Professeur	Bahloul Khalid (+212) 622-17-65-52
Chapitre	Arithmétique dans Z (l'essentiel du cours + applications)
Niveaux	Bac français / $1^{ère}$ et $2^{ème}$ Bac International SM

I) LA DIVISIBILITE DANS $\mathbb{Z}$

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 $\boldsymbol{a = kb}$;
On écrit : $\boldsymbol{b|a}$.
On dit que a est divisible par b

Exemples : $3/12$ car $12 = 3 \times 4$

- 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 :

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

Application

1) Déterminer et dénombrer les diviseurs naturels de 156
2) Déterminer dans 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 $a/-a$
- $b|a \Rightarrow |b| \leq |a|$
- $a/b \Rightarrow a/b \times c$
- $a/b \Rightarrow |a| \leq |b|$
- $b|1 \Rightarrow b \in \{-1,1\}$

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

3 Multiple commun et Diviseur 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'.

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

Application

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

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

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

2) $a/12n+1$ et $a/-2n+3$

$\Rightarrow a/12n+1 \text{ et } a/-12n+18 \Rightarrow a/19$

$\Rightarrow a \in \{\pm1;\pm19\}$

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

$\Rightarrow d/n^2+3 \text{ et } a/(2n-1)^2 \Rightarrow d/4n^2+12 \text{ et } d/4n^2-4n+1$

$\Rightarrow d/11+4n \text{ et } d/-2+4n \Rightarrow d/13$

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

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

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

$a/10x-14-10x-15 \Rightarrow a/-29 \Rightarrow a/29$

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

3 divise 4^n-1

Montrons que : $\forall n \in \mathbb{N} \quad \exists k \in \mathbb{N} / 4^n-1=3k$

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

$4^0-1=0$ est un multiple de 3

Donc P (0) est vraie.

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

$4^n=3k+1$

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

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

$4^{n+1}-1=4\times4^n-1$

$=4\times(3k+1)-1=12k+4-1=12k+3=3(4k+1)$

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

Application : 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.

4 la division euclidienne dans 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 :

$75 = 9 \times 6 + 3$ car $0 \leq 3 < 8$

la division euclidienne de 126 par 7 donne :

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

la division euclidienne de 85 par 112

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

Application 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 $0 \leq p^2 \prec 25$

donc $0 \leq p \prec 5$

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

Application : 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 $n = abq' + ar' + r$

$0 \leq ar' + r \leq b-1$ conclusion : q' est aussi le quotient de n par ab

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

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

Application : $b \in \mathbb{N}^*$ 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 :
$a-1=bq+r$ et $0 \leq r \prec b$
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 : $0 \leq (r+1)b^9-1 \prec b^{10}$???
On a : $0 \leq r \prec b$ 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 $0 \leq (r+1)b^9-1 \prec b^{10}$
conclusion : q est aussi le quotient de la division euclidienne de ab^9-1 par b^{10}

II) 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 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 diffèrent de 1 est un nombre premier

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

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

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

Application Les nombres suivants sont–ils premiers :499 ; 601 ; 703 ; 2003 ; $2n^2+3n \quad n\in\mathbb{N}$

III) PGDC et PPMC

1 propriétés et définitions

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 = $PGDC\ (a, b)$ = $a \wedge b$

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 $d|\ (a \wedge b)$

Application : 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 $d/a+1 \Rightarrow d/1 \Rightarrow d=1$

Application $n \in \mathbb{N}$ 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 : $\dfrac{n^2+3}{n+2} \in \mathbb{N}$

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) $\dfrac{n^2+3}{n+2} \in \mathbb{N} \Leftrightarrow n+2/n^2+3$ et 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 entraine que $n=5$

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

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

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 : $a \wedge b = b \wedge r$

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

Propriété : Soient a et b deux entier relatifs non nuls
Les diviseurs communs de a et b sont les diviseurs de $a \wedge b$.
On peut dire que : $D_a \cap D_b = D_{a \wedge b}$

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

Propriétés :
1) $a \vee a = |a|$ 2) $a \vee b = b \vee a$
3) $a \vee 1 = |a|$ 4) Si $b|a$ alors $a \vee b = |a|$
5) $a \vee (b \vee c) = (a \vee b) \vee c$
6) $a|(a \vee b)$; $b|(a \vee b)$ 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 $m|M$.

