Option Maths expertes	**Chapitre II (Arithmétique) :** *Divisibilité dans ℤ, division euclidienne, Congruences*	2022/2023

I) Divisibilité dans ℤ :

La notion de diviseur d'un entier a déjà été rencontrée au collège (classe de troisième : pour le calcul du pgcd de deux entiers naturels)

La méthode consistant à donner les listes des diviseurs de deux entiers naturels pour calculer leur pgcd fonctionne bien quand les nombres sont petits, sinon elle est rapidement fastidieuse.

On lui préférera l'algorithme des différences successives ou celui d'Euclide avec les divisions successives.

Cependant, on peut bien sûr écrire un algorithme de recherche de la liste des diviseurs d'un entier donné et ensuite le programmer sur un ordinateur ou une calculatrice

1) Définition et vocabulaire :

Soient a et b, deux entiers relatifs (c'est-à-dire a $\in\mathbb{Z}$ et b$\in\mathbb{Z}$)
On dit que **b divise a** (notation : b|a) si il existe ……

On dit que b est …….. ou que a est …… de b.

Remarques :

* Utilisation de la notation ∃ qui signifie « Il existe ». Par exemple : ∃ k $\in\mathbb{Z}$
* Il y a même équivalence :

$$b|a \Leftrightarrow \exists\, k \in \mathbb{Z},\ a = b\times k$$

* 1 et -1 divisent tout entier
* 0 ne divise que 0

Pour démontrer ce dernier résultat, on peut mettre en place *un raisonnement par l'absurde :*

(Pour l'utilisation d'un raisonnement par l'absurde pour démontrer un résultat « classique », voir la preuve de l'irrationalité de $\sqrt{2}$)

2) Propriétés :

Soient a,b et c trois entiers :

a) Si a est un multiple de b et si $a \neq 0$, alors $|a| \geq |b|$
b) $a \mid b \Leftrightarrow -a \mid b \Leftrightarrow a \mid -b \Leftrightarrow -a \mid -b$
c) Si a | b et b | c , alors a | c *(Transitivité de la relation de divisibilité)*
d) Si a | b et b | a, alors a = b ou a = - b (avec a et b ≠ 0)
e) Si a | b et a | c, alors $a \mid \lambda b + \mu c$, où $(\lambda , \mu) \in \mathbb{Z}^2$

Remarque : on dit que $\lambda b + \mu c$ est une combinaison linéaire de b et c à coefficients entiers
On peut donc reformuler la propriété e) : « Si a divise b et c , alors il divise toute combinaison linéaire à coefficients entiers de b et c »
Cette propriété va permettre la résolution de bon nombre de questions de divisibilité.
Démonstrations :

3) Exemples d'applications des propriétés et de la définition :

a) Déterminer les entiers relatifs n tels que $5|n+3$:

Remarque : Si $n \in \mathbb{N}$, alors $k \in \mathbb{N}^*$ (ce qui va restreindre le nombre de solutions dans certains cas)

b) Déterminer les entiers n tels que $2n + 3 \mid 5$:

c) Déterminer les entiers n tels que $2n + 1 \mid n - 3$:

d) Déterminer tous les couples d'entiers naturels (x;y) tels que $x^2 - y^2 = 9$

Remarque :

Ce type d'équation où les inconnues sont des entiers est appelée **Equation diophantienne**

$$x^2 - y^2 = 9 \Leftrightarrow (x + y)(x - y) = 9$$

Remarque importante :

$x \in \mathbb{N}$ et $y \in \mathbb{N}$, d'où : $x + y \geq x - y$ (ce qui va permettre de limiter le nombre de cas à étudier)

II) Division euclidienne :

1) Dans $\mathbb{N}$:

Soient $(a;b) \in \mathbb{N} \times \mathbb{N}^*$, alors : il existe un **unique** couple d'entiers naturels (q;r) tel que :

…….

