Terminale Maths expertes

Divisibilité, division euclidienne et congruences

Cours

Dans tout le chapitre, les lettres a, b, c, k, n, q, r… désignent des **entiers relatifs**. On rappelle que $\mathbb{N} = \{0\,;1\,;2\,;\dots\}$ et $\mathbb{Z} = \{\dots\,;-2\,;-1\,;0\,;1\,;2\,;\dots\}$.

I. Divisibilité dans $\mathbb{Z}$

1. Multiples et diviseurs

Définition 1 : multiple, diviseur

Soit a et b deux entiers relatifs. On dit que b **divise** a s'il existe un entier relatif k tel que

$$a = k\,b.$$

On dit aussi que a est un **multiple** de b, que a est **divisible** par b, ou que b est un **diviseur** de a. On note $b \mid a$ (et $b \nmid a$ si b ne divise pas a).

L'ensemble des multiples de b est noté $b\mathbb{Z} = \{kb\ ;\ k \in \mathbb{Z}\}$.

Exemples :

- $-14 = 7 \times (-2)$: donc $7 \mid -14$; -14 est un multiple de 7.
- Les diviseurs de 10 dans $\mathbb{N}$ sont 1, 2, 5 et 10.
- Les diviseurs de 26 dans $\mathbb{Z}$ sont -26, -13, -2, -1, 1, 2, 13 et 26.
- $3\mathbb{Z} = \{\dots\,;-9\,;-6\,;-3\,;0\,;3\,;6\,;9\,;\dots\}$ est l'ensemble des multiples de 3.
- $4 \nmid 10$: en effet $\dfrac{10}{4} = 2{,}5$ n'est pas un entier.

Remarques :

- $b \mid a \iff -b \mid a \iff b \mid -a$: un entier et son opposé ont les mêmes diviseurs ; on se ramène souvent aux diviseurs positifs.
- Pour $b \neq 0$: $b \mid a \iff \dfrac{a}{b} \in \mathbb{Z}$.
- $0 \mid a$ signifie $a = k \times 0 = 0$: **le seul multiple de** 0 **est** 0.
- **Attention :** « $b \mid a$ » est une **affirmation** (vraie ou fausse), et non un nombre : ne pas la confondre avec la fraction $\frac{b}{a}$.

2. Premières propriétés

Propriété 1 : premières propriétés

Soit a, b et c trois entiers relatifs.

a. 0 est un multiple de tout entier ; 1 et -1 divisent tout entier ; tout entier se divise lui-même.

b. Si $b \mid a$ et $a \neq 0$, alors $|b| \leqslant |a|$. Un entier non nul n'a donc qu'un nombre fini de diviseurs, tous compris entre $-|a|$ et $|a|$.

c. **Transitivité :** si $a \mid b$ et $b \mid c$, alors $a \mid c$.

d. Si $a \mid b$ et $b \mid a$, alors $a = b$ ou $a = -b$.

Démonstration

a. $0 = 0 \times a$; $a = a \times 1 = (-a) \times (-1)$; $a = 1 \times a$.

b. Il existe $k \in \mathbb{Z}$ tel que $a = kb$. Comme $a \neq 0$, on a $k \neq 0$; or k est un entier, donc $|k| \geqslant 1$. Par conséquent :

$$|a| = |k| \times |b| \geqslant 1 \times |b| = |b|.$$

c. Il existe $k \in \mathbb{Z}$ tel que $b = ka$ et $k' \in \mathbb{Z}$ tel que $c = k'b$. Alors $c = k'(ka) = (k'k)\,a$, avec $k'k \in \mathbb{Z}$: donc $a \mid c$.

d. Si $a = 0$: $a \mid b$ donne $b = k \times 0 = 0$, donc $a = b$.
Si $a \neq 0$: il existe $k, k' \in \mathbb{Z}$ tels que $b = ka$ et $a = k'b$. Alors $a = k'ka$, et en simplifiant par $a \neq 0$: $kk' = 1$. Deux entiers dont le produit vaut 1 sont tous deux égaux à 1 ou tous deux égaux à -1. Donc $b = a$ ou $b = -a$.

Exemples :

• $5 \mid 10$ et $10 \mid 90$, donc $5 \mid 90$ (transitivité).
• $3 \nmid 121$; donc aucun multiple de 3 ne divise 121 : si par exemple 6 divisait 121, comme $3 \mid 6$, on aurait $3 \mid 121$ par transitivité, ce qui est faux.

