Terminale SE / Arithmetique

3. PGCD, propriété et congruence :

Exercice 3386

On considère la suite (u_n) d'entiers naturels définie par :
$\begin{cases} u_0 = 14 \\ u_{n+1} = 5u_n - 6 \text{ pour tout entier naturel } n \end{cases}$

1. Calculer u_1, u_2, u_3 et u_4.
Quelle conjecture peut-on émettre concernant les deux derniers chiffres de u_n ?

2. Montrer que, pour tout entier naturel n :
$u_{n+2} \equiv u_n \pmod 4$.
En déduire que pour tout entier naturel k :
$u_{2k} \equiv 2 \pmod 4$ et $u_{2k+1} \equiv 0 \pmod 4$

3. a. Montrer par récurrence que, pour tout entier $n \in \mathbb{N}$:
$2 \cdot u_n = 5^{n+2} + 3$.

b. En déduire que, pour tout entier naturel n :
$2u_n \equiv 28 \pmod{100}$.

4. Déterminer les deux derniers chiffres de l'écriture décimale de u_n suivant les valeurs de n.

5. Montrer que le $PGCD$ de deux termes consécutifs de la suite (u_n) est constant.
Préciser sa valeur.

Correction 3386

1. Voici les cinq premiers termes de la suite (u_n) :
- $u_0 = 14$
- $u_1 = 5 \cdot u_0 - 6 = 5 \cdot 14 - 6 = 70 - 6 = 64$
- $u_2 = 5 \cdot u_1 - 6 = 5 \cdot 64 - 6 = 320 - 6 = 314$
- $u_3 = 5 \cdot u_2 - 6 = 5 \cdot 314 - 6 = 1\,570 - 6 = 1\,564$
- $u_4 = 5 \cdot u_3 - 6 = 5 \cdot 1\,564 - 6 = 7\,820 - 6 = 7\,814$

On peut conjecturer que les deux derniers chiffres des termes de la suite (u_n) vaut 14 ou 64.

2. On a l'égalité suivante :
$$\begin{aligned} u_{n+2} &= 5 \cdot u_{n+1} - 6 = 5 \cdot (5 \cdot u_n - 6) - 6 \\ &= 25 \cdot u_n - 30 - 6 = 25 \cdot u_n - 36 \\ &\equiv 1 \cdot u_n - 0 \pmod 4 \equiv u_n \pmod 4 \end{aligned}$$

Par transivité de la congruence *(ou par un raisonnement par récurrence)* :

- Pour tout entier n pair, on a :
$u_n \equiv u_0 \equiv 2 \pmod 4$
Pour k un entier naturel, $2 \cdot k$ est pair, on en déduit :
$u_{2 \cdot k} \equiv 2 \pmod 4$
- Pour tout entier n impair, on a :
$u_n \equiv u_1 \equiv 0 \pmod 4$
Pour k un entier naturel, $(2 \cdot k + 1)$ est pair, on en déduit :
$u_{2 \cdot k+1} \equiv 0 \pmod 4$

3. a. Considérons la propriété $\mathcal{P}_n$ définie pour tout entier n par la relation :
$\mathcal{P}$: "$2 \cdot u_n = 5^{n+2} + 3$"
A l'aide d'un raisonnement par récurrence, établissons que la propriété $\mathcal{P}_n$ est vraie pour tout entier naturel n :

- **Initialisation :**
On remarque que :
$2 \cdot u_0 = 2 \times 14 = 28$
$5^{0+2} + 3 = 5^2 + 3 = 28$
La propriété $\mathcal{P}_0$ est vérifiée.
- **Hérédité :**
Supposons la propriété $\mathcal{P}_n$ réalisée pour un entier naturel n quelconque. C'est à dire qu'on a l'hypothèse de récurrence :
$2 \cdot u_n = 5^{n+2} + 3$
Montrons que la relation est également vraie au rang suivant :
$$\begin{aligned} 2 \cdot u_{n+1} &= 2 \cdot (5 \cdot u_n - 6) = 10 \cdot u_n - 12 \\ &= 5 \cdot (2 \cdot u_n) - 12 = 5 \cdot (5^{n+2} + 3) - 12 \\ &= 5 \times 5^{n+2} + 15 - 12 = 5^{n+3} + 3 = 5^{(n+1)+2} + 3 \end{aligned}$$
On vient d'établir que la propriété $\mathcal{P}_{n+1}$ est vérifiée.
- **Conclusion :**
La propriété $\mathcal{P}_n$ est initialisée au rang 0 et elle vérifie la propriété d'hérédité. Par un raisonnement par récurrence, on vient d'établir que la propriété $\mathcal{P}_n$ est vraie pour tout entier naturel n.

b. On remarque l'égalité :
$$\begin{aligned} 2 \cdot u_n &= 5^{n+2} + 3 = 5^{n+2} - 5^2 + 5^2 + 3 \\ &= 5^2 \cdot (5^n - 1) + 28 \end{aligned}$$
Montrons, à l'aide d'un raisonnement par récurrence, que pour tout entier naturel n, on a :
$5^2 \cdot (5^n - 1) \equiv 0 \pmod{100}$

- **Initialisation :**
On a : $2 \cdot u_0 = 5^2 \cdot (5^0 - 1) = 25 \times (1 - 1) = 0$.
Ainsi, la propriété est réalisée au rang 0.
- **Hérédité :**
Supposons que la relation est vraie au rang n ; montrons qu'elle est vraie au rang $(n + 1)$:

$$
\begin{aligned}
2{\cdot}u_{n+1} &= 5^2{\cdot}\left(5^{n+1}-1\right)\\
&= 5^2{\cdot}\left(5^{n+1}-5^n+5^n-1\right)\\
&= 25{\cdot}\left[5^n{\cdot}(5-1)+5^n-1\right]\\
&= 25{\cdot}\left[5^n{\cdot}(5-1)\right]+25{\cdot}\left(5^n-1\right)\\
&= 25{\cdot}5^n{\cdot}4+25{\cdot}\left(5^n-1\right)\\
&= 100{\times}5^n{\cdot}4+25{\cdot}\left(5^n-1\right)\\
&\equiv 0{\times}5^n{\cdot}4+25{\cdot}\left(5^n-1\right)\pmod{100}\\
&\equiv 25{\cdot}\left(5^n-1\right)\pmod{100}
\end{aligned}
$$

La relation est vraie au rang n : $5^n-1\equiv 0 \pmod 4$

$$\equiv 25{\times}0 \pmod{100}$$

$$\equiv 0 \pmod{100}$$

La relation est vraie au rang $n+1$.

- **Conclusion :**
  La relation est initialisée au rang 0 et elle vérifie la propriété d'hérédité. On vient de montre, à l'aide d'un raisonnement par récurrence, la relation de congruence :
  $2{\cdot}u_n \equiv 0 \pmod{100}$

4. On vient de montrer la relation suivante pour tout entier naturel n :
$2{\cdot}u_n \equiv 28 \pmod{100}$
Ainsi, il existe un entier naturel k tel que :
$2{\cdot}u_n = 100\cdot k+28$
$u_n = 50\cdot k+14$
Par disjonction de cas :

- si k est pair : $u_n = 100{\cdot}k'+14$
  Ainsi, si k est pair les deux derniers chiffres de l'écriture décimale sont 14.
- si k est impair : $u_n = \left(50+100{\cdot}k'\right)+14 = 100{\cdot}k'+64$
  Ainsi, si k est impair, les deux derniers chiffres de l'écriture décimale sont 64

5. Notons $d = \text{pgcd}\left(u_{n+1}\,;u_n\right)$.

On a montré, à la question **2.**, que les termes de la suite $\left(u_n\right)$ sont congrus à 0 ou à 2 modulo 4 ; on en déduit que tous les termes de cette suite sont des nombres pairs : d est un multiple de 2.

Considérons deux termes consécutifs de la suite $\left(u_n\right)$; on utilisera la propriété suivante du $PGCD$ de deux entiers naturels a et b :
$\text{pgcd}\left(a\,;b\right) = \text{pgcd}\left(b\,;r\right)$
où r est le reste de la division euclidienne de a par b.

On a, pour tout entier naturel n :
$d = \text{pgcd}\left(5{\cdot}u_n-6\,;u_n\right)$

On a la division euclidienne $5u_n-6 = 4{\cdot}u_n+\left(u_n-6\right)$:

$= \text{pgcd}\left(u_n\,;u_n-6\right)$

Ainsi, d divise u_n et d divise u_n-6. On en déduit que d divise :
$u_n-\left(u_n-6\right) = 6$

Ainsi, d appartient à l'ensemble $\left\{1\,;2\,;3\,;6\right\}$. Or, d étant un multiple de 2, on en déduit :
$d=2 \quad ; \quad d=6$

Montrons par un raisonnement par l'absurde que $\text{pgcd}\left(u_{n+1}\,;u_n\right)$ n'est pas un multiple de 3 :
Supposons que u_n est un multiple de 3
$\Longrightarrow 2{\cdot}u_n$ est un multiple de 3
$\Longrightarrow 2{\cdot}u_n-3$ est un multiple de 3
$\Longrightarrow 5^{n+2}$ est un multiple de 3

Ce qui est absurde : les termes u_n ne sont pas divisible par 3.

On en déduit que le $PGCD$ de deux termes consécutifs de cette suite vaut 2 :
$d=2$.

4. Division euclidienne :

Exercice 3400

Déterminer la somme de tous les multiples de 11 compris entre 100 et 400. *(on pourra utiliser une suite arithmétique)*

Correction 3400

Observons les multiples suivants de 11 :

$99 = 9{\times}11$; $110 = 10{\times}11$; $396 = 36{\times}11$; $407 = 37{\times}11$

Ainsi, la somme S de tous les multiples de 11 compris entre 100 et 400 peuvent s'écrire :

$$
\begin{aligned}
S &= 110+121+\cdots+385+396\\
&= \mathbf{10}{\times}11+\mathbf{11}{\times}11+\cdots+\mathbf{35}{\times}11+\mathbf{36}{\times}11
\end{aligned}
$$

En notant $\left(u_n\right)$ la suite arithmétique de premier terme 0 et de raison 11, la somme S admet l'écriture suivante :

$$S = u_{10}+u_{11}+\cdots+u_{35}+u_{36}$$

En utilisant la somme des termes d'une suite arithmétique :

$$= \frac{\left(36-10+1\right)\left(10{\times}11+36{\times}11\right)}{2} = \frac{27{\times}46{\times}11}{2}$$

$$= 6\,831$$

Exercice 3406

α et β représentent deux entiers ; on considère les quatre phrases suivantes :

1. α est un multiple de β ;

2. α a pour multiple β ;

3. α est un diviseur β ;

4. α a pour diviseur β.

Les phrases ci-dessus sont équivalentes deux à deux ; retrouver les phrases équivalents.

Correction 3406

Les deux phrases suivantes sont équivaltentes :

- α est un multiple de β ;
- α a pour diviseur β.

Les deux phrases suivantes sont équivalentes :
- α a pour multiple β ;
- α est un diviseur de β.

