SECONDAIRE
Tle C
MATHEMATIQUES

CÔTE D'IVOIRE – ÉCOLE NUMÉRIQUE

THEME : ARITHMÉTIQUE

Durée : 10 heures **Code :**

Leçon 4 : DIVISIBILITÉ DANS $\mathbb{Z}$

A. SITUATION D'APPRENTISSAGE

Des élèves d'une classe de première C passionnés d'astronomie ont lu dans une revue les informations suivantes :
« Un corps céleste A qui apparait périodiquement tous les 105 jours a été observé un jour J_0 par un astronome. Six jours plus tard ($J_0 + 6$), il observe le corps B, dont la période d'apparition est de 81 jours. Il est mentionné dans la revue que les deux corps célestes apparaissent simultanément à certaines dates ».

Voulant en savoir davantage sur ces dates, ils te sollicitent. Tu poses le problème à toute ta classe de TC et ensemble vous décidez de faire des recherches sur les dates d'apparition simultanées de ces deux corps célestes.

B. CONTENU DE LA LEÇON

I. DIVISIBILITÉ DANS $\mathbb{Z}$

1. Diviseurs d'un nombre entier relatif

a. Définition

Soit a et b deux nombres entiers relatifs tels que :$b \neq 0$.
On dit b est un diviseur de a s'il existe un nombre entier relatif k tel que :$a = kb$.
Lorsque b est un diviseur de a, on dit aussi que b divise a ou que a est un multiple de b.

Notation
b divise a est noté$\boldsymbol{b|a}$

Exemple
$28 = 7 \times 4$, donc 28 est un multiple de 7 et de 4.
7 et 4 sont des diviseurs de 28 (on peut aussi dire que 7 et 4 divisent 28)

Remarques
- 1 et -1 divisent tout nombre entier relatif
- 0 est multiple de tout nombre entier relatif
- Tout nombre entier relatif non nul divise 0 mais 0 ne divise aucun nombre entier relatif

Notation

Soit a un nombre entier relatif.
L'ensemble des diviseurs de a se note **D**(a)

b. Propriétés

Soit a, b et c trois nombres entiers relatifs non nuls

(1) Si b divise a, alors $|b| \leq |a|$
(2) a divise a
(3) si $a \mid b$ et $b \mid a$, alors $a = b$ ou $a = -b$
(4) si a divise b et b divise c, alors a divise c
(5) Si a divise b et c, alors pour tous entiers relatifs p et q , a divise $pb + qc$
(en d'autres termes, si a divise b et c, alors a divise toute combinaison linéaire de b et c)

Exercice de fixation

Soit $n \in \mathbb{N}$, démontrez que la fraction $r = \frac{15n^2+8n+6}{30n^2+21n+13}$ est irréductible.

Solution

Posons $a = 30n^2 + 21n + 13 \ et \ b = 15n^2 + 8n + 6$.
On a : $a - 2b = 5n + 1 \ et \ b = (5n + 1)(3n + 1) + 5$.
Soit $d = PGCD(a; b)$.
Comme $d|a \ et \ d|b$ alors $d|(a - 2b)$, d'où $d = PGCD(b; 5n + 1)$.
Il existe deux entiers naturels $k \ et \ l$ tels que
$(5n + 1) = dk \ et \ (5n + 1)(3n + 1) + 5 = dl$, d'où
$dk(3n + 1) + 5 = dl \Leftrightarrow 5 = dl - dk(3n + 1) = d(l - k(3n + 1))$.
Donc $d|5 \ et \ d|(5n + 1)$ et $d|[(5n + 1) - 5n]$, c-à-d que $d|1$.
Conclusion : $d = PGCD(5; 1) = 1$. $30n^2 + 21n + 13 \ et \ 15n^2 + 8n + 6$ sont premiers entre eux donc la fraction $r = \frac{15n^2+8n+6}{30n^2+21n+13}$ est irréductible.

2. Division euclidienne

a. Division euclidienne dans $\mathbb{N}$

Propriété

Soit a et b deux nombres entiers naturels tels que $b \neq 0$.
Il existe un unique couple $(q ; r) \in \mathbb{N} \times \mathbb{N}$ tel que : $a = bq + r$ et $0 \leq r < b$

Remarque

- Effectuer la division euclidienne de a par b consiste à déterminer l'unique couple $(q ; r) \in \mathbb{N} \times \mathbb{N}$ tel que : $a = bq + r$ et $0 \leq r < b$
- q et r sont respectivement appelés *quotient* et *reste* de la division euclidienne de a par b .
- Si le reste de la division euclidienne de a par b est égal 0, alors b divise a.

Exercice

Effectue la division euclidienne de 72 par 5.

Solution

$72 = 14 \times 5 + 2$ avec $0 \leq 2 < 5$

14 et 2 sont respectivement le quotient et le reste de la division euclidienne de 72 par 5.

b. Division euclidienne dans $\mathbb{Z}$

Propriété

Soit a et b deux nombres entiers relatifs tels que $b \neq 0$.
Il existe un unique couple $(q\,; r) \in \mathbb{Z} \times \mathbb{N}$ tel que : $a = bq + r$ et $0 \leq r < |b|$.

Remarque :

- Soit $(a; b) \in \mathbb{Z} \times \mathbb{N}^*$ il existe un unique entier

$q \in \mathbb{Z}$ **tels que** $\boldsymbol{bq \leq a < b(q+1)} \Leftrightarrow \boldsymbol{bq \leq a} < bq + b \Leftrightarrow 0 \leq a - bq < b$

En posant $r = a - bq$ on a $a = bq + r$ *et* $0 \leq r < b$.

- Effectuer la division euclidienne de a par b consiste à déterminer l'unique couple $(q\,; r) \in \mathbb{Z} \times \mathbb{N}$ tel que : $a = bq + r$ et $0 \leq r < |b|$.
- Le reste d'une division euclidienne dans $\mathbb{Z}$ est toujours un entier positif.
- Si le reste de la division euclidienne de a par b est égal 0, alors b divise a.

Exemple :

Effectuez la division euclidienne de -17 par 3.

$-18 < -17 < -15 \Leftrightarrow 3 \times (-6) < -17 < 3 \times (-5)$, donc le quotient est $q = -6$, le reste de la division euclidienne de -17 par 3 est $r = (-17) - (-18) = 1$.