3. Combinaisons linéaires

Propriété 2 : combinaisons linéaires

Soit a, b et c trois entiers relatifs. Si $c \mid a$ et $c \mid b$, alors pour tous entiers relatifs u et v :

$$c \mid au + bv.$$

En particulier, c divise $a + b$ et $a - b$.

Démonstration

Il existe $k, k' \in \mathbb{Z}$ tels que $a = kc$ et $b = k'c$. Pour tous $u, v \in \mathbb{Z}$:

$$au + bv = kcu + k'cv = (ku + k'v)\,c \quad \text{avec} \quad ku + k'v \in \mathbb{Z}.$$

Donc c divise $au + bv$. Avec $u = v = 1$, puis $u = 1$ et $v = -1$, on obtient $c \mid a + b$ et $c \mid a - b$.

Remarques : conséquences utiles

• Si $c \mid a$ et $c \mid a + b$, alors $c \mid b$, car $b = (a + b) - a$.
• Si un entier N divise deux entiers consécutifs n et $n + 1$, alors N divise $(n + 1) - n = 1$: donc $N = 1$ ou $N = -1$.
• Si d divise $3n + 5$ et $2n + 3$, alors d divise $2(3n + 5) - 3(2n + 3) = 1$, donc $d = \pm 1$.

Méthode 1 : faire apparaître une combinaison linéaire

Énoncé. Déterminer tous les entiers relatifs n tels que $n - 2$ divise $n + 7$.

Solution. Pour $n = 2$, $n - 2 = 0$ ne divise pas 9 (le seul multiple de 0 est 0) : $n = 2$ ne convient pas.
On écrit $n + 7 = (n - 2) + 9$. Comme $n - 2$ divise $n - 2$:
• si $n - 2 \mid n + 7$, alors $n - 2$ divise $(n + 7) - (n - 2) = 9$;
• réciproquement, si $n - 2 \mid 9$, alors $n - 2$ divise $(n - 2) + 9 = n + 7$.
Donc $n - 2 \mid n + 7 \iff n - 2 \mid 9 \iff n - 2 \in \{-9\,;-3\,;-1\,;1\,;3\,;9\}$, soit $n \in \{-7\,;-1\,;1\,;3\,;5\,;11\}$.

Méthode 2 : factoriser pour utiliser les diviseurs

Énoncé. Déterminer tous les couples d'entiers naturels $(x\,;y)$ tels que $x^2 - xy = 35$.

Solution. L'équation s'écrit $x(x-y) = 35$. Donc x est un diviseur positif de 35 : $x \in \{1\,;5\,;7\,;35\}$, et $x - y = \dfrac{35}{x}$, soit $y = x - \dfrac{35}{x}$.

x	1	5	7	35
$x - y = \frac{35}{x}$	35	7	5	1
$y = x - \frac{35}{x}$	-34	-2	2	34
convient ?	non	non	oui	oui

Les solutions sont $(7\,;2)$ et $(35\,;34)$ (vérification : $49 - 14 = 35$ et $1225 - 1190 = 35$).

II. Division euclidienne

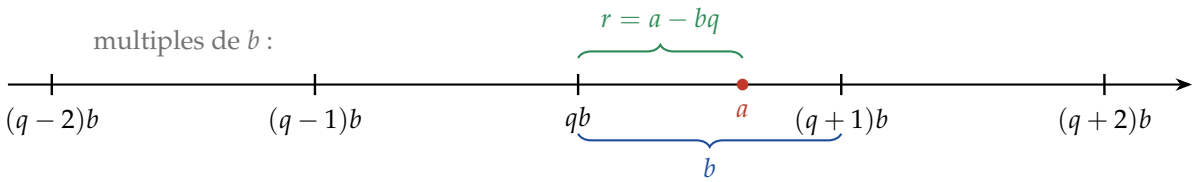
1. Le théorème

Théorème 1 : division euclidienne

Soit a un entier relatif et b un entier naturel non nul. Il existe un **unique** couple d'entiers relatifs $(q\,;r)$ tel que

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

q est le **quotient** et r le **reste** de la division euclidienne de a (le dividende) par b (le diviseur).



qb est le plus grand multiple de b inférieur ou égal à a : $qb \leqslant a < (q+1)b$, donc $0 \leqslant r < b$.