Exercice 5019

1. Déterminer à l'aide de l'algorithme d'Euclide le $PGCD$ des nombres 410 et 246 :

Dividende	Diviseur	Reste	
410	246	...	$410 = \ldots \times 246 + \ldots$
...	...	...	$\ldots = \ldots \times \ldots + \ldots$
...	...	...	$\ldots = \ldots \times \ldots + \ldots$

2. a. Simplifier la fraction $\dfrac{246}{410}$.

   b. Effectuer les calculs suivants :
   $\dfrac{246}{410} - \dfrac{8}{5}$; $\dfrac{1}{246} - \dfrac{1}{410}$

Correction 5019

1. A l'aide de la division euclidienne, on a le tableau :

Dividende	Diviseur	Reste	
410	246	164	$410 = 1 \times 246 + 164$
246	164	82	$246 = 1 \times 164 + 82$
164	82	0	$164 = 2 \times 82 + 0$

Ainsi, à l'aide de l'algorithme d'Euclide, on a :
$\text{pgcd}\,(410\,;246) = 82$

2. a. 82 étant le $PGCD$ des deux nombres 410 et 246, on en déduit la simplification :
$$\frac{246}{410} = \frac{246\div 82}{410\div 82} = \frac{3}{5}$$

   b. Calculons :
   - $\dfrac{246}{410} - \dfrac{8}{5} = \dfrac{3}{5} - \dfrac{8}{5} = \dfrac{3-8}{5} = \dfrac{-5}{5} = -1$
   - $\dfrac{1}{246} - \dfrac{1}{410} = \dfrac{1}{3\times 82} - \dfrac{1}{5\times 82}$
   $= \dfrac{5}{5\times 3\times 82} - \dfrac{3}{3\times 5\times 82} = \dfrac{5-3}{5\times 3\times 82}$
   $= \dfrac{2}{5\times 3\times 82} = \dfrac{1}{5\times 3\times 41} = \dfrac{1}{615}$

5. Bezout et gauss :

Exercice 3695

Soit (E) l'ensemble des entiers naturels écrits, en base 10, sous la forme $\overline{abba}$ où a est un chiffre supérieur ou égal à 2 et b est un chiffre quelconque.
Exemples d'éléments de (E) :
2002 ; 3773 ; 9119.

Nombre d'éléments de (E) ayant 11 comme plus petit facteur premier

1. a. Décomposer 1001 en produit de facteurs premiers.

   b. Montrer que tout élément de (E) est divisible par 11.

2. a. Quel est le nombre d'éléments de (E) ?

   b. Quel est le nombre d'éléments de (E) qui ne sont ni divisibles par 2 ni par 5 ?

3. soit n un élément de (E) s'écrivant sous la forme $\overline{abba}$.

   a. Montrer que :
   "*n est divisible par 3 équivaut à $a+b$ est divisible par 3*"

   b. Montrer que :
   "*n est divisible par 7 équivaut à b est divisible par 7*"

4. Déduire des questions précédentes le nombre d'éléments de (E) qui admettent 11 comme plus petit facteur premier.

Correction 3695

1. a. On a la décomposition suivante :
$$1001 = 7\times 11\times 13$$

   b. Tout élément de (E) s'écrit, où a est un chiffre supérieur ou égal à 2 et b un chiffre quelconque :
$$\begin{aligned}\overline{abba} &= a\times 1001 + b\times 110\\ &= a\times 7\times 11\times 13 + b\times 11\times 10\\ &= 11\cdot(91a + 10b)\end{aligned}$$
   Ainsi, tout élément de (E) est divisible par 11.

2. a. Le chiffre b peut prendre dix valeurs différentes ; le chiffre a étant supérieur ou égal à 2, il peut prendre 8 valeurs.
   Ainsi, l'ensemble (E) contient 80 éléments.

   b. On a les critères de divisibilité suivants en base 10 :
   - Un nombre est divisible par 2 si son chiffre des unités est 0, 2, 4, 6 ou 8 ;
   - Un nombre est divisible par 5 si son chiffre des unités est 0 ou 5.

   Ainsi, les éléments de (E) qui ne sont ni divisibles par 2 ni par 5 doivent avoir leur chiffre des unités égal à :
   1 ; 3 ; 7 ; 9
   Dans ce cas, le chiffre des unités, c'est à dire a peut prendre quatre valeurs différentes et le chiffre n n'a aucun contrainte.
   L'ensemble (E) possède quarante éléments.

3. a. - $\Longrightarrow$: supposons n divisible par 3 :
   Ainsi, on a l'équivalence suivante :

$$\overline{abba} \equiv 0 \pmod 3$$
$$a\cdot 10^3 + b\cdot 10^2 + b\cdot 10 + a \equiv 0 \pmod 3$$
On a : $10 \equiv 1 \pmod 3$
$$a\cdot 1^3 + b\cdot 1^2 + b\cdot 1 + a \equiv 0 \pmod 3$$
$$a + b + b + a \equiv 0 \pmod 3$$
$$2\cdot(a+b) \equiv 0 \pmod 3$$
Ainsi, le produit $2\cdot(a+b)$ est divisible par 3 ; or, 2 et 3 sont deux nombres premiers entre eux : d'après le théorème de Gauss, $(a+b)$ est divisible par 3.

- $\Longleftarrow$: supposons que $a+b$ est divisible par 3 :

D'après la question précédente, on a montré l'équivalence suivante :
$$\overline{abba} \equiv 2\cdot(a+b) \pmod 3$$
Or, $(a+b)$ est divisible par 3 :
$$\equiv 2\cdot 0 \pmod 3$$
$$\equiv 0 \pmod 3$$
Ainsi, le nombre $\overline{abba}$ est divisible par 3.

b.

- $\Longrightarrow$: supposons que n est divisible par 7 :

On a les équivalences suivantes :
$10 \equiv 3 \pmod 7$; $10^2 \equiv 2 \pmod 7$; $10^3 \equiv 6 \pmod 7$
n est un élément de (E) ; il existe deux chiffres a et b tels que : $n = \overline{abba}$
D'après l'hypothèse de départ, on a :
$$n \equiv 0 \pmod 7$$
$$\overline{abba} \equiv 0 \pmod 7$$
$$a\times 10^3 + b\times 10^2 + b\times 10 + a \equiv 0 \pmod 7$$
$$a\times 6 + b\times 2 + b\times 3 + a \equiv 0 \pmod 7$$
$$7a + 5b \equiv 0 \pmod 7$$
$$0\cdot a + 5b \equiv 0 \pmod 7$$
$$5b \equiv 0 \pmod 7$$
Ainsi, le nombre $5b$ est divisible par 7 ; or, les nombres 5 et 7 sont premiers entre eux : d'après le théorème de Gauss, on en déduit que b est divisible par 7.

- $\Longleftarrow$: supposons que b est divisible par 7 :

A la question précédente, on vient de montrer l'équivalence suivante :
$n \equiv 5b \pmod 7$
avec l'hypothèse que b est divisible par 7 :
$n \equiv 5\cdot 0 \pmod 7$
$n \equiv 0 \pmod 7$
On a en déduit que n est divisible par 7.

4. Pour que $n = \overline{abba}$ ne soit ni divisible par 2 ni par 5, le chiffre a doit avoir une des valeurs suivantes :
1 ; 3 ; 7 ; 9

En utilisant la question 3. a., voici les couples $(a\,;b)$ définissant un nombre n non divisible par 3 :

$(1;1)$; $(1;3)$; $(1;4)$; $(1;6)$; $(1;7)$; $(1;9)$

$(3;1)$; $(3;2)$; $(3;4)$; $(3;5)$; $(3;7)$; $(3;8)$

$(7;1)$; $(7;3)$; $(7;4)$; $(7;6)$; $(7;7)$; $(7;9)$

$(9;1)$; $(9;2)$; $(9;4)$; $(9;5)$; $(9;7)$; $(9;8)$

Or, pour que n ne soit pas divisible par 7, il faut que b soit différent de 7. Voici l'ensemble des éléments de (E) qui ne soit ni divisible par 2, ni divisible par 3, ni divisible par 5, ni divisible par 7 ; voici donc l'ensemble des éléments (E) qui admettent 11 comme plus petit facteur premier :

1111 ; 1331 ; 1441 ; 1661 ; 1991

3113 ; 3223 ; 3443 ; 3553 ; 3883

7117 ; 7337 ; 7447 ; 7667 ; 7997

9119 ; 9229 ; 9449 ; 9559 ; 9889

6. Nombres premiers et congruence :

Exercice 3689

On se propose dans cet exercice d'étudier le problème suivant :

"*Les nombres dont l'écriture décimale n'utilise que le seul chiffre 1 peuvent-ils être premiers ?*"

Pour tout entier naturel $p \geqslant 2$, on pose $N_p = 1\ldots1$ où 1 apparaît p fois. On rappelle dès lors que :
$$N_p = 10^{p-1} + 10^{p-2} + \cdots + 10^0.$$

1. Les nombres N_2=11, N_3=111, N_4=1111 sont-ils premiers ?

2. Prouver que $N_p = \dfrac{10^p - 1}{9}$. Peut-on être certain que $10^p - 1$ est divisible par 9 ?

3. On se propose de démontrer que si p n'est pas premier, alors N_p n'est pas premier.
On rappelle que pour tout nombre réel x et tout entier naturel n non nul,
$$x^n - 1 = (x-1)\left(x^{n-1} + x^{n-2} + \cdots + x + 1\right)$$

a. On suppose que p est pair et on pose $p=2q$, où q est un entier naturel plus grand que 1.
Montrer que N_p est divisible par N_2=11.

b. On suppose que p est un multiple de 3 et on pose $p=3q$, où q est un entier naturel plus grand que 1.
Montrer que N_p est divisible par N_3=111.

c. On suppose p non premier et on pose $p=k\cdot q$ où k et q sont des entiers naturels plus grands que 1.
En déduire que N_p est divisible par N_k.

4. Enoncer une condition nécessaire pour que N_p soit premier.
Cette condition est-elle suffisante ?

Correction 3689

1.

- Le nombre N_2 est un nombre premier.
- La recherche des diviseurs de N_3 de :
2 à $\sqrt{111} \simeq 10{,}5$
n'a rien donné ; le nombre N_3 est premier.
- Le nombre N_4 admet la décomposition suivante :

$N_4 = 11\times101$

N_4 n'est pas premier.

2. Le nombre N_p admet l'écriture suivante :

$N_p = 10^{p-1} + 10^{p-2} + \cdots + 10^o$

$= 10^0 + 10^1 + \cdots + 10^{p-2} + \cdots + 10^{p-1}$

N_p est donc la somme des p premiers termes de la suite géométrique de premier terme 1 et de raison 10 ; on a :

$$N_p = 1\times\frac{1-\left(10^p\right)}{1-10} = \frac{1-10^p}{-9} = \frac{10^p-1}{9}$$

Comme N_p est une somme d'entier, on est sur que N_p est un nombre entier. Ainsi, le quotient $\frac{10^p-1}{9}$ est un entier : 9 est un diviseur du nombre 10^p-1.

3. a. Supposons que p est un nombre pair supérieur ou égal à 2 ; il existe $q\in\mathbb{N}^*$ tel que : $p = 2\cdot q$

Considérons la propriété $\mathcal{P}_q$ définie pour tout entier naturel q non-nul par la relation :

$\mathcal{P}_q$: "$N_{2\cdot q}$ est divisible par N_2"

- **Initialisation :**

  Pour q=1, on a :

  $N_{2\times1} = N_2$ qui est divisible par N_2.

  On vient de montrer que la propriété $\mathcal{P}_1$ est vraie.

- **Hérédité :**

  Supposons que la relation est vraie pour un entier q non-nul quelconque. C'est-à-dire qu'on a l'hypothèse de récurrence :

  N_{2q} est divisible par N_2

  Ainsi, on a l'existence d'un entier k vérifiant :

  $N_{2q} = k\cdot N_2$

  Montrons maintenant que cette relation est vérifiée au rang q+1 :

$N_{2\cdot(q+1)} = N_{2\cdot q+2} = 10^{2\cdot q+1} + 10^{2\cdot q} + 10^{2\cdot q-1} + \cdots + 1$

$= 10^{2\cdot q+1} + 10^{2\cdot q} + N_{2\cdot q} = 10^{2\cdot q}\cdot\left(10^1+1\right) + \left(k\cdot N_2\right)$

$= 10^{2\cdot q}\cdot N_2 + k\cdot N_2 = N_2\cdot\left(10^{2\cdot q}+k\right)$

On vient de montrer que la propriété $\mathcal{P}_{q+1}$ est vraie.

