CENTRE D'ENCADREMENT SCOLAIRE LES MAJORANTS
**34, Rue NKENI Talangaï (Arrêt Libanga)**
**Cours de Mr. Teddy Fiacre MOBEMOUANA M**
**Tél : 06 959 57 86/05 592 21 90/01 130 18 80**

# ARITHMETIQUE

## I- LES ENSEMBLES $\mathbb{N}$ et $\mathbb{Z}$

### 1- L'ensemble $\mathbb{N}$

L'ensemble $\mathbb{N}$ désigne l'ensemble des entiers naturels et $\mathbb{N}^*$ désigne l'ensemble des entiers naturels non nul. $\mathbb{N} = \{0\,;\,1\,;\,2\,;\,3\,;\,4\,;\cdots\}$ et $\mathbb{N}^* = \{1\,;\,2\,;\,3\,;\,4\,;\cdots\}$ ou $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$

### 2- L'ensemble $\mathbb{Z}$

L'ensemble $\mathbb{Z}$ désigne l'ensemble des entiers relatifs et $\mathbb{Z}^*$ désigne l'ensemble des entiers relatifs non nul. $\mathbb{Z} = \{\cdots -4\,;\,-3\,;\,-2\,;\,-1\,;\,0\,;1\,;\,2\,;\,3\,;\,4\,;\,\cdots\}$ et $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$

### 3- Division euclidienne dans $\mathbb{Z}$ :

Soit $a$ et $b$ deux entiers relatifs tels que : $b \neq 0$
Il existe un unique couple $(q;r)$ de $\mathbb{Z} \times \mathbb{N}$ tel que $\boxed{a = bq + r}$ et $0 \leqslant r <\mid b \mid$.
Les nombres $d$ et $r$ s'appellent respectivement le quotient et le reste de la division euclidienne de $a$ par $b$.

### 4- Multiples et diviseurs d'un entier relatif :

Soit $a$ et $b$ deux entiers relatifs tels que : $b \neq 0$
S'il existe un entier relatif $k$ tel que : $\boxed{a = bk}$
On dit que $a$ est un multiple de $b$ et $b$ est un diviseur de $a$ (ou $b$ divise $a$ : on note $b \mid a$)

**Exemples :**
$35 = 5 \times 7$ : 35 est multiple de 5 et de 7 ; 5 divise 35 : $5 \mid 35$ et 7 divise 35 : $7 \mid 35$.
$15 = (-5)\times(-3)$ : 15 est multiple de -5 et de -3 ; -5 divise 15 : $-5 \mid 15$ et -3 divise 15 : $-3 \mid 15$.

**Propriétés :** Soient $a$, $b$, $c$ et $\propto$ des entiers relatifs tel que $a \neq 0$ et $b \neq 0$
- $a$ divise $a$.
- Si $a$ divise $b$ et $b$ divise $a$, alors $a = b$ ou $a = -b$.
- Si $a$ divise $b$ et $b$ divise $c$, alors $a$ divise $c$.
- Si $\propto$ divise $a$ et $b$ alors $\propto$ divise $c$ tel que : $ap + bq = c$. Pour tout entiers relatifs $p$ et $q$.

c-à-d $\propto$ divise tout combinaison linéaire de $a$ et $b$ dans $\mathbb{Z}$.

### a) Ensemble des multiples d'un entier relatif :

Soit $a$ un entier relatif non nul. L'ensemble des multiples de $a$ est noté $a\mathbb{Z}$ tel que :
$\boxed{a\mathbb{Z} = \{\cdots -4a\,;\,-3a\,;\,-2a\,;\,-a\,;\,0\,;a\,;\,2a\,;\,3a\,;\,4a\,;\,\cdots\}}$

**Exemple :**
Les multiples de 4 dans $\mathbb{Z}$ sont tel que : $4\mathbb{Z} = \{\cdots -16\,;\,-12\,;\,-8\,;\,-4\,;\,0\,;4\,;\,8\,;\,12\,;\,16\,;\,\cdots\}$

