I- Divisibilité dans $\mathbb{Z}$:

Définition :

Soient a et d deux entiers relatifs.

On dit que d divise a et on écrit d/a si et seulement si : $(\exists k \in \mathbb{Z});a = k.d$.

Exemple :

On a : $12 = 1\times 12 = 2\times 6 = 3\times 4$, donc les diviseurs positif de 12 sont : 1;2;3;4;6 et 12

✓ Conséquences :

- 0 est multiple de tout entier.
- 1 divise tout entier.
- Si a est un multiple de b et si $a \neq 0$ alors : $|a| \geqslant |b|$.
- Si a divise b et si b divise a alors $a = b$ ou $a = -b$ avec a et b non nuls.

Propriété 01 :

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

-- Si d/a , alors : $d/b \Leftrightarrow d/b-a \Leftrightarrow (\forall k \in \mathbb{Z});d/b-ka$.

Si $(a,b,c) \in (\mathbb{Z}^*)^3$, alors :

-- $ab/ac \Leftrightarrow b/c$.

-- $(a/b \text{ et } b/c) \Rightarrow a/c$ (la divisibilité dans $\mathbb{Z}$ est transitive).

-- $\begin{cases} a/b \\ a/c \end{cases} \Rightarrow \begin{cases} a/b+c \\ a/b-c \end{cases}$, plus généralement : $\begin{cases} a/b \\ a/c \end{cases} \Rightarrow \left((\forall(\alpha,\beta)\in\mathbb{Z}^2);a/\alpha b+\beta c\right)$.

Preuve :

Supposons que : d/a

Et montrons que : $d/b \Leftrightarrow d/b-a$.

On a : $d/a \Leftrightarrow (\exists k \in \mathbb{Z});a = k.d$ et $d/b \Leftrightarrow (\exists k' \in \mathbb{Z});b = k'.d$

Donc : $b-a = d(k'-k)$ par suite : $d/b-a$.

Réciproquement : si $d/b-a$,alors : $(\exists \alpha \in \mathbb{Z});b-a = \alpha.d$

Donc : $a+b-a = kd+\alpha d$ c'est à dire : $b = d(k+\alpha)$.

D'ou : d/b .

Remarque :

Soit $(a,b) \in (\mathbb{Z}^*)^2$, on a : $a^n - b^n = (a-b).\sum_{k=0}^{n-1} a^{(n-1)-k}b^k$, Où $n \in \mathbb{N}^* - \{1\}$.

Donc : $\left((\forall n \in \mathbb{N}^* - \{1\});a-b/a^n-b^n\right)$.

Et si $n \in \mathbb{N}^* - \{1\}$ est impair, alors : $a+b/a^n+b^n$.

Exercice 01:

1. Déterminer tous les couples $(x,y) \in \mathbb{N}^2$ tels que : $x^2 - 2xy = 15$.
2. Déterminer tous les entiers relatifs n tels que $n-3$ divise $n+5$.
3. Quels peuvent être les diviseurs positifs communs à $a = 9k+2$ et $b = 12k+1$? Où k est un entier naturel ($k \in \mathbb{N}$).

✓ Correction :

1. Soit $(x,y) \in \mathbb{N}^2$. On a :

$$x^2 - 2xy = 15 \Leftrightarrow x(x-2y) = 15 \Leftrightarrow \begin{cases} x = 15 \\ x-2y = 1 \end{cases} \text{ ou } \begin{cases} x = 5 \\ x-2y = 3 \end{cases}$$

Car , l'ensemble des diviseurs positifs de $15 = 1\times 15 = 3\times 5$ est $D_{15} = \{1;3;5;15\}$.

Et en plus : $x \geq x-2y$ car $(x,y) \in \mathbb{N}^2$. Donc :

$x^2 - 2xy = 15 \Leftrightarrow \begin{cases} x = 15 \\ y = 7 \end{cases}$ ou $\begin{cases} x = 5 \\ y = 1 \end{cases}$. Par suite : $(x,y) = (15,7)$ ou $(x,y) = (5,1)$.

2. Soit $n \in \mathbb{Z} - \{3\}$. On a :

$$n-3 \text{ divise } n+5 \Leftrightarrow \frac{n+5}{n-3} \in \mathbb{Z} \Leftrightarrow \frac{n-3+8}{n-3} \in \mathbb{Z} \Leftrightarrow 1+\frac{8}{n-3} \in \mathbb{Z} \Leftrightarrow \frac{8}{n-3} \in \mathbb{Z}$$

Par suite : $n-3$ divise $n+5 \Leftrightarrow n-3$ divise $8 \Leftrightarrow n-3 \in \{-8;-4;-2;-1;1;2;4;8\}$.

D'ou : $n-3$ divise $n+5 \Leftrightarrow n \in \{-5;-1;1;2;4;5;7;11\}$.

Donc , l'ensemble des entiers relatifs n tels que $n-3$ divise $n+5$ est :

$$\{-5;-1;1;2;4;5;7;11\} .$$

3. Soit $d \in \mathbb{N}$.

Si d est un diviseur commun à $a = 9k+2$ et $b = 12k+1$, alors : d divise $4a-3b$

Or $4a-3b = 5$, donc d divise 5 . Par suite : $d = 1$ ou $d = 5$.

En conclusion , les valeurs possibles de tous diviseurs positifs communs à $a = 9k+2$ et $b = 12k+1$ sont : 1 et 5 .

Exercice 02:

1. Déterminer tous les entiers relatifs n tels que : $\frac{6n+12}{2n+1} \in \mathbb{Z}$.
2. Déterminer tous les entiers relatifs n tels que $n-4$ divise $3n-17$.
3. Montrer que si n est un entier impair alors n^2-1 est divisible par 8.
4. Soit $k \in \mathbb{Z}$. quels sont les valeurs possibles d'un diviseur commun à $a = 4k+3$ et $b = 5k-7$?

✓ *Correction :*

1. *Comme :* $(\forall n\in\mathbb{Z});\dfrac{6n+12}{2n+1}=\dfrac{3(2n+1)+9}{2n+1}=3+\dfrac{9}{2n+1}$, *alors :*

$$\frac{6n+12}{2n+1}\in\mathbb{Z}\Leftrightarrow\frac{9}{2n+1}\in\mathbb{Z}\Leftrightarrow 2n+1/9\Leftrightarrow 2n+1\in\{-9;-3;-1;1;3;9\}$$

Car l'ensemble des diviseurs de est : $D_9=\{-9;-3;-1;1;3;9\}$.

D'ou : $\dfrac{6n+12}{2n+1}\in\mathbb{Z}\Leftrightarrow n\in\{-5;-2;-1;0;1;4\}$.

3. *Comme* n *est impair, alors :* $n=2k+1$ *Où* $k\in\mathbb{Z}$.

Donc : $n^2-1=(2k+1)^2-1^2=2k\times(2k+2)=4k(k+1)=8.\dfrac{k(k+1)}{2}$

D'autre part : $(\forall k\in\mathbb{Z});\dfrac{k(k+1)}{2}\in\mathbb{Z}$, *car* $k(k+1)$ *est toujours pair.*

D'ou : n^2-1 *est divisible par* 8 .

Exercice 03:

1. *Résoudre dans* $\mathbb{N}^2$ *l'équation :* $(E):x^2-4y^2=36$.

2. *Déterminer tous les entiers relatifs* x *pour lesquels :* $\dfrac{x^2-x+2}{2x+1}\in\mathbb{Z}$.

