

I) Introduction et Définition :

1) Introduction

On peut considérer que, dès l'époque préhistorique, les hommes ont utilisé leurs doigts pour compter ou effectuer des calculs sommaires. L'emploi de symboles pour désigner les nombres apparaît sans doute en Mésopotamie, vers 2000 av. J.-C, où l'on a retrouvé des tablettes babyloniennes couvertes de chiffres en base 60. Puis viennent les systèmes de numération égyptiens, grecs et romains. **C'est en Grèce qu'est fondée l'arithmétique théorique par les pythagoriciens au VI^e siècle av. J.-C.** À cette époque, les mathématiciens grecs savent déjà manipuler des notions arithmétiques comme les proportions, les moyennes, ou encore les progressions. Tout ce savoir a été, par la suite, regroupé dans les *Éléments* d'Euclide.

2) Définition

L'Arithmétique est la branche des mathématiques qui étudie les propriétés des **Nombres Entiers Naturels** $\mathbb{N}$, des **Nombres Entiers Relatifs** $\mathbb{Z}$ et des **Nombres Rationnels** $\mathbb{Q}$.

II) Rappel sur les ensembles $\mathbb{N}$; $\mathbb{Z}$ et $\mathbb{Q}$

En arithmétique, on utilise trois types de nombres : les **Nombres Entiers Naturels** $\mathbb{N}$; les **Nombres Entiers Relatifs** $\mathbb{Z}$ et les **Nombres Rationnels** $\mathbb{Q}$.

1) Ensemble des Nombres entiers naturels :

L'ensemble des entiers naturels, noté : $\mathbb{N}$ est défini en extension comme suite :

$$\mathbb{N} = \{ 0 ; 1 ; 2 ; 3 ; \dots ; n ; (n + 1) ; \dots \}$$

On définit dans $\mathbb{N}$ deux lois de compositions internes:

- **L'addition** : $\forall a \in \mathbb{N} \text{ et } \forall b \in \mathbb{N}, a + b = S \in \mathbb{N}$.
- **La multiplication** : $\forall a \in \mathbb{N} \text{ et } \forall b \in \mathbb{N}, a \times b = p \in \mathbb{N}$.

Exemple : $2 + 1 = 3 \in \mathbb{N}$ et $4 \times 3 = 12 \in \mathbb{N}$

On définit aussi dans $\mathbb{N}$ une relation d'ordre, c'est-à-dire que pour tout a et b de $\mathbb{N}$, on a :

$$\text{Soit } a \leq b, \quad \text{soit } b \leq a.$$

Propriétés

P₁ : $\mathbb{N}$ a un plus petit élément noté 0.

P₂ : $\mathbb{N}$ n'a pas de plus grand élément.

P₃ : Toute partie non vide de $\mathbb{N}$ a un plus petit élément.

2) Ensemble des Nombres entiers relatifs :

L'ensemble des entiers relatifs, noté : $\mathbb{Z}$ est défini en extension comme suite :

$$\mathbb{Z} = \{-2 ; -1 ; 0 ; 1 ; 2 ; \dots ; n ; -n ; (n + 1) ; -(n + 1), \dots\}$$

Cet ensemble a la structure d'un **anneau commutatif unitaire** :

On définit dans $\mathbb{Z}$ deux lois de composition interne : **une addition et une multiplication**.

Propriétés :

P₁ : L'addition est commutative associative dans $\mathbb{Z}$ et admet un élément neutre qui est 0.

P₂ : La multiplication est commutative associative dans $\mathbb{Z}$ et admet un élément neutre qui est 1.

P₃ : La multiplication est distributive par rapport à l'addition : $a \cdot (b + c) = ab + ac$.

P₄ : L'existence d'un élément symétrique $-a$, c'est-à-dire que $a + (-a) = 0$.

NB :

L'anneau est unitaire à cause de l'existence de l'élément neutre "1" de la multiplication.

$(\mathbb{Z} ; +)$ est un groupe commutatif.

$(\mathbb{Z} ; + ; \times)$ est un anneau commutatif unitaire.

