Chapitre 1 Divisibilité

1) Les ensembles (emboités) de nombres

Que représentent les ensembles de nombres : IN, Z, ID, Q et IR ? $IN \subset Z \subset ID \subset Q \subset IR$.

Compléter le tableau en mettant une croix si le nombre appartient à l'ensemble donné :

nombre	IN	Z	ID	Q	IR
144/27					
-8					
π					
$\sqrt{9}$					
$\sqrt{2}$					

Vrai ou faux ? justifier si c'est faux (en donnant un contre-exemple).

Ne pas confondre => et ⇔ ! Ex : Résoudre $\sqrt{x-1} = 7 - x$.

a) a est dans IN et b est dans IN => a – b est dans IN. b) a est dans Z et b est dans Z => a – b est dans Z.
c) a est dans Z et b est dans Z => a b est dans Z. d) a est dans Z et b est dans Z* => a/ b est dans Z.
e) Si a est dans $\mathbb{Z}$ et b est dans *IN,* alors a-b est dans...

Ensuite, sauf indication contraire, tous les nombres considérés sont des entiers.

2) Multiples et diviseurs

Définition : soient a et b dans Z. a est un multiple de b, ou b est un diviseur de a, ou b divise a, ou a est divisible par b, signifie : il existe k dans Z tel que $a = k.b$). Autrement dit (si $b \neq 0$) : $\frac{a}{b} = k$ est dans Z.

Définition : pour a dans *IR* on rappelle que |a| = Max (- a ; a), |a| est la valeur absolue de a.
Par exemple |4| = 4 et | -3| = 3. $|a| = \sqrt{a^2}$. |a| = a si $a \geq 0$, |a| = - a si $a \leq 0$.
|a| est la distance entre 0 et a. Plus généralement |x-y| est la distance entre x et y.

Une évidence : Si b divise a avec a non nul, alors $-|a| \leq b \leq |a|$ (c'est-à-dire $|b| \leq |a|$). **Preuve** : a = kb donc |a| = | kb| = |k| |b|. $a \neq 0$ donc $k \neq 0$ donc $|k| \geq 1$ donc $|a| \geq |b|$ donc $|a| \geq b$ et $|a| \geq -b$…

Exercices

1) Ecrire 4 phrases équivalentes avec les entiers 20 et - 5.
2) Déterminer tous les diviseurs positifs de 60. Comment s'organiser pour ne pas en oublier ?

3) Vrai ou Faux ? Prouver, si possible, si c'est vrai, ou donner un contre-exemple si c'est faux.
n est un entier naturel.
a) Si n est divisible par 6, alors n est divisible par 3.
b) Si n est divisible par 3, alors n est divisible par 6.
c) Si n est divisible par 5 et par 6, alors n est divisible par 30.
d) Si n est divisible par 5 et par 6, alors n est divisible par 30.
e) Si a et b sont divisibles par 3, alors a+b et 2a-5b sont divisibles par 3.

4) a) Vérifier que 32 + 23, 94 + 49 et 57 + 75 sont des multiples de 11.
b) Prouver que cette propriété (à énoncer) est vraie pour tous les entiers naturels s'écrivant avec deux chiffres.

Quelques propriétés immédiates (preuves : exercice) :
si a divise b et b divise c, alors Si a divise b et b divise a, alors

Si a divise b et c, alors

Oui, c'est idiot, mais aller voir Savoir-faire 1 page 15… $\{n \in \mathbb{Z} / n + 4 \text{ divise } n + 17\}$?

3) Critères de divisibilité. Nombres premiers

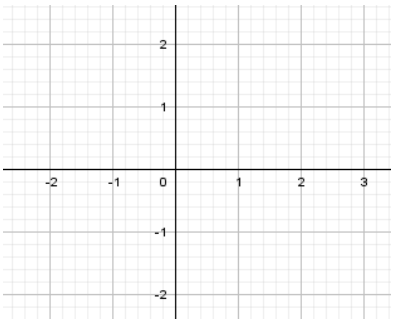
a) Rappeler les critères de divisibilité par 2 ; 3 ; 5 ; 9 ; 10. Critère de divisibilité par 4 ? Preuve : exercice

b) **Définition** : n dans *IN* est **premier** s'il a exactement deux diviseurs : 1 et lui-même.

