

Chapitre I

Divisibilité et Congruences

Table des matières

Partie A : Divisibilité dans \mathbb{Z}	2
1. Définitions	2
2. Propriétés	4
3. Activité : les règles simples de divisibilité	5
4. Exercices types	6
Partie B : Division euclidienne	9
1. La division euclidienne	9

Partie A

Divisibilité dans \mathbb{Z}

Activité d'introduction : Math'x Problème 1 page 14.

1. Définitions

Définition 1. *Diviseur - Multiple*

Soit a et b deux entiers relatifs. On dit que a est **multiple** de b s'il existe $k \in \mathbb{Z}$ tel que

$$a = kb.$$

Dans ce cas, on dira également que b est un **diviseur** de a ou même que b **divise** a .

Exemple 1.

- -84 est un multiple de -28 . En effet, $-84 = 3 \times -28$.
- 2 divise tous les nombres pairs.
- 1 et -1 divisent tous les nombres entiers relatifs.
- 0 est multiple de tous les nombres entiers relatifs. Par contre, il ne divise que lui-même.

Exercice 1.

1. Donner tous les diviseurs de 24 .
2. Montrer que la somme de trois entiers relatifs consécutifs est divisible par 3 .
La somme de 2 entiers consécutifs est-elle divisible par 2 ?

Correction.

1. Les diviseurs de 24 sont :

$$-24, -12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12, 24.$$

2. Soit $n \in \mathbb{Z}$. Montrons que la somme S de n , de $n + 1$ et de $n + 2$ est divisible par 3 .

On a :

$$S = n + (n + 1) + (n + 2) = n + n + n + 1 + 2 = 3n + 3 = 3(n + 1).$$

Ainsi, il existe $k \in \mathbb{Z}$ tel que $S = k \times 3$ (ici, $k = n + 1$). Il en résulte que la somme de trois entiers consécutifs $S = n + (n + 1) + (n + 2)$ est divisible par 3 .

Par contre, la somme de 2 entiers consécutifs n'est pas divisible par 2 . En effet, on a par exemple $1 + 2 = 3$ qui n'est pas divisible par 2 .

Notation 1.

Soit n un entier relatif. On note

$$n\mathbb{Z} = \{\dots - 3n, -2n, -n, 0, n, 2n, 3n, \dots\} = \{nk \mid k \in \mathbb{Z}\},$$

l'ensemble des multiples de n .

Par exemple, $4\mathbb{Z} = \{\dots, -12, -8, -4, 0, 4, 8, 12, \dots\}$

Exercice 2.

1. Comment appelle-t-on d'habitude l'ensemble $2\mathbb{Z}$?
2. Déterminer l'ensemble $-2\mathbb{Z}$, l'ensemble $1\mathbb{Z}$ puis l'ensemble $0\mathbb{Z}$.
3. Montrer que $12\mathbb{Z} \subset 4\mathbb{Z}$.
4. (*) Soit $n, m \in \mathbb{Z}$. Montrer que m divise n si, et seulement si, $n\mathbb{Z} \subset m\mathbb{Z}$.

Correction.

1. $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\} = \{\dots, -8, -6, -4, -2, 0, 2, 4, 6, 8, \dots\}$ est connu sous le nom d'ensemble des nombres pairs.
2. — $-2\mathbb{Z} = 2\mathbb{Z}$;
— $1\mathbb{Z} = \mathbb{Z}$;
— $0\mathbb{Z} = \{0\}$.
3. Soit $p \in 12\mathbb{Z}$. Alors, p est un multiple de 12 i.e. il existe $k \in \mathbb{Z}$ tel que $p = 12k$.
Or on a :

$$p = 12k = (4 \times 3)k = 4 \times \underbrace{3k}_{\in \mathbb{Z}};$$

donc p est un multiple de 4 - i.e. il existe $k' \in \mathbb{Z}$ tel que $p = 4k'$ (ici $k' = 3k$).

Il en résulte que p appartient à $4\mathbb{Z}$.

Ceci étant vrai quelque soit $p \in 12\mathbb{Z}$, on en déduit que $12\mathbb{Z} \subset 4\mathbb{Z}$.

