*Résumé de Cours D'ARITHMETIQUE*

**PROF : ATMANI NAJIB** **2BAC SM**

# L'ARITHMETIQUE

***A) Divisibilité dans $\mathbb{Z}$.***

***1)a)*** $a$ et $b$ deux entiers relatifs tels que $b \neq 0$

On dit que l'entier relatif $b$ divise $a$ s'il existe un entier relatif $k$ tel que $\boldsymbol{a = kb}$

On écrit : $\boldsymbol{b|a}$. et on dit que $a$ est divisible par $b$ ou $a$ est un multiple de $b$

***b)*** Si $b|m$ et $b|n$ on dit que $b$ est un diviseur commun de $m$ et $n$

c) Si $b|m$ et $b'|m$ , on dit que $m$ est un multiple commun de $b$ et $b'$

***B)* Propriétés de *Divisibilité dans* $\mathbb{Z}$.**

$a \in \mathbb{Z}$ ; $b \in \mathbb{Z}$ ; $c \in \mathbb{Z}$

1) $1|a$ et $-1|a$ et $a\,|a$ et $a\,|-a$ 2) $b|a \Rightarrow |b| \leq |a|$

3) $a/b \Rightarrow a/b \times c$ 4) $a/b \Rightarrow |a| \leq |b|$

5) $b|1 \Rightarrow b \in \{-1,1\}$ 6) $a|b$ et $b|a \Rightarrow |a| = |b|$

7) $a|b$ et c|d $\Rightarrow ac|bd$ 8) $a|b$ et $b|c \Rightarrow a|c$

9) $a|b \Rightarrow a|\ b\ c$ 10) $a|b$ et $b|c \Rightarrow a|c$

11) $a|b \Rightarrow a|\ b\ c$ 12) $a|m$ et $a|n \Rightarrow a|m + n$

13) $a|m$ et $a|n \Rightarrow a|m\ -n$

14) $a|m$ et $a|n \Rightarrow a|\alpha m + \beta n$ où $\alpha$ et $\beta$ sont des entiers relatifs quelconques.

15) $a/b \Rightarrow a^n/b^n \quad n \in \mathbb{N}$

***C) La division euclidienne dans* $\mathbb{Z}$**

$a$ et $b$ deux entiers relatifs tels que $b \neq 0$ ; ils existent un entiers relatif $q$ et un entier naturel $r$Tels que : $a = bq + r$ où $0 \leq r < |b|$

- L'entier $a$ s'appelle : ***Le divisé***
- L'entier $b$ s'appelle : ***Le diviseur***
- L'entier $q$ s'appelle : ***Le quotient***
- L'entier $r$ s'appelle : ***Le reste***

**Remarque :** Si $r$ est le reste de la division euclidienne par $b$ alors : $r \in \{0,1, \ldots, b-1\}$.

***D) Les nombres premiers***

a) On dit que l'entier $d$ est un diviseur **effectif** de l'entier relatif $a$ Si $d|a$ et $|d| \neq 1$ et $|d| \neq |a|$

b) On dit qu'un entier relatif non nul $p$ est **premier** s'il est différent de 1 et s'il n'admet pas de diviseurs effectifs.

- Un nombre premier p admet exactement deux diviseurs positifs 1 et |p|.
- Pour l'étude des nombres premiers on se contente d'étudier les nombres premiers positifs.

**c)si $\boldsymbol{a}$** un entier naturel non nul différent de 1 et non premier, le plus petit diviseur de $\boldsymbol{a}$ diffèrent de 1 est un nombre premier

**d)**Soit $n$ un entier naturel non nul, diffèrent de 1 et non premier, il existe un nombre premier $p$ qui divise l'entier $n$ et qui vérifie $p^2 \leq n$ .

