ tel que : $a\,b \equiv 1 \ [p]$.

Exemple
Démontrer que 5 est inversible modulo 3.

Démonstration.
On remarque : $5 \times 2 = 10 = 3 \times 3 + 1$. Donc : $5 \times 2 \equiv 1 \ [3]$.
Ainsi, 5 est inversible modulo 3. □

On parle d'**UN** inverse de a modulo p. En effet, un entier inversible modulo p admet une infinité d'inverses par p.
Pour reprendre l'exemple ci-dessus, le nombre 5 admet pour inverse 2 mais aussi 5, 8... (tous les nombres de l'ensemble $\{3k + 2 \mid k \in \mathbb{Z}\}$)

Exercice 7
Quel est le dernier chiffre de l'écriture en base 10 de $7^{(7^7)}$?

Démonstration.

- On commence par chercher une période dans les congruences des puissances entières de 7 modulo 10 (puisqu'on cherche le dernier chiffre en base 10 d'une puissance entière de 7).
  - × Tout d'abord : $7^0 = 1$. Donc : $7^0 \equiv 1 \ [10]$.
  - × Ensuite : $7^1 = 7$. Donc : $7^1 \equiv 7 \ [10]$.
  - × Puis : $7^2 = 49$. Donc : $7^2 \equiv 9 \ [10]$.
  - × On en déduit : $7^3 = 7^2 \times 7 \equiv 9 \times 7 \ [10]$. D'où : $7^3 \equiv 63 \ [10]$. Ainsi : $7^3 \equiv 3 \ [10]$.
    (on utilise ici la compatibilité de la relation de congruence avec le produit)
  - × Alors : $7^4 = 7^3 \times 7 \equiv 3 \times 7 \ [10]$. D'où : $7^4 \equiv 21 \ [10]$. Ainsi : $7^4 \equiv 1 \ [10]$.

Remarque
On aurait aussi pu remarquer : $7^4 = 7^2 \times 7^2 \equiv 9 \times 9$ [10]. D'où : $7^4 \equiv 81$ [10]. Ainsi : $7^4 \equiv 1$ [10].

On obtient alors, par récurrence immédiate (à faire), pour tout $k \in \mathbb{N}$:

$$\begin{aligned} 7^{4k} &\equiv 1 \ [10] \\ 7^{4k+1} &\equiv 7 \ [10] \\ 7^{4k+2} &\equiv 9 \ [10] \\ 7^{4k+3} &\equiv 3 \ [10] \end{aligned}$$

Ainsi, quatre cas se présentent :

- si $7^7 \equiv 0$ [4], alors : $7^{(7^7)} \equiv 1$ [10],
- si $7^7 \equiv 1$ [4], alors : $7^{(7^7)} \equiv 7$ [10],
- si $7^7 \equiv 2$ [4], alors : $7^{(7^7)} \equiv 9$ [10],
- si $7^7 \equiv 3$ [4], alors : $7^{(7^7)} \equiv 3$ [10].

- On cherche alors savoir dans quel cas on se trouve.
  - × Tout d'abord : $7 \equiv 3$ [4].
    (en effet : $7 = 4 \times 1 + 3$*)*
  - × Ensuite : $7^2 = 7 \times 7 \equiv 3 \times 7$ [4]. D'où : $7^2 \equiv 21$ [4]. Ainsi : $7^2 \equiv 1$ [4].
    (en effet : $21 = 4 \times 5 + 1$*)*
  - × De plus : $7^4 = 7^2 \times 7^2 \equiv 1 \times 1$ [4]. D'où : $7^4 \equiv 1$ [4].
  - × Enfin : $7^7 = 7^4 \times 7^2 \times 7 \equiv 1 \times 1 \times 3$ [4]. Ainsi : $7^7 \equiv 3$ [4].

  Avec le point précédent, on obtient que le dernier chiffre de l'écriture en base 10 de $7^{(7^7)}$ est 3.

□

IV. PGCD

IV.1. Définitions

Proposition 9. (Définition PGCD)
Soit $(a, b) \in \mathbb{Z}^* \times \mathbb{Z}$.
Il existe un unique **entier naturel** d*, diviseur commun à* a *et* b*, tel que l'ensemble des diviseurs communs à* a *et à* b *est égal à l'ensemble des diviseurs de* d.
Cet entier naturel est noté $a \wedge b$ *et est appelé* pgcd de a et b *(plus grand diviseur commun à* a *et* b*).*

Démonstration.

- Unicité.
  Soit $(d_1, d_2) \in \mathbb{N}^2$ vérifiant :

$$\begin{cases} d_1 \mid a, \quad d_1 \mid b & (1) \\ \forall d' \in \mathbb{Z},\ (d' \mid a \ \texttt{ET}\ d' \mid b) \ \Leftrightarrow \ (d' \mid d_1) & (2) \end{cases}$$

$$\text{et} \quad \begin{cases} d_2 \mid a, \quad d_2 \mid b & (3) \\ \forall d' \in \mathbb{Z},\ (d' \mid a \ \texttt{ET}\ d' \mid b) \ \Leftrightarrow \ (d' \mid d_2) & (4) \end{cases}$$

  - × Avec (2) et (3), on obtient : $d_2 \mid d_1$.
  - × Avec (1) et (4), on obtient : $d_1 \mid d_2$.

  On en déduit : $|d_1| = |d_2|$. Or $(d_1, d_2) \in \mathbb{N}^2$. Ainsi : $d_1 = d_2$.
- Existence. Algorithme d'Euclide.
  On se restreint qu cas où $(a, b) \in \mathbb{N}^* \times \mathbb{N}$ (sinon on se ramène à ce cas en travaillant sur le couple $(|a|, |b|)$. Deux cas se présentent :
  - × si $b = 0$, alors, pour tout $n \in \mathbb{N}$:

$$(n \mid a \ \texttt{ET}\ n \mid b) \ \Leftrightarrow \ (n \mid a)$$

    On en déduit : $a \wedge 0 = a$.

× si $b \neq 0$.

- On effectue la division euclidienne de a par b.
  On en déduit qu'il existe $(q_1, r_1) \in \mathbb{N}^2$ tel que :

$$\begin{cases} a &= b\,q_1 + r_1 \\ 0 \leqslant r_1 < b \end{cases}$$

  On note $Div(a,b)$ l'ensemble des diviseurs communs à a et b. Démontrons : $Div(a,b) = Div(b,r_1)$. On procède par double inclusion.

  ($\subset$) Soit $n \in Div(a,b)$. Alors :

$$\begin{aligned} & n \mid a \ \texttt{ET}\ n \mid b \\ \text{donc} \quad & n \mid bq_1 + r_1 \ \texttt{ET}\ n \mid bq_1 \\ \text{d'où} \quad & n \mid r_1 \ \texttt{ET}\ n \mid b \end{aligned}$$

  Ainsi : $n \in Div(b,r_1)$.

  ($\supset$) Soit $n \in Div(b,r_1)$. Alors :

$$\begin{aligned} & n \mid b \ \texttt{ET}\ n \mid r_1 \\ \text{donc} \quad & n \mid bq_1 \ \texttt{ET}\ n \mid r_1 \\ \text{d'où} \quad & n \mid b \ \texttt{ET}\ n \mid bq_1 + r_1 \\ \text{ainsi} \quad & n \mid b \ \texttt{ET}\ n \mid a \end{aligned}$$

  On en déduit : $n \in Div(a,b)$.

- Si $r_1 \neq 0$. On effectue alors la division euclidienne de b par r_1.
  Il existe $(q_2, r_2) \in \mathbb{N}^2$ tel que :

$$\begin{cases} b &= r_1\,q_2 + r_2 \\ 0 \leqslant r_2 < r_1 \end{cases}$$

  Avec la même démonstration que dans le point précédent, on a : $Div(b,r_1) = Div(r_1,r_2)$.

