Terminale Maths Expertes – Chapitre 02

DIVISIBILITÉ DANS $\mathbb{Z}$

$$16 \equiv 7[3]$$

Table des matières

I Divisibilité dans $\mathbb{Z}$

1) Diviseurs d'un entier relatif

DÉFINITION

Soient a et b deux entiers relatifs.
On dit que a divise b si et seulement si il existe un entier relatif k tel que $b = ka$. On peut le noter $a|b$.
On dit aussi que a est un diviseur de b ou que b est divisible par a.
Ainsi, b est alors un multiple de a.

REMARQUES

- Tout entier relatif a possède au moins 4 diviseurs : 1, -1, a et $-a$.
- Tout entier relatif a non nul possède un nombre **fini** de diviseurs compris entre $-a$ et a.
- Les diviseurs de a sont les mêmes que ceux de $-a$, et $a|b \iff a|(-b) \iff (-a)|(-b)$.
- 0 est un cas particulier car il possède une infinité de diviseurs : tous les entiers relatifs non nuls.

EXERCICES

1) Démontrer que -4 est un diviseur de 32.

2) Démontrer que $n+1$ est un diviseur de n^2-1 pour tout entier naturel n.

3) Soit n un entier relatif impair. Démontrer que la somme de n entiers consécutifs est toujours un multiple de n. (On commencera par étudier le cas $n = 3$).

4) Combien y a-t-il de multiples de 13 entre 1 et 1 000 ?

5) **a)** Combien y a-t-il de multiples de 75 compris entre 10 000 et 20 000 ?

b) Leur somme est-elle un multiple de 75 ?

6) Soit a un entier à deux chiffres et b l'entier obtenu en intervertissant les chiffres de a. Démontrer que $a-b$ est un multiple de 9 et que $a+b$ est un multiple de 11.

2) Propriétés de divisibilité

PROPRIÉTÉ

Soient a, b et c trois entiers relatifs.
Si a divise b et si b divise c, alors a divise c (propriété de *transitivité*).

DÉMONSTRATION

Si a divise b et si b divise c, alors il existe deux entiers relatifs k et k' tels que $b = ka$ et $c = k'b$.
Ainsi, $c = k'(ka) = (kk')a$. Donc c est un multiple de a, d'où a divise c.

EXEMPLES

1) Justifier que 7 divise 6 300.

2) Justifier que 3 divise 6^7.

PROPRIÉTÉ

Contraposée de la propriété :
Soient a, b et c trois entiers relatifs.
Si b ne divise pas a, alors aucun multiple de b ne peut diviser a.

DÉMONSTRATION

Démonstration (par l'absurde) :
Soient a et b deux entiers tel que b ne divise pas a.
Supposons qu'il existe un entier k tel que kb divise a.
Or b divise kb, et puisque kb divise a, alors b divise a. Impossible d'après les hypothèses.
Donc si b ne divise pas a, alors aucun multiple de b ne peut diviser a.

REMARQUE

Cette contraposée est très utile pour établir la liste des diviseurs d'un entier.

EXEMPLE

Démontrer qu'aucun nombre pair ne divise 1 001.

3) Une propriété très utile

PROPRIÉTÉ

Soient a, b et d trois entiers relatifs.
Si d divise a et b, alors d divise toute combinaison linéaire de a et de b de la forme $au+bv$ où u et v sont des entiers relatifs.

DÉMONSTRATION

Si d est un diviseur commun de a et de b, alors il existe deux entiers relatifs k et k' tels que $a=kd$ et $b=k'd$.
Soit $au+bv$ une combinaison linéaire de a et de b, avec u et v deux entiers relatifs.
On a alors $au+bv=kdu+k'dv=(ku+k'v)\times d$.
Donc $au+bv$ est un multiple de d, donc d divise bien $au+bv$.

REMARQUE

Soient a et b deux entiers relatifs.
Si $a|b$, alors $a|(a+b)$, $a|(a-b)$ et $a|(ua+vb)$ (avec u, $v\in\mathbb{Z}$) car $a|a$.