- **Conclusion :**

  La propriété $\mathcal{P}_q$ est intialisée au rang 1 et elle vérifie la propriété d'hérédité. A l'aide d'un raisonnement par récurrence, on vient de montrer que la propriété $\mathcal{P}_q$ est vraie pour tout entier q non-nul.

cette question peut aussi se faire avec la formule rappelée et le théorème de Gauss !

b. Considérons la propriété $\mathcal{P}_q$ définie pour tout $q\in\mathbb{N}^*$ par la relation :

$\mathcal{P}_q$: "$N_{3\cdot q}$ est divisible par N_3"

Montrons à l'aide d'un raisonnement par récurrence que la propriété $\mathcal{P}_q$ est vraie pour tout entier naturel q non-nul.

- **Initialisation :**

  On a : $N_{3\times1} = N_3$

  Ainsi, $\mathcal{P}_1$ est vraie.

- **Hérédité :**

  Supposons que la propriété $\mathcal{P}_q$ est vraie pour un entier naturel q non-nul quelconque. C'est-à-dire qu'on l'hypothèse de récurrence :

  "$N_{3\cdot q}$ est divisible par N_3"

  Ainsi, il existe un entier k vérifiant l'égalité :

  $N_{3\cdot q} = k\cdot N_3$

  Etablissons que cette relation est également vraie au rang $(q+1)$:

$N_{3\cdot(q+1)} = 10^{3\cdot q+2} + 10^{3\cdot q+1} + 10^{3\cdot q} + 10^{3\cdot q-1} + \cdots + 10^0$

$= 10^{3\cdot q+2} + 10^{3\cdot q+1} + 10^{3\cdot q} + N_{3\cdot q}$

$= 10^{3\cdot q}\cdot\left(10^2+10+1\right) + k\cdot N_3$

$= 10^{3\cdot q}\cdot N_3 + k\cdot N_3 = N_3\cdot\left(10^{3q}+k\right)$

On vient de montrer $\mathcal{P}_{q+1}$ est vrai.

- **Conclusion :**

  La propriété $\mathcal{P}_q$ est initialisée au rang 1 et elle vérifie la propriété d'hérédité. A l'aide du raisonnement par récurrence, on vient de montrer que $\mathcal{P}_q$ est vraie pour tout entier naturel q non-nul.

c. p un nombre non-premier ; alors il peut sécrire sous la forme d'un produit :

$p = k\cdot q$

où k et q sont distincts de 1.

$N_p = 10^{p-1} + 10^{p-2} + \cdots + 10^1 + 10^0$

$(10-1)\cdot N_p = (10-1)\cdot\left(10^{p-1} + 10^{p-2} + \cdots + 10^1 + 10^0\right)$

D'après la formule rappelée :

$9\cdot N_p = 10^p - 1$

$9\cdot N_p = 10^{k\cdot q} - 1$

$9\cdot N_p = \left(10^k\right)^q - 1$

D'après la formule rappelée :

$9\cdot N_p = \left(10^k-1\right)\cdot\left[\left(10^k\right)^{q-1}+\left(10^k\right)^{q-2}+\cdots+\left(10^k\right)^0\right]$

$9\cdot N_p = 9\cdot N_k\cdot\left[\left(10^k\right)^{q-1}+\left(10^k\right)^{q-2}+\cdots+\left(10^k\right)^0\right]$

$N_p = N_k\cdot\left[\left(10^k\right)^{q-1} + \left(10^k\right)^{q-2} + \cdots + \left(10^k\right)^0\right]$

On vient de montrer que N_p est un multiple de N_k : ainsi, N_k est divisible par N_p.

4. La question 3. c. vient de montrer que si p n'est pas premier alors le nombre N_p est également non-premier.

Donc pour que N_p soit un nombre premier, il est nécessaire que p soit un nombre premier.

Mais la réciproque est fausse : 5 est un nombre premier mais N_5 ne l'ai pas :

$N_5 = 11\,111 = 41\times271$

On dira alors que la condition n'est pas suffisante.

8. Divisibilité :

Exercice 3399

1. Compléter intuitivement les deux tableaux à double entrée suivants :

+	Pair	Impair
Pair		
Impair		

×	Pair	Impair
Pair		
Impair		

2. En remarquant les deux caractérisations suivantes :
- Si $n \in \mathbb{Z}$ est pair, il existe $k \in \mathbb{Z}$ tel que : $n = 2\cdot k$
- Si $n \in \mathbb{Z}$ est impair, il existe $k \in \mathbb{Z}$ tel que : $n = 2\cdot k + 1$

Répondre aux questions suivantes :

a. Démontrer que la somme de deux nombres impairs est pair.

b. Démontrer que le produit de deux nombres impairs est impair.

Correction 3399

1. On a :

+	Pair	Impair
Pair	pair	impair
Impair	impair	pair

×	Pair	Impair
Pair	pair	pair
Impair	pair	impair

2. a. Soit n et n' deux entiers pairs ; d'après la remarque précédente, il existe deux entiers k et k' tels que :
$n = 2\cdot k + 1 \quad ; \quad n' = 2\cdot k' + 1$
Etudions la somme de ces deux entiers :
$n + n' = \big(2\cdot k + 1\big) + \big(2\cdot k' + 1\big)$
$= 2\cdot n + 2\cdot n' + 2 = 2 \cdot \big(k + k' + 1\big)$
On en déduit que la somme de deux entiers impairs est un entier pair.

b. En reprenant le début de la question précédente, si n et n' sont deux entiers impairs, ils acceptent l'écriture suivante :
$n = 2\cdot k + 1 \quad ; \quad n' = 2\cdot k' + 1$
Ainsi, on a l'écriture suivante du produit :
$n \cdot n' = \big(2\cdot k + 1\big) \cdot \big(2\cdot k' + 1\big)$
$= 4\cdot k\cdot k' + 2\cdot k + 2\cdot k' + 1 = 2\cdot\big(2\cdot k\cdot k' + k + k'\big) + 1$
On vient de montrer que le produit de deux entiers impairs est un entier impair.

Exercice 3401

1. a. Pour k un entier naturel non-nul développer l'expression $A = \big(2\cdot k + 1\big)^2 - 1$.

b. Justifier que A est un multiple de 8.

2. On considère l'expression $B = n^2 - 1$ pour $n \in \mathbb{N}^*$:

a. Démontrer que pour n pair, B est impair.

b. Démontrer que pour n un entier impair strictement supérieur à 1, B est pair et divisible par 8.

Correction 3401

1. a. On a :
$A = \big(2\cdot k + 1\big)^2 - 1 = 4k^2 + 4k + 1 - 1$
$= 4k^2 + k = 4\cdot k\cdot\big(k + 1\big)$
Or, de deux entiers consécutifs, un des deux est un entier pair : le produit $k\cdot(k+1)$ est divisible par 2. Il existe donc un entier k' tel que :
$k\cdot\big(k + 1\big) = 2\cdot k'$
On en déduit la nouvelle écriture de A :
$A = 4\cdot k\cdot\big(k + 1\big) = 4\cdot\big(2\cdot k'\big) = 8\cdot k'$
On vient de montrer que le nombre A est un multiple de 8.

2. a. Soit n un entier pair ; il existe un entier k tel que :
$n = 2\cdot k$
On a alors :
$B = n^2 - 1 = \big(2k\big)^2 - 1 = \big(2k\big)^2 - 2 + 1$
$= 2\cdot\big(2\cdot k^2 - 1\big) + 1$
Ainsi, le nombre B est un nombre impair.

b. Pour n un entier impair, il existe k tel que :
$n = 2\cdot k + 1$
Le nombre B admet l'écriture suivante :
$B = n^2 - 1 = \big(2\cdot k + 1\big)^2 - 1 = A$
Or, on a montrer que A était divisible par 8 ; il en est donc de même pour le nombre B et comme B est divisible par 8, il est également pair.

Exercice 3424

Soit a et b deux entiers naturels.

1. Démontrer que :
$a^2\cdot b - a\cdot b^2 = 9 \implies a\cdot b$ divise 9 et $a - b$ divise 9.

2. En déduire les couples de solutions $\big(a\,;b\big)$ tels que $a^2\cdot b - a\cdot b^2 = 9$.

Correction 3424

1. On a la factorisation suivante :
$a^2\cdot b - a\cdot b^2 = 9$
$(ab)\cdot a - (ab)\cdot b = 9$
$a\cdot b\big(a - b\big) = 9$
En remarquant que le produit $a\cdot b$ est positif, on en déduit que le facteur $a-b$ est également positif.

On déduit de cette dernière égalité :
- Il existe $k \in \mathbb{N}$ tel que : $9 = k\cdot\big(a\cdot b\big)$
Ainsi, le produit $a\cdot b$ divise 9.
- Il existe $k \in \mathbb{N}$ tel que : $9 = k\cdot\big(a - b\big)$
Ainsi, $(a-b)$ divise 9.

2. Dans $\mathbb{N}$, l'ensemble des diviseurs de 9 est : $\big\{1\,;3\,;9\big\}$

Voici les différents couples $\big(a\,;b\big)$ tels que $a\cdot b$ soit un diviseur de 9 :

$a\cdot b$	
1	$\big(1\,;1\big)$
3	$\big(1\,;3\big)$; $\big(3\,;1\big)$
9	$\big(9\,;1\big)$; $\big(1\,;9\big)$; $\big(3\,;3\big)$; $\big(-3\,;-3\big)$

Il existe 24 couples de nombres vérifiant la propriété :
$a\cdot b$ diviseur de 9.
Or, on vérifie facilement qu'aucun de ces couples vérifient la relation :
$(a - b)$ est un diviseur de 9.

Ainsi, on en déduit qu'il n'existe aucun couple d'entier $\big(a\,;b\big)$ tel que :
$a^2\cdot b - a\cdot b^2 = 9$

Exercice 3426

Pour tout entier relatif n, on considère le nombre A_n défini par : $A_n = 2n^2 + 2n + 8$

Justifier que le nombre A_n est divisible par 4 pour tout entier relatif $n \in \mathbb{Z}$

Correction 3426

On a la factorisation suivante :

$$A_n = 2n^2 + 2n + 8 = 2\left(n^2 + n\right) + 8$$
$$= 2{\cdot}n{\cdot}\left(n+1\right) + 8$$

Or, de deux nombres consécutifs, un des deux est pairs ; on en déduit que le produit $n{\cdot}\left(n+1\right)$ est pair ; il existe $k \in \mathbb{Z}$ tel que :

$$n{\cdot}\left(n+1\right) = 2{\cdot}k$$

On en déduit l'écriture suivante du nombre A_n :

$$A_n = 2{\cdot}n{\cdot}\left(n+1\right) + 8 = 2{\cdot}\left(2k\right) + 8$$
$$= 4{\cdot}k + 8 = 4{\cdot}\left(k+2\right)$$

On vient de montrer que A_n est divisible par 4 pour tout $n \in \mathbb{Z}$.

Exercice 5061

Montrer que la somme des carrés de deux entiers consécutifs est un nombre impair

Correction 5061

Considérons deux entiers consécutifs. Il existe alors un entier naturel n tel que ces deux entiers s'écrivent :

$$n \quad ; \quad n+1$$

Ainsi, la somme des carrés de deux entiers consécutifs s'écrit sous la forme :

$$n^2 + (n+1)^2 = n^2 + n^2 + 2{\cdot}n + 1 = 2{\cdot}n^2 + {\cdot}n + 1$$
$$= 2{\cdot}\left(n^2 + n\right) + 1$$

On vient de montrer que cette somme est un nombre impair.

Exercice 3552

Soient p et q deux entiers naturels. Etudions la relation :

$$p^2 - 2{\cdot}q^2 = 1$$

1. Trouver deux entiers p et q vérifiant la relation précédente et tels que :
   $1 \leqslant p \leqslant 4 \quad ; \quad 1 \leqslant q \leqslant 4$
2. On suppose que les entiers p et q vérifient la relation recherchée :
   a. Démontrer que l'entier p est impair.
   b. En déduire que le nombre q est pair.