- Si $r_2 \neq 0$, on peut continuer. Il existe $(q_3, r_3) \in \mathbb{N}^2$ tel que :

$$\begin{cases} r_1 &= r_2\,q_3 + r_3 \\ 0 \leqslant r_3 < r_2 \end{cases}$$

  On obtient : $Div(r_1,r_2) = Div(r_2,r_3)$.

- On peut continuer ces divisions tant que le dernier reste n'est pas nul. Mais on ne peut continuer indéfiniment car il n'existe pas de suite $(r_k)_{k\in\mathbb{N}^*}$ strictement décroissante d'entiers (Lemme 1).
  Il existe donc $k_0 \in \mathbb{N}^*$ tel que r_{k_0+1} est le premier reste nul :

$$\begin{aligned} a &= b\,q_1 + r_1 \\ b &= r_1\,q_2 + r_2 \\ r_1 &= r_2\,q_3 + r_3 \\ &\vdots \\ r_{k_0-2} &= r_{k_0-1}\,q_{k_0} + r_{k_0} \\ r_{k_0-1} &= r_{k_0}\,q_{k_0+1} + 0 \end{aligned}$$

  On en déduit :

$$\begin{aligned} Div(a,b) &= Div(b,r_1) \\ &= Div(r_1,r_2) \\ &\vdots \\ &= Div(r_{k_0-1}, r_{k_0}) \\ &= Div(r_{k_0}, 0) = Div(r_{k_0}) \end{aligned}$$

  où la dernière égalité est obtenue grâce au cas $b = 0$ démontré plus haut).

- On note alors : $a \wedge b = d = r_{k_0}$ et il est caractérisé par la propriété :

$$\forall n \in \mathbb{N}, \quad (n \mid a \ \texttt{ET}\ n \mid b) \Leftrightarrow (n \mid d)$$

□

Lemme 1.
Il n'existe pas de suite strictement décroissante d'entiers naturels.

Démonstration.
Raisonnons par l'absurde.
Supposons qu'il existe une suite $(r_k)_{k\in\mathbb{N}}$ telle que :

× (r_k) est strictement décroissante,

× $\forall k \in \mathbb{N},\ r_k \in \mathbb{N}$.

- Tout d'abord, la suite $(r_k)_{k\in\mathbb{N}}$ est :
  × décroissante,
  × minorée par 0.
  Elle converge donc vers un réel ℓ vérifiant : $\ell \geqslant 0$.
- Démontrons maintenant par récurrence : $\forall k \in \mathbb{N}$, $\mathscr{P}(k)$ où $\mathscr{P}(k)$: $r_k \leqslant r_0 - k$.
  ▸ **Initialisation** :
  $$\begin{array}{ccc} r_0 & \leqslant & r_0 \\ & & \| \\ & & r_0 - 0 \end{array}$$
  D'où $\mathscr{P}(0)$.
  ▸ **Hérédité** : soit $k \in \mathbb{N}$.
  Supposons $\mathscr{P}(k)$ et démontrons $\mathscr{P}(k+1)$ (*i.e.* $r_{k+1} \leqslant r_0 - (k+1)$).
  $$r_{k+1} < r_k \qquad \textit{(car } (r_k) \textit{ strictement décroissante)}$$
  $$\text{donc} \quad r_{k+1} \leqslant r_k - 1 \qquad \textit{(car } r_{k+1} \in \mathbb{N} \textit{ et } r_k \in \mathbb{N}\textit{)}$$
  Or, par hypothèse de récurrence : $r_k \leqslant r_0 - k$. D'où : $r_k - 1 \leqslant r_0 - k - 1$.
  Ainsi, par transitivité :
  $$r_{k+1} \leqslant r_k - 1 \leqslant r_0 - (k+1)$$
  D'où $\mathscr{P}(k+1)$.
  Par principe de récurrence : $\forall k \in \mathbb{N}$, $r_k \leqslant r_0 - k$.
- Or : $\lim\limits_{k\to+\infty} r_0 - k = -\infty$.
  Ainsi, par théorème de comparaison : $\lim\limits_{k\to+\infty} r_k = -\infty$.
  Absurde !

□

Exemples

- L'ensemble des diviseurs communs à 12 et 30 est : $Div(12,30) = \{1,2,3,6\}$.
  Ainsi : $12 \wedge 30 = 6$.
- L'ensemble des diviseurs communs à 27 et 45 est : $Div(27,45) = \{1,3,9\}$.
  Ainsi : $27 \wedge 45 = 9$.

Exercice 8
Déterminer le pgcd de 136 et 472 à l'aide de l'algorithme d'Euclide.

Démonstration.

- On effectue la division euclidienne de 472 par 136.
  $$472 = 136 \times 3 + 64$$
- On effectue la division euclidienne de 136 par 64.
  $$136 = 64 \times 2 + 8$$
- On effectue la division euclidienne de 64 par 8.
  $$64 = 8 \times 8 + 0$$
- D'après l'algorithme d'Euclide, le pgcd de 136 et 472 est le dernier reste non nul obtenu.
  Ainsi : $136 \wedge 472 = 8$.

□

Définition PPCM
Soit $(a,b) \in \mathbb{Z}^2$.
Il existe un unique $m \in \mathbb{N}$ tel que :

1) $a \mid m$ et $b \mid m$,

2) $\forall m' \in \mathbb{N}, \quad (a \mid m' \ \texttt{ET} \ b \mid m') \ \Leftrightarrow \ (m \mid m')$.

Cet entier m est appelé *ppcm de a et b* (plus petit multiple commun) et est noté : $a \vee b$.

Exemples

$$4 \vee 6 = 12 \qquad 3 \vee 7 = 21 \qquad 5 \vee 40 = 40 \qquad 7 \vee 18 = 126$$

Remarque

- Soit $(a,b,c) \in \mathbb{Z}^3$. Par définition du pgcd et du ppcm :

$$\boxed{(a \mid b \ \texttt{ET} \ a \mid c) \ \Leftrightarrow \ a \mid b \wedge c}$$

$$\boxed{(b \mid a \ \texttt{ET} \ c \mid a) \ \Leftrightarrow \ b \vee c \mid a}$$

- En arithmétique, pour démontrer une égalité, on raisonne souvent par double divisibilité (en prenant garde aux signes).

IV.2. Propriétés

Proposition 10.
Soit $(a,b) \in \mathbb{Z}^2$.

1) $\boxed{a \wedge b = b \wedge a}$

2) Soit $\lambda \in \mathbb{Z}$. $\boxed{(\lambda\, a) \wedge (\lambda\, b) = |\lambda|\,(a \wedge b)}$

Démonstration.

1) Immédiat car : $Div(a,b) = Div(b,a)$.

2) Deux cas se présentent :

- si $\lambda = 0$, alors l'égalité : $(\lambda\, a) \wedge (\lambda\, b) = |\lambda|\,(a \wedge b)$ est triviale.
- si $\lambda \neq 0$, on procède par double divisibilité.
  - × Démontrons : $\lambda\,(a \wedge b) \mid (\lambda\, a) \wedge (\lambda\, b)$.
    Par définition de $a \wedge b$: $a \wedge b \mid a$ et $a \wedge b \mid b$. Comme $\lambda \in \mathbb{Z}$:
    $$\lambda\,(a \wedge b) \mid \lambda\, a \qquad \text{et} \qquad \lambda\,(a \wedge b) \mid \lambda\, b$$
    Par définition de $(\lambda\, a) \wedge (\lambda\, b)$:
    $$\lambda\,(a \wedge b) \mid (\lambda\, a) \wedge (\lambda\, b)$$
  - × Démontrons : $(\lambda\, a) \wedge (\lambda\, b) \mid \lambda\,(a \wedge b)$.
    On remarque :
    $$\lambda \mid \lambda\, a \qquad \text{et} \qquad \lambda \mid \lambda\, b$$
    On en déduit : $\lambda \mid (\lambda\, a) \wedge (\lambda\, b)$. Il existe donc $r \in \mathbb{Z}$ tel que : $(\lambda\, a) \wedge (\lambda\, b) = r\,\lambda$.
    Or, par définition de $(\lambda\, a) \wedge (\lambda\, b)$:
    $$(\lambda\, a) \wedge (\lambda\, b) \mid \lambda\, a \qquad \text{et} \qquad (\lambda\, a) \wedge (\lambda\, b) \mid \lambda\, b$$
    D'où :
    $$\lambda\, r \mid \lambda\, a \qquad \text{et} \qquad \lambda\, r \mid \lambda\, b$$
    Comme $\lambda \neq 0$:
    $$r \mid a \qquad \text{et} \qquad r \mid b$$
    Ainsi, par définition de $a \wedge b$: $r \mid a \wedge b$.
    D'où : $\lambda\, r \mid \lambda\,(a \wedge b)$, c'est-à-dire :
    $$(\lambda\, a) \wedge (\lambda\, b) \mid \lambda\,(a \wedge b)$$

