

L'ARITHMETIQUE

I) LA DIVISIBILITE DANS \mathbb{Z}

1) Définition et conséquences

1.1 Diviseur d'un entier

Définition : Soient a et b deux entiers relatifs tels que $b \neq 0$; on dit que l'entier relatif b divise a s'il existe un entier relatif k tel que $a = kb$;

On écrit : $b|a$.

On dit que a est divisible par b

Exemples : $3|12$ car $12=3 \times 4$ et $-6|42$

car $-42=7 \times (-6)$ et on a : 7 ne divise pas 16

Remarques :

- Si l'entier non nul b divise l'entier a alors $-b$ divise lui aussi.
- 1 divise tous les entiers relatifs
- 0 est divisible par tous les entiers non nuls : car $0 = 0 \times b$
- Si a est un entier les diviseurs de a constituent un ensemble fini noté D_a :

$$D_a = \{b \in \mathbb{Z} / b|a\}$$

Exemple :

$$D_{18} = \{-18, -9, -6, -3, -2, -1, 1, 2, 3, 6, 9, 18\}$$

$$\text{et } D_{18}^+ = \{1, 2, 3, 6, 9, 18\}$$

Exercice01 : 1) Déterminer et dénombrer les diviseurs naturels de 156

2) Déterminer dans \mathbb{Z} tous les diviseurs de -8

Solution01 : 1) 156 a 12 diviseurs :

1; 2; 3; 4; 6; 12; 13; 26; 39; 52; 78 et 156.

156 et 1 sont appelés diviseurs triviaux, les autres sont des diviseurs stricts.

2) $D_{-8} = \{-8, -4, -2, -1, 1, 2, 4, 8\}$

Propriété : $a \in \mathbb{Z}$; $b \in \mathbb{Z}$; $c \in \mathbb{Z}$

- $1/a$ et $-1/a$ et a/a et $a/-a$
- $b|a \Rightarrow |b| \leq |a|$
- $a/b \Rightarrow a/b \times c$
- $a/b \Rightarrow |a| \leq |b|$
- $b|1 \Rightarrow b \in \{-1, 1\}$

Déduction :

Si m et n sont deux entiers relatifs tels que : $mn = 1$ alors $|m| = 1$ et $|n| = 1$.

1.2 Multiple d'un entier.

Définition : On dit que a est un multiple de b si b est un diviseur de a

Remarque : Si b est un entier non nul, les multiples de b constituent Un ensemble infini noté $b\mathbb{Z}$

$$b\mathbb{Z} = \{m \in \mathbb{Z} / m = kb \text{ où } k \in \mathbb{Z}\}$$

Exemple :

$$3\mathbb{Z} = \{\leftarrow \dots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \dots \rightarrow\}$$

1.3 Diviseur commun, multiple commun de deux entiers

Définition : a) Si $b|m$ et $b|n$ on dit que b est un diviseur commun de m et n

b) Si $b|m$ et $b'|m$, on dit que m est un multiple commun de b et b' .

Exemples : 4 est un diviseur commun de 16 et 12

36 est un multiple commun de 9 et 12.

Propriété : Etant donnés des entiers relatifs non nuls. On a les propositions suivantes :

- $a|b$ et $b|a \Rightarrow |a| = |b|$
- $a|b$ et $c|d \Rightarrow ac|bd$
- $a|b$ et $b|c \Rightarrow a|c$
- $a|b \Rightarrow a|bc$
- $a|m$ et $a|n \Rightarrow a|m + n$
- $a|m$ et $a|n \Rightarrow a|m - n$
- $a|m$ et $a|n \Rightarrow a|\alpha m + \beta n$ où α et β sont des entiers relatifs quelconques.

$$\bullet a/b \Rightarrow a^n / b^n \quad n \in \mathbb{N}$$

Exercice02 :

1) $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ et $c \in \mathbb{Z}$ et $x \in \mathbb{Z}$ et $y \in \mathbb{Z}$

a) montrer que si $a/2b+c$ et $a/b+c$ alors a/c

b) montrer que si $a/2b+3c$ et $a/b+c$ alors a/c

c) montrer que si $a/x-y$ et $a/b-c$ alors $a/xb-cy$

2) $a \in \mathbb{Z}$ et $n \in \mathbb{N}$ et $a/12n+1$ et $a/-2n+3$

Montrer que $a/19$

3) $d \in \mathbb{Z}$ et $a \in \mathbb{Z}$ et d/n^2+3 et $d/2n-1$

Montrer que $d/13$

Solution02 : 1) a) $\left\{ \begin{array}{l} a/2b+c \\ a/b+c \end{array} \right\} \Rightarrow a/2(b+c) - (2b+c) \Rightarrow a/c$

$$1) b) \begin{cases} \frac{a}{2b+3c} \Rightarrow \frac{a}{2b+3c-2(b+c)} \Rightarrow \frac{a}{c} \\ \frac{a}{b+c} \end{cases}$$

$$1) c) \begin{cases} \frac{a}{x-y} \Rightarrow \frac{a}{bx-by} \text{ et } \frac{a}{by-cy} \Rightarrow \frac{a}{bx-cy} \\ \frac{a}{b-c} \end{cases}$$

$$2) \frac{a}{12n+1} \text{ et } \frac{a}{-2n+3} \\ \Rightarrow \frac{a}{12n+1} \text{ et } \frac{a}{-12n+18} \Rightarrow \frac{a}{19} \\ \Rightarrow a \in \{\pm 1; \pm 19\}$$

$$3) d \in \mathbb{Z} \text{ et } a \in \mathbb{Z} \text{ et } \frac{d}{n^2+3} \text{ et } \frac{d}{2n-1} \\ \Rightarrow \frac{d}{n^2+3} \text{ et } \frac{d}{(2n-1)^2} \Rightarrow \frac{d}{4n^2+12} \text{ et } \frac{d}{4n^2-4n+1} \\ \Rightarrow \frac{d}{11+4n} \text{ et } \frac{d}{-2+4n} \Rightarrow \frac{d}{13}$$

Exercice03 : $a \in \mathbb{Z}$ et $x \in \mathbb{Z}$

Montrer que : $\begin{cases} \frac{a}{5x-7} \Rightarrow \frac{a}{29} \\ \frac{a}{2x+3} \end{cases}$

Solution03 : $\begin{cases} \frac{a}{5x-7} \Rightarrow \frac{a}{2(5x-7)-5(2x+3)} \\ \frac{a}{2x+3} \end{cases}$

$$\frac{a}{10x-14-10x-15} \Rightarrow \frac{a}{-29} \Rightarrow \frac{a}{29}$$

Exercice04 : Montrer que : $\forall n \in \mathbb{N} : 3$

divise $4^n - 1$ **Solution04 :**

Montrons que : $\forall n \in \mathbb{N} \exists k \in \mathbb{N} / 4^n - 1 = 3k$
1 étapes : l'initialisation : Pour $n=0$ nous avons
 $4^0 - 1 = 0$ est un multiple de 3

Donc P (0) est vraie.

2 étapes : d'hérédité : Supposons que P(n) soit vraie c'est-à-dire : $\exists k \in \mathbb{N} / 4^n - 1 = 3k$ donc
 $4^n = 3k + 1$

3 étapes : Nous allons montrer que P(n+1) est vraie. Montrons alors que :

$$\exists k' \in \mathbb{N} / 4^{n+1} - 1 = 3k' \text{ ??}$$

$$4^{n+1} - 1 = 4 \times 4^n - 1 \\ = 4 \times (3k + 1) - 1 = 12k + 4 - 1 = 12k + 3 = 3(4k + 1)$$

avec $k' = 4k + 1$ Donc P(n+1) est vraie.
Conclusion. Par le principe de récurrence on a :
 $\forall n \in \mathbb{N}; 4^n - 1$ est divisible par 9

Exercice05 : Quelles sont les valeurs de l'entier relatif n pour lesquelles : $n + 2/3n + 1$

Solution05 : $n + 2/3n + 1$ et $n + 2/n + 2$

$n + 2/3n + 1$ et $n + 2/3n + 6$ donc

$n + 2/(3n + 6) - (3n + 1)$ donc $n + 2/5$

Les diviseurs de 5 sont 1 ; -1 ; 5 ; -5 donc Il faut

que $n + 2 \in \{-1; -5; 1; 5\}$ ce qui entraine que
 $n \in \{-3; -7; -1; 3\}$

On vérifie que que que si $n \in \{-3; -7; -1; 3\}$ alors
 $n + 2/3n + 1$ avant de conclure.

Conclusion : les valeurs de l'entier relatif n pour lesquelles : $n + 2/3n + 1$ sont : -7 ; -3 ; -1 ; 3

Exercice 06 : Quelles sont les valeurs de l'entier relatif n pour lesquelles la fraction $\frac{3n+8}{n+4}$

Représente un entier relatif ?

