CHAPITRE 1

DIVISIBILITÉ DANS $\mathbb{Z}$, DIVISION EUCLIDIENNE, CONGRUENCE

1.1 Prolégomènes

L'ensemble $\mathbb{N}$ des entiers naturels

C'est l'ensemble $\mathbb{N} = \{0\,;\,1\,;\,2\,;\,3\,;\ldots\ldots\}$. On notera $\mathbb{N}^* = \mathbb{N}\backslash\{0\} = \{1\,;\,2\,;\,3\,;\ldots\ldots\}$.

Parties non vides de $\mathbb{N}$

On admet les propriétés suivantes :

Propriétés 1.1.1

Dans l'ensemble $\mathbb{N}$:

- *Toute partie **non vide** de $\mathbb{N}$ possède un plus petit élément (unique).*
- *Toute partie **non vide et majorée** de $\mathbb{N}$ possède un plus grand élément (unique).*

L'ensemble $\mathbb{N}$ est archimédien

L'ensemble $\mathbb{N}$ possède la propriété d'Archimède.

Propriété 1.1.2

Soit $b \in \mathbb{N}^*$. Alors pour tout entier $a \in \mathbb{N}$, il existe un entier naturel n tel que $nb > a$.

Principe de descente infinie

Propriété

Toute suite d'entiers naturels strictement décroissante est stationnaire ; c'est-à-dire constante à partir d'un certain rang.

L'ensemble $\mathbb{Z}$ des entiers relatifs

C'est l'ensemble $\mathbb{Z} = \{0\,;\pm1\,;\pm2\,;\ldots\ldots\}$. On notera de même $\mathbb{Z}^* = \mathbb{Z}\backslash\{0\}$.

■ Parties non vides de $\mathbb{Z}$

On admet les propriétés suivantes :

Propriétés 1.1.3

Dans l'ensemble $\mathbb{Z}$:

- *Toute partie* ***non vide et minorée*** *de $\mathbb{Z}$ possède un plus petit élément (unique).*
- *Toute partie* ***non vide et majorée*** *de $\mathbb{Z}$ possède un plus grand élément (unique).*

■ Le principe du raisonnement par récurrence

Ce principe de démonstration par récurrence s'applique lorsqu'on cherche à démontrer qu'une propriété $\mathscr{P}(n)$ dépendant d'un entier naturel n est vraie pour tout entier $n \geqslant n_0$, n_0 étant un entier naturel donné.

Principe du raisonnement par récurrence 1.1.4

On considère une propriété $\mathscr{P}(n)$. Pour démontrer que $\mathscr{P}(n)$ est vraie pour tout entier $n \geqslant n_0$, on procède en trois étapes :

A) ***Initialisation*** *: on montre que la propriété est vraie pour $n = n_0$, c'est-à-dire que $\mathscr{P}(n_0)$ est vraie.*

B) ***Hérédité*** *: on démontre que :*

Si *la propriété est vraie pour un entier $k \geqslant n_0$,* ***alors*** *elle est vraie pour l'entier suivant $k+1$.*
Autrement dit ***si*** *$\mathscr{P}(k)$ est vraie* ***alors*** *$\mathscr{P}(k+1)$.*

On dit que la propriété est **héréditaire** *à partir du rang n_0.*

C) ***Conclusion*** *:*

- *La propriété est initialisée.*
- *Elle est héréditaire.*

Par conséquent[a] *$\mathscr{P}(n)$ est vraie pour tout entier $n \geqslant n_0$.*

a. Il est primordial que les **deux** conditions de ce principe soient réunies !

Exemple

On souhaite démontrer l'égalité suivante :

$$\text{pour tout } n \geqslant 1, \qquad 1+2+3+\cdots+n = \frac{n(n+1)}{2}.$$

Procédons donc par récurrence en posant pour $n \geqslant 1$, $\mathscr{P}(n) : 1+2+3+\cdots+n = \dfrac{n(n+1)}{2}$.

