AlloSchool

Mathématiques : 2Bac SMA-SMB

Séance 9-1-1 : Arithmétique dans $\mathbb{Z}$ - Partie 1 (Cours)

**Professeur : Mr CHEDDADI Haitam**

Sommaire



---

# I- P.G.C.D - P.P.M.C

## 1-1/ Rappels et compléments

### Définition 1

Soit $a$ et $b$ deux entiers relatifs non nulles.

Le plus grand commun diviseur de $a$ et $b$, noté $a \wedge b$ ou $PGCD(a, b)$, est le plus grand des diviseurs positifs communs à $a$ et $b$.

Le plus petit commun multiple de $a$ et $b$, noté $a \vee b$ ou $PPCM(a, b)$, est le plus petit des multiples strictement positifs communs à $a$ et $b$.

On convient que : $a \wedge 0 = |a|$ et $a \vee 0 = 0$

### Remarques

Soit $a$ et $b$ deux entiers relatifs non nulles. Si $d = a \wedge b$ et $m = a \vee b$ alors :

- $d \geq 1$ et $d/a$ et $d/b$
- $m \geq 1$ et $a/m$ et $b/m$
- Pour toute $c \in \mathbb{N}^*$ : $[(c/a \; et \; c/b) \Rightarrow c/d]$ et $[(a/c \; et \; b/c) \Rightarrow m/c]$
- Pour toute $c \in \mathbb{N}^*$ : $[(c/a \; et \; c/b) \Rightarrow c \leq d]$ et $[(a/c \; et \; b/c) \Rightarrow m \leq c]$
- $|a| \wedge |b| = d$ et $a \wedge 1 = 1$ et $a \wedge a = a \wedge 0 = |a|$
- $|a| \vee |b| = m$ et $a \vee 1 = |a|$ et $a \vee a = |a|$

### Proposition 1

Soit $a$, $b$ et $c$ des entiers relatifs non nulles et $n$ un entier naturel. Alors :

| | |
|---|---|
| 1 $a \wedge b = b \wedge a$ | 7 $(a \vee b) \vee c = a \vee (b \vee c)$ |
| 2 $a \vee b = b \vee a$ | 8 $(ca) \vee (cb) = \lvert c \rvert (a \vee b)$ |
| 3 $a/b \Leftrightarrow a \wedge b = \lvert a \rvert \Leftrightarrow a \vee b = \lvert b \rvert$ | 9 $\begin{cases} c/a \\ c/b \end{cases} \Rightarrow \left(\frac{a}{c}\right) \vee \left(\frac{b}{c}\right) = \frac{a \vee b}{\lvert c \rvert}$ |
| 4 $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ | 10 $a^n \wedge b^n = (a \wedge b)^n$ |
| 5 $(ca) \wedge (cb) = \lvert c \rvert (a \wedge b)$ | 11 $a^n \vee b^n = (a \vee b)^n$ |
| 6 $\begin{cases} c/a \\ c/b \end{cases} \Rightarrow \left(\frac{a}{c}\right) \wedge \left(\frac{b}{c}\right) = \frac{a \wedge b}{\lvert c \rvert}$ | 12 $(a \wedge b).(a \vee b) = \lvert ab \rvert$ |

## 1-2/ Calcul pratique du P.G.C.D : algorithme d'euclide

### Proposition 2

Soit $a \in \mathbb{Z}^*$ et $b \in \mathbb{N}^*$.

Lorsque $b$ ne divise pas $a$, le plus grand commun diviseur des entiers $a$ et $b$ est égal au dernier reste non nul obtenu grâce à l'algorithme d'Euclide.

## 1-3/ Nombres premiers entre eux

### Définition 2

Soit $a$ et $b$ deux entiers relatifs non nulles.

On dit que $a$ et $b$ sont premiers entre eux si le seul diviseur positif commun à $a$ et $b$ est 1, c'est-à-dire si $a \wedge b = 1$:

### Théorème 1

Soit $a$ et $b$ deux entiers relatifs non nulles, et $d$ un entier naturel non nul.

