ch A1 : rappels : le vocabulaire de l'arithmétique (1s)

Objectifs : introduction à l'arithmétique

déf : arithmétique = étude des nombres entiers
N = ensemble des entiers naturels (=positifs)
Z = ensemble des entiers relatifs (= positifs ou nuls)

Exemples de problèmes d'arithmétique :

6^2010 – 1 est-il multiple de 7 ?
pour quelles valeurs de n, n^2+3n+1 est-il divisible par 5 ?
quel est le pgcd de 2^63-1 et 2^60-1 ?
équations : trouver tous les couples d'entiers tels que 7x-3y=2 ?
résoudre $x^2+9 = 2^n$
problème de ccodage,
…etc….

exercice : définir : multiple, diviseur, pgcd
autres mots ? Nb premier, nb premiers entre eux, div euclidienne

I. MULTIPLES ET DIVISEURS DANS Z

1. def

def « b divise a » ⇔ « b est un diviseur de a » ⇔ « a est un multiple de b » lorsque il existe un entier relatif k tel que a = b*k

Exemple : 3 divise 15 ; les diviseurs de 15 sont :
rq :
0 est multiple de tous les entiers, mais 0 ne divise que 0
1 et -1 sont diviseurs de tous les entiers
a divise a
si /a/ ≠ 1 alors a admet au minimum quatre diviseurs : 1;-1;a;-a
exercice : la somme de trois entiers consécutifs ? → écriture d'en□ers consécu□fs
exercice : parité de A = n(n²+5) ? → raisonner par disjonc□on de cas ; écriture des entiers pairs / impairs

2. propriétés

si b divise a avec a ≠ 0 alors $|b| < |a|$

En valeur absolue, le diviseur est plus petit que le dividende.
Démonstration : b divise a, donc a = bk. Ce qui implique que |a| = |b|×|k|. Et comme a ≠ 0 ; alors |k| ≠ 0 et |k| □ 1 car k est un entier. D'où la propriété.

prop : si a divise b et b divise c alors a divise c
prop : si a divise b alors pour tout entier k , ka divise kb
prop : si c divise a et b alors pour tous entiers u et v, c divise au+bv

csq : si c divise a et b alors c divise a+b

Exercices :
Existe-t-il des entiers n pour lesquels n divise n+8 ?
Pour quels entiers n le rationnel $\frac{2n+1}{n-3}$ *est-il un nb entier ?*
Résoudre dans Z l'équation $x^2-y^2 = 13$?

II. DIV EUCLIDIENNE

1. Div euclidienne dans N

th et def Soient a et b deux entiers positifs, avec b ≠ 0 .

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

démo

* existence du couple (q;r):

considérons l'ensemble des multiples de b:

-2b ; -1b ; 0b = 0 ; 1b=b ; 2b ; 3b ; …….(ces nombres sont dans l'ordre croissant car b>0)

- si a est un multiple de b, par définition cela signifie qu'il existe k tel que a=b*k : on choisit donc q=k et r=0 et on a bien l'égalité a=bq+r et r vérifie bien l'encadrement 0 ? r < b

- si a n'est pas un multiple de b, il existe des multiples de b inférieurs à a, et d'autres supérieurs à a:
(droite graduée)

Choisissons le plus grand des multiples inférieurs à a, notons-le q*b

on a l'encadrement de a : qb < a < (q+1)b,

Posons alors r = a-b*q.

On a bien a = b*q+r , et en soustrayant bq à chaque membre de l'encadrement de a : qb < a < (q+1)b, on obtient 0<r<b : r vérifie bien l'encadrement 0 ? r < b

Dans les deux cas on a montré comment obtenir un entier q et un entier r qui vérifient les deux contraintes.

Pb : D'autres couples (construits différemment) pourraient-ils satisfaire ces contraintes ? NON:

* unicité du couple (q ; r).

Pour cela, utilisons un raisonnement par l'absurde (fréquent en arithmétique donc à retenir) :

Supposons qu'il existe deux couples distincts (q ; r) et (q' ; r'). Alors nous aurions les relations suivantes :

a = bq + r et a = bq' + r'

Donc par soustraction …0 = b(q-q')+ (r- r') càd b(q'-q) = (r- r') : r-r'est alors un multiple de b.

Or -b < r -r' < b . Au total, on a donc un multiple de b qui est plus petit que b ! La seule valeur possible est 0. Donc (r – r') = 0 et par conséquent r = r' et q = q'.

Il est donc impossible de trouver deux couples distincts (q ; r) et (q' ; r') : on a démontré l'unicité de la décomposition de a dans la division euclidienne par b.

(exercices)

1) *déterminer tous les entiers naturels qui divisés par 7 donnent un quotient égal au reste*
2) *reste de le div eucl de 4n-3 par 2n+1 ?*
3) *Déterminer selon les valeurs de n, le reste de la div de 5n+21 par n+3*

2. Division euclidienne dans Z

Cela n'a qu'une importance toute relative (et théorique) mais peut se définir ainsi :

Pour deux entiers relatifs a et b (avec b ≠ 0), il existe un unique couple (q ; r) avec q∈ℤ, r ∈ ℕ ; tel que : $a = b \times q + r$ avec $0 \leq r < |b|$

Le reste est toujours un entier naturel.

Exemples :

+ par – OK : pour 7:(-2) q=-3 et r=1 car 7 = (-2)*(-3)+1

- par + PAS OK : pour (-7):2 q=-4 et r=1 car (-7) = 2*(-4)+1

- par – PAS OK : pour (-7):(-2) q=-4 et r=1 car (-7) = (-2)*(-4)+1

NB : - par qqch : +1 car on doit avoir b*q < a

3. vocabulaire de la division euclidienne

def **Effectuer la division euclidienne de a par b (b ≠ 0), c'est trouver le couple d'entiers naturels (q ; r) tels que** $a = b \times q + r$ avec $0 \leq r < |b|$

a est le dividende ; b le diviseur ; q le quotient et r le reste

Remarques :

* on prendra bien garde à ne pas négliger la condition $0 \leq r < |b|$, souvent oubliée. Elle est pourtant essentielle. Par exemple, 24 = 7 × 2 + 10 n'est pas l'écriture de la division euclidienne de 24 par 7 : le reste est plus grand que le diviseur !

* en pratique, pour b>0, l'encadrement $0 \leq r < |b|$ peut s'écrire $0 \leq r \leq b-1$

4. applications

a) csq pour multiples et diviseurs

th **r = 0 si et seulement si b divise a**.

exercice : déterminer un multiple de 13 dont l'écriture (décimale) ne comporte que des 9.

b) application à la disjonction de cas:

Les restes possibles dans la div eucl d'un relatif a par une relatif b>0 sont 0;1;2;... b-1 donc :

th **tout entier relatif a peut s'écrire de l'une des façons suivantes: bk ou bk+1 ou bk+2 … ou bk+(b-1) avec k** $\in \mathbb{Z}$

exercice : A = n(n²+5) montrer que A est divisible par 3

c) csq pour pgcd : voir ch3

d) csq : un nouvel outil pour résoudre les pb d'arithmétique : **voir ch2**