Arithmétique partie I

i Dans ce chapitre : $a|b$, **division euclidienne**, **congruences**.

D **quelques définition**

- $\mathbb{N} = \{0\,;1\,;2\,;\ldots\}$ est l'ensemble des entiers naturels
- $\mathbb{Z} = \{\ldots\,;-2\,;-1\,;0\,;1\,;2\,;\ldots\}$ est l'ensemble des entiers relatifs
- $\mathbb{N}^* = \mathbb{N} \setminus \{0\} = \{1\,;2\,;\ldots\}$, $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\} = \{\ldots\,;-2\,;-1\,;1\,;2\,;\ldots\}$

P **quelques propriétés**

- la somme et le produit de deux entiers naturels sont des entiers naturels : on dit que $\mathbb{N}$ est **stable** pour l'addition et la multiplication
- $\mathbb{Z}$ est stable par addition, multiplication et aussi soustraction
- il n'y a pas de fraction dans $\mathbb{N}$ et il n'y a pas de fraction dans $\mathbb{Z}$

M **un peu de logique**

- les écritures suivantes signifient la même chose : « A implique B », « si A est vraie, alors B est vraie », « $A \Rightarrow B$ »
- montrer que « $A \Rightarrow B$ » revient à montrer que « $non\ B \Rightarrow non\ A$ », « $non\ B \Rightarrow non\ A$ » est la **forme contraposée** de « $A \Rightarrow B$ »
- pour démontrer que C est vraie, on peut :

– montrer que C est une conséquence logique d'une affirmation que l'on sait être vraie

ou bien, on peut :

– supposer que C est fausse, obtenir à un moment une contradiction ce qui permet finalement de rejeter l'hypothèse que C est fausse donc d'en déduire que C est vraie

- « A équivaut à B » signifie que « $A \Rightarrow B$ et $B \Rightarrow A$ »

(« $\Leftrightarrow$ » peut être remplacé par : « cela revient à dire que »)

i Sauf indication contraire, dans ce chapitre on travaille dans $\mathbb{Z}$.

D Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$. Alors « a **divise** b » signifie « il existe $k \in \mathbb{Z}$ tel que : $b = k \times a$ » ; « a divise b » se note « $a|b$ ».

▶ $a|\boldsymbol{b} \overset{déf}{\Leftrightarrow}$ il existe $k \in \mathbb{Z}$ tel que $\boldsymbol{b} = k \times a$

i On écrit : $a|\boldsymbol{b} \overset{déf}{\Leftrightarrow} \exists k \in \mathbb{Z}$ tel que $\boldsymbol{b} = k \times a$.

Lorsque $a|b$ ont dit aussi que a **est un diviseur de** b ou encore que b **est un multiple de** a.

A01 **Écrire une égalité pour justifier** …

- écrire une égalité montrant que : $5 \mid (-15)$
- écrire une égalité montant que : $(-8) \mid (-32)$
- on sait que $x \in \mathbb{Z}$, $y \in \mathbb{Z}$, $x = 7y$: quelles affirmations peut-on en déduire parmi : $x|y$, $y|x$, $x|7$, $7|x$, $7|y$ et $y|7$?
- un élève affirme « $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}$, on a : $a + b|a^2 - b^2$ », si cette affirmation est vraie la démontrer, sinon en donner un contre-exemple

P ▶Pour tout $a \in \mathbb{Z}$, on a : $\boldsymbol{1}|\boldsymbol{a}$, $(-\boldsymbol{1})|\boldsymbol{a}$, $\boldsymbol{a}|\boldsymbol{a}$ et $(-\boldsymbol{a})|\boldsymbol{a}$.

A02 Justifier chacune des affirmations de la propriété précédente.

P **Le cas particulier de 0**

Tout entier relatif divise 0 : $\forall \boldsymbol{a} \in \mathbb{Z}$, $\boldsymbol{a}|\boldsymbol{0}$, en particulier : $\boldsymbol{0}|\boldsymbol{0}$.

▶ si $\boldsymbol{a} \neq \boldsymbol{0}$, alors 0 ne divise pas a : $\boldsymbol{a} \neq \boldsymbol{0} \Rightarrow non\ (0|a)$

A03 Démontrer les deux points de la propriété précédente.

P Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$. On a les équivalences :

▶ $\boldsymbol{b}|\boldsymbol{a} \Leftrightarrow (-\boldsymbol{b})|\boldsymbol{a} \Leftrightarrow \boldsymbol{b}|(-\boldsymbol{a}) \Leftrightarrow (-\boldsymbol{b})|(-\boldsymbol{a})$

A04 Démontrer la première équivalence de la propriété précédente.

[D] Pour tout $x \in \mathbb{R}$, on pose : $|x| = \sqrt{x^2}$.

[P] Soient x et y deux réels, on a :

- $|x| \geqslant 0$
- $|0| = 0$
- **si** $x \geqslant 0$ **alors** $|x| = x$
- $|x \times y| = |x| \times |y|$
- $|-x| = |x|$
- $|1| = |-1| = 1$
- **si** $x < 0$ **alors** $|x| = -x$
- $|x| = 0 \Leftrightarrow x = 0$

A05 Démontrer chacun des points de la propriété précédente.

[P] ▶Tout diviseur positif de $a \neq 0$ est compris au sens large entre 1 et $|a|$: $\begin{cases} a \in \mathbb{Z} \setminus \{0\} \\ d \in \mathbb{N} \text{ et } d|a \end{cases} \Rightarrow 1 \leqslant d \leqslant |a|$.

A06 Démontrer la propriété précédente.

A07 Un élève dit « si $a \in \mathbb{Z}$, $d \in \mathbb{N}$ et $d|a$, alors $1 \leqslant d \leqslant |a|$ ». Trouver l'erreur.

A08 Donner sans justification les diviseurs de (-15).

[i] Pour $a \in \mathbb{Z} \setminus \{0\}$, la commande **ListeDiviseurs**(a) dans GeoGebra donne la liste des diviseurs positifs de a.

A09 Démontrer que : $\forall (a,b) \in \mathbb{Z}^2$, on a : $4|(a+b)^2 - (a-b)^2$.

A10 A-t-on « $\forall n \in \mathbb{N}$, $3|2^n + 2^{n+1}$ » ?

[D] Des entiers **consécutifs** sont des entiers dont la différence est 1.

A11 Que penser de l'affirmation « la somme de trois entiers relatifs consécutifs est divisible par 3 » ?

[P] Pour tout $(a,b,c) \in \mathbb{Z}^3$ on a l'**implication** : ▶ $a|b$ **et** $b|c \Rightarrow a|c$.
C'est la **transitivité** de la divisibilité.

A12 Démontrer la transitivité de la divisibilité.

[P] **divisibilité et combinaison linéaire**

▶ Si un entier divise deux nombres, alors il divise toute combinaison linéaire de ces deux nombres.

Remarques :
– la réciproque est vraie mais dans un exercice c'est souvent une combinaison linéaire particulière qui intervient,
– si un entier relatif divise deux nombres alors il divise leur somme et il divise leur différence (attention : la réciproque est fausse).

A13 Démontrer la propriété précédente, ainsi que sa réciproque.

A14 Que penser de l'affirmation « pour tous entiers relatifs a, b, c, d on a l'implication : $a|b$ et $c|d \Rightarrow a+c|b+d$ et $a-c|b-d$ » ?

On **ne peut pas** ajouter ou soustraire « membre à membre » des relations de divisibilité.

A15 Rappelons que, pour $a \in \mathbb{N}$ et $b \in \mathbb{N} \setminus \{0\}$, dire que b est un diviseur de a revient à dire que le reste de la division euclidienne de a par b est nul ; en **Python, le reste de cette division est : $a\%b$**.
Écrire un programme Python qui demande d'entrer un entier naturel non nul puis affiche la liste de ses diviseurs positifs.

A16 Déterminer tous les entiers naturels n tels que : $n-3|7$.

[P] ▶Tout diviseur de $a \neq 0$ est compris entre : $-|a|$ et $|a|$.
(pour tout $a \in \mathbb{Z} \setminus \{0\}$, si $d|a$ alors : $-|a| \leqslant d \leqslant |a|$ et $d \neq 0$)

A17 Déterminer les entiers relatifs n tels que : $n+3|2n+1$.