Exemples :

- $412 = 15 \times 27 + 7$ avec $0 \leqslant 7 < 15$: le quotient de 412 par 15 est 27 et le reste est 7.
- $230 = 17 \times 13 + 9$ traduit à la fois la division de 230 par 17 (reste $9 < 17$) et celle de 230 par 13 (reste $9 < 13$).
- $100 = 7 \times 13 + 9$ n'est **pas** la division euclidienne de 100 par 7, car $9 \geqslant 7$; celle-ci s'écrit $100 = 7 \times 14 + 2$.

2. Démonstration du théorème

On admet la propriété fondamentale suivante de $\mathbb{N}$: **toute partie non vide de $\mathbb{N}$ admet un plus petit élément.**

Démonstration : existence lorsque $a \geqslant 0$

On considère l'ensemble $E = \{k \in \mathbb{N} \ : \ kb > a\}$ des entiers naturels k dont le multiple kb dépasse strictement a.

- E n'est pas vide : comme $b \geqslant 1$, on a $(a+1)b \geqslant a + 1 > a$, donc $a + 1 \in E$.
- E admet donc un plus petit élément m. On a $m \neq 0$ car $0 \times b = 0 \leqslant a$, donc $0 \notin E$. Ainsi $m \geqslant 1$ et on pose $q = m - 1 \in \mathbb{N}$.
- $q < m$, donc $q \notin E$ (sinon m ne serait pas le plus petit élément) : $qb \leqslant a$. Et $m = q + 1 \in E$: $a < (q+1)b$.

On a donc $qb \leqslant a < qb + b$. On pose $r = a - bq$: c'est un entier, et en retranchant qb on obtient $0 \leqslant r < b$.

Démonstration : existence lorsque $a < 0$

Comme $-a > 0$, d'après le cas précédent il existe q' et r' entiers tels que $-a = bq' + r'$ avec $0 \leqslant r' < b$. Alors $a = b(-q') - r'$.
• Si $r' = 0$: $a = b(-q') + 0$ et le couple $(q\,;r) = (-q'\,;0)$ convient.
• Si $r' > 0$: on écrit $a = b(-q') - b + b - r' = b(-q' - 1) + (b - r')$. Comme $0 < r' < b$, on a $0 < b - r' < b$: le couple $(q\,;r) = (-q' - 1\,;b - r')$ convient.

Démonstration : unicité

Supposons que $a = bq + r = bq' + r'$ avec $0 \leqslant r < b$ et $0 \leqslant r' < b$. Alors $b(q - q') = r' - r$: $r' - r$ est un multiple de b.
De $0 \leqslant r' < b$ et $-b < -r \leqslant 0$ on tire, en additionnant : $-b < r' - r < b$.
Or le seul multiple de b strictement compris entre $-b$ et b est 0. Donc $r' - r = 0$, soit $r' = r$; puis $b(q - q') = 0$ avec $b \neq 0$, donc $q = q'$.

Méthode 3 : division euclidienne d'un entier négatif

Énoncé. Déterminer le quotient et le reste de la division euclidienne de $-5\,000$ par 17.

Solution. La calculatrice donne $5\,000 = 17 \times 294 + 2$, donc $-5\,000 = 17 \times (-294) - 2$.
Ce n'est pas la division euclidienne, car le « reste » -2 est négatif. On ajoute et on retranche 17 :

$$-5\,000 = 17 \times (-294) - 17 + 17 - 2 = 17 \times (-295) + 15 \qquad \text{avec} \qquad 0 \leqslant 15 < 17.$$

Le quotient est -295 et le reste est 15. (En Python, `-5000 // 17` renvoie `-295` et `-5000 % 17` renvoie `15`.)

3. Conséquences

Propriété 3 : divisibilité et reste

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

a. b divise a si et seulement si le reste de la division euclidienne de a par b est nul.

b. Tout entier a s'écrit d'une et d'une seule façon sous la forme bq, $bq + 1$, … ou $bq + (b - 1)$.
Exemples : tout entier est de la forme $2k$ (pair) ou $2k + 1$ (impair) ; de la forme $3k$, $3k + 1$ ou $3k + 2$.