Solution06 : Cette fraction a un sens si : $n + 4 \neq 0$ soit $n \neq -4$

On constate que $3n + 8 = 3(n + 4) - 4$

$n + 4$ divise $3(n + 4)$, donc $n + 4$ divise $3n + 8$ si
 $n + 4$ divise -4.

Les diviseurs de -4 sont 1 ; -1 ; 2 ; -2 ; 4 ; -4.

Il faut que $n + 4 \in \{-4; -2; -1; 1; 2; 4\}$ ce qui entraine que $n \in \{-8; -6; -5; -3; -2; 0\}$

On vérifie que -4 n'appartient pas à -8 ; -6 ; -5 ; -3 ; -2 ; 0 avant de conclure.

Conclusion : la fraction $\frac{3n+8}{n+4}$ représente un

entier relatif pour les valeurs de l'entier relatif n : -8 ; -6 ; -5 ; -3 ; -2 ; 0.

Exercice07 : Résoudre dans \mathbb{N}^2 les équations suivantes : a) $x^2 - y^2 = 32$ avec $x > y$

b) $2xy + 2x + y = 99$

Solution07 : a) $x^2 - y^2 = 32 \Leftrightarrow (x - y)(x + y) = 32$

$x - y$ et $x + y$ sont des diviseurs positif de 32

Et $(x - y) + (x + y) = 2x$ est un nombre pair

Donc $x - y$ et $x + y$ ont la même parité $32 = 2^5$

On dresse un tableau :

$x - y$	2	4
$x + y$	16	8
x	9	6
y	7	2

$$S = \{(6; 2); (9; 7)\}$$

b) $2xy + 2x + y = 99 \Leftrightarrow 2xy + y + 2x + 1 - 1 = 99$

$$\Leftrightarrow y(2x + 1) + 2x + 1 = 99 + 1 \Leftrightarrow (2x + 1)(y + 1) = 100$$

Donc : $2x + 1$ et $y + 1$ sont des diviseurs positif de 100

$$D_{100} = \{1; 2; 4; 5; 10; 20; 25; 50; 100\}$$

$2x + 1$	1	2	4	5	20	25	50	100
$y + 1$	100	50	25	20	5	4	2	1
x	0			2		12		
y	99			10		3		

$$S = \{(0; 99); (2; 19); (12; 3)\}$$

2) La division euclidienne

2.1 La division euclidienne dans \mathbb{N} .

Propriété : Considérons a et b deux entiers naturels tels que $b \neq 0$; ils existent deux entiers naturels q et r tels que $a = bq + r$ où $0 \leq r < b$

- L'entier a s'appelle : **Le divisé**
- L'entier b s'appelle : **Le diviseur**
- L'entier q s'appelle : **Le quotient**
- L'entier r s'appelle : **Le reste**

Remarque : Si r est le reste de la division euclidienne par b alors : $r \in \{0, 1, \dots, b - 1\}$.

Exemple1 :

la division euclidienne de 75 par 8 donne :

$$75 = 9 \times 8 + 3 \text{ car } 0 \leq 3 < 8$$

la division euclidienne de 126 par 7 donne :

$$126 = 18 \times 7 + 0 \text{ car } 0 \leq 0 < 7$$

la division euclidienne de 85 par 112

$$\text{donne : } 85 = 0 \times 112 + 85 \text{ car } 0 \leq 85 < 112$$

Exemple2 : Un entier naturel n peut s'écrire de l'une des façons suivantes

$$n = 5k \text{ ou } n = 5k + 1 \text{ ou } n = 5k + 2$$

$$\text{ou } n = 5k + 3 \text{ ou } n = 5k + 4 \text{ avec } k \in \mathbb{N}$$

Exercice 08 : déterminer le nombre entier naturel n Tel que le quotient de la division euclidienne de n par 25 est p et le reste est p^2 ($p \in \mathbb{N}$)

Solution08 : $n \in \mathbb{N} : n = 25p + p^2$ et $0 \leq p^2 < 25$
donc $0 \leq p < 5$

$$\text{Donc : } \begin{cases} p=0 \\ n=0 \end{cases} \text{ ou } \begin{cases} p=1 \\ n=26 \end{cases} \text{ ou } \begin{cases} p=2 \\ n=54 \end{cases} \text{ ou } \begin{cases} p=3 \\ n=84 \end{cases} \text{ ou } \begin{cases} p=4 \\ n=116 \end{cases}$$

$$\text{Donc : } n \in \{0; 26; 54; 84; 116\}$$

Exercice 09: n et a et b des entiers naturels
Démontrer que si q est le quotient de la division euclidienne de n par a et q' est le quotient de q par b Alors q' est aussi le quotient de n par ab

Solution09 : soit r le reste de la division euclidienne de n par a et r' le reste de la division euclidienne de q par b on a donc :
 $n = aq + r$ et $0 \leq r \leq a - 1$ et on a : $q = bq' + r'$
et $0 \leq r' \leq b - 1$ donc on déduit que :
 $n = a(bq' + r') + r = abq' + ar' + r$

Et puisque : $0 \leq r' \leq b - 1$ et $0 \leq r \leq a - 1$ alors :
 $ar' + r \leq ab - 1$ donc $n = abq' + ar' + r$
 $0 \leq ar' + r \leq ab - 1$ conclusion : q' est aussi le quotient de n par ab

2.2 La division euclidienne dans \mathbb{Z}

Propriété : Considérons a et b deux entiers relatifs tels que $b \neq 0$; ils existent un entiers relatif q et un entier naturel r

Tels que : $a = bq + r$ où $0 \leq r < |b|$

Exemple1 :1) la division euclidienne de 37 par -11 donne : $37 = (-11) \times (-3) + 4$ car $0 \leq 4 < 11$

2) la division euclidienne de -37 par 11 donne : $-37 = 11 \times (-4) + 7$ car $0 \leq 7 < 11$

3) la division euclidienne de -37 par -11 donne : $-37 = (-11) \times 4 + 7$ car $0 \leq 7 < 11$

Exercice10: $b \in \mathbb{N}^*$ et $a \in \mathbb{Z}$

si q est le quotient de la division euclidienne de $a - 1$ par b déterminer le quotient de la division euclidienne de $ab^9 - 1$ par b^{10}

Solution10 : soit r le reste de la division euclidienne de $a - 1$ par b donc :

$$a - 1 = bq + r \text{ et } 0 \leq r < b$$

$$\text{Donc : } ab^9 - b^9 = b^{10}q + rb^9$$

$$\text{Donc : } ab^9 - 1 = b^{10}q + rb^9 + b^9 - 1$$

$$\text{Donc : } ab^9 - 1 = b^{10}q + (r + 1)b^9 - 1$$

On montre que : $0 \leq (r + 1)b^9 - 1 < b^{10}$???

On a : $0 \leq r < b$ donc $0 \leq r + 1 \leq b$

donc $0 \leq (r + 1)b^9 \leq b^{10}$ donc $0 \leq (r + 1)b^9 - 1 \leq b^{10} - 1$

donc $0 \leq (r + 1)b^9 - 1 < b^{10}$

conclusion : q est aussi le quotient de la division euclidienne de $ab^9 - 1$ par b^{10}

II) LES NOMBRES PREMIERS

1) Définition et propriétés

Définitions : a) On dit que l'entier d est un diviseur **effectif** de l'entier relatif a

Si $d|a$ et $|d| \neq 1$ et $|d| \neq |a|$

b) On dit qu'un entier relatif non nul p est **premier** s'il est différent de 1 et s'il n'admet pas de diviseurs effectifs.

Remarques :

- Un nombre premier p admet exactement deux diviseurs positifs 1 et $|p|$.
- Si p est un nombre premier positif alors p n'admet pas de diviseurs effectifs de même
 - p n'admet pas de diviseurs effectif d'où :
 - $-p$ est aussi premier ;
- Pour l'étude des nombres premiers on se contente d'étudier les nombres premiers positifs.

Propriété : Soit a un entier naturel non nul différent de 1 et non premier, le plus petit

diviseur de a différent de 1 est un nombre premier

Exemple1 : Les nombres -3 et -7 et 23 sont premiers.

2) Détermination d'un nombre premier

Propriété : Soit n un entier naturel non nul, différent de 1 et non premier, il existe un nombre premier p qui divise l'entier n et qui vérifie $p^2 \leq n$.

Remarque : Cette propriété nous permet de déterminer si un nombre est premier ou non.

Corolaire : Si un entier n n'est divisible par aucun entier premier p et qui vérifie $p^2 \leq n$ alors n est premier.

