# *Cours d'Arithmétique dans l'ensemble $\mathbb{Z}$*

*Niveau : 1ère Sciences mathématiques*

*Activité :*

Montrer que la somme de trois entiers relatifs est divisible par 3

## *I- Divisibilité dans $\mathbb{Z}$*

### *1. Divisibilité dans $\mathbb{Z}$*

*Définition :*

Soient a et b deux entiers relatifs.

On dit que b divise a si et seulement si il existe un entier relatif k tel que a = kb.

On dit alors que b est un diviseur de a ou encore que a est un multiple de b.

*Exemples :*

- $45 = 3 \times 15$ : 3 et 15 sont donc des diviseurs de 45.
- $(-12) = 2 \times (-6)$ : 2 et -6 sont donc des diviseurs de -12.
- *Soit* $n \in \mathbb{N} - \{0; 1\}$. $n^3 - n = n(n-1)(n+1)$ *: Les nombres* $n, (n-1) et\ (n+1)$ *sont* des diviseurs de $n^3 - n$

*Remarques :*

- Tout nombre entier a est un diviseur de 0, en effet : $0 = a \times 0$

- 0 ne divise aucun entier non nul.

### *2. Propriétés :*

a) Soit $n \in \mathbb{Z}^*$.Tout diviseur d de n vérifie : $1 \leq |d| \leq |n|$

b) tout entier relatif non nul a un nombre fini de diviseurs.

c) Divisibilité et opérations : Dans $\boldsymbol{Z}$ :

Si $a$ divise $b$ et $a$ divise $c$, alors pour tous entiers $m\ et\ n, a$ divise $mb + nc$

*Exercice d'application :*

*Montrer dans* $\mathbb{Z}$ *que si* $a/2b+3c$ *et* $a/b+c$ *alors* $a/b$ *et* $a/c$

### *3. Division euclidienne dans* $\mathbb{Z}$

*Propriété et définition :*

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

On dira que l'on a effectué, ou écrit, la *division euclidienne* de *a* par *b*.

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

*Preuve :*

- Cas ou $b>0$

Posons $q=E\left(\frac{a}{b}\right)$.On a alors : $q\leq\frac{a}{b}<q+1$.D'ou $0\leq a-bq<b$.

Posons $r=a-bq$.

On a donc $a=bq+r$.

Montrons par l'absurde que $r$ est unique.

Supposons :

$\exists(q,q')\in\mathbb{Z}^2$ ; $\exists(r,r')\in\mathbb{N}^2$ tels que :

$$a=bq+r\ ;\ a=bq'+r'\ ;\ 0\leq r<b\ ;\ 0\leq r'<b.$$

Alors :

$b(q-q')=r'-r$ et $-b<r'-r<b$.D'où : $-b<b(q-q')<b$donc $-1<q-q'<1$ c.à.d. $q-q'=0$ donc $q=q'$ d'où $r=r'$

- Cas où $b < 0$ :

$$b < 0 \Rightarrow -b > 0 \Rightarrow \exists!\,(q;r) \in \mathbb{Z} \times \mathbb{N}: a = b(-q) + ret 0 \leq r < -b$$

*Exemples* :

Division de $-53$ par $-9$ : $-53 = (-9) \times 6 + 1$

*Exercice d'application :*

*le quotient dans la* division euclidienne *de 1517 par un entier naturel* $x$ *est* $75$.

*Calculer* $x$ *et le reste.*

## *II. Congruences*

$a, a', b, b', c$ *sont deux entiers relatifs et* $n$ *un entier naturel non nul.*

### *1. Définition :*

On dit que $a$ est congru à $b$ modulo n lorsque $a - b$ est un multiple de $n$

On écrit alors $a \equiv b[n]$

*Exemples :*

$13 \equiv -12\ [5]$ *;*

$27 \equiv 103\ [2]$ *;*

$15 \equiv -12\ [9]$

### *2. Propriétés :*

*La congruence modulo n est une relation d'équivalence c.à.d. qu'elle est :*

- Réflexive : $a \equiv a[n]$
- Symétrique :si $a \equiv b[n]$ alors $b \equiv a[n]$, c'est pourquoi on dit souvent que $a$ *et* $b$ sont congrus modulo n.
- Et transitive :si $a \equiv b[n]$ et $b \equiv c[n]$ alors $a \equiv c[n]$