Démonstration

a. Si $r = 0$, $a = bq$ et $b \mid a$. Réciproquement, si $a = bk$, alors $a = bk + 0$ avec $0 \leqslant 0 < b$: par unicité, $q = k$ et $r = 0$.
b. C'est le théorème : le reste r existe, est unique et prend l'une des b valeurs $0, 1, \ldots, b - 1$.

Python

```
def division(a, b):
    """division euclidienne de a >= 0
       par b >= 1, par soustractions"""
    q, r = 0, a
    while r >= b:
        r = r - b
        q = q + 1
    return q, r

print(division(412, 15))   # (27, 7)
```

Algorithme. Pour $a \geqslant 0$, on retranche b à a autant de fois que possible : le nombre de soustractions est le quotient q, ce qui reste est r.

En Python, les opérateurs `a // b` et `a % b` donnent directement le quotient et le reste de la division euclidienne de a par $b > 0$, **même si a est négatif**. La fonction `divmod(a, b)` renvoie le couple `(q, r)`.

Méthode 4 : raisonner par disjonction des cas

Énoncé. Démontrer que le carré de tout entier impair est de la forme $8k+1$ avec $k \in \mathbb{Z}$.

Solution. Soit n impair : $n = 2p+1$ avec $p \in \mathbb{Z}$. Alors $n^2 = 4p^2+4p+1 = 4p(p+1)+1$.
Le produit $p(p+1)$ est pair : si p est pair, $p = 2j$ et $p(p+1) = 2j(p+1)$; si p est impair, $p+1 = 2j$ et $p(p+1) = 2pj$. Dans les deux cas $p(p+1) = 2k$ avec $k \in \mathbb{Z}$, d'où $n^2 = 4\times 2k+1 = 8k+1$.
Exemples : $3^2 = 9 = 8\times 1+1$, $7^2 = 49 = 8\times 6+1$, $(-5)^2 = 25 = 8\times 3+1$.

III. Congruences dans $\mathbb{Z}$

1. Définition

On considère les nombres 1, 6, 11, 16, 21, 26, 31, 36. La différence de deux quelconques d'entre eux est divisible par 5 ; par exemple $21-6 = 15$. On dit que 21 et 6 sont **congrus modulo** 5.

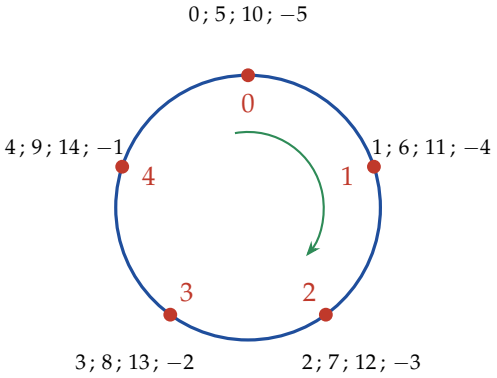
Définition 2 : congruence

Soit n un entier naturel non nul. Deux entiers relatifs a et b sont **congrus modulo** n lorsque $a-b$ est divisible par n, c'est-à-dire lorsqu'il existe $k \in \mathbb{Z}$ tel que $a = b+kn$. On note :

$$a \equiv b\ [n] \qquad \text{(on lit : « } a \text{ est congru à } b \text{ modulo } n \text{ »).}$$

Exemples :

- $21 \equiv 6\ [5]$ car $21-6 = 15 = 3\times 5$.
- $17 \equiv -3\ [10]$ car $17-(-3) = 20 = 2\times 10$.
- $100 \equiv 1\ [9]$ car $100-1 = 99 = 11\times 9$.
- $a \equiv 0\ [n]$ signifie que n divise a.
- Modulo 1, tous les entiers sont congrus : on prend en pratique $n \geqslant 2$.
- Les heures d'une horloge se lisent modulo 12 : 15 h et 3 h occupent la même position car $15 \equiv 3\ [12]$.



Modulo 5, on « enroule » $\mathbb{Z}$ sur un cercle à 5 positions : les entiers placés au même endroit sont congrus.

2. Congruence et reste

Théorème 2 : caractérisation par le reste

Soit $n \in \mathbb{N}^*$. Deux entiers a et b sont congrus modulo n si et seulement si les divisions euclidiennes de a et de b par n ont le **même reste**.

