Math93.com

Arithmétique Partie 1 (élève)

Tle Maths Experte

I. Une approche historique

Remarque historique

L'origine de l'arithmétique semble être une invention phénicienne. Dans l'école pythagoricienne, à la deuxième moitié du VIe siècle av. J.-C., l'arithmétique était, avec la géométrie, l'astronomie et la musique, une des quatre sciences quantitatives ou mathématiques (Mathemata).
Le mathématicien Euclide d'Alexandrie (vers -300) de la Grèce antique, est l'auteur d'un traité de mathématiques célèbre, les Eléments. Dans cet ouvrage d'importance considérable, il traite d'arithmétique et y expose la première preuve connue de l'infinité des nombres premiers.

II. Divisibilité dans $\mathbb{Z}$

Défi n°1

Choisir un nombre entier naturel à 3 chiffres et l'écrire deux fois côte à côte de façon à obtenir un nombre à 6 chiffres. Expliquer pourquoi ce nombre est divisible par 91 quels que soient les 3 chiffres choisis au départ.

Preuve

....

....

....

....

....

....

....

....

....

....

II.1 Multiples et diviseurs d'un entier relatif

Définition 1

a et b désignent des entiers relatifs.
Dire que a **divise** b signifie **qu'il existe un entier relatif k** tel que $b = a \times k$.
On dit alors aussi que b est un **multiple** de a et que a est un **diviseur** de b.
On peut noter : $a|b$.

Exercice 1

1. -23 divise 276 car :

Preuve

. . . .

. . . .

2. Pour tout entier relatif n, $(n-1)$ divise n^2+3n-4 car :

Preuve

. . . .

. . . .

. . . .

. . . .

3. Tout nombre entier a divise 0 car :

Preuve

. . . .

. . . .

. . . .

. . . .

4. Combien de diviseurs admet, au plus, un entier relatif non nul b ?

Preuve

. . . .

. . . .

. . . .

. . . .

. . . .

II.2 Propriétés de la relation de divisibilité

Deux entiers a et b peuvent être **en relation de divisibilité** , ou pas, suivant que $a|b$, $b|a$, ou ni l'un, ni l'autre. Cette relation a plusieurs propriétés.

Propriété 1

a, b et c désignent des entiers non nuls. u et v désignent des entiers quelconques.

1. $a|a$
2. Si $a|b$ et $b|a$, alors $a = b$ ou $a = -b$.
3. <u>Transitivité de la divisibilité</u> :
   Si $a|b$ et $b|c$, alors $a|c$.

Preuve

Propriété 2

a, b et c désignent des entiers non nuls. u et v désignent des entiers quelconques.
Si $a|b$ et $a|c$, alors $a|(ub + vc)$ soit toutes combinaison linéaires de b et c.

$$\boxed{\begin{cases} a|b \\ a|c \end{cases} \Longrightarrow a|(ub+vc)}$$

Preuve

III. Division euclidienne

Défi n°2

Voici un numéro de Sécurité Sociale (française) : 2660509160143 97.
Est-il correct ?
Les 13 premiers chiffres caractérisent l'individu qui possède le numéro ;
les deux derniers sont une clé de détection des erreurs de saisie les plus fréquentes.
Cette clé vaut 97 moins le reste de la division euclidienne du nombre à 13 chiffres par 97.

Preuve

....
....
....
....
....
....
....
....
....
....

III.1 Définition

Théorème 1 (Division Euclidienne dan $\mathbb{Z}$ (Admis))

a désigne un entier relatif et b un entier naturel non nul.
Il existe un unique couple d'entiers relatifs (q, r) tel que :

$$a = bq + r \text{ avec } 0 \leqslant r < b.\text{H}$$

On a donc : $q \in \mathbb{Z}$ et $r \in \mathbb{N}$.

Définition 2

a désigne un entier relatif et b un entier naturel non nul.
Effectuer la **division euclidienne** de a par b, c'est trouver le couple (q, r) de nombres entiers relatifs tels que :

$$a = bq + r \text{ et } 0 \leqslant r < b.$$

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

Remarque

Si $a < b$, $q = 0$ et $r = a$; si $a = b$, $q = 1$ et $r = 0$; plus généralement, $r = 0$ si et seulement si $b|a$.

Exemple

Effectuer la division euclidienne de a par b :

1. $a = 80$ et $b = 17$
2. $a = -95$ et $b = 12$
3. $a = (n+2)^2$ et $b = n + 4$ où n est un entier naturel non nul

Preuve

....
....
....
....
....
....
....
....
....
....