### b) Ensemble des diviseurs d'un entier relatif :

Soit $a$ un entier relatif non nul. L'ensemble des diviseurs de $a$ est noté $\mathcal{D}(a)$
**Exemple :**

Les diviseurs de 8 dans $\mathbb{Z}$ sont tel que : $\mathcal{D}(8) = \{-8\,;\,-4\,;\,-2\,;\,-1\,;1\,;\,2\,;\,4\,;\,8\}$

## 5- NUMERATION

### a) Base de numération

Soit $b$ un entier naturel tel que $b \geqslant 2$, $a_k$ les entiers naturels tels que : $0 \leqslant a_k < b$ et $b \neq 0$.
on appelle écriture de $x$ en base $b$, l'écriture de la forme : $\boxed{x = \overline{a_p a_{p-1} \cdots a_2 a_1 a_0}^{\,b}}$
où les $a_p$, $a_{p-1}$, $\cdots$, $a_0$ sont les restes de la division euclidienne successive de $x$ par $b$, $q_0$ par $b$, $q_1$ par $b$ ; ainsi de suite.
**Exemples :** Ecrivons 1532 en base 7

### b) système décimal

Soit $b$ un entier naturel tel que $b \geqslant 2$, $a_k$ les entiers naturels tels que : $0 \leqslant a_k < b$ et $b \neq 0$.
Ecriture du nombre $\overline{a_p a_{p-1} \cdots a_2 a_1 a_0}^{\,b}$ dans le système décimal, est de la forme :
$\boxed{\overline{a_p a_{p-1} \cdots a_2 a_1 a_0}^{\,b} = a_p \times b^p + a_{p-1} \times b^{p-1} + \cdots + a_2 \times b^2 + a_1 \times b + a_0}$
**Exemples :** Ecrivons dans le système décimal, le nombre :$\overline{7324}^{\,5}$

## II- PPCM et PGCD de deux entiers relatifs

Soient $a$ et $b$ deux entiers relatifs non nuls.

### 1- PPCM de deux entiers relatifs

#### a) Définition

On appelle plus petit commun multiple de $a$ et $b$ noté PPCM$(a\,;\,b)$, le plus petit élément strictement positif de $a\mathbb{Z} \cap b\mathbb{Z}$

**Exemple :** Déterminons le PPCM de 5 et 3
$5\mathbb{Z} = \{5; 10; 15; 20; 25; \cdots\}$ et $3\mathbb{Z} = \{3; 6; 9; 12; 15; 18; \cdots\}$. Donc $\boxed{\text{PPCM}(5;3) = 15}$

#### b)Propriétés :

Soient $a$, $b$ et $k$ trois entiers naturels non nuls, on a : $\boxed{\text{PPCM}(ka; kb) = k\text{PPCM}(a; b)}$.

**Exemple :** Déterminons le PPCM de 12 et 20
PPCM$(12; 20)$ =PPCM$(4 \times 3; 4 \times 5) = 4\times$PPCM$(3; 5) = 4 \times 15$. Donc $\boxed{\text{PPCM}(12; 20) = 60}$

**Remarques**

- Pour tous entiers relatifs non nuls $a$ et $b$, on a : $\boxed{\text{PPCM}(a\ ;\ b) = \text{PPCM}(|\ a\ |\ ;\ |\ b\ |)}$.
- Pour tous entiers relatifs non nuls $a$ et $b$, on a : $\boxed{\text{PPCM}(a\ ;\ b) = a} \Leftrightarrow a \in b\mathbb{Z}$.

### 2- PGCD de deux entiers relatifs

#### a) Définition

On appelle plus grand commun diviseur de $a$ et $b$ noté PGCD$(a\,;\,b)$, le plus grand élément de l'ensemble des diviseurs communs de $a$ et $b$ noté $\mathcal{D}(a; b)$.