Démonstration

On écrit les divisions euclidiennes : $a = nq+r$ et $b = nq'+r'$, avec $0 \leqslant r < n$ et $0 \leqslant r' < n$. Alors

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

- Si $r = r'$: $a-b = n(q-q')$ est divisible par n, donc $a \equiv b\ [n]$.
- Si $a \equiv b\ [n]$: n divise $a-b$ et $n(q-q')$, donc n divise leur différence $r-r'$ (propriété 2).

De $0 \leqslant r < n$ et $-n < -r' \leqslant 0$ on tire $-n < r-r' < n$. Le seul multiple de n strictement compris entre $-n$ et n est 0 : donc $r = r'$.

Propriété 4 : conséquences

Soit $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$.

a. Si r est le reste de la division euclidienne de a par n, alors $a \equiv r\ [n]$.

b. a est congru modulo n à **un et un seul** entier de $\{0\,;1\,;\ldots\,;n-1\}$: son reste.

c. Si $a \equiv r\ [n]$ avec $0 \leqslant r < n$, alors r est le reste de la division euclidienne de a par n.

Démonstration

a. $a = nq + r$ donne $a - r = nq$: n divise $a - r$.
b. et c. D'après a., a est congru à son reste $r \in \{0\,;\ldots\,;n-1\}$. Si $a \equiv r'\ [n]$ avec $0 \leqslant r' < n$, alors r' a le même reste que a (théorème 2) ; or le reste de r' dans la division par n est r' lui-même ($r' = n \times 0 + r'$). Donc $r' = r$.

Exemple :

$21 \equiv 6\ [5]$ et, en effet, $21 = 5 \times 4 + 1$ et $6 = 5 \times 1 + 1$ ont le même reste 1. De même, $-5\,000 \equiv 15\ [17]$ (méthode 3).

3. Propriétés de la relation de congruence

Propriété 5 : une relation d'équivalence

Soit $n \in \mathbb{N}^*$ et a, b, c des entiers relatifs.

a. Réflexivité : $a \equiv a\ [n]$.

b. Symétrie : si $a \equiv b\ [n]$, alors $b \equiv a\ [n]$.

c. Transitivité : si $a \equiv b\ [n]$ et $b \equiv c\ [n]$, alors $a \equiv c\ [n]$.

Démonstration

a. $a - a = 0 = 0 \times n$ est divisible par n.
b. Si $n \mid a - b$, alors $n \mid -(a-b) = b - a$.
c. n divise $a - b$ et $b - c$, donc n divise leur somme $(a-b) + (b-c) = a - c$ (propriété 2).

Propriété 6 : compatibilité avec les opérations

Soit $n \in \mathbb{N}^*$ et a, b, a', b' des entiers relatifs tels que $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$. Alors :

$$a + a' \equiv b + b'\ [n] \qquad a - a' \equiv b - b'\ [n] \qquad aa' \equiv bb'\ [n]$$
$$ka \equiv kb\ [n] \text{ pour tout } k \in \mathbb{Z} \qquad a^p \equiv b^p\ [n] \text{ pour tout } p \in \mathbb{N}.$$

Démonstration : somme, différence, produit

Par hypothèse, n divise $a - b$ et $a' - b'$.
Somme et différence. $(a + a') - (b + b') = (a - b) + (a' - b')$ et
$(a - a') - (b - b') = (a - b) - (a' - b')$ sont des combinaisons linéaires de $a - b$ et $a' - b'$: elles sont divisibles par n.
Produit. On fait apparaître $a - b$ et $a' - b'$ en ajoutant et retranchant ab' :

$$aa' - bb' = aa' - ab' + ab' - bb' = a(a' - b') + b'(a - b),$$

combinaison linéaire de $a' - b'$ et $a - b$: elle est divisible par n, donc $aa' \equiv bb'\ [n]$.
Produit par k. On applique le résultat précédent avec $a' = b' = k$ (on a bien $k \equiv k\ [n]$).