*3. Propriétés :*

*La congruence modulo n est compatible avec l'addition et avec la multiplication dans* $\mathbb{Z}$ *c.à.d. :*

a) Si $a \equiv a'[n]$ et $b \equiv b'[n]$alors $a + b \equiv a' + b'[n]$

b) Si $a \equiv a'[n]$ et $b \equiv b'[n]$alors $ab \equiv a'b'[n]$

*Conséquence : Compatibilité avec les puissances :*

Si $a \equiv b[n]$alors pour tout $k \in \mathbb{N}^*$on a : $a^k \equiv b^k[n]$

*3. Propriété caractéristique :*

$\boldsymbol{a \equiv b[n]} \Leftrightarrow$ *(* $\boldsymbol{a}$ *et* $\boldsymbol{b}$ *ont le même reste dans la division euclidienne par* $\boldsymbol{n}$*)*

*Cas particulier :*

*On a :* $\boldsymbol{a \equiv r[n]}$ *avec r est le reste dans la division euclidienne de* $\boldsymbol{a}$ *par* $\boldsymbol{n}$

*Preuve :*

*(⇒)* Supposons $a \equiv b[n]$ c.à.d. $n|a - b$ . On a :

$\exists(q, q') \in \mathbb{Z}^2$ ; $\exists(r, r') \in \mathbb{N}^2$ tels que :

$a = nq + r$ et $b = nq' + r'$ et $0 \leq r < n$ ; $0 \leq r' < n$

*Donc :* $a - b = n(q - q') + r - r'$

Et $-n < r' - r < n$.Or $n|a - b$

Donc $n|r - r'$

D'où $r - r' = 0$ c.à.d. $r = r'$

**(⇐)** Supposons que $a$ *et* $b$ ont le même reste r dans la division euclidienne par n.

Donc

$\exists(q, q') \in \mathbb{Z}^2 : a = nq + r$ et $b = nq' + r$.

D'où $a - b = n(q - q')$ donc $a \equiv b[n]$.

*Exercices d'application :*

*Exercice 1 :*

Déterminer le reste de la division euclidienne de a par b dans les cas suivants :

a) $a = 7^{61}$ ; $b = 4$

b) $a = 17^{500}$ ; $b = 7$

c) $a = 222^{333} + 333^{222}$ ; $b = 5$

*Exercice 2 :*

Montrer que pour tout entier naturel n on a :

a) Le nombre $7^{3n} - 1$est divisible par 9

b) Le nombre $3^{6n+3} + 1$est divisible par 7

c) Le nombre $3^{6n+2} + 3^{3n+1} + 1$est divisible par 13

## *4. Ensemble quotient $\mathbb{Z}/_{n\mathbb{Z}}$ :*

### *a.Définitions :*

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

i) Soit $a \in \mathbb{Z}$.

La classe d'équivalence de $a$est l'ensemble des entiers relatifs $x$ congrus à $a$ modulo $n$.

Elle est notée $\overline{a}$.(ou $\dot{a}$ ou $Cl(a)$)

On a alors :

$$\overline{a} = \{x \in \mathbb{Z}/x \equiv a[n]\}$$

Et on a :

$\overline{a} = \{x \in \mathbb{Z} \ / \ x\ a\ le\ même$ reste que $a$ dans la division euclidienne par n}

ii) L'ensemble noté

$$\mathbb{Z}/_{n\mathbb{Z}} = \{\overline{x}/x \in \mathbb{Z}\}$$

est appelé l'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n.

*Exercice d'application :*

*Déterminer* $\mathbb{Z}/_{n\mathbb{Z}}$ pour $n \in \{1; 2; 3; 4\}$

*b. Propriétés :*

Soit $n \in \mathbb{N}^*$.On a :

i) Il existe n classes d'équivalence modulo n et on a : $\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{0}; \overline{1}; \overline{2}; \ldots; \overline{n-1}\}$

ii) $\mathbb{Z} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \ldots \cup \overline{n-1}$ et $\forall (r; r') \in \{0; 1; 2; \ldots; n-1\}^2$ on a :

$$\overline{r} = \overline{r'} \Leftrightarrow r = r' \text{ et } r \neq r' \Leftrightarrow \overline{r} \cap \overline{r'} = \emptyset$$

iii) $\forall a \in \mathbb{Z}; \exists! r \in \{0; 1; 2; \ldots; n-1\}: a \in \overline{r}$