A) **Initialisation** : pour $n = 1$, on démontre que $\mathscr{P}(1)$ est vraie.
On a :

- d'une part la somme vaut 1 ;
- d'autre part : $\dfrac{1(1+1)}{2} = 1$.

Ainsi $\mathscr{P}(1)$ est vraie. La propriété est donc initialisée.

B) **Hérédité** : soit k un entier fixé. On suppose que $\mathscr{P}(k)$ est vraie $\left(\text{c'est-à-dire que } : 1+2+3+\cdots+k=\frac{k(k+1)}{2}\right)$, c'est hypothèse de récurrence (HR).

On veut alors démontrer que $\mathscr{P}(k+1)$ est vraie $\left(\text{c'est-à-dire que : } 1+2+3+\cdots+(k+1)=\frac{(k+1)(k+2)}{2}\right)$.

On a alors :

$$\begin{aligned} 1+2+3+\cdots+(k+1) &= \underbrace{1+2+3+\cdots+k}+(k+1) \\ &= \frac{k(k+1)}{2}+(k+1) \qquad \text{(HR)} \\ &= \frac{k(k+1)}{2}+\frac{2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2}. \end{aligned}$$

Donc $\mathscr{P}(k+1)$ est vraie.

C) **Conclusion** : la propriété est initialisée et de plus héréditaire, en vertu du principe de récurrence, $\mathscr{P}(n)$ est donc vraie pour tout $n \geqslant 1$.

Ainsi :

$$\text{pour tout } n \geqslant 1, \qquad 1+2+3+\cdots+n=\frac{n(n+1)}{2}.$$

1.2 Divisibilité dans $\mathbb{Z}$

Définition 1.2.1

Soit a et b deux entiers relatifs.

*Dire que b **divise** a signifie qu'il existe un entier $k \in \mathbb{Z}$ tel que : $\boldsymbol{a = bk}$.*

On dit aussi que :

- *b **est un diviseur de** a*
- *a **est un multiple de** b*
- *a **est divisible par** b.*

On notera $\boldsymbol{b|a}$ pour dire que b divise a.

Exemple 1

- 24 est un multiple de 3 car : $24 = 3 \times 8$.
- -4 divise 20 car : $20 = (-5) \times (-4)$.
- Pour tout entier $n \neq 1$, on a $(n-1) \big| \left(n^3-1\right)$, car $n^3-1=(n-1)\left(n^2+n+1\right)$.

Propriété 1.2.2

- *0 est multiple de tout entier.*
- *1 et -1 divisent tout entier.*
- *Si a est un multiple de b et si $a \neq 0$, alors : $|a| \geqslant |b|$.*
- *Si $a|b$ et $b|a$, alors $a = b$ ou $a = -b$ avec a et b non nuls.*

Démonstration

- Pour tout entier n, on a $0 = n \times 0$.
- Pour tout entier n, on a $n = 1 \times n = (-1) \times (-n)$.
- Soit $a \neq 0$ et b entiers tels que $b|a$. Il existe un entier $k \neq 0$ tel que $a = bk$. Ainsi $|a| = |b| \times |k| \geqslant |b|$ (car $|k| \geqslant 1$).
- Si $a|b$ et $b|a$, alors il existe des entiers k et k' tels que : $b = ak$ et $a = bk'$. Ainsi $a = akk'$. Comme $a \neq 0$ alors $kk' = 1$. Cette égalité implique que $k = k' = 1$ ou $k = k' = -1$.
  - Si $k = k' = 1$, alors $a = b$.
  - Si $k = k' = -1$, alors $a = -b$.

□

NOTATIONS : soit a est un entier relatif.

✔ On notera $\mathscr{D}(a)$ l'ensemble des diviseurs de a. Cet ensemble est une partie non vide et finie de $\mathbb{Z}$.

✔ On notera $\mathscr{D}_{\mathbb{N}}(a)$ l'ensemble des diviseurs entiers **naturels** de a.

