

L'ARITHMETIQUE

I) RAPPELS

1) Divisibilité dans $\mathbb{Z}$

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 ou a est un multiple de b

Exemples : $\frac{3}{12}$ car $12 = 3 \times 4$ et $\frac{-6}{42}$

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

Définition :

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

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

Exercice1 : 1) Déterminer et dénombrer les diviseurs naturels de 156

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

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

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

- $1/a$; $-1/a$ et a/a et $a/-a$
- $b|a \Rightarrow |b| \leq |a|$
- $a/b \Rightarrow a/b \times c$
- $a/b \Rightarrow |a| \leq |b|$
- $b|1 \Rightarrow b \in \{-1, 1\}$
- $a|b$ et $b|a \Rightarrow |a| = |b|$
- $a|b$ et $c|d \Rightarrow ac|bd$
- $a|b$ et $b|c \Rightarrow a|c$
- $a|b \Rightarrow a|b \times c$
- $a|b$ et $b|c \Rightarrow a|c$
- $a|b \Rightarrow a|b \times c$
- $a|m$ 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.
- $a/b \Rightarrow a^n/b^n$ $n \in \mathbb{N}$

Exercice2 : 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 $\frac{a}{2b+c}$ et $\frac{a}{b+c}$ alors $\frac{a}{c}$

b) montrer que si $\frac{a}{2b+3c}$ et $\frac{a}{b+c}$ alors $\frac{a}{c}$

c) montrer que si $\frac{a}{x-y}$ et $\frac{a}{b-c}$ alors $\frac{a}{xb-cy}$

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

Montrer que $\frac{a}{19}$

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

Montrer que $\frac{d}{13}$

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

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

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

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

Exercice3 : Quelles sont les valeurs de l'entier relatif n pour lesquelles la fraction $\frac{3n+8}{n+4}$

Représente un entier relatif ?

Solution : 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 entraîne 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.

Exercice4 : Résoudre dans $\mathbb{N}^2$ les équations suivantes : a) $x^2 - y^2 = 32$ avec $x > y$
b) $2xy + 2x + y = 99$

Solution : a) $x^2 - y^2 = 32 \Leftrightarrow (x-y)(x+y) = 32$
 $x-y$ et $x+y$ sont des diviseurs positifs 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 positifs 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 dans $\mathbb{Z}$

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

Exemple :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 $0 \leq 7 < 11$

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

Exercice5 : 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 ($p \in \mathbb{N}$)

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

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

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

Exercice6 : $b \in \mathbb{N}^*$ 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}

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

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

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

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

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}

b) L'inverse est-il vrai ?

3) Les nombres premiers

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 effectifs 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.

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.

Exercice7: 1) Les nombres suivants sont-ils premiers : 499 ; 601 ; 703 ; 2003 ; $2n^2 + 3n$ $n \in \mathbb{N}$

Crible d'Eratosthène. Les nombres premiers inférieurs à 100

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

Théorème : L'ensemble des nombres premiers est infini.

Exercice 8 : a) Montrer que tout nombre premier s'écrit de la forme $p=6n+1$ ou $p = 6n + 5$

4) Plus grand diviseurs commun

4.1 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) $1 \wedge a = 1$

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

$$4) \text{ Si } b|a \text{ alors } a \wedge b = |b|$$

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

$$6) a \wedge b = a \wedge (a - b)$$

Exercice9 : montrer que $\forall a \in \mathbb{Z} \quad a \wedge (a+1) = 1$

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

$$\Rightarrow d/a \text{ et } d/a+1 \Rightarrow d/1 \Rightarrow d=1$$

Exercice10 : $n \in \mathbb{N}$ 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 : $\frac{n^2+3}{n+2} \in \mathbb{N}$

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

On a : $d = A \wedge B$

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

$$\Rightarrow d/n^2+3 \text{ et } d/n+2 \text{ on utilisant la division}$$

$$\text{euclidienne : on trouve : } n^2+3 = (n+2)(n-2) + 7$$

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

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

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

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

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

$$\text{donc : } d'/A \wedge B \text{ donc } d'/d$$

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

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

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

$$\text{Donc : } \frac{n+2}{A \wedge B} \text{ Donc : } \frac{n+2}{(n+2) \wedge 7}$$

$$\text{Donc : } \frac{n+2}{7} \text{ or } 7 \text{ est premier donc :}$$

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 11: $a \in \mathbb{Z}$ 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 : $a \wedge b = b \wedge (a - bc)$

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

$$\text{On a : } \Delta_1/a \text{ et } \Delta_1/b \text{ donc } \Delta_1/a \text{ et } \Delta_1/bc \text{ donc}$$

$$\Delta_1/a - bc \text{ donc } \Delta_1/d$$

$$\text{donc } \Delta_1/d \text{ et } \Delta_1/b \text{ donc } \Delta_1/b \wedge d \text{ donc } \Delta_1/\Delta_2$$

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 : $a \wedge b = b \wedge d = b \wedge (a - bc)$

Exercice12 : $a \in \mathbb{N}$ On considère les deux nombres : $A = 35a + 57$ et $B = 45a + 76$ montrer que $A \wedge B = 1$ ou $A \wedge B = 19$

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

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

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

$\Rightarrow d/315a + 513$ et $d/315a + 532$

$\Rightarrow d/19$ or 19 est premier donc :

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

$A \wedge B = 1$ ou $A \wedge B = 19$

4.2 L'algorithme d'Euclide.

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

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

L'algorithme d'Euclide.

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

$a = bq_1 + r_1$ si $r_1 \neq 0$ alors : $b = r_1q_2 + r_2$

si $r_2 \neq 0$ alors : $r_1 = r_2q_3 + r_3$

si $r_3 \neq 0$ alors :

.....

$r_{n-2} = r_{n-1}q_n + r_n$

si $r_n \neq 0$ alors : $r_{n-1} = r_nq_{n+1} + r_{n+1}$

si $r_{n+1} = 0$ on arrête le processus.

Et d'après la propriété précédente :

$a \wedge b = b \wedge r_1 = r_1 \wedge r_2 = \dots = r_{n-1} \wedge r_n = r_n$ car : $r_n | r_{n-1}$

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) En utilisant l'algorithme d'Euclide calculer : $67 \wedge 39$

2) en déduire deux nombres relatifs u et v tel que : $39u + 67v = 1$

Solution: 1)

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

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

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

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

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

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

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

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

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

Exercice 13:

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 $a \wedge b$.

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

Exercice14 : Montrer que : $\forall n \in \mathbb{N}^*$ on a :

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

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

5) Le plus petit multiple commun.

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 : $m = \text{PPCM}(a, b) = a \vee b$

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.

6) LA CONGRUENCE MODULO n

6.1) Définition et propriétés.

Solution :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 :

$$3^{2n+1} + 2^{n+2} \text{ est divisible par } 7$$

4) Montrer que pour tout n entier naturel,

$$5n^3 + n \text{ est divisible par } 6$$

5) Montrer que si n n'est pas un multiple de 7,

$$\text{alors : } n^6 - 1 \text{ est un multiple de } 7$$

6 Montrer que pour tout entier naturel, le nombre

$$n(n^2 + 5) \text{ est divisible par } 6$$

Exercice 19 : $x \in \mathbb{N}^*$ 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 $a \wedge b = b \wedge 7$

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 :1) on pose $d = x \wedge y$ et $d' = a \wedge b$ montrons que : $d = d'$

$$d = x \wedge y \text{ donc : } \Rightarrow d/x \text{ et } d/y \Rightarrow d/a \text{ et } d/b$$

Car il divise toute combinaison de x et y

$$\Rightarrow d/a \wedge b \Rightarrow d/d'$$

Inversement :

$$d' = a \wedge b \Rightarrow d'/a \text{ et } d'/b \Rightarrow d'/9x+4y \text{ et } d'/2x+y$$

$$\Rightarrow d'/(9x+4y) - 4(2x+y) \text{ et } d'/9(2x+y) - 2(9x+4y)$$

$$\Rightarrow d'/x \text{ et } d'/y \Rightarrow d'/x \wedge y \Rightarrow d'/d$$

ce qui entraine: $d = d'$

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

a) montrons que $a \wedge b = b \wedge 7$?

la division euclidienne de $n^2 + 5n + 13$ par $n + 3$

$$\text{donne : } n^2 + 5n + 13 = (n+3)(n+2) + 7$$

$$\text{Donc : } a = b(n+2) + 7 \Leftrightarrow a - b(n+2) = 7$$

on pose $d' = b \wedge 7$ et $d = a \wedge b$

montrons que : $d = d'$

$$d = a \wedge b \Rightarrow d/a \text{ et } d/b \Rightarrow d/a - b(n+2) \text{ et } d/b$$

$$\Rightarrow d/7 \text{ et } d/b \Rightarrow d/b \wedge 7 \Rightarrow d/d'$$

$$d' = b \wedge 7 \Rightarrow d'/7 \text{ et } d'/b \Rightarrow d'/b(n+2) + 7 \text{ et } d'/b$$

$$\Rightarrow d'/a \text{ et } d'/b \Rightarrow d'/a \wedge b \Rightarrow d'/d$$

ce qui entraine: $d = d'$

b) les valeurs possibles $a \wedge b = d$??

$$\text{on a : } a \wedge b = b \wedge 7 = d$$

$$\text{donc : } d/7 \text{ donc : } d = 1 \text{ ou } d = 7$$

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 : $a \wedge b = 1$??

$$a \wedge b = 1 \Leftrightarrow n \text{ n'est pas congrue a } 0 \text{ modulo } 4$$

$$n \equiv 0[7] \text{ ou } n \equiv 1[7] \text{ ou } n \equiv 2[7] \text{ ou } n \equiv 3[7] \text{ ou } n \equiv 5[7]$$

$$\text{ou } n \equiv 6[7]$$

8) Les classes d'équivalences.

8.1 Définition et propriété :

Définition : Soit n un entier naturel non nul.

