

« Les mathématiques sont les reines des sciences et l'arithmétique la reine des mathématiques »

Gauss



I. Diviseurs et multiples d'entiers :

✚ Multiples d'entiers relatifs :

Soit un entier n , on dit que m est un multiple de n , si et seulement si, il existe $k \in \mathbb{Z}$ tel que $m = kn$.

Exemple : les multiples de 7 sont : $\{\dots, -21, -14, -7, 0, 7, 14, 21, 28, \dots\}$ ensemble noté $7\mathbb{Z}$.

Remarque : 0 est un multiple de tous les nombres.

✚ Relation de divisibilité :

Soient deux entiers relatifs a et b .

a divise b si et seulement si :

* il existe $k \in \mathbb{Z}$ tel que $b = ak$

* b est un multiple de a .

On dit aussi que a est diviseur de b ou que b est divisible par a

« a divise b » est noté $a \mid b$.

Remarques :

- 1 et -1 divisent tous les nombres.
- Un nombre a admet au minimum quatre diviseurs $\{1, -1, a, -a\}$.
- a divise a .
- a est un diviseur de 0. ($0 = a \times 0$).
- 0 est un diviseur de 0. ($0 = 0 \times k$).

Activité 2 page 148 :

$$1) D_{-15} = \{-15, -5, -3, -1, 1, 3, 5, 15\}$$

$$D_{143} = \{-143, -13, -11, -1, 1, 11, 13, 143\}$$

$$D_1 = D_{-1} = \{1, -1\}$$

$$D_0 = \mathbb{Z}$$

$$2) P \text{ est un nombre premier. } D_p = \{-p, -1, 1, p\}$$

✚ Propriétés de la relation de divisibilité :

P1: Si $b \mid a$ alors $-b \mid a$

$$b \mid a \Leftrightarrow a = bk \Leftrightarrow a = (-b)(-k) \Leftrightarrow -b \mid a.$$

P2: Si $b \mid a$ alors $|b| \leq |a|$ ($a \neq 0$)

$$b \mid a \Rightarrow a = bk \Rightarrow |a| = |b| \times |k|, \text{ or } a \neq 0 \Rightarrow k \in \mathbb{Z}^* \Rightarrow |k| \geq 1 \Rightarrow |b| \times |k| \geq |b| \Rightarrow |a| \geq |b|.$$

(En valeur absolu le diviseur est plus petit que le dividende)

P3: Si $a \mid b$ et $b \mid c$ alors $a \mid c$.

$$b = a \times k \text{ et } c = b \times k' \text{ alors } c = a \times (k \times k') \text{ alors } a \mid c.$$

P4: Si $a \mid b$ et $b \mid a$ alors $a = b$ ou $a = -b$.

$a \mid b \Rightarrow |a| \leq |b|$ et $b \mid a \Rightarrow |b| \leq |a|$; d'où $|a| = |b| \Rightarrow a = b$ ou $a = -b$.

P5: Si $a \mid b$ et $a \mid c$ alors $a \mid ub + vc$ (u et v sont deux entiers).

$a \mid b \Leftrightarrow b = a \times k$ et $a \mid c \Leftrightarrow c = a \times k'$, d'où $ub + vc = a(uk + vk') \Rightarrow a \mid ub + vc$.

P6: Si $a \mid b$ alors $a \mid bc$, $\forall c \in \mathbb{Z}$.

$a \mid b$ alors $b = ak$ donc $bc = a(ck)$

P7: Si $a \mid b$ alors $ac \mid bc$, $\forall c \in \mathbb{Z}$.

$a \mid b$ alors $b = ak$ donc $bc = (ac)k$.

Activité 4 page 149 :

1) $7 \mid 4200 \Rightarrow 7 \mid 4200^3$

$7 \mid 3521 \Rightarrow 7 \mid 3521^{10} \Rightarrow 7 \mid 4200^3 + 3521^{10}$.

2) $13 \mid 260 \Rightarrow 13 \mid 260^{260} \Rightarrow -13 \mid 260^{260} \Rightarrow 260^{260} = -13k$

Supposons que $-13 \mid 260^{260} + 11 \Rightarrow 260^{260} + 11 = -13k' \Rightarrow 11 = 13(k - k') \Rightarrow 13 \mid 11$: absurde

3) $a = 42424242424241 = 42k + 41$

Si $-42 \mid a \Rightarrow a = -42k' \Rightarrow 42k + 41 = -42k' \Rightarrow 41 = 42(k - k') \Rightarrow 42 \mid 41$: absurde.