Exercice de fixation 1

1) Chaque écriture suivante traduit-elle une division euclidienne ?
Répond par vrai ou par faux.

N°	Écritures	Réponses
1	$71 = 7 \times 9 + 8$	
2	$27 = 4 \times 5 + 7$	
3	$-161 = -12 \times 13 - 5$	
4	$-127 = -15 \times 9 + 8$	

2) Donne le quotient et le reste de la division euclidienne de :

a) 361 par 23 b) 361 par -23 c) -361 par 23 d) -361 par -23.

Solution

1)

N°	Écritures	Réponses
1	$71 = 7 \times 9 + 8$	vrai

2	$27 = 4 \times 5 + 7$	faux
3	$-161 = -12 \times 13 - 5$	faux
4	$-127 = -15 \times 9 + 8$	vrai

2) a) $361 = 15 \times 23 + 16$; $q = 15$ et $r = 16$.

b) $361 = (-15) \times (-23) + 16$; $q = -15$ et $r = 16$.

c) $-361 = -(15 \times 23 + 16) = -15 \times 23 - 16 = -15 \times 23 - 16 + 23 - 23$

$-361 = -16 \times 23 + 7$; $q = -16$ et $r = 16$.

d) $-361 = -(15 \times 23 + 16) = 15 \times (-23) - 16 = 15 \times (-23) - 16 + 23 - 23$

$-361 = 16 \times (-23) + 7$; $q = 16$ et $r = 7$.

Exercice de fixation 2

Le reste de la division euclidienne de m par 17 est 8, celui de n par 17 est 12.

Déterminez le reste de la division euclidienne par 17 de :

a- $m + n$.

b- $m \times n$.

c- m^2 .

Solution

Ecrivons euclidienne de $m\ et\ de\ n$ par 17 : il existe deux entiers naturels $q\ et\ q'$ tels que $m = 17q + 8\ \ et\ \ n = 17q' + 12$.

a. $m + n = (17q + 8) + (17q' + 12) = 17(q + q') + 20 = 17(q + q' + 1) + 3$; le reste de la division euclidienne de $m + n$ par 17 est 3.

b. $m \times n = (17q + 8)(17q' + 12) = 17^2qq' + 17 \times 12q + 17 \times 8q' + 96$

$m \times n = 17(17qq' + 12q + 8q') + 17 \times 5 + 11,$

$m \times n == 17(17qq' + 12q + 8q' + 5) + 11.$

Le reste de la division euclidienne de $m \times n$ par 17 est 11.

c. $m^2 = (17q + 8)^2 = 17^2q^2 + 2 \times 17q \times 8 + 8^2 = 17^2q^2 + 17(16q) + 64$

$m^2 = 17^2q^2 + 17(16q) + 17 \times 3 + 13 = 17(17q^2 + 16q + 3) + 13.$

le reste de la division euclidienne de m^2 par 17 est 13.

3. Congruence modulo n(n est un entier naturel non nul)

a. Définition

Soit a et b deux nombres entiers relatifs et n un entier naturel non nul.

On dit que a est congru à b modulo n si n divise$a - b$.

Notation

a est congru à b modulo n est noté $a \equiv b\ [n]$ ou $a \equiv b$ (mod n).

Exemple

- $23 \equiv 3\ [5]$ car $23 - 3 = 20$ et 5 divise 20.
- $39 \equiv -1\ [8]$ car $39 - (-1) = 40$ et 8 divise 40.

Remarque

Si $a \equiv b\ [n]$ et $0 \leq b < n$, alors b est le reste de la division euclidienne de a par n.

b. Propriétés

Propriété 1

Soit a, b, c et d quatre nombres entiers relatifs, n et k deux entiers naturels non nuls

(1) $a \equiv a\ [n]$

(2) si $a \equiv b\ [n]$, alors $b \equiv a\ [n]$

(3) si $a \equiv b\ [n]$ et $b \equiv c\ [n]$, alors $a \equiv c\ [n]$

(4) Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$, alors :

- $(a + c) \equiv (b + d\ )[n]$
- $a \times c \equiv b \times d\ [n]$
- $a^k \equiv b^k [n]$

Exercice de fixation

Soit $a = 51\ et\ b = 126$

Détermine les restes respectifs de la division euclidienne de ab, $6a - 5b$ et a^4 par 8.

Solution

- $a \equiv 3[8]$ et $b \equiv 6[8]$ alors $ab \equiv 3 \times 6\ [8]$

On a donc $ab \equiv 18\ [8]$ d'où $ab \equiv 2\ [8]$. Comme $0 \leq 2 < 8$, alors 2 est le reste de la division euclidienne de ab par 8.

- $a \equiv 3[8]$ et $b \equiv 6[8]$ alors $6a - 5b \equiv 6 \times 3 - 5 \times 6\ [8]$
  On a donc $6a - 5b \equiv -12\ [8]$ d'où $6a - 5b \equiv 4[8]$
  Comme $0 \leq 4 < 8$, alors 4 est le reste de la division euclidienne de $6a - 5b$ par 8.
- $a \equiv 3[8]$ alors $a^4 \equiv 3^4[8]$. On a donc $a^4 \equiv 81\ [8]$, d'où $a^4 \equiv 1\ [8]$.
  Comme $0 \leq 1 < 8$, alors 1 est le reste de la division euclidienne de a^4 par 8.

Propriété 2

Soit n un nombre entier naturel non nul, a et a' deux nombres entiers relatifs, r et r' les restes respectifs des divisions euclidiennes de a et a' par n.

On a : $a \equiv a'[n] \Leftrightarrow r = r'$.

Exercice

Soit a un nombre entier relatif et r le reste de la division euclidienne de a par 13.

Sachant que $a \equiv 2020[13]$, détermine r.

Solution

$2020 \equiv 5[13]$, Comme $0 \leq 5 < 13$, alors 5 est le reste de la division euclidienne de 2020 par 13.

On a donc, $a \equiv 2020[13] \Leftrightarrow r = 5$.

4. Numération

a) Propriété

Soit b un nombre entier naturel supérieur ou égal à 2.
Tout entier naturel x non nul peut s'écrire de façon unique

$$x = \sum_{k=0}^{n} a_k b^k = a_0 b^0 + a_1 b^1 + a_2 b^2 + \cdots + a_n b^n$$

où les a_k sont des nombres entiers naturels tels que : $0 \leq a_k < b$ et $a_n \neq 0$.
On appelle écriture de x en base b l'expression $x = \overline{a_n a_{n-1} \ldots a_2 a_1 a_0}^{b}$
Par convention les écritures *«sans barre »* sont en base 10.