EXEMPLES

- $\forall n\in\mathbb{N}$, 3 divise 3^n, et 3 divise 21, donc 3 divise 3^n-21.
- Soit d un entier naturel divisant $4n-1$ et $2n-1$ pour tout $n\in\mathbb{N}$. Montrer que $d=1$.
- Soit n un entier naturel supérieur ou égal à 3. On pose $a=4n+1$ et $b=3n-8$. Quels sont les diviseurs positifs communs à a et b ?

II Division euclidienne

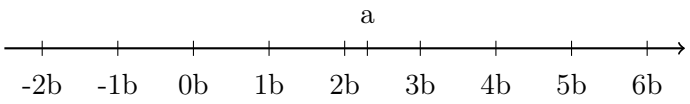
1) Énoncé du théorème

PROPRIÉTÉ & DÉFINITION

Soit a un entier relatif et b un entier naturel non nul.
Il **existe** un **unique** couple d'entiers $(q;r)$ tel que $a = b \times q + r$ avec $0 \leqslant r < b$.
Cette écriture s'appelle la division euclidienne de a par b.
q est le quotient, r est le reste, a est le dividende et b est le diviseur de cette division euclidienne.

DÉMONSTRATION

• **Existence :**
Soit x un réel. La partie entière de x est l'unique entier noté $E(x)$ tel que $E(x) \leqslant x < E(x) + 1$.



Posons $q = E\left(\frac{a}{b}\right)$. Alors $E\left(\frac{a}{b}\right) \leqslant \frac{a}{b} < E\left(\frac{a}{b}\right)$, soit $q \leqslant \frac{a}{b} < q+1$, donc $bq \leqslant a < bq+1$, donc $0 \leqslant a - bq < b$.
En posant $r = a - bq$, on a bien $a = bq + r$ avec q et r des entiers et $0 \leqslant r < b$.

• **Unicité :**
Supposons qu'il existe deux couples $(q;r)$ et $(q';r')$ vérifiant la propriété.
Alors on a $a = bq + r = bq' + r'$ d'où $r' - r = b(q - q')$.
Or $0 \leqslant r < b$, soit $-b < -r \leqslant 0$, et comme on sait que $0 \leqslant r' < b$, on obtient par addition l'encadrement : $-b < r' - r < b$.
Or $r' - r = b(q - q')$ est un multiple de b strictement compris entre $-b$ et b, il ne peut donc s'agir que de 0.
Ainsi $r - r' = 0$ d'où $r = r'$.
D'autre part, $b(q - q') = 0$ donc $q = q'$.
Conclusion, le couple $(q;r)$ vérifiant la propriété est unique.

EXEMPLE

Effectuer la division euclidienne de 48 par 5 puis de -76 par 3.

REMARQUE

A la calculatrice, le quotient de a par b se fait par l'instruction **div**(a/b) et le reste de a par b par l'instruction **mod**(a,b).

EXERCICE

Soit $n \in \mathbb{N}$. Déterminer le reste dans la division euclidienne de $7n + 16$ par $2n + 3$.

2) Propriété

PROPRIÉTÉ — admise

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$.

1) b divise $a \iff$ le reste dans la division euclidienne de a par b est 0.

2) Dans la division euclidienne de a par b, il n' y a que b restes possibles : tous les entiers entre 0 et $b-1$. Ainsi, tout entier s'écrit sous une, et une seule, de ces formes : bq, $bq+1$, $bq+2$, ..., $bq+(b-1)$, avec $q \in \mathbb{Z}$.

EXEMPLE

Tous les nombres entiers s'écrivent sous la forme $3q$, $3q+1$ ou $3q+2$.

EXERCICE

Soit $n \in \mathbb{N}$. Démontrer que pour tout entier naturel n, $n(n^2+5)$ est divisible par 3.

III Congruences

1) Définition

DÉFINITION

Soit n un entier naturel non nul.
Deux entiers a et b sont dits congrus modulo n si et seulement si ils ont le même reste dans la division euclidienne par n.
On le note : $a \equiv b\,[n]$.

