Cours & méthodes

Divisilité et congruence dans $\mathbb{Z}$

2
ALGEBRE

1 Divisibilité dans $\mathbb{Z}$

1.1 Multiples et diviseurs d'un entier relatif

Définition 1 : Divisibilité

Soient a et b deux entiers relatifs.
On dit que a **divise** b, ou encore a **est un diviseur de** b,
ou encore b **est divisible par** a, ou encore b **est un multiple de** a, s'il existe un entier relatif k tel que $b = a \times k$.
On note alors $a \mid b$.

En Vidéo

Les bases du cours

Exemple 1

$24 = 3 \times 8$ donc 3 divise 24, on note $3 \mid 24$, mais 5 ne divise pas 24, on note $5 \nmid 24$.
Attention, observez bien que nous travaillons dans $\mathbb{Z}$. $24 = -3 \times (-8)$ donc -3 divise aussi 24. $-8 \mid 24$

Méthode 1 : Prouver qu'un entier est divisible ou non par un autre

a) Démontrer que $14p^2 - 35q$ est divisible par 7 quels que soient les entiers relatifs p et q.
b) Démontrer que pour tout entier relatif n, $n+1$ divise $n^2 - 1$.

Correction

Remarque 1

0 est un multiple de tout entier relatif a (puisque $a \times 0 = 0$). En revanche, 0 n'est un diviseur d'aucun nombre.

Méthode 2 : Prouver qu'un entier est divisible par un autre

Les questions sont indépendantes

1) Démontrer que, quel que soit l'entier relatif n, $12n + 7$ n'est jamais divisible par 4.
2) Déterminer les entiers n tels que $2n - 5$ divise 6.
3) Déterminer les entiers naturels x et y tels que $4x^2 - y^2 = 20$.

Correction

Propriété 1

Tout entier relatif non nul n possède un nombre fini de diviseurs, compris entre $-n$ et n.

Exemple 2

L'ensemble des diviseurs de 24 est $D_{24} = \{-24; -12; -8; -6; -4; -3; -2; -1; 1; 2; 3; 4; 6; 8; 12; 24\} = D_{-24}$

Propriété 2

Soit a et b deux entiers relatifs tels que $a \mid b$, alors tout diviseur de a est un diviseur de b.

Méthode 3 : Déterminer si un entier est diviseur d'un autre. (Sans calculatrice !!)

Déterminer si 246 est un diviseur de 7416487.

Correction

Plan de Travail

27 p 104 ☐ 54 p 104 ☐ 29 p 104 ☐ 56 p 104 ☐ **En autonomie :** 30 p 104 ☐ 31 p 104 ☐

1.2 Propriétés de la divisibilité dans $\mathbb{Z}$

Propriété 3 : Fondamentale

Soient a, b et c trois entiers relatifs.

- Si a divise b et si b divise c alors a divise c. (On appelle cette propriété la **transitivité**.)
- Si a divise b et c alors a divise $b + c$ et $b - c$ et plus généralement, pour tous entiers u et v, a divise $b \times u + c \times v$. (On dit que $b \times u + c \times v$ est une **combinaison linéaire** de b et c.)

Démonstration 1 : Combinaison linéaire

a divise b et c donc Il existe un entier relatif k tel que $b = ka$ et il existe un entier relatif k' tel que $c = k'a$.
Ainsi, $bu + cv = uka + vk'a = (uk + vk')a$.
On a écrit $bu + cv$ sous la forme d'un entier relatif multiplié par a , donc $a \mid bu + cv$

Exemple 3

- 3 divise 6 et 6 divise 24 alors 3 divise 24.
- Si 3 divise 6 et 9 alors 3 divise $6 + 9$ et $6 - 9$ et plus généralement, pour tous entiers u et v, 3 divise $6 \times u + 9 \times v$.

Méthode 4 : Prouver qu'un entier est divisible par un autre

Déterminer les entiers relatifs n tels que $2n + 1$ divise $n + 13$.

Correction

Plan de Travail

33 p 104 ☐ 36* p 104 57 p 106 ☐ 63** p 106 ☐ 68** p 106 ☐
69** p 106 ☐ **En autonomie :** 67** p 106 ☐ 70** p 106 ☐

QCM n°1

2 Division euclidienne

2.1 Un résultat fondamental

Théorème 1

Soient a un entier relatif et b un entier naturel non nul.
Il existe un unique couple d'entiers relatifs $(q\,;r)$ tels que $a = bq + r$ **et** $0 \leqslant r < b$.

Définition 2

Soient a un entier relatif et b un entier naturel non nul.
Effectuer la division euclidienne dans $\mathbb{Z}$ de a par b, c'est trouver le couple d'entiers relatifs $(q\,;r)$ tel que $a = bq + r$ et $0 \leqslant r < b$.
Dans cette division, a est le **dividende**, b le **diviseur**, q le **quotient** et r le **reste**.

