

Maths expertes– Chapitre n°3

Divisibilité et congruence

L'arithmétique concerne l'étude des entiers naturels $\mathbb{N}$ ou relatifs $\mathbb{Z}$.

- ▶ Il est important de remarquer si la résolution se fait dans $\mathbb{N}$ ou dans $\mathbb{Z}$.
- ▶ Le mode de résolution dans les ensembles $\mathbb{N}$ ou $\mathbb{Z}$ est différent de celui dans l'ensemble des réels $\mathbb{R}$.

Propriété : Propriétés admises

- 1) Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.
- 2) Il n'existe pas de suite infinie strictement décroissante dans $\mathbb{N}$.

1 - Divisibilité dans $\mathbb{Z}$

Définition : Divisibilité, diviseur, multiple

Soient a et b deux entiers relatifs.

a divise b s'il existe un entier relatif k tel que $b = ka$, avec $k \in \mathbb{Z}$. Si a divise b , on note $a \mid b$.

On dit également :

a est un diviseur de b

b est divisible par a

b est un multiple de a

Exemples : 56 est un multiple de -8 car $56 = -7 \times (-8)$.

L'ensemble des multiples de 5 est $\{\dots; -15; -10; -5; 0; 5; 10; \dots\}$. On note cet ensemble $5\mathbb{Z}$.

0 est divisible par tout entier relatif.

Propriété : Transitivité

Soient a , b et c trois entiers relatifs.

Si a divise b et b divise c , alors a divise c .

Démonstration : Transitivité

Si a divise b et b divise c , alors il existe deux entiers relatifs k et k' tels que $b = ka$ et $c = k'b$.

On a alors $c = k'ka$. Donc il existe un entier relatif $l = kk'$ tel que $c = la$.

Donc a divise c .

Exemple : 3 divise 12 et 12 divise 36, donc 3 divise 36.

On peut appliquer également la contraposée de la propriété de transitivité : comme 2 ne divise pas 1001, aucun nombre pair ne divise 1001. En effet, si par exemple 10 divisait 1001, alors 2 diviserait 1001.

Propriété : Combinaisons linéaires

Une expression de la forme $\alpha a + \beta b$ est appelée une **combinaison linéaire** des nombres a et b .

Soient a , b et c trois entiers relatifs.

Si c divise a et b , alors c divise $\alpha a + \beta b$, où α et β sont deux entiers relatifs.

Démonstration : Combinaisons linéaires

Si c divise a et b , alors il existe deux entiers relatifs k et k' tels que $a = kc$ et $b = k'c$.

Donc

$$\alpha a + \beta b = \alpha kc + \beta k'c = (\alpha k + \beta k')c.$$

Il existe donc un entier relatif $l = \alpha k + \beta k'$ tel que $\alpha a + \beta b = lc$.

Exemples : Soit un entier relatif N qui divise les entiers relatifs n et $n + 1$. Alors N divise $n + 1 - n = 1$. Donc $N = -1$ ou $N = 1$.
Comme 3 divise 3^n et 21, alors 3 divise $3^n - 21$, pour tout entier naturel non nul n .

SF 3.1 : Utiliser les propriétés de la divisibilité

- 1) k étant un entier naturel, on pose $a = 9k + 2$ et $b = 12k + 1$. Quels peuvent être les diviseurs positifs communs à a et b ?
- 2) Déterminer les nombres entiers relatifs n tels que $n - 1$ divise $n + 5$.

SF 3.2 : Résoudre une équation

Déterminer les nombres relatifs x et y tels que

$$x^2 - y^2 = 7.$$

Toutes les règles de divisibilité peuvent être démontrées par la congruence que l'on verra dans la suite de ce chapitre.

Propriété : Règle 1 : Par une terminaison : 2, 5, 10, 25, 4

- Un entier est divisible par 2 s'il se termine par 0, 2, 4, 6, 8.
- Un entier est divisible par 5 s'il se termine par 0 ou 5.
- Un entier est divisible par 10 s'il se termine par 0.
- Un entier est divisible par 25 s'il se termine par 00, 25, 50, 75.
- Un entier est divisible par 4 si le nombre formé par les deux derniers chiffres est divisible par 4.

Exemple : 1932 est divisible par 4 car 32 est divisible par 4, par contre 1714 ne l'est pas car 14 n'est pas divisible par 4.

Propriété : Règle 2 : Par somme de ses chiffres : 3 et 9

- Un entier est divisible par 3, respectivement par 9, si la somme de ses chiffres est divisible par 3, respectivement par 9.