**Exemple :** Déterminons le PGCD de 36 et 48
$\mathcal{D}(36) = \{-36\,;-18\,;-12\,;-9\,;-6\,;-4\,;-3\,;-2\,;-1\,;1\,;2\,;3\,;4\,;6\,;9\,;12\,;18\,;36\}$
$\mathcal{D}(48) = \{-24\,;-16\,;-12\,;-8\,;-6\,;-4\,;-3\,;-2\,;-1\,;1\,;2\,;3\,;4\,;6\,;8\,;12\,;16\,;24\,;48\}$
$\mathcal{D}(36; 48) = \{-12; -6; -3; -2; -1; 1; 2; 3; 4; 6; 12\}$ Donc $\boxed{\text{PGCD}(36; 48) = 12}$

#### b) Propriétés 1 :

Soient $a$, $b$ et $k$ trois entiers naturels non nuls, on a : $\boxed{\text{PGCD}(ka; kb) = k\text{PGCD}(a; b)}$.

**Exemple :** Déterminons le PGCD de 72 et 96

PGCD$(72;96)$ =PGCD$(2\times36;2\times48) = 2\times$PGCD$(36;48) = 2\times12$. Donc $\boxed{\text{PGCD}(72;96) = 24}$

**c) Propriétés 2 :** Soient $a$ et $b$ deux entiers naturels non nuls .

• Si PGCD$(a\,;\,b) = \lambda$ alors $\lambda$ divise $a$ et $b$ ou $a$ et $b$ sont des multiples de $\lambda$

• Si PGCD$(a\,;\,b) = \lambda$ alors un entier relatif $m$ est multiple de $\lambda$ si et seulement si il existe deux entiers relatifs $u$ et $v$ tel que : $\boxed{au + bv = m}$

### 3- Relation entre PPCM et PGCD de deux entiers relatifs

Soient $a$ et $b$ deux entiers relatifs non nuls. $\boxed{\text{PPCM}(a\,;\,b)\times\text{PGCD}(a\,;\,b) = ab}$

### 4- Algorithme d'Euclide

**Propriétés :**

Soient $a$ et $b$ deux entiers naturels tels que $a > b > 0$, et $r$ le reste de la division euclidienne de $a$ par $b$ tel que : $a = b \times q + r$.

• Si $r = 0$, alors $\boxed{\text{PGCD}(a\,;\,b) = b}$

• Si $r \neq 0$, alors $\boxed{\text{PGCD}(a\,;\,b) = \text{PGCD}(b\,;\,r)}$

**Méthode :**

L'algorithme d'Euclide est une méthode qui consiste à déterminer le PGCD de deux entiers naturels $a$ et $b$ tel que $a > b > 0$, en effectuant les divisions euclidiennes successives suivantes :

• Division de $a$ par $b$, pour obtenir : $a = b \times q_0 + r_0$ avec $(0 \leqslant r_0 < b)$

On a : $\boxed{\text{PGCD}(a\,;\,b) = \text{PGCD}(b\,;\,r_0)}$

• Division de $b$ par $r_0$, pour obtenir : $b = r_0 \times q_1 + r_1$ avec $(0 \leqslant r_1 < r_0)$

On a : $\boxed{\text{PGCD}(b\,;\,r_0) = \text{PGCD}(r_0\,;\,r_1)}$

• Division de $r_0$ par $r_1$, pour obtenir : $r_0 = r_1 \times q_2 + r_2$ avec $(0 \leqslant r_2 < r_1)$

On a : $\boxed{\text{PGCD}(r_0\,;\,r_1) = \text{PGCD}(r_1\,;\,r_2)}$

• $\cdots$

Le dernier reste non nul obtenu dans ce processus est égal à PGCD$(a\,;\,b)$.