On définit dans $\mathbb{Z}$ une **relation d'ordre** ($\leq$) vérifiant les propriétés suivantes :

- 1) $a \leq b \Rightarrow a + c \leq b + c$
- 2) $a \leq b \text{ et } c > 0 \Rightarrow ac \leq bc$
- 3) $a \leq b \text{ et } c < 0 \Rightarrow ac \geq bc$

D'autres propriétés de $\mathbb{Z}$, que nous admettrons sans preuve sont :

P₁- Toute partie de $\mathbb{Z}$ qui est non vide et qui est majorée, a un plus grand élément.

P₂- Toute partie de $\mathbb{Z}$ qui est non vide et qui est minorée a un plus petit élément.

P₃- Si a et b sont deux entiers relatifs, et b est non nul, il existe un entier relatif n où $nb \geq a$.

3) Ensemble des Nombres rationnels :

L'ensemble des nombres rationnels, noté : $\mathbb{Q}$ est un ensemble qui est défini en extension comme suite : $\mathbb{Q} = \left\{ \frac{p}{q} , p \in \mathbb{Z} ; q \in \mathbb{Z}^* \right\}$

NB : $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$

III) Raisonnement par récurrence :

Principe :

Pour Démontrer qu'une proposition P_n est vraie pour tout entier naturel n , on procède de la façon suivante :

- 1^{ère} Etape : (Initialisation):

On vérifie que la proposition P_n est vraie pour le terme initial, c'est-à-dire : (P_0 est vraie).

- 2^{ème} Etape : (Transmission) :

On suppose que la proposition P_n est vraie pour tout entier naturel et ensuite on démontre qu'elle est vraie à l'ordre $n + 1$. C'est-à-dire P_{n+1} est vraie.

- 3^{ème} Etape : (Conclusion) :

On conclut qu'alors : $\forall n \in \mathbb{N} , P_n$ est vraie.

IV) Division Euclidienne dans $\mathbb{N}$

1) Définition :

Soient a et b deux entiers naturels ($b \neq 0$).

On appelle division Euclidienne de l'entier naturel a par l'entier naturel b , toute opération visant à Déterminer un couple unique $(q ; r) \in \mathbb{N} \times \mathbb{N}$, tel que $a = bq + r$.

Avec : $0 \leq r < b$.

2) Notation :

- q : est appelé le quotient de la division Euclidienne de l'entier a par l'entier b .
- r : est appelé le reste de la division Euclidienne de l'entier a par l'entier b .

3) Propriétés :

P₁ : Si b divise, alors le reste r est nul ($r = 0$) . Ainsi : $a = bq$.

P₂ : Si b divise, alors pour tout entier naturel n , b divise na .

V) Divisibilité dans $\mathbb{Z}$

Multiples et diviseurs d'un entier relatif :

a- Définitions :

Soient a et b deux entiers relatifs.

- On dit que a est un multiple de, s'il existe un entier relatif k tel que : $a = kb$.
- On dit que b est un diviseur de, si $a = qb$ (où q est le quotient de la division).

NB :

- 0 est un multiple de tout entier relatif.
- Tout entier relatif non nul divise 0, mais il ne divise aucun entier relatif.
- Si $b \neq 0$, on dit que b est un diviseur de a ou que b divise a . On note : b/a .

b- Propriété :

Soient a ; b ; c trois entiers tel que $a \neq 0$.

Si a divise b et a divise c , alors pour tout entier u et v , a divise la combinaison linéaire $bu + cv$.

VI) Système de numération

1) Définition :

Soit b un entier naturel tel que $b \geq 2$. Tout entier naturel x peut s'écrire de façon unique

telque : $x = a_0 + a_1b + a_2b^2 + \dots + a_pb^p = \sum_{k=0}^p a_kb^k$ avec $a_k \in \mathbb{N}$.

Ainsi si $0 \leq a_k < b$ et $a_p \neq 0$, on peut écrire : $x = \overline{a_p a_{p-1} \dots a_1 a_0}^b$.

Cette écriture de x est appelée x dans la base b .

