DIVISIBILITÉ, DIVISION EUCLIDIENNE, CONGRUENCE

I. Divisibilité dans ℤ

DÉFINITION

Soient a et b deux entiers relatifs.

On dit que ***b* divise *a*** (noté $b \mid a$) si, et seulement si, il existe un entier relatif k tel que : $a=kb$.

On dira aussi que ***a* est un multiple de *b***.

Remarque : l'ensemble des diviseurs de 0 est ℤ.

Exemple C1

Déterminer l'ensemble des diviseurs de 210, noté D_{210} : $\mathrm{D}_{210}=\{k\in\mathbb{Z}, k|210\}$.

Exemple A1

p. 83 méthode 1

Déterminer tous les couples d'entiers naturels $(x\,;y)$ tels que : $x^2=2xy+15$.

PROPRIÉTÉS

• Si $d \mid a$ et $a\neq 0$, alors : $|d|\leqslant|a|$.

Autrement dit, tout diviseur d'un entier a non nul est compris entre $-|a|$ et $|a|$.

Et par conséquent, tout entier relatif non nul admet un nombre fini de diviseurs.

• Si $a \mid b$ et $b \mid a$ avec a et b non nuls, alors $a=b$ ou $a=-b$.

Démonstration :

• Si $d \mid a$ avec $a\neq 0$: $\exists\, k\in\mathbb{Z},\ a=dk$.

Supposons par l'absurde que $d>|a|$.

$d>|a| \Rightarrow d>|dk| \Rightarrow d>d|k| \Rightarrow 1>|k|$ (car $d>0$)

$\Rightarrow -1<k<1$

$\Rightarrow 0=k$ (car k est un entier relatif)

$\Rightarrow a=0$ $\leftarrow$ contradiction !

Donc $d\leqslant|a|$. On montrerait de même que $-|a|\leqslant d$.

•

PROPRIÉTÉ

Si $a \mid b$ et $a \mid c$, alors a divise toute combinaison linéaire de b et c : $\forall\ (\alpha;\beta) \in \mathbb{Z}^2,\ a \mid\ \alpha b+\beta c$.

<u>Démonstration</u> :

EXEMPLE C2

Déterminer les entiers relatifs n tels que $2n-7\ \mid\ 3n+4$.

PROPRIÉTÉ (TRANSITIVITÉ)

Si $a \mid b$ et $b \mid c$, alors $a \mid c$.

<u>Démonstration</u> :

EXEMPLE C3

24 | 168 et 168 | 840 donc 24 | 840.

II. Division euclidienne

THÉORÈME (DIVISION EUCLIDIENNE DANS $\mathbb{Z}$)

$\forall\ (a;b) \in \mathbb{Z}\times\mathbb{N}^*,\ \exists\ !\ (q;r) \in \mathbb{Z}^2,\ a=bq+r$ et $0\leqslant r<b$.

DÉFINITION Dans cette division euclidienne de a par b, on dit que :

a est le ***dividende*** $\quad$ b est le ***diviseur*** $\quad$ q est le ***quotient*** $\quad$ r est le ***reste***.

<u>Démonstration de l'existence</u> : Soient $(a;b) \in \mathbb{Z}\times\mathbb{N}^*$.

- <u>1er cas</u> : $a\geqslant 0$

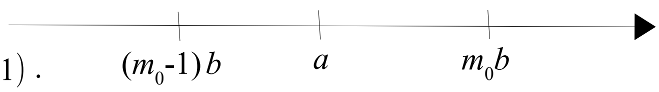
  On note : $\mathscr{E} = \{\ m \in \mathbb{N},\ mb>a\ \}$.

  $\mathscr{E}$ n'est pas vide car : $b\geqslant 1$ et $a\geqslant 0 \Rightarrow (a+1)b\geqslant a+1 \Rightarrow (a+1)b>a$.

  $\mathscr{E}$ est donc une partie non vide de $\mathbb{N}$, donc $\mathscr{E}$ admet un plus petit élément, noté m_0 .

  $m_0\geqslant 1$ car $m_0 \in \mathbb{N}$ et $0 \notin \mathscr{E}$.

  Alors : $(m_0-1)b\leqslant a<m_0 b$.



  D'où : $a=b\underbrace{(m_0-1)}_{q}+\underbrace{a-b(m_0-1)}_{r}$.

