

DIVISIBILITÉ ET CONGRUENCES

I. Divisibilité dans \mathbb{Z}

Définition : Soit a et b deux entiers relatifs.
 a **divise** b s'il existe un entier relatif k tel que $b = ka$.
 On dit également :
 - a est un **diviseur** de b ,
 - b est **divisible** par a ,
 - b est un **multiple** de a .

Notation : a divise b se note : $a | b$

Exemples :

- 56 est un multiple de -8 car $56 = -7 \times (-8)$
- L'ensemble des multiples de 5 sont $\{\dots ; -15 ; -10 ; -5 ; 0 ; 5 ; 10 ; \dots\}$. On note cet ensemble $5\mathbb{Z}$.
- L'ensemble des diviseurs de 6 sont $\{-6 ; -3 ; -2 ; -1 ; 1 ; 2 ; 3 ; 6\}$
- 0 est divisible par tout entier relatif.

Propriété (transitivité) : Soit a et b deux entiers relatifs avec b non nul.
 b divise $a \Leftrightarrow -b$ divise $a \Leftrightarrow b$ divise $-a \Leftrightarrow -b$ divise $-a$

Propriété (transitivité) : Soit a , b et c trois entiers relatifs.
 Si a divise b et b divise c alors a divise c .

Démonstration :

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

Donc $c = k'ka$ et donc il existe un entier relatif $l = kk'$ tel que $c = la$.

Donc a divise c .

Exemple :

- $3 | 12$ et $12 | 36$ donc $3 | 36$.
- 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.

Méthode : Appliquer la définition de la divisibilité (démonstration par l'absurde)

 **Vidéo** <https://youtu.be/z-CtTbP3RYA>

Démontrer que pour tout entier relatif n , le nombre $6n + 5$ n'est pas divisible par 3.

On va effectuer un raisonnement par l'absurde en supposant le contraire de ce qu'il faut démontrer.

Si notre démonstration aboutit à une « absurdité », une contradiction, cela prouvera que notre hypothèse de départ est fautive.

Supposons, *par l'absurde*, qu'il existe un entier relatif n , tel que $6n + 5$ soit divisible par 3.

Il existe alors un entier relatif k tel que $6n + 5 = 3k$.

Soit : $5 = 3k - 6n$, soit encore : $5 = 3(k - 2n)$.

Ce qui signifie que 5 est divisible par 3. C'est « absurde », donc l'hypothèse de départ est fautive.

Le nombre $6n + 5$ n'est pas divisible par 3

Propriété (combinaisons linéaires) : Soit a , b et c trois entiers relatifs.
Si c divise a et b alors c divise $ma + nb$ où m et n sont deux entiers relatifs.

Démonstration :

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

Donc $ma + nb = mkc + nk'c$ et donc il existe un entier relatif $l = mk + nk'$ tel que $ma + nb = lc$.

Exemple :

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 $N = 1$.

Méthode : Utiliser la propriété des combinaisons linéaires (démonstration avec réciproque)

 Vidéo <https://youtu.be/JGJ0VJV2Zgo>

Déterminer les entiers relatifs n , tels que $2n + 5$ divise $n - 1$.

• On a : $2n + 5 \mid 2n + 5$

Si $2n + 5 \mid n - 1$ et $2n + 5 \mid 2n + 5$, **alors** d'après la propriété des combinaisons linéaires : $2n + 5 \mid -2(n - 1) + 2n + 5$

Soit : $2n + 5 \mid -2n + 2 + 2n + 5$

Soit encore : $2n + 5 \mid 7$.

Les diviseurs de 7 sont : -7 ; -1 ; 1 et 7 .

Donc :

$2n + 5 = -7$ soit $n = -6$

$2n + 5 = -1$ soit $n = -3$

$2n + 5 = 1$ soit $n = -2$

$2n + 5 = 7$ soit $n = 1$

Les solutions possibles appartiennent à l'ensemble $\{-6 ; -3 ; -2 ; 1\}$.

L'idée est de fabriquer une combinaison linéaire de $n - 1$ et $2n + 5$ qui ne dépende plus de n .

Attention, il faut maintenant vérifier la réciproque. En effet, la propriété des combinaisons linéaires (si... alors...) donne une condition nécessaire pour avoir la divisibilité sur les combinaisons linéaires.