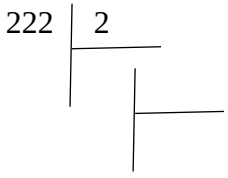
Remarque

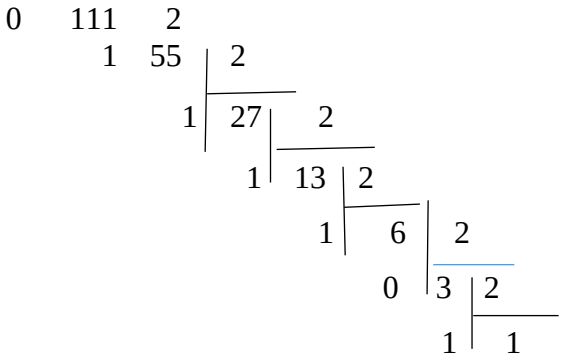
- $x = \overline{a_n a_{n-1} \ldots a_2 a_1 a_0}^{b} = a_n b^n + a_{n-1} b^{n-1} + \ldots + a_2 b^2 + a_1 b + a_0$
- $x = \overline{a_n a_{n-1} \ldots a_2 a_1 a_0}^{b}$
  Lorsque $b = 2$ on dit que x est écrit en base 2 ou base binaire.
  Lorsque $b = 10$ on dit que x est écrit en base 10 ou base décimale.
  Lorsque $b = 16$ on dit que x est écrit en base 16 ou base hexadécimale.

Exercice de fixation

Ecris en base 2 le nombre 222

Solution





Donc 222=$\overline{11011110}^{2}$

b) Bases de numération

Exemples de systèmes de numération :

- Le ***système décimal*** (base 10) utilise l'ensemble des chiffres $\{0\ ,1,2,3,4,5,6,7,8,9\}$
- Le ***système binaire*** (base 2) utilise l'ensemble des chiffres $\{0\ ,1\}$
- Le ***système octal*** (base 8) utilise l'ensemble des chiffres $\{0\ ,1,2,3,4,5,6,7\}$
- Le ***système hexadécimal*** (base 16) utilise l'ensemble des chiffres et des lettres :

$\{0,1,2,3,4,5,6,7,8,9,A,B,C,D,\ E,F\}$ tels que A=10 ; B=11 ; C=12 ; D=13 ; E=14 ; F=15

Exercice

Ecris en système décimal le nombre $\overline{10254}^{8}$.

Solution

$\overline{10254}^{8} = 4 + 5 \times 8^{1} + 2 \times 8^{2} + 0 \times 8^{3} + 1 \times 8^{4} = 4268.$

c. Quelques critères de divisibilité

Soit $\overline{x}^{a} = \gamma_p\gamma_{p-1}\gamma_{p-2}\ldots\gamma_1\gamma_0$ dans le système décimal ; on a $x = \sum_{k=0}^{p}\gamma_k 10^k$.

- ✓ ***CONGRUENCE MODULO 2***

  $10^0 \equiv 1[2]$ et pour tout $k \in \mathbb{N}^*;\ 10^k \equiv 0[2]$ donc $x \equiv \gamma_0[2]$.

  $x \equiv 0[2] \Leftrightarrow \gamma_0 \equiv 0[2]$.

- ✓ ***CONGRUENCE MODULO 3***

  Pour tout $k \in \mathbb{N};\ 10^k \equiv 1[3]$ donc $x \equiv (\sum_{k=0}^{p}\gamma_k)[3]$; d'où

  $x \equiv 0[3] \Leftrightarrow (\sum_{k=0}^{p}\gamma_k) \equiv 0[3]$

- ✓ ***CONGRUENCE MODULO 4***

  $10^0 \equiv 1[4];\ 10^1 \equiv 2[4]$, pour tout $k \in \mathbb{N}, k \geq 2;\ 10^k \equiv 0[4]$; donc

  $x \equiv (\gamma_0 + \gamma_1 10^1)[4] \Leftrightarrow x \equiv (\gamma_0 + 2\gamma_1)[4]$

$x \equiv 0[4] \Leftrightarrow (0 + 2\gamma_1) \equiv 0[4] \Leftrightarrow (\gamma_0 + 10\gamma_1) \equiv 0[4] \Leftrightarrow$ Le nombre $\gamma_1\gamma_0$ est divisible par 4.

- ✓ ***CONGRUENCE MODULO 5***
  Pour tout $10^0 \equiv 1[5]$; pour tout $k \in \mathbb{N}^*, 10^k \equiv 0[5]$. Donc $x \equiv \gamma_0[5]$.
  $x \equiv 0[5] \Leftrightarrow \gamma_0 \equiv 0[5]$.
- ✓ ***CONGRUENCE MODULO 6***
  $10^0 \equiv 1[6]$; Pour tout $k \in \mathbb{N}^*, 10^k \equiv 4[6]$; donc $x \equiv (\gamma_0 + 4\sum_{k=1}^{p} \gamma_k)[6]$

  $x \equiv 0[6] \Leftrightarrow (\gamma_0 + 4\sum_{k=1}^{p} \gamma_k) \equiv 0[6]$
- ✓ ***CONGRUENCE MODULO 8***
  $10^0 \equiv 1[8]$; $10^1 \equiv 2[8]$; $10^2 \equiv 4[8]$; pour tout $\in \mathbb{N}, k \geq 3$; $10^k \equiv 0[8]$, donc $x \equiv (\gamma_0 + \gamma_1 10^1 + \gamma_2 10^2)[8] \equiv (\gamma_0 + 2\gamma_1 + 4\gamma_2)[8]$. $x \equiv 0[n] \Leftrightarrow (\gamma_0 + 2\gamma_1 + 4\gamma_2) \equiv 0[8] \Leftrightarrow$ .Le nombre $\gamma_2\gamma_1\gamma_0$ est divisible par 8.
- ✓ ***CONGRUENCE MODULO 9***
  Pour tout $\in \mathbb{N}, 10^k \equiv 1[9]$, donc $x \equiv (\sum_{k=1}^{p} \gamma_k)[9]$. D'où
  $x \equiv 0[9] \Leftrightarrow (\sum_{k=1}^{p} \gamma_k) \equiv 0[9]$.
- ✓ ***CONGRUENCE MODULO 25***
  $10^0 \equiv 1[25]$; $10^1 \equiv 10[25]$ et pour tout $k \in \mathbb{N}, k \geq 2$, $10^k \equiv 0[8]$ donc
  $x \equiv (\gamma_0 + \gamma_1 10)[25]$. D'où $x \equiv 0[25] \Leftrightarrow (\gamma_0 + \gamma_1 10) \equiv 0[25] \Leftrightarrow$ Le nombre $\gamma_1\gamma_0$ est divisible par 25.