✓ *Correction :*

1. *Soit* $(x,y)\in\mathbb{N}^2$, *On a :* $x^2-4y^2=36\Leftrightarrow(x-2y)\times(x+2y)=36$

Les écritures possibles de **36** *en produit de deux entiers naturels sont :*

$36=1\times36=2\times18=3\times12=4\times9=6\times6$

De plus $(\forall(x,y)\in\mathbb{N}^2);x-2y\le x+2y$ *et* $x-2y$ *et* $x+2y$ *ont la même parité, Donc :*

$$x^2-4y^2=36\Leftrightarrow\begin{cases}x-2y=2\\x+2y=18\end{cases}\text{ ou }\begin{cases}x-2y=6\\x+2y=6\end{cases}\Leftrightarrow(x,y)=(10,4)\text{ ou }(x,y)=(6,0).$$

2. *Soit* $x\in\mathbb{Z}$, *On a :*

$$\begin{aligned}\frac{x^2-x+2}{2x+1}\in\mathbb{Z}&\Rightarrow 2x+1/x^2-x+2\Rightarrow 2x+1/4(x^2-x+2)\\&\Rightarrow 2x+1/(4x^2-4x+8)-(2x+1)^2\\&\Rightarrow 2x+1/-8x+7\\&\Rightarrow 2x+1/-8x+7+4(2x+1)\\&\Rightarrow 2x+1/11\end{aligned}$$

Donc : $2x+1\in\{-11;-1;1;11\}$ *c'est à dire que* $x\in\{-6;-1;0;5\}$.

Par suite : $\left\{x\in\mathbb{Z}/\dfrac{x^2-x+2}{2x+1}\in\mathbb{Z}\right\}\subset\{-6;-1;0;5\}$.

Il est facile de vérifier que l'inclusion inverse est satisfaite, donc les entiers relatifs x *pour lesquels :* $\dfrac{x^2-x+2}{2x+1}\in\mathbb{Z}$ *sont :* -6 ; -1 ; 0 et 5 .

II- La division euclidienne dans $\mathbb{Z}$:

Théorème 01:

Pour tout $(a,b)\in\mathbb{Z}\times\mathbb{N}^*$ *il existe* *un couple unique* $(q,r)\in\mathbb{Z}\times\mathbb{N}$ *tels que :* $\begin{cases}a=bq+r\\0\le r<b\end{cases}$.

(a s'appelle le dividende, b le diviseur, q le quotient et r le reste)

✓ *Preuve :*

Analyse :

Si le couple (q,r) *existe, alors :* $0\le r=a-bq<b$. *Donc :* $bq\le a<b(q+1)$.

D'ou : $q\le\dfrac{a}{b}<q+1$, *par suite :* $q=E\left(\dfrac{a}{b}\right)$ *et* $r=a-bq$.

Synthèse :

-- *Existence du couple* (q,r) :

Prenons $q=E\left(\dfrac{a}{b}\right)$ *et* $r=a-bq$; *alors* $a=bq+r$ *et* $q\le\dfrac{a}{b}<q+1$.

D'ou : $q\le\dfrac{a}{b}<q+1\Rightarrow0\le r=a-bq<b$ *et* $a=bq+r$.

-- *Unicité du couple* (q,r) :

Supposons que : $a=bq+r=bq'+r'$ *Où* $\begin{cases}0\le r<b\\0\le r'<b\end{cases}$.

Donc : $b(q-q')=r'-r$ *et comme :* $-b<r'-r<b\Rightarrow-1<q-q'<1$

Alors : $q-q'=0$ *et donc* $r'-r=0$.

D'ou l'unicité du couple (q,r).

Théorème 02:

Pour tout $(a,b)\in\mathbb{Z}\times\mathbb{Z}^*$ *il existe un couple unique* $(q,r)\in\mathbb{Z}\times\mathbb{N}$ *tels que :*

$$a=bq+r\text{ avec }0\le r<|b| .$$

Exercice 04:

1. Trouver tous les entiers a qui divisés par **5** donne un quotient égal à 3 fois le reste .
2. Lorsqu'on divise a par b, le reste est **8** et lorsqu'on divise $2a$ par b, le reste est **5** . Trouver le diviseur b .
3. On divise un entier naturel n par **152** puis par **147** . Les quotients sont égaux et les restes respectifs sont **13** et **98** . Quel est cet entier naturel ?
4. Déterminer un entier naturel N composé de quatre chiffres sachant que le reste de la division euclidienne par N de **21 685** et **33 509** est respectivement **37** et **53** .
5. On considère l'ensemble : $E=\{1;2;3;...;10\}$.

   Déterminer toutes les paires $\{a;b\}$ dont les éléments appartiennent à E et le reste de la division euclidienne de $a\times b$ par **11** est **1** .

✓ Correction :

1. Soit $a\in\mathbb{Z}$? Si la division euclidienne de a par **5** donne un quotient égal à 3 fois le reste , alors : $a=5\times(3r)+r$ Où $r\in\{0;1;2;3;4\}$.

   Donc : $a=16.r$ Où $r\in\{0;1;2;3;4\}$.

   Par suite , les entiers a qui divisés par **5** donne un quotient égal à 3 fois le reste sont : **0** , **16**, **32**, **48** et **64** .
2. Soit $(a,b)\in\mathbb{Z}\times\mathbb{Z}^*$.

   Comme lorsqu'on divise a par b, le reste est **8** et lorsqu'on divise $2a$ par b, le reste est **5**

   Alors : $\begin{cases} a=bq+8 \\ 2a=bq'+5 \end{cases}$ Où $|b|\geq 9$.

   On a : $a=bq+8\Rightarrow 2a=2bq+16$, donc : $\begin{cases} a=bq+8 \\ 2a=bq'+5 \end{cases}\Rightarrow 2bq+16=bq'+5$

   Par suite : $b(q'-2q)=11$. D'ou b est un diviseur de **11** vérifiant $|b|\geq 9$.

   Cela veut dire que : $b=11$ où $b=-11$.
3. Soit $n\in\mathbb{N}$.

   Comme la division euclidienne de n par **152** puis par **147** donnent des quotients égaux et des restes respectifs **13** et **98**, alors :

   $n=152q+13=147q+98$ Où $q\in\mathbb{N}^*$.

   Par suite : $152q-147q=98-13$, c'est à dire : $5q=85$.

   D'ou : $q=17$.

   Et par conséquent : $n=152\times17+13=147\times17+98$.

   Soit : $n=2597$.

4. En traduisant les données , on obtient :

$$\begin{cases} 21\,685=N.q+37 \\ 33\,509=N.q'+53 \end{cases} \text{ Où } (q,q')\in\mathbb{N}^2 . \text{ Donc : } \begin{cases} N.q=21\,648 \\ N.q'=33\,456 \end{cases}$$

D'ou N est diviseur commun de $a=21\,648$ et $b=33\,456$ formé de quatre chiffres .

On pourra donc conclure que : N divise $a\wedge b$ (le plus grand diviseur commun de a et b).

On a : $\begin{cases} a=2^4\times3\times11\times41 \\ b=2^4\times3\times17\times41 \end{cases}\Rightarrow a\wedge b=2^4\times3\times41=1968$

N est un diviseur de **1968** formé de quatre chiffres , donc : $N=1\,968$. Car le plus grand diviseur propre de **1968** est **984** et c'est un nombre formé de trois chiffres .

5. Soit $\{a;b\}\subset\{1;2;3;...;10\}$ tels que la division euclidienne de $a\times b$ par **11** donne **1** comme reste .

Donc : $a\times b=11k+1$ Où $k\in\{1;2;3;...;8\}$ car : $2\leq a\times b\leq 90\Leftrightarrow \frac{1}{11}\leq k\leq\frac{89}{11}$.