  On en déduit :
  $$|(\lambda\, a) \wedge (\lambda\, b)| \ = \ |\lambda\,(a \wedge b)| \ = \ |\lambda|\,|a \wedge b|$$
  Or un pgcd est positif. D'où : $(\lambda\, a) \wedge (\lambda\, b) \ = \ |\lambda|\,(a \wedge b)$.

□

Proposition 11.
Soit $(a,b) \in \mathbb{Z}^2$.

1) $\boxed{a \vee b = b \vee a}$

2) *Soit* $\lambda \in \mathbb{Z}$. $\boxed{(\lambda\, a) \vee (\lambda\, b) = |\lambda|\,(a \vee b)}$

Démonstration.

1) Immédiat car les multiples communs à a et b sont évidemment les multiples communs à b et a.

2) Deux cas se présentent :

- si $\lambda = 0$, alors l'égalité à démontrer est triviale.
- si $\lambda \neq 0$, on procède par double divisibilité.
  - × Démontrons : $(\lambda\, a) \vee (\lambda\, b) \mid \lambda\,(a \vee b)$.
    Par définition de $a \vee b$:

    $$a \mid a \vee b \qquad \text{et} \qquad b \mid a \vee b$$

    Donc :

    $$\lambda\, a \mid \lambda\,(a \vee b) \qquad \text{et} \qquad \lambda\, b \mid \lambda\,(a \vee b)$$

    Par définition de $(\lambda\, a) \vee (\lambda\, b)$:

    $$(\lambda\, a) \vee (\lambda\, b) \mid \lambda\,(a \vee b)$$

  - × Démontrons : $\lambda\,(a \vee b) \mid (\lambda\, a) \vee (\lambda\, b)$.
    On remarque : $\lambda \mid \lambda\, a$. D'où : $\lambda \mid (\lambda\, a) \vee (\lambda\, b)$.
    Ainsi, il existe $r \in \mathbb{Z}$ tel que : $(\lambda\, a) \vee (\lambda\, b) = r\,\lambda$.
    Par définition de $(\lambda\, a) \vee (\lambda\, b)$:

    $$\lambda\, a \mid (\lambda\, a) \vee (\lambda\, b) \qquad \text{et} \qquad \lambda\, b \mid (\lambda\, a) \vee (\lambda\, b)$$

    D'où :

    $$\lambda\, a \mid \lambda\, r \qquad \text{et} \qquad \lambda\, b \mid \lambda\, r$$

    Comme $\lambda \neq 0$:

    $$a \mid r \qquad \text{et} \qquad b \mid r$$

    Par définition de $a \vee b$, on obtient : $a \vee b \mid r$.
    D'où : $\lambda\,(a \vee b) \mid \lambda\, r$, c'est-à-dire :

    $$\lambda\,(a \vee b) \mid (\lambda\, a) \vee (\lambda\, b)$$

  On en déduit :

  $$|(\lambda\, a) \vee (\lambda\, b)| \;=\; |\lambda\,(a \vee b)| \;=\; |\lambda|\,|a \vee b|$$

  Or un ppcm est positif. D'où : $(\lambda\, a) \vee (\lambda\, b) \;=\; |\lambda|\,(a \vee b)$.

□

Proposition 12.
Soit $(a,b) \in \mathbb{Z}^2$. *Soit* $\lambda \in \mathbb{Z}$.

$$\boxed{a \wedge b \;=\; (a + \lambda\, b) \wedge b}$$

Démonstration.
On procède par double divisibilité.

- Démontrons : $a \wedge b \mid (a + \lambda\, b) \wedge b$.
  Par définition de $a \wedge b$, on a :

	$a \wedge b \mid a$	ET	$a \wedge b \mid b$	
donc	$a \wedge b \mid a$	ET	$a \wedge b \mid \lambda\, b$	*(car $\lambda \in \mathbb{Z}$)*
d'où	$a \wedge b \mid (a + \lambda\, b)$	ET	$a \wedge b \mid b$	
ainsi	$a \wedge b \mid (a + \lambda\, b) \wedge b$			*(par définition de $(a + \lambda\, b) \wedge b$)*

- Démontrons : $(a+\lambda b)\wedge b \mid a\wedge b$.
  On note : $d=(a+\lambda b)\wedge b$. Par définition de $(a+\lambda b)\wedge b$, on a :

$$\begin{array}{lrcll} & d \mid (a+\lambda b) & \texttt{ET} & d \mid b & \\ \text{donc} & d \mid (a+\lambda b) & \texttt{ET} & d \mid \lambda b & \textit{(car } \lambda \in \mathbb{Z}\textit{)} \\ \text{d'où} & d \mid a & \texttt{ET} & d \mid b & \\ \text{ainsi} & & \mid a\wedge b & & \textit{(par définition de } a\wedge b\textit{)} \end{array}$$

Finalement : $|a\wedge b| = |(a+\lambda b)\wedge b|$. Or un pgcd est positif. Ainsi :

$$a\wedge b \;=\; (a+\lambda b)\wedge b$$

□

Exercice 9
Soit $(a,b)\in\mathbb{Z}^2$.
Calculer $(3a+7b)\wedge(2a+5b)$ en fontion de $a\wedge b$.

Démonstration.
On calcule :

$$\begin{aligned} (3a+7b)\wedge(2a+5b) &= \big((3a+7b)-(2a+5b)\big)\wedge(2a+5b) \\ &= (a+2b)\wedge(2a+5b) \\ &= (a+2b)\wedge\big((2\cancel{a}+5b)-2(\cancel{a}+2b)\big) \\ &= (a+2b)\wedge b \\ &= \big((a+2\cancel{b})-2\cancel{b}\big)\wedge b \\ &= a\wedge b \end{aligned}$$

□

IV.3. Algorithme d'Euclide en Python

On cherche dans cette partie à coder en **Python** l'algorithme d'Euclide, présenté dans le définition du pgcd.

Remarque

- Nous avons déjà défini une fonction Descente_Fermat dans le chapitre 1 (Arithmérique - Divisibilité dans $\mathbb{Z}$) permettant d'obtenir le quotient et le reste de la division euclidienne de deux entiers. Cette fonction peut tout à fait être utilisée ici.
- Cependant, nous privilégierons ici la commande prédéfinie en **Python** pour obtenir le reste de la division euclidienne de n par p (où $(n,p)\in\mathbb{Z}^2$). Il s'agit de la commande `n % p`. Par exemple le script :

```
11 % 4
```

renvoie le reste de la division euclidienne de 11 par 4 :

```
3
```

(rappelons que le quotient n'intervient pas dans l'algorithme d'Euclide)

On propose la fonction suivante qui permet d'obtenir le pgcd de deux entiers naturels `a` et `b`.

```
def Algorithme_Euclide(a, b) :
    d = max(a, b)
    r = min(a, b)
    while d % r != 0 :
        aux = d
        d = r
        r = aux % d
    return r
```

Détaillons les éléments de ce script.