**e)**Si un entier $n$ n'est divisible par aucun entier premier $p$ et qui vérifie $p^2 \leq n$ alors $n$ est premier.

**Remarque :** Cette propriété nous permet de déterminer si un nombre est premier ou non

**Théorème :** L'ensemble des nombres premiers est infini.

***E) Plus grand diviseurs commun***

**1)**On dit que le nombre $d$ est le plus grand diviseur commun de deux entiers relatifs $a$ et $b$ lorsque $d$ divise $a$ et $d$ divise $b$ et qu'il n'y a pas d'autre plus grands diviseurs de ces deux nombres. on note $d = PGDC\ (a, b) = a \wedge b$

**Propriétés :**1) $a \wedge a = |a|$ 2) $1 \wedge a = 1$

3) $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ 4) Si $b|a$ alors $a \wedge b = |b|$

5)si $d|a$ et $d|b$ alors $d|\ (a \wedge b)$ 6) $a \wedge b = a \wedge (a - b)$

7) $a \wedge b = |a| \wedge |b|$

**Définition :** On dit que deux entier relatifs $a$ et $b$ sont premiers entre eux si $a \wedge b = 1$.

***F) L'algorithme d'Euclide.***

**1)** Soit $a$ un entier naturel et $b$ un entier naturel non nul on a : $a = bq + r$ Où $0 \leq r < b$ alors on a : $a \wedge b = b \wedge r$

**2)**Soient $a$ et $b$ deux entier naturels non nuls. Le plus grand diviseur commun de $a$ et $b$ est le dernier reste non nul dans les divisions euclidiennes successives.

**3)** Soient $a$ et $b$ deux entier relatifs non nuls. Les diviseurs communs de $a$ et $b$ sont les diviseurs de $a \wedge b$.

On peut dire que : $D_a \cap D_b = D_{a \wedge b}$

***G) Le plus petit multiple commun.***

On dit que le nombre entier naturel $m$ est le plus petit multiple commun de deux entiers relatifs $a$ et $b$ lorsque $m$ est un multiple de $a$ et de $b$ et qu'il n'y a pas d'autre plus petit multiple non nuls de ces deux nombres. On note : $m = PPCM\ (a, b) = a \vee b$

**Propriétés :**1) $a \vee a = |a|$ 2) $a \vee b = b \vee a$

3) $a \vee 1 = |a|$ 4) Si $b|a$ alors $a \vee b = |a|$

5) $a \vee (b \vee c) = (a \vee b) \vee c$ 6) $a \vee b = |a| \vee |b|$

7) $a|(a \vee b)$ ; $b|(a \vee b)$ et $(a \vee b)|ab$

8)Si $a \vee b = m$ et $M$ un multiple commun de $a$ et $b$ alors $m|M$.

9) $(a \wedge b) \times (a \vee b) = |ab|$ 10) $ca \vee cb = c(a \vee b)$

11) $ca \wedge cb = c(a \wedge b$

**12)** Soient $a$ et $b$ et des entiers relatifs non nuls :

$$a \wedge b = d \Leftrightarrow \exists (\alpha, \beta) \in \mathbb{Z}^2;\ \begin{cases} a = \alpha d \\ b = \beta d \\ \alpha \vee \beta = 1 \end{cases}$$

13) Soient $a$ et $b$ et des entiers relatifs non nuls : $a \wedge b = d \Rightarrow \exists\ (u, v) \in \mathbb{Z}^2$ ; $d = au + b$

14)Théorème (Théorème de Bézout) : Soient $a$ et $b$ et des entiers relatifs non nuls :

$a \wedge b = 1 \Leftrightarrow \exists\ (u, v) \in \mathbb{Z}^2$ ; $1 = au + bv$

15)Théorème de Gauss :Soient $a$, $b$ et $c$ des entiers relatifs non nuls : $\begin{cases} c|ab \\ c \vee a = 1 \end{cases} \Rightarrow c|b$

**16)** Soient $a$, $b$ et $c$ des entiers relatifs non nuls :

$$\begin{cases} a/c \text{ et } b/c \\ a \vee b = 1 \end{cases} \Rightarrow ab/c$$

***H) LA CONGRUENCE MODULO n***

$a$ et $b$ deux entiers relatifs ; et $n$ un entier naturel non nul.
On dit que : $\boldsymbol{a}$ est congrue à $\boldsymbol{b}$ modulo $\boldsymbol{n}$ si $n|(\boldsymbol{b}-\boldsymbol{a})$.
On écrit : $\boldsymbol{a} \equiv \boldsymbol{b}\ [\boldsymbol{n}]$

**1)**Si $a \equiv b\ [n]$ alors $a$ et $b$ ont le même reste dans la division euclidienne par $n$

**2)a)** $(\forall a \in \mathbb{Z})$ $(a \equiv a\ [n])$ on dit que la relation de congruence est réflexive**.**

**b)** $(\forall (a, b) \in \mathbb{Z}^2)$( $a \equiv b\ [n] \Leftrightarrow b \equiv a\ [n]$ ) : on dit que la relation de congruence est symétrique.

