Ensemble ℕ des entiers naturels

I – Propriétés de ℕ:

1- Propriétés de l'addition dans ℕ:

L'opération **+** est une loi de composition interne dans ℕ;

∀ a ∈ ℕ ; ∀ b ∈ ℕ, (a + b) ∈ ℕ.

- La loi **+** est commutative dans ℕ : ∀ (a ; b) ∈ $\mathbb{N}^2$, a + b = b + a.
- La loi **+** est associative dans ℕ :∀(a ; b ; c)∈$\mathbb{N}^3$, (a + b) + c = a + (b + c) ;
- 0 est l'élément neutre de **+** dans ℕ : ∀ a ∈ ℕ ; a + 0 = 0 + a
- Tout élément de ℕ est simplifiable ou régulier pour **+** dans ℕ :

∀ (x ; y ; z) ∈ $\mathbb{N}^3$, x + **z** = y + **z** ⇒ x = y.

2 - Propriétés de la multiplication dans ℕ:

La loi × est une loi de composition interne dans ℕ;

- La loi × est commutative et associative dans ℕ ;
- 1 est l'élément neutre pour la × dans ℕ ;
- Tout élément non nul est simplifiable ou régulier par la ×.

3 – Exemple de raisonnement par récurrence dans ℕ:

Démontrer par récurrence que ∀ n ∈ ℕ ; $3^{n+3} - 4^{4n+2}$ est divisible par 11.

-- 0 --

Pour n = 0 $3^3 - 4^2 = 27 - 16 = 11$ est divisible par 11.

Supposons que $3^{n+3} - 4^{4n+2}$ est divisible par 11, montrons que $3^{(n+1)+3} - 4^{4(n+1)+2}$ est divisible par 11.

$$3^{(n+1)+3} - 4^{4(n+1)+2} = 3^{n+3} \times 3^1 - 4^{4n+2} \times 4^4$$
$$= 3 \times 3^{n+3} - 256 \times 4^{4n+2}$$
$$= 3 \times 3^{n+3} - (253+3) \times 4^{4n+2}$$
$$= 3(3^{n+3} - 4^{4n+2}) - 11 \times 23 \times 4^{4n+2}$$

Puisque $3^{n+3} - 4^{4n+2}$ est divisible par 11 il existe un nombre k tel que :

$3^{n+3} - 4^{4n+2} = 11k$ et il existe k' tel que : $-11 \times 23 \times 4^{4n+2} = -11k'$.

D'où $3^{(n+1)+3} - 4^{4(n+1)+2} = 3 \times 11k - 11k'$.

⇔ $3^{(n+1)+3} - 4^{4(n+1)+2} = 11(3k - k')$ est divisible par 11.

D'après le principe de récurrence ∀n∈ℕ; $3^{n+3} - 4^{4n+2}$ est divisible par 11.

4 – Relation d'ordre « ≤ »:

« ≤ » est une relation d'ordre total sur ℕ.

Réflexive : ∀ x ∈ ℕ , x ≤ x ;

Antisymétrique : ∀ (x ; y) ∈ $\mathbb{N}^2$ $\begin{cases} x \le y \\ y \le x \end{cases} \Rightarrow x = y$;

Transitive : ∀ (x ; y ; z) ∈ $\mathbb{N}^3$ $\begin{cases} x \le y \\ y \le z \end{cases} \Rightarrow x \le z$.

Deux éléments de ℕ sont toujours comparables : ∀(x ; y)∈$\mathbb{N}^2$ x ≤ y ou y ≤ x.

II – Division euclidienne dans ℕ:

1- Activité : On donne a = 71 et b = 8. Trouver deux entiers q et r tels que :

a = bq +r avec 0≤ r < b. Que représente q et r ?.

-- 0 –

71 = (8 × 8) + 7 ⇒ q = 8 et r = 7. q = 8 est le quotient ; r = 7 est le reste.

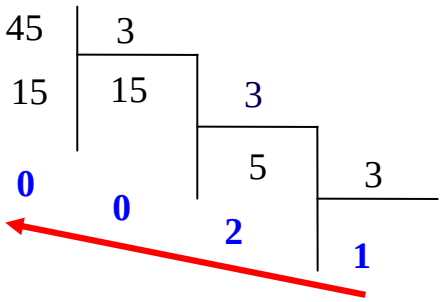
2 – Théorème et définition :

∀(a ; b)∈ℕ×ℕ*, il existe un couple unique (q ;r) tels que a = bq + r avec 0≤r< b.

a = dividende ; b = diviseur ; q = quotient ; r = reste.

III – Systèmes de numération:

1- Activité : Ecrire 45 en base 3.



45 = $\overline{1200}^{(3)}$

2 – Développement d'un entier a selon une base b de numération :

a) Théorème : Soit b un entier naturel supérieur ou égal à 2. Pour tout nombre entier naturel non nul x, il existe une et une seule suite finie (a_0 ; a_1 ; ….. ; a_i ; ….. ;a_n) de nombres entiers naturels telles que :

- ∀ i = 0 à (n – 1) ; 0 ≤a_i < b ;
- 0 < a_n < b ;
- x = a_0 + a_1 × **b** + a_2 × $\mathbf{b^2}$ +……..+a_n×$\mathbf{b^n}$.
- L'écriture **x = a_0 + a_1 × b + a_2 × b^2 +……..+ a_n×b^n** est appelée le développement du nombre x dans la base b.

Exemple : On donne x = 19473 et b = 9.

Donner le développement du nombre x dans la base neuf.

19473	9	2163	9	240	9	26	9	2	9
6	2163	**3**	240	**6**	26	**8**	2	**2**	0

$x = 6 + 3 \times 9 + 6 \times 9^2 + 8 \times 9^3 + 2 \times 9^4 = \overline{28636}^{(9)}$ d' où $19473 = \overline{28636}^{(9)}$

b) Définition :

Si le développement du nombre **x** en base **b** est :

$x = a_n \times b^n + a_{n-1} \times b^{n-1} + \ldots\ldots + a_2 \times b^2 + a_1 \times b + a_0$ alors x s'écrit:

$$x = \overline{a_n a_{n-1} \ldots a_1 a_0}^{(b)}.$$

On dit qu'on a représenté **x** dans le système de numération à base **b**.

Remarques :

– Chaque nombre est strictement inférieur à la base b et représenté par un symbole appelé chiffre.

Les symboles utilisés dans la base dix sont : 0 ; 1 ; 2 ; 3 ; 4 ; 5 ; 6 ; 7 ; 8 ; 9.

– Si la base b est supérieur à dix on utilise les lettres A ; B ; C ; D ;….. pour représenter les nombres appartenants à [10 ; b[. A = dix ; B = onze ; C = douze ; D = treize.

Exemple : Ecrire 19473 en base treize.