On a donc prouvé que, si $2n + 5$ divise $n - 1$, alors nécessairement n appartient à l'ensemble $\{-6 ; -3 ; -2 ; 1\}$. La question est maintenant de savoir s'il suffit de prendre une valeur dans cet ensemble pour que $2n + 5$ divise $n - 1$. Il faut donc prouver maintenant que si n appartient à l'ensemble $\{-6 ; -3 ; -2 ; 1\}$ alors $2n + 5$ divise $n - 1$.

• Si $n = -6$:

$2n + 5 = -7$ et $n - 1 = -7$. Or, $-7 \mid -7$, donc -6 est bien solution.

Si $n = -3$:

$2n + 5 = -1$ et $n - 1 = -4$. Or, $-1 \mid -4$, donc -3 est bien solution.

Si $n = -2$:

$2n + 5 = 1$ et $n - 1 = -3$. Or, $1 \mid -3$, donc -2 est bien solution.

Si $n = 1$:

$2n + 5 = 7$ et $n - 1 = 0$. Or, $7 \mid 0$, donc 1 est bien solution.

• Les solutions sont $-6, -3, -2$ et 1 .

II. Division euclidienne

Propriété : Soit a un entier naturel et b entier naturel non nul.

Il existe un unique couple d'entiers $(q ; r)$ tel que $a = bq + r$ avec $0 \leq r < b$.

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 :

Existence :

1^{er} cas : $0 \leq a < b$: Le couple $(q ; r) = (0 ; a)$ convient.

2^e cas : $b \leq a$: Soit E l'ensemble des multiples de b strictement supérieurs à a .

Alors E est non vide car l'entier $2b \times a$ appartient à E .

En effet $b \geq 1$ donc $2b \times a \geq 2a > a$.

E possède donc un plus petit élément c'est à dire un multiple de b strictement supérieur à a tel que le multiple précédent soit inférieur ou égal à a .

Il existe donc un entier q tel que $qb \leq a < (q + 1)b$.

Comme, $b \leq a$ on a : $b \leq a < (q + 1)b$.

Et comme $b > 0$, on a : $0 < (q + 1)b$ et donc $0 < q$.

q est donc un entier naturel.

On peut poser $r = a - bq$.

Or a, b et q sont des entiers, donc r est entier.

Comme $qb \leq a$, on a $r \geq 0$ donc r est donc un entier naturel.

Et comme $a < (q + 1)b$ on en déduit que $r < b$.

Unicité :

On suppose qu'il existe deux couples $(q ; r)$ et $(q' ; r')$.

$$\text{Donc } a = bq + r = bq' + r'.$$

$$\text{Et donc : } b(q - q') = r' - r.$$

Comme $q - q'$ est entier, $r' - r$ est un multiple de b .

On sait que $0 \leq r < b$ et $0 \leq r' < b$ donc $-b < -r \leq 0$ et $0 \leq r' < b$,
donc $-b < r' - r \leq b$.

Le seul multiple de b compris entre $-b$ et b est 0, donc $r' - r = 0$ et donc $r' = r$.

D'où $q = q'$.

Propriété : On peut étendre la propriété précédente au cas où a est un entier relatif.

- Admis -

Méthode : Déterminer le quotient et le reste d'une division euclidienne (1)

▶ **Vidéo** <https://youtu.be/bwS45UeOZrg>

Déterminer le quotient et le reste de la division de -5000 par 17 .

A l'aide de la calculatrice, on obtient :

$$\begin{array}{r} 5000 \div 17 \\ 294.1176471 \\ 5000 - 17 \times 294 \\ \hline 2 \end{array}$$

Ainsi : $5000 = 17 \times 294 + 2$

$$\text{Donc : } -5000 = 17 \times (-294) - 2$$

Le reste est un entier positif inférieur à 17 .

$$\text{Donc : } -5000 = 17 \times (-294) - 17 - 2 + 17$$

$$\text{Soit : } -5000 = 17 \times (-295) + 15$$

D'où, le quotient est -295 et le reste est 15 .

Méthode : Déterminer le quotient et le reste d'une division euclidienne (2)

▶ **Vidéo** <https://youtu.be/fv5uhr8JP3U>

Déterminer le quotient et le reste de la division de $5n + 11$ par $2n + 3$, avec n entier naturel.

- Pour tout entier naturel n , on a : $5n + 11 = 2(2n + 3) + n + 5$

On décompose $5n + 11$ en $Q(2n + 3) + R$.

On a choisi $Q = 2$ car 2 est le plus grand facteur entier tel que $5n + 11 \geq Q(2n + 3)$.

