Chapitre 4 : Divisibilité et congruences dans $\mathbb{Z}$

Notations : • On note $\mathbb{N}$ l'ensemble des nombres entiers naturels. $\mathbb{N} = \{0; 1; 2; \dots\}$
• On note $\mathbb{N}^*$ l'ensemble des nombres entiers naturels non nuls.
• On note $\mathbb{Z}$ l'ensemble des nombres entiers relatifs $\mathbb{Z} = \{\dots; -2; -1; 0; 1; 2; \dots\}$
• On note $\mathbb{Z}^*$ l'ensemble des nombres entiers relatifs non nuls.

I. Divisibilité dans $\mathbb{Z}$

A/ Définition

Définition : Soit $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$.
On dit que b divise a s'il existe $q \in \mathbb{Z}$ tel que $a = bq$.

Remarque : • Dans le cas où b divise a, on dit aussi que :
- b est un diviseur de a
- a est divisible par b
- a est un multiple de b

• Si $b \in \mathbb{N}^*$, alors on a :
b divise a ssi le reste de la division euclidienne de a par b est nul.

B/ Ensemble des diviseurs d'un entier

Pour tout $a \in \mathbb{Z}$, on note $D(a)$ l'ensemble des diviseurs de a. Ainsi $b \in D(a)$ se lit "b divise a".

Propriété : Soient a, b et c trois entiers relatifs non nuls.
1. Les éléments de $D(a)$ sont compris entre $-a$ et a et par conséquent $D(a)$ est un ensemble fini.
2. $b \in D(a) \iff -b \in D(a) \iff b \in D(-a) \iff -b \in D(-a)$
3. Si $a \in D(b)$ et $b \in D(c)$ alors $a \in D(c)$
4. Si $a \in D(b)$ et $a \in D(c)$ alors $a \in D(bu + cv)$ pour tout couple $(u; v) \in \mathbb{Z}^2$.

Remarque : Un nombre de la forme $bu + cv$ avec $(u; v) \in \mathbb{Z}^2$ s'appelle une combinaison linéaire de b et de c.

Exemples : $D(10) = \{-10 ; -5 ; -2 ; -1 ; 1 ; 2 ; 5 ; 10\}$

1. Les éléments de $D(10)$ sont bien compris entre -10 et 10 et $D(10)$ est fini.
2. On a par exemple $2 \in D(10)$; $-2 \in D(10)$; $2 \in D(-10)$; $-2 \in D(-10)$
3. 5 divise 10 et 10 divise 30 donc 5 divise 30
4. 3 divise 12 et 3 divise 15 donc 3 divise tout nombre de la forme $12u + 15v$ où $(u;v) \in \mathbb{Z}^2$.

Remarque : la propriété justifie qu'on ramène la recherche des diviseurs d'un entier à la recherche des diviseurs positifs de sa valeur absolue (on cherche donc les diviseurs positifs d'un entier positif).

II. Division euclidienne

Théorème : Division euclidienne d'un entier naturel par un entier naturel non nul
Pour tous $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$, il existe un unique couple $(q ; r)$ avec $q \in \mathbb{N}$ et $r \in \mathbb{N}$ tels que : $a = bq + r$ $(0 \leq r < b)$.

Vocabulaire : a, b, q et r sont respectivement le dividende, le diviseur, le quotient et le reste de la division euclidienne de a par b.

Exemple : Dans la division euclidienne de 524 par 17,
$524 = 30 \times 17 + 14$ 524 est le dividende, 17 est le diviseur, 30 est le quotient et 14 est le reste.

Illustration graphique :

Théorème : Division euclidienne d'un entier relatif par un entier naturel non nul
Pour tous $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, il existe un unique couple $(q ; r)$ avec $q \in \mathbb{Z}$ et $r \in \mathbb{N}$ tels que : $a = bq + r$ $(0 \leq r < b)$.

Exemple : Donner le quotient et le reste de la division euclidienne de -524 par 17.

$524 = 30 \times 17 + 14$ donc $-524 = -31 \times 17 - 17 + (-14)$

le reste ne peut pas être strictement négatif donc il ne peut pas valoir -14.

On écrit $-524 = -30 \times 17 - 17 + 17 - 14$

$= -31 \times 17 + 3$ et $0 \leq 3 < 17$

le reste de la division euclidienne de -524 par 17 est 3 et le quotient est -31.

III - Congruences dans $\mathbb{Z}$

Définition et notation : Congruence dans $\mathbb{Z}$

Soit $(a;b) \in \mathbb{Z}^2$ et $n \in \mathbb{N}^*$

On dit que a est congru à b modulo n si n divise $a-b$.

Dans ce cas on note $a \equiv b\ [n]$.

Remarques : • $\forall a \in \mathbb{Z}$, $\forall n \in \mathbb{N}^*$, $a \equiv a\ [n]$ (car $a-a=0$ est divisible par n).

• $a \equiv b\ [n] \iff b \equiv a\ [n]$ et on peut donc dire dans ce cas que a et b sont congrus modulo n.

Conséquence :

① Justifier que : $a \equiv r\ [n]$ où r est le reste de la division euclidienne de a par n.