19473	13	1497	13	115	13	8	13
12	1497	**2**	115	**11**	8	**8**	0

$19473 = \overline{8B2C}^{(13)}$ ou $19473 = \overline{8B2C}_{treize}$

3 – Principales bases :

a) Système de numération décimale (ou système à base dix) :

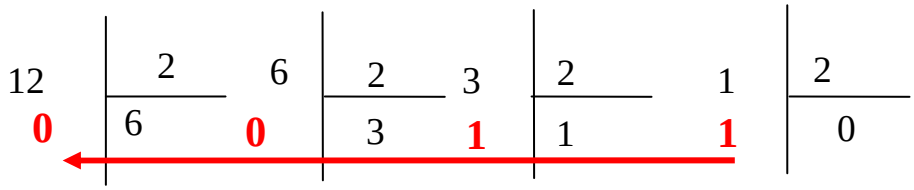
Les chiffres sont : 0 ;1 ; 2 ; 3 ; 4 ; 5 ; 6 ; 7 ; 8 ; 9.

Le nombre $a = 2.10^3 + 5.10^2 + 3.10 + 1$ s'écrit $a = \overline{2531}_{dix}$ ou a = 2531.

b) Système binaire (ou système à base deux) :

C'est la plus petite base rencontrée, les chiffres utilisés sont : 0 et 1.

Exemple : Ecrire 12 en base deux.



$12 = \overline{1100}^{(2)}$

c) ***Le système hexadécimal (ou à base seize) :***

Les chiffres utilisés sont : 0 ; 1 ; 2 ; 3 ; 4 ; 5 ; 6 ; 7 ; 8 ; 9 ; A ; B ; C ; D ; E ; F ;

Exemple : Ecrire en base seize le nombre x = 748.
On obtient $748 = \overline{2EC}^{(16)}$.

4 – Opérations dans la base deux :

a) ***Addition :*** Dresser la table d'addition en base deux puis effectuer :

$$\overline{1101101}^{(2)} + \overline{1011}^{(2)}.$$

-- 0 --

+	0	1
0	0	1
1	1	10

report → 1 1 1 1
1 1 0 1 1 0 1
\+ 1 0 1 1
.....
$= \overline{1111000}^{(2)}$

b) ***Multiplication :*** Dresser la table de multiplication en base deux puis effectuer : $\overline{1101101}^{(2)} \times \overline{1011}^{(2)}$.

×	0	1
0	0	0
1	0	1

1 1 0 1 1 0 1
× 1 0 1 1
.....
1 1 0 1 1 0 1
1 1 0 1 1 0 1
1 1 0 1 1 0 1 .
$= \overline{10010101111}^{(2)}$

Ensemble $\mathbb{Z}$ des entiers relatifs .

$\mathbb{Z} = \{\ldots\ldots ; -3 ; -2 ; -1 ; 0 ; 1 ; 2 ; 3 ; \ldots\ldots\ldots\}$

I – Extension de la division euclidienne à $\mathbb{Z}$:

Théorème : Quels que soient les entiers relatifs a et b ($a \neq b$) il existe un couple unique (q ;r) d'entiers relatifs tel que $a = bq + r$ avec $0 \leq r < |b|$.

Exemple : soit a = – 1992 et b = – 5 trouver (q ; r) $\in \mathbb{Z}^2$ tel que :

$a = bq + r$ avec $0 \leq r < |b|$. Effectuons la division euclidienne de |a| par |b|.

$1992 = 398 \times 5 + 2 \Leftrightarrow -1992 = -398 \times 5 - 2 \Leftrightarrow -1992 = (-5) \times 398 + 3 - 5$

$\Leftrightarrow -1992 = (-5) \times (398 + 1) + 3 \Leftrightarrow -1992 = (-5) \times (399) + 3$;

donc q = 399 et r = 3.

1 – Ensemble des multiples d'un nombre :

- **Définition :** Soit a et b deux entiers relatifs ; a est un multiple de b si et seulement si il existe un nombre entier relatif k tel que **a = k b.**

. (a est multiple de b) $\Leftrightarrow$ $(\exists\, !\, k \in \mathbb{Z} \ / \ a = k \times b)$.

. (a est multiple de b, $b \neq 0$) $\Leftrightarrow$ ($\frac{a}{b}$ a pour reste 0) .

Remarque :

L'ensemble des multiples de **a** est noté : $a\mathbb{Z} = \{\ldots . ; -2a ; -a ; 0 ; a ; 2a ; \ldots .\}$.

Exemple : $7\mathbb{Z} = \{\ldots . ; -14 ; -7 ; 0 ; 7 ; 14 ; \ldots .\}$; $0\mathbb{Z} = \{0\}$; $1\mathbb{Z} = \mathbb{Z}$.

2 – Ensemble des diviseurs d'un nombre :

a) Définition : Soit a $\in \mathbb{Z}$ et b $\in \mathbb{Z}^*$.

On dit que b est un diviseur de a, ou que b divise a si et seulement si a est un multiple de b. On note : b/a « lire b divise a ».

b) Propriétés : La relation (../..) est une relation d'ordre partiel sur $\mathbb{N}^*$.

c) Notations : L'ensemble des diviseurs d'un entier relatif est noté :
$\mathcal{D}_a$ ou **div (a)**.

Dans la recherche de l'ensemble des diviseurs d'un nombre on se limitera aux diviseurs positifs.

Exemples : div+(10) = {1 ; 2 ; 5 ; 10 } ; div (0) = {… ; –2 ; –1 ; 1 ; 2 ; …}.

d) Détermination de l'ensemble des diviseurs d'un nombre:

Exemple : a = 30 ; nous savons à priori que 1 et 30 sont des diviseurs de 30.
On cherche les diviseurs p de 30 compris entre 2 et $\sqrt{a}$ c'est-à-dire

$p \in [2 ; \sqrt{30}] \Rightarrow p \in \{2 ; 3 ; 4 ; 5\}$. p= 2 $\Rightarrow$ 30 = 2 $\times$15 ; p = 3 $\Rightarrow$ 30 =3 $\times$10 ;

p = 4 ne divise pas 30 ; p = 5 $\Rightarrow$ 30 = 5 $\times$ 6.

Donc l'ensemble des diviseurs de 30 est :

$\mathcal{D}_{30} = \{ -30 ; -15 ; -10 ; -6 ; -5 ; -3 ; -2 ; -1 ; 1 ; 2 ; 3 ; 5 ; 6 ; 10 ; 15 ; 30 \}$.

II – Nombres Premiers:

1- Définition : On appelle nombre premier tout élément **a** de $\mathbb{N} - \{0 ; 1\}$ qui admet comme diviseurs (–a ; –1 ; 1 ; a) dans $\mathbb{Z}^*$. Donc par définition 1 n'est pas premier. 2 ; 3 ; 5 ; 7 ; …..sont premiers, par contre 4 ; 6 ; 8 ; 10 ; ….ne sont pas premiers.

