Chapitre 1 : Divisibilité dans $\mathbb{Z}$

I- Diviseurs et multiples

1) Définition

Définition : Soient a et b deux nombres entiers relatifs non nuls . On dit que a est divisible par b 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 $-9|45$

2) Propriétés

a , b , c désignent des entiers relatifs non nuls

1) Si $a|b$ et $b|c$ alors $a|c$

2) $a|b \Leftrightarrow \forall k \in \mathbb{Z}^*$, $ka|kb$

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

$$a|b \text{ et } a|c \Rightarrow \forall (k,k') \in \mathbb{Z}^2 \text{ , a divise } kb + k'c$$

Démonstrations :

Exemples :

1) Comment choisir l'entier relatif n pour que n divise $n + 8$?

2) Ecrire la liste des diviseurs de 56 dans $\mathbb{Z}$ puis déterminer les entiers relatifs x et y tels que $(2x+1)y = 56$

Point méthode

Pour résoudre dans $\mathbb{Z}$ une équation du type $f(x)g(y) = a$ connaissant les diviseurs de a, on utilise un raisonnement exhaustif :

1) $f(x)$ et $g(y)$ sont des diviseurs associés de a
2) On utilise un critère de tri (ci-dessus $2x + 1$ est impair) qui permet de réduire le nombre de cas à envisager
3) on conclut en faisant une vérification si le raisonnement ne se fait pas par équivalence

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) Ecriture 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.

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 $a \equiv n \pmod n$

Remarques

On déduit immédiatement de la définition que :

- si $a \equiv b\ (n)$ alors $b \equiv a\ (n)$
- 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 module

Démontrer ces propriétés à titre d'exercice

IV- Les nombres premiers

a) Définition

Un entier naturel n est premier s'il admet exactement deux diviseurs positifs distincts, 1 et lui-même

Remarques :

- 1 n'est pas premier car il n'a qu'un diviseur positif.
- Le plus petit nombre premier est 2.
- Il existe 15 nombres premiers inférieurs à 50 :

Un entier naturel qui n'est pas premier est appelé un nombre composé.

Propriété:

Si un entier naturel n est composé alors il admet au moins un diviseur premier p tel que $p \leq \sqrt{n}$.

Démonstration :

Soit d le plus petit des diviseurs de $n \geq 2$. On a donc n = $d \times d'$ où d et d' sont deux entiers

Supposons alors que d n'est pas premier. d est donc divisible par un entier k tel que $1 < k < d$. Or k serait alors aussi un diviseur de n et il serait plus petit que d ce qui contredit la définition de d ainsi d est premier .

On peut donc écrire $n = d \times d'$ avec $1 < d \leq d' \leq n$ d'où $dd < dd'$ cad $d^2 \leq n$ et $d \leq \sqrt{n}$

Test de primalité :

En écrivant la contraposée de la propriété précédente, il en découle un test de reconnaissance d'un nombre premier :

Si tous les nombres premiers inférieurs à $\sqrt{n}$ ne sont pas des diviseurs de n alors n est un nombre premier

53 est-il un nombre premier ?

$\sqrt{53} \approx 7,28$. Les nombres premiers inférieurs à 7,28 sont 2 , 3 , 5 , 7 . Comme aucun d'eux ne divisent 53 alors 53 est un nombre premier.

L'ensemble des nombres premiers est infini

Démonstration

Supposons qu'il existe un nombre fini de nombres premiers que nous noterons $p_{1,} p_{2,} p_{3,\ldots,} p_n$. Considérons alors le nombre a = $p_1 p_2 p_{3\ldots} p_n + 1$. Cet entier naturel est supérieur à 2, il admet donc au moins un diviseur premier p_i de l'ensemble nombre $p_{1,} p_{2,} p_{3,\ldots,} p_n$. Cet entier p_i divise a et divise $p_1 p_2 p_{3\ldots} p_n$ donc il divise $a - p_1 p_2 p_{3\ldots} p_n$ c'est à dire 1 ce qui est impossible. L'hypothèse de départ est donc fausse c'est à dire : il existe un nombre infini de nombres premiers .

b) Décomposition en facteurs premiers

Tout entier naturel n est premier ou produit de facteurs premiers

Démonstration : Raisonnons par l'absurde

La propriété est vérifiée pour les premiers entiers : 2 ; 3 ; 4 = 2^2 ; 5 ; 6 = 2 $\times$ 3 .....

Supposons qu'il existe un entier n qui ne soit ni premier , ni produit de nombres premiers. On sait que cet entier admet au moins un diviseur premier . Notons le d . On a alors n = d $\times$ d' avec 1 < d' < n. Or n est le premier entier ne satisfaisant pas à la propriété donc d' la satisfait . L'écriture n = d $\times$ d' mène donc à une contradiction

Si n n'est pas premier, la décomposition de n en facteurs premiers est unique. On la note :

$$n = p_1^{\alpha_1} \ldots p_n^{\alpha_n}$$

où $p_{1,\ldots,} p_n$ sont des nombres premiers distincts et $\alpha_1, \ldots, \alpha_n$ des entiers naturels non nuls

Algorithme de décomposition en facteurs premiers

Voici un algorithme permettant d'obtenir la décomposition en facteurs premiers d'un entier.
 	
Programmer le sur votre calculatrice et retrouver le résultat suivant :
 	
47 432 = $2^3 \times 7^2 \times 11^2$
	Entrées : Saisir n ≥ 2
	Traitement :
	D prend la valeur 2
	Tant que N ≠ 1
	    Tant que D divise N
	        Afficher D
	        N prend la valeur N/D
	    Fin Tant que
	    D prend la valeur D + 1
	Fin Tant Que

Propriété Soit n un entier naturel supérieur ou égal à 2 admettant comme décomposition en facteurs premiers $n = p_1^{\alpha_1} \ldots p_n^{\alpha_n}$. Le nombre de diviseurs de n est : $(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_n + 1)$

Préciser le nombre de diviseurs de 47 432 :