L'ensemble des entiers relatifs qui ont le même

reste r dans 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 remarquer que $\bar{0} = \bar{7}$

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

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

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

8.2 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 $\bar{a} + \bar{b} = \overline{a+b}$

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

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

Exercice20 : Résoudre les équations

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

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

On Dresse une table comme suite :

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

Si $\bar{k} = \bar{0}$: $S = \{\bar{0}; \bar{2}\}$

Si $\bar{k} = \bar{1}$: $S = \{\bar{3}\}$

Si $\bar{k} = \bar{2}$: $S = \emptyset$

Si $\bar{k} = \bar{3}$: $S = \{\bar{1}\}$

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

suivants : $x + \bar{3}y = \bar{1}$

Solution : on Dresse une table des opérations de

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

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

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

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

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

Solution :

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

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

Exercice23 : 1) Dresser les tables des opérations de $\mathbb{Z} / 7\mathbb{Z}$

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

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

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

Propriété : Si p est premier alors

dans $\mathbb{Z} / p\mathbb{Z}$ on a :

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

Preuve : Après la décomposition.

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

9.1) 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 a une décomposition de la forme

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

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

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

Exercice 24:

- 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

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

$$\text{où } (\forall i \in \llbracket 1, n \rrbracket) (\alpha_i \leq \beta_i)$$

2) Application de la décomposition.

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 on a : $a \wedge b = |a| \wedge |b|$

Exemple : Déterminer : $(-5664) \wedge (-984)$ et $324 \wedge (-144)$

Exercice25 :

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

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

Exercice26: $a = (25^n - 1)(36^n - 1)$ et $b = (5^n - 1)(6^n - 1)$

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

Solution :

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

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

II) THEOREMES PRINCIPAUX

1) Théorème de Bézout :

Théorème1 : Soient a et b et des entiers relatifs non nuls :

$$a \wedge b = d \Leftrightarrow \exists (\alpha, \beta) \in \mathbb{Z}^2; \begin{cases} a = \alpha d \\ b = \beta d \\ \alpha \vee \beta = 1 \end{cases}$$

Preuve : ($\Rightarrow$) On suppose que $a \wedge b = d$

On a $d|a$ et $d|b$ donc $\exists (\alpha, \beta) \in \mathbb{Z}^2$ tel que : $a = \alpha d$ et $b = \beta d$ donc : $d = \alpha d \wedge \beta d = |d|(\alpha \wedge \beta)$ et puisque $d \in \mathbb{N}^*$ alors $\alpha \wedge \beta = 1$

$$(\Leftarrow) \text{ On suppose que } \exists (\alpha, \beta) \in \mathbb{Z}^2; \begin{cases} a = \alpha d \\ b = \beta d \\ \alpha \vee \beta = 1 \end{cases}$$

On a : $a \wedge b = \alpha d \wedge \beta d = |d|(\alpha \wedge \beta) = d$

Car $(|d| = d \text{ et } \alpha \wedge \beta = 1)$ cqfd

Théorème2 : Soient a et b et des entiers relatifs non nuls : $a \wedge b = d \Rightarrow \exists (u, v) \in \mathbb{Z}^2 ; d = au + b$

Preuve :

1- Si $a|b$ alors $a \wedge b = |b|$

• si $b > 0$ alors $b = 0a + 1b$

• si $b < 0$ alors $b = 0a + (-1)b$

2- Si $b|a$ (même raisonnement)

3- On suppose que b ne divise pas a tel que :

$0 < b < a$ et d'après l'algorithme d'Euclide on a :

$$a = bq_0 + r_0$$

$$r_0 \neq 0 \text{ alors : } b = r_0q_1 + r_1$$

$$\text{si } r_1 \neq 0 \text{ alors : } r_0 = r_1q_2 + r_2$$

$$\text{si } r_2 \neq 0 \text{ alors :}$$

.....

$$r_{n-2} = r_{n-1}q_n + r_n$$

$$\text{si } r_n \neq 0 \text{ alors : } r_{n-1} = r_nq_{n+1} + r_{n+1}$$

$$\text{si } r_{n+1} = 0 \text{ on arrête le processus .}$$

Et d'après la propriété précédente :

$$a \wedge b = b \wedge r_1 = r_1 \wedge r_2 = \dots = r_{n-1} \wedge r_n = r_n$$

$$\text{car : } r_n|r_{n-1} \text{ et } 0 < r_n < r_{n-1} < \dots < r_1 < r_0 < b$$

$$\text{On obtient : } r_0 = a - bq_0 = u_0a + v_0b$$

$$\text{où } u_0 = 1 \text{ et } v_0 = -q_0$$

$$r_1 = b - r_0q_1 = b - (a - bq_0)q_1 =$$

$$= -aq_1 + b(1 + q_0q_1) = u_1a + v_1b$$

$$\text{Où } u_1 = -q_1 \text{ et } v_1 = (1 + q_0q_1)$$

On répète le processus et à chaque fois on

montre que : $r_k = au_k + bv_k$:

Cette opération est valable pour tous les reste r_k

En particulier pour le dernier reste r_n qui est :

$a \wedge b$ donc :

$$\exists (u_n, v_n) \in \mathbb{Z}^2; a \wedge b = au_n + bv_n.$$

Remarque : 1) Dans l'écriture $\exists (u, v) \in \mathbb{Z}^2 :$

$a \wedge b = au + bv$ le couple (u, v) n'est pas unique.

Ex : on a : $12 \wedge 9 = 3$

$$\text{et on a } 3 = 1 \times 12 + (-1) \times 9$$

$$\text{et } 3 = (-2) \times 12 + 3 \times 9$$

2) La réciproque du théorème n'est pas vraie :

$$2 \times 12 + (-2) \times 9 = 6 \text{ mais } 12 \wedge 9 = 3 \neq 6$$

Théorème (Théorème de Bézout)

Soient a et b et des entiers relatifs non nuls :

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

Preuve : ($\Rightarrow$) C'est le théorème précédent.

($\Leftarrow$) On suppose que $1 = au + bv$

Soit $d = a \wedge b$ on aura : $d|a$ et $d|b$

$$\text{Donc : } d|ua \text{ et } d|vb \text{ par suite } d|ua + vb = 1$$

$$\text{Donc } d = 1 (d \in \mathbb{N}^*) \text{ et donc } a \wedge b = 1$$

Exemples :

$$1) (5n + 3) \wedge (2n + 1) = 1$$

$$\text{Car : } 2 \times (5n + 3) + (-5) \times (2n + 1) = 1$$

$$2) (n + 2) \wedge (n^2 + 2n - 1) = 1$$

$$\text{Car } n \times (n + 2) + (-1) \times (n^2 + 2n - 1) = 1$$

Exercice27 : montrer que : $\forall n \in \mathbb{N}$

$$(3n+1) \wedge (7n+2) = 1$$

$$\text{Solution: on a : } 7(3n+1) - 3(7n+2) = 1$$

$$\text{Donc : } \exists (u; v) \in \mathbb{Z}^2 \text{ tel que}$$

$$u(3n+1) + v(7n+2) = 1 \quad u = 7 \text{ et } v = -3$$

Donc d'après le théorème de Bézout on a :

$$(3n+1) \wedge (7n+2) = 1$$

Application 1 : L'utilisation de l'algorithme

d'Euclide pour déterminer les coefficients de

Bézout

Exemple : Montrons que : $360 \wedge 84 = 12$ et

déterminer u et v dans $\mathbb{Z}$ tels que :

$$360u + 84v = 12$$

$$\text{Solution : on a : } 360 = 2^3 \cdot 3^2 \cdot 5 \text{ et } 84 = 2^2 \cdot 3 \cdot 7$$

$$\text{Donc } 360 \wedge 84 = 2^2 \cdot 3 = 12$$

$$\text{D'autre part : } 360 = 84 \times 4 + 24 \text{ donc :}$$

$$24 = a - (b \times 4)$$

$$\text{On a : } 84 = 24 \times 3 + 12$$

$$\text{Donc : } b - (a - (b \times 4)) \times 3 = 12$$

$$\text{On a : } 24 = 12 \times 2 + 0$$

$$\text{Donc : } -3a + 13b = 12$$

Application 2 : détermination d'une solution

particulière de l'équation de la forme :

$$(E) : ax + by = 1$$

Exemple : Considérons dans $\mathbb{Z}^2$ l'équation

(E): $17x + 36y = 1$ et déterminons une solution

particulière de (E).

Solution : On a $17 \wedge 36 = 1$ donc d'après le

théorème de Bézout ; il existe u et v tels que :

$$17u + 36v = 1 \text{ donc (E) admet une solution.}$$

On pose $a = 36$ et $b = 17$ on obtient :

$$a = 2b + 2 \text{ et } b = 8 \times 2 + 1$$

$$\text{Donc : } 2 = a - 2b \text{ et } b = 8 \times (a - 2b) + 1$$

$$\text{D'où : } -8a + 17b = 1$$

Donc le couple $(-8, 17)$ est une solution de

l'équation (E).

2) Application du théorème de Bézout :

Théorème de Gauss :

Soient a, b et c des entiers relatifs non nuls :

$$\begin{cases} c|ab \\ c \vee a = 1 \end{cases} \Rightarrow c|b$$

Preuve : On a : $c \wedge a = 1$ d'après le théorème de Bézout : $(\exists(u, v) \in \mathbb{Z}^2)(au + vc = 1)$

d'où $bau + bvc = b$

Et puis que $c|ab$ alors $ab = kc$ (où $k \in \mathbb{Z}$) donc

$kcu + bvc = b$ d'où $c(ku + bv) = b$

et $ku + bv \in \mathbb{Z}$ donc $c|b$.

Remarque :

La condition $c \wedge a = 1$ dans le théorème de Gauss est indispensable ; $6|4 \times 3$

Mais $6 \nmid 3$ et $6 \nmid 4$

Théorème : Soient a, b et c des entiers relatifs

$$\text{non nuls : } \begin{cases} a/c \text{ et } b/c \\ a \vee b = 1 \end{cases} \Rightarrow ab/c$$

Preuve : On a : $a|c$ et $b|c$ donc ils existent k et h tels que : $c = ka = hb$ et puisque $a \wedge b = 1$ alors : $(\exists(u, v) \in \mathbb{Z}^2)(au + vb = 1)$

Donc : (en multipliant par c) $c = cau + cvb$

Donc : $c = hbau + kavb$

Donc : $c = ab(hu + kv)$ et par suite $ab|c$

Remarque : La condition $c \wedge b = 1$ dans le théorème précédent est indispensable.