On a : $k=1\Rightarrow ab=12\Rightarrow(\{a;b\}=\{3;4\}$ Où $\{a;b\}=\{2;6\})$

$k=2\Rightarrow ab=23\Rightarrow$ il n'y a aucune paire

$k=3\Rightarrow ab=34\Rightarrow$ il n'y a aucune paire

$k=4\Rightarrow ab=45\Rightarrow\{a;b\}=\{5;9\}$ il y a une seule paire

$k=5\Rightarrow ab=56\Rightarrow\{a;b\}=\{7;8\}$ il y a une seule paire

$k=6\Rightarrow ab=67\Rightarrow$ il n'y a aucune paire

$k=7\Rightarrow ab=78\Rightarrow$ il n'y a aucune paire

$k=8\Rightarrow ab=89\Rightarrow$ il n'y a aucune paire

En conclusion : il y a quatre paire $\{a.b\}\subset\{1;2;3;...;10\}$ tels que la division euclidienne de $a\times b$ par **11** donne **1** comme reste : $\{2;6\}$, $\{3;4\}$, $\{5;9\}$ et $\{7;8\}$.

III- Les nombres premiers :

Définition :

Un nombre premier est un entier naturel qui admet exactement deux diviseurs dans $\mathbb{N}$: **1** et lui même .

✓ Conséquences :

- 1 n'est pas un nombre premier (il n'a qu'un seul diviseur)
- Un nombre premier p est un naturel supérieur ou égal à 2 soit : $p\geqslant 2$.
- Les nombres premiers inférieurs à 100 sont :
  2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 et 97

Crible d'Eratosthène :

Sur le tableau ci-contre :
On a éliminé en bleu
Les multiples de 2 sauf 2 ,
Puis ceux de 3 sauf 3 , puis de 5 sauf 5 et ceux de 7 sauf 7 .
*Les nombres restant en jaune Sont les nombres premiers plus Petit que **100** .*

	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

- *Critère d'arrêt :*

Tout entier naturel n, $n \geq 2$, admet au moins un diviseur premier dans $\mathbb{N}$.

Si n n'est pas premier ,alors il admet un diviseur premier p tels que : $2 \leq p \leq \sqrt{n}$.

✓ *Preuve :*

- Si n est premier, il admet donc un diviseur premier : lui-même.
- Si n n'est pas premier, l'ensemble des diviseurs d de n tel que : $2 \leqslant d < n$ n'est pas vide. Il admet donc un plus petit élément p. Si p n'était pas premier, il admettrait un diviseur d' tel que $2 \leqslant d' < p$ qui diviserait n. Ceci est impossible car p est le plus petit. Donc p est premier.
- On a donc p premier et $n = p \times q$ avec $p \leqslant q$. En multipliant cette inégalité par p, on obtient :

$$p^2 \leqslant pq \quad \Leftrightarrow \quad p^2 \leqslant n \quad \text{soit} \quad p \leqslant \sqrt{n}$$

A retenir : *Si $n \geq 2$ est non premier , alors son plus petit diviseur propre est premier .*

- ***Propriété 02** :(test de primalité)*

Si un entier naturel $n \geq 2$, n'est pas divisible par aucun entier premier p tels que : $2 \leq p \leq \sqrt{n}$, alors n est premier .

- *Exemple:*

✓ *Montrons que **521** est premier .*

On a : $\sqrt{521} \simeq 22{,}8$.

*Donc les entiers premiers p tels que : $2 \leq p \leq \sqrt{521}$ sont **2, 3, 5, 7, 11 13 ,17** et **19** .*

*Le tableau suivant donne le reste de la division euclidienne de **521** par ces entiers :*

521								
p	2	3	5	7	11	13	17	19
Le reste r	1	2	1	3	4	1	11	8

*Comme **521** n'est pas divisible par aucun de ces entiers, alors il est premier .*

- *Remarque:*

Un entier naturel $n \geq 2$, est non premier si et seulement si : il existe $(p,q) \in \mathbb{N} \times \mathbb{N}$ tels que : $\begin{cases} n = p.q \\ p \geq 2 \text{ et } q \geq 2 \end{cases}$.

Application :
Montrer que $1945^4 + 4^{1945}$ n'est pas premier .

✓ *Correction :*

On utilisera l'identité de Sophie Germain :

$$x^4 + 4y^4 = (x^2+2y^2)^2 - 4x^2y^2 = (x^2+2y^2-2xy)(x^2+2y^2+2xy) = ((x+y)^2+y^2)((x-y)^2+y^2).$$

On a : $1945^4 + 4^{1945} = 1945^4 + 4 \times 4^{1944} = 1945^4 + 4 \times \left(4^{486}\right)^4$

En appliquant l'identité de Sophie Germain pour $x = 1945$ et $y = 4^{486}$, on obtient :

$$1945^4 + 4^{1945} = \left(\left(1945+4^{486}\right)^2 + 4^{972}\right) \times \left(\left(1945-4^{486}\right)^2 + 4^{972}\right)$$

Et donc $1945^4 + 4^{1945}$ n'est pas premier car il s'écrit comme produit deux entiers naturels tous plus grand que 2 .

- *Exercice 05:*

1. *Déterminer toutes les valeurs de l'entier naturel n pour que A_n soit premier dans chacun des cas suivants :* $(1): A_n = n^2 + 4n + 3$, $(2): A_n = n^2 - 8n + 15$ $(3): A_n = n^4 + 4$ *et* $(4): A_n = n^4 + n^2 + 1$.
2. *Résoudre dans $\mathbb{N}^2$ les équations :* $(E_1): x^2 - y^2 = p$ *et* $(E_2): x^2 - y^2 = p^2$.
   Où $p \geq 2$ un est entier naturel premier .
3. *Décomposer en facteurs premiers l'entier **469** , puis résoudre dans $\mathbb{N}^2$ l'équation :* $(E_3): x^3 - y^3 = 469$.

✓ *Correction :*

1. $(1): A_n = n^2 + 4n + 3$

On a : $(\forall n \in \mathbb{N}); A_n = n^2 + 4n + 4 - 1 = (n+2)^2 - 1 = (n+1)(n+3)$

$n = 0 \Rightarrow A_0 = 3 \Rightarrow 3$ est premier

Et si $n \geq 1$, alors : $n+1 \geq 2$ et $n+3 \geq 4$. Donc A_n est non premier .

Conclusion : A_n est premier $\Leftrightarrow n = 0$.

$(3): A_n = n^4 + 4$

On a : $(\forall n \in \mathbb{N}); A_n = n^4 + 4 = \left(n^2+2\right)^2 - 4n^2 = \left(n^2+2+2n\right)\left(n^2+2-2n\right)$

Par suite : $(\forall n \in \mathbb{N}); A_n = \left((n-1)^2+1\right)\left((n+1)^2+1\right)$.

$n = 1 \Rightarrow A_1 = 5 \Rightarrow 5$ est premier

Et si $n \neq 1$, alors : $(n-1)^2 + 1 \geq 2$ et $(n+1)^2 + 1 \geq 2$. Donc A_n est non premier .

Conclusion : A_n est premier $\Leftrightarrow n = 1$.

2. Résolvons dans $\mathbb{N}^2$ l'équation : $(E_1): x^2 - y^2 = p$.

On a : $(\forall (x,y) \in \mathbb{N}^2); (E_1) \Leftrightarrow (x-y)(x+y) = p \Leftrightarrow \begin{cases} x-y=1 \\ x+y=p \end{cases} \Leftrightarrow \begin{cases} x = \dfrac{p+1}{2} \\ y = \dfrac{p-1}{2} \end{cases}$.