IV) congruence modulo n

Définition : Soient a et b deux entiers relatifs ; et n un entier naturel non nul. On dit que : $\boldsymbol{a}$ est congrue à $\boldsymbol{b}$ modulo $\boldsymbol{n}$ si $n|(\boldsymbol{b} - \boldsymbol{a})$.
On écrit : $\boldsymbol{a} \equiv \boldsymbol{b}\ [\boldsymbol{n}]$

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

$(a \equiv b\ [n]$ 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**

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 $2 \not\equiv 3\ [5]$

Application : $a \in \mathbb{N}$ 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) $a+b$ 2) a^2+b^2 3) $2a-5b$

Solution15 : 1)On a : $a\equiv17[19]$ et $b\equiv15[19]$

donc : $a+b\equiv17+15[19]\Leftrightarrow a+b\equiv13[19]$

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

2) $a\equiv17[19]\Rightarrow a^2\equiv17^2[19]\Rightarrow a^2\equiv4[19]$

$b\equiv15[19]\Rightarrow b^2\equiv15^2[19]\Rightarrow b^2\equiv16[19]$

Donc : $a^2+b^2\equiv4+16[19]\Leftrightarrow a^2+b^2\equiv1[19]$

Par suite : le reste dans la division du nombre a^2+b^2 Par 19 est : 1

3) $a\equiv17[19]\Rightarrow 2a\equiv2\times17[19]\Rightarrow 2a\equiv15[19]$ **(1)**

$b\equiv15[19]\Rightarrow 5b\equiv5\times15[19]\Rightarrow 5b\equiv18[19]$

Donc : $5b\equiv-1[19]\Rightarrow -5b\equiv1[19]$ **(2)**

De **(1) et (2)** on déduit que :

$2a-5b\equiv15+1[19]\Rightarrow 2a-5b\equiv16[19]$

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

Application $x\in\mathbb{N}^*$ 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 $a\wedge b=b\wedge7$

b)en déduire les valeurs possibles $a\wedge b=d$

c)montrer que : $n\equiv4[7]\Leftrightarrow a\wedge b=7$

d)en déduire les valeurs de $n\in\mathbb{N}$ tel que : $a\wedge b=1$

Solution19 : 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 entraine: $d=d'$

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

a) montrons que $a\wedge b=b\wedge7$?

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 $d'=b\wedge7$ 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 $d/b\Rightarrow d/b\wedge7\Rightarrow d/d'$

$d'=b\wedge7\Rightarrow d'/7$ 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 entraine: $d=d'$

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

on a : $a\wedge b=b\wedge7=d$

donc : $d/7$ donc : $d=1$ ou $d=7$

c)montrons que : $n\equiv4[7]\Leftrightarrow a\wedge b=7$

$n\equiv4[7]\Leftrightarrow n+3\equiv0[7]\Leftrightarrow 7/n+3\Leftrightarrow 7/b\Leftrightarrow b\wedge7=7\Leftrightarrow b\wedge a=7$

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

$n\equiv0[7]$ ou $n\equiv1[7]$ ou $n\equiv2[7]$ ou $n\equiv3[7]$ ou $n\equiv5[7]$

ou $n\equiv6[7]$

Les classes d'équivalence

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 : $\overline{r}$ = $\{m \in \mathbb{Z} \,/\, m \equiv r\ [n]\}$ = $\{nk + r$ 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 :

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

$\overline{1} = \{m \in \mathbb{Z} \,/\, m \equiv 1\ [7]\}$ et …

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

on remarquer que $\overline{0} = \overline{7}$
Les classes d'équivalences modulo 7 constituent :un ensemble noté :

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

Généralisation : $\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0};\overline{1};\overline{2};\overline{3};\ldots;\overline{n-1}\right\}$