En effet, le produit du **diviseur** par le **quotient** ne doit pas dépasser le dividende, sinon le **reste** serait négatif !

La relation $5n + 11 = 2(2n + 3) + n + 5$ est la division euclidienne de $5n + 11$ par $2n + 3$ à condition que $0 \leq n + 5 < 2n + 3$, soit : $n > 2$ ou encore $n \geq 3$.

Ainsi, pour $n \geq 3$, dans la division euclidienne de $5n + 11$ par $2n + 3$, le quotient est 2 et le reste est $n + 5$.

- Reste donc à traiter les cas $n = 0, n = 1$ et $n = 2$

n	$5n + 11$	$2n + 3$	Quotient	Reste
0	11	3	3	2
1	16	5	3	1
2	21	7	3	0

Propriété : Soit un entier naturel b , tel que $b \geq 2$.

Alors, tout entier a s'écrit sous l'une des formes suivantes :

bq ou $bq + 1$ ou $bq + 2 \dots$ ou $bq + (b - 1)$, avec q entier relatif.

Exemples pour comprendre :

- En effectuant la division de a par 5, on a : $a = 5q + r$, avec $0 \leq r < 5$.

Ainsi, a peut s'écrire : $5q$ ou $5q + 1$ ou $5q + 2$ ou $5q + 3$ ou $5q + 4$.

- De même, a peut s'écrire : $2q$ ou $2q + 1$.

On retrouve ici, la notion de parité d'un nombre : un nombre est soit pair, soit impair.

Méthode : Effectuer une démonstration par disjonction des cas

 Vidéo <https://youtu.be/AEkdYp0Dqso>

Démontrer que pour tout entier naturel n , $n(n + 5)(n - 5)$ est divisible par 3.

Le raisonnement par disjonction de cas consiste à décomposer la proposition que l'on veut démontrer en différents cas qui seront vérifiés successivement.

On veut démontrer ici une divisibilité par 3, il peut donc être pertinent de décomposer l'entier n sous une des trois formes suivantes :

$n = 3q$ ou $n = 3q + 1$ ou $n = 3q + 2$, avec q entier relatif.

On a donc 3 cas possibles :

- Si $n = 3q$:

$n(n + 5)(n - 5) = 3q(3q + 5)(3q - 5)$ donc $n(n + 5)(n - 5)$ est divisible par 3.

- Si $n = 3q + 1$:

$n(n + 5)(n - 5) = (3q + 1)(3q + 1 + 5)(3q + 1 - 5)$
 $= (3q + 1)(3q + 6)(3q - 4)$
 $= 3(3q + 1)(q + 2)(3q - 4)$ donc $n(n + 5)(n - 5)$ est divisible par 3.

- Si $n = 3q + 2$:

$n(n + 5)(n - 5) = (3q + 2)(3q + 2 + 5)(3q + 2 - 5)$
 $= (3q + 2)(3q + 7)(3q - 3)$
 $= 3(3q + 2)(3q + 7)(q - 1)$ donc $n(n + 5)(n - 5)$ est divisible par 3.

Ainsi, pour tout entier naturel n , $n(n + 5)(n - 5)$ est divisible par 3.

III. Congruences dans \mathbb{Z}

1) Définition

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 : Soit n un entier naturel non nul.

Deux entiers a et b sont congrus modulo n lorsque $a - b$ est divisible par n .

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

Propriété : 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 :

- 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 $-n < -r \leq 0$ et $0 \leq r' < n$

Et donc $-n < r' - r \leq n$.

$r - r'$ est un multiple de n 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.

Méthode : Écrire avec des congruences

 Vidéo <https://youtu.be/BTCsGN6xwXg>

 Vidéo <https://youtu.be/wdFNCnSflgE>

1) Compléter : $13 \equiv \dots [5]$ $45 \equiv \dots [3]$ $-8 \equiv \dots [12]$

2) Démontrer que : $214 \equiv 25[9]$

1) – Les solutions sont multiples, la plus simple consisterait à écrire $13 \equiv 13[5]$!

Ce n'est évidemment pas satisfaisant, on privilégiera la recherche d'un entier naturel r tel que $13 \equiv r[5]$ avec $0 \leq r < 5$ (en référence à la division euclidienne).

En effet, si r est le reste de la division de 13 par 5, alors on a : $13 \equiv r[5]$.