4) $n \mid n - 6 \Leftrightarrow n - 6 = nk \Leftrightarrow (n-6)/n = k \in \mathbb{Z} \Leftrightarrow 1 - 6/n \in \mathbb{Z} \Leftrightarrow n \mid 6 \Leftrightarrow n \in D_6 = \{-6, -3, -2, -1, 1, 2, 3, 6\}$

II. Division euclidienne dans \mathbb{Z} :

✚ Soient a et b deux entiers naturels tels que $b \neq 0$.

Effectuer la division euclidienne de a par b , c'est trouver deux entiers q et r tels que $a = bq + r$ avec $0 \leq r < b$; q est le quotient, r est le reste, a est le dividende et b est le diviseur.

Exemples :

$36 = 2 \times 14 + 8$; $q = 2$ et $r = 8$.

$14 = 0 \times 36 + 14$; $q = 0$ et $r = 14$.

$0 = 0 \times 36 + 0$; $q = 0$ et $r = 0$.

Remarque : Ne pas négliger la condition $0 \leq r < b$.

Exemple : $24 = 2 \times 7 + 10$ n'est pas la division euclidienne de 24 par 7. ($24 = 3 \times 7 + 3$).

✚ Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$, il existe $q \in \mathbb{Z}$ et $r \in \{0, 1, 2, \dots, |b| - 1\}$ tels que $a = bq + r$; q et r sont uniques.

Exemples :

$15 = 2 \times 7 + 1$; $q = 2$ et $r = 1$.

$-15 = -2 \times 7 + (-1)$ n'est pas une division euclidienne.

$-15 = -3 \times 7 + 6$ c'est la division euclidienne -15 par 7.

✚ Soient $a' \in \mathbb{Z}_-$ et $b \in \mathbb{Z}_+$.

Pour diviser a' par b , il est conseillé de diviser $-a'$ par b d'abord.

Exemple :

$36 = 2 \times 14 + 8$

$2 \times 14 \leq 36 < 3 \times 14$

$-3 \times 14 < -36 \leq -2 \times 14$

$-36 = -3 \times 14 + 6$, $q = -3$ et $r = 6$.

En général : « Propriété d'Archimède »

- $\forall a$ et b deux entiers naturels ($b < a$) il existe $q \in \mathbb{N}$ tel que $bq \leq a < b(q+1)$
 q est le quotient de a par b .

- Tout entier $a' \in \mathbb{Z}$ peut être encadré de manière unique par deux multiples consécutifs de l'entier strictement positif b : $bq \leq a' < b(q+1)$; $a' = bq + r$ avec $0 \leq r < b$.

Exercices 7 et 8 page 157.

III. Congruence dans \mathbb{Z} :

Définition :

Soit $n \geq 1$ un entier et $a, b \in \mathbb{Z}$, on dit que a est congru à b modulo n s'il existe un entier $k \in \mathbb{Z}$ tel que $a = b + kn$; on écrit alors $a \equiv b [n]$ ou $a \equiv b \pmod{n}$ ou $a \equiv_n b$.

Remarque :

$a \equiv b [n]$ si et seulement si a et b ont le même reste dans la division euclidienne par n .

En effet :

\Leftrightarrow si $a = nq + r$ et $b = nq' + r$ avec $0 \leq r < n$ alors $a - b = n(q - q') \Rightarrow a = b + n(q - q') \Rightarrow a \equiv b [n]$.

\Rightarrow si $a \equiv b [n]$ alors $a = b + kn$.

Supposons que $a = nq + \underline{r}$ et montrons que $b = nq' + \underline{r}$

$$b = a - kn = nq + r - kn = n(q - k) + \underline{r}$$

Exemple :

$$6 \equiv -15[7] \text{ car } 6 = -15 + 7 \times 3.$$

$$-15 = -3 \times 7 + \underline{6}$$

$$6 = 0 \times 7 + \underline{6}$$

Théorème :

Soit $n \geq 1$ entier

Pour tout $a \in \mathbb{Z}$, il existe un unique entier $r \in \{0, 1, \dots, n-1\}$ tel que $a \equiv r [n]$; on dit que r est le reste modulo n de a .