4. Soit $n, m \in \mathbb{Z}$. Ici, on cherche à montrer une équivalence ("si, set seulement, si" = \Leftrightarrow) : on doit donc montrer deux implications :
— (\Rightarrow) : Si m divise n , alors $n\mathbb{Z} \subset m\mathbb{Z}$.
On suppose que m divise n . Montrons que $n\mathbb{Z} \subset m\mathbb{Z}$.
Soit $p \in n\mathbb{Z}$. Alors il existe $k \in \mathbb{Z}$ tel que $p = nk$. Or, par hypothèse, m divise n . Alors il existe $k' \in \mathbb{Z}$ tel que $n = mk'$. Par suite, on a :

$$p = nk = (mk')k = m \underbrace{(k'k)}_{\in \mathbb{Z}}.$$

Par suite, il existe $k'' \in \mathbb{Z}$ tel que $p = mk''$. Donc $p \in m\mathbb{Z}$.

Il en résulte que $n\mathbb{Z} \subset m\mathbb{Z}$.

- (\Leftarrow) : Si $n\mathbb{Z} \subset m\mathbb{Z}$, alors m divise n .
On suppose que $n\mathbb{Z} \subset m\mathbb{Z}$. Montrons que m divise n .
Comme $n \in n\mathbb{Z}$ et $n\mathbb{Z} \subset m\mathbb{Z}$, alors $n \in m\mathbb{Z}$. Par suite, il existe $k \in \mathbb{Z}$ tel que $n = mk$.
Il en résulte que m divise n .

On a montré les deux implications de l'équivalence, et ainsi, on a montré que m divise n si, et seulement si, $n\mathbb{Z} \subset m\mathbb{Z}$.

2. Propriétés

Proposition 1.

Soit a, b des entiers relatifs.

- Si b divise a et $a \neq 0$, alors $|b| \leq |a|$.
- Si b divise a et a divise b , alors $a = b$ ou $a = -b$.

Démonstration.

Soit $a, b \in \mathbb{Z}$.

- On suppose que b divise a et $a \neq 0$. Montrons que $|b| \leq |a|$.
Comme b divise a , il existe $k \in \mathbb{Z}$ tel que $a = bk$. Or $a \neq 0$, donc $k \neq 0$. Ainsi, $|k| \geq 1$ d'où :

$$|a| = |bk| = |b| \cdot \underbrace{|k|}_{\geq 1} \geq |b|.$$

ou On suppose que b divise a et a divise b . Montrons que $a = \pm b$.

D'après la propriété précédente, comme b divise a , alors $|b| \leq |a|$. De même, comme a divise b , alors $|a| \leq |b|$. Par suite,

$$|a| = |b|.$$

Il en résulte que $a = b$ ou $a = -b$. □

Théorème 1. Transitivité

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

Démonstration.

Soit $a, b, c \in \mathbb{Z}$. On suppose que c divise b et b divise a . Montrons que c divise a .

Comme c divise b , alors il existe $k \in \mathbb{Z}$ tel que $b = kc$ et comme b divise a , alors il existe $k' \in \mathbb{Z}$ tel que $a = k'b$. Par suite, on a :

$$a = k'b = k'(kc) = \underbrace{k'k}_{\in \mathbb{Z}} c.$$

Il en résulte que c divise a . □

Théorème 2. Combinaison linéaire

Soit a, b et d des entiers relatifs. Si d divise a et d divise b , alors, pour tous $u, v \in \mathbb{Z}$, d divise $ua + vb$.

En particulier, si d divise a et b , d divise $a + b$ et $a - b$.

Correction.

Soit $a, b, d \in \mathbb{Z}$. On suppose que d divise a et d divise b . Montrons que, pour tous $u, v \in \mathbb{Z}$, d divise $ua + vb$.

Soit $u, v \in \mathbb{Z}$. Comme d divise a , alors il existe $k \in \mathbb{Z}$ tel que $a = kd$ et comme d divise b , alors il existe $k' \in \mathbb{Z}$ tel que $b = k'd$. Par suite, on a :

$$ua + vb = u(kd) + v(k'd) = \underbrace{(uk + vk')}_{\in \mathbb{Z}} d.$$

Il en résulte que d divise $ua + vb$.

3. Activité : les règles simples de divisibilité

Nous prouverons les résultats de l'exercice suivant dans la partie consacrée aux congruences.

Exercice 3.

Donner, sans démonstration, les règles générales qui permettent de savoir si un nombre entier relatif est divisible par :

1. le nombre 2 ;
2. le nombre 5 ;
3. les nombres 10, 100, ... , 10^n où $n \in \mathbb{N}$;
4. le nombre 3 ;
5. le nombre 9 ;
6. pour des entiers de 2 ou 3 chiffres, le nombre 11.