P ▶Si $a|b$, alors a divise tout multiple de b.
(pour tous a, b, c dans $\mathbb{Z}$, on a l'**implication** : $a|b \Rightarrow a|b \times c$)

A18 Démontrer la propriété précédente.

A19 Résoudre dans $\mathbb{Z}$: « $n+1|2n+3$ et $n+1|3n+2$ ».

D La **partie entière** d'un réel x est l'unique **entier relatif** note $E(x)$ vérifiant : $\boldsymbol{E(x) \leqslant x < E(x)+1}$.
exemples $E(7{,}9)=7$, $E(3)=3$, $E(1{,}6)=1$, $E(-0{,}2)=-1$.

i En Python la partie entière de x est `floor(x)`, accessible après `from math import *`, ne pas utiliser int(...).

D **Division euclidienne dans $\mathbb{N}$**
Pour $a \in \mathbb{N}$ et $b \in \mathbb{N} \setminus \{0\}$, **effectuer la division euclidienne** de a par b c'est déterminer les deux entiers **naturels** q et r tels que :

$$\boldsymbol{a = q \times b + r} \text{ avec } \boldsymbol{0 \leqslant r < b}$$

i Pour une division euclidienne par $b > 0$, à priori il y a exactement b valeurs possibles pour le reste r, qui sont : $0, \ldots, b-1$.

A20 On souhaite démontrer la propriété précédente.

Soient $a \in \mathbb{N}$ et $b \in \mathbb{N} \setminus \{0\}$, on travaille dans $\mathbb{R}$, on pose $q = E\left(\frac{a}{b}\right)$.

1. **Existence**
   - **a.** Justifier que $q \geqslant 0$ puis montrer que : $0 \leqslant a - qb < b$.
   - **b.** On pose $r = a - qb$, justifier que : $a = qb + r$ et $0 \leqslant r < b$.
2. **Unicité**
   Soient q, r, q' et r' des entiers naturels vérifiant :
   $a = qb + r$, $a = q'b + r'$, $0 \leqslant r < b$ et $0 \leqslant r' < b$ avec $r \geqslant r'$
   - **a.** Démontrer que : $b|r - r'$.
   - **b.** Démontrer que : $-b < r - r' < b$.
   - **c.** Montrer que $r = r'$, en déduire que $q = q'$.

A21 Le produit de trois entiers relatifs consécutifs est-il toujours divisible par 3 ?

A22 On remarque que : $1\,336 = 57 \times 23 + 25$. En déduire le reste et le quotient de la division euclidienne de $1\,336$ par 23.

A23 $a \in \mathbb{N}$ et le reste de la division euclidienne de a par 5 est 4.
Quel est le reste de la division euclidienne de $2a$ par 5, et quel est le reste de la division euclidienne de $3a$ par 5 ?

A24 Déterminer le quotient et le reste de la division euclidienne de $16\,881$ par 12 puis écrire l'égalité qui en résulte.

A25 Pour tout $n \in \mathbb{N}$, on pose $a_n = 10n^2 + 22n + 14$, $b_n = 2n + 3$, on note r_n le reste de la division euclidienne de a_n par b_n.

- vérifier que, pour tout $n \in \mathbb{N}$, on a :
$$10n^2 + 22n + 14 = (5n+3)(2n+3) + n + 5$$
- donner un contre-exemple à « pour tout $n \in \mathbb{N}$, $r_n = n + 5$ »
- déterminer r_n en fonction de n en distinguant plusieurs cas

A26 Pour tout $n \in \mathbb{N}$, on pose : $a_n = 7n + 17$, $b_n = 2n + 5$, on note r_n le reste de la division euclidienne de a_n par b_n.

1. Déterminer a_0 et b_0 puis poser la division euclidienne de a_0 par b_0, en déduire r_0.
   Procéder de même pour a_1, b_1 et r_1.
2. À l'aide de la calculatrice, énoncer une conjecture sur r_n en fonction de n, puis démontrer cette conjecture.
3. On se propose de retrouver r_n en fonction de n par une autre méthode.
   Soit $n \in \mathbb{N}$. Poser la division euclidienne de $7n + 17$ par $2n + 5$, en déduire r_n.