4) Algorithme écrit en langage TI (Texas Instruments)

Taper sur TI un programme qui demande 2 nombres a et b puis dit si a est divisible par b. (Sortie : oui ou non)
Aide : **Définition** : pour tout réel x, il existe un unique entier n vérifiant $n \leq x < n+1$ (évident et admis).
Cet entier n est appelé partie entière de x. Notation :

On écrit n = PartEnt (x) avec TI, n = floor (x) avec Python, n = [x] ou E(x) ou Ent(x) parfois. Cette fonction, définie sur IR, est dite « en escalier ».
Ent (2,35) =
Ent (-3,42) =



$$Si\ x\ est\ un\ réel, \qquad x\ est\ dans\ \mathbb{Z} \Leftrightarrow Ent(\ x\ ) = x.$$

Aide : pour savoir si un nombre A est divisible par B, on peut regarder si le quotient A/B est un nombre entier.

- pour reconnaître un nombre entier, on peut regarder s'il est égal à sa partie entière.

5) Le même algorithme en langage Python

```
x=input("Quel est le nombre à multiplier par 2 ?")    # code à tester
print("double du nombre saisi = ",2*x)
# …raté, pour Python, x est a priori une String = un fil = une phrase, disons une suite de caractères.
# La bonne syntaxe est x=int(input("nombre à multiplier par 2 ?")), ça « transtype »,
# disons transforme, la string en int = integer = entier.
```

En Python, on peut aussi créer une fonction : Exemple :

```
def multParDeux (a) :   # a est un paramètre de la fonction (en math on dit la variable de la fonction)
   b=2*a    # sans l'indentation (retrait de 4 espaces), c'est faux.
   return  b

# La fonction multParDeux peut alors être appelée n'importe où dans le programme :
# multParDeux(6) vaut 12
```

Ecrire l'algorithme demandé en Python. (2 versions possibles, avec ou sans fonction)

6) Division euclidienne

Qu'est-ce qu'une division euclidienne ?
Exemple : Dans la division euclidienne de 23 par 5,
le quotient est 4 et le reste est 3.
On a donc l'égalité 23 = 5*4+3 avec le reste r = 3 qui vérifie $0 \leq r < 5$.

Exercice : poser la division euclidienne de 397 par 31.
Quel est le dividende ? diviseur ? quotient ? reste ?

Théorème 1 : soient a et b dans IN, $b \neq 0$. Alors il existe des entiers q et r vérifiant $a = b*q + r$ et $\mathbf{0 \leq r < b}$.

Preuve : il suffit de montrer que le nombre q défini par $q = \text{Ent}(\frac{a}{b})$ convient car
c'est un entier et il suffit donc de vérifier que r défini par $r = a - b.\text{Ent}(\frac{a}{b})$ vérifie : $0 \leq r < b$.

$\text{Ent}(\frac{a}{b}) \leq \frac{a}{b} < \text{Ent}(\frac{a}{b}) + 1$ donc $\frac{a}{b} - 1 < \text{Ent}(\frac{a}{b}) \leq \frac{a}{b}$.
On multiplie par $b > 0$: $a - b < b.\text{Ent}(\frac{a}{b}) \leq a$.
On multiplie par -1 : $-a \leq -b.\text{Ent}(\frac{a}{b}) < b - a$.
Ajoutant a, on obtient $0 \leq a - b.\text{Ent}(\frac{a}{b}) = r < b$.

Théorème 2 : les entiers q et r vérifiant ces deux conditions sont **uniques**. Ils sont appelés **q = quotient** et **r = reste** de la division euclidienne de a par b.

Preuve : s'il y a deux solutions $a = b\,q + r = b\,q' + r'$, alors $r - r' = b\,(q'-q)$.
$0 \leq r' < b$ donc $-b < -r' \leq 0$.
Ajoutant cette double inégalité à $0 \leq r < b$, on obtient $-b < r - r' < b$
donc $-b < b\,(q'-q) < b$.
Divisant par $b > 0$, on obtient $-1 < q' - q < 1$ donc $q = q'$.
On en déduit $r = r'$.

Théorème 3 : ceci fonctionne aussi si $a < 0$.
Preuve : l'hypothèse $a \geq 0$ n'a pas été utilisée ci-dessus.

Remarques : 1) On pourrait envisager de diviser par $b < 0$ mais on s'en passera. 2) Par ailleurs, en se compliquant la vie, on aurait pu éviter de supposer connue la division dans IR pour prouver le théorème 1 (en supposant quand même connue la multiplication !).

7) Exemples de raisonnement par disjonction des cas

a) Parité (deux cas à considérer : tout nombre est pair ou (ou exclusif) impair)

On utilisera parfois le fait suivant :

n est un nombre pair ⇔ il existe un entier k tel que n = 2k. (le reste de la division de
n est un nombre impair ⇔ il existe un entier k tel que n = 2k + 1.

