Arithmétique - Chapitre 1

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. □

Commentaire

- 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 : $n \in q\,\mathbb{Z}$.
  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 :*

$$a \mid b \quad \Leftrightarrow \quad -a \mid b \quad \Leftrightarrow \quad a \mid -b \quad \Leftrightarrow \quad -a \mid -b$$

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 :

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

  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 : $a \mid b$.

□

Commentaire

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 :*

$$p \mid p$$

2) *Transitivité :*

$$\big((p \mid q)\ \texttt{ET}\ (q \mid r)\big) \implies (p \mid r)$$

3) *Soit* $(\lambda, \mu) \in \mathbb{Z}^2$.

$$\big((p \mid q)\ \texttt{ET}\ (p \mid r)\big) \ \Rightarrow\ p \mid (\lambda\,q + \mu\,r)$$

En particulier :

a) $\big((p \mid q)\ \texttt{ET}\ (p \mid r)\big) \ \Rightarrow\ p \mid (q + r)$

b) $\big((p \mid q)\ \texttt{ET}\ (p \mid r)\big) \ \Rightarrow\ p \mid (q - r)$

4) *Compatibilité avec l'exponentiation entière : soit* $n \in \mathbb{N}^*$.

$$(p \mid q) \ \Rightarrow\ (p^n \mid q^n)$$

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 :

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

× 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 *anti-symétrique.*

- 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 :

- $\times$ il existe $k_1 \in \mathbb{Z}$ tel que : $q = k_1\, p$,
- $\times$ 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` $(q \mid p)$. □

Commentaire

- 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 :

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

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

- **Synthèse**.
  Vérifions maintenant que chacun des entiers de l'ensemble $\{-9, -2, 0, 1, 2, 3, 5, 12\}$ 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 : $2n - 3 \mid n + 9$.
  - × $\cdots$
  - × 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 : $\{-9, -2, 0, 1, 2, 3, 5, 12\}$. □

Commentaire

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 :

$$\begin{array}{c}\text{l'objet répond à}\\ \text{certains critères}\end{array} \Leftrightarrow \begin{array}{c}\text{l'objet s'écrit sous une}\\ \text{forme particulière}\end{array}$$

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

Exercice 3 *À faire après le 1^{er} chapitre sur les nombres complexes*
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 $b \geqslant 0$, 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 $-|a|$), *i.e.* 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.

Commentaire

- 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 : $r_1 = r_2$.

□

Commentaire

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 $b \geqslant a$, 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 :

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

    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 :

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

    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 $i \geqslant N$:

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

    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 :

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

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

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

où $\mathcal{P}(a)$: il existe $(q, r) \in \mathbb{N}^2$ tel que : $\left\{ \begin{array}{l} a = b\,q + r \\ 0 \leqslant r < b \end{array} \right.$.

▸ **Initialisation** :
Si $a = 0$, alors le couple $(q, r) = (0, 0) \in \mathbb{N}^2$ convient. En effet :

$$\left\{ \begin{array}{l} a = 0 = b \times 0 + 0 = b\,q + r \\ 0 \leqslant r < b \end{array} \right.$$

D'où $\mathcal{P}(0)$.

▸ **Hérédité** : soit $a \in \mathbb{N}$.
Supposons $\mathcal{P}(a)$ et démontrons $\mathcal{P}(a+1)$ (*i.e.* il existe $(q, r) \in \mathbb{N}^2$ tel que : $\left\{ \begin{array}{l} a+1 = b\,q + r \\ 0 \leqslant r < b \end{array} \right.$)

Par hypothèse de récurrence, il existe $(q', r') \in \mathbb{N}^2$ tel que :

$$\left\{ \begin{array}{l} a = b\,q' + r' \\ 0 \leqslant r' < b \end{array} \right.$$

Ainsi : $a + 1 = b\,q' + r' + 1$. Deux cas se présentent :

• si $r' + 1 \leq b$, alors le couple $(q, r) = (q', r' + 1) \in \mathbb{N}^2$ convient. En effet :
  × Tout d'abord :

$$a + 1 = b\,q' + (r' + 1) = b\,q + r$$

  × 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 :

$$a \;=\; b\,q' + r' + 1 \;=\; b\,q' + b \;=\; b\,(q' + 1)$$

  Ainsi le couple $(q, r) = (q' + 1, 0) \in \mathbb{N}^2$ convient. En effet :

$$\begin{cases} a + 1 \;=\; b\,(q' + 1 + 0 \;=\; b\,q + r \\ 0 \leqslant r < b \qquad (car\ r = 0) \end{cases}$$

D'où $\mathcal{P}(a + 1)$.

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

□

Commentaire

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.

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

□

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 soir 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 : $3 \not| \ n^2 - 2$.

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

$$n^2 - 2 \;=\; (3k+1)^2 - 2 \;=\; 9k^2 + 6k + 1 - 2 \;=\; 9k^2 + 6k - 3 + 2 \;=\; 3\left(3k^2 + 3k - 1\right) + 2$$

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

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

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 :

$$n^2 - 2 \;=\; (3k+2)^2 - 2 \;=\; 9k^2 + 12k + 4 - 2 \;=\; 9k^2 + 12k + 2 \;=\; 3\left(3k^2 + 4k\right) + 2$$

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

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

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 $a \equiv b \bmod(n)$.

Commentaire

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

- 1er exemple : $9 \equiv 19\ [5]$. En effet : $9 - 19 = -10$ et $5 \mid -10$.
- 2nd 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 $(n, p) \in \mathbb{Z}^2$.

$$n \equiv 0\ [p] \quad \Leftrightarrow \quad p \mid n$$

III.2. Propriétés de la congruence

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

1) *Réflexivité :* $a \equiv a\ [p]$

2) *Symétrie :*

$$a \equiv b\ [p] \quad \Leftrightarrow \quad b \equiv a\ [p]$$

3) *Transitivité :*

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

4) *Compatibilité avec l'addition :*

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

5) *Compatibilité avec la multiplication :*

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

6) *Compatibilité avec l'exponentiation entière : soit $n \in \mathbb{N}$,*

$$a \equiv b\ [p] \quad \Leftrightarrow \quad a^n \equiv b^n\ [p]$$

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

- **Initialisation** :
  D'après ***1)*** : $1 \equiv 1\ [p]$. Ainsi : $a^0 \equiv b^0\ [p]$.
  D'où $\mathcal{P}(0)$.
- **Hérédité** : soit $n \in \mathbb{N}$.
  Supposons $\mathcal{P}(n)$ et démontrons $\mathcal{P}(n+1)$ (*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 $\mathcal{P}(n+1)$.

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

□

Commentaire

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.

Commentaire

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

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

  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 :

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

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

- 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 : $7^4 \equiv 1\ [10]$.

    Commentaire

    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.

□