**c)** $(\forall (a, b, c) \in \mathbb{Z}^3)$
$(a \equiv b\ [n]$ et $b \equiv c\ [n] \Rightarrow a \equiv c\ [n])$ : on dit que la relation de congruence est transitive.
On dit que la relation de congruence est une relation d'équivalence

**3)** Soit $n$ un entier naturel non nul.
Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$ alors :
a) $a + c \equiv b + d\ [n]$ On dit que la relation de congruence est compatible avec l'addition dans $\mathbb{Z}$
b) $ac \equiv bd\ [n]$ ; On dit que la relation de congruence est compatible avec la multiplication dans $\mathbb{Z}$
4) Si $a \equiv b\ [n]$ alors pour tout $k$ dans $\mathbb{N}$ on a : $a^k \equiv b^k\ [n]$

**5)** Soient $a$, $b$ et $c$ des entiers relatifs non nuls. et $n \in \mathbb{N}^*$ et $d = n \wedge c$ on a : $ac \equiv bc\ [n] \Leftrightarrow a \equiv b\ [\frac{n}{d}]$

6) $\begin{cases} ac \equiv bc[n] \\ c \vee n = 1 \end{cases} \Rightarrow a \equiv b[n]$ 7) $\begin{cases} a \equiv b[n] \\ m/n \end{cases} \Rightarrow a \equiv b[m]$

8) $\begin{cases} ac \equiv bc[p] \\ p \text{ premier et } p \nmid c \end{cases} \Rightarrow a \equiv b[p]$

***I) Les classes d'équivalences.***

Soit $n$ un entier naturel non nul. L'ensemble des entiers relatifs qui ont le même reste $r$ dans la division euclidienne par $n$ s'appelle la classe d'équivalence de $r$ et se note :

$\overline{r} = \{m \in \mathbb{Z} / m \equiv r\ [n]\} = \{nk + r \text{ où } k \in \mathbb{Z}\}$

$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}; \overline{1}; \overline{2}; \overline{3}; ...; \overline{n-1}\}$ S'appelle ensemble quotient

**1)** On définit dans $\mathbb{Z}/n\mathbb{Z}$ les deux lois :
a) L'addition **:** On pose $\overline{a} + \overline{b} = \overline{a+b}$
b) La multiplication **:** On pose : $\overline{a} \times \overline{b} = \overline{a \times b}$
**3)** Si $p$ est **premier** alors
dans $\mathbb{Z}/p\mathbb{Z}$ on a :$(\overline{a} \times \overline{b} = \overline{0} \Leftrightarrow \overline{a} = 0$ ou $\overline{b} = \overline{0})$

***J) DECOMPOSITION D'UN ENTIER EN FACTEURS DES NOMBRES PREMIERS***

1) Chaque entier **relatif** $m$ non nul s'écrit d'une façon unique comme le produit des facteurs premiers comme suite : $m = \varepsilon p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times ... \times p_n^{\alpha_n} = \prod_{k=1}^{k=n} p_k^{\alpha_k}$ où $\varepsilon \in \{-1,1\}$

**2)**Soit $a$ un entier relatif dont la décomposition est de la forme : $a = \varepsilon p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times ... \times p_n^{\alpha_n} = \prod_{k=1}^{k=n} p_k^{\alpha_k}$

3) un entier $d$ non nul divise l'entier $a$ si et seulement si $d$ à une décomposition de la forme

$$d = \varepsilon p_1^{\beta_1} \times p_2^{\beta_2} \times p_3^{\beta_3} \times ... \times p_n^{\beta_n} = \prod_{k=1}^{k=n} p_k^{\beta_k}$$

où $(\forall i \in [\![1, n]\!])(0 \leq \beta_i \leq \alpha_i)$

**4)** $a = \varepsilon p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times ... \times p_n^{\alpha_n} = \prod_{k=1}^{k=n} p_k^{\alpha_k}$

est un entier, le nombre des diviseurs de $a$ est : $2(\alpha_1+1)(\alpha_2+1)...(\alpha_n+1)$

**5)**Soit $a$ un entier relatif dont la décomposition est de la forme : $a = \varepsilon p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times ... \times p_n^{\alpha_n} = \prod_{k=1}^{k=n} p_k^{\alpha_k}$

un entier $m$ est un multiple de $a$ si et seulement si

$$m = \varepsilon p_1^{\beta_1} \times p_2^{\beta_2} \times p_3^{\beta_3} \times ... \times p_n^{\beta_n} = \prod_{k=1}^{k=n} p_k^{\beta_k}$$