Exemple

a) Déterminer les diviseurs dans $\mathbb{N}$ de 15.

b) Déterminer les diviseurs dans $\mathbb{Z}$ de 24.

c) Déterminer tous les couples d'entiers naturels $(x\ ;\ y)$ tels que : $x^2 - xy = 12$.

d) Déterminer tous les entiers relatifs n tels que $n - 4$ divise $n + 10$.

---

a) Les diviseurs dans $\mathbb{N}$ de 15 sont les entiers naturels m et n tels que $m \times n = 15$. Ainsi :

$$\boxed{\mathscr{D}_{\mathbb{N}}(15) = \left\{1\ ;\ 3\ ;\ 5\ ;\ 15\right\}}$$

b) De même, les diviseurs dans $\mathbb{Z}$ de 24 sont :

$$\boxed{\mathscr{D}(24) = \left\{-24\ ;\ -12\ ;\ -8\ ;\ -6\ ;\ -4\ ;\ -3\ ;\ -2\ ;\ -1\ ;\ 1\ ;\ 2\ ;\ 3\ ;\ 4\ ;\ 6\ ;\ 8\ ;\ 12\ ;\ 24\right\}}$$

c) On cherche les couples d'entiers naturels $(x\ ;\ y)$ vérifiant : $x^2 - xy = 12$. L'idée consiste à écrire l'équation sous la forme $M \times N = 12$. On a :

$$x^2 - xy = 12 \iff x(x - y) = 12.$$

Ainsi les entiers x et $x-y$ sont des diviseurs associés de 12. Les diviseurs dans $\mathbb{N}$ de 12 sont $\mathscr{D}_{\mathbb{N}}(12)=\left\{1\ ;\ 2\ ;\ 3\ ;\ 4\ ;\ 6\ ;\ 12\right\}$.

De plus, comme x et y sont entiers naturels, alors $x \geqslant x-y$.
Par suite, si $(x\ ;\ y)$ est une solution de $x^2-xy=12$, alors :

$$\begin{cases} x=12 \\ x-y=1 \end{cases} \quad \text{ou} \quad \begin{cases} x=6 \\ x-y=2 \end{cases} \quad \text{ou} \quad \begin{cases} x=4 \\ x-y=3 \end{cases}$$

Donc

$$\begin{cases} x=12 \\ y=11 \end{cases} \quad \text{ou} \quad \begin{cases} x=6 \\ y=4 \end{cases} \quad \text{ou} \quad \begin{cases} x=4 \\ y=1. \end{cases}$$

Donc $(x\ ;\ y)=(12\ ;\ 11)$ ou $(x\ ;\ y)=(6\ ;\ 4)$ ou $(x\ ;\ y)=(4\ ;\ 1)$.

Réciproquement, on peut vérifier que chacun de ces trois couples est solution de l'équation $x^2-xy=12$.

d) Si $n-4$ divise $n+10$ alors il existe un entier relatif k tel que $n+10=k(n-4)$. L'idée consiste encore une à écrire une relation de la forme $M \times N =$ constante. On transforme la relation précédente dans ce sens :

$$n+10=k(n-4) \iff (n-4)+14=k(n-4) \iff (n-4)(k-1)=14.$$

Donc $(n-4)$ est un diviseur de 14. Et comme

$$\mathscr{D}(14)=\left\{-14\ ;\ -7\ ;\ -2\ ;\ -1\ ;\ 1\ ;\ 2\ ;\ 7\ ;\ 14\right\}.$$

On peut utiliser un tableau pour obtenir les valeurs possibles de n :

$n-4$	-14	-7	-2	-1	1	2	7	14
n	-10	-3	2	3	5	6	11	18

Réciproquement, si n prend une des valeurs du tableau, on vérifie également que $n-4$ divise $n+10$.

■ Propriétés de la divisibilité dans $\mathbb{Z}$

Théorème (Transitivité)

Soit trois entiers relatifs a, b et c. Si a divise b et b divise c, alors a divise c.

Démonstration

Par hypothèse, il existe k et k' entiers tels que : $b=ka$ et $c=k'b$. On a ainsi : $c=kk'a$. Par conséquent a divise c. □

Théorème (Divisibilité d'une combinaison)

Soit trois entiers relatifs a, b et c.