- **Critère de divisibilité par 2**

Un nombre entier naturel est divisible par 2 s'il est pair ; en d'autres termes si le chiffre des unités est 0 ; 2 ; 4 ; 6 ou 8.

- **Critère de divisibilité par 3**

Un nombre entier naturel est divisible par 3 si la somme de ses chiffres est divisible par 3.

- **Critère de divisibilité par 5**

Un nombre entier naturel est divisible par 5 si le chiffre des unités est 0 ou 5.

- **Critère de divisibilité par 9**

Un nombre entier naturel est divisible par 9 si la somme de ses chiffres est divisible par 9.

- **Critère de divisibilité par 10**

Un nombre entier naturel est divisible par 10 si le chiffre des unités est 0.

- **Critère de divisibilité par 11**

Un nombre entier naturel est divisible par 11 si la somme de ses chiffres de rang pair soustraite de la somme de ses chiffres de rang impair est divisible par 11.

Exercice de fixation

En appliquant les critères de divisibilités, justifie que 6485958017 est divisible par 11.

Solution

(6 + 8 + 9 + 8 + 1) – (4 + 5 + 5 + 0 + 7) =11

11 divise 11, donc 6485958017 est divisible par 11.

II. Les nombres premiers

1. Définition

On dit qu'un nombre entier naturel p est premier s'il possède exactement deux diviseurs positifs : 1 et p.

Exemple

7 est un nombre premier car les seuls diviseurs positifs de 7 sont 1 et 7.

Remarque

- 0 et 1 ne sont pas des nombres premiers
- 2 est le seul nombre premier pair

Propriétés

- Tout nombre entier naturel n strictement supérieur à 1 a au moins un diviseur premier.
- Si un nombre entier naturel n strictement supérieur à 1 n'est pas premier, alors il existe un diviseur p premier de n tel que : $2 \leq p \leq \sqrt{n}$
- Il existe une infinité de nombres premiers

Exercice de fixation

Les nombres 983 et 2419 sont-ils premiers ?

Solution

- $\sqrt{983} \approx 31{,}35$

Les nombres premiers inférieur à 31 sont : 2 ; 3 ; 5 ; 7 ; 11 ; 13 ; 17 ; 19 ; 23 ; 29 ; 31.

Aucun nombre premier inférieur ou égal à 31 ne divise 983. Donc 983 est un nombre premier.

- $2232 = 31 \times 72$.

Donc 2232 n'est pas un nombre premier.

2. Décomposition en produit de facteurs premiers

Propriété et définition

Soit n un nombre entier naturel strictement supérieur à 1

- Il existe des nombres premiers $p_1, p_2, p_3, \dots, p_k$ et des nombres entiers naturels $\propto_1, \propto_2, \propto_3, \dots, \propto_k$ tels que :

$$n = {p_1}^{\propto_1} \times {p_2}^{\propto_2} \times {p_3}^{\propto_3} \times \dots \times {p_k}^{\propto_k} \text{ où } p_1 < p_2 < p_3 < \dots < p_k$$

- Cette décomposition est unique et est appelée décomposition de n en produit de facteurs premiers.

Exercice fixation

Décompose le nombre 1092 en produit de facteurs premiers

Solution

1092	2
546	2
273	3
91	7
13	13
1	

$$1092 = 2^2 \times 3 \times 7 \times 13.$$

Propriété

Soit n un nombre entier naturel strictement supérieur à 1 et admettant la décomposition en produit de facteurs premiers : $n = {p_1}^{\propto_1} \times {p_2}^{\propto_2} \times {p_3}^{\propto_3} \times \dots \times {p_k}^{\propto_k}$

- Les diviseurs positifs de n sont de la forme :
  $n = {p_1}^{\beta_1} \times {p_2}^{\beta_2} \times {p_3}^{\beta_3} \times \dots \times {p_k}^{\beta_k}$, avec $0 \leq \beta_i \leq \alpha_i$ et $1 \leq i \leq k$
- Le nombre de diviseurs positifs de n est :

$$(1 + \alpha_1)(1 + \alpha_2) \times \dots \times (1 + \alpha_k)$$

Exercice de fixation

Détermine le nombre de diviseurs positifs de 1092.

Solution

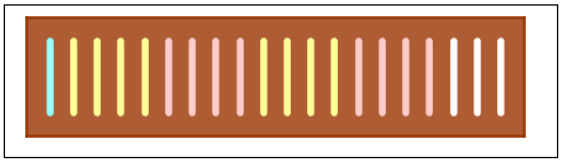
$$1092 = 2^2 \times 3 \times 7 \times 13$$

Le nombre de diviseurs positifs de 1092 est : (1+2)(1+1)(1+1)(1+1)= 24

C. SITUATION COMPLEXE

Un élève de terminale C, passionné par l'émission « fort boyard » y découvre le jeu suivant :

Le principe du jeu est que l'on dispose de 20 bâtonnets placés sur une table comme le montre la figure ci-contre.



Deux joueurs prennent chacun, à tour de rôle un,

Deux ou trois bâtonnets.
Celui qui prend le dernier bâtonnet perd la partie.

L'élève pense qu'il existe une stratégie de gagner pour le joueur qui commence la partie. N'étant pas très sûr, il te propose de l'aider à trouver cette stratégie.

À l'aide d'une production argumentée, trouve cette stratégie.

Solution

- **Pour découvrir la stratégie nous allons utiliser l'arithmétique.**

Le joueur qui commence doit toujours laisser à son adversaire un nombre de bâtonnets congru à 1 modulo 4. Ainsi à un moment de la partie l'adversaire se retrouvera avec 5 bâtonnets, car $5 \equiv 1[4]$. Donc quel que soit le nombre de bâtonnets pris par ce adversaire, il aura à la fin un dernier bâtonnet.