Exemples : 8232 est divisible par 3 car $8 + 2 + 3 + 2 = 15$ et 15 est divisible par 3.

4365 est divisible par 9 car $4 + 3 + 6 + 5 = 18$ et 18 est divisible par 9.

Propriété : Règle 3 : Par différence de ses chiffres : 11

- Un entier de trois chiffres est divisible par 11 si la somme des chiffres extrêmes est égale à celui du milieu. Par exemple, 451 est divisible par 11 car $4 + 1 = 5$. On a alors $451 = 11 \times 41$.
- D'une façon générale, un entier est divisible par 11 si la différence entre la somme des chiffres de rangs pairs et la somme des chiffres de rangs impairs est divisible par 11.

Exemples : 6457 est divisible par 11 car $(7 + 4) - (5 + 6) = 11 - 11 = 0$ et 0 est divisible par 11.

4939 est divisible par 11 car $(9 + 9) - (3 + 4) = 18 - 7 = 11$ et 11 est divisible par 11.

2 - Division euclidienne

Propriété : Division euclidienne

Soit a un entier relatif et b un entier naturel non nul.

Il existe un unique couple d'entiers $(q; r)$ tel que

$$a = bq + r \quad \text{avec} \quad 0 \leq r < b.$$

Définitions :

- q est appelé le quotient de la division euclidienne de a par b .
- r est appelé le reste.

Exemple : Dans la division euclidienne de 412 par 15, on a : $412 = 15 \times 27 + 7$.

Démonstration : Division euclidienne

Existence du couple $(q; r)$.

La suite des multiples de b est :

$$\dots; -kb; \dots; -2b; -b; 0; b; 2b; \dots; kb; \dots$$

avec $k \in \mathbb{N}$.

Premier cas : a est un multiple de b . Alors a est l'un des termes de la suite ci-dessus et il existe un nombre entier relatif q tel que $a = bq$. On obtient $a = bq + 0$, avec $0 \leq 0 < b$.

Deuxième cas : a n'est pas un multiple de b . Il existe des multiples de b inférieurs à a et d'autres supérieurs à a . On peut écrire

$$bq < a < b(q+1),$$

où $b(q+1)$ est le plus petit multiple de b supérieur à a .

Finalement, pour tout $a \in \mathbb{Z}$, il existe un entier relatif q tel que

$$bq \leq a < b(q+1),$$

c'est-à-dire $0 \leq a - bq < b$. On pose $r = a - bq$, on obtient $a = bq + r$ et $0 \leq r < b$.

Unicité du couple $(q; r)$.

On suppose qu'il existe deux couples de nombres entiers relatifs $(q; r)$ et $(q'; r')$ tels que

$$a = bq + r, \quad a = bq' + r', \quad 0 \leq r < b, \quad 0 \leq r' < b.$$

Alors, par différence,

$$0 = b(q - q') + r - r',$$

soit $r - r' = b(q' - q)$. Donc $r - r'$ est un multiple de b .

De plus, comme $0 \leq r < b$ et $0 \leq r' < b$, on a $-b < r - r' < b$.

Or, 0 est le seul multiple de b strictement compris entre $-b$ et b , donc $r - r' = 0$, soit $r = r'$. On en déduit que $b(q' - q) = 0$.

Comme $b \neq 0$, on obtient $q' = q$.

L'unicité du couple $(q; r)$ est ainsi prouvée.

SF 3.3 : Déterminer le reste d'une division euclidienne

- 1) Déterminer le quotient et le reste de la division de -5000 par 17 .
- 2) n désigne un nombre entier naturel. Déterminer le reste de la division euclidienne de $7n + 16$ par $2n + 3$.
- 3) Trouver tous les entiers qui, divisés par 5 , donnent un quotient égal à 3 fois le reste.
- 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 .

SF 3.4 : Raisonner suivant les restes possibles

n désigne un nombre entier naturel et on note

$$A = n(n^2 + 5).$$

Démontrer que, pour tout entier naturel n , A est divisible par 3.

3 - Congruences dans $\mathbb{Z}$

Exemple : On considère la suite de nombres : 1, 6, 11, 16, 21, 26, 31, 36.

Si on prend deux quelconques de ces nombres, alors leur différence est divisible par 5. Par exemple : $21 - 6 = 15$, qui est divisible par 5. On dit que 21 et 6 sont congrus modulo 5.

Définition : Congruence

Soit n un entier naturel.

Deux entiers a et b sont congrus modulo n lorsque $a - b$ est divisible par n , c'est-à-dire s'il existe un entier relatif k tel que $a - b = kn$. Le cas $n = 0$ est l'égalité.