Alors :

$$d = a \wedge b \Leftrightarrow \left[\left(\exists\,(\alpha;\beta) \in \mathbb{Z}^2\right)\; a = \alpha d \; et \; b = \beta d \; et \; \alpha \wedge \beta = 1\right]$$

### Théorème 2

Soit $(a, b) \in (\mathbb{Z}^*)^2$

On a l'implication :

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

### Remarques

Le couple $(u;v)$ n'est pas unique. Par exemple :

$$9 \wedge 4 = 1 = 1 \times 9 - 2 \times 4 \ (u = 1 \ et \ v = -2)$$
$$9 \wedge 4 = (-43) \times 9 + 97 \times 4 \ (u = -43 \ et \ v = 97)$$

La réciproque du théorème 2 est incorrecte, contre-exemple : $3 \times 5 + 7 \times (-1) = 8$ mais $3 \wedge 7 \neq 8$.

## 1-4/ Théorème de bezout

### Théorème 3

Soit $a$ et $b$ deux entiers relatifs non nulles.

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

### Applications

En utilisant le théorème de Bezout, montrer que pour tout $n \in \mathbb{N}$ :

1 $(5n+3) \wedge (2n+1) = 1$
2 $(2n-1) \wedge (3-7n) = 1$

## 1-5/ Détermination des coefficients du théorème de bezout

L'inconvénient du théorème du Bezout, sous sa forme théorique, est qu'il ne fournit pas les coefficients $u$ et $v$ intervenant dans la relation $au + bv = 1$.

L'algorithme d'Euclide fournit une réponse pratique à ce problème.

À titre d'exemple, posons : $a = 155$ et $b = 23$.

## 1-6/ Applications du théorème de bezout

### Théorème 4

Soit $a$, $b$ et $c$ des entiers relatifs non nuls.

On a l'implication : $(a/bc \ et \ a \wedge b = 1) \Rightarrow a/c$

Ce résultat est connu sous le nom de « Théorème de Gauss ».

### Remarque

Dans le théorème de Gauss, la condition $a \wedge b = 1$ est nécessaire.

Par exemple : $12/9 \times 8$ mais $12$ ne divise ni le nombre $9$ ni le nombre $8$.

### Théorème 5

Soit $a$, $b$ et $c$ des entiers relatifs non nuls.

On a l'implication : $(a/c \ et \ b/c \ et \ a \wedge b = 1) \Rightarrow ab/c$

### Remarque

Dans le théorème 5, la condition $a \wedge b = 1$ est nécessaire.

Par exemple : $8/48$ et $12/48$ mais $12 \times 8$ ne divise pas $48$.

### Proposition 3

Soit $a$, $b$ et $c$ des entiers relatifs non nuls.

Alors :

1- $(a \wedge b = 1 \; et \; a \wedge c = 1) \Leftrightarrow a \wedge bc = 1$

2- Pour tout $(m, n) \in (\mathbb{N}^*)^2$ : $(a \wedge b = 1 \Leftrightarrow a \wedge b^n = 1)$ et $(a \wedge b = 1 \Leftrightarrow a^m \wedge b^n = 1)$

## 1-7/ L'équation diophantienne $ax + by = c$

### Théorème 6

Soit $a$, $b$ et $c$ des entiers relatifs tels que $ab \neq 0$

L'équation d'inconnue $ax + by = c$ a des solutions si, et seulement si, $a \wedge b$ divise $c$.

### Théorème 7

Si le couple $(x_0; y_0)$ est une solution de l'équation $(E)$ : $ax + by = c$, alors l'ensemble solution de l'équation $(E)$ s'écrit sous la forme :

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

## 1-8/ P.G.C.D et P.P.C.M d'un nombre fini d'entiers relatifs

### Définition 3

Soit $n$ un entier naturel, $n \geq 2$, et des entiers relatifs non nuls $a_1, a_2, \ldots a_n$

Le plus grand commun diviseur des entiers $a_1, a_2, \ldots a_n$, noté $a_1 \wedge a_2 \wedge \ldots \wedge a_n$, est le plus grand des diviseurs positifs communs à $a_1, a_2, \ldots a_n$.

Le plus petit commun multiple des entiers $a_1, a_2, \ldots a_n$, noté $a_1 \vee a_2 \vee \ldots \vee a_n$ ou $PPCM\,(a_1, a_2, \ldots a_n)$, est le plus petit des multiples positifs communs $a_1, a_2, \ldots a_n$.