  On a bien : $\rightarrow q \in \mathbb{N}$ car $m_0\geqslant 1$

  $\rightarrow\ 0\leqslant r<b$ car $a\geqslant b(m_0-1)$ et $a<b\,m_0$.

• 2[e] cas : $a<0$

$-a>0$ donc d'après le 1[er] cas : $\exists\ (q';r')\in\mathbb{N}^2,\ -a=bq'+r'$ et $0\leqslant r'<b$.

donc $a=b(-q')-r'$.

→ Si $r'=0$ alors $a=bq+r$ en posant $q=-q'$ et $r=r'$.

→ Si $r'>0$: $a=b(-q')-r'=b(-q'-1)+b-r'$ avec $-q'-1<0$ et $0<b-r'<b$

donc $a=bq+r$ en posant $q=-q'-1$ et $r=b-r'$.

Démonstration de l'unicité : Soient $(a;b)\in\mathbb{Z}\times\mathbb{N}^*$.

Supposons que : $\exists\ (q;r)\in\mathbb{Z}^2,\ a=bq+r$ où $0\leqslant r<b$

$\exists\ (q';r')\in\mathbb{Z}^2,\ a=bq'+r'$ où $0\leqslant r'<b$.

Alors : $r'-r=b(q-q')$.

Or : $0\leqslant r'<b$ et $-b<-r\leqslant 0$ donc $-b<r'-r<b$.

Or, le seul multiple de b compris entre $-b$ et b est 0, d'où $r'-r=0$ et donc $r=r'$.

On a alors : $b(q-q')=0$ et, comme $b\neq 0$: $q'=q$.

Remarques :

• On aurait pu prendre $b\in\mathbb{Z}^*$, on aurait alors le théorème suivant :

$$\boxed{\forall\ (a;b)\in\mathbb{Z}\times\mathbb{Z}^*,\ \exists !\ (q;r)\in\mathbb{Z}\times\mathbb{N},\ a=bq+r \text{ et } 0\leqslant r<|b|\ .}$$

• On aurait pu démontrer l'existence plus facilement d'une façon non constructive : par récurrence sur *b*.

Exemple C4

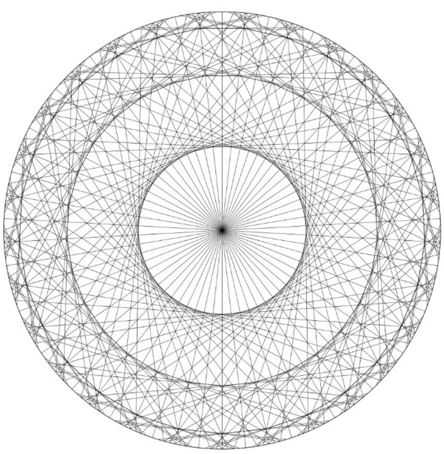
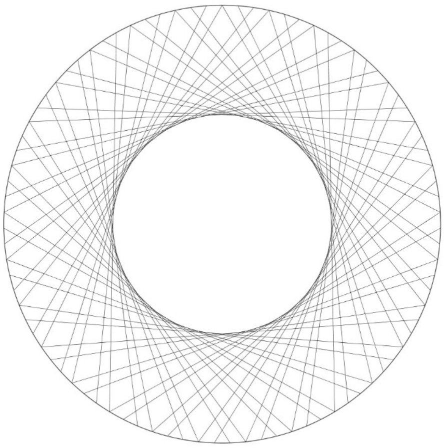
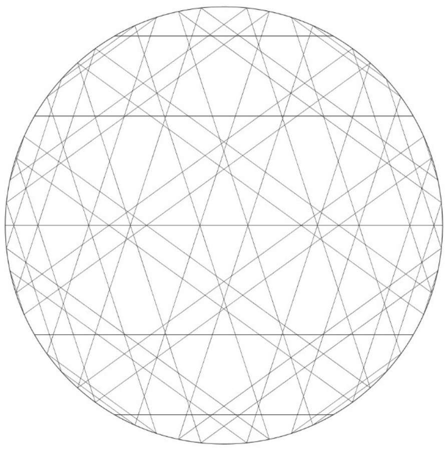
1. Déterminer la division euclidienne de 524 par 17.
2. En déduire la division euclidienne de -524 par 17.
3. De même avec -524 par -17 .