6)Soient $a = \prod_{k=1}^{k=n} p_k^{\alpha_k} = 1$ et $b = \prod_{k=1}^{k=n} p_k^{\beta_k}$ deux entiers

$$a \wedge b = \prod_{k=1}^{k=n} p_k^{\inf(\alpha_k;\beta_k)} \text{ et } a \vee b = \prod_{k=1}^{k=n} p_k^{\sup(\alpha_k;\beta_k)}$$

***K) L'équation ax + by = c***

**1)**L'équation $(E)$ : $ax + by = c$ admet une solution si et seulement si $(a \wedge b)|c$

**2)**Si le couple $(x_0; y_0)$ est une solution de l'équation $(E)$ : $ax + by = c$ alors, l'ensemble des solutions de $(E)$ est :

$$S = \left\{ \left( x_0 + \frac{kb}{a \wedge b}; y_0 - \frac{ka}{a \wedge b} \right); k \in \mathbb{Z} \right\}$$

***L) Le P.G.D.C et le P.P.M.C de plusieurs nombres.***

**1)** Soient $a_1, a_2, \ldots, a_n$ des entiers relatifs non nuls, le plus grand entier naturel $d$ qui divise en même temps tous les nombres $a_1, a_2, \ldots, a_n$ s'appelle le plus grand diviseur commun des nombres $a_1, a_2, \ldots, a_n$ et se note : $d = a_1 \wedge a_2 \wedge \ldots \wedge a_n$

**2)** Soient $a_1, a_2, \ldots, a_n$ des entiers relatifs non nuls ; on a : $a_1 \wedge a_2 \wedge \ldots \wedge a_n = (a_1 \wedge a_2 \wedge \ldots \wedge a_{n-2}) \wedge (a_{n-1} \wedge a_n)$

**3)**Théorème (*Généralisation de Bézout*)
Si $d = a_1 \wedge a_2 \wedge \ldots \wedge a_n$ alors $\exists(\alpha_i) 1 \leq i \leq n$ telle que :

$$d = \sum_{i=1}^{n} \alpha_i a_i$$

**3)** On dit que les entiers relatifs non nuls : $a_1, a_2, \ldots, a_n$ sont premiers entre eux si :$a_1 \wedge a_2 \wedge \ldots \wedge a_n = 1$

**4)**$a_1 \wedge a_2 \wedge \ldots \wedge a_n = 1$si et seulement si

$\exists(\alpha_i) 1 \leq i \leq n$ telle que : $1 = \sum_{i=1}^{n} \alpha_i a_i$

**5)** Soient $a_1, a_2, \ldots, a_n$ des entiers relatifs non nuls, le plus petit entier naturel $m$ qui est multiple en même temps tous les nombres $a_1, a_2, \ldots, a_n$ s'appelle le plus petit multiple commun des nombres $a_1, a_2, \ldots, a_n$ et se note :
$m = a_1 \vee a_2 \vee \ldots \vee a_n$

***M) Propriétés des nombres premiers.***

1) Si $p$ et $q$ sont des nombres premiers positifs alors ils sont premiers entre eux.

2) Si $p$ est premier alors il est premier avec tout nombre entier non nul $a$ tel que $p \nmid a$

**3)** $\begin{cases} p/ab \\ p \text{ premier et } p \nmid a \end{cases} \Rightarrow p/b$

4) $\begin{cases} p/ab \\ p \text{ premier} \end{cases} \Rightarrow p/a \text{ ou } p/b$

5) $\begin{cases} p/\prod_{i=1}^{n} a_i \\ p \text{ premier} \end{cases} \Rightarrow \exists 1 \le i \le n \; p/a_i$

6) $\begin{cases} p/\prod_{i=1}^{n} p_i \\ p \text{ premier} \\ \forall 1 \le i \le n;\ p_i \text{ premier} \end{cases} \Rightarrow \exists 1 \le i \le n;\ p = p_i$

***N) Théorème (théorème de Fermat)***

Si $p$ est un nombre premier et $a$ un entier relatif non nul et pas divisible par $p$ alors :

$a^{p-1} - 1$ est divisible par $p$ c'est-à-dire :