Remarque : a est premier $\Leftrightarrow$ (–a) est premier $\Leftrightarrow$ |a| est premier.

Il est donc suffisant d'étudier les nombres premiers dans $\mathbb{N}$.
Un entier naturel a est dit premier s'il est différent de 1 et admet comme diviseurs 1 et a.

2- Recherche des entiers naturels premiers:

Pour étudier si un entier a de $\mathbb{N} - \{0 ; 1\}$ est premier on peut rechercher l'ensemble des diviseurs de a : $\mathcal{D}_a$.

- Si $\mathcal{D}_a = \{0 ; 1\}$ alors a est premier ;
- Si aucun nombre premier compris au sens large entre 2 et $\sqrt{a}$, ne divise pas **a**, alors a est premier.

Exemple : 97 est-il premier ?
- Crible d'Eratosthène :
Cherchons les nombres premiers inférieurs ou égaux à 40.

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~~	

Les nombres premiers inférieurs à 40 sont :
2 ; 3 ; 5 ; 7 ; 11 ; 13 ; 17 ; 19 ; 23 ; 29 ; 31 ; 37. Vérifions si 97 est premier.

Pour cela on cherche les nombres p compris entre 2 et $\sqrt{97} \simeq 9{,}84 \Rightarrow$

$p \in \{2 ; 3 ; 5 ; 7\}$. $2 \nmid 97$; $3 \nmid 97$; $5 \nmid 97$; $7 \nmid 97$ donc 97 est premier.

Remarque : L'ensemble des nombres premiers est infini.

III – Congruence modulo n – Anneaux $\mathbb{Z}/n\mathbb{Z}$:

1– Définition :

Soit n ∈ $\mathbb{N}^*$ et x ; x' deux entiers relatifs. On dit que x est congrue à x' modulo n si et seulement ($x - x'$) est un multiple de n.
Notation : $x \equiv x'$ [n] « se lit x congrue à x' modulo n ».

Comme exemple 15 ≡ 1 [7].

$$\forall\, x \in \mathbb{Z},\ \forall\, x' \in \mathbb{Z},\ x \equiv x'\ [n] \quad \Leftrightarrow \quad (x - x') \in n\mathbb{Z}$$

2– Propriété caractéristique : Soit n ∈ $\mathbb{N}^*$; ∀ (x ; x') ∈ $\mathbb{Z}^2$.

$x \equiv x'$ [n] ⇔ (x et x' *ont même reste dans la division euclidienne par n*)

3 – Propriété de la congruence modulo n :

- **Réflexivité :** Soit n ∈ $\mathbb{N}^*$; ∀ x ∈ $\mathbb{Z}$; $x \equiv x$ [n].
  En effet : $x \equiv x$ [n] car $x - x = 0 = 0 \times n$.
- **Symétrie :** ∀ x ∈ $\mathbb{Z}$; ∀ x' ∈ $\mathbb{Z}$; $x \equiv x'$ [n] ⇔ $x' \equiv x$ [n] .
  En effet $x \equiv x'$ [n] ⇔ ∃ k ∈ $\mathbb{Z}$ / $x - x' = kn \Leftrightarrow -x + x' = -kn \Leftrightarrow x' \equiv x$ [n] .
- **Transitivité :** ∀ (x ; x'; x'') ∈ $\mathbb{Z}^3$. $\begin{cases} x \equiv x'[n] \\ x' \equiv x''[n] \end{cases} \Rightarrow x \equiv x''[n]$.
  En effet : $\begin{cases} x \equiv x'[n] \\ x' \equiv x''[n] \end{cases} \Rightarrow \begin{cases} x - x' = kn \\ x' - x'' = k'n \end{cases} \Rightarrow x - x'' = (k + k')n \Leftrightarrow x \equiv x''\ [n]$.

Conclusion : la relation de « ≡ » modulo n est une relation d'équivalence.

– Règles de calculs sur la congruence modulo n :

Soit (n ; k) ∈ $(\mathbb{N}^*)^2$; (x ; y ; z ; t) ∈ $\mathbb{Z}^4$.

R_1) Si $\begin{cases} x \equiv y\,[n] \\ z \equiv t\,[n] \end{cases}$ *alors* $(x + z) \equiv (y + t)\,[n]$;

R_2) Si $\begin{cases} x \equiv y\,[n] \\ z \equiv t\,[n] \end{cases}$ *alors* $(x \times z) \equiv (y \times t)\ [n]$;

R_3) Si $x \equiv y\,[n]$ *alors* $x^k \equiv y^k\ [n]$.

4 – Structure d'anneaux – Anneaux $\mathbb{Z}/n\mathbb{Z}$:

a) - Structure d'anneau :

– Définition : L'ensemble A est muni de + et de $\times$.

On dit que (A ; + ; $\times$) est un anneau si et seulement si :

- (A ; +) est un groupe commutatif ;
- La loi $\times$ est associative et distributive par rapport à +.

De plus si la deuxième loi est commutative on dit que A est un anneau commutatif.
Si la deuxième loi admet un élément neutre, on dit que A est un anneau commutatif unitaire (ou unifère). Exemple : ($\mathbb{Z}$; + ; $\times$) est un anneau unifère.

b) - Anneau ($\mathbb{Z}/n\mathbb{Z}$; $\dot{+}$; $\dot{\times}$) :

- **Classes modulo n :** Nous savons que la congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$. On appelle **classe d'un élément a** l'ensemble des éléments qui sont en relation avec a. On note : cl(a) ou $\dot{a}$ se lit «classe de a ».
- **Activité :** Dans la congruence modulo 3

  1) Donnez $\dot{0}$; $\dot{1}$; $\dot{2}$; $\dot{3}$; $\dot{4}$; $\dot{5}$; $\dot{6}$; $\dot{3n}$; $\dot{3n+1}$; $\dot{3n+2}$. Que remarque-t-on ?

  2) Déterminer $\dot{0}\cap\dot{1}$; $\dot{0}\cap\dot{2}$; $\dot{1}\cap\dot{2}$;

  3) Comparer $\dot{0}\cup\dot{1}\cup\dot{2}$ et $\mathbb{Z}$.

Solution

1) $\dot{0}=\{.....;-6;-3;0;3;6;9;12;.....\}=\dot{3}=-\dot{6}=\dot{9}$.

– 6 ; – 3 ; 0 ; 3 ; 6 ; ……sont les représentants de la classe de zéro.

$\dot{1}=\{.....;-8;-5;1;4;7;10;13;.....\}$; $\dot{2}=\{.....;-7;-4;-1;2;5;8;11;14;.....\}$

$$\dot{3}=\dot{0}\ ;\ \dot{4}=\dot{1}\ ;\ \dot{5}=\dot{2}\ ;\ \dot{6}=\dot{0}\ ;\ \dot{3n}=\dot{0}\ ;\ \dot{3n+1}=\dot{1}\ ;\ \dot{3n+2}=\dot{2}\ .$$

On remarque que dans la congruence modulo 3 il n'y a que 3 classes : $\dot{0}$; $\dot{1}$; $\dot{2}$.