- a : dividende - b : diviseur - q : quotient - r : reste

Remarques :

a) Il y a existence **et** unicité du couple (q;r)

b) $b|a \Leftrightarrow r = 0$

Démonstration :

Pour effectuer cette démonstration, nous avons besoin de la fonction partie entière.

Notation : E(x) (plus tellement utilisée) , on lui préfère [x]

Avec la propriété suivante : Pour tout $x \in \mathbb{R}$, $[x] \leq x < [x] + 1$

- Existence :

- Unicité :

2) Dans $\mathbb{Z}$:

On peut étendre le résultat précédent dans $\mathbb{Z}$:

Théorème :

Soient $(a;b) \in \mathbb{Z}\times\mathbb{Z}^*$, alors il existe un unique couple $(q;r)$ avec $q \in \mathbb{Z}$ et $r \in \mathbb{N}$ tel que :

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

Exemples : a) Division euclidienne de -13 par -3

$-13 = 5\times(-3) + 2$ avec $0 \leq 2 < |-3|$

Le couple (5;2) est le seul vérifiant les conditions précédentes

b) Changement de base :

On considère le nombre 3259 en base 10.

Ecrire ce nombre en base 8.

Conséquence importante :

Soit $b \in \mathbb{N}^*$, si on considère la division euclidienne d'un entier par b, les seuls restes possibles sont :

$$0;1;2\ ;....;b-1$$

Explicitement : Soient $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$, alors il existe $q \in \mathbb{Z}$, tel que :

$$a = bq \text{ ou } a = bq + 1 \text{ ou } a = bq + 2 \text{ ou } \ldots \text{ ou } a = bq + (b - 1)$$

Exemple :

Tout entier relatif s'écrit $3k$ ou $3k + 1$ ou $3k + 2$ (car $0\ ;1;2$ sont les seuls restes possibles dans la division euclidienne par 3)

Remarque : Cette conséquence sera très utile pour mener des raisonnements par disjonction des cas (voir les exercices)

Application : Montrer que si $n \in \mathbb{N}$, alors $n(n+5)(n+7)$ est toujours un multiple de 3

III) Congruences :

1) Définition :

Soient a,b deux entiers naturels, n un entier naturel non nul.
On dit que **a est congru à b modulo n** si ……

Notations : $a \equiv b[n]$ ou $a \equiv b(n)$ ou $a \equiv b \bmod n$

Exemples : $37 = 9 \times 4 + \mathbf{1}$
$64 = 9 \times 7 + \mathbf{1}$

Donc : $64 \equiv 37\ [9]$

2) Congruences et restes :

Propriété :
Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Si on note r = reste de la division euclidienne de a par n, alors :
……..

Démonstration :

Plus précisément : Soit $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$, alors a est congru modulo n à un unique r tel que :
$0 \leq r < n$

Exemples : $45 \equiv 29[4]$ car $45 = 4 \times 11 + \mathbf{1}$ et $29 = 4 \times 7 + \mathbf{1}$
Mais également : $45 \equiv 1[4]$ et $29 \equiv 1[4]$ avec $0 \leq 1 < 4$

Cas particuliers :
* Soit n un nombre entier naturel pair , alors $n \equiv 0[2]$
* Soit n un nombre entier naturel impair, alors $n \equiv 1[2]$

Preuve :

3) Théorème :

Soient a et b deux entiers relatifs et $n \in \mathbb{N}^*$, $a \equiv b\ [n] \Leftrightarrow n \mid a - b$

Cas particulier : $a \equiv 0\ [n] \Leftrightarrow n \mid a$

Démonstration :

Exemple :

$x \equiv 11[5] \Leftrightarrow \exists\ k \in \mathbb{Z},\ x = 5k + 11$

4) Propriétés :