Activité 3 page 152.

a) $31 \equiv 3[7]$; $31 = 7 \times 4 + \underline{3}$

b) $-31 \equiv 1[5]$; $-31 = -7 \times 5 + \underline{4}$

c) $-2 \equiv 2[4]$; $-2 = 4 \times (-1) + \underline{2}$.

d) $914 \equiv 21[19]$; $914 = 48 \times 19 + \underline{2} = 47 \times 19 + 21$

e) $21 = 0 \times 47 + 21$

$$-21 = -47 + \underline{26}$$

$$914 = 47 \times 19 + \underline{21} ; 26 \neq 21 \Rightarrow 914 \not\equiv -21 \pmod{47}.$$

Activité 4 page 152

1) $a \equiv 2[6] \Rightarrow a = 2 + 6q$

$$b \equiv 3[6] \Rightarrow b = 3 + 6q'$$

$$ab = (2 + 6q)(3 + 6q') = 2(1 + 3q) \times 3(1 + 2q') = 6(1 + 3q)(1 + 2q') \in 6\mathbb{Z}.$$

2) $a \in \mathbb{Z}$.

a) $a \equiv r[6]$; $r \in \{0, 1, 2, 3, 4, 5\}$.

b) $a = r + 6k$; $0 \leq r < 6$

- Si $r = 0$ alors $a = 6k \Rightarrow a^2 = 36k^2 = 6 \times 6k^2 \Rightarrow a^2 \equiv 0 \pmod{6}$

- Si $r = 1$ alors $a = 6k + 1 \Rightarrow a^2 = 36k^2 + 12k + 1 \Rightarrow a^2 = 6(6k^2 + 2k) + 1 \Rightarrow a^2 \equiv 1 \pmod{6}$

- Si $r = 2$ alors $a = 6k + 2 \Rightarrow a^2 = 36k^2 + 24k + 4 = 6(6k^2 + 4k) + 4 \Rightarrow a^2 \equiv 4 \pmod{6}$

- Si $r = 3$ alors $a = 6k + 3 \Rightarrow a^2 = 36k^2 + 36k + 9 = 6(6k^2 + 6k + 1) + 3 \Rightarrow a^2 \equiv 3 \pmod{6}$
- Si $r = 4$ alors $a = 6k + 4 \Rightarrow a^2 = 36k^2 + 48k + 16 = 6(6k^2 + 8k + 2) + 4 \Rightarrow a^2 \equiv 4 \pmod{6}$
- Si $r = 5$ alors $a = 6k + 5 \Rightarrow a^2 = 36k^2 + 60k + 25 = 6(6k^2 + 10k + 4) + 1 \Rightarrow a^2 \equiv 1 \pmod{6}$

Ainsi on a le tableau de congruence de a^2 modulo 6 :

$a \equiv \dots \pmod{6}$	0	1	2	3	4	5
$a^2 \equiv \dots \pmod{6}$	0	1	4	3	4	1

Propriétés

Soient a, b, c et d quatre entiers et $n \in \mathbb{N}^*$

- ✚ $a \equiv a[n]$
- ✚ si $a \equiv b[n]$ alors $b \equiv a[n]$
- ✚ si $a \equiv b[n]$ et $b \equiv c[n]$ alors $a \equiv c[n]$.
- ✚ si $a \equiv b[n]$ et $c \equiv d[n]$ alors $a + c \equiv b + d [n]$ et $a \times c \equiv b \times d [n]$
- ✚ si $a \equiv b[n]$ alors $ha \equiv hb[n]$ pour tout entier h
- ✚ si $a \equiv b[n]$ alors $a^m \equiv b^m[n]$ pour tout entier $m > 0$.

Exercice résolu 4 page 153.

Activité 5 page 153.

$$566 - 6 = 560 = 80 \times 7 \in 7\mathbb{Z} \Rightarrow 566 \equiv 6[7] \Rightarrow 566^2 \equiv 36[7], \text{ or } 36 \equiv 1[7] \Rightarrow 566^2 \equiv 1[7]$$

$$\Rightarrow (566^2)^n \equiv 1^n[7] \forall n \geq 0 \Rightarrow 566^{2n} \equiv 1[7].$$

Exercice résolu 5 page 153.