D. EXERCICES

Exercice 1

m et n sont des nombres entiers relatifs. Pour chacun des énoncés suivants, une seule des trois réponses proposées est exacte.
Indique la bonne réponse. (Exemple 5- A)

		Réponses		
N°	Énoncé	A	B	C
1	$n(n+1)$ est un multiple de	3	2	6
2	$n(n-1)(n+1)$ est divisible par	7	5	3
3	Le reste de la division de 23 par –3 est	2	–2	–1

Exercice 2

1) Détermine les entiers naturels *n* tels que : $5^n \equiv -1\ [13]$.
2) Détermine les entiers naturels *n* tels que 13 divise $5^n + 5^{2n}$.

Solution

1) On calcule les premiers termes et on trouve $5^0 \equiv 1\ [13]$, $5^1 \equiv 5\ [13]$, $5^2 \equiv -1\ [13]$, $5^3 \equiv -5\ [13]$, $5^4 \equiv 1\ [13]$, $5^6 \equiv 5\ [13]$, $5^7 \equiv -1\ [13]$,... On voit clairement apparaître le cycle 1,5,−1,−5,1,5,−1, ce qui nous incite à démontrer par récurrence sur $p \in \mathbb{N}$ la propriété suivante : $5^{4p} \equiv 1\ [13]$, $5^{4p+1} \equiv 5\ [13]$, $5^{4p+2} \equiv -1\ [13]$, $5^{4p+3} \equiv -5\ [13]$.
• La propriété est vraie pour $p = 0$ comme le montre le calcul précédent.

• Soit $k \in \mathbb{N}$ tel que $5^{4k} \equiv 1\ [13]$, $5^{4k+1} \equiv 5\ [13]$, $5^{4k+2} \equiv -1\ [13]$, $5^{4k+3} \equiv -5\ [13]$.
Alors on a$5^{4(k+1)} = 5^{4k} \times 5^4$et $5^{4(k+1)} \equiv 1 \times 1\ [13]$.
La démonstration pour les trois autres cas est exactement similaire.
Donc la propriété est vraie pour $k + 1$.
• Pour tout $p \in \mathbb{N}$, $5^{4p} \equiv 1\ [13]$, $5^{4p+1} \equiv 5\ [13]$, $5^{4p+2} \equiv -1\ [13]$, $5^{4p+3} \equiv -5\ [13]$

Ainsi, les entiers naturels solutions de $5^n \equiv -1\ [13]$ sont exactement les entiers de la forme $4p + 2$, avec $p \in \mathbb{N}$

2) On a $5^n + 5^{2n} = 5^n(1 + +5^n)$.
Si $13|5^n + 5^{2n}$, puisque $5 \wedge 13 = 1$, le théorème de Gauss assure que $13|1 + +5^n$, autrement dit que $5^n \equiv -1\ [13]$. D'après la question précédente, ceci est équivalent à dire que $n = 4p + 2$, avec $p \in \mathbb{N}$. Réciproquement, si $n = 4p + 2$ pour un certain $p \in \mathbb{N}$, on sait que $13|1 + +5^n$ et donc $13|5^n(1 + +5^n)$, c'est à dire $13|5^n + 5^{2n}$.
Les entiers *n* solutions sont donc exactement ceux qui s'écrivent $4p + 2$, avec $p \in \mathbb{N}$

Exercice 3

Démontre que $11|(174277^{2625} - 1)$.

Solution

$174277 \equiv (7 - 7 + 2 - 4 + 7 - 1)[11] \equiv 4[11]$.

$2625 = 5 \times 525$;

$174277^{2624} \equiv 4^{2625}[11] \equiv 4^{5\times525}[11] \equiv (4^5)^{525}[11]$ or $4^5 = 1024 \equiv 1[11]$.

Donc $174277^{2625} \equiv (1)^{525}[11] \equiv 1[11] \Leftrightarrow (174277^{2625} - 1) \equiv 0[11]$

Conclusion : $11|174277$.

Exercice 4

On donne $a = 17$ dans le système décimal. En remarquant que $a = 16 + 1$;

Ecris dans le système de numération hexadécimal les nombres : a ; a^2 ; a^3 ; a^4 .

Solution

Les chiffres du système hexadécimal sont : $0; 1; 2; 3; 4; 5; 6; 7; 8; 9; A; B; C; D; E; F$.

$a = 17 = 16 + 1 = 1 \times 16^1 + 1 \times 16^0$.

Donc $\overline{a} = 11$.

$a^2 = (16 + 1)^2 = 16^2 + 2 \times 16 + 1 = 1 \times 16^2 + 2 \times 16^1 + 1 \times 16^0$.

Donc $\overline{a^2} = 121$.

$a^3 = (16 + 1)^3 = 16^3 + 3 \times 16^2 + 3 \times 16 + 1 = 1 \times 16^3 + 3 \times 16^2 + 3 \times 16^1 + 1 \times 16^0$

Donc $\overline{a^3} = 1331$.

$a^4 = a^2 \times a^2$. Je pose l'opération

$$\begin{array}{r} 121 \\ \times\ 121 \\ \hline 121 \\ 242 \\ 121 \\ \hline 14641 \end{array}$$

$\overline{a^4} = 14641$.

Exercice 5

Soit l'entier naturel $x = 2^n - 1, n \geq 2$ dans le système décimal.

1) Déterminez l'écriture de x dans le système binaire.
2) Soient les entiers y et z d'écriture binaire respective $\overline{11111}$ et $\overline{1111111111}$; Démontrez que $y|z$.

Solution

1) $x = 2^n - 1 = (2-1)(2^{n-1} + 2^{n-2} + \cdots + 2 + 1) = 2^{n-1} + 2^{n-2} + \cdots + 2 + 1$. Donc on a : $\overline{x} = 111 \ldots 1$ où il y a n chiffres 1.
2) $\overline{y} = 11111$ donc en système décimal $y = 2^5 - 1$
   $\overline{z} = 1111111111$ donc en système décimal $z = 2^{10} - 1$.
   $z = 2^{10} - 1 = 2^{2\times5} - 1 = (2^5)^2 - 1 = (2^5 - 1)(2^5 + 1) = y(2^5 + 1)$.
   Comme $(2^5 + 1) \in \mathbb{N}$ alors $y|z$.
   Autre méthode :
   $y = 2^5 - 1 = 31$ et $z = 2^{10} - 1 = 1023 = 31 \times 33$. Donc $y|z$.