Si a divise b et a divise c, alors :

- *a divise $b+c$ et a divise $b-c$;*
- *a divise $mb+nc$ où m et n sont des entiers (on dit a divise toute combinaison linéaire de b et c).*

Démonstration

On sait que a divise b et c, donc il existe deux entiers k et k' tels que :

$$b = ka \quad \text{et} \quad c = k'a.$$

Donc $b+c = \underbrace{(k+k')}_{\text{entier}}a$ et $b-c = \underbrace{(k-k')}_{\text{entier}}a$. De plus si m et n sont des entiers, alors $mb+nc = \underbrace{(mk+nk')}_{\text{entier}}a$.

Donc a divise $b+c$, $b-c$ et $mb+nc$. □

Exemple

a) Démontrer que pour tout entier naturel n, 7 divise $7^{2n} - 21$.

b) k étant un entier naturel, on pose $a = 5k+7$ et $b = 2k+8$. Démontrer que si d est un diviseur positif commun à a et b, alors d divise 26.

c) Déterminer les entiers relatifs n tels que $n-4$ divise $2n+3$.

d) Montrer que la somme de trois entiers consécutifs est divisible par 3.

e) Montrer que si n est un entier pair alors l'entier $B = (n+2)(3n+4)$ est un multiple de 4.

---

a) Soit $n \in \mathbb{N}$. Comme $7 \mid 7^{2n}$ et $7|21$ alors par différence $7 \mid 7^{2n} - 21$.

b) Soit d un diviseur commun à a et b. Alors d divise toute combinaison linéaire $ma+nb$. Il suffit alors de choisir judicieusement m et n pour que l'entier k ne figure plus dans le multiple.
En prenant $m = -2$ et $n = 5$, alors $d | -2(5k+7)+5(2k+8)$, et donc que $d|26$.

Ainsi d est un diviseur positif de 26.

c) Soit $n \in \mathbb{Z}$ tel que $n-4$ divise $2n+3$. Comme $n-4$ divise $n-4$ alors par combinaison $n-4 \mid 2n+3-2(n-4)$, donc $n-4 \mid 11$.

Réciproquement, si $n-4 \mid 11$ et comme $n-4 \mid 2(n-4)$, alors par somme $n-4 \mid 2(n-4)+11$ et donc $n-4 \mid 2n+3$.

Conclusion : $n-4$ divise $2n+3$ si, et seulement si, $n-4$ divise 11. Comme $\mathscr{D}(11) = \left\{-11 ; -1 ; 1 ; 11\right\}$, on peut encore donner les valeurs de n à l'aide d'un tableau :

$n-4$	-11	-1	1	11
n	-7	3	5	15

d) Pour tout $n \in \mathbb{Z}$, le nombre $S = n + (n+1) + (n+2)$ est la somme de trois entiers consécutifs. On a $S = 3n + 3 = 3(n+1)$ qui est bien divisible par 3 puisque $n+1$ est un entier.

e) Soit $n \in \mathbb{Z}$. Si n est pair, alors il existe un entier p tel que $n = 2p$. On a alors $B = (n+2)(3n+4) = (2p+2)(3(2p)+4) = 2(p+1) \times 2(3p+2) = 4\underbrace{(p+1)(3p+2)}_{\text{entier}}$.

Ceci justifie que si n est pair, alors l'entier $(n+2)(3n+4)$ est divisible par 4.

1.3 La division euclidienne

Théorème 1.3.1

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Alors il existe un unique couple d'entiers $(q; r)$ tels que :

$$a = bq + r \qquad \text{avec} \qquad 0 \leqslant r < b.$$

*On dit que l'on fait la **division euclidienne** de a par b.*

a s'appelle le dividende, b le diviseur, q le quotient et r le reste.

Démonstration

► **Existence du couple $(q\ ;\ r)$.**

Sans restreindre la généralité, on peut supposer $a \geqslant 0$.