**On adopte généralement la disposition pratique du tableau suivant :**

| Dividende | $a$ | $b$ | $r_0$ | $r_1$ | $\cdots$ |
|---|---|---|---|---|---|
| diviseur | $b$ | $r_0$ | $r_1$ | $r_2$ | $\cdots$ |
| quotient | $q_0$ | $q_1$ | $q_2$ | $q_3$ | $\cdots$ |
| reste | $r_0$ | $r_1$ | $r_2$ | $r_3$ | $\cdots$ |

ou

| Dividende | diviseur | quotient | reste |
|---|---|---|---|
| $a$ | $b$ | $q_0$ | $r_0$ |
| $b$ | $r_0$ | $q_1$ | $r_1$ |
| $r_0$ | $r_1$ | $q_2$ | $r_2$ |
| $r_1$ | $r_2$ | $q_3$ | $r_3$ |
| $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ |

**Exemple :**

On utilisons l'algorithme d'Euclide, déterminons PGCD$(30\,;24)$ et PGCD$(48\,;23)$

### 5- Nombres premiers entre eux

**a) Définition** : Soient $a$ et $b$ deux entiers relatifs non nuls.

On dit que $a$ et $b$ sont premiers entre eux si leur PGCD est égal à 1. On note $\boxed{\text{PGCD}(a\,;b) = 1}$

**Exemple :**

On utilisons l'algorithme d'Euclide, montrons que 19 et 12 sont premier entre eux

**Propriété :**

Soient $x$ , $y$ et $a$ trois entiers relatifs non nuls.

Si PGCD$(x\,;y) = a$ , alors il existe $x', y' \in \mathbb{Z}$ tels que : $x = ax'$ , $y = ay'$ , PGCD$(x'\,;y') = 1$

**b) Théorème de Bézout :**
Soient $a$ et $b$ deux entiers relatifs non nuls. $a$ et $b$ sont premiers entre eux si et seulement si il existe deux entiers relatifs $u$ et $v$ tels que : $\boxed{au + bv = 1}$

**c) Théorème de Gauss :**
Soient $a$ , $b$ et $c$ trois entiers relatifs non nuls.
Si $a$ divise $bc$ et si $a$ et $b$ sont premiers entre eux (PGCD$(a\,;b) = 1$), alors $a$ divise $c$.

**Remarque :**
Si $a$ divise $b$ ( $a \,|\, b$ ) , alors il existe un entier relatif $k$ tel que : $b = ak$ et $|\ a\ | \leqslant |\ b\ |$

**6- Equation diophantienne : $ax + by = c$**
**a) Existence des solutions dans $\mathbb{Z}^2$ de l'équation, $ax + by = c$**
L'équation du type $ax + by = c$ admet au moins une solution dans $\mathbb{Z}^2$ si et seulement si $c$ est un multiple de PGCD$(a\,,b)$ ou le PGCD$(a\,,b)$ divise $c$.

**b) Résolution dans $\mathbb{Z}^2$ de l'équation $ax + by = c$**
Soient $a$ et $b$ deux nombres premiers entre eux. Cela veut dire que PGCD$(a\,;b) = 1$
Pour résoudre dans $\mathbb{Z}^2$ l'équation du type $ax + by = c$ :
• **On résout dans $\mathbb{Z}^2$ l'équation $ax + by = 0$ de la manière suivante :**
$*$ $ax + by = 0 \Rightarrow ax = -by \Rightarrow b$ divise $ax$ or $PGCD(a\,,\,b) = 1 \Rightarrow b$ divise $x$
alors il existe $k \in \mathbb{Z}$ tel que : $\underline{x = bk}$
$*$ Remplaçons $x = bk$ dans $ax + by = 0$ : $a(bk) + by = 0 \Rightarrow by = -abk \Rightarrow \underline{y = -ak}$
La solution dans $\mathbb{Z}^2$ l'équation $ax + by = 0$ est : $\boxed{S = \{(bk\,,\,-ak)\,;\,k \in \mathbb{Z}\}}$
• **On détermine la solutions particulières $(x_0\,,\,y_0)$ de l'équation : $ax + by = c$**
En utilisant l'algorithme d'Euclide, on trouve le couple $(x_0\,,\,y_0)$ d'entiers relatifs
tels que : $ax_0 + by_0 = c$
• **On déduit les solutions de $ax + by = c$ sous la forme :**
$x = x_0 + bk$ et $y = y_0 - ak$ Donc $\boxed{S = \{(x_0 + bk\,,\,y_0 - ak)\,;\,k \in \mathbb{Z}\}}$