Ex : $6|12$ et $3|12$ mais $6 \times 3 = 18 \nmid 12$.

Exercice28 : résoudre dans $\mathbb{Z}^2$ l'équation suivante : $(E) \quad 7(x-2) = 3(y+1)$

$$\text{Solution : } 7(x-2) = 3(y+1) \Leftrightarrow 7/3(y+1)$$

Or on sait que : $7 \wedge 3 = 1$

Donc d'après le théorème de Gauss : $7/y+1$

$$\text{Donc } \exists k \in \mathbb{Z} / y+1 = 7k \Leftrightarrow \exists k \in \mathbb{Z} / y = 7k-1$$

$$(E) \Leftrightarrow \begin{cases} 7(x-2) = 3(y+1) \\ \exists k \in \mathbb{Z} / y = 7k-1 \end{cases} \Leftrightarrow \begin{cases} 7(x-2) = 3 \times 7k \\ \exists k \in \mathbb{Z} / y = 7k-1 \end{cases}$$

$$\Leftrightarrow \begin{cases} x-2 = 3k \\ \exists k \in \mathbb{Z} / y = 7k-1 \end{cases} \Leftrightarrow \begin{cases} x = 3k+2 \\ \exists k \in \mathbb{Z} / y = 7k-1 \end{cases}$$

$$\text{Donc } S = \{(3k+2; 7k-1) / k \in \mathbb{Z}\}$$

Exercice29 : déterminer l'entier naturel n

$$\text{tel que : } \frac{n(n^2+3n-2)}{n+1} \in \mathbb{N}$$

$$\text{Solution : } 1) \quad \frac{n(n^2+3n-2)}{n+1} \in \mathbb{N} \Leftrightarrow \frac{n+1}{n(n^2+3n-2)} \text{ or}$$

$$\text{on a : } 1 = (n+1) \wedge n \text{ car } (n+1) - n = 1 \text{ (bezout)}$$

$$\text{Donc : } \frac{n+1}{n^2+8n-2}$$

La division euclidienne de n^2+3n-2 par $n+1$

$$\text{Donne : } n^2+3n-2 = (n+1)(n+2) - 4$$

$$\frac{n+1}{n^2+3n-2} \stackrel{\text{et } n+1}{\Rightarrow} \frac{n+1}{n^2+3n-2-(n+1)(n+2)} \\ \Rightarrow \frac{n+1}{-4} \Rightarrow \frac{n+1}{4}$$

Il faut que $n+1 \in \{1; 2; 4\}$ ce qui entraîne :

$$n \in \{0; 1; 3\}$$

Inversement : On vérifie que $0; 1; 3$ vérifient

$$\frac{n(n^2+3n-2)}{n+1} \in \mathbb{N} \text{ Avant de conclure que : } \\ \frac{n(n^2+3n-2)}{n+1} \in \mathbb{N} \Leftrightarrow n \in \{0; 1; 3\}$$

Propriétés : Soient a, b et c des entiers relatifs non nuls :

$$1) \begin{cases} a \vee b = 1 \\ a \vee c = 1 \end{cases} \Leftrightarrow a \vee (bc) = 1$$

$$2) a \wedge b = 1 \Leftrightarrow a \wedge b^n = 1 \quad (n \in \mathbb{N}^*)$$

$$3) a \wedge b = 1 \Leftrightarrow a^n \wedge b^m = 1 \quad (n \in \mathbb{N}^*) \text{ et } (m \in \mathbb{N}^*)$$

Preuve :

$$1)(\Rightarrow) \text{ On suppose que } \begin{cases} a \vee b = 1 \\ a \vee c = 1 \end{cases} \text{ donc :}$$

$$(\exists(u, v) \in \mathbb{Z}^2)(au + vb = 1)$$

$$(\exists(\alpha, \beta) \in \mathbb{Z}^2)(a\alpha + \beta c = 1)$$

Par le produit on obtient : $(au + vb)(a\alpha + \beta c) = 1$; d'où après développement on obtient :

$$a^2u\alpha + au\beta c + vb\alpha a + vb\beta c = 1$$

$$\text{et donc } (au\alpha + u\beta c + vb\alpha)a + (v\beta)bc = 1$$

$$\text{Donc : d'après Bézout } a \wedge bc = 1$$

$$(\Leftarrow) \text{ On suppose que } a \wedge bc = 1$$

$$\text{Donc } (\exists(u, v) \in \mathbb{Z}^2)(au + vbc = 1)$$

D'où $au + (vb)c = 1$ donc :

$$a \wedge c = 1 \text{ et } au + (vc)b = 1 \text{ donc } a \wedge b = 1$$

2)($\Rightarrow$) On suppose que $a \wedge b = 1$ et on montre par récurrence que : $a \wedge b^n = 1$

• Pour $n = 1$ la propriété est vraie.

• On suppose que la propriété est vraie pour n

• On montre qu'elle est vraie pour $n + 1$

$$\text{On a : } \begin{cases} a \vee b^n = 1 \\ a \vee b = 1 \end{cases} \Rightarrow a \vee (b^n \times b) = 1 \text{ d'après 1)}$$

d'où $a \wedge b^{n+1} = 1$ Donc si $a \wedge b = 1$ alors :

$$a \wedge b^n = 1 \text{ pour tout } n \text{ dans } \mathbb{N}^*$$

($\Leftarrow$) On suppose que $a \wedge b^n = 1$ donc et d'après le théorème de Bézout $(\exists(u, v) \in \mathbb{Z}^2)(au + vb^n = 1)$

$$\text{Donc : } au + (vb^{n-1})b = 1 \text{ donc } (\exists(u', v') \in \mathbb{Z}^2)$$

$$(au' + v'b = 1) \text{ et par suite } a \wedge b = 1$$

3) Est un résultat immédiat de 2)

Exercice30: 1) Montrer que : $\forall a \in \mathbb{Z}^*$ et $\forall b \in \mathbb{Z}^*$

$$\text{on a : } a \wedge b = 1 \Rightarrow \begin{cases} a \wedge (a+b) = 1 \\ b \wedge (a+b) = 1 \\ a \wedge b(a+b) = 1 \\ (a+b) \wedge ab = 1 \end{cases}$$

Solution: on pose $d = a \wedge (a+b)$

montrons que : $d = 1$

$$d = a \wedge b \Rightarrow \frac{d}{a} \text{ et } \frac{d}{a+b} \Rightarrow \frac{d}{a} \text{ et } \frac{d}{a+b-a} \\ \Rightarrow \Rightarrow \frac{d}{a} \text{ et } \frac{d}{b} \Rightarrow \frac{d}{b \wedge a} \Rightarrow \frac{d}{1} \Rightarrow d = 1$$

ce qui entraîne: $1 = a \wedge (a+b)$ (1)

de même on montre que : $1 = b \wedge (a+b)$ (2)

de (1) et (2) en déduit que : $(a+b) \wedge ab = 1$

D'après une proposition

Et on a $a \wedge (a+b) = 1$ et $a \wedge b = 1$ donc

$a \wedge b(a+b) = 1$ D'après la même proposition

Exercice31 : Montrer que : $\forall n \in \mathbb{N}$

$$(2n+5) \wedge (n^2+5n+6) = 1$$

Solution : on a : $n^2+5n+6 = (n+2)(n+3)$

Et on a : $(2n+5) - 2(n+2) = 1$

Donc d'après le théorème de Bézout

$$(n+2) \wedge (2n+5) = 1 \quad (1)$$

De même : on a : $2(n+3) - (2n+5) = 1$

Donc d'après le théorème de Bézout

$$(n+3) \wedge (2n+5) = 1 \quad (2)$$

de (1) et (2) en déduit que

$$(2n+5) \wedge ((n+3)(n+2)) = 1$$

Donc : $(2n+5) \wedge (n^2+5n+6) = 1$

3) L'équation $ax + by = c$

Théorème : (fondamental)

L'équation (E) : $ax + by = c$ admet une solution si et seulement si $(a \wedge b) | c$

Preuve :

($\Leftarrow$) On suppose que $d = (a \wedge b) | c$ alors :

$(\exists k \in \mathbb{Z})(c = kd)$ et on a :

$(\exists (u, v) \in \mathbb{Z}^2)(au + vb = d)$

$$kd = k(a \wedge b) = (ku)a + (kv)b$$

C'est-à-dire : $c = (ku)a + (kv)b$

donc l'équation (E) admet (x_0, y_0) comme solution où $x_0 = ku$ et $y_0 = kv$

($\Rightarrow$) Inversement : On suppose que : $ax + by = c$

admet une solution (x_0, y_0) , donc: $a \cdot x_0 + b \cdot y_0 = c$

Puisque : $(a \wedge b) | a$ et $(a \wedge b) | b$

alors $(a \wedge b) | x_0 \cdot a$ et $(a \wedge b) | y_0 \cdot b$

donc $(a \wedge b) | (x_0 \cdot a + y_0 \cdot b) = c$

donc : $(a \wedge b) | c$.

Théorème : Si le couple $(x_0; y_0)$ est une solution de l'équation (E) : $ax + by = c$ alors, l'ensemble des solutions de (E) est :

$$S = \left\{ \left(x_0 + \frac{kb}{a \wedge b}; y_0 - \frac{ka}{a \wedge b} \right); k \in \mathbb{Z} \right\}$$

Preuve : On pose : $A = \left\{ \left(x_0 + \frac{kb}{a \wedge b}; y_0 - \frac{ka}{a \wedge b} \right); k \in \mathbb{Z} \right\}$

et on montre que : $A \subset S$ et $S \subset A$?