### Théorème 8

Soit $n$ un entier naturel, $n \geq 2$, et des entiers relatifs non nuls $a_1, a_2, \ldots a_n$.

I1 existe des entiers relatifs $u_1, u_2, \ldots u_n$ tels que : $\sum_{i=1}^{n} a_i . u_i = \delta$, où $\delta$ désigne le plus grand commun diviseur de $a_1, a_2, \ldots a_n$.

### Définition 4

Soit $n$ un entier naturel, $n \geq 2$, et des entiers relatifs non nuls $a_1, a_2, \ldots a_n$.

On dit que les entiers $a_1, a_2, \ldots a_n$ sont premiers entre eux si 1 est le seul diviseur positif commun à tous ces entiers, c'est-à-dire : $a_1 \wedge a_2 \wedge \ldots \wedge a_n = 1$

### Remarques

Attention, dire que des entiers sont premiers entre eux ne signifie pas qu'ils sont entre eux deux à deux. Par exemple, les trois entiers $a = 8$, $b = 7$ et $c = 12$ sont premiers entre eux. Pourtant, les entiers $a$ et $c$ ont 4 pour grand diviseur commun : $a \wedge c = 4 > 1$

La relation $(a \vee b).(a \wedge b) = |ab|$ n'est pas valable pour plus de deux entiers relatifs.

Contre-exemple : $6 \vee 10 \vee 15 = 30$ et $6 \wedge 10 \wedge 15 = 1$

donc : $(6 \vee 10 \vee 15).(6 \wedge 10 \wedge 15) = 30 \neq 6 \times 10 \times 15$

c'est-à-dire qu'on a en général : $(a \vee b \vee c).(a \wedge b \wedge c) \neq |abc|$

Le résultat du théorème 8 reste aussi valable pour plus de deux entiers. Plus précisément : $(n \geq 2)$ $\delta = a_1 \wedge a_2 \wedge \ldots \wedge a_n$ signifie qu'il existe $(a'_1, a'_2, \ldots a'_n) \in \mathbb{Z}^n$ tel que pour tout $i \in \{1; 2; \ldots; n\}$ : $a_i = \delta a'_i$ et $a'_1 \wedge a'_2 \wedge \ldots \wedge a'_n = 1$.

### Théorème 9

Soit $n$ un entier naturel, $n \geq 2$, et des entiers relatifs non nuls $a_1, a_2, \ldots a_n$.

Les entiers $a_1, a_2, \ldots a_n$ sont premiers entre eux si, et seulement si :

$$\exists\, (u_1; u_2; \ldots u_n) \in \mathbb{Z}^n \ ; \ \sum_{i=1}^{n} a_i . u_i = 1$$

Autrement dit :

$$(a_1 \wedge a_2 \wedge \ldots \wedge a_n = 1) \Leftrightarrow \left[\exists\, (u_1; u_2; \ldots u_n) \in \mathbb{Z}^n \ ; \ \sum_{i=1}^{n} a_i . u_i = 1\right]$$

## 1-9/ Congruence modulo n (rappels et compléments)

### Définition 5

Soit $n$ un entier naturel non nul.

On dit que deux entiers relatifs $a$ et $b$ sont congrus modulo $n$ si $n$ divise $b - a$, c'est-à-dire s'il existe un entier $k \in \mathbb{Z}$ tel que $b = a + kn$.

On écrit : $a \equiv b \ [n]$

### Proposition 4

Soit $n$ un entier naturel non nul.

La relation « de congruence» est une relation d'équivalence sur $\mathbb{Z}$, c'est-à-dire :

1) Elle est réflexive : $(\forall a \in \mathbb{Z})\ a \equiv a \ [n]$

2) Elle est symétrique : $\left(\forall\, (a; b) \in \mathbb{Z}^2\right)\ (a \equiv b \ [n] \Rightarrow b \equiv a \ [n])$

3) Elle est transitive : $\left(\forall\, (a; b; c) \in \mathbb{Z}^3\right)\ (a \equiv b \ [n]\ et\ b \equiv c \ [n] \Rightarrow a \equiv c \ [n])$

### Proposition 5

Soit $n$ un entier naturel non nul et $(a; b; c; d) \in \mathbb{Z}^4$. Alors :

1) $a \equiv b \ [n] \Leftrightarrow$(Les restes respectifs des divisions euclidiennes de $a$ et $b$ par $n$ sont égaux)

2) Si $a \equiv b \ [n]$ et $c \equiv d \ [n]$, alors : $a + c \equiv b + d \ [n]$ et $ac \equiv bd \ [n]$.