- **Début de la fonction**
  On commence par préciser la structure de la fonction :
  × cette fonction se nomme `Algorithme_Euclide`,
  × elle prend en entrée les paramètres `a` et `b`,
  × elle admet pour variable de sortie `r`.

```
1  def Algorithme_Euclide(a, b) :
```

```
8          return r
```

  On initialise ensuite les variables `d` et `r`. Pour chaque division euclidienne à venir :
  - la variable `d` va contenir le dividende,
  - la variable `r` va contenir le diviseur.
  On choisit donc d'initialiser :
  - `d` au plus grand entier entre `a` et `b`,
  - `r` au plus petit entier entre `a` et `b`.

```
2          d = max(a, b)
3          r = min(a, b)
```

- **Structure itérative**
  Les lignes 4 à 7 consistent à déterminer le pgcd de `a` et `b`. Pour cela, on doit déterminer la suite $(r_k)_{k\in\mathbb{N}}$ des restes des divisions euclidiennes de `d` par `r`, jusqu'à trouver un reste nul. Autrement dit, on doit calculer les restes des divisions euclidiennes de `d` par `r` tant qu'on n'obtient un reste non nul. Pour cela, on utilise une structure itérative (boucle while).

```
4          while d % r != 0 :
```

  À chaque tour de boucle, on doit mettre à jour les variables `d` et `r`. Pour ce faire, on introduit une variable auxiliaire `aux`. Détaillons le principe de la mise à jour dans cette boucle while (on se place dans le cas $a \geqslant b$).
  × avant le 1er tour de boucle :

$$\texttt{d} \text{ contient } a \quad \text{et} \quad \texttt{r} \text{ contient } b$$

  lors du 1er tour de boucle :

`aux = d` $\left(\begin{array}{l}\texttt{aux} \text{ contient alors } a,\\ \text{valeur contenue dans } \texttt{d}\end{array}\right)$

`d = r` $\left(\begin{array}{l}\texttt{d} \text{ contient alors } b,\\ \text{dernière valeur en date de } \texttt{r}\end{array}\right)$

`r = aux % d` $\left(\begin{array}{l}\texttt{r} \text{ contient alors le reste de la}\\ \text{division euclidienne de } a \text{ par } b,\\ \text{dernières valeurs en date de } \texttt{aux} \text{ et}\\ \texttt{d} \text{ respectivement}\end{array}\right)$

  Remarque
  Si on avait réalisé en ligne 7 l'affectation `r = d % r` alors, on aurait affecté à la variable `r` le reste de la division euclidienne de b (dernière valeur en date de `d`) par b (dernière valeur en date de `r`).
  × avant le 2ème tour de boucle, d'après ce qui précède et en notant r_1 le reste de la division euclidienne de a par b :

$$\texttt{d} \text{ contient } b \quad \text{et} \quad \texttt{r} \text{ contient } r_1$$

  lors du 2ème tour de boucle :

`aux = d` $\left(\begin{array}{l}\texttt{aux} \text{ contient alors } b,\\ \text{valeur actuelle de } \texttt{d}\end{array}\right)$

`d = r` $\left(\begin{array}{l}\texttt{d} \text{ contient alors } r_1,\\ \text{dernière valeur en date de } \texttt{r}\end{array}\right)$

`r = aux % d` $\left(\begin{array}{l}\texttt{r} \text{ contient alors le reste de la}\\ \text{division euclidienne de } b \text{ par } r_1,\\ \text{dernières valeurs en date de } \texttt{aux} \text{ et}\\ \texttt{d} \text{ respectivement}\end{array}\right)$

× ...

× avant le $k_0^{\text{ème}}$ tour de boucle, où r_{k_0} est le dernier reste non nul dans l'algorithme d'Euclide (on rappelle qu'on a démontré son existence dans la démonstration) :

$$\texttt{d} \text{ contient } r_{k_0-2} \quad \text{et} \quad \texttt{r} \text{ contient } r_{k_0-1}$$

lors du $k_0^{\text{ème}}$ tour de boucle :

`aux = d`	`aux` contient alors r_{k_0-2}, valeur actuelle de `d`
`d = r`	`d` contient alors r_{k_0-1}, dernière valeur en date de `r`
`r = (aux % d)`	`r` contient alors le reste de la division euclidienne de r_{k_0-2} par r_{k_0-1}, dernières valeurs en date de `aux` et `d` respectivement

À l'issue de ce $k_0^{\text{ème}}$ tour de boucle, le reste de la division euclidienne de r_{k_0-1} (valeur contenue dans `d`) par r_{k_0} (valeur contenue dans `r`) est : $r_{k_0+1} = 0$. La boucle s'arrête donc et renvoie la dernière valeur contenue dans `r`, c'est-à-dire : $r_{k_0} = a \wedge b$.

Remarque

On peut également proposer une version récursive de cet algorithme.

```
1  def Euclide_recursif(a, b):
2      d = max(a, b)
3      r = min(a,b)
4      if d % r == 0 :
5          return r
6      else :
7          return Euclide_recursif(r, d % r)
```

V. Nombres premiers entre eux

Définition (Nombres premiers entre eux)

Soit $(a, b) \in \mathbb{Z}^2$.

On dit que les entiers a et b sont premiers entre eux si : $\boxed{a \wedge b = 1}$.

Il ne faut pas confondre « $a \wedge b = 1$ » et « a ne divise pas b ».

Remarque

Soit $(a, b) \in \mathbb{Z}^2$.

Pour montrer que a et b sont premiers entre eux, il suffit de montrer : $a \wedge b \mid 1$.

Exercice 10

Soit $n \in \mathbb{N}$. Démontrer : $(2^n + 3^n) \wedge (2^{n+1} + 3^{n+1}) = 1$.

Démonstration.

On pose : $d = (2^n + 3^n) \wedge (2^{n+1} + 3^{n+1})$. Par définition de d, on a :

$$d \mid (2^n + 3^n) \quad (1) \qquad d \mid (2^{n+1} + 3^{n+1}) \quad (2)$$

- On déduit de (1) : $d \mid 3\,(2^n + 3^n)$. D'où : $d \mid (3 \times 2^n + 3^{n+1})$.
  En utilisant (2), on obtient alors :
  $$d \mid \left(3 \times 2^n + \cancel{3^{n+1}} - (2^{n+1} + \cancel{3^{n+1}})\right)$$
  D'où : $d \mid (3 \times 2^n - 2 \times 2^n)$. Ainsi : $d \mid 2^n$.
- De même, en utilisant (1) : $d \mid 2\,(2^n + 3^n)$. D'où : $d \mid (2^{n+1} + 2 \times 3^n)$.
  En utilisant (2), on obtient alors :
  $$d \mid \left(\cancel{2^{n+1}} + 2 \times 3^n - (\cancel{2^{n+1}} + 3^{n+1})\right)$$
  D'où : $d \mid (2 \times 3^n - 3 \times 3^n)$. Ainsi : $d \mid -3^n$. On en déduit : $d \mid 3^n$.

Finalement : $d \mid 2^n \wedge 3^n$.

Or : $2 \wedge 3 = 1$. Donc : $2^n \wedge 3^n = 1$. Ainsi : $d \mid 1$. Finalement : $d = 1$. □

VI. Nombres premiers

VI.1. Définition et propriétés

Définition (Nombre premier)
Soit $p \in \mathbb{N}$.
On dit que p est un nombre **premier** si :

- $p \geqslant 2$,
- $\forall q \in \mathbb{N}^*, \quad (q \mid p \quad \Leftrightarrow \quad q = 1 \ \texttt{OU} \ q = p)$
  (les seuls diviseurs **positifs** *de p sont 1 et p)*

Un nombre qui n'est pas premier est dit **composé**.

Remarque
Le nombre 2 est le seul nombre premier pair.