L'ensemble des classes modulo 3 est noté : $\mathbb{Z}/3\mathbb{Z}$ et s'appelle ensemble quotient.

2) $\dot{0}\cap\dot{1}=\varnothing$; $\dot{0}\cap\dot{2}=\varnothing$; $\dot{1}\cap\dot{2}=\varnothing$; $\dot{0}$; $\dot{1}$; $\dot{2}$ sont disjoints deux à deux.

3) $\dot{0}\cup\dot{1}\cup\dot{2}=\mathbb{Z}$.

Conclusion : On dit que la relation de congruence modulo 3 définie donc une partition de $\mathbb{Z}$ en 3 classes (autant que de restes possibles dans la division euclidienne par 3).

Plus généralement soit n$\in\mathbb{N}^*$, $\mathbb{Z}/n\mathbb{Z}=\left\{\dot{0}\,;\dot{1}\,;\dot{2}\,;.....;\ \overbrace{\dot{n-1}}\right\}$ car 0 ;1 ;2 ; …;n-1 sont les restes possibles dans la division euclidienne par n.

Remarque : La classe d'un élément a est généralement représentée par le plus petit élément positif ou nul de cette classe.

Exemple : Dans $\mathbb{Z}/5\mathbb{Z}$ on a : cl(16) est notée $\dot{1}$; cl(–12) est notée $\dot{3}$.

$$\forall (x\,;y)\in\ \mathbb{Z}^2\ ,\ \dot{x}=\dot{y}\ \Leftrightarrow\ x\equiv y\ [n]$$

- **Opérations dans $\mathbb{Z}/n\mathbb{Z}$:**

➢ **Addition :** Soit n ∈ $\mathbb{N}$ – {0 ; 1}, dans $\mathbb{Z}/n\mathbb{Z}$ on définit une loi de composition interne notée $\dot{+}$ et définie par : $\forall\,\dot{x}\in\ \mathbb{Z}/n\mathbb{Z}$; $\forall\ \dot{y}\in\ \mathbb{Z}/n\mathbb{Z}$;

$$\dot{x}\,\dot{+}\,\dot{y}=\overbrace{x+y}^{\cdot}$$

La loi $\dot{+}$ est appelée la loi quotient du + par la congruence modulo n.

Exemple : Dresser la table d'addition dans $\mathbb{Z}/3\mathbb{Z}$ et dans $\mathbb{Z}/4\mathbb{Z}$.

➢ **Multiplication :** De façon analogue dans $\mathbb{Z}/n\mathbb{Z}$ on définit une loi de composition interne notée $\dot{\times}$ et définie par : $\forall\,\dot{x}\in\ \mathbb{Z}/n\mathbb{Z}$;$\forall\ \dot{y}\in\ \mathbb{Z}/n\mathbb{Z}$;

$$\dot{x}\,\dot{\times}\,\dot{y}=\overbrace{x\times y}^{\cdot}$$

La loi $\dot{\times}$ est appelée la loi quotient du $\times$ par la congruence modulo n.

Exemple : Dresser la table de multiplication dans $\mathbb{Z}/5\mathbb{Z}$.

5 – Anneau intègre:

a) Définition et propriété :

On dit qu'un anneau commutatif A est intègre si et seulement si ∀x ∈ A ;∀y∈ A ;

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

(L'anneau commutatif A est intègre) ⇔ ($x\times y = 0\ \Rightarrow\ x = 0$ ou $y = 0$)

Exemple : $(\mathbb{Z}\ ;+\ ;\times)$ est un anneau intègre par contre : $(\mathbb{Z}/9\mathbb{Z}\ ;\dot{+}\ ;\dot{\times})$ est non intègre car $\dot{6}\dot{\times}\dot{3}=\dot{0}$ *mais* $\dot{6}$ *et* $\dot{3}$ sont tous non nuls dans $\mathbb{Z}/9\mathbb{Z}$. On dit que $\dot{6}$ *et* $\dot{3}$ sont des *diviseurs de zéro* dans $\mathbb{Z}/9\mathbb{Z}$. Plus généralement dans un anneau commutatif unifère, s'ils existent deux éléments non nuls dont le produit est nul :

- ✓ Ces éléments sont des diviseurs de zéro ;
- ✓ L'anneau est non intègre.

b) Dans un anneau intègre : $\begin{cases} a\,x=b\,x \\ et\ \ x\neq 0 \end{cases} \Rightarrow a=b$**.** Ceci est faux dans un anneau non intègre. Dans $\mathbb{Z}/4\mathbb{Z}$ on a : $\dot{2}\dot{\times}\dot{2}=\dot{2}\dot{\times}\dot{0}$ *mais* $\dot{2}\neq\dot{0}$.

c) Si n est premier $(\mathbb{Z}/n\mathbb{Z}\ ;\dot{+}\ ;\dot{\times})$ est anneau intègre.

d) Si n n'est pas premier, il existe dans $\mathbb{Z}/n\mathbb{Z}$ des diviseurs de zéro ; $\mathbb{Z}/n\mathbb{Z}$ est un anneau non intègre.

Exercice : Montrer que ∀ n ∈ ℕ, $4^n + 15n - 1$ est divisible par 9.

1ère Méthode : (Raisonnons par récurrence)

Il suffit de montrer que $4^n + 15n - 1 \equiv 0\ [9] \Leftrightarrow \dot{4}^{n}\dot{+}\dot{15}\dot{n}\dot{-}\dot{1}=\dot{0} \Leftrightarrow \dot{4}^{n}=\dot{3}\dot{n}\dot{+}\dot{1}$.

$$Si\ \ n=0\ \ alors \left|\begin{array}{l} \dot{4}^{n}=\dot{1} \\ \dot{3}\dot{n}\dot{+}\dot{1}=\dot{1} \end{array}\right. \ vraie.$$

Supposons $\dot{4}^{n}=\dot{3}\dot{n}\dot{+}\dot{1}$ et montrons que $\dot{4}^{(n+1)}=\dot{3}(\dot{n+1})\dot{+}\dot{1}$.

$\dot{4}^{n+1}=\dot{4}^{n}\dot{\times}\dot{4}=\dot{4}(\dot{3}\dot{n}\dot{+}\dot{1}) \Leftrightarrow \dot{4}^{n+1}=\dot{12}\dot{n}\dot{+}\dot{4} \Leftrightarrow \dot{4}^{n+1}=\dot{3}\dot{n}\dot{+}\dot{4}=\dot{3}\dot{n}\dot{+}\dot{3}\dot{+}\dot{1} \Leftrightarrow \dot{4}^{n+1}=\dot{3}(\dot{n+1})\dot{+}\dot{1}$. D'où ∀ n ∈ ℕ, $4^n + 15n - 1$ est divisible par 9.