III.2 Écritures d'un nombre entier quelconque (et disjonction des cas)

Les restes possibles dans la division euclidienne d'un entier relatif quelconque a par un nombre entier naturel non nul b sont :

$$0, 1, 2, \cdots, b-1$$

Propriété 3

b étant un entier naturel non nul, tout nombre entier relatif a peut s'écrire sous la forme bk ou $bk+1$ ou $bk+2$ ou ... ou $bk+(b-1)$ avec k est un entier relatif.

Méthode

Disjonction des cas.
On utilise souvent cette propriété, qui peut sembler évidente, pour démontrer une propriété de divisibilité par disjonction de cas.

Pour k entier naturel,

- on peut par exemple dire qu'un entier n est, soit pair, soit impair, donc de la forme $2k$ ou $2k+1$.
- ou qu'un entier n (par division euclidienne par 3) est de la forme $3k$, $3k+1$ ou $3k+2$.
- ou qu'un entier n (par division euclidienne par 4) est de la forme $4k$, $4k+1$, $4k+2$ ou $4k+3$.
- etc ...

Vous utiliserez cette propriété dans de nombreux exercice, l'énoncé indique parfois qu'il faut procéder par disjonction des cas, mais il faut souvent en prendre l'initiative !

IV. Congruences

Défi n°3

Choisir un nombre entier non nul. Le multiplier par 9 et soustraire 5. Faire la somme des chiffres du résultat et recommencer jusqu'à avoir un nombre à un chiffre. Quel nombre trouvez-vous ? On pourra le prouver bientôt...

Dans ce qui suit, a et b désignent deux entiers relatifs et n est un **entier naturel supérieur ou égal à 2**.

IV.1 Définition

Définition 3

Dire que a et b sont **congrus modulo n** signifie que a et b ont le même reste dans la division euclidienne par n.
On note :

$$\boxed{a \equiv b\,[n]} \text{ ou } \boxed{a \equiv b\,(n)} \text{ ou } \boxed{a \equiv b\,(\operatorname{mod} n)} \text{ ou } \boxed{a \equiv b \mod n}$$

La dernière, celle du mathématicien allemand Gauss (1777-1850), est préconisée par la norme ISO/CEI 80000-2 de 2009.

Remarque

Si r est le reste de la division euclidienne de a par n, alors $a \equiv r[n]$ mais la réciproque est fausse car par exemple $10 \equiv 4\ [2]$ mais 4 n'est pas le reste de la division euclidienne de 10 par 2.

Exemple

1. $7 \equiv 1\ [3]$ car $7 = 3 \times \cdots\cdots + \cdots\cdots$
2. $-5 \equiv 3\ [2]$ car $-5 = 2 \times \cdots\cdots + \cdots\cdots$

Exercice 2

A quel(s) entier(s) peut être congru, modulo 3, un entier donné ?

Preuve

....
....
....
....
....

IV.2 Congruence : Relation d'équivalence

n étant fixé, deux entiers a et b peuvent être **en relation de congruence**, ou pas, suivant que a est congru à b, ou pas.

Cette <u>relation de congruence</u> est une relation dite <u>relation d'équivalence</u> car elle possède les 3 propriétés suivantes :

Propriété 4

a, b et c désignent des entiers relatifs.

1. <u>Réflexivité</u> : $a \equiv a\ [n]$
2. <u>Symétrie</u> : Si $a \equiv b\ [n]$, alors $b \equiv a\ [n]$.
3. <u>Transitivité</u> : Si $a \equiv b\ [n]$ et $b \equiv c\ [n]$ alors $a \equiv c\ [n]$.

Preuve

IV.3 Une propriété fondamentale

Propriété 5

$a \equiv b\ [n]$ si et seulement si n divise $a - b$.
Ce que l'on peut noter :

$$\boxed{a \equiv b\ [n] \iff n \mid (a-b) \iff n \mid (b-a)}$$

Preuve

IV.4 Compatibilité avec les opérations

Propriété 6

a, b, c et d désignent des entiers relatifs et n un entier naturel supérieur ou égal à 2.

Si $\begin{cases} a \equiv b\ [n] \\ c \equiv d\ [n] \end{cases}$ Alors :

1. Somme : $a + c \equiv b + d\ [n]$
2. Produit : $a \times c \equiv b \times d\ [n]$
3. Puissance : pour tout entier naturel p, on a : $a^p \equiv b^p\ [n]$.

Preuve

. . . .

Fin du cours