Correction 3552

1. Le couple $\left(3\,;2\right)$ est une solution de ce problème :
   $p^2 - 2{\cdot}q^2 = 3^2 - 2 \cdot 2^2 = 9 - 8 = 1$
2. a. On a la relation :
   $p^2 - 2{\cdot}q^2 = 1$
   $p^2 = 2{\cdot}q^2 + 1$
   Ainsi, le nombre p^2 est un nombre impair.
   Or, le carrée d'un nombre est impair si, et seulement, ce nombre est impair : on en déduit que l'entier p est impair.
   b. p étant un entier impair, il existe un entier k tel que :
   $p = 2{\cdot}k + 1$
   On peut donc écrire :
   $$p^2 - 2{\cdot}q^2 = 1$$
   $$\left(2{\cdot}k+1\right)^2 - 2{\cdot}q^2 = 1$$
   $$4{\cdot}k^2 + 4{\cdot}k + 1 - 2{\cdot}q^2 = 1$$
   $$4{\cdot}k^2 + 4{\cdot}k + 1 - 1 = 2{\cdot}q^2$$
   $$2{\cdot}q^2 = 4{\cdot}k^2 + 4{\cdot}k$$
   $$q^2 = 2{\cdot}k^2 + 2{\cdot}k$$
   $$q^2 = 2{\cdot}\left(k^2 + k\right)$$
   On en déduit que l'entier q^2 est pair.
   Or, le carré d'un nombre est pair, si et seulement si, ce nombre est pair : on en déduit que l'entier q est pair.

11. ax+by=c :

Exercice 3326

On rappelle que 2 003 est un nombre premier.

1. a. Déterminer deux entiers relatifs u et v tels que :
   $123u + 2003v = 1$
   b. En déduire un entier relatif k_0 tel que :
   $123k_0 \equiv 1 \pmod{2003}$
   c. Montrer que, pour tout entier relatif x,
   $123x \equiv 456 \pmod{2003}$ si, et seulement si, $x \equiv 456k_0 \pmod{2003}$
   d. Montrer qu'il existe un unique entier n tel que :
   $1 \leqslant n \leqslant 2002$ et $123n \equiv 456 \pmod{2003}$
2. Soit a un entier tel que : $1 \leqslant a \leqslant 2002$
   a. Déterminer : $PGCD(a\,;2003)$
   En déduire qu'il existe un entier m tel que :
   $am \equiv 1 \pmod{2003}$
   b. Montrer que, pour tout entier b, il existe un unique entier x tel que :
   $0 \leqslant x \leqslant 2002$ et $ax \equiv b \pmod{2003}$

Correction 3326

1. a. Déterminons le $PGCD$ de 123 et 2 003 à l'aide de l'algorithme d'Euclide ; on a les divisions euclidiennes suivantes :
   i. $2003 = 16{\times}123 + 35$
   ii. $123 = 3{\times}35 + 18$

iii. $35 = 1\times18 + 17$

iv. $18 = 1\times17 + 1$

v. $17 = 17\times1 + 0$

En notant $a = 2\,003$ et $b = 123$:

i. $2003 = 16\times123 + 35$

$a = 16\cdot b + 35$

$a - 16\cdot b = 35$

$35 = a - 16\cdot b$

ii. $123 = 3\times35 + 18$

$b = 3\times\big(a - 16\cdot b\big) + 18$

$b = 3\cdot a - 48\cdot b + 18$

$-3\cdot a + 49\cdot b = 18$

$18 = -3\cdot a + 49\cdot b$

iii. $35 = 1\times18 + 17$

$\big(a - 16\cdot b\big) = 1\times\big(-3\cdot a + 49\cdot b\big) + 17$

$a - 16\cdot b = -3\cdot a + 49\cdot b + 17$

$4\cdot a - 65\cdot b = 17$

$17 = 4\cdot a - 65\cdot b$

iv. $18 = 1\times17 + 1$

$-3\cdot a + 49\cdot b = 1\times\big(4\cdot a - 65\cdot b\big) + 1$

$-3\cdot a + 49\cdot b = 4\cdot a - 65\cdot b + 1$

$-7\cdot a + 114\cdot b = 1$

$1 = -7\cdot a + 114\cdot b$

Ainsi, le couple $\big(114\,;\,-7\big)$ est une solution de l'équation :

$123\cdot u + 2\,003\cdot v = 1$

b. De la question précédente, on en déduit l'égalité :

$123\times114 + 2003\times(-7) = 1$

La congruence permet d'écrire :

$123\times114 + 2003\times(-7) \equiv 1 \pmod{2003}$

$123\times114 + 0\times(-7) \equiv 1 \pmod{2003}$

$123\times114 \equiv 1 \pmod{2003}$

Ainsi, $k_0 = 114$.

c. • $\Longleftarrow$: supposons que $x \equiv 456\cdot k_0 \pmod{2\,003}$

On a :

$x \equiv 456\cdot k_0 \pmod{2\,003}$

$123\cdot x \equiv 123\cdot456\cdot k_0 \pmod{2\,003}$

$123\cdot x \equiv 456\cdot\big(123\cdot k_0\big) \pmod{2\,003}$

$123\cdot x \equiv 456\cdot1 \pmod{2\,003}$

$123\cdot x \equiv 456 \pmod{2\,003}$

• $\Longrightarrow$: supposons que $123\cdot x \equiv 456 \pmod{2\,003}$

On a :

$123\cdot x \equiv 456 \pmod{2003}$

$k_0\cdot123\cdot x \equiv k_0\cdot456 \pmod{2003}$

$\big(123\cdot k_0\big)\cdot x \equiv k_0\cdot456 \pmod{2003}$

D'après la question précédente :

$x \equiv k_0\cdot456 \pmod{2003}$

d. Supposons l'existence de deux entiers n et n' vérifiant les conditions suivantes :

$1 \leqslant n \leqslant 2002$; $123\cdot n \equiv 456 \pmod{2\,003}$

$1 \leqslant n' \leqslant 2002$; $123\cdot n' \equiv 456 \pmod{2\,003}$

En effectuant membre à membre les inégalités et les équivalences, on obtient :

$-2001 \leqslant n - n' \leqslant 2001$; $123\cdot\big(n - n'\big) \equiv 0 \pmod{2003}$

De la dernière équivalence, on en déduit que le produit $123\cdot\big(n - n'\big)$ est un multiple de 2 003.

Le nombre 2 003 est premier ; ainsi, 2 003 et 123 sont deux nombres premiers entre eux. D'après le théorème de Gauss, on en déduit que 2 003 divise $(n - n')$.

Or, $(n - n') \in \big[-2001\,;\,2001\big]$ et $(n - n')$ est un multiple de 2 003 ; on en déduit :

$n - n' = 0$

$n = n'$

2. a. 2 003 est un nombre premier ; ainsi, a et 2 003 sont premiers entre eux. On en déduit :

$PGCD(a\,;\,2\,003) = 1$

D'après le théorème de Bezout, il existe un couple d'entiers $(u\,;v)$ tels que :

$u\cdot a + v\cdot2\,003 = 1$

La congruence permet d'écrire :

$u\cdot a + v\cdot2\,003 \equiv 1 \pmod{2003}$

$u\cdot a + v\cdot0 \equiv 1 \pmod{2003}$

$u\cdot a \equiv 1 \pmod{2003}$

On vient de montrer l'existence d'un entier m tel que :

$a\cdot m \equiv 1 \pmod{2\,003}$

b. D'après la question précédente, on a :

$a\cdot m \equiv 1 \pmod{2003}$

Soit b un entier quelconque :

$a\cdot m\cdot b \equiv 1\cdot b \pmod{2003}$

En notant $y = b\cdot m$:

$a\cdot y \equiv b \pmod{2003}$

L'entier x recherché est le reste de la division euclidienne de y par 2 003.

Exercice 3541

Les parties **A** et **B** sont indépendantes.

Partie A

On considère l'équation (E) : $7x-6y=1$ où x et y sont des entiers naturels.

1. Donner une solution particulière de l'équation (E).

2. Déterminer l'ensemble des couples d'entiers naturels solutions de l'équation (E).

Partie B

Dans cette partie, on se propose de déterminer les couples $(n\,;m)$ d'entiers naturels non nul vérifiant la relation :

$7^n - 3\times2^m = 1$ (F)

1. On suppose $m \leqslant 4$.
Montrer qu'il y a exactement deux couples solutions.

2. On suppose maintenant que $m \geqslant 5$.

a. Montrer que si le couple $(n\,;m)$ vérifie la relation (F) alors :

$7^n \equiv 1 \pmod{32}$

b. En étudiant les restes de la division par 32 des puissances de 7, montrer que si le couple $(n\,;m)$ vérifie la

relation (F) alors n est divisible par 4.

c. En déduire que si le couple $(n\,;m)$ vérifie la relation (F) alors : $7^n \equiv 1 \pmod 5$.

d. Pour $m \geqslant 5$, existe-t-il des couples $(n\,;m)$ d'entiers naturels vérifiant la relation (F) ?

3. Conclure, c'est-à-dire déterminer l'ensemble des couples d'entiers naturels non nuls vérifiant la relation (F).

Correction 3541

Partie A :

1. Le couple $(1\,;1)$ est une solution de l'équation :
$7{\cdot}x - 6{\cdot}y = 7\times1 - 6\times1 = 1$

2. Soit $(x\,;y)$ une couple solution de l'équation (E) ; on a légalité :
$$\begin{aligned} 7{\cdot}x - 6{\cdot}y &= 1\\ 7{\cdot}x - 6{\cdot}y &= 7\times1 - 6\times1\\ 7{\cdot}x - 7\times1 &= 6{\cdot}y - 6\times1\\ 7{\cdot}(x-1) &= 6{\cdot}(y-1)\end{aligned}$$
On en déduit les deux remarques suivantes :
- L'entier 7 divise le produit $6{\cdot}(y-1)$. Or, les entiers 6 et 7 sont premiers entre eux ; d'après le théorème de Gauss, on en déduit que 7 divise $y-1$. Ainsi, il existe un entier relatif k' vérifiant :
$$\begin{aligned} y-1 &= 7{\cdot}k'\\ y &= 7{\cdot}k'+1\end{aligned}$$
- L'entier 6 divise le produit $7{\cdot}(x-1)$. Or, les entiers 6 et 7 sont premiers entre eux ; d'après le théorème de Gauss, on en déduit que 6 divise $x-1$. Ainsi, il existe un entier relatif k vérifiant :
$$\begin{aligned} x-1 &= 6{\cdot}k\\ x &= 6{\cdot}k+1\end{aligned}$$

Ainsi, les couples solutions de l'équation (E) admettent l'écriture :
$\big(6{\cdot}k{+}1\,;7{\cdot}k'{+}1\big)$

Vérifions sous quelles conditions un couple précédent est solution de l'équation (E) :
$$\begin{aligned} 7{\cdot}x - 6{\cdot}y &= 1\\ 7{\cdot}(6{\cdot}k+1) - 6{\cdot}(7{\cdot}k'+1) &= 1\\ 42{\cdot}k + 7 - 42{\cdot}k' - 6 &= 1\\ 42{\cdot}k - 42{\cdot}k' + 1 &= 1\\ 42{\cdot}(k-k') &= 0\\ k-k' &= 0\\ k &= k'\end{aligned}$$
Ainsi, les couples solutions de l'équation (E) admettent l'écriture :
$\big(6{\cdot}k{+}1\,;7{\cdot}k{+}1\big)$

Partie B

1. Considérons m un entier non nul inférieur ou égal à 4 :
- Pour $m=1$:
$$\begin{aligned} 7^n - 3\times2^m &= 1\\ 7^n - 3\times2^1 &= 1\\ 7^n - 6 &= 1\\ 7^n &= 7\end{aligned}$$
On en déduit que le couple $(1\,;1)$ est solution de l'équatino (F).
- Pour $m=2$:
On cherche n afin de vérifier l'égalité suivante :
$$\begin{aligned} 7^n - 3\times2^m &= 1\\ 7^n - 3\times2^2 &= 1\\ 7^n - 3\times4 &= 1\\ 7^n - 12 &= 1\\ 7^n &= 13\end{aligned}$$
Il n'existe pas de couple $\big(n\,;2\big)$ vérifiant l'égalité (F).
- Pour $m=3$:
On cherche n afin de vérifier l'égalité suivante :
$$\begin{aligned} 7^n - 3\times2^m &= 1\\ 7^n - 3\times2^6 &= 1\\ 7^n - 3\times8 &= 1\\ 7^n - 24 &= 1\\ 7^n &= 25\end{aligned}$$
Il n'existe pas de couple $\big(n\,;3\big)$ vérifiant l'égalité (F).
- Pour $m=4$:
$$\begin{aligned} 7^n - 3\times2^m &= 1\\ 7^n - 3\times2^4 &= 1\\ 7^n - 3\times16 &= 1\\ 7^n - 48 &= 1\\ 7^n &= 49\end{aligned}$$
On en déduit que le couple $\big(2\,;4\big)$

Il y a exactement 2 solutions de l'équation (F).