2) Propriétés :

P₁ : Par convention , dans le système décimal (**appelé aussi à base 10**), les nombres sont écrits à l'aide des dix chiffres décimaux , à savoir : 0 ; 1 ; 2 ; 3 ; 4 ; 5 ; 6 ; 7 ; 8 ; 9.

C'est-à-dire tout nombre sans barre, est écrit en base 10.

Exemple :

$$3201 = \overline{3201}^{10} = 1 \times 10^0 + 0 \times 10^1 + 2 \times 10^2 + 3 \times 10^3 = 1 + 0 + 200 + 3000 = 3201$$

Donc, les chiffres **1 ; 0 ; 2 ; 3** sont les coefficients respectifs des puissances croissantes de la base 10.

P₂ : Au Delas des 10 chiffres décimaux, on peut adopter les lettres : A ; B ; C ; D ; E...etc. pour : 10 ; 11 ; 12 ; 13 ; 14 etc.

3) Changement de base :

a- Système binaire ou système en base 2 :

Dans le système binaire les symboles utilisés sont : 0 et 1

b- Système octal ou système en base 8 :

Dans le système octal les symboles utilisés sont : 0 ; 1 ; 2 ; 3 ; 4 ; 5 ; 6 ; 7

c- Système hexadécimal ou système en base 16 :

Dans le système hexadécimal les symboles utilisés sont : 0 ; 1 ; 2 ; ...9 ; A ; B ; C ; D , E ; F

VII) Congruence Modulo n

Considérons les nombres entiers relatifs ci-dessous, où n est un entier naturel supérieur à 1,

$a = -2n + 1$ et $b = 15n + 1$. Des relations ci-dessus, on note que :

- a et b ont un même reste (à savoir 1) lorsqu'ils sont divisés par n
- $a - b = -2n - (15n) = -17n$, c'est-à-dire que $a - b$ est un multiple de n .

De ces observations, nous donnons la définition de la congruence modulo n comme suite :

1) Définitions :

Définition 1: On dit que l'entier relatif a est congru à l'entier relatif b , modulo n , si la division de a par n , et celle de b par n , ont le même reste. Ceci est symbolisé par : $a \equiv b(n)$.

Définition 1 : On dit que l'entier relatif a est congru à l'entier relatif b , modulo n , si la différence $a - b$ est un multiple de n . Autrement dit $a \equiv b(n) \Leftrightarrow \exists k \in \mathbb{Z} ; a - b = kn$.

Remarque : $a \equiv b(n) \Leftrightarrow a = kn + b$ c'est-à-dire le reste de la division euclidienne de a par n est b .

2) Propriétés :

La relation de congruence modulo n est une **relation d'équivalence**, car elle met en évidence les propriétés suivantes :

P₁ : la relation de congruence modulo n est **Réflexive**, c'est-à-dire :

$$\forall a \in \mathbb{Z}, \text{ on a : } a \equiv a[n].$$

P₂ : la relation de congruence modulo n est **Symétrique**, c'est-à-dire :

$$\forall (a ; b) \in \mathbb{Z}^2, \text{ Si } a \equiv b[n] \text{ Alors } b \equiv a[n]$$

P₃ : la relation de congruence modulo n est **Transitive**, c'est-à-dire :

$$\forall (a ; b ; c) \in \mathbb{Z}^3, \text{ Si } a \equiv b[n] \text{ et } b \equiv c[n] \text{ alors } a \equiv c[n].$$

3) Autres propriétés caractéristiques :

$$\mathbf{P_1 : } a \equiv b[n] \Rightarrow n \text{ divise } a - b$$

$$\mathbf{P_2 : } a \equiv b[n] \Leftrightarrow \forall k \in \mathbb{N}, ka \equiv kb[n]$$

$$\mathbf{P_3 : } a \equiv b[n] \Leftrightarrow \forall p \in \mathbb{N}, a^p \equiv b^p[n]$$

4) Congruences particulières (Critères de divisibilité) :

a- Divisibilité par 2

Un entier N est divisible par 2 si et seulement si son chiffre des unités simples est pair, c'est-à-dire si l'entier x est terminé par 0 ; 2 ; 4 ; 6 ou 8.