1) Montrons que $A \subset S$: il suffit de montrer que le

couple $\left(x_0 + \frac{kb}{a \wedge b}; y_0 - \frac{ka}{a \wedge b} \right)$ est solution de

l'équation (E) : On a :

$$a \left(x_0 + \frac{kb}{a \wedge b} \right) + b \left(y_0 - \frac{ka}{a \wedge b} \right)$$

$$= ax_0 + \frac{kab}{a \wedge b} + by_0 - \frac{kba}{a \wedge b} = ax_0 + by_0 = c$$

Donc le couple $\left(x_0 + \frac{kb}{a \wedge b}; y_0 - \frac{ka}{a \wedge b} \right)$ (pour $k \in \mathbb{Z}$)

est solution : d'où : $A \subset S$.

2) On suppose que le couple $(x, y) \in S$

Donc (x, y) est solution de l'équation (E)

d'où $ax + by = c$; or : $(x_0; y_0)$ est une solution de

l'équation (E) donc : $ax_0 + by_0 = c$

Donc (la différence membre à membre) donne :

$$a(x - x_0) = -b(y - y_0)$$

Soit $d = a \wedge b$ on a : $(\exists (\alpha, \beta) \in \mathbb{Z}^2)$

$a = \alpha d$ et $b = \beta d$ et $\alpha \wedge \beta = 1$

Donc : $(x, y) \in S \Leftrightarrow a(x - x_0) = -b(y - y_0)$

$$\Leftrightarrow \alpha d(x - x_0) = -\beta d(y - y_0)$$

$$\Leftrightarrow \alpha(x - x_0) = -\beta(y - y_0) \quad (*) \quad (d \neq 0)$$

On conclut que : $\beta | \alpha(x - x_0)$ et puisque :

$\alpha \wedge \beta = 1$ alors (d'après T. Gauss) $\beta | (x - x_0)$

Donc $(\exists k \in \mathbb{Z})(x - x_0) = k\beta$

et par suite : $(*) \alpha k\beta = -\beta(y - y_0)$

d'où : $y - y_0 = -k\alpha$ Par suite :

$$(x, y) \in S \Leftrightarrow (y - y_0) = -k\alpha \text{ et } (x - x_0) = k\beta$$

où $k \in \mathbb{Z}$

en remplaçant α par $\frac{a}{d}$ et β par $\frac{b}{d}$ on obtient :

$$(x, y) \in S \Leftrightarrow x = x_0 + \frac{kb}{d} \text{ et } y = y_0 - \frac{ka}{d} \quad \text{cqfd}$$

Exemple : Considérons l'équation :

$$(E): 756x - 245y = 14$$

1- Montrer l'équation (E) admet une solution.

2- Déterminer une solution particulière de (E)

3- Résoudre l'équation (E)

Solution : $756 = 2^2 \times 3^3 \times 7$ et $245 = 5 \times 7^2$

1) On a : $756 \wedge 245 = 7$ et $7|14$ donc l'équation (E) admet une solution dans $\mathbb{Z}^2$

2- En utilisant l'algorithme d'Euclide on obtient :

$$a = 756 \text{ et } b = 245$$

$$a = 3 \times b + 21$$

$$b = 11 \times 21 + 14$$

$$21 = 14 + 7$$

$$\text{On a donc : } 21 = a - 3b$$

$$b = 11 \times (a - 3b) + 14 \Leftrightarrow 14 = 34b - 11a$$

$$7 = (a - 3b) - (34b - 11a) \Leftrightarrow 7 = 12a - 37b$$

Finalement : $14 = 24a - 74b$ et donc le couple $(24, 74)$ est une solution particulière de (E)

$$\text{D'où : } S = \left\{ \left(24 - \frac{245}{7}k; 74 - \frac{756}{7}k \right); k \in \mathbb{Z} \right\}$$

$$S = \left\{ (24 - 35k; 74 - 108k); k \in \mathbb{Z} \right\}$$

$$S = \left\{ (24 + 35k; 74 + 108k); k \in \mathbb{Z} \right\}$$

4) La congruence modulo n, complément.

Théorème : Soient a, b et c des entiers relatifs non nuls. et $n \in \mathbb{N}^*$ et $d = n \wedge c$ on a :

$$ac \equiv bc [n] \Leftrightarrow a \equiv b \left[\frac{n}{d} \right]$$

Preuve : $(\Rightarrow)$ On suppose : $ac \equiv bc [n]$,

$$\text{donc } n|(ac - bc) = c(a - b) \text{ donc } \frac{n}{d} | \frac{c}{d} (a - b)$$

et comme $\frac{n}{d} \wedge \frac{c}{d} = 1$ Alors : (D'après théorème de

$$\text{Gauss}) \frac{n}{d} | (a - b) \text{ donc : } a \equiv b \left[\frac{n}{d} \right]$$

$$(\Leftarrow) \text{ On suppose que : } a \equiv b \left[\frac{n}{d} \right]$$

$$\text{donc } a = b + k \frac{n}{d} \quad (k \in \mathbb{Z}) \text{ donc } da = db + kn$$

$$(d = n \wedge c \Rightarrow c = ad)$$

$$\text{Donc : } ada = adb + \alpha kn$$

$$\text{D'où } ca = cb + hn \text{ donc } ac \equiv bc [n].$$

Propriété :

$$1) \begin{cases} ac \equiv bc [n] \\ c \vee n = 1 \end{cases} \Rightarrow a \equiv b [n]$$

$$2) \begin{cases} a \equiv b [n] \\ m | n \end{cases} \Rightarrow a \equiv b [m]$$

$$3) \begin{cases} ac \equiv bc [p] \\ p \text{ premier et } p \nmid c \end{cases} \Rightarrow a \equiv b [p]$$

Preuve : Ce sont des résultats immédiats du théorème précédent.

Exercice32 : déterminer dans $\mathbb{N}^2$ les couples

$$(x; y) / \begin{cases} x + y = 48 \\ x \wedge y = 4 \end{cases} \text{ avec } x \leq y$$

$$\text{Solution : } \begin{cases} x + y = 48 \\ x \wedge y = 4 \end{cases} \Leftrightarrow \exists (x'; y') \in \mathbb{N}^2 / \begin{cases} x = 4x' \\ y = 4y' \\ x + y = 48 \end{cases}$$

$$\Leftrightarrow \exists (x'; y') \in \mathbb{N}^2 / 4x' + 4y' = 48$$

$$\Leftrightarrow \exists (x'; y') \in \mathbb{N}^2 / x' + y' = 12$$

On Dresse une table comme suit :

x'	0	1	2	3	4	5	6
y'	12	11	10	9	8	7	6
x	0	4	8	12	16	20	24
y	48	44	40	36	32	28	24

Donc :

$$S = \{(0; 48); (4; 44); (8; 40); (12; 36); (16; 32); (20; 28); (24; 24)\}$$

Exercice33: résoudre dans $\mathbb{Z}$ le système

$$\text{suivant: } \begin{cases} 2x \equiv 3 [7] \\ 3x \equiv 1 [5] \end{cases}$$

$$\text{Solution: } \begin{cases} 2x \equiv 3 [7] \\ 3x \equiv 1 [5] \end{cases} \Leftrightarrow \begin{cases} 2x \equiv -4 [7] \\ 3x \equiv 1 [5] \end{cases} \Leftrightarrow \begin{cases} x \equiv -2 [7] \\ 3x \equiv 1 [5] \end{cases}$$

$$\text{Car } 2 \wedge 7 = 1$$

$$\Leftrightarrow \begin{cases} x \equiv 5 [7] \\ 3x \equiv 1 [5] \end{cases} \Leftrightarrow \begin{cases} x = 5 + 7k; k \in \mathbb{Z} \\ 3x \equiv 1 [5] \end{cases}$$

$$\Leftrightarrow \begin{cases} x = 5 + 7k; k \in \mathbb{Z} \\ 3(5 + 7k) \equiv 1 [5] \end{cases} \Leftrightarrow \begin{cases} x = 5 + 7k; k \in \mathbb{Z} \\ k \equiv 1 [5] \end{cases} \Leftrightarrow \begin{cases} x = 5 + 7k; k \in \mathbb{Z} \\ k = 1 + 5k' \end{cases}$$

$$\Leftrightarrow x = 5 + 7(1 + 5k'); k' \in \mathbb{Z} \Leftrightarrow x = 35k' + 12; k' \in \mathbb{Z}$$

$$S = \{35k' + 12; k' \in \mathbb{Z}\}$$

5) Le P.G.D.C et le P.P.M.C de plusieurs nombres.

Définition : Soient $a_1, a_2, \dots, a_n$ des entiers relatifs non nuls, le plus grand entier naturel d qui divise en même temps tous les nombres $a_1, a_2, \dots, a_n$ s'appelle le plus grand diviseur commun des nombres $a_1, a_2, \dots, a_n$ et se note : $d = a_1 \wedge a_2 \wedge \dots \wedge a_n$

Théorème : Soient $a_1, a_2, \dots, a_n$ des entiers relatifs non nuls ; on a :

$$a_1 \wedge a_2 \wedge \dots \wedge a_n = (a_1 \wedge a_2 \wedge \dots \wedge a_{n-2}) \wedge (a_{n-1} \wedge a_n)$$

Exemple :

$$756 \wedge 350 \wedge 616 = 756 \wedge (350 \wedge 616) \\ = 756 \wedge 14 = 14$$

Théorème (Généralisation de Bézout)

Si $d = a_1 \wedge a_2 \wedge \dots \wedge a_n$ alors $\exists (\alpha_i)_{1 \leq i \leq n}$ telle que

$$: d = \sum_{i=1}^n \alpha_i a_i$$

Preuve : par récurrence

Définition : On dit que les entiers relatifs non nuls : $a_1, a_2, \dots, a_n$ sont premiers entre eux si : $a_1 \wedge a_2 \wedge \dots \wedge a_n = 1$

Remarque : Les entiers relatifs non nuls $a_1, a_2, \dots, a_n$ sont premiers entre eux ne veut pas dire que les entiers $a_1, a_2, \dots, a_n$ sont premiers entre eux deux à deux.

Exemple : 3, 5 et 6 sont premiers entre eux. Alors que : 3 et 6 ne sont pas premiers entre eux.