**EXERCICE :**
1- Montrer que 27 et 13 puis 37 et 25 sont premiers entre eux.
2- Résoudre dans $\mathbb{Z}^2$ les équations $(E_1) : 27x - 13y = 1$ et $(E_2) : 25x + 37y = 2$

**5) Structure de l'ensemble-quotient $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{Z}_n$**

**a) Classes d'équivalence**
La classe d'équivalence d'un entier x notée $\dot{x}$ est l'ensemble $\boxed{\dot{x} = \{y \mid x \equiv y[n]\}}$
**Théorème**
Chaque classe $\dot{x}$ comprend un élément unique $x'$ tel que $0 \leqslant x' < n$. Où $x'$ est le reste de la division euclidienne de $x$ par $n$.

**b) Ensemble-quotient**
On appelle ensemble quotient, l'ensemble de toutes les classes d'équivalence suivant la relation de congruence modulo $n$ noté $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{Z}_n$. tel que : $\mathbb{Z}/n\mathbb{Z} = \{\ \dot{0}\ ,\ \dot{1}\ ,\ \dot{2}\ ,\cdots,(n-1)\}$

**Exemples :** $\mathbb{Z}/5\mathbb{Z} = \{\ \dot{0}\ ,\ \dot{1}\ ,\ \dot{2}\ ,\ \dot{3}\ ,\ \dot{4}\ \}$ $\mathbb{Z}/6\mathbb{Z} = \{\ \dot{0}\ ,\ \dot{1}\ ,\ \dot{2}\ ,\ \dot{3}\ ,\ \dot{4}\ ,\ \dot{5}\ \}$

### c) Tables d'addition et de multiplication dans $\mathbb{Z}/n\mathbb{Z}$

**Table d'addition de $\mathbb{Z}/5\mathbb{Z}$ :**

| $+$ | $\dot{0}$ | $\dot{1}$ | $\dot{2}$ | $\dot{3}$ | $\dot{4}$ |
|---|---|---|---|---|---|
| $\dot{0}$ | $\dot{0}$ | $\dot{1}$ | $\dot{2}$ | $\dot{3}$ | $\dot{4}$ |
| $\dot{1}$ | $\dot{1}$ | $\dot{2}$ | $\dot{3}$ | $\dot{4}$ | $\dot{5}$ |
| $\dot{2}$ | $\dot{2}$ | $\dot{3}$ | $\dot{4}$ | $\dot{5}$ | $\dot{0}$ |
| $\dot{3}$ | $\dot{3}$ | $\dot{4}$ | $\dot{5}$ | $\dot{0}$ | $\dot{1}$ |
| $\dot{4}$ | $\dot{4}$ | $\dot{5}$ | $\dot{0}$ | $\dot{1}$ | $\dot{2}$ |

**Table de multiplication de $\mathbb{Z}/5\mathbb{Z}$ :**

| $\times$ | $\dot{0}$ | $\dot{1}$ | $\dot{2}$ | $\dot{3}$ | $\dot{4}$ |
|---|---|---|---|---|---|
| $\dot{0}$ | $\dot{0}$ | $\dot{0}$ | $\dot{0}$ | $\dot{0}$ | $\dot{0}$ |
| $\dot{1}$ | $\dot{0}$ | $\dot{1}$ | $\dot{2}$ | $\dot{3}$ | $\dot{4}$ |
| $\dot{2}$ | $\dot{0}$ | $\dot{2}$ | $\dot{4}$ | $\dot{1}$ | $\dot{3}$ |
| $\dot{3}$ | $\dot{0}$ | $\dot{3}$ | $\dot{1}$ | $\dot{4}$ | $\dot{2}$ |
| $\dot{4}$ | $\dot{0}$ | $\dot{4}$ | $\dot{3}$ | $\dot{2}$ | $\dot{1}$ |

## III- CONGRUENCE MODULO

Soit $n$ un entier naturel, $a$ et $b$ deux entiers relatifs.

