Multiples. Division euclidienne. Congruence

Table des matières

1 Avant propos

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 1 : Admise

1) Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.
2) Toute suite dans $\mathbb{N}$ strictement décroissante est stationnaire au bout d'un certain rang.

2 Multiples et diviseurs dans $\mathbb{Z}$

2.1 Définition

Définition 1 : Soit a et b deux entiers relatifs.

a est un multiple de b, si et seulement si, il existe un entier relatif k tel que :

$$a = kb, \qquad k \in Z$$

3 autres formulations sont possibles :

- a est divisible par b
- b est un diviseur de a
- b divise a

Exemples :

- 54 est un multiple de 3 car $54 = 18 \times 3$
- -5 divise 45 car $45 = (-9) \times (-5)$

2.2 Propriétés

- 0 est multiple de tout entier.
- 1 divise tout entier.
- Si a est un multiple de b et si $a \neq 0$ alors : $|a| \geqslant |b|$.
- Si a divise b et si b divise a alors $a = b$ ou $a = -b$ avec a et b non nuls.

2.3 Règles de divisibilité

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

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 2 derniers chiffres est divisible par 4.

  1 932 *est divisible par* 4 *car* 32 *est divisible par* 4,

  par contre 1 714 *ne l'est pas car* 14 *n'est pas divisible par* 4

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).

  8 232 *est divisible par* 3 *car :*

$$8+2+3+5=15 \quad \textit{et} \quad 15 \textit{ est divisible par } 3$$

  4 365 *est divisible par* 9 *car :*

$$4+3+6+5=18 \quad \textit{et} \quad 18 \textit{ est divisible par } 9$$

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.

  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.

  6 457 *est divisible par* 11 *car :*

$$(7+4)-(5+6) = 11-11 = 0 \quad \textit{et} \quad 0 \textit{ est divisible par } 11$$

  4 939 *est divisible par 11 car :*

$$(9+9)-(3+4) = 18-7 = 11 \quad \textit{et} \quad 11 \textit{ est divisible par } 11$$

Application :

Trouver tous les diviseurs des nombres suivants : 20, 36 et 120

Grâce aux règles de divisibilité, on montre facilement que :

1) Les diviseurs de 20 sont : 1, 2, 4, 5, 10, 20
2) Les diviseurs de 36 sont : 1, 2, 3, 4, 6, 9, 12, 18, 36
3) Les diviseurs de 120 sont : 1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120

Algorithme : Déterminer un algorithme qui donne l'ensemble de diviseur d'un entier naturel donné.
L'algorithme suivant est basé sur le fait que si d divise N, alors $N = kd$ donc le quotient k est aussi un diviseur de N. Lorsque l'on trouve un diviseur de N, on en trouve un second.

Par exemple avec 120 :

diviseur d	quotient k
1	120
2	60
3	40
4	30
5	24
6	20
8	15
10	12

La première colonne s'arrête lorsque le diviseur d est supérieur à $\sqrt{N}$. On peut donc écrire le programme suivant, en utilisant deux listes L_1 et L_2 qui correspondent aux deux colonnes du tableau. On fusionne ensuite les deux listes pour n'en faire qu'une seule L_1.

Variables : N, K, I entiers
L_1, L_2 listes
Entrées et initialisation
Lire N
$0 \to K$
$1 \to I$
Effacer les listes L_1 et L_2
Traitement
tant que $I \leqslant \sqrt{N}$ **faire**
si $E\left(\dfrac{N}{I}\right) = \dfrac{N}{I}$ **alors**
$K + 1 \to K$
$I \to L_1(K)$
$\dfrac{N}{I} \to L_2(K)$
fin
$I + 1 \to I$
fin
pour I de 1 à K **faire**
$L_2(K - I + 1) \to L_1(K + I)$
fin
Sorties : Afficher L_1

2.4 Exercices d'applications

1) Déterminer tous les couples d'entiers naturels tels que : $x^2 - 2xy = 15$

2) Déterminer tous les entiers relatifs n tels que $(n - 3)$ divise $n + 5$

1) On cherche à mettre le terme de droite en facteur de façon à faire apparaître des diviseurs de 15. En factorisant, on trouve : $x(x - 2y) = 15$

