

Chapitre 2 : Divisibilité dans \mathbb{Z} , 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 :

$a \mid b$ qui signifie a divise b

Exemple : 45 est un multiple de -9 ou -9 est un diviseur de 45 que l'on note $-9 \mid 45$

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 $a \mid b$ et $b \mid a$ alors $a = b$ ou $a = -b$

2) Opération sur les multiples

Propriété 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 :

$a \mid b$ et $a \mid c \Rightarrow$ il existe $(\alpha, \beta) \in \mathbb{Z}^2$, 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 $a \mid \alpha b + \beta c$

Remarque: Bien noté que la réciproque de cette propriété est fausse

exemple: voir 4 videos sur le site

3) Algorithme : liste des diviseurs

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

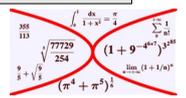
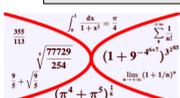
Soit a et b deux diviseurs associés d'un entier n avec $a \leq b$. On a donc $ab = n$ et :

$$\begin{array}{ll} a \leq b & a \leq b \\ a^2 \leq ab & ab \leq b^2 \\ a^2 \leq n & n \leq b^2 \\ a \leq \sqrt{n} & \sqrt{n} \leq b \end{array}$$

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

En langage python



| entier naturel n donné | |
|---|---|
| $i \leftarrow 1$ Tant que $i \leq \sqrt{n}$ Si le reste de la div eucli de n par i est nul alors afficher i Si n/i est différent de i alors afficher n/i $i \leftarrow i+1$ Fin si Fin tant que | def liste_diviseurs(n) : $i = 1$ while $i \leq \sqrt{n}$: if $\text{int}(n/i) == n/i$: print(i) if $\text{int}(n/i) != i$: print($\text{int}(n/i)$) $i = i+1$ |

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 $0 \leq r < b$.

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

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

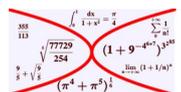
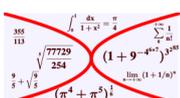
Exemples:

- $a = 356 ; b = 17$: $356 = 17 \times 20 + 16$ 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 :

| | |
|--|---|
| $c \leftarrow 0$ Si $a \geq 0$ alors : Tant que $a > b$: $c \leftarrow c+1$ $a \leftarrow a - b$ Fin du TQ Sinon Tant que $a < b$: $c \leftarrow c+1$ $a \leftarrow a + b$ Fin TQ Afficher c (le quotient) Afficher a (le reste) | def div_eucli(a,b) : $c=0$ if $a \geq 0$: while $a > b$: $c = c + 1$ $a = a - b$ else : while $a < b$: $c = c + 1$ $a = a + b$ print ("le quotient est",c) print (" le reste est", a) |
|--|---|



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

Propriété Soit b un entier naturel supérieur ou égal à 2

Tout entier relatif s'écrit sous l'une des formes suivantes : $bk, bk + 1, bk + 2, \dots, bk + (b-1)$
où k est un entier relatif

Explications : Les restes possibles dans la division euclidienne de a par b sont $0, 1, 2, \dots, b - 1$.

Donc tout entier relatif a peut s'écrire bk ou $bk + 1$ ou $bk + 2 \dots$ 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.

Exemple : [Voir deux vidéos sur le site](#)

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 $a - b = kn$

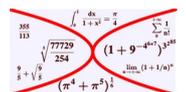
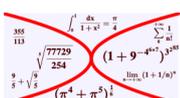
c'est à dire $a = kn + b$. Or $b = nq' + r'$ donc $a = n(k + q') + r'$ avec $0 \leq r' < n$. Ainsi, r' est le reste de la division euclidienne de a par n donc $r = r'$

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 :

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

Exemples :

- $-37 \equiv 18 \pmod{11}$ car $18 - (-37) = 55 = 5 \times 11$
- L'écriture $n \equiv 1 \pmod{5}$ 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 $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$ alors

- | | | | |
|-----------------------------|-------------------------------|------------------------------------|-------------------------------|
| (1) Addition : | $a + c \equiv b + d \pmod{n}$ | (2) Soustraction : | $a - c \equiv b - d \pmod{n}$ |
| (3) Multiplication : | $ac \equiv bd \pmod{n}$ | (4) pour tout entier naturel p , | $a^p \equiv b^p \pmod{n}$ |

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

[Voir deux vidéos sur le site](#)