3) Si $a \equiv b \ [n]$ et $k \in \mathbb{Z}$, alors : $ka \equiv kb \ [n]$

4) Si $a \equiv b \ [n]$ et $p \in \mathbb{N}$, alors : $a^p \equiv b^p \ [n]$

### Théorème 10

Soit $a$, $b$ et $c$ des entiers relatifs non nulles et $n \in \mathbb{N}^*$.

Si $d = c \wedge n$ alors :

$$ac \equiv bc \ [n] \Leftrightarrow a \equiv b \ \left[\frac{n}{d}\right]$$

### Proposition 6

Soit $a$, $b$ et $c$ des entiers relatifs non nuls et $(n; p) \in (\mathbb{N}^*)^2$ tels que $c \wedge n = 1$

Alors :

$$1\ \ ac \equiv bc\ [n] \Leftrightarrow a \equiv b\ [n]$$

$$2\ \begin{cases} a \equiv b\ [n] \\ p/n \end{cases} \Rightarrow a \equiv b\ [p]$$

$$3\ \begin{cases} ac \equiv bc\ [p] \\ p\ premier \\ p\ ne\ divise\ pas\ c \end{cases} \Rightarrow a \equiv b\ [p]$$

# II- Les nombres premiers

## 2-1/ Rappels et compléments

### Définition 6

Un entier relatif $p$ est dit premier lorsqu'il admet exactement quatre diviseurs.

### Remarques

Si $p$ est un entier premier dans $\mathbb{N}$, alors $-p$ est premier dans $\mathbb{Z}$. C'est pourquoi dans cette section, nous nous limitons à l'ensemble $\mathbb{N}$ des entiers naturels.

L'ensemble des nombres premiers (positifs) est noté $\mathbb{P}$.

Un entier $n \geq 2$ non premier est dit composé.

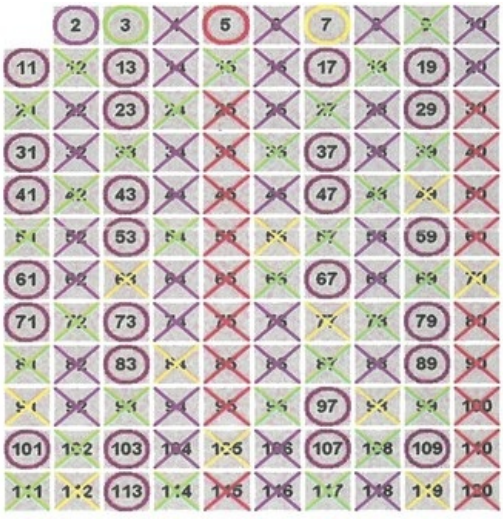
### Théorème 11

Soit $n$ un entier composé supérieur ou égal à 2. Alors :

1) Le plus petit diviseur positif de n différent de 1 est un nombre premier.

2) $n$ est un produit de nombres premiers. En particulier, $n$ possède au moins un diviseur premier.

3) $n$ possède un facteur premier $p$ tel que $p^2 \leq n$.



| | | | |
|---|---|---|---|
| 2 | 3 | 5 | 7 |
| 11 | 13 | 17 | 19 |
| 23 | 29 | 31 | 37 |
| 41 | 43 | 47 | 53 |
| 59 | 61 | 67 | 71 |
| 73 | 79 | 83 | 89 |
| 97 | 101 | 103 | 107 |
| 109 | 113 | | |

Les nombres premiers inférieures ou égales à 120

### Théorème 12

L'ensemble $\mathbb{P}$ des nombres premiers positifs est infini.