On note

$$a \equiv b [n].$$

Propriété : Congruence et reste

Soit n un entier naturel non nul.

Deux entiers a et b sont congrus modulo n , si et seulement si, la division euclidienne de a par n a le même reste que la division euclidienne de b par n .

Démonstration : Congruence et reste

On écrit les divisions euclidiennes de a et b par n :

$$a = nq + r, \quad b = nq' + r', \quad 0 \leq r < n, \quad 0 \leq r' < n.$$

Si $r = r'$:

$$a - b = nq + r - nq' - r' = n(q - q').$$

Donc $a - b$ est divisible par n et donc $a \equiv b [n]$.

Si a et b sont congrus modulo n :

$$a - b = nq + r - nq' - r' = n(q - q') + r - r'.$$

Donc

$$r - r' = a - b - n(q - q').$$

Comme $a \equiv b [n]$, $a - b$ est divisible par n , et donc $r - r'$ est divisible par n .

Par ailleurs, $0 \leq r < n$ et $0 \leq r' < n$, donc $-n < r - r' < n$. Ainsi, $r - r'$ est un multiple de n strictement compris entre $-n$ et n . Donc $r - r' = 0$, soit $r = r'$.

Exemple : On a vu que $21 \equiv 6 [5]$.

Les égalités euclidiennes $21 = 4 \times 5 + 1$ et $6 = 1 \times 5 + 1$ montrent que le reste de la division de 21 par 5 est égal au reste de la division de 6 par 5.

Propriété : RST

Soit n un entier naturel non nul.

a) $a \equiv a [n]$, pour tout entier relatif a .

b) Si $a \equiv b [n]$, alors $b \equiv a [n]$.

c) Si $a \equiv b [n]$ et $b \equiv c [n]$, alors $a \equiv c [n]$.

On dit que la congruence est une **relation d'équivalence**.

Réflexivité
Symétrie
Transitivité

Démonstration : RST

a) $a - a = 0$ est divisible par n .

- b)** Si $a \equiv b [n]$, alors n divise $a - b$. Donc n divise $-(a - b) = b - a$, et ainsi $b \equiv a [n]$.
- c)** Si $a \equiv b [n]$ et $b \equiv c [n]$, alors n divise $a - b$ et $b - c$. Donc n divise $a - b + b - c = a - c$, et ainsi $a \equiv c [n]$.

Propriété : Opérations avec les congruences

Soit n un entier naturel non nul.

Soient a, b, a' et b' des nombres relatifs tels que $a \equiv b [n]$ et $a' \equiv b' [n]$. Alors on a :

$$a + a' \equiv b + b' [n],$$

$$a - a' \equiv b - b' [n],$$

$$a \times a' \equiv b \times b' [n],$$

$$a^p \equiv b^p [n] \quad \text{avec} \quad p \in \mathbb{N}.$$

Démonstration : Congruence et puissance

On démontre la propriété $a^p \equiv b^p [n]$ par récurrence sur $p \in \mathbb{N}$.

Initialisation : la démonstration est triviale pour $p = 0$ ou $p = 1$.

Hérédité : supposons qu'il existe un entier k tel que la propriété soit vraie : $a^k \equiv b^k [n]$.

Démontrons que la propriété est vraie au rang $k + 1$:

$$a^{k+1} = a \times a^k \equiv b \times b^k \equiv b^{k+1} [n].$$

Conclusion : la propriété est vraie pour $p = 0$ et héréditaire à partir de ce rang. D'après le principe de récurrence, elle est vraie pour tout entier naturel p .

Exemples : On a $7 \equiv 4 [3]$ et $11 \equiv 20 [3]$, donc $7 + 11 \equiv 4 + 20 \equiv 24 [3]$, et on a alors $7 + 11 \equiv 0 [3]$.

De même, $7 \times 11 \equiv 4 \times 20 \equiv 80 [3]$, et on a alors $7 \times 11 \equiv 2 [3]$.

SF 3.5 : Raisonner avec les congruences

1) Déterminer les entiers x tels que

$$6 + x \equiv 5 [3].$$

2) Déterminer les entiers x tels que

$$3x \equiv 5 [4].$$

3)

a) x désigne un nombre entier relatif. Démontrer que si x n'est pas multiple de 3, alors

$$x^2 \equiv 1 [3].$$

b) Démontrer que, pour tous entiers relatifs a et b , le nombre

$$N = ab(a^2 - b^2)$$

est divisible par 3.

SF 3.6 : Déterminer le reste d'une division

1) Déterminer le reste de la division de 2^{456} par 5.

2) Déterminer le reste de la division de 2^{437} par 7.