Théorème (Généralisation de Bézout)

$a_1 \wedge a_2 \wedge \dots \wedge a_n = 1$ si et seulement si

$$\exists (\alpha_i)_{1 \leq i \leq n} \text{ telle que : } 1 = \sum_{i=1}^n \alpha_i a_i$$

Définition : Soient $a_1, a_2, \dots, a_n$ des entiers relatifs non nuls, le plus petit entier naturel m qui est multiple en même temps tous les nombres $a_1, a_2, \dots, a_n$ s'appelle le plus petit multiple commun des nombres $a_1, a_2, \dots, a_n$ et se note : $m = a_1 \vee a_2 \vee \dots \vee a_n$

Exercice 34 : montrer que l'ensemble des solutions du système suivant est non vide :

$$\begin{cases} n \equiv 2[11] \\ n \equiv 3[7] \end{cases}$$

Solution :

$$\begin{cases} n \equiv 2[11] \\ n \equiv 3[7] \end{cases} \Leftrightarrow \exists (x; y) \in \mathbb{Z}^2 / \begin{cases} n = 11x + 2 \\ n = 7y + 3 \end{cases}$$

$$\Leftrightarrow \exists (x; y) \in \mathbb{Z}^2 / 11x + 2 = 7y + 3$$

$$\Leftrightarrow \exists (x; y) \in \mathbb{Z}^2 / 11x - 7y = 1$$

Or on sait que : $7 \wedge 11 = 1$

Donc d'après le théorème de Bézout :

$$\exists (u; v) \in \mathbb{Z}^2 / 11u + 7v = 1$$

Donc il suffit de prendre : $\begin{cases} x = u \\ y = -v \end{cases}$

$$\text{Donc } \exists (x; y) \in \mathbb{Z}^2 / \begin{cases} n = 11x + 2 \\ n = 7y + 3 \end{cases}$$

Par suite : l'ensemble des solutions du système est non vide

Exercice 35 : résoudre dans $\mathbb{Z}^2$ l'équation suivante: (E) $5x - 3y = 1$

Solution : On a : $5 \times 2 - 3 \times 3 = 1$ donc (2;3) est une solution particulière de l'équation

$$\text{Donc : } 5x - 3y = 5 \times 2 - 3 \times 3$$

$$\text{Donc : } 5(x - 2) = 3(y - 3) \Rightarrow 5/3(y - 3)$$

Or on sait que : $5 \wedge 3 = 1$

Donc d'après le théorème de Gauss : $5/y - 3$

$$\text{Donc } \exists k \in \mathbb{Z} / y - 3 = 5k \Leftrightarrow \exists k \in \mathbb{Z} / y = 5k + 3$$

$$(E) \Leftrightarrow \begin{cases} 5(x - 2) = 3(y - 3) \\ \exists k \in \mathbb{Z} / y = 5k + 3 \end{cases} \Leftrightarrow \begin{cases} 5(x - 2) = 3 \times 5k \\ \exists k \in \mathbb{Z} / y = 5k + 3 \end{cases}$$

$$\begin{cases} x - 2 = 3k \\ \exists k \in \mathbb{Z} / y = 5k + 3 \end{cases} \Leftrightarrow \exists k \in \mathbb{Z} / \begin{cases} x = 3k + 2 \\ y = 5k + 3 \end{cases}$$

$$\text{Donc } S = \{(3k + 2; 5k + 3) / k \in \mathbb{Z}\}$$

6) Propriétés des nombres premiers.

Théorème :

1) Si p et q sont des nombres premiers positifs alors ils sont premiers entre eux.

2) Si p est premier alors il est premier avec tout nombre entier non nul a tel que $p \nmid a$

Remarque :

La réciproque de 1) n'est pas vraie ; 14 et 9 sont premiers entre eux mais aucun d'eux n'est premier.

Propriétés :

$$1) \begin{cases} p \mid ab \\ p \text{ premier et } p \nmid a \end{cases} \Rightarrow p \mid b$$

$$2) \begin{cases} p \mid ab \\ p \text{ premier} \end{cases} \Rightarrow p \mid a \text{ ou } p \mid b$$

$$3) \begin{cases} p \mid \prod_{i=1}^n a_i \\ p \text{ premier} \end{cases} \Rightarrow \exists 1 \leq i \leq n \text{ } p \mid a_i$$

$$4) \begin{cases} p \mid \prod_{i=1}^n p_i \\ p \text{ premier} \\ \forall 1 \leq i \leq n; p_i \text{ premier} \end{cases} \Rightarrow \exists 1 \leq i \leq n; p = p_i$$

7) Le petit théorème de Fermat.

Théorème : Si p est un nombre premier et a un entier relatif non nul et pas divisible par p alors :

$a^{p-1} - 1$ est divisible par p c'est-à-dire a

$$a^{p-1} \equiv 1[p] \text{ ou encore : } a^p \equiv a[p]$$

Preuve : Soient p un nombre premier et k un entier naturel tel que $1 \leq k \leq p - 1$

On a p premier et $p > k$ donc $p \nmid k$ et par suite $p \wedge k = 1$ d'autre part :

$$kC_p^k = k \frac{p!}{k!(p-k)!} = \frac{p(p-1)!}{(k-1)!(p-k)!} = pC_{p-1}^{k-1}$$

Donc p/kC_p^k et comme $p \wedge k = 1$ alors d'après

T. Gauss p/C_p^k

$$\text{Montrons que } p \mid (a+1)^p - a^p - 1?$$

D'après la formule de binôme On a :

$$(a+1)^p = a^p + C_p^1 a^{p-1} + C_p^2 a^{p-2} + \dots + C_p^{p-1} a^1 + 1$$

Donc $(a+1)^p - a^p - 1 = C_p^1 a^{p-1} + C_p^2 a^{p-2} + \dots + C_p^{p-1} a^1$

Et comme p/C_p^k pour $1 \leq k \leq p-1$

Alors : $p/(a+1)^p - a^p - 1$

On a donc : $(a+1)^p - a^p - 1 \equiv 0[p]$

donc : $(a+1)^p - 1 \equiv a^p[p]$

Montrons par récurrence sur a (On prend pour le moment $a \in \mathbb{N}$) que $a^p \equiv a[p]$?

a) Pour $a = 0$ la propriété est vraie car $0 \equiv 0[p]$

b) On suppose que la propriété est vraie pour a c'est-à-dire $a^p \equiv a[p]$

c) Montrons que la propriété est vraie pour $(a+1)$ c'est-à-dire $(a+1)^p \equiv a+1[p]$?

On a : d'après les questions précédentes

$(a+1)^p - 1 \equiv a^p[p]$ Or d'après H.R : $a^p \equiv a[p]$

donc : $(a+1)^p \equiv a+1[p]$

Donc $(\forall a \in \mathbb{N})(\forall p \in \mathbb{P})(a^p \equiv a[p])$

Si $a < 0$ alors $-a > 0$:

o Si $p = 2$ on aura $a^2 = (-a)^2 \equiv (-a)[2]$

et $-a \equiv a[2]$ car $(2|(a - (-a)) = 2a)$

o si $p \geq 3$ alors p est impaire et $(-a)^p = -a^p$ et

$(-a)^p \equiv -a[p]$ on en déduit que $-a^p \equiv -a[p]$ et

finalement $a^p \equiv a[p]$ D'où le théorème.

Exemple : Montrons que : $(\forall n \geq 2) : n^5 \equiv n[30]$

Solution : On a : d'après le petit théorème de Fermat : $n^5 \equiv n[5]$ Donc : $5/n^5 - n$

D'autre part : $n^5 - n = n(n^4 - 1) = n((n^2)^2 - 1)$

$n^5 - n = n(n^4 - 1) = n(n-1)(n+1)(n^2 + 1)$

Donc $2|n(n-1)$ et $3|(n-1)n(n+1)$ et puisque 2 et 3 sont premiers alors $6 = (2 \times 3)$ divise $n^5 - n$

Finalement :

$$\begin{cases} 5/n^5 - n \\ 6/n^5 - n \Rightarrow 30 = 6 \times 5/n^5 - n \\ 6 \wedge 5 = 1 \end{cases}$$

Donc : $n^5 \equiv n[30]$

III) SYSTEMES DE NUMERATION

1) Théorème et définition

Théorème : Soit b un entier naturel tel que: $b > 1$

Chaque entier naturel non nul n s'écrit d'une façon unique de la forme :

$$n \equiv a_m b^m + a_{m-1} b^{m-1} + \dots + a_1 b^1 + a_0$$

Où : les $(a_i)_{1 \leq i \leq n}$ sont des entiers naturels

$0 \leq a_i \leq b-1$ et $a_m \neq 0$

Preuve : En utilisant la division Euclidienne de n par b on obtient : $n = q_1 b + a_0$ où $0 \leq a_0 < b$

• Si $q_1 \leq b-1$ on s'arrête et $a_1 = q_1$

• si $q_1 \geq b$, On effectue une autre division Euclidienne de q_1 sur b on obtient: $q_1 = q_2 b + a_1$ et par suite :

$$n = (q_2 b + a_1) b + a_0 = q_2 b^2 + a_1 b + a_0.$$

- Si $q_2 \leq b-1$ on s'arrête et $a_2 = q_2$

- Si non on continue le processus

Notation :

Si $n \equiv a_m b^m + a_{m-1} b^{m-1} + \dots + a_1 b^1 + a_0$ on écrit :

$$n \equiv \overline{a_m a_{m-1} \dots a_1 a_0}_{(b)}$$
 Cette écriture s'appelle

l'écriture de l'entier n dans la base b

Exemple1 : Le nombre $n = 2987$ s'écrit

$$n = \overline{2987}_{(10)}$$

$$\text{Car : } n = 2 \times 10^4 + 9 \times 10^3 + 8 \times 10^2 + 7$$

Essayons d'écrire n dans la base 6 :

$$\text{On a : } 2987 = 6 \times 497 + 5$$

$$497 = 6 \times 82 + 5$$

$$82 = 6 \times 13 + 4$$

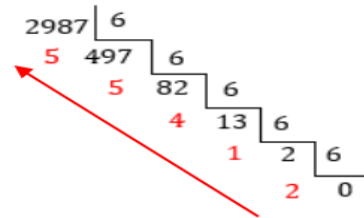
$$13 = 6 \times 2 + 1$$

$$2 = 6 \times 0 + 2$$

$$\text{Donc } 2987 = 2 \times 6^4 + 1 \times 6^3 + 4 \times 6^2 + 5 \times 6 + 5$$

$$n = \overline{21455}_{(6)}$$

Cette succession de divisions Euclidiennes se représente comme suite :