2ème Méthode : (restes de la division de 4^n par 9)

$4^0 \equiv 1\ [9]$ période = 3

$4^1 \equiv 4\ [9]$ donc ∀ k ∈ ℕ, $4^{3k} \equiv 1\ [9]$

$4^2 \equiv 7\ [9]$ $4^{3k+1} \equiv 4\ [9]$

$4^3 \equiv 1\ [9]$ $4^{3k+2} \equiv 7\ [9]$.

- Si n = 3k on a : $4^n \equiv 1\ [9]$

$15n \equiv 0\ [9]$

$-1 \equiv 8\ [9]$

$4^n + 15n - 1 \equiv 0\ [9]$

- Si n = 3k+1 on a : $4^n \equiv 4\ [9]$

$15n \equiv 6\ [9]$

$-1 \equiv 8\ [9]$

$4^n + 15n - 1 \equiv 0\ [9]$

- Si n = 3k+2 on a : $4^n \equiv 7\ [9]$

$15n \equiv 3\ [9]$

$-1 \equiv 8\ [9]$

$4^n + 15n - 1 \equiv 0\ [9]$.

D'où $\forall\ n \in \mathbb{N}$, $4^n + 15n - 1$ est divisible par 9.

3ème Méthode : on peut aussi calculer les valeurs prises par $4^n + 15n - 1$ lorsqu'on substitue à n les valeurs respectives : $\dot{0}\ ;\ \dot{1}\ ;\ \dot{2}\ ;\ \dot{3}\ ;\ \dot{4}\ ;\ \dot{5}\ ;\ \dot{6}\ ;\ \dot{7}\ ;\ \dot{8}$.

6 – Équations dans $(\mathbb{Z}/n\mathbb{Z}\ ;\ \dot{+}\ ;\ \dot{\times})$:

a) Équations $\dot{a}x + \dot{b} = \dot{0}$ **:** résoudre dans $\mathbb{Z}/5\mathbb{Z}$; $\dot{2}x + \dot{1} = \dot{0}$;

1ère méthode : $\mathbb{Z}/5\mathbb{Z} = \{\ \dot{0}\ ;\ \dot{1}\ ;\ \dot{2}\ ;\ \dot{3}\ ;\ \dot{4}\ \}$

x	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{2}$x	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{1}$	$\dot{3}$
$\dot{2}$x + $\dot{1}$	$\dot{1}$	$\dot{3}$	$\dot{0}$	$\dot{2}$	$\dot{4}$

2ème méthode :

Définition : un élément **a** de $\mathbb{Z}/n\mathbb{Z}$ est dit inversible si et seulement si il existe un élément noté :$\mathbf{a^{-1}}$ de tel que : $\mathbf{a} \times \mathbf{a^{-1}} = 1$. $\mathbf{a^{-1}}$ est appelé l'inverse de **a.**

- Dans l'équation $\dot{a}x + \dot{b} = \dot{0}$**,** si a est inversible on multiplie les deux membres par $\mathbf{a^{-1}}$. $\dot{2}x + \dot{1} = \dot{0}$, $\dot{2}$ est inversible dans $\mathbb{Z}/5\mathbb{Z}$ et son inverse est $\dot{3}$.

$\dot{2}x + \dot{1} = \dot{0} \Leftrightarrow \dot{6}x + \dot{3} = \dot{0} \Leftrightarrow x = \dot{2}$.

b) Equations : $\dot{a}x^2 + \dot{b}x + \dot{c} = \dot{0}$:

Exemple 1 : résoudre dans $\mathbb{Z}/7\mathbb{Z}$: $x^2 + \dot{2}x + \dot{6} = \dot{0}$.

$x^2 + \dot{2}x + \dot{6} = \dot{0} \Leftrightarrow (x+\dot{1})^2 - \dot{1} + \dot{6} = \dot{0} \Leftrightarrow (x+\dot{1})^2 + \dot{5} = \dot{0} \Leftrightarrow (x+\dot{1})^2 - \dot{2} = \dot{0}$ comme $\dot{4} \times \dot{4} = \dot{2}$ alors $(x+\dot{1})^2 - (\dot{4})^2 = \dot{0} \Leftrightarrow (x+\dot{1}-\dot{4})(x+\dot{1}+\dot{4}) = \dot{0}$ puisque $\mathbb{Z}/7\mathbb{Z}$ est un anneau intègre, on a :

$(x-\dot{3})(x+\dot{5}) = \dot{0} \Leftrightarrow x - \dot{3} = \dot{0} \Leftrightarrow x = \dot{3}$ *ou* $x + \dot{5} = \dot{0} \Leftrightarrow x = -\dot{5} \Leftrightarrow x = \dot{2}$; $S = \{\dot{2}\ ;\ \dot{3}\}$.

Exemple 2 : résoudre dans $\mathbb{Z}/13\mathbb{Z}$: $x^2 + x + \dot{6} = \dot{0}$.

En général si n est premier on cherche l'inverse de $\dot{2}$ noté $\dot{2}^{-1}$ et on multiplie b par $\dot{2} \times \dot{2}^{-1}$. $\dot{7}$ est l'inverse de $\dot{2}$. $x^2 + x + \dot{6} = \dot{0} \Leftrightarrow x^2 + (\dot{2} \times \dot{7})x + \dot{6} = \dot{0} \Leftrightarrow$ $(x + \dot{7})^2 - \dot{7}^2 + \dot{6} = \dot{0} \Leftrightarrow (x + \dot{7})^2 + \dot{9} = \dot{0} \Leftrightarrow (x + \dot{7})^2 - \dot{4} = \dot{0} \Leftrightarrow (x + \dot{5})(x + \dot{9}) = \dot{0}$ puisque l'anneau est intègre on a :

$x + \dot{5} = \dot{0} \Leftrightarrow x = \dot{8}$ *ou* $x + \dot{9} = \dot{0} \Leftrightarrow x = -\dot{9} \Leftrightarrow x = \dot{4}$; $S = \left\{ \dot{4} ; \dot{8} \right\}$.

Exemple 3 : résoudre dans $\mathbb{Z}/6\mathbb{Z}$: $x^2 + x + \dot{6} = \dot{0}$.