Proposition 13.

1) *Soit $a \in \mathbb{N}^*$. Soit p un nombre premier. Alors :*
- × *soit : $p \mid a$*
- × *soit : $a \wedge p = 1$*

2) *Deux entiers premiers distincts sont premiers entre eux.*

3) *Soit $a \in \mathbb{N}^*$. Soient p et q deux nombres premiers distincts.*

$$\left.\begin{array}{l} p \mid a \\ q \mid a \end{array}\right\} \quad \Rightarrow \quad pq \mid a$$

4) *Soit $a \in \mathbb{N}^*$. Soient p_1, …, p_r r nombres premiers distincts.*

$$\forall i \in [\![1, r]\!], \ p_i \mid a \qquad \Rightarrow \qquad \prod_{i=1}^{r} p_i \mid a$$

Démonstration.

1) Soit $a \in \mathbb{N}^*$. Soit p un nombre premier.
Comme p est premier : $Div(p) = \{1, p\}$. Or : $Div(a, p) \subset Div(p)$. On en déduit :
- × soit $Div(a, p) = \{1, p\}$, et donc : $p \mid a$.
- × soit $Div(a, p) = \{1\}$ et donc : $p \wedge a = 1$.

2) Évident avec le point précédent.

3) Soit $a \in \mathbb{N}^*$. Soient p et q deux nombres premiers distincts.
Supposons : $p \mid a$ et $q \mid a$.
Comme p et q sont premiers et distincts, d'après ***2)*** : $p \wedge q = 1$. Ainsi :

$$p \mid a, \qquad q \mid a \qquad \text{et} \qquad p \wedge q = 1$$

Par corollaire du théorème de Gauss : $pq \mid a$.

4) Soit $a \in \mathbb{N}^*$. Démontrons par récurrence : $\forall r \in \mathbb{N}^*$, $\mathscr{P}(r)$
où $\mathscr{P}(r)$: pour tout $(p_1, \ldots, p_r) \in [\![2, +\infty[\![^r$ premiers distincts :

$$\forall i \in [\![1, r]\!], \ p_i \mid a \qquad \Rightarrow \qquad \prod_{i=1}^{r} p_i \mid a$$

- ▸ **Initialisation**
  Soit $p_1 \in [\![2, +\infty[\![$ premier. Supposons : $p_1 \mid a$.
  Alors : $\prod_{i=1}^{1} p_i = p_1$. Donc : $p_1 \mid a$.
  D'où $\mathscr{P}(1)$.
- ▸ **Hérédité** : soit $r \in \mathbb{N}^*$.
  Supposons $\mathscr{P}(r)$ et démontrons $\mathscr{P}(r+1)$ (*i.e.* pour tout $(p_1, \ldots, p_{r+1}) \in [\![2, +\infty[\![^{r+1}$ premiers distincts : $\forall i \in [\![1, r+1]\!], \ p_i \mid a \quad \Rightarrow \quad \prod_{i=1}^{r+1} p_i \mid a$)
  Soit $(p_1, \ldots, p_{r+1}) \in [\![2, +\infty[\![^{r+1}$ premiers distincts. Supposons : $\forall i \in [\![1, r+1]\!]$, $p_i \mid a$.
  - × Par hypothèse de récurrence : $\prod_{i=1}^{r} p_i \mid a$.

× Ainsi :

$$\prod_{i=1}^{r} p_i \mid a, \quad p_{r+1} \mid a \quad \text{et} \quad \left(\prod_{i=1}^{r} p_i\right) \wedge p_{r+1} = 1$$

Par corollaire du théorème de Gauss : $\prod_{i=1}^{r+1} p_i \mid a$.

D'où : $\mathscr{P}(r+1)$.

□

Proposition 14.
Soit $a \in \mathbb{N}^*$. Soit p un nombre premier.

1) $\boxed{p \mid a^2 \quad \Rightarrow \quad p \mid a}$

2) Pour tout $n \in \mathbb{N}^*$:

$$\boxed{p \mid a^n \quad \Rightarrow \quad p \mid a}$$

Démonstration.

1) Supposons : $p \mid a^2$.
Raisonnons par l'absurde. Supposons : $p \nmid a$.
Comme p est premier, on en déduit : $p \wedge a = 1$. On obtient donc :

$$p \mid a \times a \qquad \text{et} \qquad p \wedge a = 1$$

Par théorème de Gauss : $p \mid a$.
Absurde !

2) Démontrons par récurrence : $\forall n \in \mathbb{N}^*$, $\mathscr{P}(n)$ où $\mathscr{P}(n) : p \mid a^n \Rightarrow p \mid a$.

▸ **Initialisation**
Supposons : $p \mid a^1$. Alors : $p \mid a$.
D'où $\mathscr{P}(1)$.

▸ **Hérédité** : soit $n \in \mathbb{N}^*$.
Supposons $\mathscr{P}(n)$ et démontrons $\mathscr{P}(n+1)$ (*i.e.* $p \mid a^{n+1} \Rightarrow p \mid a$)
Supposons : $p \mid a^{n+1}$.
Raisonnons par l'absurde.
Supposons : $p \nmid a$. Comme p est premier, alors : $p \wedge a = 1$. Ainsi :

$$p \mid a^n \times a \qquad \text{et} \qquad p \wedge a = 1$$

Par théorème de Gauss : $p \mid a^n$.
Par hypothèse de récurrence ; on obtient : $p \mid a$.
Absurde !
On en déduit : $p \mid a$.
D'où $\mathscr{P}(n+1)$.

□

Proposition 15.
Tout entier naturel au moins égal à 2 admet au moins un diviseur premier.

Démonstration.
Démontrons par récurrence (forte) : $\forall n \in [\![2, +\infty[\![$, $\mathscr{P}(n)$ où $\mathscr{P}(n)$: n admet au moins un diviseur premier.

▸ **Initialisation**
Le nombre 2 admet 2 comme diviseur premier.
D'où $\mathscr{P}(2)$.

▸ **Hérédité** : soit $n \in [\![2, +\infty[\![$.
Supposons : $\forall d \in [\![2, n]\!]$, $\mathscr{P}(d)$. Démontrons $\mathscr{P}(n+1)$ (*i.e.* $n+1$ admet au moins un diviseur premier).
Deux cas se présentent :

× si $n+1$ est premier, alors il admet un diviseur premier : lui-même.

× si $n+1$ n'est pas premier, alors il admet des diviseurs positifs autres que 1 et $n+1$.
Notons d l'un de ces diviseurs positifs. Alors il existe $k \in \mathbb{N}$ tel que : $n+1 = k\,d$. De plus :

$$\begin{array}{rccccl} & 1 & < & d & < & n+1 \\ \text{donc} & 2 & \leqslant & d & \leqslant & n \qquad \textit{(car } d \in \mathbb{N}\textit{)} \end{array}$$

Par hypothèse de récurrence, d admet un diviseur premier. Notons le δ.
Alors il existe $k' \in \mathbb{N}$ tel que : $d = k'\,\delta$. D'où :

$$n+1 \;=\; k\,d \;=\; k\,k'\,\delta$$

Ainsi : $\delta \mid n+1$. Comme δ est premier, on en déduit que $n+1$ admet bien un diviseur premier.
D'où $\mathscr{P}(n+1)$.

□

Remarque
On peut utiliser cette propriété pour démontrer que deux entiers a et b sont premiers entre eux en raisonnant par l'absurde.

1) On suppose : $a \wedge b \neq 1$.
Alors il existe $p \in [\![2, +\infty[\![$ premier tel que : $p \mid a \wedge b$.

2) On démontre : $p \mid 1$. Absurde !

Exercice 11
Soit $(a, b) \in \mathbb{Z}^2$ tel que :

$$a \wedge b = 1, \qquad a \text{ impair} \qquad \text{et} \qquad b \text{ impair}$$

Démontrer : $(a^2+b^2) \wedge ab = 1$.