*c. Opérations dans* $\mathbb{Z}/_{n\mathbb{Z}}$ *:*

*a.Définitions :*

On définit dans $\mathbb{Z}/_{n\mathbb{Z}}$ l'addition et la multiplication par :

$\forall (\overline{a}; \overline{b}) \in \left(\mathbb{Z}/_{n\mathbb{Z}}\right)^2 : \overline{a} + \overline{b} = \overline{a+b}$ et $\overline{a} \times \overline{b} = \overline{ab}$

*Exercices d'application :*

*Exercice 1 :*

Calculer dans $\mathbb{Z}/_{10\mathbb{Z}}$ :

$$\overline{3} \times \overline{7}; \overline{3} + \overline{7}; \overline{9} \times \overline{9}; \overline{3}^{100}$$

*Exercice 2 :*

Résoudre dans $\mathbb{Z}/_{8\mathbb{Z}}$ les équations :

$$\overline{2}x = \overline{4} \; ; \; \overline{3}x^2 + \overline{4}x + \overline{1} = \overline{0}$$

*Exercice 3 :*

Résoudre dans $\left(\mathbb{Z}/_{7\mathbb{Z}}\right)^2$ le système :

$$\begin{cases} \overline{3}x + 5\overline{y} = \overline{6} \\ x + \overline{2}y = \overline{3} \end{cases}$$

## *III. Nombres premiers*

*Activités :*

Citer les diviseurs positifs des nombres : $2\ ;13\ ;41\ ;101$

### *1. Définition :*

Un entier naturel n est premier si et seulement s'il a exactement 2 diviseurs positifs.

*Remarques :*

- ✓ 2 est le seul nombre premier pair.
- ✓ 1 n'est pas un nombre premier.

*Exercice d'application :*

*Préciser les nombres premiers parmi les nombres suivants :*

*47 ;51 ;783 ; 111111*

### *2.Test de primalité d'un entier.*

*Propriétés :*

i)Le plus petit diviseur positif autre que $1$ d'un entier naturel supérieur ou égal a $2$ est un nombre premier.

ii) Soit $n \in \mathbb{N}/n \geq 2$. On a :

($n$ est premier) si et seulement si ($n$ n'est divisible par aucun nombre premier dont le carré est inferieur a $n$)

*Démonstrations :*

i) Si n n'est pas premier alors n possède un plus petit diviseur d distinct de  et de n :

$2 \leq d < n$

Si d n'est pas premier alors d possède un diviseur d' tel que :$2 \leq d' < d$.d' est un diviseur de n tel que $2 \leq d' < d < n$.Contradiction.

ii) Supposons n non premier. Soit p le plus petit diviseur de n distinct de 1. $2 \leq p < n$

On a : $\exists k \in \mathbb{Z}: n = pk$ donc k divise n et $2 \leq k \leq p < n$ donc $p \leq k \Rightarrow p^2 \leq kp = n$

*Remarque :*

*il y'a 25 Nombres premiers inférieurs ou égal à 100 :*

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,

43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 et 97

*Exercice d'application :*

Déterminer parmi les nombres suivants ceux qui sont premiers :

$$1499\,;961;1001;\ 2501\ ;\ 4441$$

*3. Théorème fondamental de l'arithmétique :*

Tout entier naturel $n \geq 2$ se décompose en un produit de facteurs premiers et cette décomposition est unique à l'ordre des facteurs près sous la forme :

$$n = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\ldots{p_k}^{\alpha_k}$$

Avec $p_1; p_2; \ldots; p_k$ des nombres premiers et $\alpha_1; \alpha_2; \ldots; \alpha_k$ des entiers naturels.