Donc si $p=2$, alors : $S = \varnothing$. Et si $p \geq 3$, alors : $S = \left\{ \left(\dfrac{p+1}{2}, \dfrac{p-1}{2} \right) \right\}$.

Pour l'équation : $(E_2): x^2 - y^2 = p^2$, On a :

$$(\forall (x,y) \in \mathbb{N}^2); (E_2) \Leftrightarrow (x-y)(x+y) = p^2 \Leftrightarrow \begin{cases} x-y=1 \\ x+y=p^2 \end{cases} \text{ ou } \begin{cases} x-y=p \\ x+y=p \end{cases}$$

$$\Leftrightarrow \begin{cases} x = \dfrac{p^2+1}{2} \\ y = \dfrac{p^2-1}{2} \end{cases} \text{ ou } \begin{cases} x=p \\ y=0 \end{cases}$$

Donc : si $p=2$, alors : $S = \{(2,0)\}$.

Et si $p \geq 3$, alors : $S = \left\{ (p,0); \left(\dfrac{p^2+1}{2}, \dfrac{p^2-1}{2} \right) \right\}$.

3. Résolution de l'équation $(E_3): x^3 - y^3 = 469$.

La décomposition de **469** en facteurs premiers est : $469 = 7 \times 67$.

Donc : $(\forall (x,y) \in \mathbb{N}^2); (E_3) \Leftrightarrow \begin{cases} x-y=1 \\ x^2+xy+y^2=469 \end{cases} \text{ou} \begin{cases} x-y=7 \\ x^2+xy+y^2=67 \end{cases}$

D'une part : $(\forall (x,y) \in \mathbb{N}^2); \begin{cases} x-y=1 \\ x^2+xy+y^2=469 \end{cases} \Leftrightarrow \begin{cases} x=y+1 \\ y(y+1)=156 \end{cases} \Leftrightarrow \begin{cases} x=13 \\ y=12 \end{cases}$

Et d'autre part : $(\forall (x,y) \in \mathbb{N}^2); \begin{cases} x-y=7 \\ x^2+xy+y^2=67 \end{cases} \Leftrightarrow \begin{cases} x=y+7 \\ y(y+7)=6 \end{cases}$

Or ce dernier système n'a pas de solution dans $\mathbb{N}^2$.

Donc l'ensemble des solutions de l'équation (E_3) est : $S = \{(13,12)\}$.

- **Propriété 03 :(infinité des nombres premiers)**

Il existe une infinité de nombres premiers .

✓ **Preuve :** On raisonne par l'absurde .

Supposons qu'il existe un nombre fini de nombres premiers : $p_1,\ p_2,\ p_3, \dots,\ p_n$.

Posons : $N = p_1 \times p_2 \times p_3 \times \ldots \times p_n + 1$.

Comme $N \geq 2$, alors d'après le critère d'arrêt il admet au moins un diviseur premier.

Soit p_k ce diviseur, où $1 \leq k \leq n$.

D'une part : p_k divise N et d'autres part : p_k divise $p_1 \times p_2 \times p_3 \times \ldots \times p_n$.

Par suite : p_k divise $N - p_1 \times p_2 \times p_3 \times \ldots \times p_n$, c'est à dire que : p_k divise 1 .

Ce qui est absurde ; car un nombre premier ne divise jamais 1.

- **Exercice 06:(les nombres de Mersenne)**

Un nombre de Mersenne s'écrit sous la forme : $M_n = 2^n - 1$, Où $n \in \mathbb{N}^*$.

1. Calculer les six premiers nombres de Mersenne . Que constatez vous .

2. Montrer que si M_n est premier alors n l'est aussi . (Raisonner par contraposition)

3. La réciproque de l'implication précédente est-elle vraie ? justifier la réponse .

- On rappelle que : $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \ldots + x^2 + x + 1)$.

✓ **Correction :**

1. Les six premiers nombres de Mersenne sont :

$M_1 = 1$, $M_2 = 3$, $M_3 = 7$, $M_4 = 15$, $M_5 = 31$ et $M_6 = 63$

On constate que pour les n égaux à **2 ,3 ,5** les nombres de Mersenne sont premiers .

Est-ce que si n est premier , M_n est premier ? la réponse est négative comme le montrera la réponse à la question **3.** En effet , on a : $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$.

Donc malgré que **11** est premier , M_{11} ne l'est pas .

2. Supposons que $n \geq 2$ n'est pas premier , donc : $n = d.q$ Où $d \geq 2$ et $q \geq 2$.

On a : $M_n = 2^n - 1 = (2^d)^q - 1 = (2^d - 1) \times \sum_{k=0}^{q-1} (2^d)^k$.

Comme M_n se décompose en produit de deux entiers tous les deux plus grand que **2**

Alors il n'est pas premier .

D'ou si n n'est pas premier alors M_n ne l'est pas non plus .

En utilisant la contraposée : si M_n est premier alors n l'est également .

IV- Le plus grand commun diviseur et le plus petit commun multiple :

1)- Plus grand commun diviseur :

✓ **Introduction :**

On a : $D_{45}=\{1;3;5;9;15;45\}$ et $D_{54}=\{1;2;3;6;9;18;27;54\}$.

Donc : $D_{45}\cap D_{54}=\{1;3;9\}$, **9** est le plus grand commun diviseur de **45** et **54**.

On écrit : $45\wedge 54=9$.

o **Définition :**

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

L'ensemble $D_a\cap D_b$ des diviseurs communs à a et b est non vide (car : $1\in D_a\cap D_b$)

Il est majoré par $\max(|a|,|b|)$, donc il admet un plus grand élément .

Ce plus grand élément est appelé le plus grand commun diviseur de a et b.

On le note : $a\wedge b$ ou $\text{pgcd}(a,b)$ ou $\Delta(a,b)$.

✓ **Conséquences :**

- Pour tout $a\in\mathbb{Z}^*$, on a : $a\wedge 1=1$ et $a\wedge 0=|a|$.
- Pour tout $(a,b)\in(\mathbb{Z}^*)^2$, on a : $a\wedge b\in\mathbb{N}^*$, $b\wedge a=a\wedge b$ et $a\wedge b=|a|\wedge|b|$.

o **Propriété 04 :**

-- On a : $\left(\forall(a,b)\in(\mathbb{Z}^*)^2\right);a\wedge b=|b|\Leftrightarrow b \text{ divise } a$.

En particulier : $\left(\forall(a,b)\in(\mathbb{N}^*)^2\right);a\wedge b=b\Leftrightarrow b \text{ divise } a$.

-- On a : $\left(\forall(a,b,c)\in(\mathbb{Z}^*)^3\right);a\wedge b=b\wedge(a-bc)$.

✓ **Preuve :**

Soit $(a,b)\in(\mathbb{Z}^*)^2$. Montrons que : $a\wedge b=|b|\Leftrightarrow b \text{ divise } a$.

Si b divise a, alors tout diviseur de b est un diviseur de a. Donc : $D_b\subset D_a$.

Et comme : $D_b\subset D_a\Rightarrow D_a\cap D_b=D_b$ alors : $a\wedge b=|b|$.

Réciproquement :

Si $a\wedge b=|b|$, alors $|b|$ divise a.

Et comme b divise $|b|$ alors par transitivité b divise a.

Soit $(a,b,c)\in(\mathbb{Z}^*)^3$. Pour montrer que : $a\wedge b=b\wedge(a-bc)$, il suffit de montrer que :

$D_a\cap D_b=D_b\cap D_{(a-bc)}$ (en montrant une double inclusion).

o **Exercice 07:**

Pour tout $n\in\mathbb{N}$; on pose : $a_n=n^3-2n+5$ et $b_n=n+1$.