Démonstration.
Raisonnons par l'absurde.
Supposons : $d = (a^2+b^2) \wedge ab \neq 1$.
Alors il existe $p \in [\![2, +\infty[\![$ premier tel que : $p \mid d$.

- Alors, par définition du PGCD :

$$p \mid (a^2+b^2) \qquad \text{et} \qquad p \mid ab$$

On en déduit :

$$p \mid \underset{\substack{\| \\ (a+b)^2}}{(a^2+b^2+2\,ab)} \qquad \text{et} \qquad p \mid \underset{\substack{\| \\ (a-b)^2}}{(a^2+b^2-2\,ab)}$$

Comme p est premier, on en conclut :

$$p \mid (a+b) \qquad \text{et} \qquad p \mid (a-b)$$

Ainsi : $p \mid 2a$ et $p \mid 2b$.

- Par ailleurs, comme a est impair et b est impair, on en déduit que ab est impair.
Or : $p \mid ab$. D'où : $p \neq 2$. Ainsi :
  - × $p \mid 2a$ et $p \wedge 2 = 1$ (2 est le seul nombre premier pair). Par théorème de Gauss : $p \mid a$.
  - × $p \mid 2b$ et $p \wedge 2 = 1$. Par théorème de Gauss : $p \mid b$.

  On en déduit : $p \mid a \wedge b$. C'est-à-dire : $p \mid 1$.

Absurde ! (car $p \geqslant 3$)
On en conclut : $(a^2+b^2) \wedge ab = 1$. □

Proposition 16.
L'ensemble des nombres premiers est infini.

Démonstration.
Raisonnons par l'absurde.
Supposons que l'ensemble $\mathcal{P}$ des nombres premiers est fini.
Alors il existe $N \in \mathbb{N}^*$ et $(p_1, \ldots, p_N) \in \mathbb{N}^N$ tel que : $\mathcal{P} = \{p_1, \ldots, p_N\}$.

- On considère l'entier :

$$n \;=\; p_1\,p_2 \cdots p_N + 1$$

Comme $n \in [\![2, +\infty[\![$, d'après la proposition précédente, cet entier n admet au moins un diviseur premier.
Or l'ensemble des nombres premiers est $\mathcal{P} = \{p_1, \ldots, p_N\}$. Il existe donc $k \in [\![1, N]\!]$ tel que : $p_k \mid n$.

- On obtient alors :

$$p_k \mid n \qquad \text{et} \qquad p_k \mid p_1\,p_2 \cdots p_N$$

On en déduit :

$$\begin{array}{ccc} p_k & | & (n - p_1\, p_2 \cdots p_N) \\ & & \shortparallel \\ & & 1 \end{array}$$

Absurde ! (car $p_k \geqslant 2$)

□

VI.2. Comment savoir si un nombre est premier ?

VI.2.a) Condition suffisante de primalité

Proposition 17.
Soit $n \in [\![2, +\infty[\![$.
Si n n'est pas premier, alors il admet au moins un diviseur d tel que :

$$\boxed{2 \leqslant d^2 \leqslant n}$$

Démonstration.
Soit $n \in [\![2, +\infty[\![$.
Supposons que n n'est pas premier.
Alors il admet un diviseur autre que 1 et n. Il existe donc $(d_1, d_2) \in \mathbb{N}^2$ tel que :

$$n = d_1 \times d_2 \qquad \text{et} \qquad 2 \leqslant d_1 \leqslant d_2$$

Comme $d_1 > 0$, on obtient :

$$\begin{array}{ccccc} 2\, d_1 & \leqslant & d_1^2 & \leqslant & d_1\, d_2 \\ & & & & \shortparallel \\ & & & & n \end{array}$$

De plus, comme $d_1 > 1$, alors : $d_1^2 \geqslant 2\, d_1 \geqslant 2$. Ainsi, on a bien :

$$2 \leqslant d_1^2 \leqslant n$$

□

Remarque

- Soit $n \in [\![2, +\infty[\![$. Le théorème précédent implique en particulier que si n n'est pas premier, alors il admet au moins un diviseur **premier** p tel que : $p^2 \leqslant n$, *i.e.* $p \leqslant \sqrt{n}$.
- En pratique, c'est plutôt la contraposée de cette implication qui est utilisée : « si l'entier n n'admet aucun diviseur premier p tel que $p \leqslant \sqrt{n}$, alors n est premier ».

Exercice 12
Le nombre 163 est-il premier ?

Démonstration.
On teste la divisibilité de 163 par tous les nombres premiers p tels que : $p^2 \leqslant 163$.

- Comme $2^2 = 4 \leqslant 163$, on teste la divisibilité par 2.
  On a : $163 = 81 \times 2 + 1$ et $0 < 1 < 2$. L'entier 163 n'est donc pas divisible par 2.
- Comme $3^2 = 9 \leqslant 163$, on teste la divisibilité par 3.
  On a : $163 = 54 \times 3 + 1$ et $0 < 1 < 3$. L'entier 163 n'est donc pas divisible par 3.
- Comme $5^2 = 25 \leqslant 163$, on teste la divisibilité par 5.
  On a : $163 = 32 \times 5 + 3$ et $0 < 3 < 5$. L'entier 163 n'est donc pas divisible par 5.
- Comme $7^2 = 49 \leqslant 163$, on teste la divisibilité par 7.
  On a : $163 = 23 \times 7 + 2$ et $0 < 2 < 7$. L'entier 163 n'est donc pas divisible par 7.
- Comme $11^2 = 121 \leqslant 163$, on teste la divisibilité par 11.
  On a : $163 = 14 \times 11 + 9$ et $0 < 9 < 11$. L'entier 163 n'est donc pas divisible par 11.
- Comme $13^2 = 169 > 163$, on ne teste pas la divisibilité par 13.

Le nombre 163 est donc un nombre premier. □

VI.2.b) Crible d'Ératostène

L'algorithme suivant, dû à Ératostène de Cyrène (176-194 av. J.-C.), permet de déterminer les nombres premiers inférieurs à un nombre donné n.

1) On commence par représenter dans un tableau les entiers naturels successifs compris entre 2 et n.

2) Le nombre 2 est premier. On barre alors tous les multiples de 2 autre que 2.

3) Le nombre non barré suivant est 3, qui est donc premier. On barre alors tous les multiples de 3 autres que 3.

4) On itère le procédé jusqu'à ce qu'il ne reste plus de nombres composés.

Exercice 13
À l'aide du crible d'Ératostène, déterminer le nombre de nombres premiers inférieurs ou égaux à 127.
Notons que, comme :

$$11^2 \leqslant 127 \qquad \text{et} \qquad 12^2 > 127$$

après avoir rayé les multiples de 11, on est sûr d'avoir barré tous les nombres composés inférieurs à 127.

2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19
~~20~~	~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~
29	~~30~~	31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37
~~38~~	~~39~~	~~40~~	41	~~42~~	43	~~44~~	~~45~~	~~46~~
47	~~48~~	~~49~~	~~50~~	~~51~~	~~52~~	53	~~54~~	~~55~~
~~56~~	~~57~~	~~58~~	59	~~60~~	61	~~62~~	~~63~~	~~64~~
~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~	71	~~72~~	73
~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~	~~81~~	~~82~~
83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~	~~91~~
~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~
101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~	109
~~110~~	~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~
~~119~~	~~120~~	~~121~~	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	127

Codons maintenant en **Python**, à l'aide du crible d'Eratostène, une fonction permettant d'obtenir l'ensemble des nombres premiers inférieurs ou égaux à un entier `n` (où $n \in [\![2, +\infty[\![$).

```
1  def Eratostene(n) :
2      L = [i for i in range(2, n+1)]
3      i = 0
4      d = L[i]
5      p = len(L)
6      while d**2 <= n :
7          for k in L[i+1:p] :
8              if k % d == 0 :
9                  L.remove(k)
10         i = i + 1
11         d = L[i]
12         p = len(L)
13     return L
```

Détaillons les éléments de ce script.