Démonstration : compatibilité avec les puissances

On démontre par récurrence sur $p \in \mathbb{N}$ la propriété $\mathcal{P}(p)$: « $a^p \equiv b^p\ [n]$ ».
• *Initialisation :* $a^0 = 1$ et $b^0 = 1$, donc $a^0 \equiv b^0\ [n]$: $\mathcal{P}(0)$ est vraie.
• *Hérédité :* supposons $\mathcal{P}(p)$ vraie pour un entier $p \geqslant 0$, c'est-à-dire $a^p \equiv b^p\ [n]$. Comme $a \equiv b\ [n]$, la compatibilité avec le produit donne $a^p \times a \equiv b^p \times b\ [n]$, soit $a^{p+1} \equiv b^{p+1}\ [n]$: $\mathcal{P}(p+1)$ est vraie.
• *Conclusion :* $\mathcal{P}(0)$ est vraie et la propriété est héréditaire ; d'après le principe de récurrence, $a^p \equiv b^p\ [n]$ pour tout $p \in \mathbb{N}$.

Exemples :

$7 \equiv 1\ [3]$ et $11 \equiv 2\ [3]$, donc : $7 + 11 \equiv 1 + 2 = 3 \equiv 0\ [3]$ (en effet $18 = 3 \times 6$) ; $7 \times 11 \equiv 1 \times 2 = 2\ [3]$ (en effet $77 = 3 \times 25 + 2$) ;
et comme $11 \equiv -1\ [3]$: $11^{2026} \equiv (-1)^{2026} = 1\ [3]$.

Attention

• **On ne simplifie pas une congruence :** $2 \times 3 \equiv 2 \times 1\ [4]$ (car $6 - 2 = 4$), mais $3 \not\equiv 1\ [4]$.
• Un produit peut être congru à 0 sans qu'aucun facteur ne le soit : $2 \times 3 \equiv 0\ [6]$, alors que $2 \not\equiv 0\ [6]$ et $3 \not\equiv 0\ [6]$.
• **On ne remplace pas un exposant par un entier congru :** $5 \equiv 0\ [5]$, mais $2^5 = 32 \equiv 2\ [5]$ alors que $2^0 = 1$.

IV. Applications des congruences

Méthode 5 : reste d'une grande puissance

Principe. On cherche une puissance a^k congrue à 1 (ou à -1) modulo n, puis on divise l'exposant par k.

a. Reste de la division de 2^{456} par 5. $2^4 = 16 \equiv 1\ [5]$ et $456 = 4 \times 114$, donc

$$2^{456} = \left(2^4\right)^{114} \equiv 1^{114} = 1\ [5]. \qquad \text{Le reste est 1.}$$

b. Reste de la division de 2^{437} par 7. $2^3 = 8 \equiv 1\ [7]$ et $437 = 3 \times 145 + 2$, donc

$$2^{437} = \left(2^3\right)^{145} \times 2^2 \equiv 1^{145} \times 4 = 4\ [7]. \qquad \text{Le reste est 4.}$$

c. Chiffre des unités de 7^{2026}. Le chiffre des unités d'un entier naturel est son reste modulo 10.
$7^2 = 49 \equiv -1\ [10]$, donc $7^4 \equiv 1\ [10]$; $2026 = 4 \times 506 + 2$, d'où

$$7^{2026} = \left(7^4\right)^{506} \times 7^2 \equiv 1 \times 49 \equiv 9\ [10]. \qquad 7^{2026} \text{ se termine par 9.}$$

Méthode 6 : résoudre une équation avec des congruences

a. Déterminer les entiers x tels que $6 + x \equiv 5\ [3]$.
On ajoute -6 aux deux membres (compatibilité avec l'addition) : $x \equiv 5 - 6 = -1\ [3]$, soit $x \equiv 2\ [3]$.
Les solutions sont les entiers de la forme $2 + 3k$, $k \in \mathbb{Z}$.

b. Déterminer les entiers x tels que $3x \equiv 5\ [4]$.
Comme $5 \equiv 1\ [4]$, l'équation équivaut à $3x \equiv 1\ [4]$. Or x est congru à l'un des entiers 0, 1, 2, 3 modulo 4 ; on étudie tous les cas dans un **tableau de congruences** (ci-contre) : seul $x \equiv 3\ [4]$ donne $3x \equiv 1\ [4]$.
Les solutions sont les entiers de la forme $3 + 4k$, $k \in \mathbb{Z}$.

$x \equiv \ \ldots\ [4]$	0	1	2	3
$3x \equiv \ \ldots\ [4]$	0	3	2	1

Méthode 7 : démontrer une divisibilité pour tout entier n

Énoncé. Démontrer que pour tout entier n, $n^3 - n$ est divisible par 3.