Exercice: 1) Les nombres suivants sont-ils premiers : 499 ; 601 ; 703 ; 2003 ; $2n^2 + 3n$ $n \in \mathbb{N}$

Théorème : L'ensemble des nombres premiers est infini.

III) PLUS GRAND DIVISEUR COMMUN, PLUS PETIT MULTIPLE COMMUN.

1) Plus grand diviseurs commun

1.1 Définition et propriété

Définition : On dit que le nombre d est le **plus grand diviseur commun** de deux entiers relatifs a et b lorsque d divise a et d divise b et qu'il n'y a pas d'autre plus grands diviseurs de ces deux nombres.

On note $d = PGDC(a, b) = a \wedge b$

Exemple :

$-48 \wedge 36 = 12$

Propriétés : 1) $a \wedge a = |a|$ 2) $1 \wedge a = 1$

3) $(a \wedge b) \wedge c = a \wedge (b \wedge c)$

4) Si $b|a$ alors $a \wedge b = |b|$

5) si $d|a$ et $d|b$ alors $d|(a \wedge b)$

Exercice11 : montrer que $\forall a \in \mathbb{Z} \quad a \wedge (a+1) = 1$

Solution11 : on pose $d = a \wedge (a+1)$

$\Rightarrow d/a$ et $d/a+1 \Rightarrow d/1 \Rightarrow d=1$

Exercice12 : $n \in \mathbb{N}$ On considère les deux nombres : $A = n^2 + 3$ et $B = n + 2$

1) montrer que $A \wedge B = (n+2) \wedge 7$

2) déterminer l'entier naturel n tel que : $\frac{n^2+3}{n+2} \in \mathbb{N}$

Solution12 : 1) on pose $d = A \wedge B$ et $d' = (n+2) \wedge 7$

On a : $d = A \wedge B$

$\Rightarrow d/A$ et $d/B \Rightarrow d/n^2+3$ et $d/n+2$

$\Rightarrow d/n^2+3$ et $d/n+2$ on utilisant la division euclidienne : on trouve : $n^2 + 3 = (n+2)(n-2) + 7$

$n^2 + 3 - (n+2)(n-2) = 7$

$\Rightarrow d/n^2 + 3 - (n+2)(n-2)$

$\Rightarrow d/7$ et $d/n+2 \Rightarrow d/(n+2) \wedge 7 \Rightarrow d/d'$

Inversement : On a : $d' = (n+2) \wedge 7$

$\Rightarrow d'/n+2$ et $d'/7 \Rightarrow d'/(n+2)(n-2)$ et $d'/7$

$\Rightarrow d'/(n+2)(n-2)+7$ et $d'/7 \Rightarrow d'/n^2+3$ et $d'/7$

donc : $d'/A \wedge B$ donc d'/d

donc d'/d' et d'/d et $d \in \mathbb{N}$ et $d' \in \mathbb{N}$ donc

donc $d = d'$ donc : $A \wedge B = (n+2) \wedge 7$

2) $\frac{n^2+3}{n+2} \in \mathbb{N} \Leftrightarrow n+2/n^2+3$ et on a : $n+2/n+2$

Donc : $n+2/A \wedge B$ Donc : $n+2/(n+2) \wedge 7$

Donc : $n+2/7$ or 7 est premier donc :

Il faut que $n+2 \in \{1; 7\}$ ce qui entraîne que $n=5$

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

Exemple : 21 et 10 sont premiers entre eux.

Exercice 13: $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ et $c \in \mathbb{Z}$ et $d \in \mathbb{Z}$ tels que : $a = bc + d$

1) montrer que $a \wedge b = b \wedge d$

2) En déduire que : $a \wedge b = b \wedge (a - bc)$

Solution13 : 1) on pose $\Delta_1 = a \wedge b$ et $\Delta_2 = b \wedge d$

On a : Δ_1/a et Δ_1/b donc Δ_1/a et Δ_1/bc donc

$\Delta_1/a-bc$ donc Δ_1/d

donc Δ_1/d et Δ_1/b donc $\Delta_1/b \wedge d$ donc Δ_1/Δ_2

inversement On a : Δ_2/b et Δ_2/d donc Δ_2/d et

Δ_2/bc donc $\Delta_2/bc+d$ donc Δ_2/a

donc Δ_2/a et Δ_2/b donc $\Delta_2/a \wedge b$ donc Δ_2/Δ_1

On a donc : Δ_1/Δ_2 et Δ_2/Δ_1 et $\Delta_1 \in \mathbb{N}$ et $\Delta_2 \in \mathbb{N}$

donc $\Delta_1 = \Delta_2$

donc : $a \wedge b = b \wedge d$

2) on a : $a = bc + (a - bc)$ si on prend : $d = a - bc$ et d'après 1) on aura : $a \wedge b = b \wedge d = b \wedge (a - bc)$

Exercice14 : $a \in \mathbb{N}$ On considère les deux nombres : $A=35a+57$ et $B=45a+76$ montrer que $A \wedge B=1$ ou $A \wedge B=19$

Solution14 : 1) on pose $d = A \wedge B$

$$\Rightarrow d/A \text{ et } d/B \Rightarrow d/35a+57 \text{ et } d/45a+76$$

$$\Rightarrow d/9(35a+57) \text{ et } d/7(45a+76)$$

$$\Rightarrow d/315a+513 \text{ et } d/315a+532$$

$$\Rightarrow d/19 \text{ or } 19 \text{ est premier donc :}$$

Il faut que $d \in \{1;19\}$ ce qui entraîne que :

$$A \wedge B=1 \text{ ou } A \wedge B=19$$

1.2 L'algorithme d'Euclide.

Théorème : Soit a un entier naturel et b un entier naturel non nul on a : $a = bq + r$

$$\text{Où } 0 \leq r < b \text{ on a : } a \wedge b = b \wedge r$$

L'algorithme d'Euclide.

Propriété : Soient a et b deux entiers naturels non nuls. Le plus grand diviseur commun de a et b est le dernier reste non nul dans les divisions euclidiennes successives.

Application :

1- Trouver le PGDC (362154, 82350).

2- Déterminer tous les diviseurs communs de 362154 et 82350.

Propriété : Soient a et b deux entiers relatifs non nuls

Les diviseurs communs de a et b sont les diviseurs de $a \wedge b$.

$$\text{On peut dire que : } D_a \cap D_b = D_{a \wedge b}$$

Exercice : Montrer que : $\forall n \in \mathbb{N}^*$ on a :

$$1) n \wedge (n+1) = 1 \quad 2) n \wedge (2n+1) = 1$$

$$3) (2n+1) \wedge (3n+1) = 1$$

2) Le plus petit multiple commun.

Définition et propriété

Définition : On dit que le nombre entier naturel m est le **plus petit multiple commun** de deux entiers relatifs a et b lorsque m est un multiple de a et de b et qu'il n'y a pas d'autre plus petit multiple non nuls de ces deux nombres. On note : $m = PPCM(a, b) = a \vee b$

$$\text{Exemple : } -48 \wedge 36 = 144$$

Propriétés :

$$1) a \vee a = |a| \quad 2) a \vee b = b \vee a$$

$$3) a \vee 1 = |a| \quad 4) \text{ Si } b|a \text{ alors } a \vee b = |a|$$

$$5) a \vee (b \vee c) = (a \vee b) \vee c$$

$$6) a|(a \vee b) ; b|(a \vee b) \text{ et } (a \vee b)|ab$$

Propriété : Considérons a et b deux entiers relatifs. Si $a \vee b = m$ et M un multiple commun de a et b alors $m|M$.

Indications pour preuve :

Poser $M = qm + r$ on a : $a|m, a|M$ conclure.

De même pour b et si $r \neq 0$ aboutir à une contradiction.

IV) LA CONGRUENCE MODULO n

1) Définition et propriétés.

Activité : Quelle relation y a-t-il entre ces nombres $-11, 15, 67, 28, 132$ et 13 .

Définition : Soient a et b deux entiers relatifs ; et n un entier naturel non nul. On dit que : a est congrue à b modulo n si $n|(b - a)$.

On écrit : $a \equiv b [n]$

Exemples : $122 \equiv 27 [5]$ $34 \equiv 13 [7]$

Propriété : Si $a \equiv b [n]$ alors a et b ont le même reste de la division euclidienne sur n

Propriété fondamentale :

1) $(\forall a \in \mathbb{Z})(a \equiv a [n])$ on dit que la relation de congruence est réflexive.

2) $(\forall (a, b) \in \mathbb{Z}^2)(a \equiv b [n] \Leftrightarrow b \equiv a [n])$: on dit que la relation de congruence est symétrique.