2. On suppose que $m \geqslant 5$:

a. Puisque m est supérieur ou égal à 5, on a :
$m = 5 + (m-5)$ où $m \geqslant 5$.
On en déduit l'égalité :
$$\begin{aligned} 7^n - 3\times2^m &= 1\\ 7^n - 3\times2^5\times2^{5-m} &= 1\\ 7^n - 3\times32\times2^{5-m} &= 1\end{aligned}$$
On en déduit l'équivalence :
$$\begin{aligned} 7^n - 3\times0\times2^{5-m} &\equiv 1 \pmod{32}\\ 7^n &\equiv 1 \pmod{32}\end{aligned}$$

b. On remarque que :
$7^4 = 2401 = 75\times32 + 1 \equiv 32 \pmod{32}$
Le reste de la division euclidienne de n par 4 donne l'existence d'un couple $(q\,;r)$ vérifiant :
$n = q\times4 + r$ où $0 \leqslant r < 4$
On a les trois posibilités suivantes :
- $r=0$:
$$\begin{aligned} 7^{q\times4+r} &= 7^{q\times4+0} = \big(7^4\big)^q\\ &\equiv 1^q \equiv 1 \pmod{32}\end{aligned}$$
- $r=1$:
$$\begin{aligned} 7^{q\times4+r} &= 7^{q\times4+1} = \big(7^4\big)^q\times7^1\\ &\equiv 1^q\times7 \equiv 7 \pmod{32}\end{aligned}$$
- $r=2$:
$$\begin{aligned} 7^{q\times4+r} &= 7^{q\times4+2} = \big(7^4\big)^q\times7^2\\ &\equiv 1^q\times7^2 \equiv 49 \equiv 17 \pmod{32}\end{aligned}$$
- $r=2$:
$$\begin{aligned} 7^{q\times4+r} &= 7^{q\times4+3} = \big(7^4\big)^q\times7^3\\ &\equiv 1^q\times343 \equiv 23 \pmod{32}\end{aligned}$$
Ainsi, si $(n\,;m)$ est un couple solution de l'équation (F) ; alors, il doit vérifier, d'après la question a., l'équivalence suivante :
$7^n \equiv 1 \pmod{32}$
Alors, nécessairement pour vérifier l'équivalence précédente, on doit avoir :

$n \equiv 0 \pmod 4$

c. La question précédente montre que l'entier n est un multiple de 4 ; il existe un entier naturel k tel que :
$n = 4 \cdot k$
On a l'égalité :
$7^n = 7^{4\cdot k} = \left(7^4\right)^k = 2401^k$
$\equiv 1^k \pmod 5 \equiv 1 \pmod 5$

d. Soit $(n\,;m)$ un couple de solution de l'équation (E) ; on a l'égalite et les équivalences suivantes :

$7^n - 3\times 2^m = 1$
$7^n - 3\times 2^m \equiv 1 \pmod 5$
$1 - 3\times 2^m \equiv 1 \pmod 5$
$-3\times 2^m \equiv 0 \pmod 5$
$3\times 2^m \equiv 0 \pmod 5$

Cela signifie que 5 divise le produit 3×2^m ; or, les nombres 3 et 5 sont premiers entre eux, d'après le théorème de Gauss, on en déduit que 5 divise le facteur 2^m ce qui est une absurdité.
Il n'existe pas de couple vérifiant l'égalite (F) pour $m \geqslant 5$.

3. On en déduit qu'il n'existe que deux couples solutions de cette équation :
$\mathcal{S} = \left\{ (1\,;1)\ ;\ (2\,;4) \right\}$

Exercice 5447

Partie A - Restitution organisée des connaissances

On rappelle ci-dessous le théorème de Bézout et le théorème de Gauss.

Théorème de Bézout :
Deux entiers relatifs a et b sont premiers entre eux si, et seuleemnt si, il existe un couple $(u\,;v)$ d'entiers relatifs vérifiant $a\cdot u + b\cdot v = 1$.

Théorème de Gauss :
Soient a, b, c des entiers relatifs.
Si a divise le produit $b\cdot c$ et si a et b sont premiers entre eux, alors a divise c

1. En utilisant le théorème de Bézout, démontrer le théorème de Gauss.

2. Soient p et q deux entiers naturels tels que p et q sont premiers entre eux.
Déduire du théorème de Gauss que, si a est un entier relatif, tel que $a \equiv 0 \pmod p$ et $a \equiv 0 \pmod q$, alors $a \equiv 0 \pmod{pq}$

Partie B

On se propose de déterminer l'ensemble $\mathcal{S}$ des entiers relatifs n vérifiant le système :
$\begin{cases} n \equiv 9 \pmod{17} \\ n \equiv 3 \pmod 5 \end{cases}$

1. Recherche d'un élément de $\mathcal{S}$.
On désigne par $(u\,;v)$ un couple d'entiers relatifs tels que : $17\cdot u + 5\cdot v = 1$

a. Justifier l'existence d'un tel couple $(u\,;v)$.

b. On pose : $n_0 = 3\times 17u + 9\times 5v$.
Démontrer que n_0 appartient à $\mathcal{S}$.

c. Donner un exemple d'entier n_0 appartenant à $\mathcal{S}$.

2. Caractérisation des éléments de $\mathcal{S}$.

a. Soit n un entier relatif appartenant à $\mathcal{S}$.
Démontrer que : $n - n_0 \equiv 0 \pmod{85}$.

b. En déduire qu'un entier relatif n appartient à $\mathcal{S}$ si, et seulement, si il peut s'écrire sous la forme $n = 43 + 85k$ où k est un entier relatif.

3. Application.
Zoé sait qu'elle a entre 300 et 400 jetons.
Si elle fait des tas de 17 jetons, il lui en reste 9.
Si elle fait des tas de 5 jetons, il lui en reste 3.
Combien a-t-elle de jetons ?

Correction 5447

Partie A

1. Soit a, b et c trois entiers relatifs non-nuls.
Supposons que a divise $b\cdot c$ et que a et b sont premiers entre eux.

a divise $b\cdot c$. On en déduit l'existence d'un entier relatif k tels que :
$b\cdot c = k\cdot a$

a et b étant premiers entre eux : $\text{pgcd}\left(a\,;b\right) = 1$.
D'après l'identité de Bézout, on en déduit l'existence d'un couple d'entiers $(u\,;v)$ vérifiant :
$a\cdot u + b\cdot v = 1$

On a les égalités suivantes :
$a\cdot u + b\cdot v = 1$
$a\cdot u + b\cdot v = 1$
$c\cdot\left(a\cdot u + b\cdot v\right) = c$
$a\cdot\left(u\cdot c\right) + \left(b\cdot c\right)\cdot v = c$

D'après la première remarque :
$a\cdot\left(u\cdot c\right) + \left(k\cdot v\right)\cdot v = c$
$a\cdot\left(u\cdot c + v\right) = c$

L'égalité précédente montre que l'entier a divise c.

2. Soit a un entier relatif tel que :
$a \equiv 0 \pmod p$; $a \equiv 0 \pmod q$

Puisque $a \equiv 0 \pmod p$, il existe un entier relatif k tel que :
$a = k\cdot p$

Du fait que $a \equiv 0 \pmod q$, on en déduit que l'entier q divise le produit $k\cdot p$. Or, d'après les hypothèses, p et q sont deux entiers premiers entre eux.
D'après le théorème de Gauss, on en déduit que l'entier q divise k. Ainsi, on a l'existence d'un entier relatif k' vérifiant l'égalité :
$k = k'\cdot q$.

L'entier a admet donc pour écriture :
$a = k'\cdot p\cdot q$.
On en déduit que le produit $p\cdot q$ est un diviseur de a :
$a \equiv 0 \pmod{p\cdot q}$

Partie B

1. a. Deux justifications sont possibles pour cette question :

- La simple présentation du couple $(-2\,;7)$ vérifiant l'égalité permet de justifier l'affirmation :
$17{\cdot}u+5{\cdot}v=17\times(-2)+5\times7=-34+35=1$
- Le théorème de Bezout justifie l'existence d'au moins un couple vérifiant cette égalité.
Les nombres 17 et 5 étant deux nombres premiers, ils sont nécessairement premiers entre eux. Le théorème de Bezout assure l'existence d'un couple $(u\,;v)$ vérifiant l'égalité :
$17{\cdot}u+5{\cdot}v=1$

b. Testons le nombre n_0 dans les deux classes de congruences :

- $n_0=3\times17u+9\times5v=3\times17u+9\times(1-17u)$
$=3\times17u+9-9\times17u$
$\equiv 3\times0\times u+9-9\times0\times u \pmod{17}$
$\equiv 0+9-0 \pmod{17}$
$\equiv 9 \pmod{17}$
- $n_0=3\times17u+9\times5v=3\times(1-5v)+9\times5v$
$=3-3\times5v+9\times5v$
$\equiv 3-3\times0\times v+9\times0\times v \pmod{5}$
$\equiv 3-0+0 \pmod{5}$
$\equiv 3 \pmod{5}$

On en déduit que l'entier n_0 appartient à $\mathcal{S}$.

c. En utilisant le couple obtenu à la question a., on a :
$n_0=3\times17u+9\times5v=3\times17\times(-2)+9\times5\times7=213$

2. a. Soit n un entier relatif appartenant à l'ensemble $\mathcal{S}$. Cet entier vérifie les deux relations de congruence suivantes :
$n\equiv 9 \pmod{17}$; $n\equiv 3 \pmod{5}$
Ainsi, on a :
$n-n_0\equiv 9-9\equiv 0 \pmod{17}$; $n-n_0\equiv 3-3\equiv 0 \pmod{5}$
Les nombres 7 et 17 sont des nombres premiers, à fortiori, ce sont des nombres premiers entre eux.
D'après la propriété 2. établie à la partie **A**, on a :
$n-n_0\equiv 0 \pmod{85}$

b. - De la congruence précédente, on en déduit l'existence d'un entier k tel que :
$n-n_0=85{\cdot}k$
$n=n_0+85{\cdot}k$
$n=213+85{\cdot}k$
$n=45+2\times85+85{\cdot}k$
$n=45+85{\cdot}(k+2)$
On vient de montrer que tout entier appartenant à l'ensemble $\mathcal{S}$ admettait une écriture de la forme :
$n=43+85{\cdot}k$ où k est un entier relatif.

- Réciproquement, prenons un entier n tel que :
$n=43+85{\cdot}k$
et montrons que cet entier appartient à l'ensemble $\mathcal{S}$. On a les congruences :
$\Rightarrow\ n=43+85{\cdot}k=3+8\times5+5\times17{\cdot}k$
$\equiv 3+8\times0+0\times17{\cdot}k \pmod{5}$
$\equiv 3+0+0 \pmod{5}$
$\equiv 3 \pmod{5}$
$\Rightarrow\ n=43+85{\cdot}k=9+2\times17+5\times17{\cdot}k$
$\equiv 9+2\times0+5\times0\times k \pmod{17}$
$\equiv 9+0+0 \pmod{17}$
$\equiv 9 \pmod{17}$
On en déduit que l'entier n est un élément de $\mathcal{S}$.