Exemple2 : soit $N = \overline{dcba}_{(10)}$ un entier naturel

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

Solution :

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

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

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

2) Les opérations dans une base de numération

2.1 La somme : On peut effectuer la somme dans une base donnée b par deux façons différentes :

a) **La décomposition :**

$$\overline{2534}_{(7)} + \overline{631}_{(7)} = 2 \times 7^3 + 5 \times 7^2 + 3 \times 7^1 + 4 \times 7^0 + 6 \times 7^2 + 3 \times 7^1 + 1 \times 7^0$$

$$\overline{2534}_{(7)} + \overline{631}_{(7)} = 2 \times 7^3 + 11 \times 7^2 + 6 \times 7^1 + 5 \times 7^0$$

$$\overline{2534}_{(7)} + \overline{631}_{(7)} = 3 \times 7^3 + 4 \times 7^2 + 6 \times 7^1 + 5 \times 7^0$$

$$\overline{2534}_{(7)} + \overline{631}_{(7)} = \overline{3465}_{(7)}$$

b) Calcul direct avec le retenu

2.2 Le produit :

Il est préférable d'effectuer le produit en utilisant le calcul direct avec le retenu car la décomposition risque d'être longue :

$$\text{Pour vérifier : } \overline{327}_{(8)} \times \overline{56}_{(8)}$$

$$= (3 \times 8^2 + 2 \times 8 + 7) \times (5 \times 8 + 6)$$

$$= 9890$$

$$= \overline{23242}_{(8)}$$

$$\begin{array}{r} 1 \\ \overline{2534}_{(7)} \\ + \overline{631}_{(7)} \\ \hline = \overline{3465}_{(7)} \end{array}$$

$$\begin{array}{r} 14 \\ 25 \\ \times \overline{327}_{(8)} \\ \hline \overline{56}_{(8)} \\ + 2412 \\ + 2063 \\ \hline = \overline{23242}_{(8)} \end{array}$$

2.3 Opérations dans différentes bases :

Pour effectuer des opérations dans différentes bases on développe les deux nombres dans la base 10 ; on effectue

L'opération et on écrit le résultat dans la base demandée.

Exemple : effectuer dans la base 9

$$\overline{6432}_{(7)} \times \overline{54}_{(8)}$$

$$\text{Solution : } \overline{6432}_{(7)} \times \overline{54}_{(8)} =$$

$$= (6 \times 7^3 + 4 \times 7^2 + 3 \times 7 + 2) \times (5 \times 8 + 4)$$

$$= 100188$$

$$= 1 \times 9^5 + 6 \times 9^4 + 2 \times 9^3 + 3 \times 9^2 + 8 \times 9 + 0$$

$$= \overline{162380}_{(9)}$$

IV) CRITERES DE DIVISIBILITE DES NOMBRES 5,25,3,9,11 ET 4

Théorème :

Soit x un entier naturel non nul tel que :

$$x \equiv a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 10^1 + a_0 \text{ où } 0 \leq a_i \leq 9 ;$$

on a :

$$1) x \equiv 0 [5] \Leftrightarrow a_0 = 0 \text{ ou } a_0 = 5$$

$$2) x \equiv 0 [25] \Leftrightarrow \overline{a_1 a_0} \in \{0, 25, 50, 75\}$$

$$3) x \equiv 0 [3] \Leftrightarrow \sum_{i=0}^n a_i \equiv 0 [3]$$

$$4) x \equiv 0 [9] \Leftrightarrow \sum_{i=0}^n a_i \equiv 0 [9]$$

$$5) x \equiv 0 [11] \Leftrightarrow \sum_{i=0}^n (-1)^i a_i \equiv 0 [11]$$

$$6) x \equiv 0 [4] \Leftrightarrow \overline{a_1 a_0} \equiv 0 [4]$$

V) L'ENSEMBLE $\mathbb{Z}/p\mathbb{Z}$ OU p EST UN NOMBRE PREMIER.

Théorème : Pour tous entiers relatifs non nuls a et n : $a \wedge n = 1 \Leftrightarrow (\exists m \in \mathbb{Z})(am = 1 [n])$

Preuve : ($\Rightarrow$) On suppose que : $a \wedge n = 1$, alors d'après T. Bézout $(\exists(m, u) \in \mathbb{Z}^2)(ma + un = 1)$

Donc : $(\exists(m, u) \in \mathbb{Z}^2)(un = 1 - ma)$

donc $n | ma - 1$ et finalement : $am = 1 [n]$

($\Leftarrow$) On suppose que : $(\exists m \in \mathbb{Z})(am = 1 [n])$ donc

$n | (am - 1)$ donc $(\exists k \in \mathbb{Z})(am - 1 = kn)$

donc : $am - kn = 1$ et d'après T. Bézout inverse

$a \wedge n = 1$

Théorème : Si p est un nombre premier positif

alors tout élément $\bar{x} \neq \bar{0}$ admet un inverse

dans $\mathbb{Z}/p\mathbb{Z}$

Preuve : Soit p un nombre premier positif ; on

pose : $E = \mathbb{Z}/p\mathbb{Z} - \{\bar{0}\}$

$$\bar{x} \in E \Leftrightarrow (\exists \alpha \in \{1, 2, \dots, p-1\}) / \bar{x} = \bar{\alpha}$$

(p étant, premier donc p ne divise aucun nombre de l'ensemble $\{1, 2, \dots, p-1\}$ d'où $p \wedge \alpha = 1$)

Et d'après la propriété précédente :

$$(\exists y \in \mathbb{Z}^*)(y\alpha \equiv 1[p])$$

$$\text{donc : } \bar{y} \times \bar{\alpha} = \bar{1} \text{ et comme } \bar{x} = \bar{\alpha} \text{ donc : } \bar{y} \times \bar{x} = \bar{1}$$

VI) Exercices :

Exercice 36 : soit p un nombre premier positif et

$$a \in \mathbb{N}^* \text{ et } p \wedge a = 1 \text{ on pose } F_p(a) = \frac{a^{p-1} - 1}{p}$$

1) vérifier que : $F_p(a) \in \mathbb{N}$

2) soit $b \in \mathbb{N}^*$ tel que : $p \wedge b = 1$

Démontrer que : $F_p(ab) \equiv F_p(a) + F_p(b) [p]$

Solution : 1) on a : $p \wedge a = 1$ et p un nombre

premier donc : d'après le théorème de Fermat :

$$a^{p-1} - 1 \equiv 0 [p] \text{ donc : } \frac{a^{p-1} - 1}{p} \in \mathbb{Z}$$

Donc : $F_p(a) \in \mathbb{N}$

2) d'après le théorème de Fermat :

$$a^{p-1} - 1 \equiv 0 [p] \text{ et } b^{p-1} - 1 \equiv 0 [p]$$

$$\text{Donc : } (a^{p-1} - 1)(b^{p-1} - 1) \equiv 0 [p^2]$$

$$\text{Donc : } (ab)^{p-1} - a^{p-1} - b^{p-1} + 1 \equiv 0 [p^2]$$

$$\text{Donc : } (ab)^{p-1} - 1 \equiv (a^{p-1} - 1) + (b^{p-1} - 1) [p^2]$$

$$\text{Donc : } \frac{(ab)^{p-1} - 1}{p} \equiv \frac{a^{p-1} - 1}{p} + \frac{b^{p-1} - 1}{p} [p]$$

$$\text{Donc : } F_p(ab) \equiv F_p(a) + F_p(b) [p]$$

Exercice 37 : soit $n \in \mathbb{Z}$ on pose :

$$u_n = 5n^7 + 7n^5 + 23n$$

1) Démontrer que : $u_n \equiv 0 [5]$

2) Démontrer que : $u_n \equiv 0 [7]$

3) en déduire que : $\frac{n^7}{7} + \frac{n^5}{5} + \frac{23n}{35} \in \mathbb{Z}$

Solution : 1)

on a : 5 est un nombre premier donc : d'après le théorème de Fermat : $n^5 \equiv n[5]$

et on a : $5n^7 \equiv 0[5]$ et $7n^5 \equiv 7n \equiv 2n[5]$

et $23n \equiv 3n[5]$

donc : $u_n = 5n^7 + 7n^5 + 23n \equiv 0[5]$

2) on a : 7 est un nombre premier donc : d'après le théorème de Fermat : $n^7 \equiv n[7]$

et on a : $5n^7 \equiv 5n[7]$ et $7n^5 \equiv 0[7]$

et $23n \equiv 2n[7]$ donc $u_n \equiv 7n[5]$

donc : $u_n \equiv 0[7]$

3) on a : $5/u_n$ et $7/u_n$ et $5 \wedge 7 = 1$

Donc : $5 \times 7 / u_n$ cad $35/u_n$

Donc : $\frac{u_n}{35} \in \mathbb{Z}$ donc : $\frac{5n^7 + 7n^5 + 23n}{35} \in \mathbb{Z}$

donc : $\frac{n^7}{7} + \frac{n^5}{5} + \frac{23n}{35} \in \mathbb{Z}$

Exercice38 : Considérons dans $\mathbb{Z}^2$ l'équation (E) : $x^4 + 781 = 3y^4$

1)monter que : $\forall x \in \mathbb{Z} : x^4 \equiv 1[5]$ ou $x^4 \equiv 0[5]$

2) monter que : $\forall x \in \mathbb{Z} : x^4 + 781 \equiv 2[5]$

Ou $x^4 + 781 \equiv 1[5]$

3) en déduire les solutions de l'équation(E)

Solution : 1)on a : 5 est un nombre premier donc : a)si 5 ne divise pas x alors :d'après le théorème de Fermat : $x^4 \equiv 1[5]$

b)si 5 divise x alors :d'après le théorème de Fermat : $x^4 \equiv 0[5]$

donc : $\forall x \in \mathbb{Z} : x^4 \equiv 1[5]$ ou $x^4 \equiv 0[5]$

2) on a : $\forall x \in \mathbb{Z} : x^4 \equiv 1[5]$ ou $x^4 \equiv 0[5]$

Donc : $\forall x \in \mathbb{Z} : x^4 + 781 \equiv 2[5]$ ou $x^4 + 781 \equiv 1[5]$