3) $(\forall (a, b, c) \in \mathbb{Z}^3)$

$(a \equiv b [n] \text{ et } b \equiv c [n]) \Rightarrow a \equiv c [n]$: on dit que la relation de congruence est transitive.

Définition : Puisque la relation est de congruence est réflexive, symétrique et transitive on dit que la relation de congruence est une

relation d'équivalence

2) Compatibilité de la relation d'équivalence avec l'addition et la multiplication dans \mathbb{Z} .

Propriété et définition : Soit n un entier naturel non nul. Si $a \equiv b [n]$ et $c \equiv d [n]$ alors :

1) $a + c \equiv b + d [n]$; On dit que la relation de congruence est compatible avec l'addition dans \mathbb{Z}

2) $ac \equiv bd [n]$; On dit que la relation de congruence est compatible avec la multiplication dans \mathbb{Z}

Corolaire : Si $a \equiv b [n]$ alors pour tout k dans \mathbb{N} on a : $a^k \equiv b^k [n]$

Remarque : La réciproque du corolaire n'est pas vraie : $2^4 \equiv 3^4 [5]$ mais $2 \not\equiv 3 [5]$

Exercice15 : $a \in \mathbb{N}$ et $b \in \mathbb{N}$ Si 17 est le reste de la division euclidienne de a par 19 Et Si 15 est le reste de la division euclidienne de b par 19 Déterminer le reste de la division euclidienne des nombres suivants par 19 :

$$1) a+b \quad 2) a^2+b^2 \quad 3) 2a-5b$$

Solution15 : 1) On a : $a \equiv 17 [19]$ et $b \equiv 15 [19]$

$$\text{donc : } a+b \equiv 17+15 [19] \Leftrightarrow a+b \equiv 13 [19]$$

Par suite : le reste dans la division du nombre $a+b$ Par 19 est : 13

$$2) a \equiv 17[19] \Rightarrow a^2 \equiv 17^2[19] \Rightarrow a^2 \equiv 4[19]$$

$$b \equiv 15[19] \Rightarrow b^2 \equiv 15^2[19] \Rightarrow b^2 \equiv 16[19]$$

Donc : $a^2 + b^2 \equiv 4 + 16[19] \Leftrightarrow a^2 + b^2 \equiv 1[19]$
 Par suite : le reste dans la division du nombre $a^2 + b^2$ Par 19 est : 1

$$3) a \equiv 17[19] \Rightarrow 2a \equiv 2 \times 17[19] \Rightarrow 2a \equiv 15[19] \text{ (1)}$$

$$b \equiv 15[19] \Rightarrow 5b \equiv 5 \times 15[19] \Rightarrow 5b \equiv 18[19]$$

$$\text{Donc : } 5b \equiv -1[19] \Rightarrow -5b \equiv 1[19] \text{ (2)}$$

De (1) et (2) on déduit que :

$$2a - 5b \equiv 15 + 1[19] \Rightarrow 2a - 5b \equiv 16[19]$$

Par suite : le reste dans la division du nombre $2a - 5b$ Par 19 est : 16

Exercice16 : 1) Déterminer et discuter suivants les valeurs de l'entier naturel n le reste de la division par 10 du nombres 3^n

2) en déduire le chiffre des unités du nombres 2019^{2020}

3) Déterminer les valeurs de l'entier naturel n tel que : $3^n + 5n + 2 \equiv 0[10]$

Solution16 : 1) $3^n \equiv r[10]$ et $r \in \{0;1;2;3;4;5;6;7;8;9\}$

$$\text{On a : } 3^0 \equiv 1[10] \text{ et } 3^1 \equiv 3[10] \text{ et } 3^2 \equiv 9[10]$$

$$\text{et } 3^3 \equiv 7[10] \text{ et } 3^4 \equiv 1[10]$$

Si $n \in \mathbb{N}$ alors : $n = 4k + r$ avec $r \in \{0;1;2;3\}$

$$\text{On a : } 3^4 \equiv 1[10] \text{ donc : } (3^4)^k \equiv 1^k[10]$$

$$\text{donc : } 3^{4k} \equiv 1[10] \text{ et } 3^{4k+1} \equiv 3[10] \text{ et } 3^{4k+2} \equiv 9[7]$$

$$\text{et } 3^{4k+3} \equiv 7[10]$$

2) le chiffre des unités du nombres 2019^{2020} est le reste dans la division du nombre 2019^{2020} Par 10 cad : on cherche r tel que : $2019^{2020} \equiv r[10] \text{ ??}$

$$\text{On a : } 2019 = 2010 + 9 \text{ donc : } 2019 \equiv 9[10]$$

$$\text{donc : } 2019^{2020} \equiv 9^{2020}[10] \text{ donc : } 2019^{2020} \equiv 3^{4040}[10]$$

$$\text{or : } 4040 = 4 \times 1010 = 4 \times k$$

$$\text{donc : } 2019^{2020} \equiv 3^{4k}[10] \text{ donc : } 2019^{2020} \equiv 1[10]$$

le chiffre des unités du nombres 2019^{2020} est 1
 Autre méthode : $2019 \equiv 9[10]$

$$\text{donc : } 2019 \equiv -1[10] \text{ donc : } 2019^{2020} \equiv 1[10]$$

3) On Dresse une table comme suite :

n	$4k$	$4k+1$	$4k+2$	$4k+3$
3^n	$\equiv 1[10]$	$\equiv 3[10]$	$\equiv 9[10]$	$\equiv 7[10]$
$5n$	$\equiv 0[10]$	$\equiv 5[10]$	$\equiv 0[10]$	$\equiv 5[10]$
$3^n + 5n + 2$	$\equiv 3[10]$	$\equiv 0[10]$	$\equiv 1[10]$	$\equiv 4[10]$

$$\text{donc : } 3^n + 5n + 2 \equiv 0[10] \Leftrightarrow n = 3k + 1 \text{ avec } k \in \mathbb{N}$$

Exercice17 : 1) montrer que $\forall n \in \mathbb{N}^*$

$$(n+2)^{n+2} - 2^{n+2}(n+1) \equiv 0[n^2]$$

2) montrer que: $7^{7^{7^{7^7}}} \equiv 3[10]$

Solution17 : 1) on a : $(n+2)^{n+2} = \sum_{k=0}^{n+2} C_{n+2}^k n^k 2^{n+2-k}$ Donc :

$$(n+2)^{n+2} = C_{n+2}^0 n^0 2^{n+2} + C_{n+2}^1 n^1 2^{n+1} + \sum_{k=2}^{n+2} C_{n+2}^k n^k 2^{n+2-k}$$

$$(n+2)^{n+2} = 2^{n+2} + (n+2)n2^{n+1} + \sum_{k=2}^{n+2} C_{n+2}^k n^k 2^{n+2-k}$$

$$\text{Donc : } (n+2)^{n+2} = 2^{n+1}(2+n^2+2n) + n^2 \sum_{k=2}^{n+2} C_{n+2}^k n^k 2^{n-k}$$

$$(n+2)^{n+2} = 2^{n+1}(2+2n) + 2^{n+1}n^2 + n^2 \sum_{k=2}^{n+2} C_{n+2}^k n^k 2^{n-k}$$

$$(n+2)^{n+2} - 2^{n+2}(1+n) = n^2 \left(2^{n+1} + \sum_{k=2}^{n+2} C_{n+2}^k n^k 2^{n-k} \right)$$

$$\text{on a : } n^2 \left(2^{n+1} + \sum_{k=2}^{n+2} C_{n+2}^k n^k 2^{n-k} \right) \equiv 0[n^2]$$

$$\text{donc : } (n+2)^{n+2} - 2^{n+2}(n+1) \equiv 0[n^2]$$

$$2) \text{ on a : } 7 \equiv 7[10] \text{ et } 7^2 \equiv -1[10] \text{ donc } 7^4 \equiv 1[10]$$

$$\text{Donc : } 7^{4k} \equiv 1[10] \text{ et } 7^{4k+1} \equiv 7[10] \text{ et } 7^{4k+2} \equiv 9[10]$$

$$7^{4k+3} \equiv 3[10]$$

$$\text{On aussi : } 7 \equiv 3[4] \text{ et } 7^2 \equiv 1[4]$$

$$\text{Donc } 7^{2k} \equiv 1[4] \text{ et } 7^{2k+1} \equiv 3[4]$$

$$\text{Or : } 7^{7^{7^{7^7}}} \equiv 1[2] \text{ (car impair)}$$

$$\text{Donc : } 7^{7^{7^{7^7}}} \equiv 3[10]$$

Exercice 18 : 1) Déterminer le reste de la division euclidienne de 45872^{2018} par 9

2) Déterminer le reste de la division euclidienne de 25614^{6512} par 13

3) Montrer que pour tout n entier naturel : $3^{2n+1} + 2^{n+2}$ est divisible par 7