1. Montrer que : $(\forall n\in\mathbb{N});a_n\wedge b_n=b_n\wedge 6$. Quels sont les valeurs possibles du $a_n\wedge b_n$?
2. Déterminer toutes les valeurs de n pour lesquels : $\frac{a_n}{b_n}\in\mathbb{N}$.
3. Déterminer toutes les valeurs de n pour lesquels : $a_n\wedge b_n=6$.
4. Déterminer toutes les valeurs de n pour que : $a_n\wedge b_n=3$ (respectivement $a_n\wedge b_n=2$).
5. En déduire toutes les valeurs de n pour lesquels : $a_n\wedge b_n=1$.

✓ **Correction :**

o **Définition :**

On dit que deux entiers a et b sont premiers entre eux si et seulement si : $a\wedge b=1$.

✓ **Exemple :**

On a : $8\wedge 15=1$, donc **8** et **15** sont premiers entre eux.

✓ **Remarque :**

Il ne faut pas confondre des nombres premiers entre eux et des nombres premiers .

En effet : **8** et **15** ne sont pas premiers et pourtant ils sont premiers entre eux.

o **Propriété 05 :**

Soit $(a,b)\in\mathbb{N}^2$. Si a et b sont premiers et distincts , alors ils sont premiers entre eux.

✓ **Preuve :**

Posons $d=a\wedge b$.

On a : d divise a et a est premier , donc : $d=a$ ou $d=1$.

Si $d=a$, alors a serait un diviseur de b : ce qui est impossible car b est premier et $b\neq a$.

Donc nécessairement $d=1$. Par suite a et b sont premiers entre eux.

- **Exercice 07:** (les nombres de Fermat)

1. Soit $m \in \mathbb{N}^*$. Montrer que si $2^m + 1$ est premier, alors $m = 2^n$ Où $n \in \mathbb{N}$.

2. Un nombre de Fermat s'écrit sous la forme : $F_n = 2^{2^n} + 1$ Où $n \in \mathbb{N}$.

Soient m et n deux entiers naturels tels que $n < m$. Posons : $m = n + k$ Où $k \in \mathbb{N}^*$.

a)- Montrer que F_n divise $F_{n+k} - 2$.

b)- En déduire que F_n et F_{n+k} sont premiers entre eux.

c)- Enoncer le résultat démontré.

✓ Correction :

Outils : Si k est un entier naturel impair ; alors :

$$x^k + 1 = (x+1)\left(x^{k-1} + x^{k-2} + ... + x^2 + x + 1\right)$$

1. Soit $m \in \mathbb{N}^*$. Montrons que si $2^m + 1$ est premier, alors $m = 2^n$ Où $n \in \mathbb{N}$.

Supposons que $2^m + 1$ est premier Où $m \in \mathbb{N}^*$ et que m n'est pas une puissance de 2.

alors : $m = pq$ Où $p = 2^\alpha$ avec $\alpha \in \mathbb{N}$ et $q \geq 3$ un entier naturel impair.

Donc : $2^m + 1 = \left(2^p\right)^q + 1 = \left(2^p + 1\right) \times \left(2^{p(q-1)} + 2^{p(q-2)} + ... + 2^{2p} + 2^p + 1\right)$

Cela signifie que $2^m + 1$ n'est pas premier (car il s'écrit comme produit de deux entiers tous les deux plus grand que 2) ce qui est impossible.

2. a)- Montrons que F_n divise $F_{n+k} - 2$.

Outils : $\boxed{(a,b) \in \left(\mathbb{Z}^*\right)^2 \text{ et } q \in \mathbb{N} ; \text{ alors } a - b \text{ divise } a^q - b^q.}$

On a : $F_{n+k} - 2 = 2^{2^{n+k}} - 1 = \left(2^{2^n}\right)^{2^k} - (-1)^{2^k}$

En appliquant le résultat précédent pour $a = 2^{2^n}$, $b = -1$ et $q = 2^k$: On obtient F_n divise $F_{n+k} - 2$.

b)- Posons : $d = F_n \wedge F_{n+k}$, On a : $\left(d / F_n \text{ et } F_n / F_{n+k} - 2\right) \Rightarrow d / F_{n+k} - 2$

Et comme d / F_{n+k} alors : $d / F_{n+k} - \left(F_{n+k} - 2\right)$. C'est à dire que : $d / 2$.

Les nombres de Fermat étant impairs, donc d est un diviseur impair de 2.

D'où $d = 1$ et par suite : $F_n \wedge F_{n+k} = 1$.

c)- Le résultat démontré est le suivant :

- **Propriété :**

$\boxed{\text{Deux nombres de Fermat distincts sont premiers entre eux.}}$

2)- **Algorithme d'Euclide :**

Soit $(a,b) \in \left(\mathbb{N}^*\right)^2$ tels que $b < a$ et b ne divise pas a.

La suite des divisions euclidiennes suivantes finit par s'arrêter. Le dernier reste non nul est alors le plus grand commun diviseur de a et b :

a Par b	$a = b.q_0 + r_0$	Où $0 < r_0 < b$	Donc : $a \wedge b = b \wedge r_0$
b Par r_0	$b = r_0.q_1 + r_1$	Où $0 \leq r_1 < r_0$	Donc : $b \wedge r_0 = r_0 \wedge r_1$
r_0 Par r_1	$r_0 = r_1.q_2 + r_2$	Où $0 \leq r_2 < r_1$	Donc : $r_0 \wedge r_1 = r_1 \wedge r_2$
.	.	.	.
.	.	.	.
.	.	.	.
r_{n-2} Par r_{n-1}	$r_{n-2} = r_{n-1}.q_n + r_n$	Où $0 \leq r_n < r_{n-1}$	Donc : $r_{n-2} \wedge r_{n-1} = r_{n-1} \wedge r_n$
r_{n-1} Par r_n	$r_{n-1} = r_n.q_{n+1} + r_{n+1}$	Où $r_{n+1} = 0$	Donc : $r_{n-1} \wedge r_n = r_n \wedge 0 = r_n$

D'ou : $a \wedge b = r_n$ Où r_n est le dernier reste non nul dans les divisions successives.

✓ **Exemple :**

Déterminons $4539 \wedge 1958$ en utilisant l'algorithme d'Euclide.

Le tableau suivant résume la méthode des divisions successives :

Le quotient	2	3	7
$a = 4539$	$b = 1958$	623	89
623	89	0	Le reste

D'ou : $4539 \wedge 1958 = 89$.

- **Remarque :**

On a : $\begin{aligned} & a = 2.b + 623 \Rightarrow 623 = a - 2b \\ & b = 3 \times 623 + 89 \Rightarrow 89 = b - 3(a - 2b) \Rightarrow 89 = -3a - 6b \end{aligned}$, donc : $a \wedge b = -3a - 6b$

Ainsi, en plus de la détermination du plus grand commun diviseur l'algorithme d'Euclide nous permet de déterminer un couple $(u,v) \in \mathbb{Z}^2$ tels que : $a \wedge b = au + bv$.

- **Exercice 08:**

On considère les entiers naturels : $a = 257$ et $b = 45$.

1. Déterminer en utilisant l'algorithme d'Euclide $d = a \wedge b$.

2. Déterminer un couple $(u,v) \in \mathbb{Z}^2$ tels que : $d = 257u + 45v$.

✓ **Conséquences de l'algorithme d'Euclide :**

-- On a : $\left(\forall (a,b,c) \in \left(\mathbb{Z}^*\right)^3\right) ; (ab) \wedge (ac) = |a|.(b \wedge c)$.