### 1- Définition :

On dit que $a$ est congru à $b$ modulo $n$ si $a-b$ est un multiple de $n$. On écrit $\boxed{a \equiv b[n]}$

**Exemples :**

- $26 \equiv 6[10]$ : car $26-6=20$ est un multiple de 10
- $-7 \equiv 2[9]$ : car $-7-2=-9$ est un multiple de 9
- $-21 \equiv 0[7]$ : car $-21-0=-21$ est un multiple de 7
- $8 \equiv -2[10]$ : car $8+2=10$ est un multiple de 10

**Propriétés :**

Soient $n$ un entier naturel non nul, $a$, $a'$, $b$, $b'$ et $c$ des entiers relatifs

- $P_1$) $a \equiv a[n]$
- $P_2$) Si $a \equiv b[n]$, alors $b = a[n]$
- $P_3$) Si $a \equiv b[n]$ et $b \equiv c[n]$, alors $a \equiv c[n]$
- $P_4$) Si $a \equiv a'[n]$ et $b \equiv b'[n]$ , alors $\boxed{a \times b \equiv a' \times b'[n]}$
- $P_5$) Si $a \equiv a'[n]$ et $b \equiv b'[n]$ , alors $\boxed{a+b \equiv a'+b'[n]}$
- $P_6$) Si $a \equiv b[n] \Rightarrow a^k \equiv b^k[n]$. où $k$ est un entier naturel non nul.
- $P_7$) Si $x \equiv p[n]$, alors il existe $k \in \mathbb{Z}$ tel que : $\boxed{x = p+nk}$ où $x, p \in \mathbb{Z}$
- $P_8$) $a$ est divisible par $n$ si $a$ est congru à 0 modulo $n$. On écrit : $\boxed{a \equiv 0[n]}$

### 2- Détermination de restes :

Si $r$ est le reste de la division euclidienne de $a$ par $n$, alors on écrit : $\boxed{a \equiv r[n]}$

**Détermination du reste de la division euclidienne de a par n tel que :** $a \equiv b[n]$

Soient $a$, $b$, $c$ et $k$ quatre entiers relatifs, et $n$ un entier naturel non nul tel que : $a \equiv b[n]$.

- $a \equiv b[n]$. Si $b \geqslant 0$ et $b < n$, alors $r = b$ on a : $a \equiv r[n]$

Donc le reste de la division euclidienne de $a$ par $n$ est $r = b$.

**Exemples :** $a \equiv 5[6]$ on a : $5 > 0$ et $5 < 6 \Rightarrow r = 5$

Donc le reste de la division euclidienne de $a$ par 6 tel que $a \equiv 5[6]$ est $r = 5$.

- $a \equiv b[n]$. Si $b < 0$ et $\mid b \mid < n$, alors $r = n + b$ on a : $a \equiv r[n]$

Donc le reste de la division euclidienne de $a$ par $n$ est $r = n + b$.

**Exemples :** $a \equiv -3[5]$ on a : $-3 < 0$ et $\mid -3 \mid < 5 \Rightarrow r = 5 - 3 \Rightarrow r = 2$

Donc le reste de la division euclidienne de $a$ par 5, tel que $a \equiv -3[5]$ est $r = 2$.

• $a \equiv b[n]$. Si $\mid b \mid > 0$ et $\mid b \mid > n$ tel que : $b = nk + c$ ;
si $c > 0$ et $c < n$, alors $r = c$ on a : $a \equiv r[n]$
Donc le reste de la division euclidienne de $a$ par $n$ est $r = c$.