Les opérations sur Z /nZ

Définition : Soit n un entier naturel non nul.
On définit dans $\mathbb{Z}/n\mathbb{Z}$ les deux lois :

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

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

Application : Résoudre les équations suivantes dans $\mathbb{Z}/_{4\mathbb{Z}}$: 1) $\overline{2}x=\overline{3}$ 2) $x^2+\overline{3}x=\overline{0}$
3) $\overline{2013}x^3+\overline{2}x=\overline{k}$

Solution20 : On a : $\mathbb{Z}/4\mathbb{Z}=\{\overline{0};\overline{1};\overline{2};\overline{3}\}$

1)On Dresse une table comme suite :

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

Et en utilisant cette une table on déduit que Cette équation n'admet pas de solutions

Donc : $S=\varnothing$

1)On Dresse une table comme suite :

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

Et en utilisant cette une table on déduit que $\overline{0}$ et $\overline{1}$ sont solutions de l'équation

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

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

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

On Dresse une table comme suite :

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

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

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

Application : Résoudre dans $\left(\mathbb{Z}/5\mathbb{Z}\right)^2$ les système suivants : $\begin{cases}\overline{3}x+\overline{2}y=\overline{1}\\ \overline{2}x+\overline{4}y=\overline{3}\end{cases}$

Solution22 :

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

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

Décomposition d'un nombre entier en facteurs premiers

Théorème :

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

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

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

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

où $\varepsilon\in\{-1,1\}$

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

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

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

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

$(\forall i \in [\![1, n]\!])(0 \leq \beta_i \leq \alpha_i)$

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

On en déduit que :

Propriété 2 :

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

est un entier, le nombre des diviseurs de a est : $2(\alpha_1 + 1)(\alpha_2 + 1)\ldots(\alpha_n + 1)$

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

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

un entier m est un multiple de a si et seulement si $m = \varepsilon p_1^{\beta_1} \times p_2^{\beta_2} \times p_3^{\beta_3} \times \ldots \times p_n^{\beta_n} = \prod_{k=1}^{k=n} p_k^{\beta_k}$

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

Propriété : Soient a et b deux entiers naturels

1) Le plus grand entier n qui vérifie :
$n \leq a$ et $n \leq b$ est inf (a, b)

2) Le plus petit entier n qui vérifie :
$n \geq a$ et $n \geq b$ est sup (a, b)

Exemple : $a = 7$ et $b = 10$
Le plus grand des entiers n tel que
$n \leq 7$ et $n \leq 10$ est : $7 = \inf(10,7)$
Le plus petit des entiers n tel que :
$n \geq 7$ et $n \geq 10$ est $10 = \sup(10,7)$

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

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

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

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

Remarque : Soient a et b deux entiers relatifs
on a : $a \wedge b = |a| \wedge |b|$

Application :déterminer : $d = (-8316) \wedge 1080$ et
$m = 8316 \vee 1080$

Solution : la décomposition des nombres 8316 et 1080 en produit des facteurs premiers
Donnent : $8316 = 2^2 \times 3^3 \times 7 \times 11$ et
$1080 = 2^3 \times 3^3 \times 5$
$d = 8316 \wedge 1080 = 2^2 \times 3^3 = 108$ et
$m = 8316 \vee 1080 = 2^3 \times 3^3 \times 5 \times 7 \times 11 = 11880$

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

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

déterminer : $a \vee b$

<u>Solution :</u> on a $a \wedge b) \times (a \vee b) = |ab|$

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

Application : 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

<u>Solution :</u> 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 $n = abq' + ar' + r$

$0 \leq ar' + r \leq b - 1$ conclusion : q' est aussi le quotient de n par ab

Application Déterminer le reste de la division euclidienne de $19^{52} \times 23^{41}$ par 7

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

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

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

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

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

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

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

conclusion :1est le reste de la division euclidienne de $19^{52} \times 23^{41}$ par 7

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

<u>**Solution26 :**</u>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 $n \in \mathbb{N}$.

1étapes : 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.

2étapes : d'hérédité ou Hypothèse de récurrence : Supposons que P(n) soit vraie c'est-à-dire : « 9 divise U_n »

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