Exemple 4 : Divisions euclidiennes élémentaires

- Prenons $a = 2122$ et $b = 7$. On peut écrire : $2122 = 7 \times 303 + 1$.
  On a bien $0 \leqslant 1 < 7$ donc le reste de cette division euclidienne est bien 1.
  Le quotient de la division euclidienne de 2122 par 7 est 303.
- Prenons $a = 247$ et $b = 6$. On peut écrire : $247 = 6 \times 40 + 7$.
  Mais on observe que $7 > 6$ donc 7 ne peut pas être le reste de la division euclidienne.
  Pour autant, il ne s'agit pas de la division euclidienne de 247 par 6 : le reste doit être impérativement inférieur à 6.

Méthode 5 : Déterminer le quotient et reste d'une division euclidienne.

a) À l'aide de la calculatrice, déterminer le quotient et le reste de la division euclidienne de 432 par 17; en déduire, sans calculatrice, le quotient et le reste de la division euclidienne de -432 par 17.

b) Sachant que $1159 = 47 \times 24 + 31$, en déduire le quotient q et le reste r de la division euclidienne de : **a)** 1159 par 24; **b)** -1159 par 24.

Correction

Méthode 6 : Prouver qu'un entier est divisible par un autre

Soit n un entier naturel. Déterminer, selon les valeurs de n, le quotient et le reste de la division euclidienne de $7n + 5$ par $3n + 1$, puis de $7n + 13$ par $3n + 2$.

Correction

Propriété 4

Soient a un entier relatif et b un entier naturel non nul.
b divise a si, et seulement si, le reste de la division euclidienne de a par b est nul.

Démonstration 2

Pour prouver l'équivalence (« si et seulement si »), on procède en deux étapes :
Démonstration directe par implication, puis démonstration réciproque encore par implication.
Si le reste de la division euclidienne de a par b est nul, alors il existe un entier relatif q tel que $a = bq$, donc $b \mid a$.
Si b divise a, alors il existe un entier relatif q tel que $a = bq = bq + 0$.
Par unicité de la division euclidienne, le reste de la division de a par b vaut 0.

Plan de Travail

En classe : 20 p 104 ☐ 21 p 104 ☐ 22 p 104 ☐ 23 p 104 ☐ 24 p 104 ☐ 40 p 104 ☐

2.2 Écriture d'un entier relatif quelconque

Propriété 5

Soit b un entier naturel supérieur ou égal à 2.
Tout entier relatif peut s'écrire sous l'une des formes suivantes : bq, $bq + 1$, $bq + 2$, ..., $bq + (b - 1)$ où $q \in \mathbb{Z}$.

Remarque 2

Cela vient du fait que les restes possibles dans la division euclidienne de a par b sont $0, 1, 2, \ldots, b - 1$.

Exemple 5

Si $b = 4$, on peut dire que tout entier, il existe un entier k tél qu'il s'écrive sous la forme : $4k$ ou $4k + 1$ ou $4k + 2$ ou $4k + 3$. Par exemple, $14 = 4 \times 4 + 1$; $35 = 8 \times 4 + 3$; ...

Méthode 7 : Prouver qu'un entier n'est pas divisible par un autre

Soit n un entier naturel. Montrons que $n^2 + 1$ n'est jamais divisible par 3.

Correction

Méthode 8 : Prouver qu'un entier est divisible par un autre

Soient a et b deux entiers relatifs tels que $a^2 - 2b^2 = 1$.
Démontrer que a est impair puis que b est pair.

Correction

Méthode 9 : Prouver qu'un entier est divisible par un autre

Soit n un entier. On pose $a = n(n^2 - 4)$. Démontrer que a est un multiple de 3.

Correction

Plan de Travail

En classe : 38 p 104 ☐ 42 p 104 ☐ 43 p 104 ☐ 44 p 104 ☐

QCM n°2

3 Congruences dans $\mathbb{Z}$

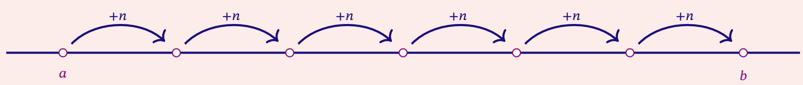
3.1 Définition et propriétés

Définition 3

En Vidéo

Soient a et b deux entiers relatifs et soit n un entier naturel non nul.
On dit que a **est congru à** b **modulo** n s'il existe un entier k tel que $b = a + kn$.
Cette relation se note $a \equiv b\ [n]$ ou $a \equiv b\ (n)$ ou encore $a \equiv b \pmod{n}$.

Illustration



Dans cette situation, on a bien $b = a+kn$, c'est à dire $a \equiv b\ [n]$

Exemple 6

$25 = 6 \times 4 + 1$ donc $25 \equiv 1[4]$

Propriété 6

Soient a et b deux entiers relatifs et soit n un entier naturel non nul.
a **est congru à** b **modulo** n est équivalent à dire que n divise $b - a$

Propriété 7 : Bilan pour les matheux !

Soient a et b deux entiers relatifs et soit n un entier naturel non nul.

$$a \equiv b\ [n] \iff n \mid b - a \iff \exists k \in \mathbb{Z}, b = a + kn$$

.

