

Chapitre n° 2 : Divisibilité dans \mathbb{Z}

1 Avant-propos

L'arithmétique a pour objet l'étude des nombres entiers.

« L'arithmétique, c'est être capable de compter jusqu'à vingt sans enlever ses chaussures. »

Walt Disney (1901-1966)

On admettra les propriétés suivantes :

Propriété 1

- **Principe du bon ordre** : toute partie **non vide** de \mathbb{N} admet un plus petit élément.
- **Principe de descente infinie** : toute suite décroissante **et à valeurs dans** \mathbb{N} est constante à partir d'un certain rang.

2 Multiples et diviseurs dans \mathbb{Z}

2.1 Définition et propriétés

Définition 1: multiple

Soit a et b deux entiers relatifs.

a est un **multiple** de b si, et seulement si, **il existe** un entier relatif k tel que : $a = kb$.

Remarque 1 (diviseur):

- D'autres formulations sont possibles : « a est divisible par b », « b divise a », « b est un **diviseur** de a » pour décrire la relation $a = kb$.
- On utilise la notation $b|a$ pour signifier que b divise a .

Exemple 1:

① $6 = 2 \times 3$ donc 2 et 3 sont des diviseurs de 6.

Les diviseurs dans \mathbb{N} de 6 sont : 1, 2, 3, 6.

② $-52 = (-4) \times 13$ donc -4, 4, -13 et 13 sont des diviseurs de -52.

Les diviseurs dans \mathbb{Z} de -52 sont : -52, -26, -13, -4, -2, -1, 1, 2, 4, 13, 26, 52.

Propriété 2

- ① 0 est **multiple** de tout entier a car il existe un entier k tel que $0 = k \times a$, il suffit de prendre $k = 0$.
- ② 0 est **diviseur** de 0 car $0 = 0 \times a$ car il existe un entier k tel que $0 = k \times 0$, on peut même choisir l'entier que l'on veut pour k .
- ③ 1 **divise** tout entier a car $a = a \times 1$.
- ④ Si a est un **multiple** de b et si $a \neq 0$, alors : $|a| \geq |b|$.
- ⑤ Soit a et b non nuls. Si a **divise** b et si b **divise** a , alors $a = b$ ou $a = -b$.

Méthode 1 (Utiliser la divisibilité pour résoudre un problème): Comme un entier ne possède qu'un nombre restreint de diviseurs (du moins dans les exercices), on cherchera à factoriser une équation diophantienne^a de manière à se ramener à un problème de divisibilité.

Exercice

Déterminer tous les couples d'entiers naturels $(x; y)$ tels que : $x^2 - 2xy = 15$.

Correction

Exercice

Déterminer tous les entiers relatifs n tels que $(n - 3)$ divise $(n + 5)$.

Correction

Si $(n - 3)$ divise $(n + 5)$, alors

De l'astuce $5 = -3 + 8$, on obtient :

Donc $(n - 3)$ est un diviseur de 8.

L'ensemble des diviseurs dans \mathbb{Z} de 8 est $\mathcal{D}[8] = \{-8; -4; -2; -1; 1; 2; 4; 8\}$.

On a donc le tableau suivant correspondant aux valeurs possibles de n :

| | | | | | | | | |
|-------|----|----|----|----|---|---|---|----|
| $n-3$ | -8 | -4 | -2 | -1 | 1 | 2 | 4 | 8 |
| n | -5 | -1 | 1 | 2 | 4 | 5 | 7 | 11 |

On vérifie que $(n - 3)$ divise bien $(n + 5)$ pour toutes ces valeurs de n :
 $-8|0; \quad -4|4; \quad -2|6; \quad -1|7; \quad 1|9; \quad 2|10; \quad 4|12; \quad 8|16$

^a. équation à coefficients entiers et dont on cherche les solutions entières

2.2 Opérations sur les multiples

Propriété 3: combinaisons linéaires

Soit trois entiers relatifs a , b et c .

Si a **divise** b et c , alors a **divise** $b + c$; $b - c$ ou toute **combinaison linéaire** de b et de c , c'est-à-dire tout entier de la forme $\alpha b + \beta c$, où α et β sont deux entiers relatifs.