3. Soit n le nombre de jetons obtenu par Zoé. Traduisons les conditions de l'énoncé :

- Si elle fait des tas de 17 jetons, il lui en reste 9 :
$n\equiv 9 \pmod{17}$
- Si elle fait des tas de 5 jetons, il lui en reste 3 :
$n\equiv 3 \pmod{5}$

Ces deux conditions étant vérifiées par l'entier n, on en déduit que l'entier n est un élément de $\mathcal{S}$.

Ainsi, il existe k tel que $n=43+85{\cdot}k$.

La condition que le nombre de jetons possédait par Zoé se situe entre 300 et 400 se traduit par l'encadrement :
$300\leqslant 43+85{\cdot}k\leqslant 400$
$300-43\leqslant 85{\cdot}k\leqslant 400-43$
$257\leqslant 85{\cdot}k\leqslant 357$
$\dfrac{257}{85}\leqslant k\leqslant\dfrac{357}{85}$
$3{,}02\leqslant k\leqslant 4{,}2$
k étant un entier relatif, de l'encadrement précédent, on en déduit que $k=4$.

Ainsi, Zoé possède exactement :
$n=43+85\times4=43+340=383$

---

12. PGCD et nombres premiers entre eux :

Exercice 5359

Dans le système d'équation ci-dessous, les nombres x et y ci-dessous représentent des entiers naturels où $x<y$:

$$\begin{cases} x{\cdot}y &= 135\\ \text{pgcd}\,(x\,;y) &= 3\end{cases}$$

Résoudre ce système d'équations.

Correction 5359

Puisque pgcd$(x\,;y)$=3, il existe deux entiers naturels k et k' premiers entre eux tels que :
$x=3{\cdot}k$; $y=3{\cdot}k'$

Le produit des deux nombres x et de y vérifie l'égalité :
$x{\cdot}y=135$
$(3{\cdot}k){\cdot}(3{\cdot}k')=135$
$9{\cdot}k{\cdot}k'=135$
$k{\cdot}k'=15$
Sachant que le nombre 15 admet la décomposition en pro-

duits de facteurs premiers :

$15 = 3\times5$

On en déduit l'existence de quatre couples $(k\,;k')$ vérifiant l'égalité $k\cdot k' = 15$:

$(1\,;15)$; $(3\,;5)$; $(5\,;3)$; $(15\,;1)$

Pour chaque couple $(k\,;k')$, on associe une solution du système :

$(3\,;45)$; $(9\,;15)$; $(15\,;9)$; $(45\,;3)$

Exercice 6023

Soit a et b deux entiers naturels avec $a>b$. Montrer l'équivalence :

$\frac{a}{b}$ est irréductible $\iff$ $\frac{a-b}{a\cdot b}$ est irréductible.

Correction 6023

Etablissons les deux équivalences :

- Supposons $\frac{a}{b}$ est irréductible : c'est à dire pgcd $(a\,;b)=1$.

  Notons d le PGCD des deux nombres $a-b$ et $a\cdot b$.

  Ainsi, d divise les deux nombres $a-b$ et $a\cdot b$.

  Il divise donc :

  $a\cdot(a-b)+a\cdot b = a^2 - a\cdot b + a\cdot b = a^2$

  d divise les deux nombres $a\cdot b$ et a^2. Or, on a :

  $\text{pgcd}\left(a\cdot b\,;a^2\right) = a\cdot\text{pgcd}\left(a\,;b\right) = a\times1 = a$

  Il divise donc :

  $a\cdot b - b\cdot(a-b) = a\cdot b - a\cdot b + b^2 = b^2$

  d divise les deux nombres $a\cdot b$ et b^2. Or, on a :

  $\text{pgcd}\left(a\cdot b\,;b^2\right) = b\cdot\text{pgcd}\left(a\,;b\right) = b\times1 = b$

  Ainsi, d divise a et b. Or, ces deux nombres étant premiers, on en déduit que d=1.

  La fraction $\frac{a-b}{a\cdot b}$ est irréductible.

- Supposons $\frac{a-b}{a\cdot b}$ est irréductible :

  C'est-à-dire : pgcd $(a-b\,;a\cdot b)=1$

  Notons d le $PGCD$ de a et de b.

  d divise également $a-b$ et $a\cdot b$: ainsi, d divise le PGCD de $a-b$ et de $a\cdot b$. Puisque pgcd $(a-b\,;a\cdot b)=1$, on en déduit que d=1.

  Les entiers a et b sont premiers entre eux.

13. Nombres premiers :

Exercice 3427

1. Déterminer la décomposition en produit de facteurs premiers des nombres suivants :

   a. 2 016 b. 2 100 c. 864

2. Effectuer les opérations suivantes et donner le résultat sous forme simplifiée :

   a. $\frac{2\,016}{2\,100}$ b. $\frac{1}{2\,100}+\frac{1}{864}$

Correction 3427

1. Voici les tableaux utilisés pour l'algorithme de décomposition d'un entier en produit de facteurs premiers :

2016	2
1008	2
504	2
252	2
126	2
63	3
21	7
3	3
1	

2100	2
1050	2
525	5
105	5
21	3
7	7
1	

864	2
432	2
216	2
108	2
54	2
27	3
9	3
3	3
1	

Ainsi, on a les décompositions suivantes :

$2016 = 2^5\times3^2\times7$; $2100 = 2^2\times5^2\times3\times7$

$864 = 2^5\times3^3$

2. a. $\frac{2016}{2100} = \frac{2^5\times3^2\times7}{2^2\times3\times5^2\times7} = 2^3\times3\times5^{-2}$

   b. $\frac{1}{2100}+\frac{1}{864} = \frac{1}{2^2\times5^2\times3\times7}+\frac{1}{2^5\times3^3}$

   $= \frac{2^3\times3^2}{2^5\times3^3\times5^2\times7}+\frac{5^2\times7}{2^5\times3^3\times5^2\times7}$

   $= \frac{2^3\times3^2+5^2\times7}{2^5\times3^3\times5^2\times7} = \frac{13\times19}{2^5\times3^3\times5^2\times7}$

Exercice 5059

1. Soit n un entier naturel. Exprimer le reste de la division euclidienne de n^2 par 8 en fonction du reste de la division euclidienne de n par 4.

2. Soit a et b deux entiers. Etablir la propriété suivante :

   "Si a^2+b^2 est un entier divisible par 8 alors a et b sont des entiers pairs"

Correction 5059

1. Soit n un nombre entier. La division euclidienne de n par 4 donne l'existence d'un unique couple $(q\,;r)$ vérifiant :

$n = 4{\cdot}q + r$

On en déduit :

$$n^2 = \left(4{\cdot}q + r\right)^2 = 16{\cdot}q^2 + 8{\cdot}q{\cdot}r + r^2$$
$$= 8{\cdot}\left(2{\cdot}q^2 + q{\cdot}r\right) + r^2$$

On en déduit que le nombre n^2 a, par la division euclidienne par 8, un reste égal à r^2.

2. Soit k un nombre entier. Le reste de la division euclidienne de k par 4 prend ses valeurs parmi 0, 1, 2 et 3. Ainsi, le reste de la division euclidienne de k^2 par 8 a pour valeur :

Reste de k par 4	0	1	2	3
k^2	0	1	4	9
Reste de k^2 par 8	0	1	4	1

Supposons que $a^2 + b^2$ est un entier divisible par 8 alors le reste de la division euclidienne de $a^2 + b^2$ par 8 vaut 0.

Or, d'après le tableau des restes de k^2 par 8 peut donner les valeurs 0, 1 ou 4. Ainsi, pour que la somme de deux entiers ait un reste de 0 par la division euclidienne, il faut :

- soit que les deux entiers a^2 et b^2 aient pour reste 0 par la division euclidienne par 8 : on en déduit que les deux entiers a et b doivent avoir 0 pour reste par la division euclidienne par 4.
  Alors les deux entiers a et b sont divisibles par 4 : ils sont pairs.
- soit que les deux entiers a^2 et b^2 aient pour reste 4 par la division euclidienne par 8 : on en déduit que les deux entiers a et b doivent avoir 2 pour reste par la division euclidienne par 4 :

$$\begin{array}{l|l} a = 4\times k + 2 & b = 4\times k' + 2 \\ \quad = 2\times(2k+1) & \quad = 2\times(2k'+1) \end{array}$$

On en déduit que les deux entiers a et b sont des entiers pairs.

Exercice 5060

Déterminer l'ensemble des couples $\left(a\,;b\right)$ d'entiers relatifs vérifiant l'égalité :

$a^2 - b^2 = 11$

Correction 5060

Considérons l'équation de départ :

$$a^2 - b^2 = 11$$

On a la factorisation :

$(a+b)(a-b) = 11$

11 étant un nombre impair, voici les couples $\left(a+b\,;a-b\right)$ vérifiant cette relation :

$\left(-1\,;-11\right)$; $\left(1\,;11\right)$; $\left(11\,;1\right)$; $\left(-11\,;-1\right)$

Traitons ces quatres cas :

- On a le système $\begin{cases} a + b = -1 \\ a - b = -11 \end{cases}$

  Par addition de ces deux équations, on obtient :

  $2{\cdot}a = -12$

  $a = \dfrac{12}{2}$

  $a = -6$

  On en déduit la valeur de b :

  $a + b = -1$

  $-6 + b = -1$

  $b = -1 + 6$

  $b = 5$

  Le couple $\left(-6\,;5\right)$ est solution de cette équation.

- On a le système $\begin{cases} a + b = 1 \\ a - b = 11 \end{cases}$

  Par addition de ces deux équations, on obtient :

  $2{\cdot}a = 12$

  $a = \dfrac{12}{2}$

  $a = 6$

  De la première équation, on en déduit :

  $a + b = 1$

  $6 + b = 1$

  $b = 1 - 6$

  $b = -5$

  Le couple $\left(6\,;-5\right)$ est solution de cette équation.

- On a le système $\begin{cases} a + b = -11 \\ a - b = -1 \end{cases}$

  Par addition des deux lignes, on a :

  $2{\cdot}a = -12$

  $a = \dfrac{-12}{2}$

  $a = -6$

  De la première équation, on en déduit :

  $a + b = -11$

  $-6 + b = -11$

  $b = -11 + 6$

  $b = -5$

  Le couple $\left(-6\,;-5\right)$ est solution de cette équation.

- On a le système $\begin{cases} a + b = 11 \\ a - b = 1 \end{cases}$

  Par addition des deux lignes, on a :

  $2{\cdot}a = 12$

  $a = \dfrac{12}{2}$

  $a = 6$

  De la première équation, on en déduit :

  $a + b = 11$

  $6 + b = 11$

  $b = 11 - 6$

  $b = 5$

  Le couple $\left(6\,;5\right)$ est solution de cette équation.

Ainsi, cette équation admet pour ensemble de solution :

$\mathcal{S} = \left\{\left(-6\,;5\right)\,;\left(6\,;-5\right)\,;\left(-6\,;-5\right)\,;\left(6\,;5\right)\right\}$

Exercice 3392

Soit a et b deux entiers naturels non nuls ; on appelle "*réseau*" associé aux entiers a et b l'ensemble des points du plan, muni d'un repère orthonormal, dont les coordonnées $(x\,;y)$ sont des entiers vérifiant les conditions :

$0 \leqslant x \leqslant a \quad ; \quad 0 \leqslant y \leqslant b$

On note $R_{a,b}$ ce réseau.

Le but de l'exercice est de relier certaines propriétés arithmétiques des entiers x et y à des propriété géométriques des points correspondants du réseau.

A - Représentation graphique de quelques ensemble

Dans cette question, les réponses sont attendues sans explication, sous la forme d'un graphique qui sera dûment complété sur la feuille annexe à rendre avec la copie.
Représenter graphiquement les points $M\,(x\,;y)$ du réseau $R_{8,8}$ vérifiant :

1. $x \equiv 2 \pmod 3$ et $y \equiv 1 \pmod 3$,
sur le graphique 1 de la feuille annexe.