$13 \equiv r[5]$ signifie que $13 = r + 5k$, soit $r = 13 - 5k$, $k \in \mathbb{Z}$.
 On cherche donc un entier relatif k , tel que $0 \leq 13 - 5k < 5$.
 En prenant $k = 2$, on a : $r = 13 - 5k = 13 - 5 \times 2 = 3$.
 Ainsi : $13 \equiv 3[5]$.

– On cherche r , tel que $45 \equiv r[3]$ et $0 \leq r < 3$.
 $45 \equiv r[3]$ signifie que $r = 45 - 3k$, $k \in \mathbb{Z}$.
 Avec $k = 15$, on trouve $r = 0$.
 Ainsi : $45 \equiv 0[3]$.

– On cherche r , tel que $-8 \equiv r[12]$ et $0 \leq r < 12$.
 $-8 \equiv r[12]$ signifie que $r = -8 - 12k$, $k \in \mathbb{Z}$.
 Avec $k = -1$, on trouve $r = 4$.
 Ainsi : $-8 \equiv 4[12]$.

2) $214 \equiv 25[9]$ signifie qu'il existe un entier relatif k , tel que $214 - 25 = 9k$.
 C'est vrai !
 En effet, $k = 21$ convient : $214 - 25 = 189 = 21 \times 9$.

2) Propriétés sur les congruences

Propriétés : Soit n un entier naturel non nul.

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

b) Si $a \equiv b[n]$ et $b \equiv c[n]$ alors $a \equiv c[n]$ (Relation de transitivité)

Démonstration :

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

b) $a \equiv b[n]$ et $b \equiv c[n]$ donc n divise $a - b$ et $b - c$ donc n divise $a - b + b - c = a - c$.

Propriété (Opérations) : Soit n un entier naturel non nul.

Soit a, b, a' et b' des nombres relatifs tels que $a \equiv b[n]$ et $a' \equiv b'[n]$ alors on a :

- $a + a' \equiv b + b'[n]$
- $a - a' \equiv b - b'[n]$
- $a \times a' \equiv b \times b'[n]$
- $a^p \equiv b^p[n]$ avec $p \in \mathbb{N}$.

Démonstration de la dernière relation :

• **Initialisation :** La démonstration est triviale pour $p = 0$ ou $p = 1$

• **Hérédité :**

- **Hypothèse de récurrence :**

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

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

• **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 :

- $7 + 11 \equiv 4 + 20[3] \equiv 24[3] \equiv 0[3]$ et on a alors $18 \equiv 0[3]$

- $7 \times 11 \equiv 4 \times 20[3] \equiv 80[3] \equiv 2[3]$ et on a alors $77 \equiv 2[3]$

Attention la réciproque est fautive :

Si $k \times a \equiv k \times b[n]$, on n'a pas nécessairement $a \equiv b[n]$.

Méthode : Appliquer les propriétés sur les congruences

 Vidéo https://youtu.be/4RRjMC8_Dio

Compléter le tableau :

a	$\equiv 1[4]$	$\equiv -1[7]$	$\equiv 1[10]$
b	$\equiv 2[4]$	$\equiv 4[7]$	$\equiv -5[10]$
$a + b$	$\equiv \dots [4]$	$\equiv \dots [7]$	$\equiv \dots [10]$
$a - b$	$\equiv \dots [4]$	$\equiv \dots [7]$	$\equiv \dots [10]$
a^2	$\equiv \dots [4]$	$\equiv \dots [7]$	$\equiv \dots [10]$
$4b$	$\equiv \dots [4]$	$\equiv \dots [7]$	$\equiv \dots [10]$
$a^2 + 4b - 6$	$\equiv \dots [4]$	$\equiv \dots [7]$	$\equiv \dots [10]$

a	$\equiv 1[4]$	$\equiv -1[7]$	$\equiv 1[10]$
b	$\equiv 2[4]$	$\equiv 4[7]$	$\equiv -5[10]$
$a + b$	$\equiv 1 + 2[4] \equiv 3[4]$	$\equiv 3[7]$	$\equiv 6[10]$
$a - b$	$\equiv 1 - 2[4] \equiv -1[4]$ $\equiv 3[4]$	$\equiv 2[7]$	$\equiv 6[10]$
a^2	$\equiv 1^2[4] \equiv 1[4]$	$\equiv 1[7]$	$\equiv 1[10]$
$4b$	$\equiv 4 \times 2[4] \equiv 8[4]$ $\equiv 0[4]$	$\equiv 2[7]$	$\equiv 0[10]$
$a^2 + 4b - 6$	$\equiv 1 + 0 - 6[4]$ $\equiv -5[4] \equiv 3[4]$	$\equiv 4[7]$	$\equiv 5[10]$