Exercice 1 (les 2 premières questions sont indépendantes) : (remarque : 'prouver = montrer = démontrer')

1) Démontrer que si a est un entier pair, alors a^2 l'est aussi.

2) Démontrer que si a est un entier impair, alors a^2 l'est aussi.

3) Prouver que 2) montre que la réciproque de 1) est vraie aussi.(idem en inversant 1 et 2)

On pourra donc désormais utiliser le fait qu'un nombre entier et son carré ont toujours la même parité.

Exercice 2 : déterminer pour quels entiers naturels n, le nombre $(n^2 - 1)$ est divisible par 8.

b) SF7 page 19 : prouver que pour tout n dans $\mathbb{Z}$, $n(n^2 - 4)$ est divisible par 3. Voir la ligne 1 de la méthode 1 (là il y a **trois cas à considérer**)
… et finir en 2 petites lignes. …

idem avec pour tout n dans $\mathbb{Z}$, $n(n^2 - 1)$ est divisible par 3.

8) Exemple de démonstration par l'absurde (voir aussi Ex 2 3) de 7) qui en était une sans le dire)

On veut démontrer que $\sqrt{2}$ est un nombre irrationnel. (c'est-à-dire n'est pas dans Q)

Principe : *On va supposer au contraire que $\sqrt{2}$ est un nombre rationnel, c'est-à-dire qu'il peut s'écrire sous la forme $\frac{p}{q}$ où p et q sont des entiers naturels non nuls et que cette fraction est irréductible (= non simplifiable).*
Nous allons alors élaborer un raisonnement qui nous mènera à une contradiction, ce qui voudra dire que notre hypothèse était fausse et donc que $\sqrt{2}$ est un nombre irrationnel.

Démonstration : on suppose donc que $\sqrt{2} = \frac{p}{q}$ *(fraction irréductible)*

1) A partir de cette égalité, montrer que $p^2 = 2q^2$.
2) En déduire que p^2 est pair, puis que p est pair.
3) Démontrer alors que q est aussi pair.
4) Conclure.

Méthode : prouver par l'absurde que A vraie implique B vraie :

9) « Petits » algorithmes (à faire à la maison ?)

Essayer d'écrire en langage naturel puis en Python et sur votre calculatrice :
- un algorithme qui donne le quotient et le reste de la division euclidienne de a par b (avec $a > 0$ et $b > 0$), ces deux nombres a et b pouvant être choisis par l'utilisateur.
- un algorithme qui donne tous les diviseurs positifs d'un nombre N choisi par l'utilisateur.
  Aide : si on cherche les diviseurs de N fixé, pour savoir si un nombre d est un diviseur de N, il suffit de s'intéresser au cas où $d \leq \sqrt{N}$. Preuve :

10) Un morceau de code Python (solution du 5))

```
    #   Avec ce #, c'est un commentaire, destiné aux humains,
# indentation libre, attention ensuite aux retraits de 4 espaces lignes 7,9,10
from math import * # import d'une bibliothèque
def est_divisible_par(a,b):  # nom de fonction formé d'un seul mot
# la fonction prend deux paramètres a et b.
    assert (b>0)  # vérification du fait que b > 0
    # La ligne de code : est_divisible_par(20,-4) arrêterait le programme.
    if       floor(a/b) == a/b:  # u==v est un test, noter ce ==.
        print(a,"est divisible par",b,":",a,"=",b,"*(",a/b     ,").")
    else:    # on n'écrit pas "then"
        print(a     ," n'est pas divisible par",b,
        ", le reste est ",       a%b,".") # espaces brouillons !
 # a%b est le reste de la div euclidienne de a par b.
# On peut alors appeler la fonction est_divisible_par dans le programme :
                              # (ou sur la console)
est_divisible_par(-30,6)
est_divisible_par(50,4)
```

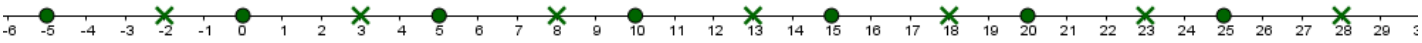
Console Python

```
*** Console de processus distant Réinitialisée ***
>>>
-30 est divisible par 6 : -30 = 6 *( -5.0 ).
50  n'est pas divisible par 4 , le reste est  2 .
>>>
```

11) Congruences

Définition : *Soient* x, y *et* n *des entiers, avec* $n > 0$.
On dit que x *est congru à* y *modulo* n
s'il existe un entier k *tel que* $x - y = k.n$.
On l'écrit $x \equiv y \ [n]$.
Exemple : $17 \equiv 7 \ [5]$.
Bien sûr $x \equiv y \ [n] \Rightarrow y \equiv x \ [n]$. *On dit que* x *et* y *sont congrus modulo* n.
Encore plus évident : on a toujours $x \equiv x \ [n]$.