Exercice 6

Démontrez que le nombre entier naturel x qui s'écrit en base a , $a > 1$; $\overline{11111 \ldots 111}$, n chiffres égaux à 1 s'écrit $x = \frac{a^n - 1}{a - 1}$.

Solution

Soit x l'entier naturel qui s'écrit en base a , $a > 1$; $\overline{x} = 111 \ldots 1$ où il y a n chiffres 1.

On sait que : $x = a^{n-1} + a^{n-2} + \cdots + a^2 + a + 1$,
or $(a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1) = a^n - 1$.

Comme $a \neq 1$, alors $\frac{a^n - 1}{a - 1} = a^{n-1} + a^{n-2} + \cdots + a + 1 = x$.

Exercice 7

1) Soit $q \in \mathbb{N}$, on veut démontrer que $q\ impair \Leftrightarrow q^2\ est\ impair$.
   a- Démontrez que si q est impair alors q^2 est impair.
   b- Démontrez que si q^2 est impair alors q est impair.
2) Démontrez que si q est impair alors $q^2 \equiv 1[8]$.

Solution

1°) Soit $q \in \mathbb{N}$.

a. Supposons que q soit impair, il existe $k \in \mathbb{N}$ tel que $q = 2k + 1$.

$q^2 = (2k+1)^2 = 2(2k^2 + 2k) + 1 = 2l + 1\ \ avec\ l = (2k^2 + 2k) \in \mathbb{N}$. Donc q^2 est impair.

b. Supposons que q^2 soit impair, il existe $k \in \mathbb{N}$ tel que $q^2 = 2k + 1 \Leftrightarrow q^2 - 1 = 2k$

Soit $(q-1)(q+1) = 2k \Leftrightarrow 2|(q-1)(q+1)$. Comme 2 est un nombre premier alors $2|(q-1)\ \ ou\ \ 2|(q+1)$ d'après le théorème de Gauss.
Donc $q = 2l + 1\ \ ou\ \ q = 2l - 1\ \ , l \in \mathbb{N}$ .D'où q est impair.

2°) Supposons que q soit impair, il existe $k \in \mathbb{N}$ tel que $q = 2k + 1$;

$q^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1 \Leftrightarrow q^2 - 1 = 4k(k+1)$.

- Si k est pair alors $k = 2l\ , l \in \mathbb{N}$. $q^2 - 1 = 4(2l)(2l+1) = 8l(2l+1)$.
- Si k est impair alors $k = 2l + 1\ , l \in \mathbb{N}$.
  $q^2 - 1 = 4(2l+1)(2l+1+1) = 8(l+1)(2l+1)$
- Dans tous les cas si q est impair, $8|(q^2-1)$, donc $(q^2 - 1) \equiv 0[8]$.

Exercice 8

1) Démontrez que si un entier naturel n est premier alors $n + 7$ n'est pas premier.
2) Soit $a \in \mathbb{Z}$;
   a- Développez le produit $(a^2 - a + 1)(a^2 + a + 1)$.
   b- L'entier $a^4 + a^2 + 1$ peut-il être un nombre premier ?
3) Déterminez l'ensemble des entiers x tels que :
   a- $(x + 5) \equiv 3[8]$.
   b- $3x \equiv 5[8]$.
4) Démontrez que si $2|(a^2 + b^2)$ alors $2|(a+b)^2$; où $a\ \ et\ \ b$ sont deux entiers.

Solution

1) Soit $n \in \mathbb{N}$, supposons que n soit un nombre premier.

- Si $n = 2$ alors $n + 7 = 2 + 7 = 9 = 3 \times 3$, $n + 7$ n'est pas un nombre premier.
- Pour $n > 2$, tout nombre premier plus grand que 2 est un nombre impair.
  Donc $n = 2k + 1\ , k \in \mathbb{N}\ \ avec\ k \neq 0$; $n + 7 = 2k + 1 + 7 = 2k + 8 = 2(k+4)$.
  $n + 7$ est un nombre composé car $k + 4 > 4$, donc $n + 7$ n'est pas un nombre premier.

Conclusion :
Si n est un nombre premier alors $n + 7$ n'est pas un nombre premier.

2) Soit $a \in \mathbb{Z}$.

a. $(a^2-a+1)(a^2+a+1)=[(a^2+1)-a][(a^2+1)+a]=(a^2+1)^2-a^2$;
$(a^2-a+1)(a^2+a+1)=a^4+a^2+1$.

b. Si $(a^2-a+1)=1$ alors $a^2-a=0$; ce qui donne $a=0\ ou\ a=1$.

- Pour $a=0$, $a^4+a^2+1=1$ n'est pas un nombre premier.
- Pour $a=1$, $a^4+a^2+1=3$ est un nombre premier.

Si $(a^2+a+1)=1$ alors $a^2+a=0$; ce qui donne $a=0\ \ ou\ a=-1$.

- Pour $a=0$, $a^4+a^2+1=1$ n'est pas un nombre premier.
- Pour $a=-1$, $a^4+a^2+1=3$ est un nombre premier.

Pour $a\neq 1\ et\ a\neq -1$;

- Si $a\geq 2$ alors $a^2\geq 4$; ce qui donne $a^2+a+1\geq 7$.
  $a^2-a+1=(a-\frac{1}{2})^2+\frac{3}{4}$, or pour $a\geq 2$; $a-\frac{1}{2}\geq\frac{3}{2}$ donc $(a-\frac{1}{2})^2\geq\frac{9}{4}$.
  D'où $(a-\frac{1}{2})^2+\frac{3}{4}\geq 3$.
  Comme $a^4+a^2+1=(a^2-a+1)(a^2+a+1)$ avec
  $a^2+a+1\geq 7\ et\ a^2-a+1\geq 3$, alors a^4+a^2+1 n'est pas un nombre premier.
- Si $a\leq -2$ alors $a^2\geq 4$; ce qui donne $a^2-a+1\geq 7$.
  $a^2+a+1=(a+\frac{1}{2})^2+\frac{3}{4}$, or $a\leq -2$ entraine $\left(a+\frac{1}{2}\right)\leq -\frac{3}{2}$, ce qui donne
  $(a+\frac{1}{2})^2\geq\frac{9}{4}$; donc $(a+\frac{1}{2})^2+\frac{3}{4}\geq 3$.
  Comme $a^4+a^2+1=(a^2-a+1)(a^2+a+1)$ avec
  $a^2-a+1\geq 7\ et\ a^2+a+1\geq 3$, alors a^4+a^2+1 n'est pas un nombre premier.

