

Arithmétique

Partie 1

Divisibilité

Terminale Mathématiques Expertes

Lycée Pierre Mendès France - Tunis

Table des matières

1	Divisibilité dans \mathbb{Z}	2
2	Division euclidienne	4
3	Congruences dans \mathbb{Z}	6

1 Divisibilité dans \mathbb{Z}

\mathbb{N} est l'ensemble des entiers naturels ; \mathbb{Z} celui des entiers relatifs.

Définition 1

Soient a et b deux entiers relatifs avec $b \neq 0$. On dit que b divise a ou que b est un diviseur de a s'il existe un entier relatif k tel que $a = bk$. On dit aussi que a est un multiple de b .

Remarque

0 est un multiple de n'importe quel entier b ($0 = b \times 0$) mais 0 ne divise aucun nombre.

Exemples

4 divise 24 car $24 = 4 \times 6$; -4 divise aussi 24 car 24 est un multiple de 4 et -4.

Propriété 1

Soient a et b deux entiers relatifs avec $b \neq 0$. On a les implications suivantes.

- Si b divise a alors les multiples de a sont des multiples de b .
- Si b divise a alors les diviseurs de b sont des diviseurs de a .

Remarque

L'ensemble des multiples d'un entier relatif b dans \mathbb{Z} est noté $b\mathbb{Z}$ et l'ensemble des diviseurs de b est noté $D(b)$. D'après la propriété précédente, si $b \neq 0$ divise a alors $a\mathbb{Z} \subset b\mathbb{Z}$ et $D(b) \subset D(a)$.

Exemples

Les multiples de 24 sont aussi des multiples de 3, ce qui s'écrit $24\mathbb{Z} \subset 3\mathbb{Z}$.

Les diviseurs de 12 sont des diviseurs de 24 : $D(12) = \{-12; -6; -4; -3; -2; -1; 1; 2; 3; 4; 6; 12\}$ et $D(24) = \dots\dots\dots$

On observe bien que $D(12) \subset D(24)$.

Propriété 2

Soient a et b deux entiers relatifs avec $b \neq 0$.
 b divise $a \Leftrightarrow -b$ divise $a \Leftrightarrow b$ divise $-a \Leftrightarrow -b$ divise $-a$.

Conséquence

a et $-a$ ont les mêmes diviseurs dans \mathbb{Z} . On restreindra souvent l'étude de la divisibilité à \mathbb{N} .

Propriété 3

Tout entier relatif non nul n possède un nombre fini de diviseurs compris entre $-n$ et n .

Démonstration

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Remarque

Le nombre de multiples d'un entier non nul est infini.

Propriété 4 (*extrêmement importante*)

- Soient a , b et c des entiers relatifs avec $a \neq 0$ et $b \neq 0$. Si a divise b et b divise c , alors a divise c .
- Soient a , b et c des entiers relatifs avec $a \neq 0$. Si a divise b et c , alors a divise toute combinaison linéaire de b et c , c'est-à-dire tout entier de la forme $au + bv$ où u et v sont des entiers relatifs.

Démonstration

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Exemple

Montrer que si a divise deux entiers consécutifs, il est égal à 1 ou -1.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Exercice

Déterminer les entiers relatifs n tels que $2n + 1$ divise $n + 13$.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

2 Division euclidienne

Théorème 1

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

Il **existe** un **unique** couple d'entiers relatifs $(q; r)$ tel que $a = bq + r$ et $0 \leq r < b$.
 q est le quotient et r le reste de la division euclidienne de a par b .

Exemple

Donne la division euclidienne de 114 par 8

.....

Démonstration. Longue et technique. A bien suivre.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Remarques

- Dans la division euclidienne par b , il y a b restes possibles qui sont $\dots\dots$
- Il existe plusieurs écritures de la forme $a = bq + r$ mais une seule correspond à la division euclidienne : celle vérifiant $0 \leq r < b$. Par exemple, $56 = 17 \times 3 + 5 = 17 \times 2 + 22$ mais cette dernière égalité n'est pas une division **euclidienne** car $22 > 17$.

Propriété 5

Soit b un entier supérieur ou égal à 2.

Tout entier relatif s'écrit sous l'une des formes $bq, bq + 1, bq + 2, \dots, bq + (b - 1)$, où q est un entier relatif.

Démonstration

Il s'agit d'une conséquence immédiate du théorème précédent. Pour info, une telle propriété, qui découle immédiatement d'un théorème, est appelé un lemme.

Exemple

n désignant un entier, montrer que $n^2 + 1$ n'est jamais divisible par 3.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Exercice

Montrer que le produit de trois entiers consécutifs est divisible par 3.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

3 Congruences dans \mathbb{Z}

Préambule : Jouons à « la course à 20 ».

Définition 2

Soient a et b deux entiers relatifs et n un entier naturel non nul.

On dit que a **est congru à** b modulo n , et on note $a \equiv b[n]$ ou $a \equiv b(\text{mod } n)$, lorsque $a - b$ est un multiple de n .

Exemples

- $15 - 7 = 8 = 2 \times 4$ dont $15 \equiv 7[2]$ et $15 \equiv 7[4]$.
- $-5 \equiv -1[4]$.

Remarque

Par définition, on remarque que $a \equiv b[n] \Leftrightarrow b \equiv a[n]$. On dit aussi que a et b sont congrus modulo n .

Propriété 6 (*Propriété clé*)

Soient a et b deux entiers relatifs et n un entier naturel non nul.

$a \equiv b[n]$ si et seulement si a et b ont le même reste dans la division euclidienne par n .

Démonstration

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Exemple

$11 = 4 \times 2 + 3$ et $7 = 4 \times 1 + 3$ avec $0 \leq 3 < 4$, donc 11 et 7 sont congrus modulo 4.

Propriété 7 (*Calculs avec les congruences*)

Soient a, b, c et d des entiers relatifs et n un entier naturel non nul.

1. Si $a \equiv b[n]$ alors $a + c \equiv b + c[n]$
2. Si $a \equiv b[n]$ et $c \equiv d[n]$ alors $a + c \equiv b + d[n]$.
On dit que les congruences sont compatibles avec l'addition (1 et 2).
3. Si $a \equiv b[n]$ alors $ac \equiv bc[n]$
4. Si $a \equiv b[n]$ et $c \equiv d[n]$ alors $ac \equiv bd[n]$.
On dit que les congruences sont compatibles avec la multiplication (3 et 4).
5. Si $a \equiv b[n]$ alors, pour tout entier naturel non nul p , $a^p \equiv b^p[n]$.

Remarque

Les réciproques des propriétés 3, 4 et 5 sont fausses. Par exemple, la réciproque de la propriété 3 est fausse (les congruences ne sont pas compatibles avec la division). En voici un exemple : $5 \times 4 \equiv 5 \times 6[10]$ mais 4 et 6 ne sont pas congrus modulo 10.

Exercices types

Exercice 1.

Résoudre les équations suivantes dans \mathbb{Z} .

1. $x + 3 \equiv 2[7]$

2. $3x \equiv 2[5]$

3. $x^2 \equiv 0[4]$

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Exercice 2. Montrer une divisibilité à l'aide des congruences.

1. Montrer que pour tout entier naturel n non nul, $2^{3n} - 1$ est un multiple de 7.
2. Déterminer les valeurs de l'entier naturel n pour lesquelles $n^2 - 3n + 6$ est divisible par 4.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Exercice 3. Montrer une divisibilité à l'aide des congruences.

Déterminer le reste de la division euclidienne de 11^{2021} par 3.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....