- **Début de la fonction**
  On commence par préciser la structure de la fonction :
  - × cette fonction se nomme `Eratostene`,
  - × elle prend en entrée le paramètre `n`,
  - × elle admet pour variable de sortie la variable `L`.

```
1  def Eratostene(n) :
```

```
13     return L
```

On initialise ensuite différentes variables :

- × la liste `L` qui contient tous les entiers de 2 à `n`. À l'issue de ce script, on souhaite que cette liste contienne seulement les nombres premiers inférieurs à `n`.

```
2      L =      L = [i for i in range(2, n+1)]
```

- × l'entier `i` qui prend la valeur 0. Cette variable désigne la coordonnée, dans la liste `L`, du nombre premier dont on souhaite supprimer les multiples.

```
3  i = 0
```

- × l'entier `d` qui prend la valeur 2. Cette variable désigne le nombre premier dont on souhaite supprimer les multiples.

```
4  d = L[i]
```

- × l'entier `p` qui est la longueur de la liste `L`.

```
5      p = len(L)
```

- **Structure itérative**
  Les lignes 6 à 12 consistent à supprimer les nombres composés de la liste `L` afin de n'en conserver que les nombres premiers. On considère donc chaque nombre `d` de la liste `L` pour en supprimer les multiples. D'après la condition suffisante de primalité d'un nombre entier, il suffit de considérer les entiers `d` tels que $\texttt{d}^2 \leqslant n$.

```
6      while d**2 <= n :
```

À chaque tour de boucle, on doit donc :

1) supprimer de la liste `L` tous les multiples de `d`, qui sont donc strictement supérieurs à `d = L[i]`. Pour cela on met en place une nouvelle structure itérative (boucle for).

```
7           for k in L[i+1:p] :
8               if k % d == 0 :
9                   L.remove(k)
```

2) mettre à jour `i` et `d` pour que la variable `d` contienne le nombre premier suivant dans la liste `L`.

```
10          i = i + 1
11          d = L[i]
```

On met enfin à jour la variable `p` pour qu'elle contienne la nouvelle longueur de la liste `L`.

```
12          p = len(L)
```

VII. Décomposition d'un entier en produit de facteurs premiers

VII.1. Théorème

Théorème 2. (Théorème fondamental de l'arithmétique)
Tout entier naturel au moins égal à 2 se décompose, de façon unique, en un produit de facteurs premiers.
En d'autres termes, pour tout $n \in [\![2, +\infty[\![$, il existe des entiers premiers p_1, …, p_r et des entiers naturels α_1, …, α_r non nuls tels que :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

Cette écriture est unique à l'ordre près des facteurs.
(notons que les p_i sont deux à deux distincts)

Démonstration.

- Existence. Démontrons par récurrence (forte) : $\forall n \in [\![2, +\infty[\![$, $\mathscr{P}(n)$ où $\mathscr{P}(n)$: n peut s'écrire comme un produit de nombres premiers.
  - **Initialisation**
    L'entier 2 s'écrit bien comme un produit de nombres premiers puisqu'il est premier.
    D'où $\mathscr{P}(2)$.
  - **Hérédité** : soit $n \in [\![2, +\infty[\![$.
    Supposons : $\forall k \in [\![2, n-1]\!]$, $\mathscr{P}(k)$. Démontrons $\mathscr{P}(n)$ (*i.e.* n peut s'écrire comme un produit de nombres premiers).
    L'entier n admet au moins un diviseur premier p. Deux cas se présentent alors :
    - si $p = n$, alors n est bien un produit de facteurs premiers.
    - si $p < n$, alors, il existe $q \in \mathbb{N}^*$ tel que : $n = p \times q$ et $1 < q < n$.
      Comme q est un entier, on en déduit : $2 \leqslant q \leqslant n-1$. Ainsi, par hypothèse de récurrence, q s'écrit comme produit de nombres premiers.
      Donc $n = p \times q$ aussi.

    D'où $\mathscr{P}(n)$.

- Unicité.
Soit $(r,s) \in \left(\mathbb{N}^*\right)^2$, soit $(p_1,\dots,p_r,p'_1,\dots,p'_s) \in \left([\![2,+\infty[\![\right)^{r+s}$ des entiers premiers et
soit $(\alpha_1,\dots,\alpha_r,\alpha'_1,\dots,\alpha'_s) \in \left(\mathbb{N}^*\right)^{r+s}$ tels que :

$$n = \prod_{i=1}^{r} p_i^{\alpha_i} \qquad \text{et} \qquad n = \prod_{i=1}^{s} (p'_i)^{\alpha'_i}$$

- Alors : $p'_1 \mid n$.
Raisonnons par l'absurde. Supposons : $p'_1 \notin \{p_1,\dots,p_r\}$. Alors, comme p'_1 est premier :

$$p'_1 \wedge p_1 = 1, \quad p'_1 \wedge p_2 = 1, \quad \dots, \quad p'_1 \wedge p_r = 1$$

Toujours parce que p'_1 est premier :

$$p'_1 \wedge p_1^{\alpha_1} = 1, \quad p'_1 \wedge p_2^{\alpha_2} = 1, \quad \dots, \quad p'_1 \wedge p_r^{\alpha_r} = 1$$

Et enfin :

$$p'_1 \wedge \left(\prod_{i=1}^{r} p_i^{\alpha_i}\right) = 1$$

Ainsi : $p'_1 \wedge n = 1$.
Absurde ! On en déduit : $p'_1 \in \{p_1,\dots,p_r\}$.
- De même, on conclut : $\forall i \in [\![1,s]\!]$, $p'_i \in \{p_1,\dots,p_r\}$. Ainsi :

$$\{p'_1,\dots,p'_s\} \subset \{p_1,\dots,p_r\}$$

- Toujours de même, en inversant le rôle des p_i et p'_i :

$$\{p_1,\dots,p_r\} \subset \{p'_1,\dots,p'_s\}$$

On en déduit :

$$\{p_1,\dots,p_r\} = \{p'_1,\dots,p'_s\}$$

Et donc :
× $r = s$
× à renumérotation près : $\forall i \in [\![1,r]\!]$, $p_i = p'_i$.
- On obtient :

$$\prod_{i=1}^{r} p_i^{\alpha_i} = n = \prod_{i=1}^{r} p_i^{\alpha'_i}$$

Raisonnons par l'absurde. Supposons : $\alpha_1 \neq \alpha'_1$. Deux cas se présentent :
× si $\alpha_1 < \alpha'_1$, alors :

$$\cancel{p_1^{\alpha_1}} \left(\prod_{i=2}^{r} p_i^{\alpha_i}\right) = \cancel{p_1^{\alpha_1}}\, p_1^{\alpha'_1-\alpha_1} \left(\prod_{i=2}^{r} p_i^{\alpha'_i}\right)$$

D'où :

$$\left(\prod_{i=2}^{r} p_i^{\alpha_i}\right) = p_1^{\alpha'_1-\alpha_1} \left(\prod_{i=2}^{r} p_i^{\alpha'_i}\right)$$

Or :

$$p_1 \nmid \left(\prod_{i=2}^{r} p_i^{\alpha_i}\right) \qquad \text{et} \qquad p_1 \mid p_1^{\alpha'_1-\alpha_1} \left(\prod_{i=2}^{r} p_i^{\alpha'_i}\right) \qquad (\textit{car } \alpha'_1-\alpha_1 > 0)$$

Absurde !
× si $\alpha_1 > \alpha'_1$, alors :

$$\cancel{p_1^{\alpha'_1}} \left(\prod_{i=2}^{r} p_i^{\alpha'_i}\right) = \cancel{p_1^{\alpha'_1}}\, p_1^{\alpha_1-\alpha'_1} \left(\prod_{i=2}^{r} p_i^{\alpha_i}\right)$$

D'où :

$$\left(\prod_{i=2}^{r} p_i^{\alpha'_i}\right) = p_1^{\alpha_1-\alpha'_1} \left(\prod_{i=2}^{r} p_i^{\alpha_i}\right)$$

Or :

$$p_1 \nmid \left(\prod_{i=2}^{r} p_i^{\alpha'_i}\right) \qquad \text{et} \qquad p_1 \mid p_1^{\alpha_1-\alpha'_1} \left(\prod_{i=2}^{r} p_i^{\alpha_i}\right) \qquad (\textit{car } \alpha_1-\alpha'_1 > 0)$$

Absurde !
On en déduit : $\alpha_1 = \alpha'_1$.
- De même : $\forall i \in [\![2,r]\!]$, $\alpha_i = \alpha'_i$.