4) Montrer que pour tout n entier naturel, $5n^3 + n$ est divisible par 6

5) Montrer que si n n'est pas un multiple de 7, alors : $n^6 - 1$ est un multiple de 7

6) Montrer que pour tout entier naturel, le nombre $n(n^2 + 5)$ est divisible par 6

Exercice19 : $x \in \mathbb{N}^*$ et $y \in \mathbb{N}^*$ On considère les deux nombres : $a = 9x + 4y$ et $b = 2x + y$

1) montrer que $x \wedge y = a \wedge b$

2) $n \in \mathbb{N}$ on pose : $a = n^2 + 5n + 13$ et $b = n + 3$

a) montrer que $a \wedge b = b \wedge a$
 b) en déduire les valeurs possibles $a \wedge b = d$
 c) montrer que : $n \equiv 4[7] \Leftrightarrow a \wedge b = 7$
 d) en déduire les valeurs de $n \in \mathbb{N}$ tel que :
 $a \wedge b = 1$
Solution 19 : 1) on pose $d = x \wedge y$ et $d' = a \wedge b$
 montrons que : $d = d'$
 $d = x \wedge y$ donc : $\Rightarrow d/x$ et $d/y \Rightarrow d/a$ et d/b
 Car il divise toute combinaison de x et y
 $\Rightarrow d/a \wedge b \Rightarrow d/d'$
 Inversement :
 $d' = a \wedge b \Rightarrow d'/a$ et $d'/b \Rightarrow d'/9x+4y$ et $d'/2x+y$
 $\Rightarrow d'/(9x+4y) - 4(2x+y)$ et $d'/9(2x+y) - 2(9x+4y)$
 $\Rightarrow d'/x$ et $d'/y \Rightarrow d'/x \wedge y \Rightarrow d'/d$
 ce qui entraîne: $d = d'$
 2) $n \in \mathbb{N}$ on pose : $a = n^2 + 5n + 13$ et $b = n + 3$
 a) montrons que $a \wedge b = b \wedge a$?
 la division euclidienne de $n^2 + 5n + 13$ par $n + 3$
 donne : $n^2 + 5n + 13 = (n + 3)(n + 2) + 7$
 Donc : $a = b(n + 2) + 7 \Leftrightarrow a - b(n + 2) = 7$
 on pose $d' = b \wedge 7$ et $d = a \wedge b$
 montrons que : $d = d'$
 $d = a \wedge b \Rightarrow d/a$ et $d/b \Rightarrow d/a - b(n + 2)$ et d/b
 $\Rightarrow d/7$ et $d/b \Rightarrow d/b \wedge 7 \Rightarrow d/d'$
 $d' = b \wedge 7 \Rightarrow d'/7$ et $d'/b \Rightarrow d'/b(n + 2) + 7$ et d'/b
 $\Rightarrow d'/a$ et $d'/b \Rightarrow d'/a \wedge b \Rightarrow d'/d$
 ce qui entraîne: $d = d'$
 b) les valeurs possibles $a \wedge b = d$??
 on a : $a \wedge b = b \wedge a = d$
 donc : $d/7$ donc : $d = 1$ ou $d = 7$
 c) montrons que : $n \equiv 4[7] \Leftrightarrow a \wedge b = 7$
 $n \equiv 4[7] \Leftrightarrow n + 3 \equiv 0[7] \Leftrightarrow 7/n + 3 \Leftrightarrow 7/b \Leftrightarrow b \wedge 7 = 7 \Leftrightarrow b \wedge a = 7$
 d) les valeurs de $n \in \mathbb{N}$ tel que : $a \wedge b = 1$??
 $a \wedge b = 1 \Leftrightarrow n$ n'est pas congrue a 0 modulo 4
 $n \equiv 0[7]$ ou $n \equiv 1[7]$ ou $n \equiv 2[7]$ ou $n \equiv 3[7]$ ou $n \equiv 5[7]$
 ou $n \equiv 6[7]$

3) Les classes d'équivalences.

3.1 Définition et propriété :

Activité : Déterminer l'ensemble des entiers relatifs qui admettent 2 pour reste de la division par 7.

Définition : Soit n un entier naturel non nul. L'ensemble des entiers relatifs qui ont le même reste r de la division euclidienne par n s'appelle

la classe d'équivalence de r et se note : $\bar{r} = \{m \in \mathbb{Z} / m \equiv r [n]\} = \{nk + r \text{ où } k \in \mathbb{Z}\}$

Exemple : Pour $n = 7$ les restes possibles sont les éléments de l'ensemble : $\{0, 1, 2, 3, 4, 5, 6\}$

Donc on peut définir les classes d'équivalences suivantes :

$$\bar{0} = \{m \in \mathbb{Z} / m \equiv 0 [7]\}$$

$$\bar{1} = \{m \in \mathbb{Z} / m \equiv 1 [7]\} \text{ et } \dots$$

$$\bar{6} = \{m \in \mathbb{Z} / m \equiv 6 [7]\}$$

on remarque que $\bar{0} = \bar{7}$

Les classes d'équivalences modulo 7 constituent : un ensemble noté :

$$\mathbb{Z} / 7\mathbb{Z} = \{\bar{0}; \bar{1}; \bar{2}; \bar{3}; \bar{4}; \bar{5}; \bar{6}\}$$

$$\text{Généralisation : } \mathbb{Z} / n\mathbb{Z} = \{\bar{0}; \bar{1}; \bar{2}; \bar{3}; \dots; \overline{n-1}\}$$

3.2 Les opérations sur $\mathbb{Z} / n\mathbb{Z}$

Définition : Soit n un entier naturel non nul.

On définit dans $\mathbb{Z} / n\mathbb{Z}$ les deux lois :

1) **L'addition :** On pose $\overline{a+b} = \overline{a+b}$

2) **La multiplication :** On pose : $\overline{a \times b} = \overline{a \times b}$

Exemple : Dans $\mathbb{Z} / 6\mathbb{Z}$: $\bar{3} \times \bar{4} = \bar{0}$ et $\bar{5} + \bar{4} = \bar{3}$

Exercice 20 : Résoudre les équations

suites dans $\mathbb{Z} / 4\mathbb{Z}$: 1) $\bar{2}x = \bar{3}$ 2) $x^2 + \bar{3}x = \bar{0}$

3) $\overline{2013}x^3 + \bar{2}x = \bar{k}$

Solution 20 : On a : $\mathbb{Z} / 4\mathbb{Z} = \{\bar{0}; \bar{1}; \bar{2}; \bar{3}\}$

1) On Dresse une table comme suite :

x	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}x$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$

Et en utilisant cette une table on déduit que

Cette équation n'admet pas de solutions

Donc : $S = \emptyset$

1) On Dresse une table comme suite :

x	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
x^2	$\bar{0}$	$\bar{1}$	$\bar{0}$	$\bar{1}$
$\bar{3}x$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$
$x^2 + \bar{3}x$	$\bar{0}$	$\bar{0}$	$\bar{2}$	$\bar{2}$

Et en utilisant cette une table on déduit que :

$\bar{0}$ et $\bar{1}$ sont solutions de l'équation

Donc : $S = \{\bar{0}; \bar{1}\}$

$$2) \overline{2013x^3 + 2x} = \overline{k} \Leftrightarrow \overline{1x^3 + 2x} = \overline{k} \Leftrightarrow x^3 + 2x = \overline{k}$$

Car : $2013 = 503 \times 4 + 1$

On Dresse une table comme suite :

x	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
x^3	$\overline{0}$	$\overline{1}$	$\overline{0}$	$\overline{3}$
$\overline{2x}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$x^3 + \overline{2x}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{1}$

Si $\overline{k} = \overline{0}$: $S = \{\overline{0}; \overline{2}\}$ Si $\overline{k} = \overline{1}$: $S = \{\overline{3}\}$

Si $\overline{k} = \overline{2}$: $S = \emptyset$ Si $\overline{k} = \overline{3}$: $S = \{\overline{1}\}$

Exercice21 : Résoudre dans $(\mathbb{Z}/5\mathbb{Z})^2$ l'équations

suiuants : $x + \overline{3y} = \overline{1}$

Solution21 : on Dresse une table des opérations

de $\mathbb{Z}/5\mathbb{Z} = \{\overline{0}; \overline{1}; \overline{2}; \overline{3}; \overline{4}\}$ Comme suite

	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{3}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$	$\overline{4}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$	$\overline{0}$
$\overline{4}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{1}$	$\overline{1}$

$$S = \{(\overline{0}; \overline{2}); (\overline{1}; \overline{0}); (\overline{2}; \overline{3}); (\overline{3}; \overline{1}); (\overline{4}; \overline{3}); (\overline{4}; \overline{4})\}$$