Soient x,y,z,t des entiers, n et m, deux entiers naturels non-nuls :

a) $x \equiv x[n]$ (La relation de congruence est **réflexive**)

b) Si $x \equiv y[n]$, alors $y \equiv x[n]$ (La relation de congruence est **symétrique**)

c) Si $x \equiv y[n]$ et $y \equiv z[n]$, alors $x \equiv z[n]$ (La relation de congruence est **transitive**)

Compatibilité avec les opérations :

d) Si $x \equiv y\ [n]$ et $z \equiv t\ [n]$, alors $x + z \equiv y + t\ [n]$

e) Si $x \equiv y\ [n]$ et $z \equiv t\ [n]$, alors $xz \equiv yt\ [n]$

f) Si $x \equiv y\ [n]$ et $p \in \mathbb{N}$, alors $x^p \equiv y^p\ [n]$

Remarque importante : *La congruence n'est pas compatible avec la division*

En effet , par exemple : $18 \equiv 6\ [12]$ car $12 \mid 18 - 6 = 12$

C'est-à-dire $6 \times 3 \equiv 6 \times 1\ [12]$, mais 3 n'est pas congru à 1 modulo 12

Démonstration des propriétés :

Applications :

1) Critères de divisibilité (voir exercices)

2) Exercice : *Déterminer les entiers naturels n tels que $n^3 + 2n^2 - 1$ soit divisible par 5*

Rappel : $x \in \mathbb{N}$ est divisible par $5 \Leftrightarrow x \equiv 0[5]$

On peut dresser un tableau de congruences modulo 5 : (on reconstitue progressivement l'expression)

Quand on raisonne modulo 5, il n'y a que 5 restes possibles dans la division euclidienne : 0 ou 1 ou 2 ou 3 ou 4.
Ensuite, on remplit le tableau en utilisant les propriétés des congruences.

$n \equiv$	0	1	2	3	4
$n^2 \equiv$	0	1	4	4	1
$n^3 \equiv$	0	1	3	2	4
$n^3 + 2n^2 \equiv$	0	3	1	0	1
$n^3 + 2n^2 - 1$	4	2	0	4	0

Dans la dernière ligne du tableau, il n'y a que deux 0.
Les solutions sont donc les $n \equiv 2$ [5] et les $n \equiv 4$ [5]
C'est-à-dire : $n = 5k + 2$, avec $k \in \mathbb{Z}$ ou $n = 5k + 4$ avec $k \in \mathbb{Z}$

$S = \{ 5k + 2 ; 5k + 4 , k \in \mathbb{Z}\}$

IV) Quelques brefs rappels sur les nombres premiers :

1) Définition :
Soit $n \in \mathbb{N}^* \setminus \{1\}$ est dit **premier** s'il n'admet comme diviseur que 1 et lui-même.
Exemples : 2 est le seul nombre premier pair. Les suivants sont : 3,5,7,11,etc...
(Les tests de primalité seront vus dans le prochain chapitre d'arithmétique)

2) PGCD de deux entiers naturels :
Soient a et b, deux entiers naturels. On note D(a;b) : ensemble des diviseurs communs à a et à b
PGCD(a;b) = le plus grand élément de D(a;b)
Pour le calculer, on peut mettre en œuvre des algorithmes : algorithme des différences, et surtout algorithme d'Euclide.
Dans ce dernier, on utilise le fait que PGCD(a;b) = PGCD(b;r) où r est le reste dans la division euclidienne de a par b. PGCD(a;b) = dernier reste non-nul des divisions successives.

(preuve : dans le prochain chapitre d'arithmétique)

Programmes du la calculatrice (vus en TD)

3) Nombres premiers entre eux :

Soient a et b, deux entiers naturels :

a et b sont **premiers entre eux** ⇔ a et b n'ont que 1 comme diviseur commun

⇔ PGCD(a;b) = 1

Exemple : 21 et 10 ne sont pas des nombres premiers. En effet, par exemple 3|21 et 5|10

MAIS, PGCD(21;10) = 1 : ils sont donc premiers entre eux.