Et en particulier, si $(a,b,c) \in \left(\mathbb{N}^*\right)^3$ alors : $(ab) \wedge (ac) = a.(b \wedge c)$.

✓ *A retenir :*

Soit $(a,b)\in(\mathbb{Z}^*)^2$. $\boxed{\text{Si } d=a\wedge b, \text{ alors : } \begin{cases} a=dx \\ b=dy \end{cases} \text{ Où } (x,y)\in(\mathbb{Z}^*)^2 \text{ et } x\wedge y=1}$.

3)- Théorèmes de Bézout et Gauss :

Propriété 06 :

Soit $(a,b)\in(\mathbb{Z}^*)^2$. Si $d=a\wedge b$, alors $(\exists(u,v)\in\mathbb{Z}^2);d=au+bv$.

✓ *Preuve :*

Soit G l'ensemble des entiers naturels non nuls de la forme $am+bn$ Où $(m,n)\in\mathbb{Z}^2$.

Il est évident que $G\neq\varnothing$, car $|a|\in G$: $|a|=\pm1\times a+0\times b$.

Soit δ le plus petit élément de G. Nous allons montrer que $\delta=d$.

On a : $\delta=au+bv$ Où $(u,v)\in\mathbb{Z}^2$. Car $\delta\in G$.

Comme $d=a\wedge b$, alors d divise à la fois a et b. Donc d divise $\delta=au+bv$.

D'ou : $d\leq\delta$ (1).

Montrons maintenant que δ divise à la fois a et b.

En effectuant la division euclidienne de a par δ, on obtient : $\begin{cases} a=\delta q+r \\ 0\leq r<\delta \end{cases}$.

Or : $\delta=au+bv$, Donc $\begin{cases} r=a(1-uq)+b(-vq) \\ 0\leq r<\delta \end{cases}$.

Ceci implique $r=0$, car sinon r serait un élément de G strictement plus petit que δ ce qui est impossible .

On a : $r=0\Rightarrow a=\delta q$, donc δ divise a.

On procède de la même manière pour montrer que δ divise aussi b.

δ est un diviseur commun de a et b. Donc $\delta\leq d$ (2).

D'après (1) et (2) on déduit que $\delta=d$. Par suite $d=au+bv$ Où $(u,v)\in\mathbb{Z}^2$.

✓ *Conséquences :*

- Tout diviseur commun à a et b est un diviseur de leur pgcd .

Théorème de Bézout :

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

Théorème de Gauss :

Soient $(a,b,c)\in(\mathbb{Z}^*)^3$, On a : $\boxed{\begin{cases} a/bc \\ a\wedge b=1 \end{cases}\Rightarrow a/c}$.

✓ *Preuve du théorème de Gauss :*

Si a divise le produit bc, alors il existe un entier k tel que : $bc=ka$

Si a et b sont premiers entre eux, d'après le théorème de Bézout, il existe deux entiers u et v tels que : $au+bv=1$

En multipliant par c, on a :

$$\begin{aligned} acu+bcv&=c \quad \text{or } bc=ka, \text{ donc :} \\ acu+kav&=c \\ a(cu+kv)&=c \end{aligned}$$

Donc a divise c.

Exercice 09:

Montrer que l'ensemble des solutions de l'équation : $(E):5(x-1)=7y$ dans $\mathbb{Z}^2$ est :

$S=\{(7k+1,5k)/k\in\mathbb{Z}\}$.

Exercice 10:

Dans le plan muni d'un repère orthonormé , on considère un point $A(a,b)$ tels que :

$(a,b)\in(\mathbb{Z}^*)^2$ et $a\wedge b=1$. Soit $M(x,y)$ un point du segment $[OA]$ distinct de O et A.

✓ Montrer que les cordonnés de M ne peuvent pas être à la fois des entiers relatifs .

On pourra raisonner par l'absurde et appliquer le théorème de Gauss .

Corollaire :

Soient $(a,b,c)\in(\mathbb{Z}^*)^3$, On a : $\boxed{\begin{cases} b/a \\ c/a \\ b\wedge c=1 \end{cases}\Rightarrow bc/a}$.

Démonstration : : Si b et c divise a, alors il existe k et k' entiers relatifs tels que :

$$a=kb \quad \text{et} \quad a=k'c \quad \text{donc :} \quad kb=k'c$$

b divise $k'c$, or $\text{pgcd}(b,c)=1$ donc d'après le théorème de Gauss b divise k' donc : $k'=k''b$

$$a=k'c=k''bc$$

Donc bc divise a.

Exercice 11:

1. Montrer qu'un entier naturel est divisible par 12 Si et seulement s'il est divisible à la fois par 3 et 4 .

2. Déterminer les chiffres x et y pour que le nombre $N=\overline{26x95y}_{(10)}$ soit divisible par 12 .

4)- Plus petit commun multiple :

Définition :

Si $(a,b)\in(\mathbb{Z}^*)^2$, *alors* $|a.b|$ *est un multiple commun strictement positif de a et b .*
Le plus petit commun multiple de a et b est le plus petit multiple commun strictement positif de a et b . On le note : $a\vee b$, $M(a,b)$ *ou* $ppcm(a,b)$.

En particulier : $(\forall a\in\mathbb{Z}^*);a\vee a=a\vee 1=|a|$.

En plus , $\forall(a,b)\in(\mathbb{Z}^*)^2$ On a : $a\vee b=|a|\vee|b|$ *et* $a\vee b=|a|\Leftrightarrow b$ divise a .

Propriété 07 :

-- $\forall(a,b)\in(\mathbb{N}^*)^2$ On a : $\boxed{(a\wedge b).(a\vee b)=a.b \text{ et } a\wedge b=1\Rightarrow a\vee b=ab}$.

✓ **Preuve :** *Montrons que :* $\left(\forall(a,b)\in(\mathbb{N}^*)^2\right);(a\vee b)\times(a\wedge b)=ab$.

On pose : $d=a\wedge b$ *donc* $\begin{cases}a=d\alpha\\ b=d\beta\end{cases}$ *Où* $(\alpha,\beta)\in(\mathbb{N}^*)^2$ et $\alpha\wedge\beta=1$.

Montrons que : $a\vee b=d.\alpha\beta$.
Comme : $d.\alpha\beta=a\beta=b\alpha$ *alors est un multiple commun à a et b . Montrons qu'il est le plus petit multiple de a et b .*
Soit $k\in\mathbb{N}^*$ *un multiple commun à a et b . Montrons que* $k\le d.\alpha\beta$.

Il existe $(x,y)\in(\mathbb{N}^*)^2$ *tels que :* $k=ax=by$.

On a : $ax=by\Leftrightarrow\alpha x=\beta y$ *et* $\begin{cases}\alpha/\beta y\\ \alpha\wedge\beta=1\end{cases}$ *comme alors d'après le théorème de Gauss*

α/y . *Par suite :* $y=k'\alpha$ *Où* α/y *et donc :* $k=k'b\alpha=k'(d\alpha\beta)$.
D'ou : $k/d\alpha\beta$ *et par conséquent :* $k\le d\alpha\beta$. *La preuve est donc achevée .*
En conclusion : $a\vee b=d.\alpha\beta$ *et par suite :* $(a\vee b)\times(a\vee b)=d^2.\alpha\beta=a.b$.

✓ **Conséquences :**

- $\forall(a,b)\in(\mathbb{Z}^*)^2$ On a : $\boxed{(a\wedge b).(a\vee b)=|a.b| \text{ et } a\wedge b=1\Rightarrow a\vee b=|ab|}$.
- *Si* $k\in\mathbb{Z}^*$ *est un diviseur commun à a et b, alors :* $\left(\dfrac{a}{k}\right)\wedge\left(\dfrac{b}{k}\right)=\dfrac{a\wedge b}{|k|}$.
- $\forall(a,b,c)\in(\mathbb{Z}^*)^3$ On a : $(ab)\vee(ac)=|a|(b\vee c)$.