Exercice22 : Résoudre dans $(\mathbb{Z}/5\mathbb{Z})^2$ les

système suivants :
$$\begin{cases} \overline{3x} + \overline{2y} = \overline{1} \\ \overline{2x} + \overline{4y} = \overline{3} \end{cases}$$

Solution22 :

$$\begin{cases} \overline{3x} + \overline{2y} = \overline{1} \\ \overline{2x} + \overline{4y} = \overline{3} \end{cases} \Leftrightarrow \begin{cases} (\overline{3} + \overline{2})x + (\overline{2} + \overline{4})y = \overline{3} + \overline{1} \\ \overline{2x} + \overline{4y} = \overline{3} \end{cases}$$

$$\begin{cases} y = \overline{4} \\ \overline{2x} + \overline{4y} = \overline{3} \end{cases} \Leftrightarrow \begin{cases} x = \overline{1} \\ y = \overline{4} \end{cases} \text{ donc } S = \{(\overline{1}; \overline{4})\}$$

Exercice : 1) Dresser les tables des opérations de $\mathbb{Z}/7\mathbb{Z}$

2) Résoudre dans $\mathbb{Z}/7\mathbb{Z}$ les équations :

a) $\overline{2x} - \overline{1} = \overline{0}$ b) $\overline{4x} + \overline{1} = x + \overline{3}$

c) $\overline{5x^2} + \overline{3x} + \overline{1} = \overline{0}$

Propriété : Si p est **premier** alors dans $\mathbb{Z}/p\mathbb{Z}$ on a :

$$(\overline{a} \times \overline{b} = \overline{0} \Leftrightarrow \overline{a} = 0 \text{ ou } \overline{b} = \overline{0})$$

Preuve : Après la décomposition.

IV) DECOMPOSITION D'UN ENTIER EN FACTEURS DES NOMBRES PREMIERS

1) Définition et propriétés

Activité : Décomposer en produit de facteurs premiers le nombre : 24816

Théorème :

a) Chaque entier **naturel** m non nul s'écrit d'une façon unique comme le produit des facteurs premiers comme suite :

$$m = p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \dots \times p_n^{\alpha_n} = \prod_{k=1}^{k=n} p_k^{\alpha_k}$$

b) Chaque entier **relatif** m non nul s'écrit d'une façon unique comme le produit des facteurs premiers

comme suite :

$$m = \varepsilon p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \dots \times p_n^{\alpha_n} = \prod_{k=1}^{k=n} p_k^{\alpha_k}$$

où $\varepsilon \in \{-1, 1\}$

Propriété 1: Soit a un entier relatif dont la décomposition est de la forme :

$$a = \varepsilon p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \dots \times p_n^{\alpha_n} = \prod_{k=1}^{k=n} p_k^{\alpha_k}$$

un entier d non nul divise l'entier a si et seulement si d à une décomposition de la forme

$$d = \varepsilon p_1^{\beta_1} \times p_2^{\beta_2} \times p_3^{\beta_3} \times \dots \times p_n^{\beta_n} = \prod_{k=1}^{k=n} p_k^{\beta_k} \delta n \text{ où}$$

$$(\forall i \in \llbracket 1, n \rrbracket) (0 \leq \beta_i \leq \alpha_i)$$

δn un diviseur de a le nombre des valeurs possibles de δi est $\alpha_i + 1$

On en déduit que :

Propriété 2 :

$$a = \varepsilon p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \dots \times p_n^{\alpha_n} = \prod_{k=1}^{k=n} p_k^{\alpha_k}$$

est un entier, le nombre des diviseurs de a

$$\text{est : } 2(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_n + 1)$$

Exercice :

1- Décomposer le nombre 2975 en facteurs des nombres premiers

2- Déterminer le nombre des diviseurs de 2975.

3- Déterminer tous les diviseurs positifs de 2975.

Propriété 3 : Soit a un entier relatif dont la décomposition est de la forme :

$$a = \varepsilon p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \dots \times p_n^{\alpha_n} = \prod_{k=1}^{k=n} p_k^{\alpha_k}$$

un entier m est un multiple de a si et seulement

$$\text{si } m = \varepsilon p_1^{\beta_1} \times p_2^{\beta_2} \times p_3^{\beta_3} \times \dots \times p_n^{\beta_n} = \prod_{k=1}^{k=n} p_k^{\beta_k}$$

où $(\forall i \in [1, n]) (\alpha_i \leq \beta_i)$

2) Application de la décomposition.

Propriété : Soient a et b deux entiers naturels

1) Le plus grand entier n qui vérifie :

$$n \leq a \text{ et } n \leq b \text{ est } \inf(a, b)$$

2) Le plus petit entier n qui vérifie :

$$n \geq a \text{ et } n \geq b \text{ est } \sup(a, b)$$

Exemple : $a = 7$ et $b = 10$

Le plus grand des entiers n tel que :

$$n \leq 7 \text{ et } n \leq 10 \text{ est : } 7 = \inf(7, 10)$$

Le plus petit des entiers n tel que :

$$n \geq 7 \text{ et } n \geq 10 \text{ est } 10 = \sup(7, 10)$$

2.1 Le P.G.C.D de deux nombres.

Soient $a = \prod_{k=1}^{k=n} p_k^{\alpha_k} = 1$ et $b = \prod_{k=1}^{k=n} p_k^{\beta_k}$ deux entiers ; le P. G. D. C (a, b) est l'entier

$$a \wedge b = \prod_{k=1}^{k=n} p_k^{\inf(\alpha_k; \beta_k)}$$

Remarque : Soient a et b deux entiers relatifs

$$\text{on a : } a \wedge b = |a| \wedge |b|$$

Exemple : Déterminer : $(-5664) \wedge (-984)$ et

$$324 \wedge (-144)$$

Exercice :

1- Décomposer les nombres 362154 et 82350 en produit des facteurs premiers

2- Déterminer le P.G.C.D de 362154 et 82350

3- Déterminer tous les diviseurs communs de 362154 et 82350

2.2 Le P.P.C.M de deux nombres.

Soient $a = \prod_{k=1}^{k=n} p_k^{\alpha_k} = 1$ et $b = \prod_{k=1}^{k=n} p_k^{\beta_k}$ deux entiers ; le ppmc (a, b) est l'entier

$$a \vee b = \prod_{k=1}^{k=n} p_k^{\sup(\alpha_k; \beta_k)}$$

Exemple : déterminer : $d = (-8316) \wedge 1080$ et

$$m = 8316 \vee 1080$$

Solution : la décomposition des nombres 8316 et 1080 en produit des facteurs premiers

$$\text{Donnent : } 8316 = 2^2 \times 3^3 \times 7 \times 11 \text{ et}$$

$$1080 = 2^3 \times 3^3 \times 5$$

$$d = 8316 \wedge 1080 = 2^2 \times 3^3 = 108 \text{ et}$$

$$m = 8316 \vee 1080 = 2^3 \times 3^3 \times 5 \times 7 \times 11 = 11880$$

2.3 Applications de la décomposition.

Propriété : Soient a et b deux entiers relatifs non nuls, on a les assertions suivantes :

$$1) (a \wedge b) \times (a \vee b) = |ab|$$

$$2) ca \vee cb = c(a \vee b)$$

$$3) ca \wedge cb = c(a \wedge b)$$

Exemple : si $2 = a \wedge b$ et $-12 = a \times b$

déterminer : $a \vee b$

Solution : on a $(a \wedge b) \times (a \vee b) = |ab|$

$$\text{donc : } a \vee b = |a \times b| / a \wedge b = |-12| / 2 = 6$$

Exercice23: $a = (25^n - 1)(36^n - 1)$ et $b = (5^n - 1)(6^n - 1)$

Calculer les $a \vee b$ ($n \in \mathbb{N}$)

Solution23 :

$$a = ((5^n)^2 - 1)((6^n)^2 - 1) = (5^n - 1)(5^n + 1)(6^n - 1)(6^n + 1)$$

$$a = b(5^n + 1)(6^n + 1) \text{ donc : } \frac{b}{a} \text{ donc : } a \vee b = a$$

V) Exercices avec solutions

Exercice24: n et a et b des entiers naturels

Démontrer que si q est le quotient de la division euclidienne de n par a et q' est le quotient de q par b Alors q' est aussi le quotient de n par ab