2. $x + y \equiv 1 \pmod 3$,
sur le graphique 2 de la feuille annexe.

3. $x \equiv y \pmod 3$,
sur le graphique 3 de la feuille annexe.

B - Résolution d'une équation

On considère l'équation (E): $7x-4y=1$, où les inconnues x et y sont des entiers relatifs.

1. Déterminer un couple d'entiers relatifs $(x_0\,;y_0)$ solution de l'équation (E).

2. Déterminer l'ensemble des couples d'entiers relatifs solutions de l'équation (E).

3. Démontrer que l'équation (E) admet une unique solution $(x\,;y)$ pour laquelle le point $M\,(x\,;y)$ correspondant appartient au réseau $R_{4,7}$.

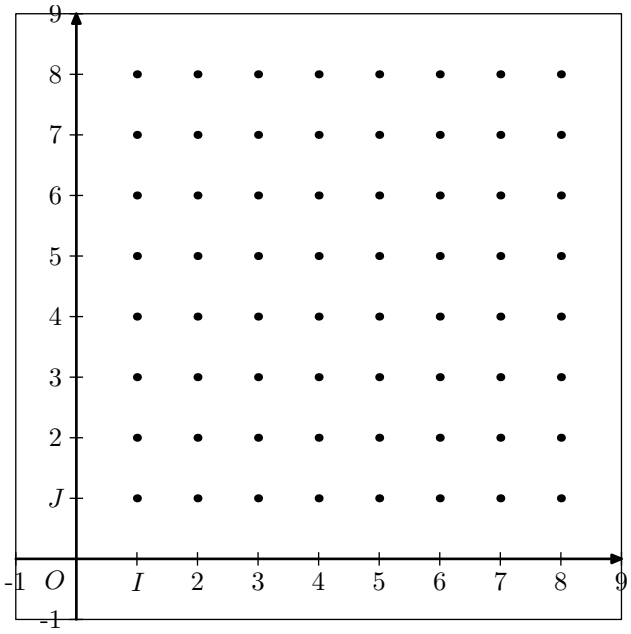
C - Une propriété des points situés sur la diagonale du réseau.

Si a et b sont deux entiers naturels non nuls, on considère la diagonale $[OA]$ du réseau $R_{a,b}$ avec $O\,(0\,;0)$ et $A\,(a\,;b)$.

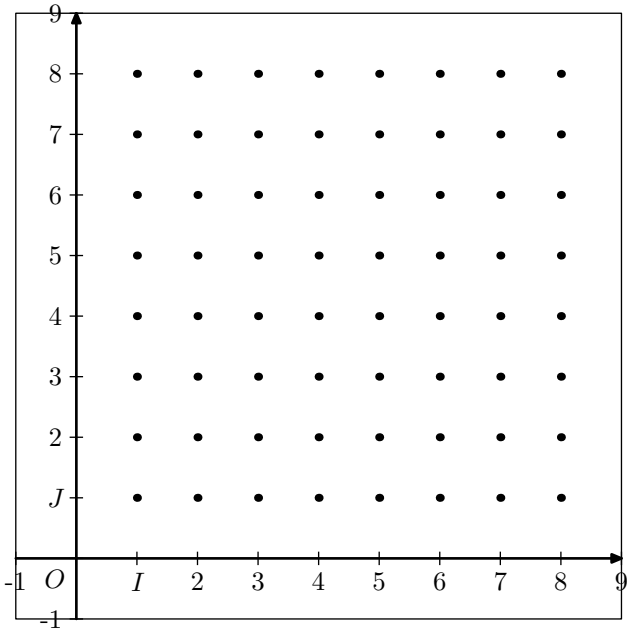
1. Démontrer que les points du segment $[OA]$ sont caractérisés par les conditions :
$0 \leqslant x \leqslant a \quad ; \quad 0 \leqslant y \leqslant b \quad ; \quad ay = bx$

2. Démontrer que si a et b sont premiers entre eux, alors les points O et A sont les seuls points du segment $[OA]$ appartenant au réseau $R_{a,b}$.

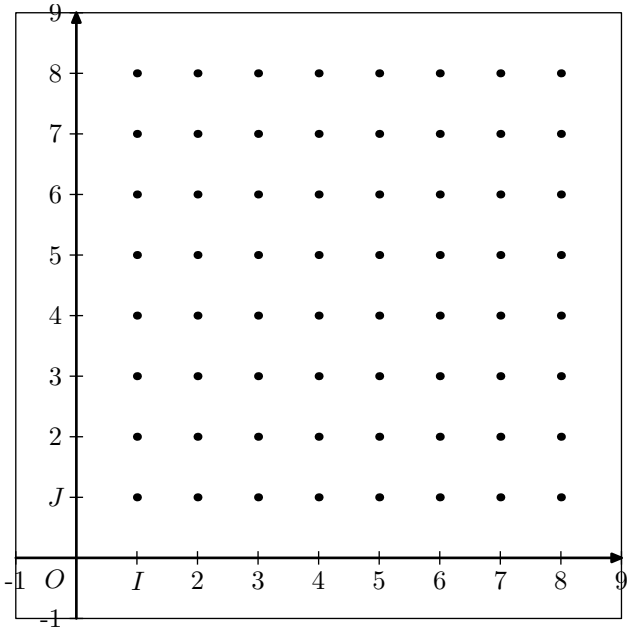
3. Démontrer que si a et b ne sont pas premiers entre eux, alors le segment $[OA]$ contient au moins un autre point du réseau.
(On pourra considérer le pgcd d des nombres a et b et poser $a=da'$ et $b=db'$)



Graphique 1



Graphique 2

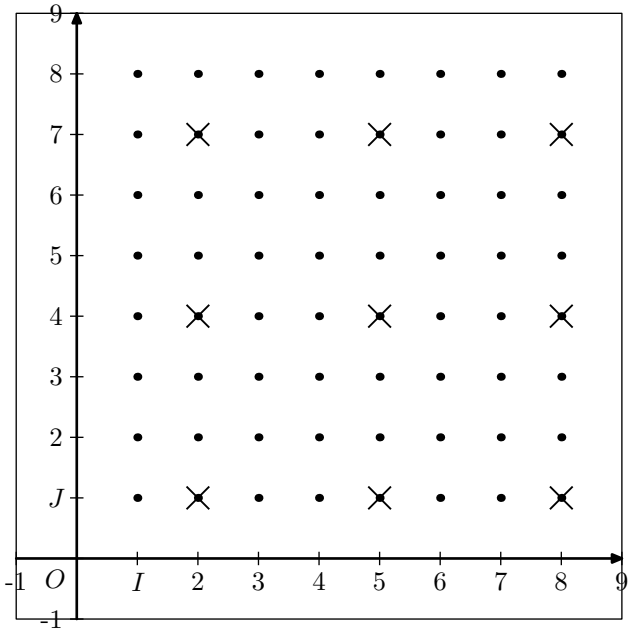


Graphique 3

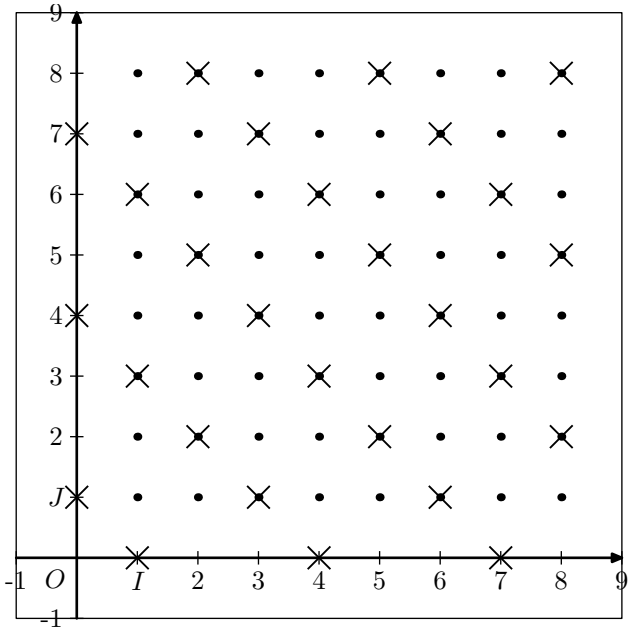
Correction 3392

Partie A

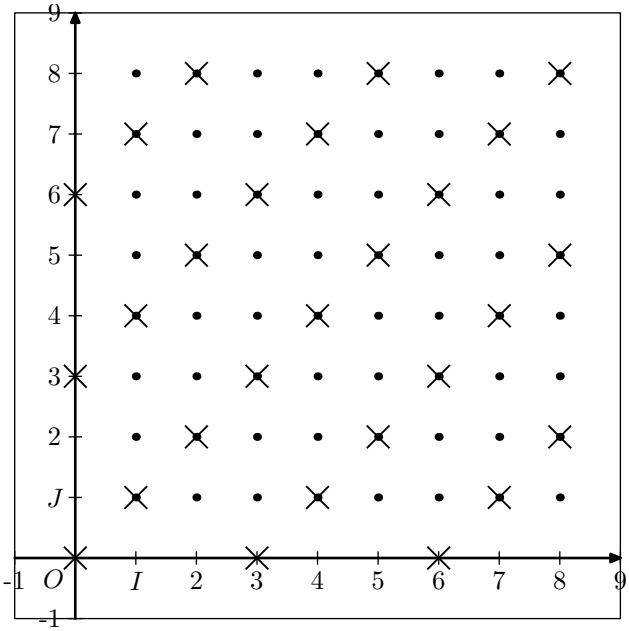
1.



2.



3.



Partie B

1. Le couple $(-1\,;-2)$ est solution de cette équation :
$7{\cdot}x-4{\cdot}y=7\times(-1)-4\times(-2)=-7+8=1$

On peut remarquer aussi que le couple $(3\,;5)$ est solution de l'équation (E) :
$7{\cdot}x-4{\cdot}y=7\times3-4\times5=21-20=1$

2. Soit $(x\,;y)$ un couple de solution de l'équation (E) ; on a l'égalité suivante :
$7{\cdot}x-4{\cdot}y=1$

La question précédente, permet d'écrire :

$7{\cdot}x-4{\cdot}y=7\times(-1)-4\times(-2)$

$7{\cdot}(x+1)=4{\cdot}(y+2)$

L'entier 7 est premier, on en déduit que les nombres 7 et 4 sont premiers entre eux.

- D'après l'égalité précédemment établie, l'entier 7 divise le produit $4{\cdot}(y+2)$. Or, les entiers 7 et 4 étant premiers entre eux, on en déduit, à l'aide du théorème de Gauss, que 7 divise le facteur $(y+2)$.
Il existe ainsi un entier k' vérifiant :
$y+2=7{\cdot}k'$
$y=7{\cdot}k'-2$
- On remarque que l'entier 4 divise le produit $7{\cdot}(x+1)$. Or, les entiers 7 et 4 étant premiers entre eux, on en déduit, à l'aide du théorème de Gauss, que l'entier 4 divise le facteur $(x+1)$.
Il existe ainsi un entier k vérifiant :
$x+1=4{\cdot}k$
On en déduit :
$x=4{\cdot}k-1$

Ainsi, les couples solutions de l'équation (E) s'écrivent sous la forme :
$\left(4{\cdot}k-1\,;7{\cdot}k'-2\right)$

Maintenant, cherchons parmi l'ensemble :
$\mathcal{E}=\left\{\left(4{\cdot}k-1\,;7{\cdot}k'-2\right)\;\middle|\;k\in\mathbb{Z}\text{ et }k'\in\mathbb{Z}\right\}$
les couples qui sont solutions de l'équation (E).