Preuve 1: On sait que a divise b et c , donc il existe deux entiers relatifs k et k' tels que :

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

On a alors : $b + c = (k + k')a$; $b - c = (k - k')a$ et $\alpha b + \beta c = (\alpha k + \beta k')a$.

Donc a divise $b + c$; $b - c$ et $\alpha b + \beta c$.

Exemple 2: k étant un entier naturel, on pose $a = 9k + 2$ et $b = 12k + 1$.

Pour déterminer une condition sur les diviseurs positifs communs à a et b , on cherche à éliminer k par une combinaison linéaire. La combinaison linéaire qui permet d'éliminer k consiste à trouver le plus petit multiple commun à 9 et 12, soit 36.

Soit d un diviseur commun à a et b .

Comme d divise a et b , il divise aussi $c = 4a - 3b$, soit

$$c = 4(9k + 2) - 3(12k + 1) = 36k + 8 - 36k - 3 = 5.$$

Donc d doit diviser 5. Comme 5 n'a que deux diviseurs positifs 1 et 5, les diviseurs positifs communs à a et b sont à chercher dans $\{1 ; 5\}$.

3 La division euclidienne

Définition 2

Soit a un entier relatif et b un entier naturel non nul.

On appelle **division euclidienne** de a par b , l'opération qui, au couple $(a ; b)$, associe l'unique couple $(q ; r)$ tel que :

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

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

Preuve 2:

Existence du couple $(q; r)$:

Unicité du couple $(q; r)$:

Exemple 3:

① La division euclidienne de 114 par 8 correspond à : $114 = 8 \times 14 + 2$.

Ainsi $q = 14$ et $r = 2$.

② Pour avoir un reste positif dans la division euclidienne de -114 par 8, on écrit : $-2 = 6 - 8$.

On obtient alors : $-114 = 8 \times (-14) - 2 = 8 \times (-14) - 8 + 6 = 8 \times (-15) + 6$.

Ainsi $q = -15$ et $r = 6$.

Remarque 2:

- Le reste est toujours un entier naturel inférieur au diviseur. Par conséquent, dans la division par 7, par exemple, il existe 7 restes possibles : 0, 1, 2, 3, 4, 5, 6.

- On peut schématiser la division euclidienne comme on pose une division :
$$\begin{array}{r} a \mid b \\ r \mid q \end{array}$$

Ainsi, en reprenant l'exemple de la division de 114 par 8, on a :

$$\begin{array}{r} 114 \mid 8 \\ 34 \mid 14 \\ 2 \end{array}$$
Méthode 2 (Utiliser la définition de la division euclidienne):**Exercice**

Trouver tous les entiers dont le quotient dans la division euclidienne par 5 donne un quotient égal à 3 fois le reste.

Correction

Exercice Lorsqu'on divise a par b , le reste est 8 et lorsqu'on divise $2a$ par b , le reste est 5. Déterminer le diviseur b .

Correction

4 Relation de congruence

Définition 3: Entiers congrus à n

Soit n un entier naturel ($n \geq 2$), a et b deux entiers relatifs.

On dit que deux entiers a et b sont **congrus modulo n** si, et seulement si, a et b ont le même reste dans la division euclidienne par n .

On note alors $a \equiv b \pmod{n}$ ou $a \equiv b (n)$ ou $a \equiv b [n]$

Exemple 4:

- ① $57 \equiv 15 [7]$ car : $57 = 7 \times 8 + 1$ et $15 = 7 \times 2 + 1$
 $41 \equiv -4 [9]$ car : $41 = 9 \times 4 + 5$ et $-4 = 9 \times (-1) + 5$
- ② Un nombre est congru à son reste modulo n dans la division euclidienne par n .
 $2008 \equiv 8 [10]$ car $2008 = 10 \times 200 + 8$; $17 \equiv 1 (4)$; $75 \equiv 3 [9]$.
- ③ Si $x \equiv 0 [2]$, alors x est pair.
Si $x \equiv 1 [2]$, x est impair.

Propriété 4: Réflexivité, symétrie et transitivité

- $a \equiv 0 [n] \Leftrightarrow a$ est un multiple de n ou n est un diviseur de a .
- La congruence est une relation d'équivalence, c'est-à-dire, pour tous entiers a, b, c , on a :
 - ① $a \equiv a [n]$ (**réflexivité**)
 - ② Si $a \equiv b [n]$, alors $b \equiv a [n]$ (**symétrie**)
 - ③ Si $a \equiv b [n]$ et si $b \equiv c [n]$, alors $a \equiv c [n]$ (**transitivité**)

Preuve 3: Application directe de la définition.