*Conséquences :*

- Soit $d \in \mathbb{N}^*$ et $n \in \mathbb{N}^*$

(d est un diviseur de n)$\Leftrightarrow d = {p_1}^{\beta_1}{p_2}^{\beta_2}\ldots{p_k}^{\beta_k}$

avec $\beta_1; \beta_2; \ldots; \beta_k \in \mathbb{N}$ et $\beta_i \leq \alpha_i$

- Le nombre de diviseurs positifs de n est : $(1+\alpha_1)(1+\alpha_2)\ldots(1+\alpha_k)$

*Démonstrations :*

*Existence de la décomposition*

Soit $n \in \mathbb{N}$ tel que : $n \geq 2$

- Si n est premier on a : $n = n$

- Sinon , alors le plus petit diviseur $p_1$de n distinct de 1 est premier et on a : $\exists q_1 \in \mathbb{N}^*: n = p_1 q_1$

Si $q_1$ est premier alors $n = p_1 q_1$

Sinon : alors le plus petit diviseur $p_2$de $q_1$ distinct de 1 est premier et on a : $\exists q_2 \in \mathbb{N}^*: q_1 = p_2 q_2$

Si $q_2$ est premier alors $n = p_1 p_2 q_2$ avec $2 \leq p_k \leq \ldots \leq p_2 \leq p_1 < n$et ainsi de suite …

Comme l'ensemble des diviseurs de n est fini alors cette algorithme d'arrête et on aura : $n = p_1 p_2 \ldots p_k$

***Unicité de la décomposition ( Th. De Gauss : Niveau Bac.Sc.Maths )***

Supposons que n a deux décompositions en un produit de facteurs premiers :

$n = p_1 p_2 \ldots p_k = q_1 q_2 \ldots q_{k'}$ avec $k \leq k' k = k'$

$p_1 | n \Rightarrow p_1 | q_1 q_2 \ldots q_{k'}$ or $q_1; q_2; \ldots; q_{k'}$ sont premiers donc ….$\exists m \in \{1; 2; \ldots; k'\}/$ $p_1 = q_m$

De même pour $p_2; p_3; \ldots; p_k$….donc $k = k'$ et $\{p_1; p_2; \ldots; p_k\} = \{q_1; q_2; \ldots; q_{k'}\}$

***4. Théorème :***

Il y a une infinité de nombres premiers

***Démonstration :*** *Par l'absurde*

Supposons que l'ensemble $P$ des nombres premiers positifs est fini :$P = \{p_1; p_2; \ldots; p_k\}$

Examinons le nombre $n = p_1 p_2 \ldots p_k + 1$

Comme $n \geq 2$ alors d'près le théorème fondamental de l'arithmétique

$$\exists p \in P \,/\, p \; divise \; n$$

*Or* $p \; divise \; p_1 p_2 \ldots p_k$ *donc* $p \; divise \; 1$ .Contradiction. Donc $P$ est infini.

***Exercice d'application :***

Décomposer en produit de facteurs premiers les nombres suivants :

$$a = 2772; b = 2904; c = 3276$$

En déduire le PGCD et le PPCM de

1. $a \; et \; b$
2. $b \; et \; c$
3. $a, b \; et \; c$

## *IV. Plus grand diviseur commun- Plus petit multiple commun*

### *1.Définitions :*

Soient $a, b \in \mathbb{Z}^*$

-Le plus grand diviseur commun de $a\ et\ b$ est le plus grand commun diviseur de *a et b* noté $PGCD(a,b)$ *ou* $a \wedge b$*ou* $\Delta(a,b)$

- Le plus petit multiple commun de *a et b* est le plus petit commun multiple strictement positif de $a\ et\ b$ noté $PPCM(a,b)$ *ou* $a \vee b$*ou* $M(a,b)$

***Remarque :***

*Si dans* $\mathbb{Z}$ *on a :* $a = bx + c$ *alors :* $a \wedge b = x \wedge c$

### *2. Propriétés :*

*Si* $a = \varepsilon \prod_{i=1}^{k} {p_i}^{\alpha_i}$ *et* $b = \varepsilon \prod_{i=1}^{k} {q_i}^{\beta_i}$ *;* $\varepsilon \in \{-1; 1\}$ et $p_1; p_2; \ldots; p_k$ *;* $q_1; q_2; \ldots; q_k$ étant des nombres premiers alors :

$$a \wedge b = \prod_{i=1}^{k} {p_i}^{\gamma_i}$$

$$a \vee b = \prod_{i=1}^{k} {p_i}^{\mu_i}$$

*Avec* $\gamma_i = inf\{\alpha_i; \beta_i\}$ *;* $\mu_i = sup\{\alpha_i; \beta_i\}$ *pour tout* $i \in \mathbb{N}\ et\ 0 \leq i \leq k$