Solution. Tout entier n est congru à 0, 1 ou 2 modulo 3. Par compatibilité avec les opérations, on calcule $n^3 - n$ modulo 3 dans chaque cas (tableau ci-contre). Dans tous les cas, $n^3 - n \equiv 0\ [3]$: 3 divise $n^3 - n$.

$n \equiv \ \ldots\ [3]$	0	1	2
$n^3 \equiv \ \ldots\ [3]$	0	1	$8 \equiv 2$
$n^3 - n \equiv \ \ldots\ [3]$	0	0	0

Propriété 7 : critères de divisibilité

Soit $N = \overline{a_k a_{k-1} \ldots a_1 a_0} = a_k \times 10^k + \cdots + a_1 \times 10 + a_0$ un entier naturel écrit en base 10 (chiffres a_0, $\ldots$, a_k).

a. N est divisible par 2 (resp. 5, 10) si et seulement si son chiffre des unités a_0 l'est.

b. N est divisible par 4 si et seulement si le nombre $\overline{a_1 a_0}$ formé par ses deux derniers chiffres l'est.

c. N est divisible par 3 (resp. 9) si et seulement si la somme de ses chiffres l'est.

d. N est divisible par 11 si et seulement si la somme alternée $a_0 - a_1 + a_2 - a_3 + \ldots$ l'est.

Démonstration

a. $10 \equiv 0\ [2]$, donc $10^j \equiv 0\ [2]$ pour $j \geqslant 1$ et $N \equiv a_0\ [2]$. De même modulo 5 et 10.

b. $100 \equiv 0\ [4]$, donc $10^j \equiv 0\ [4]$ pour $j \geqslant 2$ et $N \equiv 10a_1 + a_0 = \overline{a_1 a_0}\ [4]$.

c. $10 \equiv 1\ [9]$, donc $10^j \equiv 1^j = 1\ [9]$ pour tout j, et $N \equiv a_k + \cdots + a_1 + a_0\ [9]$. Comme $10 \equiv 1\ [3]$, la même preuve vaut modulo 3.

d. $10 \equiv -1\ [11]$, donc $10^j \equiv (-1)^j\ [11]$ et $N \equiv a_0 - a_1 + a_2 - \cdots + (-1)^k a_k\ [11]$.

Dans chaque cas, N et le nombre associé sont congrus : ils ont le même reste, et en particulier l'un est divisible si et seulement si l'autre l'est.

Exemple : $N = 123\,456\,789$

• Somme des chiffres : $1 + 2 + \cdots + 9 = 45$, multiple de 9 : $9 \mid N$.
• Somme alternée (en partant des unités) : $9 - 8 + 7 - 6 + 5 - 4 + 3 - 2 + 1 = 5$: le reste de N modulo 11 est 5.
• $\overline{89} = 89$ n'est pas divisible par 4 : $4 \nmid N$.

Python

```
print(pow(2, 456, 5))      # reste : 1
L = [pow(2, k, 7) for k in range(9)]
print(L)  # [1, 2, 4, 1, 2, 4, 1, 2, 4]
```

L'essentiel du chapitre

Divisibilité	$b \mid a \iff$ il existe $k \in \mathbb{Z}$ tel que $a = kb$. Si $c \mid a$ et $c \mid b$, alors $c \mid au + bv$ pour tous $u, v \in \mathbb{Z}$.
Division euclidienne	$a \in \mathbb{Z}$, $b \in \mathbb{N}^*$: il existe un unique couple $(q\,;r)$ tel que $a = bq + r$ et $0 \leqslant r < b$. $b \mid a \iff r = 0$.
Congruence	$a \equiv b\ [n] \iff n \mid a - b \iff a$ et b ont le même reste dans la division par n.
Opérations	On ajoute, soustrait, multiplie membre à membre, on élève à une puissance $p \in \mathbb{N}$; on **ne simplifie pas** et on **ne réduit pas les exposants** modulo n.
Méthodes	Reste de a^N : chercher $a^k \equiv 1$ (ou -1) $[n]$; équations et divisibilités : tableau de congruences.
Critères	3 et 9 : somme des chiffres ; 11 : somme alternée ; 4 : nombre formé par les deux derniers chiffres.