D **Division euclidienne dans $\mathbb{Z}$**

▶Soit $a \in \mathbb{Z}$ et $b \in \mathbb{Z} \setminus \{0\}$. Alors il existe un unique couple (q, r) tel que : $q \in \mathbb{Z}$, $r \in \mathbb{N}$ et $\boldsymbol{a = qb + r}$ avec $\boldsymbol{0 \leqslant r < |b|}$.

💣 le **reste r** est toujours **positif ou nul**

Pour la division euclidienne de a par $b \neq 0$: a est le **dividende**, q est le **quotient**, b est le **diviseur** et r est le **reste**.

i Pour une division euclidienne par $b \neq 0$, à priori il y a exactement $|b|$ valeurs possibles pour le reste r, qui sont : $0, \ldots, |b| - 1$.

i Soient $a \in \mathbb{N}$ et $b \in \mathbb{N} \setminus \{0\}$, la division euclidienne dans $\mathbb{N}$ et celle dans $\mathbb{Z}$ donnent le même couple d'entiers (q, r).

A27 Écrire l'égalité traduisant la division euclidienne de 123 par 10 puis déterminer le quotient et le reste de la division euclidienne de 123 par (-10), de (-123) par 10 et enfin de (-123) par (-10).

i Pour une division euclidienne de $a > 0$ par $b > 0$ les commandes partEnt(…), reste(…) de la calculatrice et les commandes $//$, $\%$ de Python sont utilisables, 💣 si a ou b est négatif elles sont interdites.

A28 Déterminer le quotient et le reste de la division euclidienne de 132 par (-5).

A29 Déterminer le quotient et le reste de la division euclidienne de $(-1\,245)$ par (-12).

A30 Déterminer le quotient et le reste de la division euclidienne de (-75) par 80.

D ▶On dit que $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ sont **congrus modulo $\boldsymbol{m} \in \mathbb{N} \setminus \{0\}$** lorsque a et b ont **même reste** pour la division euclidienne par m, on écrit : $\boldsymbol{a \equiv b\ [m]}$, $\boldsymbol{a \equiv b\ (m)}$ ou encore $\boldsymbol{a \equiv b}$ **mod $\boldsymbol{m}$**.

i 💣 m est nécessairement strictement positif

A31 Justifier que $176 \equiv 36\ [5]$.

A32 Justifier que $32 \equiv 20\ [6]$.

P Soient $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ et $m \in \mathbb{N} \setminus \{0\}$, on a l'équivalence :

▶ $\boldsymbol{a \equiv b\ [m] \Leftrightarrow m|a - b}$

(deux entiers sont congrus modulo $m \Leftrightarrow m$ divise leur différence)

A33 Preuve.

Lemme Pour tout réel x et tout réel $\varepsilon > 0$, on a l'équivalence : $-\varepsilon < x < \varepsilon \Leftrightarrow |x| < \varepsilon$.

Les divisions euclidiennes de a par m et b par m s'écrivent : $a = qm + r$ et $b = q'm + r'$ avec $0 \leqslant r < m$ et $0 \leqslant r' < m$.

1. Montrer que : $|r - r'| < m$.
2. On suppose $a \equiv b\ [m]$, montrer que : $m|a - b$.
3. On suppose $m|a - b$.
   - **a.** Montrer que : $m|r - r'$.
   - **b.** On suppose que $r \neq r'$, déduire de **a.** que $m \leqslant |r - r'|$. Mettre en évidence une contradiction, en déduire $a \equiv b\ [m]$.
4. Démontrer le Lemme.

A34 Justifier que : $317 \equiv 17\ [50]$.

P Pour $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $c \in \mathbb{Z}$ et $m \in \mathbb{N} \setminus \{0\}$:

▶ $\boldsymbol{a \equiv a\ [m]}$

▶ $\boldsymbol{a \equiv b\ [m] \Leftrightarrow b \equiv a\ [m]}$

▶ $\boldsymbol{a \equiv b\ [m]}$ **et** $\boldsymbol{b \equiv c\ [m] \Rightarrow a \equiv c\ [m]}$

i La relation $\equiv$ est : **réflexive**, **symétrique** et **transitive**.

▶ $\boldsymbol{m|a \Leftrightarrow a \equiv 0\ [m]}$

Une relation de **divisibilité** avec diviseur positif **se traduit donc par une congruence à zéro**.