### *3. Propriétés :*

Pour tous $a, b, c \in \mathbb{Z}$ on a :

i) $a \wedge b = b \wedge a$ ; $a \vee b = b \vee a$

*ii)* $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ ; $(a \vee b) \vee c = a \vee (b \vee c)$

*iii)* $a|b \Leftrightarrow a \wedge b = |a|$ ; $a|b \Leftrightarrow a \vee b = |b|$

*iv)* $(ca) \wedge (cb) = |c|(b \wedge a)$ ; $(ca) \vee (cb) = |c|(b \vee a)$

*v)* $(a \wedge b) \times (a \vee b) = |ab|$

## *4. Algorithme d'Euclide :*

### *Propriétés :*

- Si $(a, b) \in \mathbb{N}^{*2}$ tel que $b$ne divise pas $a$ et si $r$est le reste de la division euclidienne de $a\ par\ b$ alors : $a \wedge b = b \wedge r$
- Le $PGCD(a, b)$ est le dernier reste non nul dans l'algorithme des divisions successives de $a\ par\ b$

De plus on a :

- Pour tous $d \in \mathbb{N}^*$ *;*$a, b \in \mathbb{Z}^*$, on a : $a \wedge b = d \Rightarrow \exists (u, v) \in \mathbb{Z}^2 : d = au + bv$

*L'implication réciproque est fausse.*

***Preuve :***

Division euclidienne de $a\ par\ b$ : $a = bq_1 + r_1$ ; $0 \leq r_1 < b$

→ Si $r_1 = 0$ alors b divise a et PGCD (a ; b) = b

→ Sinon $r_1 \neq 0$ alors : $b = q_2 r_1 + r_2$ ; $0 \leq r_2 < r_1$

→ Si $r_2 = 0$ alors $r_1$ divise b et PGCD (a ; b) = PGCD (b ; $r_1$)= $r_1$

→ Sinon : $r_1 = q_3 r_2 + r_3$ ; $0 \leq r_3 < r_2$ et on a : $a \wedge b = b \wedge r_1 = r_1 \wedge r_2 = r_3$

→… Ainsi on construit ainsi une suite $(r_k)_{k \geq 1}$ strictement décroissante d'entiers naturels donc elle est finie tels que :

$$b > r_1 > r_2 > r_3 > \ldots > r_n > 0 \text{ et } r_{n+1} = 0$$

Avec n le plus petit entier tel que :

$$r_n \neq 0 \text{ et } r_{n+1} = 0. \text{Donc } a \wedge b = b \wedge r_1 = \ldots = r_n \wedge 0 = r_n$$

Comme chaque reste s'écrira sous forme d'une combinaison linéaire de $a\ et\ b$ alors le dernier reste non nul aussi, qui est le pgcd de $a\ et\ b$.

***Généralisation :***

*Dans* $\mathbb{Z}$ *:*

$$\boldsymbol{a_1 \wedge a_2 \wedge \ldots \wedge a_n = d \Rightarrow \exists (u_1, u_2, \ldots, u_n) \in \mathbb{Z}^2 : a_1 u_1 + a_2 u_2 + \ldots + a_n u_n = d}$$

***Preuve :*** *A faire par récurrence*

## *Exercices d'application :*

### *Exercice 1 :*

*Soit* $n \in \mathbb{N} / n \geq 5$.*Il s'agit de déterminer le* $pgcd(2n+1; n-5)$.

*Pour cela :*

*-Démontrer que :* $pgcd(2n+1; n-5) = pgcd(n-5\,; 11)$

*-En déduire les valeurs possibles du* $pgcd(2n+1; n-5)$ *suivant les valeurs de n.*

### *Exercice 2 :*

*Déterminer le pgcd de* $a$ *et* $b$ :

$$a)\ a = 2323\,;\ b = 2020 \quad b)\ a = 57123\,; b = 34722$$

### *Exercice 3 :*

*Déterminer* $d = a \wedge b$ *puis déterminer u et v dans* $\mathbb{Z}$ *tels que :* $au + bv = d$

*a)* $a = 202; b = 33$ *b)* $a = 1050; b = 735$