Exercice 12:

✓ *Résoudre dans* $(\mathbb{N}^*)^2$, *l'équation :* $(E):(x\wedge y)+(x\vee y)=y+9$.

V- Décomposition en facteurs premiers :

Théorème :(fondamentale de l'arithmétique)

-- *Tout entier naturel* $n\ge 2$, *se décompose de façon unique sous la forme :*
$n=p_1^{\alpha_1}\times p_2^{\alpha_2}\times\ldots\times p_m^{\alpha_m}$ *Où* $p_1<p_2<\ldots<p_m$ *sont les diviseurs premiers de* n

et $(\alpha_1,\alpha_2,\ldots,\alpha_m)\in(\mathbb{N}^*)^m$.

✓ **Exemple :**

Décomposons **16 758** *en produit de facteur premier .*
Pour décomposer un entier, on effectue des divisions successives par des nombres premiers dans l'ordre croissant .
On a donc : $16\ 578=2\times3^2\times7^2\times19$.

16 758	2
8 379	3
2 793	3
931	7
133	7
19	19
1	

Propriété 08 :

Soit $(a,b)\in(\mathbb{N}^*)^2$.
Le plus grand commun diviseur de a et b est égal au produit des facteurs communs dans leurs décompositions élevés à la plus petite puissance .
Le plus petit commun multiple de a et b est égale au produit des facteurs communs et non communs élevés à la plus grande puissance .

✓ **Exemple :**

Soit à calculer $126\wedge735$ *et* $126\vee735$.
Décomposons les deux nombres : $126=2\times3^2\times7$ *et* $126=3\times5\times7^2$
Donc : $126\wedge735=3\times7=21$ *et* $126\vee735=2\times3^2\times5\times7^2=4410$.

126	2
63	3
21	3
7	7
1	

735	3
245	5
49	7
7	7
1	

Propriété 09 :

-- *Un entier naturel d est un diviseur de* $n=p_1^{\alpha_1}\times p_2^{\alpha_2}\times\ldots\times p_m^{\alpha_m}$ *si et seulement si :*
$d=p_1^{\beta_1}\times p_2^{\beta_2}\times\ldots\times p_m^{\beta_m}$ *Où* $(\forall k\in\{1;2;\ldots;m\});0\le\beta_k\le\alpha_k$.

-- *Un entier naturel M est un multiple de* $n=p_1^{\alpha_1}\times p_2^{\alpha_2}\times\ldots\times p_m^{\alpha_m}$ *si et seulement si :*
$M=p_1^{\beta_1}\times p_2^{\beta_2}\times\ldots\times p_m^{\beta_m}\times p_{m+1}^{\beta_{m+1}}\times\ldots\times p_r^{\beta_r}$ *Où* $(\forall k\in\{1;2;\ldots;m\});\beta_k\ge\alpha_k$.

✓ **Conséquence :**

D'après le principe du produit le nombre de diviseurs de $n=p_1^{\alpha_1}\times p_2^{\alpha_2}\times\ldots\times p_m^{\alpha_m}$ *est :*
$N=(1+\alpha_1).(1+\alpha_2)\ldots(1+\alpha_m)$.

Exercice 12:

1. *Trouver le nombre de diviseurs de* **120** *puis déterminer tous ces diviseurs .*
2. *Un entier naturel* n *a* **15** *diviseurs . On sait de plus que* n *est divisible par* **6** *mais pas par* **8** *. Déterminer cet entier* n .
3. *Quel est le plus petit entier naturel possédant* **28** *diviseurs ?*

VI- Congruence :

1)- Entiers congru modulo n :

Définition :

Soient $n\in\mathbb{N}^*-\{1\}$ *et* $(a,b)\in\mathbb{Z}^2$.

On dit que a est congru à b modulo n et on écrit $a\equiv b[n]$ *si et seulement si : n est un diviseur de* $a-b$ *C'est à dire :* $(\exists k\in\mathbb{Z});a-b=k\times n$.

En particulier : $a\equiv 0[n]$ *signifie que a est divisible par n.*

Et $a\equiv b[2]$ *Signifie que les entiers a et b ont la même parité .*

Remarque :

Pour tout $(a,b,c)\in\mathbb{Z}^3$, *On a :*

1. $a\equiv a[n]$ *(La congruence est réflexive)*
2. $a\equiv b[n]\Rightarrow b\equiv a[n]$ *(La congruence est symétrique)*
3. $(a\equiv b[n]\text{ et } b\equiv c[n])\Rightarrow a\equiv c[n]$ *(La congruence est transitive)*

Ces trois propriétés exprime que la congruence est une relation d'équivalence dans $\mathbb{Z}$.

Propriété 10 :(Compatibilité avec l'addition et la multiplication)

Si $(a,b,c,d)\in\mathbb{Z}^4$ *tels que :* $a\equiv b[n]$ *et* $c\equiv d[n]$, *alors :*

-- $a+c\equiv b+d[n]$ *(Compatibilité avec l'addition)*

-- $a.c\equiv b.d[n]$ *(Compatibilité avec la multiplication)*

-- $(\forall k\in\mathbb{N});a^k\equiv b^k[n]$ *(Compatibilité avec la puissance)*

✓ **Preuve :**

-- *On sait que :* $a\equiv b[n]$ *et* $c\equiv d[n]$. *Donc* $\exists(k,k')\in\mathbb{Z}^2$ *tels que :* $\begin{cases}a-b=k.n\\ c-d=k'.n\end{cases}$

En sommant n on obtient : $(a+c)-(b+d)=(k+k')n$ *; d'ou* $a+c\equiv b+d[n]$.

D'autre part : $ac-bd=(a-b)c+b(c-d)=(kc+k'b).n$ *; donc* $a.c\equiv b.d[n]$.

-- *Maintenant si :* $a\equiv b[n]$ *, alors : n divise* $a-b$

Et comme $a-b$ *divise* a^k-b^k *pour tout* $k\in\mathbb{N}$*; alors par transitivité n divise* a^k-b^k .

Par conséquent : $(\forall k\in\mathbb{N});a^k\equiv b^k[n]$.

Propriété 11 :

Si $(a,b)\in\mathbb{Z}^2$, *alors* $a\equiv b[n]$ *si et seulement si la division euclidienne de a et b par n donne le même reste .*

✓ **Preuve :**

Supposons que : $a\equiv b[n]$ *; donc* $(\exists k\in\mathbb{Z});a-b=k\times n$.

Si $a=qn+r$ *Où* $0\le r\le n-1$, *alors* $b=a-k\times n=(q-k)n+r$

Par suite la division euclidienne de a et b par n donne le même reste .

Réciproquement : si $a=qn+r$ *et* $b=q'n+r$ *Où* $0\le r\le n-1$ *. Alors :*

$a-b=(q-q')n$ *; donc :* $a\equiv b[n]$ *. CQFD*

✓ **Conséquence :**

- *Si* $a\equiv b[n]$ *alors :* $a\equiv 0[n]\Leftrightarrow b\equiv 0[n]$.

Cela veut dire que si a est congru à b modulo n, alors a est divisible par n si et seulement si b est divisible par n (Ce résultat est à retenir).