3) a. $(x+5)\equiv 3[8]\Leftrightarrow x+5=3+8k,k\in\mathbb{Z}\Leftrightarrow x=-2+8k,k\in\mathbb{Z}$
   $\Leftrightarrow x=6+8k,k\in\mathbb{Z}\Leftrightarrow x\equiv 6[8]$.
   b. Remplissons un tableau de multiplication modulo 8

$\overline{x}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$3\overline{x}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{1}$	$\overline{4}$	$\overline{7}$	$\overline{2}$	$\overline{5}$

On en déduit que $3x\equiv 5[8]\Leftrightarrow x\equiv 7[8]\Leftrightarrow x=7+8k,k\in\mathbb{Z}$.

4) Supposons que 2 divise (a^2+b^2), il existe $k\in\mathbb{Z}$ tel que $(a^2+b^2)=2k$, or
   $(a^2+b^2)=(a+b)^2-2ab$, donc
   $(a+b)^2=(a^2+b^2)+2ab=2k+2ab=2(k+ab)$.
   Comme $a\in\mathbb{Z},b\in\mathbb{Z}\ et\ k\in\mathbb{Z}$ alors $(k+ab)\in\mathbb{Z}$.
   Conclusion :
   Si $2|(a^2+b^2)$ alors $2|(a+b)^2$.

Exercice 9

CODAGE AFFINE.

Le codage est défini par l'application
$\underset{x\mapsto y}{f:\mathcal{F}\to\mathcal{F}}$, où y est le reste de la division euclidienne de $x+10$ par 26 :
$x+10=26k+y$, $0\leq y<26$, c'est-à-dire que : $(x+10)\equiv y[26]$, $0\leq y<26$.

a- Codez le mot MATHS.
b- Démontrez que tout élément $a \in \mathcal{F}$ est l'image par f d'un seul élément de $\mathcal{F}$.
c- Décodez le mot : VIWK

Solution

a- Codage du mot MATHS.

	M	A	T	H	S
X	12	0	19	7	18
y	22	10	3	17	2

- $12 + 10 = 22 = 0 \times 26 + 22$
- $0 + 10 = 10 = 0 \times 26 + 10$
- $19 + 10 = 29 = 1 \times 26 + 3$
- $7 + 10 = 17 = 0 \times 26 + 17$
- $18 + 10 = 28 = 1 \times 26 + 2.$

Le codage du mot MATHS est : WKDRC.

b- Soit $a \in \mathcal{F}$.
$f(x) = a \Leftrightarrow (x + 10) = 26k + a\,, 0 \leq a < 26\,, k \in \mathbb{Z}$.
$f(x) = a \Leftrightarrow x = (a - 10) + 26k, k \in \mathbb{Z} \Leftrightarrow x \equiv (a - 10)[26]$. Or $-10 \equiv 16[26]$.
Donc $f(x) = a \Leftrightarrow x \equiv (a + 16)[26]$.
Conclusion :
Si $x \equiv (a + 16)[26]$ alors $f(x) = a$.

c- Décodage de VIWK.

	V	I	W	K
a	21	8	22	10
x	11	24	12	0

- $21 + 16 = 37 = 1 \times 26 + 11$
- $8 + 16 = 24 = 0 \times 26 + 24$
- $22 + 16 = 1 \times 26 + 12$
- $10 + 16 = 26 = 1 \times 26 + 0.$

Le mot codé par VIWIK est LYMA.

Exercice 10

CODAGE EXPONENTIEL.

On affecte à chaque entier compris entre 0 et 28 une lettre de l'alphabet ou un symbole.

Lettres	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Chiffres	0	1	2	3	4	5	6	7	8	9	10	11	12	13

Lettres	O	P	Q	R	S	T	U	V	W	X	Y	Z	α	β	γ
chiffres	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

On définit ainsi l'ensemble $\mathcal{G}$ suivant :

$\mathcal{G} = \{0; 1; 2; 3; 4; 5; 6; 7; 8; 9; 10; 11; 12; 13; 14; 15; 16; 17; 18; 19; 20; 21; 22; 23; 24; 25; 26; 27; 28\}$

Le codage est défini par :

$\begin{matrix} f:\mathcal{G}\to\mathcal{G} \\ x\mapsto y \end{matrix}$, où y est le reste de la division euclidienne de x^3 par 29 :

$x^3 = 29k + y$, $0 \leq y < 29$, c'est-à-dire que : $x^3 \equiv y[29]$, $0 \leq y < 29$.

Soit $g(x) = x^3$. $f(x) = y \Leftrightarrow g(x) \equiv y[29]$.

a- Codez les mots : MER et LYCEE.

b- En remarquant que $3 \times 19 - 28 \times 2 = 1$, démontrez que 3 et 28 sont premiers entre eux.

c- Démontrez que si $f(x) = f(x')$ alors $x = x'$.

d- En déduire que deux éléments différents de $\mathcal{G}$ ont des images différentes par f.

e- Soit $(x; y) \in \mathcal{G} \times \mathcal{G}$ tel que $y = x^3$. Démontrez que $y^{19} \equiv x[29]$.

f- Décodez alors les mots : $TW\beta TIG \;\; et \;\; ZM\alpha R$.

Solution

a) Codage du mot MER.

	M	E	R
X	12	4	17
y	17	6	12

- $12^3 = 1728 = 29 \times 59 + 17$
- $4^3 = 64 = 29 \times 2 + 6$
- $17^3 = 4913 = 29 \times 169 + 12.$

Le codage du mot MER est : RGM.

Codage du mot : LYCEE.

	L	Y	C	E
X	11	24	2	4
y	26	20	8	6

- $11^3 = 1331 = 29 \times 45 + 26$
- $24^3 = 13824 = 29 \times 476 + 20$
- $2^3 = 8 = 29 \times 0 + 8$
- $4^3 = 64 = 29 \times 2 + 6$.

Le mot LYCEE est codé par : $\alpha UIGG$.