3)on a : $\forall y \in \mathbb{Z} : y^4 \equiv 1[5]$ ou $y^4 \equiv 0[5]$

Donc : $3y^4 \equiv 0[5]$ ou $3y^4 \equiv 3[5]$

Mais on a :

$\forall x \in \mathbb{Z} : \begin{cases} x^4 + 781 \equiv 1[5] \\ 3y^4 \equiv 0[5] \end{cases}$ ou $\begin{cases} x^4 + 781 \equiv 2[5] \\ 3y^4 \equiv 3[5] \end{cases}$

Donc : $\forall x \in \mathbb{Z}$ et $\forall y \in \mathbb{Z} : x^4 + 781 \neq 3y^4$

Donc : $S = \emptyset$

Exercice39 : soit dans $\mathbb{Z}^2$ l'équation suivante: (E) : $36x - 25y = 5$

1)montrer que si $(x; y)$ est une solution de l'équation (E) alors x est un multiple de 5

2)déterminer une solution particulière de l'équation (E) et résoudre (E)

3) soit $(x; y)$ une solution de l'équation (E)

Et $x \wedge y = d$. Déterminer les valeurs possibles de d et Déterminer les solutions $(x; y)$ de (E) tel que $x \wedge y = 1$

Solution : 1) $(x; y) \in S \Leftrightarrow 36x - 25y = 5$

$\Leftrightarrow 36x = 5(1 + 5y) \Rightarrow 5/36x$

Or on sait que : $5 \wedge 36 = 1$

Donc d'après le théorème de Gauss : $5/x$

Donc x est un multiple de 5

Donc : $\exists x' \in \mathbb{Z} : x = 5x'$

2)déterminons une solution particulière de l'équation (E) ?

On a : $36x - 25y = 5 \Leftrightarrow 36 \times 5x' - 25y = 5$

$\Leftrightarrow 36x' - 5y = 1$

On remarque que : $(1; 7)$ est une solution

particulière de l'équation : $36x' - 5y = 1$

Donc : $(5; 7)$ est une solution particulière de l'équation (E)

$(x; y) \in S \Leftrightarrow 36x - 25y = 5$ et $36 \times 5 - 25 \times 7 = 5$

x	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\bar{10}$
x^2	$\bar{0}$	$\bar{1}$	$\bar{4}$	$\bar{9}$	$\bar{5}$	$\bar{3}$	$\bar{3}$	$\bar{5}$	$\bar{9}$	$\bar{4}$	$\bar{1}$

$\Leftrightarrow 36(x - 5) = 25(y - 7)$

On a donc : $36/25(y - 7)$ Et puisque : $25 \wedge 36 = 1$

Alors : $36/y - 7$ Donc :

$\exists k \in \mathbb{Z} / y - 7 = 36k \Leftrightarrow \exists k \in \mathbb{Z} / y = 36k + 7$

(E) $\Leftrightarrow \begin{cases} 36(x - 5) = 25(y - 7) \\ \exists k \in \mathbb{Z} / y = 36k + 7 \end{cases}$

$\begin{cases} x - 5 = 25k \\ \exists k \in \mathbb{Z} / y = 36k + 7 \end{cases} \Leftrightarrow \exists k \in \mathbb{Z} / \begin{cases} x = 25k + 5 \\ \exists k \in \mathbb{Z} / y = 36k + 7 \end{cases}$

Inversement : $(25k + 5; 36k + 7)$ est solution de l'équation (E)

Donc $S = \{(25k + 5; 36k + 7) / k \in \mathbb{Z}\}$

3)soit $(x; y) \in S$ déterminons : $x \wedge y = d$

On a : $\exists k \in \mathbb{Z} / x = 25k + 5$ et $y = 36k + 7$

Et on a : $\begin{cases} d/x \\ d/y \end{cases} \Rightarrow d/36x - 25y = 5$

Donc : $d = 1$ ou $d = 5$

Si $d = 5$ alors $5/y = 7 + 36k$ car $5/x$
 Donc : $7 + 36k \equiv 0[5]$ cad $2 + k \equiv 0[5]$ cad $k \equiv 3[5]$
 Si $d = 1$ alors $k \equiv 4[5]$ ou $k \equiv 2[5]$ ou $k \equiv 1[5]$
 ou $k \equiv 0[5]$ donc :

$k = 4 + 5\alpha$ ou $k = 2 + 5\alpha$ ou $k = 1 + 5\alpha$ ou $k = 5\alpha$

Avec : $\alpha \in \mathbb{Z}$

Donc : $(x; y) \in S$ et $x \wedge y = 1$ ssi

$(x; y) \in \{(125\alpha + 30; 180\alpha + 43); (125\alpha + 55; 180\alpha + 79);$
 $(125\alpha + 105; 180\alpha + 151); (125\alpha + 5; 180\alpha + 7); \alpha \in \mathbb{Z}\}$

Exercice40: on pose $A = \mathbb{Z}/11\mathbb{Z}$

1) soit $a \in A$ discuter suivant a le nombre de solutions de l'équation : $(E) x^2 = a$ dans A

2) soient p et q deux éléments de A

On considère l'équation : $(F) x^2 - 2px + q = \bar{0}$

Montrer que l'équation : (E) admet une solution ssi $p^2 - q$ appartient à un ensemble B à déterminer

3) application :

a) résoudre dans A l'équation: $x^4 + 3x^2 + 4 = \bar{0}$ (G)

b) déterminer les nombres entiers naturels b

Tels que : 11 divise $10304_{(b)}$

Solution :1) On Dresse une table comme suite : l'équation : (E) admet une solution unique dans A si $a = 0$

l'équation : (E) admet deux solution différentes

dans A si $a \in \{\bar{1}; \bar{3}; \bar{4}; \bar{5}; \bar{9}\}$

l'équation : (E) n'admet pas de solution dans A

si $a \in \{\bar{2}; \bar{6}; \bar{7}; \bar{8}; \bar{10}\}$

2) $x \in A$; $(F) x^2 - 2px = (x - p)^2 - p^2$

$x^2 - 2px + q = \bar{0} \Leftrightarrow (x - p)^2 = p^2 - q$

l'équation : (F) admet une solution dans A ssi

$p^2 - q \in \{\bar{0}; \bar{1}; \bar{3}; \bar{4}; \bar{5}; \bar{9}\}$ donc : $B = \{\bar{0}; \bar{1}; \bar{3}; \bar{4}; \bar{5}; \bar{9}\}$

3) a) résoudre dans A l'équation : $x^2 + 3x + 4 = \bar{0}$ (G) ?

$x^4 + 3x^2 + 4 = \bar{0} \Leftrightarrow X^2 + 3X + 4 = \bar{0}$ avec : $X = x^2$

$\Leftrightarrow X^2 - 8X + 16 = \bar{0}$ car $\bar{4} = \bar{15}$ et $\bar{3} = -\bar{8}$

$\Leftrightarrow (X - \bar{4})^2 = \bar{1} \Leftrightarrow X - \bar{4} = \bar{1}$ ou $X - \bar{4} = \bar{10}$

(G) $\Leftrightarrow X = \bar{5}$ ou $X = \bar{3}$

$\Leftrightarrow x^2 = \bar{5}$ ou $x^2 = \bar{3}$

$\Leftrightarrow x = \bar{4}$ ou $x = \bar{7}$ ou $x = \bar{5}$ ou $x = \bar{6}$

Donc : l'ensemble des solutions de (G) est :

$S = \{\bar{4}; \bar{5}; \bar{6}; \bar{7}\}$

3)b) déterminons les nombres entiers naturels b

Tels que : 11 divise $10304_{(b)}$?

On a : $10304_{(b)} = b^4 + 3b^2 + 4$

$11 \nmid 10304_{(b)} \Leftrightarrow b^4 + 3b^2 + 4 \equiv 0[11]$

$\Leftrightarrow \bar{b}^4 + 3\bar{b}^2 + \bar{4} = \bar{0}$ dans A

$\Leftrightarrow \bar{b} \in \{\bar{4}; \bar{5}; \bar{6}; \bar{7}\}$

$\Leftrightarrow \bar{b} \in \bar{4} \cup \bar{5} \cup \bar{6} \cup \bar{7} \Leftrightarrow b = 11k + r$ et $r \in \{4; 5; 6; 7\}$

Et $k \in \mathbb{N}$

Exercice41

1) Montrer pour tout entier naturel n , non nul : $n^3 - n$ est divisible par 3.

2) Soit p un nombre premier différent de 2,

démontrer que $N = \sum_{k=0}^{p-2} 2^k$ est divisible par p .

Solution :

1. Le corollaire du théorème de Fermat affirme : Pour tout entier naturel a et tout nombre premier p , on a: $a^p \equiv a[p]$

Donc $a^p - a \equiv 0[p]$, c'est à dire $a^p - a$ est divisible par p .

$n \in \mathbb{N}^*$ et 3 est un nombre premier donc $n^3 - n$ est divisible par 3.

Remarques : on peut aussi justifier par une factorisation ou un raisonnement par récurrence.

2) $N = 2^0 + 2^1 + 2^2 + \dots + 2^{p-2}$

est la somme des $(p-1)$ premiers termes de la suite géométrique de raison 2 et de premier terme $2^0 = 1$

Donc: $N = \frac{1 - 2^{p-1}}{1 - 2} = 2^{p-1} - 1$

p est un nombre premier différent de 2 donc p est premier avec 2.

On utilise le théorème de Fermat: 2^{p-1} est divisible par p

Par suite : N est divisible par p .

Exercice42 : Le corollaire du théorème de Fermat affirme :

Pour tout entier naturel a et tout nombre

Premier p , on a: $a^p \equiv a[p]$

La réciproque est-elle vraie ?

C'est à dire si pour tout entier naturel a , on a $a^p \equiv a[p]$ (avec p entier naturel supérieur ou

égal à 2) alors a-t-on p premier ?