$\mathbb{Z}/6\mathbb{Z}$ est un anneau non intègre car 6 n'est pas premier, donc admet des diviseurs de zéro : $\dot{2}$; $\dot{3}$; $\dot{4}$. Les paires de diviseurs associés sont : $\left\{ \dot{2} ; \dot{3} \right\}$; $\left\{ \dot{3} ; \dot{4} \right\}$. $x^2 + x + \dot{6} = \dot{0} \Leftrightarrow x^2 + x = \dot{0} \Leftrightarrow x(x + \dot{1}) = \dot{0} \Leftrightarrow$

$\begin{cases} x = \dot{0} \\ x + \dot{1} = \dot{0} \end{cases} \Leftrightarrow \begin{cases} x = \dot{0} \\ x = \dot{5} \end{cases}$ ou $\begin{cases} x = \dot{2} \\ x + \dot{1} = \dot{3} \end{cases} \Rightarrow \begin{cases} x = \dot{2} \\ x = \dot{2} \end{cases} \Rightarrow x = \dot{2}$ *ou* $\begin{cases} x = \dot{3} \\ x + \dot{1} = \dot{2} \end{cases} \Leftrightarrow \begin{cases} x = \dot{3} \\ x = \dot{1} \end{cases}$ *impossible*

ou $\begin{cases} x = \dot{4} \\ x + \dot{1} = \dot{3} \end{cases} \Rightarrow \begin{cases} x = \dot{3} \\ x = \dot{1} \end{cases}$ *impossible* *ou* $\begin{cases} x = \dot{3} \\ x + \dot{1} = \dot{4} \end{cases} \Leftrightarrow \begin{cases} x = \dot{3} \\ x = \dot{3} \end{cases} \Rightarrow x = \dot{3}$; $S = \left\{ \dot{0} ; \dot{2} ; \dot{3} ; \dot{5} \right\}$.

Autre méthode : puisque n est petit nombre.

x	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
x^2	$\dot{0}$	$\dot{1}$	$\dot{4}$	$\dot{3}$	$\dot{4}$	$\dot{1}$
$x^2 + x$	$\dot{0}$	$\dot{2}$	$\dot{0}$	$\dot{0}$	$\dot{2}$	$\dot{0}$

L'ensemble des solutions est : $S = \left\{ \dot{0} ; \dot{2} ; \dot{3} ; \dot{5} \right\}$.

7 – Systèmes d'équations:

a) Résolvez dans $\mathbb{Z}/6\mathbb{Z}$ le système $\begin{cases} \dot{2}x - \dot{4}y = \dot{2} \\ x + \dot{5}y = \dot{2} \end{cases}$

b) Résolvez dans $\mathbb{Z}/6\mathbb{Z}$ le système $\begin{cases} \dot{3}x + \dot{6}y = \dot{5} \\ \dot{5}x + \dot{2}y = \dot{3} \end{cases}$

a) méthode : (substitution)

Mise en garde : $\mathbb{Z}/6\mathbb{Z}$ étant non intègre ne jamais essayer de simplifier une des équations.

$$\begin{cases} \dot{2}x - \dot{4}y = \dot{2} & (1) \\ x + \dot{5}y = \dot{2} & (2) \end{cases} \qquad (2) \Rightarrow x = -\dot{5}y + \dot{2},$$

en remplaçant x par sa valeur dans (1) on a :

$$\dot{2}(\dot{2} - \dot{5}y) - \dot{4}y = \dot{2} \Leftrightarrow \dot{4} - \dot{10}y - \dot{4}y = \dot{2} \Leftrightarrow \dot{4} + \dot{4}y = \dot{2} \Leftrightarrow \dot{4}y = \dot{4}; \quad y \in \{\dot{1}\,;\ \dot{4}\}$$

* si y = $\dot{1}$ alors x = $\dot{3}$

* si y = $\dot{4}$ alors x = $\dot{0}$; $S = \{(\dot{3}\,;\dot{1})\,;(\dot{0}\,;\dot{4})\}$

8 – Critères de divisibilité:

- **Divisibilité par 2 :** Un nombre est divisible par 2 s'il est terminé par 0 ; ou 2 ; ou 4 ; ou 6 ; ou 8.
- **Divisibilité par 3 :** Un nombre est divisible par 3 si la somme des ses chiffres est divisible par 3.
- **Divisibilité par 4 :** Un nombre est divisible par 4 si le nombre constitué de ses deux derniers chiffres de la gauche vers la droite est divisible par 4.
- **Divisibilité par 11 :** Un nombre est divisible par 11 si la somme de ses chiffres de rang impair moins la somme de ses chiffres de rang pair (de la droite vers la gauche) est divisible par 11.

Exemple :

Soit **x = 4 3 7 1 9 5**

5 – 9 + 1 – 7 + 3 – 4 = – 11 divisible par 11 donc x est divisible par 11.

Plus Petit Commun Multiple – Plus Grand Commun Diviseur .

I – Plus petit commun multiple de deux nombres :

1) Exemple : Trouver $2\mathbb{Z}\cap 3\mathbb{Z}$; que représente $2\mathbb{Z}\cap 3\mathbb{Z}$. Quel est le plus petit élément positif non nul de $2\mathbb{Z}\cap 3\mathbb{Z}$?

$2\mathbb{Z} = \{.....; -6; -4 ; -2 ; 0 ; 2 ; 4 ; 6 ; 8 ; .....\}$

$3\mathbb{Z} = \{.....; -9; -6 ; -3 ; 0 ; 3 ; 6 ; 9 ; 12 ; .....\}$

$2\mathbb{Z}\cap 3\mathbb{Z} = \{.....; -12; -6 ; 0 ; 6 ; 12 ; 6 ; 9 ; 12 ; .....\} = 6\mathbb{Z}$.

Le plus petit élément positif non nul de $2\mathbb{Z}\cap 3\mathbb{Z}$ est **6**. Cet élément est appelé le plus petit commun multiple à 2 et 3. On note : P.P.C.M (2 ; 3) = 6 ou $2\vee 3 = 6$.

2) Définition : Soit a et b deux éléments de $\mathbb{Z}^*$. On appelle plus petit commun multiple de a et b, le plus petit élément positif non nul de $a\mathbb{Z}\cap b\mathbb{Z}$.

On note : PPCM (a ; b) ou $a \vee b$.

Exemple : PPCM(–3 ; 5) = 15.

3) Théorème Fondamental:

L'ensemble des multiples communs à deux nombres est l'ensemble des multiples de leur PPCM. Autrement dit, lorsque PPCM(a ; b) = μ on a :

- $a\mathbb{Z}\cap b\mathbb{Z} = \mu\,\mathbb{Z}$;
- $\forall m \in \mathbb{Z}$, [m est multiple de a et b] $\Leftrightarrow$ [m est multiple de μ].

4) Propriétés:

P_1) Soient a et b deux entiers relatifs non nuls

$\forall\, k \in \mathbb{N}^*$, PPCM (k a ; k b) = $k \times$ PPCM(a ; b).

P_2) Tout nombre divisible par a et par b n'est pas toujours divisible par $a\times b$.

Exemple : 20 est divisible par 4 et par 10 ; mais 20 n'est pas divisible par 40.

II – Plus grand commun diviseur de deux nombres :

1) Exemple : Soit a = 12 et b = 8. Déterminer l'ensemble des diviseurs positifs de 12 et de 8. Quel est le plus grand élément de $\mathcal{D}_{12}\cap\mathcal{D}_8$?.