$b - 3 \times 19 - 28 \times 2 = 1$ d'après le théorème de Bézout 3 et 28 sont premiers entre eux.

a- Soit $(x; x') \in \mathcal{G} \times \mathcal{G}$ tel que $f(x) = f(x')$.
$x^3 = 29k + f(x), k \in \mathbb{Z}$ et $x'^3 = 29k' + f(x'), k' \in \mathbb{Z}$.
$\begin{cases} f(x) = x^3 - 29k\ ,\ k \in \mathbb{Z} \\ f(x') = (x')^3 - 29k', k' \in \mathbb{Z} \end{cases} \Leftrightarrow x^3 \equiv (x')^3[29]$.
Donc $(x^3)^{19} \equiv ((x')^3)^{19}[29] \Leftrightarrow x^{3\times19} \equiv (x')^{3\times19}[29]$; or $3 \times 19 - 28 \times 2 = 1$ d'où
$3 \times 19 = 2 \times 28 + 1$ et $x^{28\times2+1} \equiv (x')^{28\times2+1}[29] \Leftrightarrow x^{2\times28} \times x \equiv (x')^{2\times28} \times x'[29]$
Soit $(x^{28})^2 \times x \equiv ((x')^{28})^2 \times x'^{[29]}$.
Comme 29 est un nombre premier et ne divise pas x et x' ($x < 29$ et $x' < 29$) alors d'après le petit théorème de Fermat $x^{28} \equiv 1[29]$ et $(x')^{28} \equiv 1[29]$.
D'où $(x^{28})^2 \equiv 1[29]$ et $((x')^{28})^2 \equiv 1[29]$.
On a alors $\begin{cases} [x^{28}]^2 \times x \equiv x[29] \\ [(x')^{28}]^2 \times x' \equiv x'[29] \end{cases} \Leftrightarrow x \equiv x'[29]$.
Comme $x < 29$ et $x' < 29$ alors $x' = x$.

Donc par contraposée, si $x' \neq x$ $alors$ $f(x') \neq f(x)$.

d- Soit $(x; y) \in \mathcal{G} \times \mathcal{G}$ tel que $y \equiv x^3[29]$.
$y^{19} \equiv (x^3)^{19}[29] \Leftrightarrow y^{19} \equiv x^{3\times19}[29]$.
Or $3 \times 19 - 28 \times 2 = 1 \Leftrightarrow 3 \times 19 = 28 \times 2 + 1$ donc
$y^{19} \equiv x^{28\times2+1}[29]$.
Comme 29 est premier et ne divise pas x ($x < 29$) alors d'après le petit théorème de Fermat,
$x^{28} \equiv 1[29] \Leftrightarrow (x^{28})^2 \equiv 1[29]$; $y^{19} \equiv x^{28\times2} \times x[29] \Leftrightarrow y^{19} \equiv x[29]$.

$e-$ Décodage.

- Le mot : $TW\beta TGI$.

	T	W	β	T	G	I
Y	19	22	27	19	6	8
x	8	13	3	8	4	2

$19 = 18 + 1 = 2 \times 9 + 1$.

- $19^{19} = 19^{18} \times 19 = (19^2)^9 \times 19$; $19^2 = 361 = 29 \times 12 + 13$
  $19^2 \equiv 13[29]$ $donc$ $19^{18} \equiv 13^9[29] \equiv 5[29]$. On en déduit que :
  $19^{19} = 19^{18} \times 19 \equiv 5 \times 19[29] \equiv 8[29]$.
- $22^2 \equiv 20[29]$ $donc$ $22^{18} \equiv 20^9[29]$; $20^9 = (20^4)^2 \times 20$ or
  $20^4 \equiv 7[29]$ $d'o\grave{u}$ $28^8 \equiv 7^2[29] \equiv 20[29]$ et
  $20^9 \equiv 20 \times 20[29] \equiv 23[29]$.
  Conclusion : $22^{19} \equiv 23 \times 22[29] \equiv 13[29]$.
- $27^{19} = 27^{18} \times 27 = (27^2)^9 \times 27$.
  $27^2 \equiv 4[29]$ $donc$ $(27^2)^9 \equiv 4^9[29] \equiv 13[29]$.
  $27^{19} \equiv 13 \times 27[29] \equiv 3[29]$.

- $6^{19} = 6^{18} \times 6 = (6^9)^2 \times 6$, $6^9 \equiv 22[29]$ donc $6^{18} \equiv 22^2[29] \equiv 20[29]$
  $6^{19} \equiv 20 \times 6[29] \equiv 4[29]$.
- $8^{19} = 8^{18} \times 8 = (8^9)^2 \times 8$; $8^2 \equiv 6[29]$, d'où
  $(8^2)^9 \equiv 6^9[29] \equiv 22[29]$. Donc $8^{19} \equiv 22 \times 8[29] \equiv 2[29]$.
  D'où le mot $TW\beta TGI$ correspond à INDICE.

- Le mot: $ZM\alpha R$.

	Z	M	α	R
Y	25	12	26	17
x	20	17	11	12

- $25^{19} = 25^{18} \times 25 = (25^2)^9 \times 25$; $25^2 \equiv 16[29]$ donc
  $25^{18} \equiv 16^9[29] \equiv (16^2)^4 \times 16[29] \equiv 24^4 \times 16[29] \equiv 16 \times 16[29]$ d'où
  $25^{18} \equiv 24[29]$ et $25^{19} \equiv 24 \times 25[29] \equiv 20[29]$.
- $26^{19} = 26^{18} \times 26 = (26^2)^9 \times 26$; $26^2 \equiv 9[29]$ d'où
  $26^{18} \equiv 9^9[29] \equiv 6[29]$ et $26^{19} \equiv 6 \times 26[29] \equiv 11[29]$
- $12^{19} = 12^{18} \times 12 = (12^2)^9 \times 12$ or $12^2 \equiv 28[29] \equiv (-1)[29]$.
  $12^{18} \equiv (12^2)^9[29] \equiv (-1)^9[29] \equiv (-1)[29] \equiv 28[29]$.
  $12^{19} \equiv 28 \times 12[29] \equiv 17[29]$.
- $17^{19} = 17^{18} \times 17 = (17^2)^9 \times 17$; $17^2 \equiv 28[29] \equiv (-1)[29]$.
  $17^{18} \equiv (-1)^9[29] \equiv (-1)[29]$ donc
  $17^{19} \equiv (-1) \times 17[29] \equiv (-17)[29] \equiv 12[29]$.

Donc $ZM\alpha R$ correspond au mot : URLM.