**Exemples :**
$a \equiv 24[7]$ or $24 = \underbrace{7 \times 3}_{21=0} + 3 = 3[7] \Rightarrow a \equiv 3[7] \Rightarrow r = 3$
Donc le reste de la division euclidienne de $a$ par 7, tel que $a \equiv 24[7]$ est $r = 3$.
$a \equiv -25[7]$ or $-25 = \underbrace{7 \times (-3)}_{-21=0} - 4 = -4[7] \Rightarrow a \equiv -4[7] \Rightarrow r = 7 - 4 = 3$
Donc le reste de la division euclidienne de $a$ par 7, tel que $a \equiv -25[7]$ est $r = 3$.

**Propriétés :**
• Si $r$ et $r'$ sont respectivement les restes de la division euclidienne de $a$ et $a'$ par $n$,
alors $a \equiv a'[n] \Leftrightarrow r = r'$.
• $a$ et $a'$ ont le même reste dans la division euclidienne par $n$ Si $\boxed{a - a' \equiv 0[n]}$.

**3- Inverse modulo d'un entier relatif**
Soient $a$ et $b$ deux entiers relatifs non nuls premiers entre eux tel que : $a > b$.
On appelle inverse de $a$ modulo $b$, tout entier relatif $x_0$ qui vérifie : $ax_0 \equiv 1[b]$.

**Détermination d'un inverse modulo d'un entier relatif**
Soit à déterminer l'inverse de $a$ modulo $b$. où $a$ et $b$ sont deux entiers naturels non nuls.
**Première méthode :**
∗ On dresse un tableau des valeurs de la classe de $b$ ;
∗ La valeur $x_0$ de la classe de $b$ qui correspond à : $ax_0 \equiv 1[b]$ est l'inverse de $a$ modulo $b$.
**Deuxième méthode :**
∗ On effectue la division euclidienne successive de $a$ par $b$.
∗ On détermine deux entiers relatifs $x_0$ et $y_0$ tels que : $ax_0 + by_0 = 1$
$x_0$ est l'inverse de $a$ en modulo $b$ que l'on note : $\boxed{a^{-1} \equiv x_0[b]}$
$y_0$ est l'inverse de $b$ en modulo $a$ que l'on note : $\boxed{b^{-1} \equiv y_0[a]}$.
**Notation :** si $x_0$ est l'inverse de $a$ en modulo $b$, on note : $\boxed{a^{-1} \equiv x_0[b]}$

**Propriété**
• $a$ est l'inverse de $b$ modulo $n$, si $\boxed{ab \equiv 1[n]}$
• Soit un entier naturel $n > 1$ et $a$ un entier relatif tel que $a$ et $n$ sont premiers entre eux.
Si $a^{-1} \equiv x_0[n]$ tel que $ax \equiv b[n]$, alors on a : $a^{-1}ax \equiv x_0 b[n] \Rightarrow \boxed{x \equiv x_0 b[n]}$

**Exemple :** Trouver l'inverse de 5 modulo 11 et de 21 modulo 17 .

## IV- EQUATIONS MODULAIRES
### 1- Equation de la forme : $ax \equiv n[b]$
Pour résoudre une équation modulaire de la forme : $ax \equiv n[b]$, on détermine l'inverse de $a$ modulo $b$, en utilise l'une des deux méthodes suivantes :
**• Première méthode :**
∗ On dresse un tableau des valeurs ;
∗ On donne à $x$ les valeurs de la classe de $b$

$*$ On retient la valeur $x_0$ de $x$ qui correspond à : $ax_0 \equiv 1[b]$

• **Deuxième méthode :**
$*$ On effectue la division euclidienne successive de $a$ par $b$.
$*$ On détermine deux entiers relatifs $x_0$ et $y_0$ tels que : $\underline{ax_0 + by_0 = 1}$
$x_0$ est l'inverse de $a$ en modulo $b$.
Ainsi, on écrit : $x_0 \times ax \equiv x_0 \times n[b] \Rightarrow x \equiv x_0 \times n[b]$
Si $x_0 \times n \equiv p[b]$ alors $x \equiv p[b]$ , il existe $k \in \mathbb{Z}$ tel que : $x = bk + p$. Donc $\boxed{S = \{bk + p\,,\, k \in \mathbb{Z}\}}$