Solution : soit r le reste de la division

euclidienne de n par a et r' le reste de la division euclidienne de q par b on a donc :

$$n = aq + r \text{ et } 0 \leq r \leq a - 1 \text{ et on a : } q = bq' + r' \text{ et}$$

$$0 \leq r' \leq b - 1 \text{ donc on déduit que :}$$

$$n = a(bq' + r') + r = abq' + ar' + r$$

Et puisque : $0 \leq r' \leq b - 1$ et $0 \leq r \leq a - 1$ alors :

$$ar' + r \leq ab - 1 \text{ donc } n = abq' + ar' + r$$

$$0 \leq ar' + r \leq ab - 1 \text{ conclusion : } q' \text{ est aussi le}$$

quotient de n par ab

Exercice25: Déterminer le reste de la division

euclidienne de $19^{52} \times 23^{41}$ par 7

Solution25 : on a $19 \equiv 5[7]$ donc $19^2 \equiv 4[7]$

$$\text{donc : } 19^4 \equiv 2[7] \text{ donc } 19^{52} \equiv 2^{13}[7]$$

$$\text{Et on a } 23 \equiv 2[7] \text{ donc } 23^{41} \equiv 2^{41}[7] \text{ donc}$$

$$23^{41} \times 19^{52} \equiv 2^{13} \times 2^{41}[7]$$

$$\text{donc } 23^{41} \times 19^{52} \equiv 2^{54}[7] \text{ donc}$$

$$23^{41} \times 19^{52} \equiv (2^3)^{18}[7] \text{ donc } 23^{41} \times 19^{52} \equiv 8^{18}[7]$$

$$\text{et puisque : } 8 \equiv 1[7] \text{ donc } 23^{41} \times 19^{52} \equiv 1[7]$$

conclusion : 1 est le reste de la division

euclidienne de $19^{52} \times 23^{41}$ par 7

Exercice26: $n \in \mathbb{N}$ on pose $U_n = 4^n - 3n - 1$

1) montrer que $\forall n \in \mathbb{N} \quad U_{n+1} = 4U_n + 9n$

2) En déduire que $\forall n \in \mathbb{N} \quad 9$ divise $4^n - 3n - 1$

Solution26 : 1) on a $U_{n+1} = 4^{n+1} - 3(n+1) - 1$

donc $U_{n+1} = 4 \times 4^n - 3n - 3 - 1$

et puisque : $U_n = 4^n - 3n - 1$ donc :

$4^n = U_n + 3n + 1$ donc : $U_{n+1} = 4U_n + 9n$

2) notons P(n) La proposition suivante : « 9 divise U_n » . Nous allons démontrer par récurrence que P(n) est vraie pour tout $n \in \mathbb{N}$.

1 étapes : l'initialisation : Pour $n=0$ nous avons

$U_0 = 4^0 - 3 \times 0 - 1 = 0$ donc 9 divise 0 .

Donc P (0) est vraie.

2 étapes : d'hérédité ou Hypothèse de récurrence

: Supposons que P(n) soit vraie c'est-à-dire : « 9 divise U_n »

3 étapes : Nous allons montrer que P(n+1) est vraie.

Montrons alors que : « 9 divise U_{n+1} » ??

c'est-à-dire Montrons que $U_{n+1} \equiv 0[9]$??

On a d'après l'hypothèse de récurrence: « 9 divise U_n » donc $U_n \equiv 0[9]$ donc $4U_n \equiv 0[9]$

Et on a : $9n_n \equiv 0[9]$ donc $U_n + 9n_n \equiv 0[9]$ donc

$U_{n+1} \equiv 0[9]$

Conclusion : $\forall n \in \mathbb{N} \quad 9$ divise $4^n - 3n - 1$

Exercice27: 1) Résoudre dans $\mathbb{Z}/5\mathbb{Z}$ l'équation:

$$\bar{4}x - \bar{3} = \bar{0}$$

2) Résoudre dans $(\mathbb{Z}/5\mathbb{Z})^2$ le système suivant :

$$\begin{cases} \bar{3}x + \bar{2}y = \bar{1} \\ \bar{2}x + \bar{4}y = \bar{3} \end{cases}$$

3) Résoudre dans $\mathbb{Z}/5\mathbb{Z}$ l'équation: $x^2 - x - \bar{2} = \bar{0}$

Solution27 : 1) on Dresse une table des

opérations de $\mathbb{Z} / 5\mathbb{Z} = \{\bar{0}; \bar{1}; \bar{2}; \bar{3}; \bar{4}\}$

Comme suite :

x	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{4}x$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$
$\bar{4}x - \bar{3}$	$\bar{2}$	$\bar{1}$	$\bar{0}$	$\bar{4}$	$\bar{3}$

Et on utilisons cette une table on déduit que $\bar{2}$ est la seul solution de l'équation

Donc : $S = \{\bar{2}\}$..

$$2): \begin{cases} \bar{3}x + \bar{2}y = \bar{1} \\ \bar{2}x + \bar{4}y = \bar{3} \end{cases} \Leftrightarrow \begin{cases} (\bar{3} + \bar{2})x + (\bar{2} + \bar{4})y = \bar{3} + \bar{1} \\ \bar{2}x + \bar{4}y = \bar{3} \end{cases}$$

$$\begin{cases} y = \bar{4} \\ \bar{2}x + \bar{4}y = \bar{3} \end{cases} \Leftrightarrow \begin{cases} x = \bar{1} \\ y = \bar{4} \end{cases} \text{ donc } S = \{(\bar{1}; \bar{4})\}$$

3) on Dresse une table des opérations de

$$\mathbb{Z} / 5\mathbb{Z} = \{\bar{0}; \bar{1}; \bar{2}; \bar{3}; \bar{4}\}$$

Comme suite :

x	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
x^2	$\bar{0}$	$\bar{1}$	$\bar{4}$	$\bar{4}$	$\bar{1}$
$x^2 - x - \bar{2}$	$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{4}$	$\bar{0}$

Et on utilisons cette une table on déduit que $\bar{2}$ et $\bar{4}$ sont les solutions de l'équation

Donc : $S = \{\bar{2}; \bar{4}\}$

Exercice28: $n \in \mathbb{Z}$ on pose $\alpha_n = n^4 - n^2 + 16$

1) montrer que $n^2 - 3n + 4$ et $n^2 + 3n + 4$ sont des nombres paires

2) En déduire que α_n n'est pas un nombre premier

Solution28 : 1) soit $n \in \mathbb{Z}$

$$n^2 - 3n + 4 \equiv n^2 - n[2] \text{ donc}$$

$$n^2 - 3n + 4 \equiv n(n-1)[2]$$

Or $n(n-1)$ est le produit de deux nombres consécutifs donc paire

$$\text{donc } n(n-1) \equiv 0[2] \text{ donc } n^2 - 3n + 4 \equiv 0[2]$$

donc $n^2 - 3n + 4$ est un nombre paire

$$\text{et on a : } n^2 + 3n + 4 \equiv n^2 + n[2] \text{ donc}$$

$$n^2 + 3n + 4 \equiv n(n+1)[2]$$

Or $n(n+1)$ est le produit de deux nombres consécutifs donc paire

$$\text{donc } n(n+1) \equiv 0[2] \text{ donc } n^2 + 3n + 4 \equiv 0[2]$$

donc $n^2 + 3n + 4$ est un nombre paire

2)

$$\alpha_n = n^4 - n^2 + 16 = (n^2 + 4)^2 - 9n^2 = (n^2 - 3n + 4)(n^2 + 3n + 4)$$

Et puisque $n^2 - 3n + 4$ et $n^2 + 3n + 4$ sont des nombres paire

$$\text{alors : } n^2 - 3n + 4 \neq 1 \text{ et } n^2 + 3n + 4 \neq 1$$

donc α_n n'est pas un nombre premier

Exercice29: $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ et $c \in \mathbb{Z}$ et $d \in \mathbb{Z}$ tels que : $a = bc + d$

1) montrer que $a \wedge b = b \wedge d$

2) En déduire que : $a \wedge b = b \wedge (a - bc)$

Solution29 : 1) on pose $\Delta_1 = a \wedge b$ et $\Delta_2 = b \wedge d$

On a : Δ_1/a et Δ_1/b donc Δ_1/a et Δ_1/bc donc

$\Delta_1/a - bc$ donc Δ_1/d

donc Δ_1/d et Δ_1/b donc $\Delta_1/b \wedge d$ donc Δ_1/Δ_2

inversement On a : Δ_2/b et Δ_2/d donc Δ_2/d et

Δ_2/bc donc $\Delta_2/bc + d$ donc Δ_2/a

donc Δ_2/a et Δ_2/b donc $\Delta_2/a \wedge b$ donc Δ_2/Δ_1

On a donc : Δ_1/Δ_2 et Δ_2/Δ_1 et $\Delta_1 \in \mathbb{N}$ et $\Delta_2 \in \mathbb{N}$

donc $\Delta_1 = \Delta_2$

donc : $a \wedge b = b \wedge d$

2) on a : $a = bc + (a - bc)$ si on prend : $d = a - bc$ et

d'après 1) on aura : $a \wedge b = b \wedge d = b \wedge (a - bc)$

Exercice30: $a \in \mathbb{N}^*$ et $b \in \mathbb{N}^*$ et $a \geq 3$ et a est impair On pose : $d = (2^a - 1) \wedge (2^b + 1)$