-- 0 --

$\mathcal{D}_{12} = \{1 ; 2 ; 3 ; 4 ; 6 ; 12\}$; $\mathcal{D}_{12} = \{1 ; 2 ; 4 ; 8 ; \}$ alors a : $\mathcal{D}_{12}\cap\mathcal{D}_8 = \{1 ; 2 ; 4\}$.

4 est le plus grand élément. On note : **P.G.C.D (12 ; 8) = 4 ou $12\wedge 8 = 4$** .

2) Définition : Soit a et b deux éléments de $\mathbb{Z}^*$. On appelle plus grand commun diviseur de a et b, le plus grand élément de :$\mathcal{D}_a\cap\mathcal{D}_b$.

On note : PGCD (a ; b) ou $a \wedge b$.

3) Théorème Fondamental:

Lorsque PGCD(a ; b) = δ on a :

- $\mathcal{D}_a \cap \mathcal{D}_b = \mathcal{D}_\delta$;
- $\forall d \in \mathbb{Z}^*$, [d/a et d/b $\Leftrightarrow$ d/δ] .

4) Détermination pratique du PGCD de deux nombres:

a) 1ère méthode : (Prendre le max de $\mathcal{D}_a \cap \mathcal{D}_b$).
Elle est bonne lorsque a et b sont des petits nombres.

b) 2ème méthode : on utilise la propriété suivante, pour tout nombre entier relatif non nul ; P.G.C.D(x ; y) = P.G.C.D (x – y ; y) .

Exemple : x = 924 et y = 336.

PGCD(924 ; 336) = PGCD(924–336 ; 336) = PGCD(588 ; 336)
= PGCD(588–336 ; 336) = PGCD(336 ; 252) = PGCD(252 ; 84)
=PGCD(168 ; 84) PGCD(84 ; 84) = 84.

c) 3ème méthode : (Algorithme d'Euclide).

Propriété (P) : PGCD(a ; b) = PGCD(b ; r) avec a = bq + r.

Exemple : a = 5775 et b = 784.

5775 = 7 ×784 + 287. Donc PGCD(5775 ; 784) = PGCD(784 ; 287).
En réitérant 7 fois la propriété (P) on obtient le tableau ci-dessous.

a_i	5775	784	287	210	77	56	21	14
b_i	784	287	210	77	56	21	14	7
r_i	287	210	77	56	21	14	7	0

Le PGCD cherché est le dernier reste non nul. **D'où PGCD(5775 ; 784) = 7.**

5) Nombres étrangers (ou nombres premiers entre eux) :

a) Définition : Si a ∧ b = 1 alors on dit que a et b sont étrangers.

b) Théorème de Bézout :
Deux entiers non nuls a et b sont dits étrangers s'il existe deux entiers relatifs k et ℓ tel que : a k + b ℓ = 1.

- Formulation : $[a \wedge b = 1] \Leftrightarrow [\exists (k ; \ell) \in \mathbb{Z}^2 / a k + b \ell = 1]$.

- Exemple: Déterminer $354 \wedge 25$ et trouver deux entiers relatifs k et ℓ tel que :

$$354k + 25\ell = 1.$$

Divisions	354	25	4	1
Quotients		14	6	4
Restes		4	1	0

$$\mathbf{354 = 25} \times 14 + 4 \Rightarrow 4 = \mathbf{354 - 25} \times 4.$$

$$\mathbf{25} = 6 \times 4 + 1 \Rightarrow 1 = \mathbf{25} - 6 \times 4$$

$$1 = \mathbf{25} - 6\times(\mathbf{354 - 25}\times 14) \Leftrightarrow 1 = \mathbf{25} - 6\times\mathbf{354 + 25}\times 84) \Leftrightarrow$$

$$1 = \mathbf{354}\times\mathbf{(-}\ 6) + \mathbf{25}\times(\ 85)$$

D'où $k = -6$ et $\ell = 85$.

c) Théorème de GAUSS :

$\forall$ (a ; b ; c) $\in (\mathbb{Z}^*)^3$, si a / bc et a est étranger à b alors a/c.

$$\left.\begin{array}{l} Si \quad a / bc \\ et \quad a \wedge b = 1 \end{array}\right\} \quad Alors \quad a / c$$

d) Propriétés :

P_1) $\forall$ (a_1 ; a_2 ; b) $\in (\mathbb{Z}^*)^3$, [PGCD(a_1 ; a_2 ; b) = 1 $\Leftrightarrow$ $\begin{cases} a_1 \wedge b = 1 \\ a_2 \wedge b = 1 \end{cases}$] ;

P_2) $\forall$ (a_1 ; a_2) $\in (\mathbb{Z}^*)^2$, $\forall n \in \mathbb{Z}$ $\begin{cases} a_1 \wedge a_2 = 1 \\ a_1 / n \\ a_2 / n \end{cases} \Rightarrow a_1 a_2 / n$;

P_3) Si $a \wedge b = 1$ alors $a \wedge b^n = 1$ ($\forall n \in \mathbb{N}$) ;

P_4) PGCD(a ; b) = $\delta \Leftrightarrow \exists!$ (a_1 ; b_1) $\in (\mathbb{N}^*)^2$ tel que : $\begin{cases} a = \delta a_1 \\ b = \delta b_1 \\ a_1 \wedge b_1 = 1 \end{cases}$

P_5) Si $a \wedge b = 1$ alors PPCM (a ; b) = ab ;

P_6) Si a est multiple de b alors PPCM(a ; b) = a et PGCD(a ; b) = b ;

P_7) Soit m $\in \mathbb{N}^*$ et m $\in a\mathbb{Z} \cap b\mathbb{Z}$.

PPCM(a ; b) = m $\Leftrightarrow$ $\frac{m}{a}$ *et* $\frac{m}{b}$ *sont étrangers*.

e) Relation entre PGCD et PPCM :

$\forall (a ; b) \in (\mathbb{Z}^*)^2$, PGCD (a ; b) × PPCM (a ; b) = |a b|

6) Exemple d'utilisation du PGCD, du PPCM :

Déterminer tous les couples d'entiers naturels (a ; b) tels que $\begin{cases} a \wedge b = 7 \\ a \vee b = 84 \end{cases}$

-- 0 --

En utilisant la propriété P_4) on a :

PGCD(a ; b) = δ $\Leftrightarrow$ ∃! $(a_1 ; b_1) \in (\mathbb{N}^*)^2$ tel que : $\begin{cases} a = \delta a_1 \\ b = \delta a_2 \\ a_1 \wedge b_1 = 1 \end{cases} \Leftrightarrow \begin{cases} a = 7a_1 \\ b = 7b_1 \\ a_1 \wedge b_1 = 1 \end{cases}$;

$a \vee b = 84 \Leftrightarrow 7a_1 \vee 7b_1 = 84 \Leftrightarrow 7(a_1 \vee b_1) = 84 \Leftrightarrow 7 a_1 b_1 = 84 \Leftrightarrow a_1 b_1 = 12 \Rightarrow$

$a_1 \in \mathcal{D}_{12}$ et $b_1 \in \mathcal{D}_{12}$ avec $a_1 \wedge b_1 = 1$. $\mathcal{D}_{12} = \{1 ; 12 ; 2 ; 6 ; 3 ; 4\}$.