**EXERCICE :**
Résoudre dans $\mathbb{Z}$ les équations suivantes : a) $21x \equiv 3[17]$ et b) $5x \equiv 7[11]$

**2- Equation de la forme : $P(x) \equiv 0[n]$**
Soit $P(x)$ un polynôme de degré supérieur ou égal à 2 et de racines entières.
**Soit $P(x)$ un polynôme du second degré :** $P(x) = ax^2 + bx + c$ **,** $a \neq 0$
Si $P(x)$ admet deux racines $x_1$ et $x_2$ en modulo $n$, alors on a :

$$P(x) \equiv 0[n] \Leftrightarrow (x-x_1)(x-x_2) \equiv 0[n] \Rightarrow \begin{cases} x - x_1 \equiv 0[n] \\ \text{ou} \\ x - x_2 \equiv 0[n] \end{cases} \Leftrightarrow \begin{cases} x \equiv x_1[n] \\ \text{ou} \\ x \equiv x_2[n] \end{cases} \Leftrightarrow \begin{cases} x = nk + x_1 \\ \text{ou} \\ x = nk + x_2 \end{cases}$$

Donc $\boxed{S = \{nk + x_1\,;\, nk + x_2\,,\, k \in \mathbb{Z}\}}$

**EXERCICE :**
Résoudre dans $\mathbb{Z}$ les équations suivantes : a) $x^2 \equiv 2[7]$ , b) $5x^2 \equiv 3[7]$ et c) $x^2 - 4x + 5 \equiv 0[6]$

**Théorème de Fermat :**
Si $p$ est un nombre premier et si $a$ est un entier qui n'est pas divisible par $p$, alors $\boxed{a^{p-1} \equiv 1[p]}$

**Exemple :** $7^{5-1} \equiv 1[5] \Rightarrow 7^4 \equiv 1[5]$
. Car $7^4 = 7^2 \times 7^2 = 49 \times 49 \equiv 4 \times 4[5]$ or $16 = \underbrace{5 \times 3}_{15=0} + 1 \equiv 1[5] \Rightarrow 7^4 \equiv 1[5]$

## V- SYSTEMES D'EQUATIONS MODULAIRES

Dans cette partie, nous considérons les systèmes d'équations modulaires de la forme :

$$(S_1) : \begin{cases} ax \equiv a_1[m] \\ bx \equiv b_1[n] \end{cases} \quad \text{et} \quad (S_2) : \begin{cases} ax \equiv a_1[m_1] \\ bx \equiv b_1[m_2] \\ cx \equiv c_1[m_3] \end{cases}$$

Pour résoudre le système $(S_1)$ :
• On trouve l'inverse de $a$ modulo $m$ et l'inverse de $b$ modulo $n$
• On écrit le système sous la forme : $\begin{cases} x \equiv c[m] \\ x \equiv c'[n] \end{cases}$ , il existe $p, q \in \mathbb{Z}$ tels que : $\begin{cases} x = mp + c \\ x = nq + c' \end{cases}$
• On pose $x = x$, on trouve l'équation diophantienne : $mp - nq = c' - c$, d'inconnues $p$ et $q$
• On résout l'équation diophantienne : $mp - nq = c' - c$, pour trouver $p$ ou $q$
• On remplace $p$ ou $q$ trouvé dans $x = mp + c$ ou $x = nq + c'$.
• On trouve $x$ sous la forme : $x = sk + r$ où $r, s \in \mathbb{Z}$. Dons $\boxed{S = \{sk + r, k \in \mathbb{Z}\}}$
La résolution du système $(S_2)$ se fait de la même manière.

**EXERCICE :**
Résoudre dans $\mathbb{Z}$ le système d'équation : $\begin{cases} 2x \equiv 1[5] \\ 3x \equiv 2[7] \end{cases}$