Exemple 7

- $a \equiv b\ [3]$ signifie que $b = a + 3k$ avec $k \in \mathbb{Z}$.
- $11 \equiv 5\ [3]$ car $11 = 5 + 2 \times 3$
- $20 = 8 + 2 \times 6$ donc on peut dire que $20 \equiv 8\ [6]$

Méthode 10 : Prouver qu'un entier est divisible par un autre

Justifier que $11 \equiv -4\ [3]$.

Correction

Propriété 8 : Conséquences immédiates

Soient a, b, c et r quatre entiers relatifs et soit n un entier naturel non nul.

- $a \equiv a\ [n]$ (réflexivité)
- Si $a \equiv b\ [n]$, alors $b \equiv a\ [n]$ (symétrie)
- Si $a \equiv b\ [n]$ et si $b \equiv c\ [n]$ alors $a \equiv c\ [n]$ (transitivité)
- a est divisible par n si, et seulement si, a est congru à 0 modulo n.
- r est la reste dans la division euclidienne de a par n si, et seulement si, $a \equiv r\ [n]$ et $0 \leqslant r < n$.

Remarque 3

- Les relations de congruences généralisent la relation de divisibilité : $n \mid a \iff a \equiv 0\ [n]$
- La condition $0 \leqslant r < n$ est essentielle comme le montre l'exemple $47 \equiv 14\ [3]$: 14 n'est pas le reste de la division euclidienne de 47 par 3.

Propriété 9

Soient a et b deux entiers relatifs et soit n un entier naturel non nul.
a est congru à b modulo n si, et seulement si, a et b ont le même reste dans la division euclidienne par n.

Exemple 8

$41 = 4 \times 10 + 1$ et $29 = 4 \times 7 + 1$ donc $41 \equiv 29\ [4]$

Plan de Travail

46 p 105 ☐ 92 p 108 ☐ 93 p 108 ☐

3.2 Compatibilité avec les opérations

Théorème 2

Soient a, b, c et d quatre entiers relatifs et soit n un entier naturel non nul tels que $a \equiv b\ [n]$ et $c \equiv d\ [n]$. Alors :

- $a + c \equiv b + d\ [n]$ et $a - c \equiv b - d\ [n]$.
- $a \times c \equiv b \times d\ [n]$.
- $\forall p \in \mathbb{N}^*,\ a^p \equiv b^p\ [n]$

Synthèse générale

Attention

Les relations de congruences ne sont pas compatibles avec la division.
Par exemple, $3 \times 7 \equiv 3 \times 5\ [6]$ **mais** 7 et 5 ne sont pas congrus modulo 6.

Méthode 11 : Utiliser les congruences avec la division euclidienne

Déterminer le reste de la division euclidienne de 383 par 7 en utilisant les congruences.

Correction

Méthode 12 : Utiliser les opérations avec les congruences.

Soit a et b deux entiers tels que $a \equiv 2\ [5]$ et $b \equiv 3\ [5]$.
Déterminer le reste de la division euclidienne de $a^2 + b$ et de $4a - 3b$ par 5.

Correction

En Vidéo

Démontrer que pour tout entier naturel n impair, $n^2 - 1$ est divisible par 8

Exercice corrigé

Plan de Travail

94 p 108 ☐ 99 p 108 ☐ 47 p 105 ☐ 50 p 105 ☐ 51 p 105 ☐

QCM n°3

Méthode 13 : Résoudre une équation avec les congruences

Déterminer l'ensemble des entiers naturels x tels que :

a) $x + 3 \equiv 2\ [7]$ b) $3x \equiv 2\ [5]$

Correction

Méthode 14 : Prouver qu'un entier est divisible par un autre

Déterminer l'ensemble des entiers naturels n tels que $n^2 - 3n + 6$ soit divisible par 4.

Correction

Méthode 15 : Prouver qu'un entier est divisible par un autre

Quel est le reste de la division euclidienne de 11^{2020} par 3 ?

Correction

Plan de Travail

106 p 110 ☐ 107 p 110 ☐ 108 p 110 ☐

102 p 110 ☐ 103* p 110 ☐ 104 p 110 ☐ 105 p 110 ☐

QCM n°4

4 Inverse modulo m

Définition 4 : Inverse modulo n

Soient a un entier relatif et n un entier naturel non nul.
On dit que a est **inversible modulo** n lorsqu'il existe un entier b tel que $a \times b \equiv 1[n]$.

QCM n°5

Exemple 9

8 est inversible modulo 3 car $8 \times 2 \equiv 1[3]$. 2 est donc un inverse de 8 modulo 3.

Méthode 16 : Déterminer l'inverse modulo n d'un entier

Déterminer si 7 est inversible modulo 4.

Correction

QCM n°6

Plan de Travail

52 p 105 ☐ 53 p 105 ☐

Sujets Bac : 117*** p 111 ☐ 121*** p 112 ☐ 123*** p 113 ☐ 126*** p 113 ☐

Corrigés des exercices