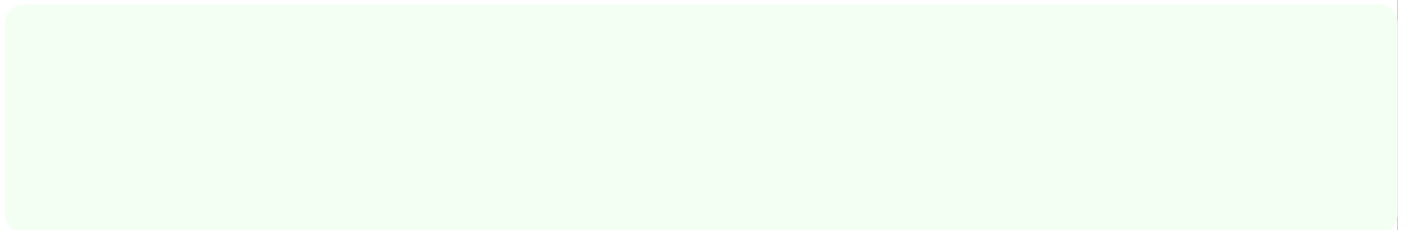
Théorème 5

Soit n un entier naturel ($n \geq 2$), a et b deux entiers relatifs.

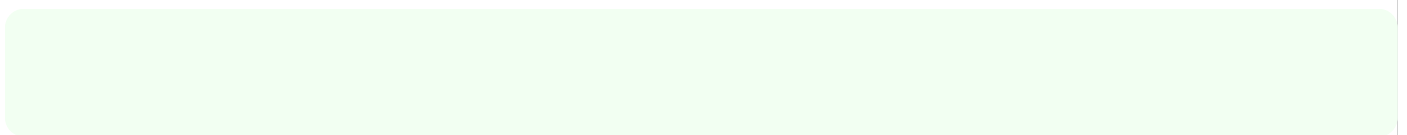
$$a \equiv b [n] \Leftrightarrow a - b \equiv 0 [n]$$

Preuve 4: Comme il s'agit d'une équivalence, il faut démontrer la propriété dans les deux sens.

- Dans le sens direct :



- Réciproquement :



Théorème 6: Compatibilité de la congruence avec l'addition et la multiplication

Soit n un entier naturel ($n \geq 2$) et a, b, c, d des entiers relatifs vérifiant :

$$a \equiv b [n] \quad \text{et} \quad c \equiv d [n].$$

La relation de congruence est compatible :

- ① avec l'addition : $a + c \equiv b + d [n]$
- ② avec la multiplication : $ac \equiv bd [n]$
- ③ conséquence : pour tout entier naturel k , $a^k \equiv b^k [n]$

ATTENTION : $k^a \not\equiv k^b [n]$

Par exemple, $2 \equiv 5 [3]$ et $2^2 \not\equiv 2^5 [3]$

Preuve 5:

① Compatibilité avec l'addition

② Compatibilité avec la multiplication

Méthode 3 (Déterminer un reste dans une division euclidienne):**Exercice**

Déterminer les restes dans la division euclidienne par 7 des nombres :

① 50^{100}

② 100

③ 100^3

④ $50^{100} + 100^{100}$

Correction

Remarque 3: La notion de congruence prend ici tout son intérêt. Par exemple, bien que l'on ne puisse calculer $50^{100} + 100^{100}$, on peut connaître son reste dans la division par 7 de façon simple et rapide.

Méthode 4 (Démontrer qu'un nombre est divisible par un autre nombre):**Exercice**

Montrer que : $\forall n \in \mathbb{N}, \quad 3^{n+3} - 4^{4n+2}$ est divisible par 11.

Correction**Méthode 5 (Construire un tableau de congruence):**

Un tableau de congruence est un tableau permettant de présenter des résultats de manière exhaustive en se référant aux restes possibles dans une division euclidienne.

Exercice

① Déterminer suivant les valeurs de l'entier relatif n , le reste de la division de n^2 par 7.

② En déduire alors les solutions de l'équation $x^2 \equiv 2 [7]$.

Correction