b- Divisibilité par 3 et par 9

Un entier N est divisible par 3 (respectivement par 9) si et seulement si la somme de ces chiffres est divisible par 3 (respectivement par 9).

c- Divisibilité par 5

Un entier N est divisible par 5 si et seulement si cet entier est terminé par 0 ou 5.

d- Divisibilité par 11

Un entier N est divisible par 11 si et seulement si la différence de la somme des chiffres de rang pair et de la somme des chiffres de rang impair est divisible par 11.

e- Divisibilité par 4 et par 25

Un entier N est divisible par 4 (respectivement par 25) si et seulement si le nombre formé par les deux derniers chiffres est divisible par 4 (respectivement par 25).

VIII) Congruence et structure d'anneau ($\mathbb{Z}/n\mathbb{Z}$) :**1) Classe d'équivalence modulo n** **a- Définition :**

Lorsqu'un nombre quelconque x de $\mathbb{Z}$ est divisé par un entier naturel n , les restes possibles sont : $0 ; 1 ; 2 ; \dots ; n - 1$.

On dit qu'un élément x de $\mathbb{Z}$ appartient à la **classe $\dot{p}$ modulo n** si : $x \equiv p$ avec $n - 1 \geq 0$.

D'une manière générale, si $\dot{x}$ est un élément de $\mathbb{Z}$, alors la classe de x modulo n est l'ensemble de tous les éléments de $\mathbb{Z}$ qui ont le même reste que x dans la division par n ; on le note

$$cl(x) = \dot{x} \text{ tel que : } cl(x) = \dot{x} = \{y \in \mathbb{Z} / x - y \equiv 0[n]\}$$

b- Ensemble quotient $\mathbb{Z}/n\mathbb{Z}$:

L'ensemble des classes $\dot{p}$ modulo n est noté par $\mathbb{Z}/n\mathbb{Z}$ et s'appelle groupe quotient de $\mathbb{Z}/n\mathbb{Z}$ tel que : $\mathbb{Z}/n\mathbb{Z} = \{\dot{0} ; \dot{1} ; \dot{2} ; \dot{3} ; \dots ; \overbrace{\dot{n} - 1}^{\dot{0}}\}$.

2) Propriétés dans $\mathbb{Z}/n\mathbb{Z}$ **a- Propriétés (Addition) :**

- 1) L'associativité : $\dot{x} + (\dot{y} + \dot{z}) = (\dot{x} + \dot{y}) + \dot{z}$
- 2) La commutativité : $\dot{x} + \dot{y} = \dot{y} + \dot{x}$
- 3) L'élément neutre : $\dot{0}$ (car $\dot{x} + \dot{0} = \overbrace{\dot{x} + \dot{0}}^{\dot{x}} = \dot{x}$)
- 4) L'élément : $\overline{-\dot{x}}$, symétrique de x (car $\overbrace{-\dot{x} + \dot{x}}^{\dot{0}} = \dot{0}$)

b- Propriétés (Multiplication) :

- 1) L'associativité : $\dot{x} \times (\dot{y} \times \dot{z}) = (\dot{x} \times \dot{y}) \times \dot{z}$

2) La commutativité : $\dot{x} \times \dot{y} = \dot{y} \times \dot{x}$

3) L'élément neutre : $\dot{1}$ (car $\dot{1} \times \dot{x} = \overbrace{\dot{1} \times \dot{x}} = \dot{x}$)

4) La distributivité par rapport à l'addition, soit : $\dot{x} \times (\dot{y} + \dot{z}) = (\dot{x} \times \dot{y}) + (\dot{x} \times \dot{z})$

NB :

On dit qu'un anneau commutatif unitaire A est **intègre** si pour tout x, y de A, on a :

$$x \times y = 0 \Rightarrow x = 0 \text{ ou } y = 0$$

Lorsque l'anneau n'est pas intègre, il existe x et y , tous non nuls, dont le produit est zéro.

On dit alors que x et y sont des **diviseurs de zéro**.