Correction.

1. Tout nombre entier relatif finissant par 0, 2, 4, 6 ou 8 est divisible par 2.
2. Tout nombre entier relatif finissant par 0 ou 5 est divisible par 5.
3. Tout nombre entier relatif finissant par n zéros est divisible par 10^n .
4. Tout nombre entier relatif dont les sommes successives des chiffres aboutissent à 3, 6 ou 9 est divisible par 3.
5. Tout nombre entier relatif dont les sommes successives des chiffres aboutissent à 9 est divisible par 9.
6. Tout nombre entier relatif de deux chiffres égaux est divisible par 11 et tout nombre entier relatif de trois chiffres dont la somme des deux chiffres extrêmes est égal au chiffre central

est divisible par 11 .

4. Exercices types

Voici quelques exercices classiques de divisibilité :

Exercice 4. Couple d'entiers satisfaisant une équation

On considère l'équation d'inconnues x et y :

$$x^2 = 15 + 2xy.$$

Existe-t-il des couples (x, y) d'entiers naturels qui sont solutions de l'équation précédente ?

Le principe est de résolution de ce genre d'exercices est le suivant :

- On transforme l'équation de telle sorte qu'on puisse trouver :
 - dans le membre de gauche, tous les termes faisant apparaître x et y ;
 - dans le membre de droite, tous les termes constants - dans ces exercices, il s'agira obligatoirement d'un **nombre entier**.
- On factorise le membre de gauche (celui avec les x et y de telle sorte qu'on puisse faire apparaître 2 facteurs (ou plus).
les inconnues x et y étant supposées entières, les facteurs précédents le sont aussi. Ce sont donc des diviseurs de l'entier présent dans le membre de droite.
- On établit la liste des diviseurs du membre de droite et on réunit ceux dont le produit est égal au membre de droite.
- Finalement, on fait correspondre les facteurs du membre de gauche avec chaque réunion de diviseurs et on résout les systèmes obtenus.

Correction.

L'équation $x^2 = 15 + 2xy$ est équivalente à :

$$x^2 - 2xy = 15 \quad \Leftrightarrow \quad x(x - 2y) = 15$$

Les diviseurs dans \mathbb{N} de 15 sont 1, 3, 5 et 15. Les décompositions de 15 en produits de deux facteurs entiers sont donc :

$$15 \times 1 \text{ ou } 1 \times 15 \text{ ou } 5 \times 3 \text{ ou } 3 \times 5.$$

On remarque de plus, que comme x, y sont positifs, $x \geq x - 2y$ donc les seuls décompositions possibles de la forme $x(x - 2y)$ sont :

$$\begin{cases} x & = 15 \\ x - 2y & = 1 \end{cases} \text{ ou } \begin{cases} x & = 5 \\ x - 2y & = 3 \end{cases}$$

On en déduit :

$$\begin{cases} x & = 15 \\ y & = 7 \end{cases} \text{ ou } \begin{cases} x & = 5 \\ y & = 1 \end{cases}$$

Ainsi, les seuls couples (x, y) d'entiers naturels solutions de $x^2 = 15 + 2xy$ sont $(15, 7)$ et $(15, 1)$.

Exercice corrigé : Exercice 2 p19

Exercices supplémentaires : Exercice 4 p33, Exercice 11 p34

Exercice 5.

Déterminer tous les nombres entiers relatifs n tels que $3n + 2$ divise $4n + 1$.

Le principe est de résolution de ce genre d'exercices est le suivant :

- On cherche une combinaison linéaire des deux termes de l'énoncé qui élimine la variable n recherchée ;
- On utilise le théorème 2 sur les combinaisons linéaires pour obtenir un relation de divisibilité avec un nombre entier relatif simple.
- On établit la liste des diviseurs de cet entier, et on vérifie, pour chaque diviseur, s'il fait l'affaire.

Correction.