REMARQUES

- On le note aussi $a \equiv b\,(n)$ ou $a \equiv b\,(\text{mod } n)$
- On dit aussi que a est congru à b modulo n.
- Par définition, $a \equiv b\,[n] \iff b \equiv a\,[n]$ et $a \equiv a\,[n]$.
- Si r est le reste de la division euclidienne de a par n, alors $a \equiv [n]$ et r est l'unique entier tel que $0 \leqslant r < n$ et $a \equiv r\,[n]$.

EXEMPLES

- $11 \equiv 5\,[3]$ (car $11 = 3\times 3+2$ et $5 = 3\times 1+2$)
- $-4 \equiv 2\,[3]$ (car $-4 = 3\times(-2)+2$ et $2 = 3\times 0+2$)

2) Propriété fondamentale

PROPRIÉTÉ

Soient n un entier naturel non nul et a et b deux entiers relatifs.
$a \equiv b\,[n]$ si et seulement si n divise $a-b$.

DÉMONSTRATION

Démonstration (par double implication) :
• $\Rightarrow$ Si $a \equiv b\,[n]$, alors a et b ont le même reste r dans la division euclidienne par n, c'est-à-dire qu'il existe deux entiers relatifs q et q' tels que $a = nq + r$ et $b = nq' + r$.
Ainsi, $a - b = n(q - q')$, avec $q - q'$ entier, donc n divise $a - b$.
• $\Leftarrow$ Réciproquement, si n divise $a - b$, alors il existe un entier k tel que $a - b = kn$, d'où $a = b + kn$.
La division euclidienne de a par n se traduit par l'existence de deux entiers q et r tels que $a = nq + r$ et $0 \leqslant r < n$.
Ainsi, $b + kn = nq + r$ donc $b = n(q - k) + r$ avec $q - k$ entier et $0 \leqslant r < n$.
On en déduit que r est aussi le reste de la division euclidienne de b par n, soit $a \equiv b\,[n]$.

REMARQUE

$a \equiv 0\,[n]$ si et seulement si n divise a.

3) Opérations sur les congruences

PROPRIÉTÉS

Soient n et n deux entiers naturels non nuls.
Soient a, a', b, b' et c des entiers relatifs.
Alors on a les relations suivantes :

1) Si $a \equiv b\,[n]$ et $b \equiv c\,[n]$, alors $a \equiv c\,[n]$ (propriété de transitivité).

2) $a \equiv b\,[n]$ si et seulement si $a - b \equiv 0\,[n]$.

3) Si $a \equiv a'\,[n]$ et $b \equiv b'\,[n]$, alors $a + b \equiv a' + b'\,[n]$, $a - b \equiv a' - b'\,[n]$ et $ab \equiv a'b'\,[n]$.

4) Si $a \equiv b\,[n]$, alors $ac \equiv bc\,[n]$ et, pour tout $m \in \mathbb{N}^*$, $a^m \equiv b^m\,[n]$.

DÉMONSTRATION

1) Si $a \equiv b\,[n]$, alors $n|(a-b)$, et si $b \equiv c\,[n]$, alors $n|(b-c)$.
Ainsi, $n|(a+b)+(b-c)$, donc $n|(a-c)$ donc $a \equiv c\,[n]$.

2) $a \equiv b\,[n]$ si et seulement si $a-b$ est divisible par n, c'est-à-dire $a-b-0$ divisible par n, d'où $a-b \equiv 0\,[n]$.

3) Si $a \equiv a'\,[n]$ et $b \equiv b'\,[n]$, alors $a-a'$ et $b-b'$ sont des multiples de n, dont toute combinaison linéaire des deux est un multiple de n. Ainsi on a :
$(a-a')+(b-b') = (a+b)-(a'+b')$ est un multiple de n, donc $a+b \equiv a'+b'\,[n]$.
$(a-a')-(b-b') = (a-b)-(a'-b')$ est un multiple de n, donc $a-b \equiv a'-b'\,[n]$.
$(a-a')\times b+(b-'b)\times a' = ab-a'b+a'b-a'b' = ab-a'b'$ est un multiple de n, donc $ab \equiv a'b'\,[n]$.