Soit $\mathscr{A} = \left\{n \in \mathbb{N} \mid bn \leqslant a\right\}$. L'ensemble $\mathscr{A}$ est un ensemble non vide car $n = 0 \in \mathscr{A}$. De plus pour $n \in \mathscr{A}$, on a $n \leqslant a$. L'ensemble $\mathscr{A}$ possède donc un nombre fini d'éléments, il possède donc un plus grand élément : notons le q.
Comme $q \in \mathscr{A}$, alors $qb \leqslant a$ et $(q+1)b > a$ car $q+1 \notin \mathscr{A}$. On a donc :

$$qb \leqslant a < (q+1)b \iff qb \leqslant a < qb + b.$$

On définit le nombre $r = a - qb$; ce nombre r vérifie par définition $0 \leqslant r = a - qb < b$. On a bien montré l'existence d'un couple d'entiers $(q\ ;\ r)$ vérifiant : $a = bq + r$ et $0 \leqslant r < b$.

► **Unicité du couple $(q\ ;\ r)$.**

On suppose qu'il existe deux couples d'entiers (q, r) et (q', r') tels que :

$$\begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases} \qquad \text{et} \qquad \begin{cases} a = bq' + r' \\ 0 \leqslant r' < b \end{cases}$$

De $a = bq + r$ et $a = bq' + r'$ on déduit $r' - r = b(q - q')$, donc $r' - r$ est multiple de b. Par ailleurs $0 \leqslant r < b$ et $0 \leqslant r' < b$ donnent $-b < r' - r < b$.
Ainsi comme $r' - r$ est un multiple de b et que 0 est le seul multiple de b strictement compris entre $-b$ et b, alors $r' - r = 0$, et $r = r'$.
Puisque $b \neq 0$, de $b(q - q') = 0$ on déduit que $q = q'$. L'unicité est acquise.

$\square$

Exemple

- La division euclidienne de 186 par 8 : $186 = 8 \times 23 + 2$.
- La division euclidienne de -37 par 3 : $-37 = 3 \times (-13) + 2$

Exemple

a) Déterminer tous les entiers qui divisés par 7 donne un quotient égal à deux fois le reste.

b) Lorsqu'on divise a par b, le reste est 5 et lorsqu'on divise $3a$ par b, le reste est 3. Déterminer le diviseur b.

---

a) Soit n un entier relatif. En écrivant la division euclidienne de n par 7, on a $n = 7q + r$ avec $0 \leqslant r < 7$. La condition de l'énoncé s'écrit : $n = 7(2r) + r = 15r$. Ainsi :

$$\begin{cases} n = 15r \\ 0 \leqslant r < 7 \end{cases} \iff \begin{cases} n = 15r \\ 0 \leqslant r \leqslant 6. \end{cases}$$

Les entiers répondant au problème sont donc tous les entiers de la forme $n = 15r$ où $0 \leqslant r \leqslant 6$. On obtient ces entiers n en construisant un tableau :

r	0	1	2	3	4	5	6
$n = 15r$	0	15	30	45	60	75	90

b) Écrivons les deux divisions euclidiennes, en notant q et q' les quotients :

$$\begin{cases} a = bq + 5 & \text{avec} \quad b > 5 \\ 3a = bq' + 3 & \text{avec} \quad b > 3. \end{cases}$$

En multipliant la première ligne par 3 et en égalisant avec la deuxième, on obtient :

$$3bq + 15 = bq' + 3 \quad \text{avec} \quad b > 5.$$

Donc

$$b(q' - 3q) = 12$$

Par suite b est un diviseur de 12 avec la condition $b > 5$. Le seul diviseur convenable est $b = 6$ car si $b = 12$, la deuxième division euclidienne donnerait $a = bq + 1$.

■ Utilisation de la division euclidienne : écriture d'un entier relatif

Propriété 1.3.2

Soit b un entier naturel non nul. Tout entier relatif n s'écrit de manière unique $n = bq + r$ avec $r = 0,\ 1,\ 2, \dots,\ b-1$ et où q est un entier relatif.