On suppose que $3n + 2$ divise $4n + 1$. Comme, de plus, $3n + 2$ divise $3n + 2$, d'après le théorème 2, $3n + 2$ divise la combinaison linéaire :

$$4(3n + 2) - 3(4n + 1) = 12n - 12n + 8 - 3 = 5.$$

Ainsi, $3n + 2$ divise 5. Or 5 admet quatre diviseurs dans \mathbb{Z} :

$$-5, -1, 1, 5.$$

Par suite, on a les possibilités suivantes :

- $3n + 2 = -5$ ce qui implique $n = \frac{-7}{3}$. Impossible !
- $3n + 2 = -1$ ce qui implique $n = -1$.
- $3n + 2 = 1$ ce qui implique $n = \frac{-1}{3}$. Impossible !
- $3n + 2 = 5$ ce qui implique $n = 1$.

Ainsi, les deux solutions potentielles sont $n = -1$ et 1. On vérifie alors que ces valeurs conviennent bien :

- $3 \times (-1) + 2 = -1$ divise $-3 = 4 \times (-1) + 1$ donc $n = -1$ est bien solution ;
- $3 \times 1 + 2 = 5$ divise $5 = 4 \times 1 + 1$ donc $n = 1$ est bien solution.

Exercice corrigé : Exercice 3 p19

Exercices supplémentaires : Exercice 29 p36, Exercice 33 p36

Partie B

Division euclidienne

Activité d'introduction : Math'x Problème 3 page 15.

1. La division euclidienne

La division euclidienne est l'un des outils principaux de l'arithmétique.

a. La division euclidienne dans \mathbb{N}

Théorème 3. Division euclidienne dans \mathbb{N}

Soit a, b des entiers **naturels** tels que $b \neq 0$.

Il existe un **unique** couple (q, r) d'entiers naturels tels que :

$$a = bq + r \quad \text{et} \quad 0 \leq r < b.$$

Démonstration.

Soit $a, b \in \mathbb{N}$ tels que $b \neq 0$.

- **Existence.** On considère le sous-ensemble M de \mathbb{N} suivant :

$$M = \{k \in \mathbb{N} \mid bk \leq a\}.$$

Comme $b \neq 0$, M est majoré par le premier entier supérieur au nombre rationnel $\frac{a}{b}$ (il s'agit de l'entier $E\left(\frac{a}{b}\right) + 1$). Et de plus, M est non vide car $0 \in M$.

Ainsi, M est une partie non vide et majorée de \mathbb{N} ; elle admet donc un plus grand élément q . On admet ici le résultat : toute partie non vide et majorée de \mathbb{N} admet un plus grand élément.

Par suite, bq est le plus grand multiple de b inférieur ou égal à a et donc on a :

$$bq \leq a < b(q+1).$$

En posant $r = a - bq$, on obtient, en retranchant bq dans l'inégalité précédente :

$$0 \leq r < b.$$

et on a bien $bq + r = bq + (a - bq) = a$.

- **Unicité.** Supposons que les couples (q, r) et (q', r') vérifient :

$$a = bq + r \quad \text{avec} \quad 0 \leq r < b \quad \text{et} \quad a = bq' + r' \quad \text{avec} \quad 0 \leq r' < b.$$

Alors :

$$0 = a - a = b(q - q') + (r - r'),$$

d'où $b(q' - q) = r - r'$.

Par suite, $r - r'$ est un multiple de b qui vérifie $-b < r - r' < b$. Or 0 est le seul multiple de b strictement compris entre $-b$ et b .

Donc $0 = r - r' = b(q' - q)$. Ainsi $r = r'$ et $q = q'$ (car $b \neq 0$).

Il en résulte qu'il n'existe qu'un seul couple (q, r) d'entiers naturels tels que :

$$a = bq + r \quad \text{et} \quad 0 \leq r < b.$$

□

Remarque 1.

Dans la division euclidienne de a par b - $a = bq + r$ avec $0 \leq r < b$:

- a est appelé le **dividende** ;
- b est appelé le **diviseur** ;
- q est appelé le **quotient** ;
- r est appelé le **reste** ;

Exercice 6.

En utilisant les souvenirs enfouis dans votre mémoire, effectuer, à la main, les divisions euclidiennes suivantes :

12 par 5; 129 par 11; 4237 par 7;

b. Algorithme de la division euclidienne dans \mathbb{N}

Algorithme de la division euclidienne dans \mathbb{N}

```
1 Variables : a,b entiers naturels
2
3 Initialisation : reste=a, quotient=0
4
5 Traitement :
6   TANT QUE reste>=b FAIRE
7     reste = reste-b
8     quotient = quotient+1
9   FIN TANT QUE
10
11 Sortie :
12   RETOURNER quotient, reste
```