4) $a \equiv b\,[n]$ donc $a-b$ est divisible par n
donc $c(a-b)$ est divisible par n
donc $ca-cb$ est divisible par n
donc $ca \equiv cb\,[n]$
donc $ac \equiv bc\,[n]$.
Démonstration par récurrence pour $a^m \equiv b^m\,[n]$: à faire en exo, utiliser $ab \equiv a'b'\,[n]$.

4) Applications

1) On donne $a \equiv 6\,[11]$ et $b \equiv 5\,[11]$.
  a) Déterminer le reste dans la division euclidienne par 11 de $2a+3b$, a^2+b^2 et ab.
  b) Montrer que a^2-b^2 est divisible par 11.

2) Montrer que pour tout entier naturel n, 7^n+3^n+2 est divisible par 4.

3) Montrer que 7305^3 et 7322^3 ont le même reste dans la division euclidienne par 17.

4) Déterminer le reste dans la division euclidienne par 7 de 25×2^{17}.

5) Déterminer le reste dans la division euclidienne par 13 de 124×3^{21}.

6) Déterminer le reste dans la division euclidienne par 11 de 2014^{21014}.

7) Déterminer le reste dans la division euclidienne par 11 de 2012^{2012}.

8) Déterminer le reste dans la division euclidienne par 17 de 2^{2013}.

9) Déterminer le reste dans la division euclidienne par 15 de 2^{2015}.

10) Montrer que $2^{11}+1$ est divisible par 3.

11) Montrer que $5^{10}+1$ est divisible par 13.

12) Déterminer le chiffre des unités de 11^{1000}.

13) Déterminer le chiffre des unités de 3^{1000}.

14) Déterminer le chiffre des unités de 2^{63}.

15) En étudiant les restes possibles de x dans la division euclidienne par 7, résoudre les équations suivantes :
  a) $3x \equiv 1\,[7]$.
  b) $5x \equiv 1\,[7]$.

5) Inverse

DÉFINITION

Soient a et n deux entiers avec $n \geqslant 2$.
On dit que a est **inversible modulo** n lorsqu'il existe un entier b tel que $ab \equiv 1[n]$.

EXEMPLES

1) Montrer que 3 est inversible modulo 5.

2) Montrer que 4 n'admet pas d'inverse modulo 6.

6) Critères de divisibilité

PROPRIÉTÉS

- Un entier naturel est divisible par 2 si son chiffre des unités est 0, 2, 4, 6 ou 8.
- Un entier naturel est divisible par 3 si la somme de ses chiffres est un nombre divisible par 3.
- Un entier naturel est divisible par 4 si le nombre formé de ses deux derniers chiffres est divisible par 4.
- Un entier naturel est divisible par 5 si son chiffre des unités est 0 ou 5.
- Un entier naturel est divisible par 9 si la somme de ses chiffres est un nombre divisible par 9.

DÉMONSTRATION

Démonstration pour 2 (identique pour les autres, leur faire faire) :
Soit N un entier naturel.
Alors $N = \overline{a_n a_{n-1} ... a_2 a_1 a_0}$, soit $N = a_n \times 10^n + a_{n-1} \times 10^{n-1} + ... + a_2 \times 10^2 + a_1 \times 10 + a_0$, avec n un entier naturel égal au nombre de chiffres de N et a_k un entier naturel compris entre 0 et 9.

$10 = 2 \times 5$ donc $10 \equiv 0\,[2]$ donc $10^k \equiv 0\,[2]$ pour tout k entre 0 et n.
Donc $a_k \times 10^k \equiv 0\,[2]$ pour tout k entre 0 et n.
Donc par somme, $N \equiv a_0\,[2]$.
Or a_0 est un entier compris entre 0 et 9. Donc $N \equiv 0\,[2] \Leftrightarrow a_0 \equiv 0\,[2] \Leftrightarrow a_0 \in \{0\,;2\,;4\,;6\,;8\}$.

