Divisibilité dans $\mathbb{Z}$

Created by Dhaouadi Nejib 2020

I. Diviseurs et Multiples d'entiers

☛ Définition

Soient a un entier et d un entier non nul
On dit que **d est un diviseur de a** ou que **a est divisible par d** (ou encore **a est un multiple de d**) s'il existe un entier q tel que $a = qd$ et on note **d|a**
L'ensemble des multiples de d est noté d$\mathbb{Z}$

Exemple ✍
5 divise 25, -4 divise 16, 7 divise -28

Propriétés

Soient a et b deux entiers non nuls et c un entier
- a|a , a|(-a) , 1|a , (-1)|a et a|0
- Si a|b et b|a alors a=b ou a=-b
- Si a|b et b|c alors a|c
- Si a|b et a|c alors a| (αb+βc) où α et β sont deux entiers

Démonstration

- C'est évident car a=1×a , (-a)=(-1)×a , a=1×a , a=(-1)×(-a) et 0=a×0
- a|b et b|a ⇒ b=qa et a=pb où p,q ∈ $\mathbb{Z}$ donc b=pqb avec b≠0 ce qui donne pq=1 or -1 et 1 sont les seuls diviseurs de 1 alors p=q=1 ou p=q=-1 ou encore a=-b ou a=b
- a|b et b|c ⇒ b=pa et c=qb donc c=pqa d'où a|c
- a|b et a|c ⇒ b=pa et c=qa ⇒ αb+βc=αpa+βqa=a(αp+βq) donc a|(αb+βc)

Exemple ✍
On pose $a = 3n - 2$ et $b = 7n - 5$ où n∈$\mathbb{Z}$
Soit d un entier non nul tel que d|a et d|b donc d|(7a-3b) or 7a-3b=7(3n-2)-3(7n-5)=21n-14-21n+15=1 donc d|1 alors d=1 ou d=-1

Exercice 1

1) Determiner L'ensemble des entiers n tels que n-4 divise n+1.

2) Determiner L'ensemble des entiers n tels que n+1 divise n^2+5n+10.

Cliquer ici pour voir les solutions

Exercice 2

Démontrer que pour tout entier naturel n, $3^{2n+2}-2^{n+1}$ est divisible par 7.

Cliquer ici pour voir les solutions

II. Division Euclidienne dans $\mathbb{Z}$

Rappel

On appel partie entière d'un réel x et on note E(x), le plus grand entier inferieur ou égal à x, ou encore c'est l'unique entier n tel que n≤x<n+1
Exemples: E(11)=11, E(-5)=-5, E(1.4)=1, E(-13,34)=-14; E($\sqrt{17}$)=4

☛ Définition

Soit a un entier et b un entier non nul
On appelle **quotient de a par b** l'entier q défini par:

$q = E\left(\frac{a}{b}\right) \quad \text{si} \quad b > 0$

q est le plus petit entier superieur ou égal à $\frac{a}{b}$ si $b < 0$

Conséquence

Soit q le quotient de a par b où a est un entier et b un entier non nul

- Si a est divisible par b alors $q = \frac{a}{b}$
- Si a n'est pas divisible par b alors:
  - $q = E\left(\frac{a}{b}\right) \quad \text{si } b > 0$
  - $q = E\left(\frac{a}{b}\right)+1 \quad \text{si } b < 0$

Exemples ✍

- a=129 et b=17>0, $\frac{a}{b} \simeq 7.6$ donc le quotient de 129 par 17 est égal à E (7.6)= 7
- a=-129 et b=17>0, $\frac{a}{b} \simeq -7.6$ donc le quotient de -129 par 17 est égal à E(-7.6)=-8

- a=129 et b=-17<0, $\frac{a}{b} \simeq -7.6$ donc le quotient de -129 par 17 est égal à E(-7.6)+1=-7
- a=-129 et b=-17<0, $\frac{a}{b} \simeq 7.6$ donc le quotient de -129 par -17 est égal à E(7.6)+1=8

N.B: Remarquons que même si les rapports $\frac{a}{b}$ sont égaux les quotients ne sont pas forcément les mêmes.

