

I. Divisibilité dans \mathbb{Z}	1	III. Congruence	3
II. Division euclidienne	2		

I. Divisibilité dans \mathbb{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 : $a = k b$.

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

REMARQUE : l'ensemble des diviseurs de 0 est \mathbb{Z} .

EXEMPLE C1

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

EXEMPLE A1

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



p. 83 méthode 1

PROPRIÉTÉS

- Si $d \mid a$ et $a \neq 0$, alors : $|d| \leq |a|$.

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 $d > |a|$.

$$\begin{aligned} d > |a| &\Rightarrow d > |dk| \Rightarrow d > d|k| \Rightarrow 1 > |k| \text{ (car } d > 0) \\ &\Rightarrow -1 < k < 1 \\ &\Rightarrow 0 = k \text{ (car } k \text{ est un entier relatif)} \\ &\Rightarrow a = 0 \quad \leftarrow \text{contradiction !} \end{aligned}$$

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

•

PROPRIÉTÉ

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

Démonstration :

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 $a \mid c$.

Démonstration :

EXEMPLE C3

$24 \mid 168$ et $168 \mid 840$ donc $24 \mid 840$.

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 $0 \leq r < b$.

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

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

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

• 1^{er} cas : $a \geq 0$

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

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

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

$m_0 \geq 1$ car $m_0 \in \mathbb{N}$ et $0 \notin \mathcal{E}$.

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

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

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

$\rightarrow 0 \leq r < b$ car $a \geq b(m_0 - 1)$ et $a < b m_0$.



- 2^e cas : $a < 0$

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

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

→ Si $r' = 0$ alors $a = b q + r$ 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 $a = b q + r$ en posant $q = -q' - 1$ et $r = b - r'$.

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

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

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

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

Or : $0 \leq r' < b$ et $-b < -r \leq 0$ 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 :

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

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

EXEMPLE C4

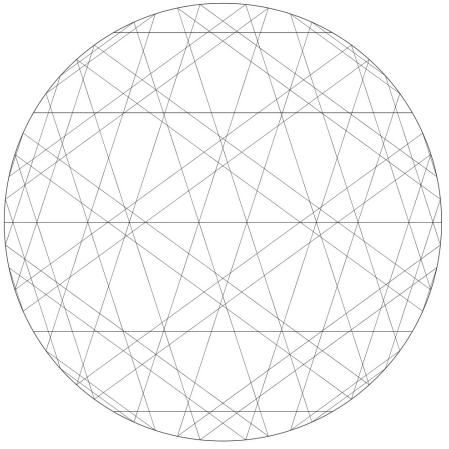
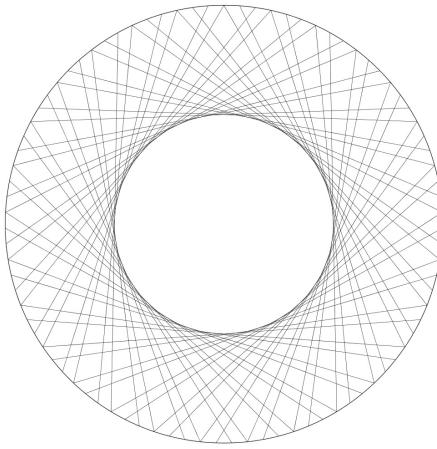
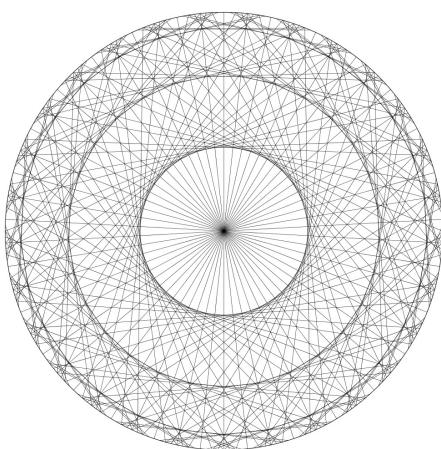
1. Déterminer la division euclidienne de 524 par 17.
2. En déduire la division euclidienne de -524 par 17.
3. De même avec -524 par -17 .

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 : $a \equiv b \pmod{n}$.

On peut aussi noter $a \equiv b \pmod{n}$ ou $a \equiv b \text{ mod } n$.

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 \equiv est l'œuvre du prince des mathématiciens, Carl Friedrich Gauss, qui publie en 1801 l'ouvrage *Disquisitiones arithmeticæ*, 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 .

EXAMPLE 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 :

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

Démonstrations :

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

EXEMPLE A2

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



p. 87 méthode 4

EXEMPLE A3

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 $n^2 \equiv 2 [7]$.



p. 87 méthode 5

→ 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-ytm](#)