### Théorème 13

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

En d'autres termes : $(p \in \mathbb{P}\ et\ q \in \mathbb{P}\ et\ p \neq q) \Rightarrow p \wedge q = 1$

2) Si $p \in \mathbb{P}$, alors $p$ est premier avec tous les entiers qu'il ne divise pas.

En d'autres termes : $(\forall a \in \mathbb{Z})\ (\forall p \in \mathbb{P})\ [(p\ ne\ divise\ pas\ a) \Rightarrow p \wedge a = 1]$

### Proposition 7

Soit $(a, b) \in \mathbb{Z}^2$ et $p$ un nombre premier. Alors :

$$p/ab \Leftrightarrow (p/a\ ou\ p/b)$$

### Corollaire

Soit $a_1, a_2, \ldots a_n$ des entiers relatifs et $p$ un nombre premier. Alors :

$$p/a_1.a_2.\ldots.a_n \Leftrightarrow (\exists i \in \{1; 2; \ldots; n\}\ p/a_i)$$

Soit $a \in \mathbb{Z}$ et $p$ un nombre premier. Alors :

$$(\forall n \in \mathbb{N}^*)\ p/a^n \Leftrightarrow p/a$$

Soit $p_1, p_2, \ldots, p_n$ et $p$ des nombres premiers. Alors :

$$p/p_1.p_2.\ldots.p_n \Leftrightarrow (\exists i \in \{1; 2; \ldots; n\}\ p = p_i)$$

## 2-2- Petit théorème de fermat

### Théorème 14

1) Si $p$ est un nombre premier positif, alors il divise $a^p - a$, pour tout $a \in \mathbb{Z}$.

Autrement dit : $(\forall a \in \mathbb{Z})\ a^p \equiv a\ [p]$

2) Si $p$ est un nombre premier positif, alors pour tout $a \in \mathbb{Z}$ : $p \wedge a = 1 \Rightarrow a^{p-1} \equiv 1\ [p]$

### Remarques

La réciproque du petit théorème de Fermat n'est pas vraie. Autrement dit, si $a^{p-1} \equiv 1\ [p]$, alors l'entier $p$ n'est pas nécessairement premier. A titre d'exemple, le nombre
$p = 341 = 31 \times 11$ n'est pas premier, or, il divise $2^{341} - 2$ car :

$$2^{341} - 2 = 2\left(2^{340} - 1\right) = 2\left(\left(2^{10}\right)^{34} - 1\right) = 2\left(2^{10} - 1\right)\sum_{k=0}^{33} 2^{10k} = 2 \times 3 \times 341 \times \sum_{k=0}^{33} 2^{10k}$$

Le petit théorème de Fermat permet de calculer le reste de n'importe quel entier assez grand modulo un nombre premier positif $p$.

## 2-3/ Décomposition en produit de facteurs premiers

### Théorème 15

Tout élément de $\mathbb{Z}^* - \{1; -1\}$ admet une décomposition en produit de nombres premiers, unique à
l'ordre près des facteurs.

Autrement dit, si $n \in \mathbb{Z}^* - \{1; -1\}$, il existe $N \in \mathbb{N}^*$, $\varepsilon \in \{1; -1\}$, des nombres premiers deux à deux distincts $p_1, p_2, \ldots p_N$, et des entiers $\alpha_1, \alpha_2, \ldots \alpha_N$ tels que :
$n = \varepsilon.{p_1}^{\alpha_1}.{p_2}^{\alpha_2}\ldots{p_N}^{\alpha_N}$

Ce théorème est connu sous le nom « Théorème fondamental de l'arithmétique ».

## 2-4/ Applications de la décomposition en produit de facteurs premiers

### Théorème 16

Soit $n \in \mathbb{Z}^* - \{1; -1\}$ et sa décomposition $n = \varepsilon.{p_1}^{\alpha_1}.{p_2}^{\alpha_2}\ldots{p_N}^{\alpha_N}$ en produit de facteurs premiers.

Les diviseurs de $n$ sont les entiers relatifs : $d = \varepsilon' . {p_1}^{\gamma_1} . {p_2}^{\gamma_2} \ldots {p_N}^{\gamma_N}$ avec
$\forall k \in \{1; 2; \ldots; N\}\ 0 \leq \gamma_k \leq \alpha_k$ et $\varepsilon' \in \{1; -1\}$

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