A35 Démontrer les quatre points précédents.

A36 Résoudre dans $\mathbb{Z}$: $x \equiv 3\ [7]$.

P Pour $a \in \mathbb{Z}, b \in \mathbb{Z}, c \in \mathbb{Z}, m \in \mathbb{N} \setminus \{0\}$ on a les équivalences :
▶ $\boldsymbol{a \equiv b\ [m] \Leftrightarrow a + c \equiv b + c\ [m]}$
▶ $\boldsymbol{a \equiv b\ [m] \Leftrightarrow a - c \equiv b - c\ [m]}$
▶ $\boldsymbol{a \equiv b\ [m] \Rightarrow a \times c \equiv b \times c\ [m]}$ c'est une **implication** !
On peut donc :
– ajouter/soustraire membre à membre deux congruences,
– multiplier par un même entier relatif les deux membres d'une relation de congruence et c'est une **implication**.

A37 Démontrer les trois points de la propriété précédente.

A38 Justifier que : $5 \times 6 \equiv 1 \times 6\ [3]$; a-t-on « $5 \equiv 1\ [3]$ » ?

i On ne doit pas « simplifier par c » la relation $ac \equiv bc\ [m]$.

P Soient $a \in \mathbb{Z}, b \in \mathbb{Z}$ et $m \in \mathbb{N} \setminus \{0\}$, on a les équivalences :
▶ $\boldsymbol{a \equiv b\ [m] \Leftrightarrow \exists k \in \mathbb{Z}, a = b + km}$

A39 Démontrer la propriété précédente puis l'utiliser pour traduire :
• $x \equiv 4\ [9]$ • $\exists k \in \mathbb{Z}, y = 3 + 5k$

A40 Résoudre dans $\mathbb{Z}$: $x - 1 \equiv 2\ [8]$.

A41 Déterminer les entiers relatifs x compris entre 10 et 20 tels que : $x + 3 \equiv 5\ [6]$.

P Pour tous $a \in \mathbb{Z}$, $k \in \mathbb{Z}$ et $m \in \mathbb{N} \setminus \{0\}$, on a :
▶ $\boldsymbol{a \equiv a + km\ [m]}$
▶ $\boldsymbol{a \equiv a - km\ [m]}$
(on peut ajouter/soustraire à un membre un multiple du modulo)

A42 Démontrer le premier point de la propriété **précédente**.

A43 Vérifier que : $5^2 \equiv 3^2\ [8]$; a-t-on $5 \equiv 3\ [8]$?

P Soient $a \in \mathbb{Z}, b \in \mathbb{Z}, m \in \mathbb{N} \setminus \{0\}$ et $n \in \mathbb{N}$, on a l'implication :
▶ $a \equiv b\ [m] \Rightarrow a^n \equiv b^n\ [m]$.
(la congruence est compatible avec l'élévation à un même exposant naturel et c'est une implication)

i rappelons que dans le cours d'arithmétique on a posé : $0^0 = 1$

A44 Démontrer par récurrence la propriété précédente.

A45 Démontrer que : • $\forall n \in \mathbb{N} : 7 | 8^n - 1$ • $21^{135} \equiv 1\ [4]$

A46 Un élève affirme « pour tout entier naturel n : $5 | 2^{5n} - 12^n$ ».
Si cette affirmation est fausse en trouver un contre-exemple, sinon la démontrer.

P Soient $a, b, c, d \in \mathbb{Z}$ et $m \in \mathbb{N} \setminus \{0\}$ tels que :
$\boldsymbol{a \equiv b\ [m]}$ et $\boldsymbol{c \equiv d\ [m]}$.
Alors :
$\boldsymbol{a + c \equiv b + d\ [m]}$, $\boldsymbol{a - c \equiv b - d\ [m]}$ et $\boldsymbol{ac \equiv bd\ [m]}$.
On peut donc ajouter/soustraire/multiplier membre à membre des relations de congruence de même modulo, c'est une **implication**.

A47 Démontrer la propriété précédente.

A48 Démontrer que : $\forall n \in \mathbb{N}$, on a : $7 | 22^n + 15^n - 2$.

