Chapitre 1 : Multiple, division euclidienne, congruence

I- Diviseurs et multiples

1) Définition

Définition : Soient a et b deux nombres entiers relatifs non nuls .
a est **divisible par b** si et seulement si il existe un entier relatif k tel que : a = bk .
On dit alors que b est un **diviseur de a** ou que a est un **multiple de** b et on note :
a | b qui signifie a divise b

Exemple : 45 est un multiple de -9 ou -9 est un diviseur de 45 que l'on note -9|45
A noter que :

- 0 est un multiple de tout entier a car
- 1 divise tout entier a car
- Si a est un multiple de b alors $|a| \geq |b|$
- Si a | b et b | a alors a = b ou a = - b

Méthode : Utiliser la divisibilité pour résoudre un problème

Enoncé : Déterminer tous les entiers naturels x et y tels que $x^2 - 2xy = 15$

On factorise par x : $x^2 - 2xy = 15 \Leftrightarrow x(x-2y) = 15$

On remarque donc que x et $x-2y$ sont des **diviseurs associés** de 15

De plus, comme x et y sont des positifs, on a x ≥ x - 2y d'où 15 = 1×15 = 3×5 il faut résoudre :

$$\begin{cases} x = 15 \\ x-2y = 1 \end{cases} \text{ ou } \begin{cases} x = 5 \\ x-2y = 3 \end{cases} \Leftrightarrow \begin{cases} x = 15 \\ y = 7 \end{cases} \text{ ou } \begin{cases} x = 5 \\ y = 1 \end{cases}$$

Les couples solutions sont donc $(x;y) = (15;7)$ et $(x;y) = (5;1)$

2) Opération sur les multiples

a , b , c désignent des entiers relatifs non nuls

Si a divise b et c alors a divise toute combinaison linéaire de b et c en d'autres termes :

a | b et a | c ⇒ $\forall (\alpha, \beta) \in \mathbb{Z}^2$, a divise $\alpha b + \beta c$

Démonstration :

On sait que a divise b et c donc il existe deux entiers k et k' tels que b = ka et c = k'a d'où

$\alpha b + \beta c = (\alpha k + \beta k')a$ et donc a | $\alpha b + \beta c$

Méthode

Enoncé 1 : Soit k un entier naturel. On pose a = $9k+2$ et b = $12k+1$.
Justifier que les seuls diviseurs positifs de a et b ne peuvent être que 1 ou 5

Soit d un diviseur positif de a et b . d divise donc toute combinaison linéaire de a et de b . On cherche donc une combinaison qui élimine k. Ainsi d divise $4a-3b$ c'est à dire d divise $4(9k+2)-3(12k+1)$ = 5.

Comme 5 ne possède que deux diviseurs positifs 1 et 5, nous avons répondu à la question

Enoncé 2 : Déterminer toutes les valeurs de l'entier relatif n pour lesquelles $n-3$ divise 2n + 5

$n-3$ | 2n + 5 et $n-3$ | $n-3$ donc $n-3$ divise toute combinaison de 2n + 5 et $n-3$. On en cherche donc une qui élimine n : $n-3$ divise 2n+5 – 2(n – 3) = 11 d'où comme 11 a pour diviseur -11 , -1 , 1 , 11 on peut dresser le tableau suivant :

n-3	-11	-1	1	11
n	-8	2	4	14

Il faut alors penser à vérifier que pour n = –8 , 2 , 4 et 14 , on a bien n – 3 qui divise 2n+5 car la propriété utilisée n'est pas réciproque :

n	-8	2	4	14
n-3	-11	-1	1	11
2n+5	-11	9	13	33

3) Règles de divisibilité

En observant le nombre

- un entier est divisible par 2 s'il se termine par 0 , 2 , 4 , 6 ou 8
- un entier est divisible par 5 s'il se termine par 0 ou 5
- un entier est divisible par 10 s'il se termine par 0
- un entier est divisible par 25 s'il se termine par 00 , 25 , 50 , 75
- un entier est divisible par 4 si le nombre formé par ses deux derniers chiffres est divisible par 4 (ex : 1936)

Par somme des chiffres

Un entier est divisible par 3 (ou resp. 9) si la somme de ses chiffres est divisible par 3 (ou resp. 9)

Par différence des chiffres

Un entier est divisible par 11 si la différence entre la somme de ses chiffres de rangs pairs et la somme des chiffres de rangs impairs est divisible par 11 :

- 3454 est divisible par 11 car $(4+4)-(5+3)=0$ divisible par 11
- 15763 est divisible par 11 car $(3+7+1)-(6+5)=0$ divisible par 11

4) Algorithme : liste des diviseurs

L'algorithme ci-dessous permet de déterminer les diviseurs d'un entier naturel. Il est basé sur la fait que lorsque l'on trouve un diviseur, on en a un autre.