On se propose de donner un contre-exemple.

1. Décomposer 561 en produit de facteurs premiers.

2. Démontrer que si x est un entier alors, pour tout $n \in \mathbb{N}^*$, $(x^n - 1)$ est un multiple de $(x - 1)$
3. Démontrer que $a^{561} - a$ est divisible par 3 puis par 11, puis par 17.
4. En déduire que pour tout entier naturel a :
 $a^{561} - a \equiv 0[561]$

Solution : 1) $561 = 3 \times 11 \times 17$

$$2) x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \dots + 1)$$

Si x est un entier alors :

$x^{n-1} + x^{n-2} + \dots + 1$ est un entier et $x - 1$ est un entier.

Conséquence : $(x^n - 1)$ est un multiple de $(x - 1)$

Remarque : on peut aussi effectuer un raisonnement par récurrence pour justifier le résultat)

$$3) a^{561} - a = a(a^{560} - 1)$$

On considère la décomposition de 560 en produit de facteurs premiers : $560 = 2^4 \times 5 \times 7$

560 a donc $5 \times 2 \times 2 = 20$ diviseurs de 560

$$D_{560} = \{1; 2; 4; 5; 7; 8; 10; 14; 16; 20; 28; 35; 40; 56; 70; 80; 140; 280; 560\}$$

$$560 = 2 \times 280 \text{ donc : } a^{560} = (a^2)^{280}$$

On pose $x = a^2$ et $n = 280$

$a^{560} - 1$ est un multiple de $a^2 - 1$. Donc il existe

$$K \in \mathbb{N} \text{ tel que : } a^{560} - 1 = (a^2 - 1)K$$

$$\text{Par suite, } a^{561} - a = a(a^{560} - 1)$$

$$a^{561} - a = a(a^2 - 1)K \text{ donc } a^{561} - a = (a^3 - a)K$$

Or $a^3 - a$ est divisible par 3

Donc, $a^{561} - a$ est divisible par 3

$$a^{560} = (a^{10})^{56} \text{ On pose } x = a^{10} \text{ et } n = 56$$

$a^{560} - 1$ est un multiple de $a^{10} - 1$.

$$\text{Donc il existe } K' \in \mathbb{N} \text{ tel que : } a^{560} - 1 = (a^{10} - 1)K'$$

$$\text{Par suite, } a^{561} - a = a(a^{560} - 1)$$

$$a^{561} - a = a(a^{10} - 1)K' \text{ donc } a^{561} - a = (a^{11} - a)K''$$

Or $a^{11} - a$ est divisible par 11

Donc, $a^{561} - a$ est divisible par 11

$$a^{560} = (a^{16})^{35}$$

On pose $x = a^{16}$ et $n = 35$

$a^{560} - 1$ est un multiple de $a^{16} - 1$.

Donc il existe $K'' \in \mathbb{N}$ tel que :

$$a^{560} - 1 = (a^{16} - 1)K''$$

$$\text{Par suite } a^{561} - a = a(a^{560} - 1)$$

$$a^{561} - a = a(a^{16} - 1)K'' \text{ donc } a^{561} - a = (a^{17} - a)K'''$$

Or $a^{17} - a$ est divisible par 17

Donc, $a^{561} - a$ est divisible par 17

4) 3; 11 et 17 sont trois nombres premiers donc premiers entre eux 2 à 2.

$a^{561} - a$ est divisible par 3; 11 et 17.

Donc $a^{561} - a$ est divisible par $3 \times 11 \times 17 = 561$

$$\text{Par suite : } a^{561} - a \equiv 0[561]$$

$a^{561} \equiv a[561]$ et pourtant 561 n'est pas un nombre premier.

Donc la réciproque du corollaire du théorème de Fermat n'est pas vraie.

Exercice 43 : On suppose qu'il existe des entiers naturels non nuls m , n et a tels que :

$$(4m + 3)(4n + 3) = 4a^2 + 1$$

1) Soit p un nombre premier quelconque divisant $4m + 3$.

Montrer que p est impair et que :

$$(2a)^p - 1 \equiv (-1)^{\frac{p-1}{2}} [p]$$

2) En utilisant le théorème de Fermat, montrer que : $p \equiv 1[4]$

3. En utilisant la décomposition de $4m + 3$ en facteurs premiers obtenir une contradiction

$$\text{Solution : 1) } 4m \equiv 0[2] \text{ donc } 4m + 3 \equiv 3[2]$$

$$\text{donc } 4m + 3 \equiv 1[2]$$

$4m + 3$ n'est pas divisible par 2 donc $p \neq 2$ et donc p est impair.

p est impair donc $p = 2q + 1$ avec $q \in \mathbb{N}$

p est un diviseur de $4m + 3$

$4m + 3$ est un diviseur de $4a^2 + 1$

Donc p est un diviseur de $4a^2 + 1$

$$\text{Par suite : } 4a^2 + 1 \equiv 0[p] \text{ donc } 4a^2 \equiv -1[p]$$

$$\text{donc } (2a)^2 \equiv -1[p] \text{ donc } (2a)^{2q} \equiv (-1)^q [p]$$

$$\text{Or, } 2q \equiv p - 1 \text{ donc } q \equiv \frac{p-1}{2}$$

$$\text{On a donc : } (2a)^p - 1 \equiv (-1)^{\frac{p-1}{2}} [p]$$

2) Pour pouvoir utiliser le théorème de Fermat, on doit vérifier que p et $2a$ sont premiers entre eux.

p étant un nombre premier il suffit de vérifier que p n'est pas un diviseur de $2a$.

$$\text{On suppose que } 2a \equiv 0[p]$$

$$\text{On a alors } 4a^2 \equiv 0[p] \text{ et donc } 4a^2 + 1 \equiv 1[p]$$

$$\text{Or, on a vu dans la question précédente que : } 4a^2 + 1 \equiv 0[p]$$

Donc p n'est pas un diviseur de $2a$ et p et $2a$ sont premiers entre eux

$$\text{D'après le théorème de Fermat : } (2a)^{p-1} \equiv 1[p]$$

Or d'après la première question :

$$(2a)^p - 1 \equiv (-1)^{\frac{p-1}{2}} [p]$$

$$\text{On a donc : } (-1)^{\frac{p-1}{2}} \equiv 1[p]$$

Cela signifie que $\frac{p-1}{2}$ est un nombre pair.

$$\text{Or } q \equiv \frac{p-1}{2} \text{ Donc } q \text{ est un nombre pair.}$$

Il existe $q' \in \mathbb{N}$ tel que $q = 2q'$

$p=2q+1$ donc $p=4q'+1$ et donc : $p \equiv 1[4]$

3) $4m+3 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m} \equiv 1[p]$

$p_1 ; p_2 ; \dots ; p_m$ sont des nombres premiers distincts. et $\alpha_1; \alpha_2; \dots; \alpha_m$ sont des entiers naturels non nuls.

$p_1 ; p_2 ; \dots ; p_m$ sont des nombres premiers qui divisent $4m+3$

D'après la question précédente :

$p_1 \equiv 1[4]$ et $p_2 \equiv 1[4]$ et et $p_m \equiv 1[4]$

Donc : $p_1^{\alpha_1} \equiv 1[4] ; p_2^{\alpha_2} \equiv 1[4] \dots p_m^{\alpha_m} \equiv 1[4]$

Par suite : $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m} \equiv 1[4]$

$4m+3 \equiv 1[4]$

Or, $4m \equiv 0[4]$ donc : $4m+3 \equiv 3[4]$

Il y a contradiction, il n'existe pas des entiers naturels non nuls m, n et a tels que:

$(4m+3)(4n+3) = 4a^2+1$

Exercice44 : Démontrer que pour tout entier naturel non nul n on a $N=n^{13}-n$ est divisible par 13; 7; 5; 3 et 2.

Solution :

13 est un nombre premier, donc d'après le corollaire du théorème de Fermat :

$n^{13}-n$ est divisible par 13.

$n^{13}-n = n(n^{12}-1)$

$12 = 2^2 \times 3$ donc : Le nombre 12 à 6 diviseurs

$D_{12} = \{1 ; 2 ; 3 ; 4 ; 6 ; 12\}$

$n^{13}-n = n(n^{12}-1) = n(n^6-1)(n^6+1) = (n^7-n)(n^6+1)$

7 est un nombre premier, donc d'après le corollaire du théorème de Fermat :

n^7-n est divisible par 7.

Par suite, $n^{13}-n$ est divisible par 7.

$n^{13}-n = n(n^{12}-1) = n[(n^4)^3-1]$

On utilise le résultat de l'exercice précédent :

$n[(n^4)^3-1]$ est un multiple de n^4-1

Donc il existe $K \in \mathbb{N}$ tel que : $(n^4)^3-1 = (n^4-1)K$

$n^{13}-n = n(n^{12}-1) = n[(n^4)^3-1] = (n^4-1)K = (n^5-n)K$

5 est un nombre premier, donc d'après le corollaire du théorème de Fermat :

n^5-n est divisible par 5. Par suite, $n^{13}-n$ est divisible par 5

$n^{13}-n = n(n^{12}-1) = n[(n^2)^6-1]$

On utilise le résultat de l'exercice précédent :

$(n^2)^6-1$ est un multiple de n^2-1 .

Donc il existe $K' \in \mathbb{N}$ tel que : $(n^2)^6-1 = (n^2-1)K'$

$n^{13}-n = n(n^{12}-1) = (n^3-n)K'$

3 est un nombre premier, donc d'après le corollaire du théorème de Fermat :

n^3-n est divisible par 3.

Par suite, $n^{13}-n$ est divisible par 3.

$n^{13}-n = n(n^{12}-1)$

On utilise le résultat de l'exercice précédent :

$n^{12}-1$ est un multiple de $n-1$

Donc il existe $K'' \in \mathbb{N}$ tel que: $n^{12}-1 = (n-1)K''$
 $n^{13}-n = n(n^{12}-1) = n(n-1)K'' = (n^2-n)K''$

2 est un nombre premier, donc d'après le corollaire du théorème de Fermat : n^2-n est divisible par 2.

Par suite, $n^{13}-n$ est divisible par 2.

« 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