On a donc bien obtenu l'unicité à l'ordre des facteurs près. □

Exemples

a) $56 = 2^3 \times 7^1$

b) $225 = 3^2 \times 5^2$

c) $117 = 3^2 \times 13$

d) $6120 = 2^3 \times 3^2 \times 5^1 \times 17^1$

Remarquons que si les p_i doivent être distincts dans une décomposition en facteurs premiers, ce n'est pas le cas des α_i.

Dans une décomposition en facteurs premiers, les α_i ne sont pas nuls. Ainsi $56 = 2^3 \times 7^1 \times 11^0$ n'est pas une décomposition en facteurs premiers (on comprend bien que l'unicité de la décomposition serait alors impossible à obtenir).

VII.2. Application au calcul de PGCD et PPCM

Proposition 18.
Soit $n \in [\![2, +\infty[\![$. Si la décomposition en facteurs premiers de n est :

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

(les p_i sont des entiers premiers distincts et $\alpha_i \in \mathbb{N}^*$)
alors un entier naturel m divise n si et seulement si la décomposition en facteurs premiers de m est :

$$m = p_1^{\beta_1} \cdots p_r^{\beta_r} \qquad \text{avec } 0 \leqslant \beta_i \leqslant \alpha_i$$

Démonstration.
On raisonne par double implication.

($\Leftarrow$) Supposons que la décomposition en facteurs premiers d'un entier m est :

$$m = p_1^{\beta_1} \cdots p_r^{\beta_r} \qquad \text{avec } 0 \leqslant \beta_i \leqslant \alpha_i$$

Alors :

$$n = \left(\prod_{i=1}^{r} p_i^{\alpha_i - \beta_i}\right) \times m$$

Comme $\prod_{i=1}^{r} p_i^{\alpha_i - \beta_i} \in \mathbb{N}$ (car : $\forall i \in [\![1, r]\!]$, $\alpha_i \geqslant \beta_i$), on en déduit que m divise n.

($\Rightarrow$) Supposons qu'un entier m divise n.
Alors tout nombre premier p intervenant dans la décomposition de m doit diviser n, donc doit appartenir à $\{p_1, \ldots, p_r\}$. Ainsi :

$$m = \prod_{i=1}^{r} p_i^{\beta_i}$$

Il reste à démontrer : $\forall i \in [\![1, r]\!]$, $\alpha_i \geqslant \beta_i$.

× Démontrons par l'absurde : $\alpha_1 \geqslant \beta_1$.
Supposons : $\alpha_1 < \beta_1$. Comme : $m \mid n$, alors :

$$p_1^{\beta_1}\left(\prod_{i=2}^{r} p_i^{\beta_i}\right) \mid p_1^{\alpha_1}\left(\prod_{i=2}^{r} p_i^{\alpha_i}\right)$$

D'où :

$$p_1^{\beta_1 - \alpha_1}\left(\prod_{i=2}^{r} p_i^{\beta_i}\right) \mid \left(\prod_{i=2}^{r} p_i^{\alpha_i}\right)$$

Or, comme $\alpha_1 < \beta_1$:

$$p_1 \mid p_1^{\beta_1 - \alpha_1}\left(\prod_{i=2}^{r} p_i^{\beta_i}\right) \qquad \text{mais} \qquad p_1 \wedge \left(\prod_{i=2}^{r} p_i^{\alpha_i}\right) = 1$$

Absurde !

× De même : $\forall i \in [\![2, r]\!]$, $\alpha_i \geqslant \beta_i$.

□

Exercice 14
Déterminer l'ensemble des diviseurs positifs de 224.

Démonstration.
- La décomposition en facteur premier de 224 est :
$$224 \;=\; 2^5 \times 7$$
- Les diviseurs positifs de 224 sont donc les entiers naturels d qui peuvent s'écrire sous la forme : $d = 2^\alpha \times 7^\beta$, avec $\alpha \in [\![0,5]\!]$ et $\beta \in \{0,1\}$. On en déduit :
$$Div(224) \;=\; \{1,2,4,8,16,32,7,14,28,56,112,224\}$$

□

Proposition 19.
Soient a et b deux entiers dont on connaît les décompositions en facteurs premiers. On peut écrire en rassemblant tous ces facteurs :
$$a \;=\; \prod_{i=1}^{r} p_i^{\alpha_i} \qquad et \qquad b \;=\; \prod_{i=1}^{r} p_i^{\beta_i} \qquad (\forall i \in [\![1,r]\!],\ (\alpha_i,\beta_i) \in \mathbb{N}^2)$$
Alors :
$$\boxed{a \wedge b \;=\; \prod_{i=1}^{r} p_i^{\min(\alpha_i,\beta_i)}}$$
$$\boxed{a \vee b \;=\; \prod_{i=1}^{r} p_i^{\max(\alpha_i,\beta_i)}}$$

Exemples

a) Déterminer $4 \wedge 6$.

Démonstration.
- D'une part : $6 = 2^1 \times 3^1$.
- D'autre part : $4 = 2^2 = 2^2 \times 3^0$.

Or : $\min(1,2) = 1$ et $\min(1,0) = 0$. D'où : $4 \wedge 6 = 2^1 \times 3^0 = 2$. □

b) Déterminer $882 \wedge 25\,725$.

Démonstration.
- D'une part : $882 = 2^1 \times 3^2 \times 7^2 = 2^1 \times 3^2 \times 5^0 \times 7^2$.
- D'autre part : $25\,725 = 3^1 \times 5^2 \times 7^3 = 2^0 \times 3^1 \times 5^2 \times 7^3$.

Or : $\min(1,0) = 0$, $\min(2,1) = 1$, $\min(0,2) = 0$ et $\min(2,3) = 2$.
D'où : $882 \wedge 25\,725 = 2^0 \times 3^1 \times 5^0 \times 7^2 = 3^1 \times 7^2\,(= 147)$. □

c) Déterminer $882 \vee 25\,725$.

Démonstration.
- D'une part : $882 = 2^1 \times 3^2 \times 5^0 \times 7^2$.
- D'autre part : $25\,725 = 2^0 \times 3^1 \times 5^2 \times 7^3$.

Or : $\max(1,0) = 1$, $\max(2,1) = 2$, $\max(0,2) = 2$ et $\max(2,3) = 3$.
D'où : $882 \vee 25\,725 = 2^1 \times 3^2 \times 5^2 \times 7^3\,(= 154\,350)$. □

d) Déterminer $76 \wedge 33$ et $76 \vee 33$.

Démonstration.
- D'une part : $76 = 2^2 \times 19^1 = 2^2 \times 3^0 \times 11^0 \times 19^1$.
- D'autre part : $33 = 3^1 \times 11^1 = 2^0 \times 3^1 \times 11^1 \times 19^0$.

Ainsi :
- × $76 \wedge 33 = 2^0 \times 3^0 \times 11^0 \times 19^0 = 1$
  (les entiers 76 et 33 sont premiers entre eux)
- × $76 \vee 33 = 2^2 \times 3^1 \times 11^1 \times 19^1\,(= 2\,508)$

□