Comme x et y sont des entiers naturels, on a la relation suivante : $x \geqslant x - 2y$.
De plus les diviseurs de 15 sont : $D_{15} = \{1, 3, 5, 15\}$

Les décompositions possibles sont donc :

$$\begin{cases} x = 15 \\ x - 2y = 1 \end{cases} \quad \text{ou} \quad \begin{cases} x = 5 \\ x - 2y = 3 \end{cases}$$

$$\begin{cases} x = 15 \\ y = \dfrac{15 - 1}{2} = 7 \end{cases} \quad \text{ou} \quad \begin{cases} x = 5 \\ y = \dfrac{5 - 3}{2} = 1 \end{cases}$$

On obtient alors les couples solutions : $(15, 7)$ et $(5, 1)$

2) Si $(n - 3)$ divise $(n + 5)$ alors il existe un entier k tel que : $n + 5 = k(n - 3)$

On cherche à factoriser par $(n - 3)$ en faisant ressortir ce terme à gauche :

$$\begin{aligned}(n-3)+8 &= k(n-3)\\ k(n-3)-(n-3) &= 8\\ (n-3)(k-1) &= 8\end{aligned}$$

donc $(n-3)$ est un diviseur de 8. L'ensemble des diviseurs de 8 dans $\mathbb{Z}$ est :

$$D_8 = \{-8, -4, -2, -1, 1, 2, 4, 8\}$$

On a donc le tableau suivant correspondant aux valeurs possibles de n :

$n-3$	-8	-4	-2	-1	1	2	4	8
n	-5	-1	1	2	4	5	7	11

2.5 Opération sur les multiples

Théorème 1 : Soit trois entiers relatifs a, b et c.

Si a divise b et c alors a divise $b+c$, $b-c$ ou toute combinaison linéaire de b et de c : $\alpha b + \beta c$.

ROC **Démonstration :**
On sait que a divise b et c, donc il existe deux entiers relatifs k et k' tels que :

$$b = ka \quad \text{et} \quad c = k'a$$

On a alors : $b+c = (k+k')a$, $b-c = (k-k')a$ et $\alpha b + \beta c = (\alpha k + \beta k')a$

Donc a divise $b+c$, $b-c$ et $\alpha b + \beta c$

Application : 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 ?

Soit d un diviseur commun à a et b.
Comme d divise a et b, il divise $c = 4a - 3b$, soit

$$c = 4(9k+2) - 3(12k+1) = 36k + 8 - 36k - 3 = 5$$

donc d divise 5. Comme 5 n'a que 2 diviseurs positifs 1 et 5, on a alors $d = 1$ et $d = 5$

Les diviseurs positifs possibles communs à a et b sont : 1 et 5.

3 La division euclidienne

Définition 2 : Soit a un entier relatif et b un entier naturel non nul.
On appelle division euclidienne de a par b, l'opération qui au couple $(a;b)$ associe le couple $(q;r)$ tel que :

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

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

Exemples :

- La division euclidienne de 114 par 8 : $114 = 8 \times 14 + 2$
- La division de -17 par 3 : $-17 = 3 \times (-6) + 1$

Application :

1) Trouver tous les entiers qui divisés par 5 donne un quotient égal à 3 fois le reste.
2) 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.

1) Soit a l'entier cherché. On divise a par 5, on a alors :

$$a = 5q + r \quad \text{avec} \quad 0 \leqslant r < 5$$

Comme $q = 3r$, on a : $a = 15r + r = 16r \quad \text{avec} \quad 0 \leqslant r < 5$

On trouve toutes les valeurs de a en faisant varier r de 0 à 4 compris, on a alors l'ensemble solution suivant :

$$S = \{0, 16, 32, 48, 64\}$$

2) Écrivons les deux divisions, en notant q et q' les restes respectifs :

$$\begin{cases} a = bq + 8 \quad \text{avec} \quad b > 8 \\ 2a = bq' + 5 \quad \text{avec} \quad b > 5 \end{cases}$$