A49 Vérifier que $4 \equiv 1\ [3]$; a-t-on : $2^4 \equiv 2^1\ [3]$?

M ▶Dans un calcul avec congruence, on a le droit de remplacer tout nombre par un équivalent SAUF si c'est un exposant.

A50 Démontrer que : $\forall n \in \mathbb{N}$, on a : $5 | 2^{4n} + 6^n - 2$.

P Soient $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ et $m \in \mathbb{N}^*$.
- si $a \equiv \boldsymbol{b}\ [\boldsymbol{m}]$ et $\boldsymbol{0 \leqslant b < m}$,
  alors b est le reste de la division euclidienne de a par m
- si r est le reste de la division euclidienne de a par m,
  alors : $\boldsymbol{a \equiv r\ [m]}$ avec $\boldsymbol{0 \leqslant r < m}$ (rappel de définition)

A51 Démontrer le premier point de la propriété précédente.

A52 Soit $a \in \mathbb{Z}$ tel que $a \equiv 127\ [10]$, déterminer le reste de la division euclidienne de a par 10.

D Soient $a \in \mathbb{Z}$, $b \in \mathbb{N}$ et $m \in \mathbb{N}^*$.

Alors : b est le **reste modulo m de** $a \in \mathbb{Z} \overset{déf}{\Longleftrightarrow} b$ est le reste de la division euclidienne de a par m

A53 Déterminer le reste modulo 6 de 17^{213}.

i Rappel $m \in \mathbb{N}^*$, $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $n \in \mathbb{N}$, alors on a l'implication :
$a \equiv b\ [m] \Rightarrow a^n \equiv b^n\ [m]$
mais si $p \equiv q\ [m]$, alors il est possible que : $a^p \not\equiv a^q\ [m]$

A54 Déterminer le reste modulo 3 de 11^{157}. $(r = 2)$

A55 Déterminer le reste modulo 6 de 19^{123}. $(r = 1)$

A56 Déterminer le reste modulo 9 de 13^{208}. $(r = 4)$

A57 Déterminer le reste modulo 11 de 7^{152}. $(r = 5)$

D Soit $m \in \mathbb{N} \setminus \{0\}$. Alors :
$a \in \mathbb{Z}$ est **inversible modulo m**
$\overset{déf}{\Longleftrightarrow} \exists b \in \mathbb{Z}$ tel que : $a \times b \equiv 1\,[m]$ ou $b \times a \equiv 1\ [m]$.

A58 Donner un inverse de 7 modulo 5, en trouver un deuxième.

A59 Soit b un inverse de a modulo m, montrer que pour tout entier relatif k : $b + km$ est un inverse de a modulo m.

A60 Montrer que 4 n'a pas d'inverse modulo 6.

Un entier relatif a n'admet pas toujours d'inverse modulo m.
Lorsqu'il en admet, il n'est pas unique.

A61 Résoudre dans $\mathbb{Z}$: $5x \equiv 2\ [3]$.

Activités avec indication

A62 Déterminer le reste modulo 5 de 12^{307}. $(r = 3)$

A63 Déterminer le reste modulo 13 de 8^{5678}. $(r = 12)$

A64 Démontrer que, pour tout entier naturel n, on a :
$10n^2 + 31n + 15 \equiv 6n^2 + 13n - 5\ \ [2n + 5]$

A65 Quel est le chiffre des unités de 3^{151} ? (7)

A66 Déterminer le reste modulo 11 de 17^{5632}. $(r = 3)$

A67 Résoudre dans $\mathbb{Z}$ l'équation : $2x \equiv 3\ [5]$. $(x \equiv 4\ [5])$

A68 Résoudre dans $\mathbb{Z}$ l'équation : $4x - 5 \equiv 3\,[6]$.
$(x \equiv 2$ ou $5\,[6])$

A69 Déterminer les solutions dans $\mathbb{Z}$ de chacune des équations :
• $x^2 - 2 \equiv 4\ [5]$ • $x^4 \equiv 3\ [5]$ $(x \equiv 1$ ou $4\ [5]; \emptyset)$

A70 Démontrer que 6 n'admet pas d'inverse modulo 8.

A71 Démontrer que pour tout entier relatif a, on a : $5 | a(a^4 - 1)$.