IV PGCD de deux entiers naturels

1) Définition du PGCD

Soient a et b deux entiers naturels.
On notera dans cette partie $D(a)$ l'ensemble des diviseurs positifs de a et $D(a\,;b)$ l'ensemble des diviseurs positifs communs à a et b.

REMARQUES

- $D(a\,;b) \subset \mathbb{Z}$.
- $D(a\,;b) \neq \varnothing$ (car il contient au moins 1)
- $D(a\,;b)$ est majoré par $|a|$ donc il possède un plus grand élément.

DÉFINITION

Soient a et b deux entiers naturels non simultanément nuls.
On appelle PGCD$(a\,;b)$ le plus grand diviseur commun à a et à b.

EXEMPLE

Les diviseurs de 36 et 63 sont :
$D(36) = \{1;2;3;4;6;9;12;18;36\}$
$D(63) = \{1;3;7;9;21;63\}$
Donc le PGCD de 36 et 63 est PGCD(36 ; 63)=9.

2) Propriétés du PGCD

PROPRIÉTÉS

Soient a et b deux entiers naturels non simultanément nuls.

1) $D(a;b) = D(a) \cap D(b)$ est un ensemble fini et non vide. Il possède toujours un plus grand élément, le PGCD$(a\,;b)$.

2) $D(a;b) = D(b\,;a)$ et PGCD$(a\,;b)$=PGCD$(b\,;a)$.

3) $D(a\,;0) = D(a)$ et PGCD$(a\,;0)=a$.

4) Si b divise a, alors $D(b) \subset D(a)$ et PGCD$(a\,;b)=b$.

DÉMONSTRATION

1) Le nombre de diviseurs positifs de a est inférieur à a (il est compris entre 1 et a), donc $D(a\,;b)$ est un ensemble fini. De plus, 1 appartient à $D(a\,;b)$ qui n'est donc pas vide : il possède ainsi un plus grand élément.

2) évident.

3) L'ensemble des diviseurs de 0 est $D(0) = \mathbb{N}^*$ donc $D(a\,;0) = D(a) \cap D(0) = D(a)$. Le plus grand diviseur de a étant lui-même, PGCD$(a\,;0)=a$.

4) Si b divise a, tout diviseur de b est un diviseur de a, d'où $D(b) \subset D(a)$. On en déduit que $D(a\,;b) = D(a) \cap D(b) = D(b)$, et par suite PGCD$(a\,;b)$=b.

PROPRIÉTÉ

Soient a et b deux entiers naturels non nuls. En notant r le reste de la division euclidienne de a par b, on a alors $D(a\,;b) = D(b\,;r)$ et PGCD$(a\,;b)$=PGCD$(b\,;r)$.

DÉMONSTRATION

Soit q le quotient de la division euclidienne de a par b, on a $a = bq + r$.

Soit d un élément de $D(b\,;r)$. Comme d divise b et r, alors d divise $a = bq + r$, d'où $d \in D(a\,;b)$.
On en déduit que $D(b\,;r) \subset D(a\,;b)$.

Soit d un élément de $D(a;b)$. Comme d divise a et b, alors d divise $r = a - bq$, d'où $d \in D(b\,;r)$.
On en déduit que $D(a\,;b) \subset D(b\,;r)$.

En conclusion, $D(a\,;b) = D(b\,;r)$.
Il en découle directement que PGCD$(a\,;b)$=PGCD$(b\,;r)$.

EXEMPLE

En divisant 474 par 118, on obtient $474 = 118 \times 4 + 2$.
Ainsi, $D(474\,;118) = D(118\,;2)$ et PGCD$(474\,;118)$=PGCD$(118\,;2)$.
Or 2 divise 118 donc PGCD$(118\,;2)$=2 donc on peut en déduire que PGCD$(474\,;118)$=2.