☛ Définition

Soit a un entier et b un entier non nul
On appelle reste de a par b, l'entier r tel que $r = a - bq$ où q est le quotient de a par b.

Exemples ✍

Reprenons les exemples précédents :

- Pour a=129 et b=17, r=129-17×7=10
- Pour a=-129 et b=17, r=-129-17×(-8)=7
- Pour a=129 et b=-17, r=129-(-17)×(-7)=10
- Pour a=-129 et b=-17, r=-129-(-17)×8=7

☛ Théorème et définition

Pour tout entier a et pour tout entier b non nul, il existe et unique un couple d'entiers (q,r) tel que $a = bq + r$ où $0 \leqslant r < |b|$
L'écriture $a = bq + r$ avec r∈{0,1,...,|b|-1} est appelée division euclidienne de a par b.
a s'appelle **le dividende**, b **le diviseur**, q **le quotient** et r **le reste**.

Démonstration

Pour l'existance, considerons le quotient q de a par b et le reste r de a par b.
Montrons que 0≤ r < |b|
✻Si b|a, $q = \frac{a}{b}$ et r=a-bq=0 donc 0≤ r < |b|
✻Si a n'est pas divisible par b

- Si b>0, $q = E\left(\frac{a}{b}\right)$ et $r = a - bE\left(\frac{a}{b}\right)$

  On a $E\left(\frac{a}{b}\right) < \frac{a}{b} < E\left(\frac{a}{b}\right) + 1 \Leftrightarrow bq < a < bq + b \Leftrightarrow 0 < a - bq < b$

- Si b<0, $q=E\left(\frac{a}{b}\right)+1$ et $r=a-b\left(E\left(\frac{a}{b}\right)+1\right)$

  On a $E\left(\frac{a}{b}\right)<\frac{a}{b}<E\left(\frac{a}{b}\right)+1 \Leftrightarrow q-1<\frac{a}{b}<(q-1)+1 \Leftrightarrow bq-b>a>bq$
  $\Leftrightarrow -b>a-bq>0$ donc $0\leq r<|b|$

Montrons l'unicité
Supposons qu'il existe deux couples (q,r) et (q',r') tels que a=bq+r=bq'+r'
où $0\leqslant r<|b|$ et $0\leqslant r'<|b|$
Donc b(q-q')=r'-r ⇒ |b||q-q'|=|r-r'|<|b| or |b|>0 donc |q-q'|<1 alors q-q'=0
d'où q=q' et par suite r=r'.

Exemples ✍

Reprenons les exemples précédents :

- Pour a=129 et b=17, q=7 et r=10 donc 129=17×7+10
- Pour a=-129 et b=17,q=-8 et r=7 donc -129=17×(-8)+7
- Pour a=129 et b=-17,q=-7 et r=10 donc 129=(-17)×(-7)+10
- Pour a=-129 et b=-17,q=8 et r=7 donc -129=(-17)×8+7

Exercice 3

Trouver tous les entiers dont le quotient dans la division euclidienne par 5 donne un quotient égal à 3 fois le reste.

Cliquer ici pour voir les solutions

Exercice 4

Lorsqu'on divise a par b, le reste est 8 et lorsqu'on divise 2a par b, le reste est 5. Déterminer le diviseur b.

Cliquer ici pour voir les solutions

Division Euclidienne

124 | 70 | Ok

Le résultat s'affiche ici

III. Congruence modulo n

☛ Définition et notation

Soit n un entier naturel non nul et a et b deux entiers.
On dit que a est congru à b modulo n (ou a et b sont congrus modulo n) si a - b est un multiple de n. On note alors $a \equiv b$ (mod n) .

☛ Théorème et définition

Soit n un entier naturel non nul .
Pour tout entier a, il existe un unique entier r appartenant à {0, ..., n-1} tel que $a \equiv r$ (mod n).
On dit que r est le reste modulo n de a.