IX) Nombre entier naturel premier :

1) Définition :

On dit qu'un nombre entier naturel p est premier s'il a exactement deux diviseurs, 1 et p .

D'une manière générale :

Pour Montre qu'un nombre entier naturel p est premier, il suffit de le diviser par les entiers naturels premiers successifs qui lui sont inférieure afin d'obtenir un entier premier d qui ne le divise pas avec ($d^2 < a$)

2) Théorèmes :

Théorème1 : Tout entier naturel n supérieur à 1, admet au moins un diviseur premier.

Théorème 2 : L'ensemble des nombres premiers est infini.

Théorème 3 :

Tout entier naturel n supérieur à 1 admet au moins un diviseur premier d tel que : $1 < d^2 \leq n$

NB :

L'ensemble des nombres premiers compris entre 1 et 100 peut s'obtenir par **l'algorithme d'Eratosthène** que nous décrivons comme suit :

- 1) On construit une table des nombres allant de 1 à 100.
- 2) On élimine le nombre 1 qui n'est pas premier
- 3) On garde le nombre 2 et on élimine de la table tous ses multiples
- 4) Le nombre suivant non éliminé est 3, que l'on garde. On élimine de la table tous les multiples de 3;

5) On procède ainsi jusqu'au nombre 100 .

6) Les nombres non éliminés de la table sont tous premiers.

On obtient alors la table suivante :

~~1~~	~~2~~	~~3~~	~~4~~	5	~~6~~	7	~~8~~	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Théorème 4 : (Décomposition d'un nombre entier en produit de facteur premier).

Tout entier naturel supérieur à 1 se décompose de façon unique comme un produit de facteurs premiers. La décomposition prend la forme générale : $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_k^{\alpha_k}$ où α_i est le nombre de termes de valeur p_i contenus dans n .

X) PPCM et PGCD de deux entiers naturels a et b :

1) Plus Petit Commun Multiple (PPCM)

a- Définition :

Soient a et b deux entiers relatifs non nuls. On appelle plus petit commun multiple de a et b , le plus petit élément strictement positif de $(a\mathbb{Z} \cap b\mathbb{Z})$.

Notation :

Le plus petit commun multiple de a et b peut être noté comme suit:

$$\text{PPCM}(a; b) = (a \vee b) = m.$$

b- Propriétés

$$\mathbf{P_1:} \forall (a; b) \in \mathbb{Z}^2; \text{PPCM}(a; b) = \text{PPCM}(|a|; |b|)$$

C'est à dire cherché le PPCM de deux entiers relatifs, revient à cherché le PPCM de deux entiers naturels non nuls.

$$\mathbf{P_2:} \forall (a; b) \in (\mathbb{N}^*)^2, \text{ on a : } m(a; b) \leq \text{PPCM}(a; b) \leq a \cdot b$$

$$\mathbf{P_3:} \forall (a; b) \in (\mathbb{N}^*)^2, \text{ on a : } \text{PPCM}(a; b) = a \Leftrightarrow a \in (b\mathbb{Z}).$$

$$\mathbf{Exemple :} \text{PPCM}(12; 4) = 12 \Leftrightarrow 12 \in (4\mathbb{Z}).$$

$\mathbf{P_4:}$ L'ensemble des multiples communs de deux entiers naturels non nuls a et b est l'ensemble des multiples de leurs PPCM, c'est-à-dire si $\text{PPCM}(a; b) = m$; alors : $(\mathbb{Z} \cap b\mathbb{Z}) = m\mathbb{Z}$.

$$\mathbf{Exemple :} \text{PPCM}(12; 16) = 48 \text{ donc } (12\mathbb{Z} \cap 16\mathbb{Z}) = 48\mathbb{Z}.$$

$$\mathbf{P_5:}$$
 Soit $a; b$ et k trois entiers naturels non nuls. On a : $\text{PPCM}(ka; kb) = k\text{PPCM}(a; b)$

$$\mathbf{Exemple :} \text{PPCM}(120; 168) = \text{PPCM}(24 \times 5; 24 \times 7) = 24 = 24 \cdot \text{PPCM}(5; 7) = 24 \times 35$$

$$= > \text{PPCM}(120; 168) = 840$$

2) Plus Grand Commun Diviseur (PGCD)

a- Définition :

Soient a et b deux entiers relatifs non nuls. On appelle Plus Grand Commun Diviseur de a et b , le plus grand élément commun strictement positif de $(a \in \mathbb{Z} \cap b \in \mathbb{Z})$.