- 1er cas : si $a_1 = 1$ et $b_1 = 12$ alors a = 7 et b = 84.
- 2ème cas : si $a_1 = 2$ et $b_1 = 6$ impossible car 2 et 6 sont non étrangers.
- 3ème cas : si $a_1 = 3$ et $b_1 = 4$ alors a = 21 et b = 28.

L'ensemble des solutions est : $S = \{(7;84);(84;7);(21;28) ; (28;21)\}$.

7) PGCD et PPCM de plusieurs nombres :

Exemple : PGCD (15 ; 21 ; 35) = PGCD (3 ; 35) = 1 ;
PPCM (34 ; 51 ; 78) = PPCM (102 ; 78) = 1326.

8) Formule du binôme de Newton :

$$(a+b)^n = \sum_{k=0}^{n} C_n^k \, a^{n-k} \, b^k = C_n^0 \, a^n \, b^0 + C_n^1 \, a^{n-1} \, b + \ldots\ldots\ldots + C_n^{n-1} \, a \, b^{n-1} + C_n^n \, a^0 \, b^n$$

$$C_n^k = \frac{n!}{(n-k)! \times k!}$$

9) Décomposition en produit de facteurs premiers :

a) Exemples : Décomposer les nombres a = 60 et b = 975 en produit de facteurs premiers.

60	2
30	2
15	3
5	5
1	

$60 = 2^2 \times 3 \times 5$

975	5
195	5
39	3
13	13
1	

$975 = 3 \times 5^2 \times 13$

b) Application à la recherche du PGCD et du PPCM :

Prenons a = 7875 et b = 975 on a les décompositions suivantes

$$a = 3^2 \times 5^3 \times 7$$

$$b = 3 \times 5^2 \times 13$$

D'où PGCD (7875 ; 975) = 3×5^2 = 75.

Et PPCM (7875 ; 975) = $3^2 \times 5^3 \times 7 \times 13$ = 102375.

III –Application à la résolution d'une équation du 1er degré dans $\mathbb{Z} \times \mathbb{Z}$:

En général soit à résoudre l'équation : ax + by = c ; (a ; b) $\in (\mathbb{Z}^*)^2$, (x ; y) sont les inconnues dans $\mathbb{Z} \times \mathbb{Z}$. (E) : ax + by = c.

On cherche le PGCD (a ; b) = δ.

- Si δ ne divise pas c alors S(E) = Ø.
- Si δ/c alors on simplifie l'équation par δ on obtient (E_1) : $a_1x + b_1y = c_1$ avec $a_1 \wedge b_1 = 1$.

On cherche une solution évidente (x_0 ; y_0) de (E_1) à partir des multiples de a_1 et b_1 dont la différence donne c_1.

$$a_1x + b_1y = c_1$$

$$-$$

$$a_1x_0 + b_1y_0 = c_1$$

$$a_1(x - x_0) + b_1(y - y_0) = 0$$

- $a_1(x - x_0) + b_1(y - y_0) = 0 \Leftrightarrow a_1(x - x_0) = -b_1(y - y_0) \Rightarrow$
  $a_1 / -b_1(y - y_0) \Rightarrow$ d'après Gauss que $a_1 / -(y - y_0) \Rightarrow$
  $\exists\, k \in \mathbb{Z} /\ y - y_0 = -k\, a_1 \Leftrightarrow y = y_0 - ka_1$.
- De même $b_1 / a_1(x - x_0) \Rightarrow$ d'après Gauss que $b_1/(x - x_0) \Rightarrow$

  $\exists\, k \in \mathbb{Z} /\ x - x_0 = k\, b_1 \Leftrightarrow x = x_0 + kb_1$.

  D'où l'ensemble des solutions de l'équation est :

$$S = \{(\ x_0 + kb_1; y_0 - ka_1) / k \in \mathbb{Z}\}.$$

Utilisation de la congruence:

$a_1x + b_1y = c_1 \Leftrightarrow a_1x = -b_1y + c_1 \Leftrightarrow a_1x \equiv c_1[\, b_1] \Leftrightarrow x \equiv x_0[\, b_1] \Rightarrow$

$\exists\, k \in \mathbb{Z} / x = b_1k + x_0$. En remplaçant x par valeur on a : $y = a_1k + y_0$.

Exemples : Résoudre les équations

a) $4x - 8y = 3$;

b) $14x - 22y = 4$.

-- 0 –

a) $4x - 8y = 3$; $4 \wedge 8 = 4 \Rightarrow \delta = 4$ ne divise pas 3 donc $S = \emptyset$.

b) $14x - 22y = 4$; $14 \wedge 22 = 2$; δ /4 donc on a : (E1) : $7x - 11y = 2$.
Une solution particulière de (E_1) est le couple $(x_0 ; y_0) = (5 ; 3)$ à partir de $7\mathbb{N}$ et $11\mathbb{N}$.

$$\begin{array}{r} 7x - 11y = 2 \\ - \\ 7x_0 - 11y_0 = 2 \\ \hline 7(x - x_0) - 11(y - y_0) = 0. \end{array}$$

$7(x - x_0) - 11(y - y_0) = 0 \Leftrightarrow 7(x - 5) = 11(y - 3) \Rightarrow$

- $7/11(y - 3) \Rightarrow$d'après Gauss $7/(y - 3) \Rightarrow y - 3 = 7k \Rightarrow y = 7k + 3$.
- $11/7(x - 5) \Rightarrow$d'après Gauss $11/(x - 5) \Rightarrow x - 5 = 11k \Rightarrow x = 11k + 5$.

L'ensemble solution est $S = \{(11k + 5 ; 7k + 3) / k \in \mathbb{Z}\}$.

Autre méthode : (utilisation de la congruence)

$14x - 22y = 4$; $14 \wedge 22 = 2$; 2 /4 donc on a : (E_1) : $7x - 11y = 2$.

$7x = 11y + 2 \Leftrightarrow 7x \equiv 2\ [11]$ en multipliant par 8 on a :

$56x \equiv 16\ [11] \Leftrightarrow x \equiv 5\ [11] \Rightarrow x = 11k + 5$. En remplaçant x par sa valeur dans l'équation $7x - 11y = 2$, on obtient $y = 7k + 3$.

D'où l'ensemble solution est : $S = \{(11k + 5 ; 7k + 3) / k \in \mathbb{Z}\}$.