Démonstration

Il suffit de faire la division euclidienne de a par n
On sait qu'il existe un unique couple (q,r) tel que a=qn+r avec r ∈ {0,1,...,n-1} ou encore a-r=qn avec r ∈ {0,1,...,n-1} donc il existe et unique r∈{0,1,...,n-1} tel que $a \equiv r$ (mod n)

Conséquence

Soit n un entier naturel non nul.
Deux entiers sont congrus modulo n, si et seulement si, ils ont le même reste modulo n.

Remarques

a et b sont deux entiers et n un entier naturel non nul.

- $a \equiv 0 \pmod{n} \Leftrightarrow n|a$
- Si $a \equiv b$ (mod n) alors pour tout diviseur d>0 de n on a $a \equiv b$ (mod d)
- Si r est le reste de la division euclidienne de a par n alors $a \equiv r$ (mod n)

Exemples ✍

- $143 \equiv 0$ (mod 11) car 11 divise 143 (143=13 ×11)
- $329 \equiv 53$ (mod 3) car 329 et 53 ont le même reste dans la division euclidienne par 3
- $41 \equiv -4$ (mod 9) car 41=4×9+5 et -4=(-1)×9+5
- $675237 \equiv 7$ (mod 10) car 675237=10× 67523+7 (c'est le chiffre des unités)
- $67567283 \equiv 83$ (mod 100), $67567283 \equiv 283$ (mod 1000) etc ...

Propriétés

Soit a, b, c et d des entiers et n un entier naturel non nul.

- $a \equiv a \pmod{n}$
- $a \equiv b \pmod{n} \Leftrightarrow b \equiv a \pmod{n}$
- $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$
- Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$ alors $a+c \equiv b+d \pmod{n}$ et $ac \equiv bd \pmod{n}$ et en conséquence:
  $ka \equiv kb \pmod{n}$ pour tout entier k et $a^m \equiv b^m \pmod{n}$ pour tout entier m>0

Exemples ✍

Déterminer les restes dans la division euclidienne par 7 des nombres :

1) 50^{100} 2) 100^3 3) $50^{100}+100^{100}$

---

1) $50 = 7 \times 7 + 1 \Longrightarrow 50 \equiv 1 \pmod{7}$ donc $50^{100} \equiv 1^{100} \equiv 1 \pmod{7}$
2) $50 \equiv 1 \pmod{7} \Longrightarrow 50 \times 2 \equiv 1 \times 2$ ou encore $100 \equiv 2 \pmod{7}$ donc $100^3 \equiv 2^3 \equiv 8 \equiv 1 \pmod{7}$
3) $100^{100} = 100^{3\times 33+1} = (100^3)^{33} \times 100$ donc $100^{100} \equiv 1^{33} \times 2 \equiv 2 \pmod{7}$
$50^{100} + 100^{100} \equiv 1 + 2 \equiv 3 \pmod{7}$ donc 3 est le reste de la division euclidienne de $50^{100} + 100^{100}$ par 7.

Exercice 5

Montrer que pour tout entier naturel n, $3^{n+3} - 4^{4n+2}$ est divisible par 11.

Cliquer ici pour voir les solutions

Exercice 6

1) Déterminer suivant les valeurs de l'entier n, le reste de la division de n^2 par 7.
2) En déduire alors les solutions de l'équation $x^2 \equiv 2 \pmod{7}$.

Cliquer ici pour voir les solutions

Exercice 7

1) Soit a un entier naturel. Montrer que 7 divise $(a^3-1)(a^4+a)$
2) Déterminer les entiers a tels que $a^{600} \equiv 1 \pmod{7}$

Rappel (Théorème de Fermat)

Pour tout entier a et pour tout entier naturel premier p on a
$a^p \equiv a \pmod{p}$
Si p ne divise pas a alors $a^{p-1} \equiv 1 \pmod{p}$

Cliquer ici pour voir les solutions