Notation :

Le Plus Grand Commun Diviseur de a et b peut avoir les notations suivantes :

$$\text{PGCD}(a; b) = (a \wedge b) = d = \Delta.$$

b- Propriétés :

$$P_1 : \forall (a; b) \in \mathbb{Z}^2 ; \text{PGCD}(a; b) = \text{PGCD}(|a|; |b|)$$

C'est à dire chercher le PGCD de deux entiers relatifs, revient à chercher le PGCD de deux entiers naturels non nuls.

P_2 : Soient a et b deux entiers naturels non nuls. On a :

$$\text{PGCD}(a; b) = d \Rightarrow D(a; b) = D_d \text{ où } D_d \text{ désigne l'ensemble des diviseurs de } d.$$

Exemple :

$$\text{PGCD}(24; 30) = 6 \Rightarrow \text{PGCD}(24; 30) = D_6 = \{1; 2; 3; 6\}$$

P_3 : Soient $a; b$ et k trois entiers naturels non nuls. On a :

$$\text{PGCD}(ka; kb) = k \text{ PGCD}(a; b).$$

Exemple :

$$\text{PGCD}(228; 95) = \text{PGCD}(19 \times 12; 19 \times 5) = 19 \text{ PGCD}(12; 5) = 19 \times 1 = 19$$

$$P_4 : \text{Si } b > a \text{ alors } \text{PGCD}(a; b) = \text{PGCD}(a; b - a) = \text{PGCD}[b - a; a - (b - a)]$$

Exemple 1 :

$$\begin{aligned} \text{PGCD}(143; 27) &= \text{PGCD}(27; 116) = \text{PGCD}(27; 89) = \text{PGCD}(77; 62) = \text{PGCD}(27; 35) \\ &= \text{PGCD}(27; 8) = \text{PGCD}(8; 19) = 1 \end{aligned}$$

Exemple 2 :

$$\begin{aligned} \text{PGCD}(2n + 3; 5n - 2) &= \text{PGCD}(3n - 5; 2n + 3) = \text{PGCD}(n - 8; 2n + 3) \\ &= \text{PGCD}(n + 11; n - 8) = \text{PGCD}(19; n - 8) = 19 \end{aligned}$$

P₅ : D'après l'algorithme d'Euclide, si $a = bq + r$ ($r \neq 0$) alors :

Activité

Consigne : Montre que $\text{PGCD}[(5n^3 - n); (n + 2)] = \text{PGCD}[(n + 2); 38]$

Synthèse

La division Euclidienne de $(5n^3 - n)$ par $(n + 2)$ donne pour quotient :

$$q = 5n^2 - 10n + 19 \text{ et pour reste } r = -38.$$

Puisque : $\text{PGCD}(a; b) = \text{PGCD}(b; r)$ alors on a :

$$\text{PGCD}[(5n^3 - n); (n + 2)] = \text{PGCD}[(n + 2); -38] = \text{PGCD}[(n + 2); 38]$$

P₆ : Soit $(a; b) \in (\mathbb{N}^*)^2$ et d leur PGCD. Un entier relatif m est un multiple de d si et seulement si, il existe deux entiers relatifs u et v tel que $m = au + bv$

Exemple :

38 est un multiple de 19 ; donc il existe un couple $(u; v) \in \mathbb{Z}^2$ tel que :

$$38 = 228u + 95v \Rightarrow 38 = 228(1) + (-2)(95) \Rightarrow u = 1 \text{ et } v = -2$$

XI) Algorithme d'Euclide :

1) Définition :

Soient a et b deux entiers tels que : $0 < b < a$ et r le reste de la division Euclidienne de a par b .