En multipliant la première division par 2 et en égalisant avec la deuxième, on obtient :

$$\begin{aligned} 2bq + 16 &= bq' + 5 \quad \text{avec} \quad b > 8 \\ b(2q - q') &= -11 \\ b(q' - 2q) &= 11 \end{aligned}$$

b est donc un multiple positif non nul de 11, supérieur à 8, donc : $b = 11$

Algorithme : On peut proposer l'algorithme suivant, pour la division euclidienne, par soustractions successives :

```
Variables : a, b, q, r entiers
Entrées et initialisation
    Lire a, b
    0 → q
Traitement
    si a ⩾ 0 alors
        tant que a ⩾ b faire
            a − b → a
            q + 1 → q
        fin
    sinon
        tant que a < 0 faire
            a + b → a
            q − 1 → q
        fin
    fin
    a → r
Sorties : Afficher "le quotient est", q
          Afficher "le reste est", r
```

4 Congruence

4.1 Entiers congrus modulo n

Définition 3 : Soit n un entier naturel ($n \geqslant 2$), a et b deux entiers relatifs.

On dit que deux entiers a et b sont congrus modulo n si, et seulement si, a et b ont même reste par la division euclidienne par n. On note alors :

$$a \equiv b \mod n \qquad \text{ou} \qquad a \equiv b \ (n)$$

Exemples :

1) $57 \equiv 15 \ (7)$ car : $57 = 7 \times 8 + 1$ et $15 = 7 \times 2 + 1$

2) Un nombre est congru à son reste modulo n par la division euclidienne par n.

$$2008 \equiv 8 \ (10) \qquad 17 \equiv 1 \ (4) \qquad 75 \equiv 3 \ (9) \qquad \dots$$

3) si $x \equiv 0 \ (2)$, alors x est pair et si $x \equiv 1 \ (2)$, x est impair

Propriétés : Comme la congruence est une relation d'équivalence, elle est :

1) Réflexive : $a \equiv a \ (n)$

2) Symétrique : si $a \equiv b \ (n)$ alors $b \equiv a \ (n)$

3) Transitive : si $a \equiv b \ (n)$ et $b \equiv c \ (n)$ alors $a \equiv c \ (n)$

Remarque : comme nous allons le voir dans les exemples suivants, la notion de congruence prend tout son intérêt, dès lors qu'on s'intéresse seulement au reste, pour une propriété donnée. Par exemple, lorsqu'on s'intéresse au jour de la semaine d'une date donnée, on travaillera modulo 7.

Théorème 2 : Soit n un entier naturel ($n \geqslant 2$), a et b deux entiers relatifs.

$$a \equiv b \ (n) \quad \Leftrightarrow \quad a - b \equiv 0 \ (n)$$

Démonstration : Comme il s'agit d'une équivalence, il faut démontrer la propriété dans les deux sens.

- *Dans le sens* $\Rightarrow$

  On sait donc que $a \equiv b \ (n)$. Il existe donc q, q', et r tel que :

  $$a = nq + r \quad \text{et} \quad b = nq' + r \quad \text{avec} \quad 0 \leqslant r < n$$

  On en tire : $a - b = n(q - q')$

  Donc $a - b$ est un multiple de n, donc son reste par la division par n est nul, donc : $a - b \equiv 0 \ (n)$

- *Dans le sens* $\Leftarrow$ (réciproquement)

  On sait donc que $a - b \equiv 0\ (n)$. Il existe k tel que : $a - b = kn$ (1)

  Si l'on effectue la division de a par n, on a : $a = nq + r$ (2)

  De (1) et (2), on obtient :

$$\begin{aligned} nq + r - b &= kn \\ -b &= kn - nq - r \\ b &= (q-k)n + r \end{aligned}$$

  On en déduit donc : $a \equiv b\ (n)$

4.2 Compatibilité avec la congruence

Théorème 3 : Soit n un entier naturel $(n \geqslant 2)$, a, b, c, d des entiers relatifs vérifiant :

$$a \equiv b\ (n) \quad \text{et} \quad c \equiv d\ (n)$$

La congruence est compatible :

1) avec l'addition : $a + c \equiv b + d\ (n)$

2) avec la multiplication : $ac \equiv bd\ (n)$

3) avec les puissances : $\forall\, k \in \mathbb{N} \quad a^k \equiv b^k\ (n)$

ROC

Démonstration :