$a^{p-1} \equiv 1[p]$ ou encore : $a^p \equiv a[p]$

***P) SYSTEMES DE NUMERATION***

**1)** Soit $b$ un entier naturel tel que: $b > 1$

Chaque entier naturel non nul $n$ s'écrit d'une façon unique de la forme : $n \equiv a_m b^m + a_{m-1} b^{m-1} + ... + a_1 b^1 + a_0$

Où : les $(a_i)1 \le i \le n$ sont des entiers naturels

$0 \le a_i \le b - 1$ et $am \neq 0$

**Notation :**

Si $n \equiv a_m b^m + a_{m-1} b^{m-1} + ... + a_1 b^1 + a_0$ on écrit :

$n \equiv \overline{a_m a_{m-1} ... a_1 a_0}_{(b)}$ Cette écriture s'appelle l'écriture de l'entier $n$ dans la base $b$

**Remarques :**

**1)** On peut effectuer la somme dans une base donnée $b$ par deux façons différentes :

a) La décomposition :

$\overline{2534}_{(7)} + \overline{631}_{(7)} = 2\times7^3 + 5\times7^2 + 3\times7^1 + 4\times7^0 +$

$+6\times7^2 + 3\times7^1 + 1\times7^0$

$\overline{2534}_{(7)} + \overline{631}_{(7)} = 2\times7^3 + 11\times7^2 + 6\times7^1 + 5\times7^0$

$\overline{2534}_{(7)} + \overline{631}_{(7)} = 3\times7^3 + 4\times7^2 + 6\times7^1 + 5\times7^0$

$\overline{2534}_{(7)} + \overline{631}_{(7)} = \overline{3465}_{(7)}$

b) Calcul direct avec le retenu

**2)** Le produit : Il est préférable d'effectuer le produit en utilisant le calcul direct avec le retenu car la décomposition

3)Pour effectuer des opérations dans différentes bases on développe les deux nombres dans la base 10 ; on effectue L'opération et on écrit le résultat dans la base demandée.

**Exemple :** effectuer dans la base 9

$\overline{6432}_{(7)} \times \overline{54}_{(8)}$

**Solution :** $\overline{6432}_{(7)} \times \overline{54}_{(8)} =$

$= (6 \times 7^3 + 4 \times 7^2 + 3 \times 7 + 2) \times (5 \times 8 + 4)$

$= 100188$

$= 1 \times 9^5 + 6 \times 9^4 + 2 \times 9^3 + 3 \times 9^2 + 8 \times 9 + 0$

$= \overline{162380}_{(9)}$

***Q) CRITERES DE DIVISIBILITE DES NOMBRES 5,25,3,9,11 ET 4 :*** Soit $x$ un entier naturel non nul tel que :

$x \equiv a_n 10^n + a_{n-1} 10^{n-1} + ... + a_1 10^1 + a_0$ où $0 \le a_i \le 9$ ; on a :

1) $x \equiv 0\ [5] \Leftrightarrow a_0 = 0$ ou $a_0 = 5$

2) $x \equiv 0\ [25] \Leftrightarrow \overline{a_1 a_0} \in \{0,25,50,75\}$

3) $x \equiv 0\ [3] \Leftrightarrow \sum_{i=0}^{n} a_i \equiv 0\ [3]$

4) $x \equiv 0\ [9] \Leftrightarrow \sum_{i=0}^{n} a_i \equiv 0\ [9]$

5) $x \equiv 0\ [11] \Leftrightarrow \sum_{i=0}^{n} (-1)^i a_i \equiv 0\ [11]$

6) $x \equiv 0\ [4] \Leftrightarrow \overline{a_1 a_0} \equiv 0\ [4]$

***X) L'ENSEMBLE $\mathbb{Z}/p\mathbb{Z}$ OU $p$ EST UN NOMBRE PREMIER.***

1)Pour tous entiers relatifs non nuls $a$ et n :

$a \wedge n = 1 \Leftrightarrow (\exists m \in \mathbb{Z})(am = 1\ [n])$

**2)**Si $p$ est un nombre premier positif alors tout élément $\overline{x} \neq \overline{0}$ admet un inverse dans $\mathbb{Z}/p\mathbb{Z}$

*« C'est en forgeant que l'on devient forgeron » Dit un proverbe.*

*C'est en s'entraînant régulièrement aux calculs et exercices*

*Que l'on devient un mathématicien*