Soit a et b deux diviseurs associés d'un entier n avec a ≤ b . On a donc ab = n et :

$a \leq b$	$a \leq b$
$a^2 \leq ab$	$ab \leq b^2$
$a^2 \leq n$	$n \leq b^2$
$a \leq \sqrt{n}$	$\sqrt{n} \leq b$

On obtient ainsi $a \leq \sqrt{n} \leq b$ ce qui justifie le test d'arrêt de cet algorithme

Algorithme de recherche des diviseurs positifs d'un entier naturel n donné

```
    i ← 1
    Tant que i ≤ √n
          Si le reste de la division euclidienne de n par i est nul alors
                    afficher i
                    Si n/i est différent de i alors
                           afficher n/i
          i ← i+1
    Fin du si
Fin tant que
```

II- Division euclidienne

1) Rappel

Propriété : Soit a $\in \mathbb{N}$ et b $\in \mathbb{N}^*$.

Il **existe** un **unique** couple (q ; r) d'entiers relatifs tels que a = bq + r avec $0 \leq r < b$

Effectuer la division euclidienne de a par b , c'est trouver le couple (q;r) tel que a = bq + r avec $0 \leq r < b$

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

Exemples:

- a = 356 ; b = 17 : $356 = 17 \times 20 + 16$ et $0 \leq 16 < 17$ donc q = 20 et r = 16
- a = –356 ; b = 17 : $-356 = 17 \times (-20) - 16$ mais $-16 < 0$

  $-356 = 17 \times (-21) + 1$ et $0 \leq 1 < 17$ donc q = –21 et r = 1

2) Et en algorithmique

On peut donner cet algorithme qui calcule le quotient et le reste de la division de a par b par la méthode des soustractions successives :

```
c ← 0
Si a ≥ 0 alors :
    Tant que a > b :
        c ← c+1
        a ← a – b
    Fin du TQ
Sinon
    Tant que a < b :
        c ← c+1
        a ← a + b
    Fin TQ
Afficher c ( le quotient )
Afficher a  ( le reste )
```

3) Une conséquence : l'écriture d'un entier relatif quelconque

Les restes possibles dans la division euclidienne de a par b sont 0 , 1 , 2 , ... , b – 1.
Donc tout entier relatif a peut s'écrire bk ou bk + 1 ou bk + 2 ..... ou bk + b –1 avec k $\in \mathbb{Z}$.

Cette règle est très utile quand on veut **raisonner par disjonction de cas**. Par exemple, tout entier relatif a peut s'écrire 2k ou 2k + 1 avec k $\in \mathbb{Z}$ car les restes possibles dans la division par 2 sont 0 ou 1 .

De même, tout entier relatif a peut s'écrire 5k , 5k+1, 5k+2, 5k+3 , 5k+4 avec k $\in \mathbb{Z}$ car les restes possibles dans la division par 5 sont 0,1,2,3,4.

Méthode Déterminer par **disjonction de cas** l'ensemble des entiers naturels tels que n^2+n soit divisible par 5

On est dans la division par 5 or d'après ce qui précède un entier peut s'écrire 5k , 5k+1 , 5k+2 , 5k+3 , 5k+4.