1) *Compatibilité avec l'addition.*

   On sait que : $a \equiv b\ (n)$ et $c \equiv d\ (n)$, donc $(a - b)$ et $(c - d)$ sont des multiples de n. Il existe donc deux entiers relatifs k et k' tels que :

$$a - b = kn \quad \text{et} \quad c - d = k'n$$

   En additionnant ces deux égalités, on obtient :

$$\begin{aligned} a - b + c - d &= kn + k'n \\ (a+c) - (b+d) &= (k+k')n \end{aligned}$$

   Donc $(a + c) - (b - d)$ est un multiple de n, donc d'après le théorème 2, on obtient :

$$a + c \equiv b + d\ (n)$$

2) *Compatibilité avec la multiplication.*

   On sait que : $a \equiv b\ (n)$ et $c \equiv d\ (n)$, donc, il existe deux entiers relatifs k et k' tels que :

$$a = b + kn \quad \text{et} \quad c = d + k'n$$

   En multipliant ces deux égalités, on obtient :

$$\begin{aligned} ac &= (b+kn)(d+k'n) \\ ac &= bd + k'bn + kdn + kk'n^2 \\ ac &= bd + (k'b + kd + kk'n)n \\ ac - bd &= (k'b + kd + kk'n)n \end{aligned}$$

Donc $(ac - bd)$ est un multiple de n, donc d'après le théorème 2, on a :

$$ac \equiv bd\ (n)$$

3) *Compatibilité avec les puissances.*
On prouve cette compatibilité par récurrence sur k, à l'aide de la compatibilité avec la multiplication. Nous en confions la preuve au lecteur.

4.3 Applications de la congruence

4.3.1 Reste

Déterminer les restes successifs dans la division par 7 des nombres suivants : 50^{100}, 100, 100^3, $50^{100} + 100^{100}$.

1) Reste de 50^{100} par la division par 7.
On a $50 \equiv 1\ (7)$ car $50 = 7 \times 7 + 1$. D'après la compatibilité avec les puissances, on a :

$$50^{100} \equiv 1^{100} \equiv 1\ (7)$$

Le reste est 1.

2) Reste de 100 par la division par 7.
$100 = 50 \times 2$, comme $50 \equiv 1\ (7)$, d'après la compatibilité avec la multiplication, on a :

$$100 \equiv 2\ (7)$$

Le reste est 2.

3) Reste de 100^3 par la division par 7
Comme $100 \equiv 2\ (7)$, d'après la compatibilité avec les puissances, on a :

$$100^3 \equiv 2^3 \equiv 8 \equiv 1\ (7)$$

le reste est 1.

4) Reste de $50^{100} + 100^{100}$ par la division par 7
$100^{100} = 100^{3\times 33+1} = \left(100^3\right)^{33} \times 100$, donc d'après la compatibilité avec les puissances et la multiplication, on a :

$$100^{100} \equiv 1^{33} \times 2 \equiv 2\ (7)$$

Par compatibilité avec l'addition, on a alors :

$$50^{100} + 100^{100} \equiv 1 + 2 \equiv 3\ (7)$$

Le reste est 3.

4.3.2 Divisibilité

Montrer que : $\forall n \in \mathbb{N}, \quad 3^{n+3} - 4^{4n+2}$ est divisible par 11

On a : $3^{n+3} = 3^n \times 3^3 = 27 \times 3^n$, or $27 \equiv 5\ (11)$, donc d'après la compatibilité avec la multiplication, on a

$$\forall n \in \mathbb{N}, \quad 3^{n+3} \equiv 5 \times 3^n\ (11)$$

On a : $4^{4n+2} = \left(4^4\right)^n \times 4^2$, or $4^2 \equiv 5\ (11)$ donc $4^4 \equiv 5^2 \equiv 3\ (11)$, donc :

$$\forall n \in \mathbb{N}, \quad 4^{4n+2} \equiv 3^n \times 5\ (11)$$

On en déduit donc :

$$3^{n+3} - 4^{4n+2} \equiv 0\ (11)$$

La proposition est donc vérifiée $\forall x \in \mathbb{N}$.