On appelle **Algorithme d'Euclide**, toute opération visant à Détermine le PGCD des deux entiers a et b en effectuant les divisions Euclidiennes successives suivantes :

- Division de a par b pour obtenir : $a = bq_0 + r_0$; Avec $0 \leq r_0 < b$.
- Division de b par r_0 pour obtenir : $b = r_0q_1 + r_1$; Avec $0 \leq r_1 < r_0$.
- Division de r_0 par r_1 pour obtenir : $r_0 = r_1q_2 + r_2$; Avec $0 \leq r_2 < r_1$.

Et ainsi de suite jusqu'à obtention du dernier reste non nul qui correspond au PGCD des deux entiers a et b .

NB : toutes ces opérations peuvent être résumées dans un tableau appelé : tableau **d'Algorithme** qui se présente sous la forme :

Quotients	q_0	q_1	q_2	$\dots q_{n+1}$
Dividendes	Diviseurs	r_0	r_1	$\dots r_n$
Restes	r_0	r_1	r_2	$\dots r_{n+1}$

XII) Nombres Premiers entre eux ou Nombres étrangers :

1) Définitions :

Définition 1 :

Soient a et b deux nombres entiers relatifs non nuls.

On dit que a et b sont premiers entre eux (ou sont étrangers) si $\text{PGCD}(a; b) = 1$.

Définition 2:

On dit également que a et b sont premiers entre eux (ou sont étrangers) s'ils n'admettent pas de diviseur commun (en dehors de l'unité c'est-à-dire 1).

2) Théorèmes :

➤ **Théorème 1 : (Théorème de Bézout).**

Soient a et b deux entiers relatifs non nuls. a et b sont étrangers s'il existe un couple $(u; v) \in \mathbb{N}$ tel que : $au + bv = 1$.

➤ **Théorème 2 : (Théorème de Gauss).**

Soient $a; b$ et c trois entiers relatifs non nuls. Si a divise bc et que a et b sont premiers entre eux c'est-à-dire : $(\text{PGCD}(a; b) = 1)$, alors a divise c .

➤ **Théorème 3 : (Théorème de Fermat).**

Soit a un nombre entier non nul, et p un nombre premier. Si p ne divise pas a , alors il s'en suit la congruence suivante : $a^{p-1} \equiv 1[p]$

➤ **Théorème 4 :**

Si a et b sont premiers entre eux ($\text{PGCD}(a; b) = 1$) et si a et b divisent c , alors le produit ab divise c .

➤ **Théorème 5 :**

Si a et b sont premiers entre eux ($\text{PGCD}(a; b) = 1$), alors $\text{PPCM}(a; b) = ab$

3) Relation Entre PGCD et PPCM :

Soient a et b deux entiers naturels non nuls. Si d et m désignent respectivement le **PGCD** et le **PPCM** des entiers naturels : a et b , on a : $a \cdot b = m \cdot d$

Ainsi il existe deux entiers a' et b' premiers entre eux ($\text{PGCD}(a'; b') = 1$) tel que :

$$a = a' \cdot d \quad \text{et} \quad b = b' \cdot d \quad \Rightarrow a \cdot b = d^2 \cdot a' b'$$

Puisque a' et b' sont premiers entre eux ($\text{PGCD}(a'; b') = 1$), alors on a le théorème

Suivant : $\text{PPCM}(a'; b') = a' \cdot b'$

XIII) Résolution dans $\mathbb{Z}^2$ des équations Diophantiennes

Equations du type ($ax + by = c$)

1) Définition :

On appelle équation Diophantienne, toute équation de $\mathbb{Z}^2$ dont l'ensemble solution se présente sous forme de couple $(x; y)$.

Résolution d'un cas particulier : Equation du type $ax + by = c$.

$ax + by = c$ où : $a; b; c$ sont tous des entiers (avec a et b non nul)

Théorème

L'équation : $ax + by = c$, admet des solutions dans $\mathbb{Z}^2$ si et seulement si c est un multiple du $\text{PGCD}(a; b)$.

2) Résolution

Pour Résoudre de telles équations, nous pouvons utiliser deux méthodes :

La méthode par Congruence ou La méthode d'algorithme