② $\forall a \in \mathbb{Z}$, a est congru modulo n à l'une des valeurs suivantes : $0; 1; \dots; n-1$

③ $\forall a \in \mathbb{Z}$, a est divisible par $n \iff a \equiv 0\ [n]$

Propriétés des congruences : • Soient a, b, c et d quatre nombres relatifs et n un entier naturel non nul.

• Si $a \equiv b\ [n]$ et $b \equiv c\ [n]$ alors $a \equiv c\ [n]$

• Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$ alors $a + c \equiv b + d\ [n]$

• Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$ alors $a \times c \equiv b \times d\ [n]$

• Soit $p \in \mathbb{N}^*$. Si $a \equiv b\ [n]$ alors $a^p \equiv b^p\ [n]$

Exercice d'application : Montrer en utilisant un tableau de congruence que pour tout entier relatif n, $n(n+1)(2n+1)$ est divisible par 3.

$n \equiv \ldots [3]$	0	1	2
$n+1 \equiv \ldots [3]$	1	2	0
$2n+1 \equiv \ldots [3]$	1	0	2
$n(n+1)(2n+1) \equiv \ldots [3]$	0	0	0

Donc $\forall n \in \mathbb{Z}$, $n(n+1)(2n+1) \equiv 0 \ [3]$.
Donc $n(n+1)(2n+1)$ est divisible par 3.

Définition : Inverse modulo n
Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. On dit que a est inversible modulo n lorsqu'il existe un entier b tel que le produit $a \times b \equiv 1 \ [n]$.

Exemple : Justifier que 8 est inversible modulo 3.
On a $8 \times 2 \equiv 1 \ [3]$ donc 2 est un inverse de 8 modulo 3.

Exercice d'application :
① Montrer que 3 est inversible modulo 5.
② Montrer que 4 n'a pas d'inverse modulo 6.

① On a $3 \times 2 \equiv 1 \ [5]$
Donc 2 est un inverse de 3 modulo 5.

② On cherche $b \in \mathbb{Z}$ tel que $4 \times b \equiv 1 \ [6]$.

$b \equiv \ldots [6]$	0	1	2	3	4	5
$4b \equiv \ldots [6]$	0	4	2	0	4	2

D'après le tableau, il n'existe pas d'entier b tel que $4 \times b \equiv 1 \ [6]$.
Donc 4 n'a pas d'inverse modulo 6.

• Exercices d'application

Exercice 1 : Résolution d'équations dans $\mathbb{Z}$ ou $\mathbb{N}$
Déterminer les entiers naturels a et b vérifiant $a^2 - b^2 = 35$.

Exercice 2 : Déterminer tous les entiers n tels que $(2n+7) / (n-3)$

→ Exercice 1

$a^2 - b^2 = 35 \iff (a-b)(a+b) = 35$

Donc $a-b$ et $a+b$ sont des diviseurs de 35.

Or $a \in \mathbb{N}$ et $b \in \mathbb{N}$ donc $a+b \in \mathbb{N}$. $a+b$ est un diviseur positif de 35.

Donc $a-b$ est aussi un diviseur positif de 35.

On résout dans $\mathbb{N}^*$

$\begin{cases} a+b = 35 \\ a-b = 1 \end{cases} \iff \begin{cases} 2a = 36 \\ a-b = 1 \end{cases} \iff \begin{cases} a = 18 \\ b = a-1 \end{cases} \iff \begin{cases} a = 18 \\ b = 17 \end{cases}$

$\begin{cases} a+b = 7 \\ a-b = 5 \end{cases} \iff \begin{cases} 2a = 12 \\ b = 5-a \end{cases} \iff \begin{cases} a = 6 \\ b = 1 \end{cases}$

Les diviseurs positifs de 35 sont 1; 5; 7 et 35.

On vérifie que les couples $(18;17)$ et $(6;1)$ vérifient l'équation.

→ Exercice 2

Par hypothèse, $(2n+7) / (n-3)$ $\times 2$

$(2n+7) / (2n+7)$ $\times 1$

Donc $(2n+7) / (2n+7) - 2(n-3)$ par combinaison linéaire.

Ainsi $(2n+7) / 13$.

Les diviseurs de 13 sont $-13; -1; 1$ et 13.

$2n+7 = -13 \iff 2n = -20 \iff n = -10$

$2n+7 = -1 \iff 2n = -8 \iff n = -4$

$2n+7 = 1 \iff 2n = -6 \iff n = -3$

$2n+7 = 13 \iff 2n = 6 \iff n = 3$

Les valeurs de n possibles sont $-10; -4; -3$ et 3.

Réciproquement, on vérifie si ces valeurs vérifient la condition de l'énoncé.

$n = -10$	$2\times(-10)+7 = -13$:	$-10-3 = -13$	$-13/-13$
$n = -4$	$2\times(-4)+7 = -1$:	$-4-3 = -7$	$-1/-7$
$n = -3$	$2\times(-3)+7 = 1$:	$-3-3 = -6$	$1/-6$
$n = 3$	$2\times 3+7 = 13$:	$3-3 = 0$	$13/0$

Les solutions sont $-10; -4; -3$ et 3.