Exemple C5

1. Démontrer que tout entier naturel n s'écrit sous la forme $3q+r$ avec $r\in\{0\ ;1\ ;2\}$.
2. Démontrer que, pour tout entier naturel n : $n(n-2)(n+2)$ est un multiple de 3.

III. Congruence

→ À lire : *La beauté modulaire des tables de multiplication* sur mon site

DÉFINITION

Soit $n \in \mathbb{N}^*$. Soient $(a\,;b) \in \mathbb{Z}^2$.

On dit que a et b sont ***congrus modulo n*** si, et seulement si, a et b ont le même reste dans la division euclidienne par n. On note alors : $a \equiv b\ [n]$.

On peut aussi noter $a \equiv b\ [n]$ ou $a \equiv b \mod n$.

Pourquoi congru ? En latin, *congruens* signifie « qui s'accorde ».

Pourquoi modulo ? Il s'agit de l'ablatif du nom latin *modulus*, qui signifie « mesure ».

Le symbole ≡ est l'œuvre du prince des mathématiciens, Carl Friedrich Gauss, qui publie en 1801 l'ouvrage *Disquisitiones arithmeticae*, et donne ainsi une naissance rigoureuse à l'arithmétique modulaire, qui révolutionnera la théorie algébrique des nombres mais aussi notre quotidien, puisque l'arithmétique de base des ordinateurs travaille sur des « nombres » de taille fixe, et est par conséquent une arithmétique modulaire.

Conséquence immédiate :

PROPRIÉTÉ

Soit $n \in \mathbb{N}^*$. Un entier relatif est congru à son reste dans la division euclidienne par n.

EXEMPLE C6

$265 = 4 \times 66 + 1$ donc $265 \equiv 1\ [4]$.

PROPRIÉTÉS (ÉVIDENTES)

Pour tout entier naturel n non nul, pour tous entiers relatifs a, b et c :

- $a \equiv a\ [n]$ ← ***réflexivité***
- $a \equiv b\ [n] \Rightarrow b \equiv a\ [n]$ ← ***symétrie***
- $a \equiv b\ [n]$ et $b \equiv c\ [n] \Rightarrow a \equiv c\ [n]$ ← ***transitivité***

on dit que ≡ est une ***relation d'équivalence***

PROPRIÉTÉ

Pour tout entier naturel n non nul, pour tous entiers relatifs a et b : $a \equiv b\ [n] \Leftrightarrow n \mid a-b$.

Démonstration :

PROPRIÉTÉS

Pour tout entier naturel n non nul, pour tous entiers relatifs a, b, c et d :

- $a \equiv b\ [n]$ et $c \equiv d\ [n] \Rightarrow\ a+c \equiv b+d\ \ [n]$ ← compatibilité de ≡ avec l'addition
- $a \equiv b\ [n]$ et $c \equiv d\ [n] \Rightarrow\ ac \equiv bd\ \ [n]$ ← compatibilité de ≡ avec la multiplication
- $a \equiv b\ [n] \Rightarrow \forall\, p \in \mathbb{N},\ a^p \equiv b^p\ \ [n]$ ← compatibilité de ≡ avec les puissances

Démonstrations :

ATTENTION : pas de compatibilité avec la division. En effet, par exemple : 62 ≡ 26 [4] mais 31 ≡ 3 [4] et 13 ≡ 1 [4] donc 31 et 13 ne sont pas congrus modulo 4.

EXEMPLE A2


p. 87 méthode 4

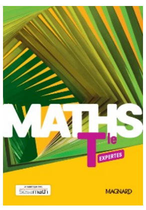
Montrer que, pour tout entier naturel n, $3^{n+3}-4^{4n+2}$ est divisible par 11.

EXEMPLE A3


p. 87 méthode 5

Déterminer les restes possibles de la division de n^2 par 7 suivant les valeurs de l'entier relatif n. En déduire les solutions de $n^2 \equiv 2\ [7]$.

→ BILAN DU CHAPITRE & TRAVAIL EN AUTONOMIE ←



- Fiche bilan → p.97
- QCM 12 questions corrigées → p.98
- Exercices corrigés → 107 à 122 p.99
- Exercices types corrigés → méthodes 6 et 7 p.88/89

- Méthodes et exercices corrigés en vidéo : → maths-et-tiques : tome-a1-ym