Remarque : $x \equiv y \ [n] \iff x$ *et* y *ont le même reste pour la division euclidienne par* n.
Exemple :
les nombres congrus à 3 *modulo* 5 : $\ldots -7, -2, 3, 8, 13, 18\ 23\ldots$



Par définition les nombres x congrus à 3 modulo 5 vérifient : il existe k entier tel que x – 3 = 5 k, bref il s'agit de tous les x du type x = 3 + 5 k avec k dans $\mathbb{Z}$.

Preuve : $\Leftarrow$: *simple car* $x = qn + r$ *et* $y = q'n + r$ *impliquent* $x - y = (q' - q)n$.
$\Rightarrow$: $x - y = kn$, $x = qn + r$ *avec* $0 \leq r < n$ *et* $y = q'n + r'$. *avec* $0 \leq r' < n$ *impliquent*
$kn = qn + r - (q'n + r')$ *donc* $n(k - q + q') = r - r'$ *avec* $-n < r - r' < n$ *donc* $-n < n(k - q + q') < n$
d'où $-1 < k - q + q' < 1$ *en divisant par* $n > 0$ *donc* $k - q + q' = 0$ *et finalement* $r - r' = 0$.

Définition : Soient x, y et z des réels, $z > 0$.
On dit que x est congru à y modulo z
s'il existe un entier k tel que $x - y = k.z$.
On l'écrit $x \equiv y\ [z]$.
Exemple : $\frac{\pi}{6} \equiv \frac{37\pi}{6}\ [2\pi]$ *car* $\frac{\pi}{6} - \frac{37\pi}{6} = -3.2\pi$.

Deux évidences :

Si $a \equiv b\ [n]$ *alors* $b \equiv a\ [n]$?
Si $a \equiv b\ [n]$ *et* $b \equiv c\ [n]$,
alors $a \equiv c\ [n]$?

Propriétés simples : Si $a \equiv b\ [n]$ *et* $c \equiv d\ [n]$, *alors*
1) $a + c \equiv b + d\ [n]$,
et même pour tous u *et* v *(entiers!) :*
$ua + vc \equiv ub + vd\ [n]$.
2) $ac \equiv bd\ [n]$.
On peut "ajouter des congruences"
ou "les multiplier" si on a le même modulo.

Propriété moins simple : Si $a \equiv b\ [n]$,
alors pour tout entier $k > 0$: $a^k \equiv b^k\ [n]$.
Preuve : faire une récurrence
ou développer

$$(a-b)(a^{k-1} + a^{k-2}b + a^{k-2}b^2 + \ldots\ldots + ab^{k-2} + b^{k-1}) = (a-b).\sum_{i=0}^{i=k-1} a^{k-1-i}b^i$$

Remarque : Soit n un entier naturel fixé.
Alors tout entier est congru modulo n
à un et un seul des entiers $0, 1, 2, \ldots, n-1$.
$(\forall k \in \mathbb{N}, \exists! r \in \{0,1,2,\ldots,n-1\}\ /k \equiv r\ [n].)$ Vrai ou faux ?

Exercice calculer sans machine le reste de la division euclidienne de 81 par 10 puis le reste de la division euclidienne de 3^{1000} par 10.

Exercice : Soit $N = 5^{2018}$.
1) *Montrer que l'écriture de N comporte plus de 1 000 chiffres.*
2) *Déterminer a tel que* $5^a \equiv 1\ [17]$.
3) *Faire la division euclidienne de 2018 par a.*
4) *Donner le reste de la division euclidienne de N par 17.*

On tape un programme sur TI pour le 2). (résultat dans le menu Stat/Edit)
Nom : CONGPUISS
Disp ''RESTE DE'' (dans E/S = Entrées/Sorties)
Disp ''X^K PAR N''
Input ''X='',X
Input ''N='',N
EffListeL_1 (dans le menu Stat)
EffListeL_2
For(K,1,20)
K->L_1(K)
Remainder(X^K,N)->L2(K) (Reste dans math/NUM)
End

	k	reste de la div de 5^k par 17
2	1	5
3	2	8
4	3	6
5	4	13
6	5	14
7	6	2
8	7	10
9	8	16
10	9	12
11	10	9
12	11	11
13	12	4
14	13	3
15	14	15
16	15	7
17	16	1
18	17	5
19	18	8
20	19	6
21	20	#NOMBRE!

tableur : en B2, taper =MOD(5^A2;17)