1) a) montrer que $2^{ab} \equiv 1[d]$

b) montrer que $2^{ab} \equiv -1[d]$

2) En déduire que : $d \in \{1; 2\}$

3) montrer que $d = 1$

Solution31 : 1) a) montrons que $2^{ab} \equiv 1[d]$

On a : $d = (2^a - 1) \wedge (2^b + 1)$

Donc il existent : $\alpha \in \mathbb{N}^*$ et $\beta \in \mathbb{N}^*$ tels que :

$2^a - 1 = d\alpha$ et $2^b + 1 = d\beta$ donc :

$2^{ab} = (2^a)^b = (d\alpha + 1)^b$

Et on a : $d\alpha + 1 \equiv 1[d]$ Donc $(d\alpha + 1)^b \equiv 1[d]$

Par suite : $2^{ab} \equiv 1[d]$

1) a) montrons que $2^{ab} \equiv -1[d]$

On a : $2^{ab} = (2^b)^a = (d\beta - 1)^a$

Et on a : $d\beta - 1 \equiv -1[d]$ Donc $(d\beta - 1)^a \equiv (-1)^a [d]$

et puisque a est impair on a $(d\beta - 1)^a \equiv -1[d]$

Par suite : $2^{ab} \equiv -1[d]$

2) $d \in \{1; 2\}$???

on a : $2^{ab} \equiv 1[d]$ et $2^{ab} \equiv -1[d]$ donc $0 \equiv 2[d]$

donc $d/2$ et on a $d \in \mathbb{N}^*$ donc $d \in \{1; 2\}$

3) montrons que $d = 1$

On a : $2^a - 1$ et $2^b - 1$ sont impairs donc d est impair

Et puisque $d \in \{1; 2\}$ donc $d = 1$

Exercice32 :

1) a) montrer que : $2^{4k+r} \equiv 2^r [5] \forall (k; r) \in \mathbb{N}^2$

b) Déterminer et discuter suivants les valeurs de l'entier naturel n le reste de la division par 5 du nombres 2^n

2) montrer que $\frac{5}{17^{4p+2}} + 32^{4p+3} + 3 \forall p \in \mathbb{N}^*$

3) montrer que $\frac{5}{1^{2006}} + 2^{2006} + 3^{2006} + 4^{2006}$

Solution33 : 1) a) on a : $2^4 \equiv 1[5]$ donc

$(2^4)^k \equiv 1^k [5]$ donc $2^{4k} \equiv 1[5]$ donc $2^{4k} \times 2^r \equiv 2^r [5]$

Donc $2^{4k+r} \equiv 2^r [5] \forall (k; r) \in \mathbb{N}^2$

b) $2^n \equiv r[5]$ et $r \in \{0; 1; 2; 3; 4\}$

Si $n \in \mathbb{N}$ alors : $n = 4k + r$ avec $r \in \{0; 1; 2; 3\}$

donc : $2^{4k} \equiv 1[5]$ et $2^{4k+1} \equiv 2[5]$ et $2^{4k+2} \equiv 4[5]$

et $2^{4k+3} \equiv 3[5]$

2) montrons que $\frac{5}{17^{4p+2}} + 32^{4p+3} + 3 \forall p \in \mathbb{N}^* ?$

on a : $17 \equiv 2[5]$ donc : $17^{4p+2} \equiv 2^{4p+2} [5]$

$32^{4p+3} \equiv -2^{4p+3} [5]$ $17^{4p+2} \equiv 4[5]$

on a : $32 \equiv 2[5]$ donc : $32^{4p+3} \equiv 2^{4p+3} [5]$

donc : $32^{4p+3} \equiv 3[5]$ donc $32^{4p+3} \equiv 2[5]$

donc $17^{4p+2} + 32^{4p+3} + 3 \equiv 4 + 3 + 3[5]$

donc $17^{4p+2} + 32^{4p+3} + 3 \equiv 0[5]$

donc $\frac{5}{17^{4p+2}} + 32^{4p+3} + 3 \forall p \in \mathbb{N}^*$

3)

on a : $1 \equiv 1[5]$ et $2 \equiv 2[5]$ et $3 \equiv -2[5]$ et $4 \equiv -1[5]$

donc : $1^{2006} \equiv 1^{2006} [5]$ et $2^{2006} \equiv 2^{2006} [5]$ et

$3^{2006} \equiv (-2)^{2006} [5]$ et $4^{2006} \equiv (-1)^{2006} [5]$

donc ; $1^{2006} + 2^{2006} + 3^{2006} + 4^{2006} \equiv 2 + 2 \times 2^{2006} [5]$

$1^{2006} + 2^{2006} + 3^{2006} + 4^{2006} \equiv 2 + 2^{2007} [5]$

Or : $2007 = 4 \times 501 + 3$ donc : $2^{2007} \equiv 3[5]$

Donc : $1^{2006} + 2^{2006} + 3^{2006} + 4^{2006} \equiv 2 + 3[5] \equiv 0[5]$

Exercice34 : déterminer le chiffre des unités

des nombres suivants : 1) $2019^{2020^{2021}}$ 2) $1987^{1991^{1983}}$

Solution34 :1) on a : $2019 \equiv -1[10]$ donc

$$2019^{2020^{2021}} \equiv (-1)^{2020^{2021}} [10] \text{ et puisque } 2020^{2021}$$

Est paire donc : $2019^{2020^{2021}} \equiv 1[10]$

le chiffre des unités est 1

2) on a : $1987 \equiv 7[10]$ donc $1987^2 \equiv 9[10]$

Et $1987^3 \equiv 3[10]$ et $1987^4 \equiv 1[10]$

Donc : $1987^{4k} \equiv 1[10]$ et $1987^{4k+1} \equiv 7[10]$ et

$1987^{4k+2} \equiv 9[10]$ et $1987^{4k+3} \equiv 3[10]$

$1991^{1983} \equiv ?[4]$

$1991 \equiv 3[4]$ et $1991^2 \equiv 1[4]$

on a : $1983 \equiv 1[2]$ donc : $1991^{1983} \equiv 3[4]$

donc : $1987^{1991^{1983}} \equiv 3[10]$

Le chiffre des unités est 3

Exercice35 : soit $N = \overline{dcba}$ un entier naturel

montrer que : $N \equiv a - b + c - d [11]$

Solution35 :on a :

$$N = \overline{dcba} = a + b \times 10 + c \times 10^2 + d \times 10^3$$

et on a : $10 \equiv -1[11]$ et $10^2 \equiv 1[11]$ et $10^3 \equiv -1[11]$

Donc : $N \equiv a - b + c - d [11]$

Exercice36 :

1)En utilisant l'algorithme d'Euclide calculer :

$$67 \wedge 39$$

2) en déduire deux nombres relatifs u et v tel

$$\text{que : } 39u + 67v = 1$$

Solution36 :1)

$$(1) 67 = 1 \times 39 + \boxed{28} \quad (2) 39 = 1 \times 28 + \boxed{11}$$

$$(3) 28 = 2 \times 11 + \boxed{6} \quad (4) 11 = 1 \times 6 + \boxed{5}$$

$$(5) 6 = 1 \times 5 + \boxed{1} \quad (6) 5 = 1 \times 5 + \boxed{0}$$

Donc : $67 \wedge 39 = 1$ c'est le dernier reste non nul dans l'algorithme d'Euclide

$$2) (5) 6 = 1 \times 5 + \boxed{1} \Rightarrow 6 - 1 \times 5 = \boxed{1}$$

$$\Rightarrow 6 - 1 \times (11 - 1 \times 6) = \boxed{1} \Rightarrow 2 \times 6 - 1 \times 11 = \boxed{1}$$

$$\Rightarrow 2 \times (28 - 2 \times 11) - 1 \times 11 = \boxed{1} \Rightarrow 2 \times 28 - 5 \times 11 = \boxed{1}$$

$$\Rightarrow 2 \times 28 - 5 \times (39 - 1 \times 28) = \boxed{1} \Rightarrow 7 \times 28 - 5 \times 39 = \boxed{1}$$

$$\Rightarrow 7 \times (67 - 1 \times 39) - 5 \times 39 = \boxed{1} \Rightarrow \boxed{7 \times 67 - 12 \times 39 = \boxed{1}}$$

« C'est en forgeant que l'on devient forgeron » Dit un proverbe.

C'est en s'entraînant régulièrement aux calculs et exercices

Que l'on devient un mathématicien