3) Exemples d'applicationMéthode : Résoudre une équation avec des congruences

 Vidéo <https://youtu.be/Hb39SqG6nbq>

 Vidéo https://youtu.be/aTn05hp_b7l

a) Déterminer les entiers x tels que $6 + x \equiv 5[3]$

b) Déterminer les entiers x tels que $3x \equiv 5[4]$

a) $6 + x \equiv 5[3]$

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

$$x \equiv -1[3]$$

$$x \equiv 2[3]$$

Les entiers x solutions sont tous les entiers de la forme $2 + 3k$ avec $k \in \mathbb{Z}$.

b) $3x \equiv 5[4]$ donc $3x \equiv 1[4]$

Or x est nécessairement congru à l'un des entiers 0, 1, 2 ou 3 modulo 4.

Par disjonction des cas, on a :

x modulo 4	0	1	2	3
$3x$ modulo 4	0	3	2	1

Donc $3 \times 3 \equiv 1[4]$. On en déduit que $x \equiv 3[4]$.

Les entiers x solutions sont tous les entiers de la forme $3 + 4k$ avec $k \in \mathbb{Z}$.

Méthode : Démontrer une divisibilité à l'aide des congruences

 Vidéo https://youtu.be/ZzIPFO59_t0

Démontrer que pour tout entier naturel n , $n(n+5)(n-5)$ est divisible par 3.

On retrouve le même exercice (résolu ici à l'aide des congruences) que celui proposé dans le paragraphe II.

On veut démontrer ici une divisibilité par 3, il peut donc être pertinent d'écrire n à l'aide de modulo 3 :

$$n \equiv 0[3] \text{ ou } n \equiv 1[3] \text{ ou } n \equiv 2[3]$$

On a donc 3 cas possibles, on va effectuer la démonstration par disjonction des cas en présentant les calculs dans un tableau :

$n \equiv 0[3]$	$n \equiv 1[3]$	$n \equiv 2[3]$
$n + 5 \equiv 2[3]$	$n + 5 \equiv 0[3]$	$n + 5 \equiv 1[3]$
$n - 5 \equiv 1[3]$	$n - 5 \equiv 2[3]$	$n - 5 \equiv 0[3]$
$n(n+5)(n-5) \equiv 0[3]$	$n(n+5)(n-5) \equiv 0[3]$	$n(n+5)(n-5) \equiv 0[3]$

Ainsi, pour tout entier naturel n , $n(n+5)(n-5)$ est divisible par 3.

Méthode : Déterminer le reste d'une division euclidienne à l'aide de congruences

 Vidéo <https://youtu.be/uVS-oeibDJ4>

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

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

a) Toute puissance de 2 est égale à 1. On cherche donc à faire apparaître une puissance de 2 qui est égale à 1 modulo 5.

On choisit alors de décomposer 456 à l'aide du facteur 4 car $2^4 \equiv 16 \equiv 1[5]$.

$$\begin{aligned} 2^{456} &\equiv 2^{4 \times 114}[5] \\ &\equiv (2^4)^{114}[5] \end{aligned}$$

On applique la formule de congruence des puissances : $(2^4)^{114} \equiv 1^{114}[5]$

$$\begin{aligned} 2^{456} &\equiv 1^{114}[5] \\ &\equiv 1[5] \end{aligned}$$

Le reste est égal à 1.

b) On cherche donc une puissance de 2 qui est égale à 1 modulo 7.

On choisit alors de décomposer 437 à l'aide du facteur 3 car $2^3 \equiv 8 \equiv 1[7]$.

$$\begin{aligned} 2^{437} &\equiv 2^{3 \times 145 + 2} [7] \\ &\equiv (2^3)^{145} \times 2^2 [7] \\ &\equiv 1^{145} \times 4 [7] \\ &\equiv 4 [7] \end{aligned}$$

Le reste est égal à 4.

Étude d'un problème de chiffrement : Appliquer un codage (Cryptographie) :

 Vidéo <https://youtu.be/GC7IFz4WGsc>



Hors du cadre de la classe, aucune reproduction, même partielle, autres que celles prévues à l'article L 122-5 du code de la propriété intellectuelle, ne peut être faite de ce site sans l'autorisation expresse de l'auteur.

www.maths-et-tiques.fr/index.php/mentions-legales