Propriété 12 :

Si $n\in\mathbb{N}^*-\{1\}$, *alors pour tout* $a\in\mathbb{Z}$ *il existe un unique* $r\in\{0;1;2;...;n-1\}$ *tels que :* $a\equiv r[n]$ *. (r est le reste de la division euclidienne de a par n).*

Exercice 13:

1. *Déterminer le reste de la division euclidienne de* $a=5^{100}+100^{100}$ *par 7.*
2. *Déterminer toutes les valeurs de l'entier naturel n pour lesquels :* $2^n\equiv 1[9]$.
3. **a)**- *Recopier et compléter cette table de congruence modulo 4 :*

$x\equiv...[4]$	0	1	2	3
$x^2\equiv...[4]$				

b)- *En déduire que l'équation :* $(E):7x^2-4y^2=1$ *n'a pas de solutions dans* $\mathbb{Z}^2$.

c)- *Résoudre dans* $\mathbb{Z}$ *l'équation :* $(F):(x+3)^2\equiv 1[4]$.

Exercice 14:

1. *Déterminer suivant les valeurs de* $n\in\mathbb{N}$ *le reste de la division euclidienne de* 2^n *par 5 .*
2. *En déduire le reste de la division euclidienne de l'entier* $a=2^{2048}$ *par 5 .*
3. *Soit* $x\in\mathbb{N}$ *tels que :* $x\equiv 2[5]$.

✓ *Montrer que l'entier* $b=1+x+x^2+x^3+...+x^{2047}$ *est divisible par 5.*

Exercice 15:

1. *Montrer que pour tout* $x\in\mathbb{N}$, *On a :* $3x\equiv 8[10]\Leftrightarrow x\equiv 6[10]$

Et que : $x^2\equiv 6[10]\Leftrightarrow(x\equiv 4[10]\text{ ou } x\equiv 6[10])$.

2. *On pose :* $N=n^2+(n+1)^2+(n+2)^2$ *Où* $n\in\mathbb{N}$.

a)- *Montrer que :* $N\equiv 0[10]\Leftrightarrow(n\equiv 3[10]\text{ ou } n\equiv 5[10])$.

b)- *En déduire tous les multiples de* **10** *, plus petit que* **5 000** *et qui s'écrivent comme somme de trois carrés parfaits consécutifs .*

2)- Critères de divisibilité :

- Introduction :

Notre système de numération est un système décimal : il est constitué de **10** chiffres dont la position indique le nombres d'unités de la puissance de **10** correspondante .

Par exemple : $4752 = 4\times10^3 + 7\times10^2 + 5\times10^1 + 2\times10^0$.

Donc en résumé tout entier naturel N s'écrit dans le système décimal sous la forme :

$N = a_m\times10^m + a_{m-1}\times10^{m-1} + \ldots + a_2\times10^2 + a_1\times10 + a_0$

Où $(\forall k\in\{0;1;2;\ldots;m\});0\le a_k\le 9$ et $a_m\ne 0$. On écrit : $N=\overline{a_m a_{m-1}\ldots a_2 a_1 a_0}_{\ (10)}$.

Propriété 13 :

-- L'entier naturel N est divisible par **3** (respectivement par **9**) si et seulement si la somme de ses chiffres $C=\sum_{k=0}^{m} a_k$ est divisible par **3** (respectivement par **9**) .

-- L'entier naturel N est divisible par **2** (respectivement par **5**) si et seulement si :
$a_0\in\{0;2;4;6;8\}$ (respectivement $a_0\in\{0;5\}$).

-- L'entier naturel N est divisible par **4** (respectivement par **25**) si et seulement si :
$a_1\times10+a_0$ est divisible par **4** (respectivement $a_1\times10+a_0\in\{00;25;50;75\}$).

-- N est divisible par **11** si et seulement si : $a_0-a_1+a_2-a_3+\ldots+(-1)^m.a_m$ est divisible par **11** .

✓ Preuve :

Outils : $\boxed{\text{Si } a\equiv b[n] \text{ et si } d \text{ est un diviseur positif de } n\text{, alors : } a\equiv b[d]}$.

-- On a :

$10\equiv1[9]\Rightarrow(\forall k\in\mathbb{N});10^k\equiv1[9]$

$\Rightarrow N\equiv\sum_{k=0}^{m} a_k[9]$; donc $N\equiv0[9]\Leftrightarrow\sum_{k=0}^{m} a_k\equiv0[9]$.

D'autre part : **3** est un diviseur positif de **9** ; donc : $N\equiv\sum_{k=0}^{m} a_k[9]\Rightarrow N\equiv\sum_{k=0}^{m} a_k[3]$.

Par suite : $N\equiv0[3]\Leftrightarrow\sum_{k=0}^{m} a_k\equiv0[3]$.

-- On a : $N=a_0+10\times\sum_{k=1}^{m} a_k\times10^{k-1}\Rightarrow N\equiv a_0[10]$, donc : $N\equiv0[10]\Leftrightarrow a_0=0$.

D'autre part : **2** et **5** sont des diviseurs positifs de **10** ; donc : $N\equiv a_0[2]$ et $N\equiv a_0[5]$.

Par suite : $N\equiv0[2]\Leftrightarrow a_0\in\{0;2;4;6;8\}$ et $N\equiv0[5]\Leftrightarrow a_0\in\{0;5\}$.

-- On a : $N=a_0+a_1\times10+100\times\sum_{k=2}^{m} a_k\times10^{k-2}\Rightarrow N\equiv a_0+a_1\times10[100]$.

Donc : $N\equiv0[100]\Leftrightarrow a_0=a_1=0$.

D'autre part : **4** et **25** sont des diviseurs positifs de **100** .

Donc : $N\equiv a_0+a_1\times10[4]$ et $N\equiv a_0+a_1\times10[25]$. Par suite :

$N\equiv0[4]\Leftrightarrow a_0+a_1\times10\equiv0[4]$ et $N\equiv0[25]\Leftrightarrow a_0+a_1\times10\in\{00;25;50;75\}$.

-- On a :

$10\equiv-1[11]\Rightarrow(\forall k\in\mathbb{N});10^k\equiv(-1)^k[11]$

$\Rightarrow N\equiv\sum_{k=0}^{m}(-1)^k.a_k[11]$; donc $N\equiv0[11]\Leftrightarrow\sum_{k=0}^{m}(-1)^k.a_k\equiv0[11]$.

Exercice 16:

1. Déterminer les chiffres x et y pour que l'entier naturel $N_1=\overline{26x95y}$ soit divisible par **3** et **11** .

2. Déterminer les chiffres a et b pour que l'entier naturel $N_2=\overline{aba7}$ soit divisible par **7** .

Exercice 17:

On pose : $a=\sum_{k=0}^{9}(2011)^k$ et $N=\sum_{k=0}^{2009}(2011)^k$.

1. Montrer que : $a\equiv60[100]$. Puis en déduire que a^n est divisible par **100** pour tout $n\in\mathbb{N}^*-\{1\}$.

2. Montrer que : $N\equiv201a[100]$. Puis en déduire le chiffres des unités et des dizaines de N .

Exercice 18:

1. a)- Résoudre dans $\mathbb{Z}$, l'équation : $(E):3x\equiv23[7]$.

b)- En déduire l'ensemble des solutions de l'équation $(F):3x-7y=23$ dans $\mathbb{Z}^2$.

2. Résoudre dans $\mathbb{Z}^2$, le système $(S):\begin{cases}3x-7y=23\\ x\wedge y=23\end{cases}$.

Complément sur les nombres de Fermat :

Exercice 19:

1. Montrer que : $(\forall n\in\mathbb{N});F_{n+1}=(F_n-1)^2+1$.

2. Calculer F_2; F_3 et F_4. Que constatez-vous ?

3. Déterminer le chiffre des unités de F_n pour tout $n\in\mathbb{N}^*-\{1\}$.

Fin Du Sujet .