3) L'algorithme d'Euclide

PROPRIÉTÉ

Soient a et b des entiers naturels non nuls.
L'algorithme d'Euclide consiste à effectuer la division euclidienne de a par b, puis les divisions euclidiennes successives du diviseur par le reste de chacune des divisions précédentes, jusqu'à ce que le reste soit nul.
Ce processus se termine toujours et le PGCD de a et b est alors le dernier reste non nul de l'algorithme.

DÉMONSTRATION

La suite (r_k) des restes est strictement décroissante car r_{k+1} est le reste dans la division euclidienne par r_k, donc $0 \leqslant r_{k+1} \leqslant r_k$.
D'après le principe de descente infinie, il existe donc un entier n tel que $r_{n+1} = 0$.
La propriété précédente justifie que :
$D(a\,;b) = D(b\,;r_0) = D(r_0\,;r_1) = \ldots = D(r_{n-1}\,;r_n) = D(r_n\,;0) = D(r_n)$.
On en déduit que le plus grand diviseur commun à a et b est r_n.

EXEMPLE

On applique l'algorithme d'Euclide pour calculer le PGCD de 364 et 247 :
$364 = 247 \times 1 + 117$.
$247 = 117 \times 2 + 13$.
$117 = 13 \times 9 + 0$.
On en déduit que PGCD$(364\,;247)$=13.

4) Conséquences

PROPRIÉTÉ

Soient a et b deux entiers naturels non nuls.
Les diviseurs communs de a et de b sont les diviseurs de leur PGCD.

DÉMONSTRATION

La démonstration est immédiate car la démonstration de la propriété précédente s'appuie sur le fait que $D(a\,;b) = D(r_n) = D(PGCD(a\,;b))$

PROPRIÉTÉS

Pour tous entiers naturels a, b et k :
- $\text{PGCD}(ka\,;kb) = k\times \text{PGCD}(a\,;b)$;
- Si k non nul tel que k divise a et b, alors $\text{PGCD}\left(\frac{a}{k}\,;\frac{b}{k}\right) = \frac{1}{k}\text{PGCD}(a\,;b)$.

DÉMONSTRATION

- Soit $G = \text{PGCD}(ka\,;kb)$ et $g = \text{PGCD}(a\,;b)$.
$g|a$ et $g|b$ donc $kg|ka$ et $kg|kb$, donc $kg|G$, donc $\exists \ell \in \mathbb{N}$ tel que $G = \ell kg$.
De plus, G divise ka et kb donc ℓkg divise ka et kb, donc ℓg divise a et b, donc ℓg divise g.
Ainsi, on a $\ell = 1$ et $G = kg$, c'est-à-dire $\text{PGCD}(ka\,;kb) = k\text{PGCD}(a\,;b)$.

- $\text{PGCD}(a\,;b) = \text{PGCD}\left(k\times\frac{a}{k}\,;k\times\frac{b}{k}\right)$, d'où le résultat à l'aide de la propriété précédente.

EXEMPLE

On peut ainsi simplifier le calcul de PGCD lorsqu'un facteur commun évident apparait :
$\text{PGCD}(170\,;210) = 10\times\text{PGCD}(17\,;21) = 10\times 1 = 10$

5) Nombres premiers entre eux

DÉFINITION

Soient a et b deux entiers relatifs non nuls.
On dit que a et b sont premiers entre eux si et seulement si leur PGCD vaut 1.

REMARQUE

Autrement dit, a et b sont premiers entre eux si et seulement si ils n'ont pas d'autres diviseurs communs que -1 et 1.

PROPRIÉTÉ

Soient a et b deux entiers naturels non nuls.
Si d=PGCD$(a\,;b)$, alors il existe deux nombres entiers naturels a' et b' premiers entre eux tels que $a = da'$ et $b = db'$.

DÉMONSTRATION

Si d=PGCD$(a\,;b)$, alors d divise a et b et il existe donc un entier naturel a' tel que $a = da'$ et un entier naturel b' tel que $b = db'$.
Donc d=PGCD$(a\,;b)$=PGCD$(da'\,;db')$=d $\times$ PGCD$(a'\,;b')$.
Or d est différent de 0 donc par simplification, on obtient 1 = PGCD$(a'\,;b')$.