On étudie donc chaque cas :

n = 5k	n = 5k + 1	n = 5k + 2	n = 5k + 3	n = 5k + 4
$n^2+n=25k^2+5k$	$n^2+n=\ldots=5\mathrm{K}+2$	$n^2+n=\ldots=5\mathrm{K}+6$	$n^2+n=\ldots=5\mathrm{K}+11$	$n^2+n=\ldots=5\mathrm{K}+20$
$n^2+n=5(5k^2+k)$				
$n^2+n=5\mathrm{K}$				

On constate donc que n doit être multiple de 5 ou avoir pour reste 4 dans la division par 5 pour que n^2+n soit multiple de 5

III- Congruence dans $\mathbb{Z}$

Soit n un entier naturel supérieur ou égal à 2

a) Une propriété fondamentale

Propriété Deux entiers relatifs a et b ont le même reste dans la division euclidienne par n si et seulement si $a - b$ est un multiple de n

Démonstration :

Soit $a = nq + r$ et $b = nq' + r'$

- Si a et b ont le même reste dans la division euclidienne par n alors $r = r'$.
  On a alors $a - b = nq - nq' = n(q - q')$ d'où $a - b$ est un multiple de n
- réciproquement, si $a - b$ est un multiple de n alors il existe un entier relatif k tel que $a - b = kn$
  c'est à dire $a = kn + b$. Or $b = nq' + r'$ donc $a = n(k + q') + r'$ avec $0 \leq r' < n$. Ainsi, r' est le reste de la division euclidienne de a par n donc $r = r'$

b) Congruences

Définition : Dire que deux entiers relatifs a et b sont **congrus modulo n** signifie que a et b ont même reste dans la division euclidienne par n

« a et b sont congrus modulo n » s'écrit $a \equiv b\ [n]$ ou $a \equiv b\ (n)$ ou $a \equiv b \pmod{n}$

Remarques

On déduit immédiatement de la définition que :

- $a \equiv b\ (n) \Leftrightarrow b \equiv a\ (n)$
- si $a \equiv b\ (n)$ et $b \equiv c\ (n)$ alors $a \equiv c\ (n)$
- si r est le reste de la division euclidienne de a par n alors $a \equiv r\ (n)$

Exemples:

- $-37 \equiv 18\ (11)$ car $18 - (-37) = 55 = 5 \times 11$
- L'écriture $n \equiv 1\ (5)$ signifie $n = 1 + 5k$ avec $k \in \mathbb{Z}$.

c) Compatibilité avec les opérations

a , b c et d désignent des entiers relatifs

Propriétés : Si $a \equiv b\ (n)$ et $c \equiv d\ (n)$ alors

(1) **Addition :** $a + c \equiv b + d\ (n)$

(2) **Soustraction :** $a - c \equiv b - d\ (n)$

(3) **Multiplication :** $ac \equiv bd\ (n)$

(4) pour tout entier naturel p, $a^p \equiv b^p\ (n)$

En résumé, on peut additionner, soustraire, multiplier membre à membre des congruences de même modulo

Démontrer ces propriétés à titre d'exercice

d) Quelques exemples

Méthode Déterminer le reste du nombre suivant dans la division par 7 : $50^{100}+100^{100}$ (on pourra considérer 100^3)

On raisonne modulo 7 :

1) 50^{100} $50 \equiv 1$ (7) car $50=7\times7+1$ donc d'après la compatibilité avec les puissances, $50^{100} \equiv 1^{100} \equiv 1(7)$

2) 100^{100} $100 \equiv 2(7)$ car $100=7\times14+2$ donc d'après la compatibilité avec les puissances : $100^{100} \equiv 2^{100}(7)$

or difficile de déterminer le reste de 2^{100} par 7 . On utilise alors $100^3 \equiv 2^3 \equiv 1(7)$. On a alors :

$$100^{100}=100^{3\times33+1} = (100^3)^{33}\times100^1 \equiv 1^{33}\times2(7) \equiv 2\ (7)$$

3) D'après la compatibilité avec l'addition, on obtient donc : $50^{100}+100^{100} \equiv 1+2\ (7) \equiv 3\ (7)$

Le reste est 3

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

On raisonne modulo 11 :

$3^{n+3}=3^n\times3^3=3^n\times27$ or $27 \equiv 5$ (11) donc $3^{n+3} \equiv 5\times3^n$ (11)

$4^{4n+2}=(4^4)^n\times4^2$ Or $4^2=16 \equiv 5$ (11) donc $(4^2)^2 = 4^4 \equiv 5^2 \equiv 3$ (11) donc

$4^{4n+2} \equiv 3^n\times5$ (11)

On obtient donc par addition des congruences : $3^{n+3}-4^{4n+2} \equiv 0$ (11) ce qui signifie $3^{n+3}-4^{4n+2}$ divisible par 11