Soit $(x\,;y)\in\mathcal{E}$ solution de (E) :

$$7\cdot(4\cdot k-1)-4\cdot(7\cdot k'-2)=1$$
$$28\cdot k-7-28\cdot k'+8=1$$
$$28\cdot(k-k')+1=1$$
$$28\cdot(k-k')=0$$
$$k-k'=0$$
$$k=k'$$

Ainsi, l'ensemble des solutions de l'équation (E) est :

$$\mathcal{E}'=\left\{(4\cdot k-1\,;7\cdot k-2)\ \middle|\ k\in\mathbb{Z}\right\}$$

3. Soit $(x\,;y)$ une solution de (E), il existe un entier k vérifiant :

$$(x\,;y)=(4\cdot k-1\,;7\cdot k-2)$$

Cherchons la valeur de l'entier k afin que :

$$0\leqslant 4\cdot k-1\leqslant 4$$
$$1\leqslant 4\cdot k\leqslant 5$$
$$\frac{1}{4}\leqslant k\leqslant\frac{5}{4}$$

Ainsi, la seule solution de (E) appartenant au réseau $R_{4,7}$ est $(3\,;5)$

Partie C

1. La droite passant par les points O et A a pour coefficient directeur :

$$\frac{y_A-y_O}{x_A-x_O}=\frac{b-0}{a-0}=\frac{b}{a}$$

Passant par le point O, cette droite représente une fonction linéaire dont l'équation est :

$$y=\frac{b}{a}\cdot x$$
$$a\cdot y=b\cdot x$$

2. Supposons que le point de coordonnée $(x\,;y)$ appartient au segment $[OA]$, alors ses coordonnées vérifient l'égalité :

$$a\cdot y=b\cdot x$$

- Ainsi, l'entier a divise $b\cdot x$; or, sachant que a et b sont premiers entre eux, d'après le théorème de Gauss, on en déduit que l'entier a doit diviser x. Il existe un entier k tel que :

$$x=k\cdot a$$

L'égalité devient :

$$a\cdot y=b\cdot x$$
$$a\cdot y=b\cdot(k\cdot a)$$
$$y=b\cdot k$$

Le nombre y est un multiple de b.

- De même, en observant que b divise $a\cdot y$, on montre l'existence, à l'aide du théorème de Gauss, d'un entier k vérifiant :

$$y=k\cdot b$$

L'égalité devient :

$$a\cdot(k\cdot b)=b\cdot x$$
$$a\cdot k=x$$

Le nombre x est un multiple de b.

Ainsi, les seuls points à coordonnées entières ont pour coordonnée :

$$(k\cdot a\,;k\cdot b)\quad\text{où } k\in\mathbb{Z}$$

Dans le réseau $R_{a,b}$, les seuls points de la diagonales $[OA]$ ayant des coordonnées entières sont les points O et A.

3. Soit a et b deux nombres non-premiers entre eux ; notons $d=PGCD(a\,;b)$. On a $d>1$.

Il existe deux entiers k et k' tels que :

$$a=k\cdot d\quad;\quad b=k'\cdot d\qquad\text{où } 1\leqslant k<a \text{ et } 1\leqslant k'<b$$

Considérons le point de coordonnées $C\left(k\,;k'\right)$. Ce point C appartient au réseau $R_{a,b}$ et on a les deux valeurs suivantes :

$$a\cdot y_C=a\cdot k'=k\cdot d\cdot k'\quad;\quad b\cdot x_C=b\cdot k=k'\cdot d\cdot k'$$

On en déduit l'égalité : $a\cdot y_C=b\cdot x_C$

D'après la question 1., que le point $\left(k\,;k'\right)$ est un point de la diagonale $[OA]$; et ce point appartient au réseau $R_{a,b}$.

15. Reste de la division euclidienne :

Exercice 3423

Dans cet exercice, on s'intéresse à la division euclidienne par 4 et plus particulièrement au reste de la division par 4 :

1. Soit x et y deux nombres entiers dont le reste par la division euclidienne par 4 vaut respectivement 2 et 3
   a. Donner une expression caractérisant la division euclidienne de x et y par 4.
   b. Etablir que le reste de la division $(x+y)$ par 4 vaut 1.
   c. Etablir que le reste de la division $x\cdot y$ par 4 vaut 2

2. Soit x et y deux nombres entiers ; on note r_x et r_y les restes de la division respectivement de x et de y par 4.

   On considère les deux tableaux ci-dessous :

r_y \ r_x	0	1	2	3
0				
1				
2				
3				

r_{x+y}

r_y \ r_x	0	1	2	3
0				
1				
2				
3				

$r_{x\cdot y}$

On note r_{x+y} et $r_{x\cdot y}$ les restes respectifs par la division par 4 des nombres $(x+y)$ et $(x\cdot y)$.

   a. Inscrire dans ces deux tableaux, les résultats obtenus à la question 1..
   b. Compléter de manière "*intuitive*" entièrement ces deux tableaux.

Correction 3423

1. a. Le reste de la division euclidienne de x par 4 vaut 2 ;

on en déduit l'existence d'un nombre $k \in \mathbb{Z}$ tel que :
$x = 4{\cdot}k + 2$

De même, puisque la division euclidienne de y par 4 donne 3, on a l'existence de $k' \in \mathbb{Z}$ tel que :
$y = 4{\cdot}k' + 3$

b. On en déduit que la somme de x et de y peut s'écrire :
$x + y = \big(4{\cdot}k + 2\big) + \big(4{\cdot}k' + 3\big)$
$= 4{\cdot}\big(k + k'\big) + 5 = 4{\cdot}\big(k + k' + 1\big) + 1$

On en déduit que le reste de la division euclidienne de $x + y$ par 4 est 3.

c. De même, on peut écrire pour la multiplication :
$x{\cdot}y = \big(4{\cdot}k + 2\big){\cdot}\big(4{\cdot}k' + 3\big)$
$= \big(4{\cdot}k\big){\cdot}\big(4{\cdot}k'\big) + \big(4{\cdot}k\big){\cdot}3 + 2{\cdot}\big(4{\cdot}k'\big) + 2{\cdot}3$
$= 16{\cdot}k{\cdot}k' + 12{\cdot}k + 8{\cdot}k' + 6$
$= 4{\cdot}\big(4{\cdot}k{\cdot}k' + 3{\cdot}k + 2{\cdot}k'\big) + 6$
$= 4{\cdot}\big(4{\cdot}k{\cdot}k' + 3{\cdot}k + 2{\cdot}k' + 1\big) + 2$

On en déduit que le reste de la division euclidienne de $x{\cdot}y$ par 4 vaut 2

2.

r_y \ r_x	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

r_{x+y}

r_y \ r_x	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$r_{x{\cdot}y}$

Exercice 3425

Déterminer l'ensemble des entiers naturels n tels que le quotient de la division euclidienne de n par 5 soit égal au reste par la même division.

Correction 3425

La division euclidienne de n par 5 donne deux entiers naturels q et r vérifiant :
$n = q \cdot 5 + r \qquad$ où $0 \leqslant r \leqslant 5$

Or, on demande que le quotient doit être égal au reste de cette division, on en déduit :
$n = r \cdot 5 + r \qquad$ où $0 \leqslant r < 5$

La valeur de r ne prenant que 5 valeur distincte, énumérons ces possibilités :

r	$n = r \cdot 5 + r$
0	0
1	6
2	12
3	18
4	24

---

16. Identité et Théorème de Bézout :

Exercice 3664

Indiquer si la proposition suivante est vraie ou fausse et donner une justification de la réponse choisie :

Pour tout entier naturel n non nul, n et $2n{+}1$ sont premiers entre eux.

Correction 3664

Considérons la combinaison linéaire de n et de $2n{+}1$ suivante :
$-2{\cdot}n + 1{\cdot}\big(2n + 1\big) = -2n + 2n + 1 = 1$

Le théorème de Bezout permet d'affirmer que les entiers a et b sont premiers entre eux.

Exercice 3817

Soit n un entier relatif. On définit la valeur des entiers a et b en fonction de celle de n.

Pour chaque question, montrer que es entiers a et b sont premiers entre eux quelque soit la valeur de l'entier naturel n.

1. $a = 3n{-}1$; $b = -2n{+}1$ 2. $a = 6n{+}1$; $b = 9n{+}1$

Correction 3817

1. Pour montrer que les deux entiers $a{=}3n{-}1$ et $b{=}-2n{+}1$ sont premiers entre eux, supposons l'existence deux entiers relatifs u et v vérifiant :
$u{\cdot}a + v{\cdot}b = 1$

Ainsi, on a :
$u{\cdot}a + v{\cdot}b = 1$
$u{\cdot}\big(3n - 1\big) + v{\cdot}\big(-2n + 1\big) = 1$
$3{\cdot}u{\cdot}n - u - 2{\cdot}v{\cdot}n + v = 1$
$\big(3{\cdot}u - 2{\cdot}v\big){\cdot}n + \big(v - u\big) = 1$

Par identification des deux membres pour toutes valeurs de n, on obtient le système :
$\begin{cases} 3{\cdot}u - 2{\cdot}v = 0 \\ v - u = 1 \end{cases}$

On en déduit les valeurs suivantes : $u{=}2$; $v{=}3$

Vérifions que ces deux valeurs vérifient la combinaison linéaire de a et b souhaitée :
$u{\cdot}a + v{\cdot}b = 2{\cdot}\big(3n - 1\big) + 3{\cdot}\big(-2n + 1\big)$
$= 6n - 2 - 6n + 3 = 1$

D'après le théorème de Bezout, on en déduit que les entiers a et b sont premiers entre eux quelle que soit la valeur de n.

2. De même, déterminons l'existence de u et v tels que pour tout entier naturel n, on a :

$$u\cdot a + v\cdot b = 1$$
$$u\cdot(6n+1) + v\cdot(9n+1) = 1$$
$$6\cdot u\cdot n + u + 9\cdot v\cdot n + v = 1$$
$$(6\cdot u + 9\cdot v)\cdot n + (u+v) = 1$$

Par identification des polynômes en n formant les deux membres de l'égalité, on obtient le système :

$$\begin{cases} 6\cdot u + 9v = 0 \\ u + v = 1 \end{cases}$$

On en déduit les valeurs : $u=3$; $v=-2$

Vérifions que ces deux valeurs vérifient la combinaison linéaire de a et b souhaitée :

$$u\cdot a + v\cdot b = 3\cdot(6n+1) - 2\cdot(9n+1)$$
$$= 18n + 3 - 18n - 2 = 1$$

D'après le théorème de Bezout, les entiers a et b sont premiers entre eux pour tout entier naturel n.

Exercice 3820

1. Déterminer un couple $(x\,;y)$ d'entiers solution de l'équation :
$$56\cdot x + 45\cdot y = 1$$

2. En déduire un couple $\left(x'\,;y'\right)$ d'entiers relatifs vérifiant l'égalité :
$$56\cdot x' + 45\cdot y' = 3$$

Correction 3820

1. L'algorithme d'Euclide, appliqué aux nombres 56 et 45, permet d'obtenir le tableau ci-dessous :

Dividende	Diviseur	Reste	
56	45	11	$56 = 1 \times 45 + 11$
45	11	1	$45 = 4 \times 11 + 1$
11	1	0	$11 = 11 \times 1 + 0$

On en déduit : $\text{pgcd}\left(56\,;45\right) = 1$. Les deux entiers 56 et 45 sont premiers entre eux.
Le théorème de Bezout donne l'existence de deux entiers, il existe deux entiers x et y tels que :

$$x\cdot 56 + y\cdot 45 = 1$$

Exprimant les restes, obtenues dans le tableau de l'algorithme d'Euclide, à l'aide des deux nombres a=56 et b=45 :

- $56 = 1\times 45 + 11$
  $a = 1\times b + 11$
  $a - b = 11$
  $11 = a - b$
- $45 = 4\times 11 + 1$
  $b = 4\times(a-b) + 1$
  $-4a + 5b = 1$
  $1 = -4a + 5b$

On en déduit une valeur possible du couple $(x\,;y)$:
$(x\,;y) = \left(-4\,;5\right)$

2. De la question précédente, on a :

$$56\times(-4) + 45\times 5 = 1$$
$$3\cdot\left[56\times(-4) + 45\times 5\right] = 3\times 1$$
$$56\times\left[3\times(-4)\right] + 45\times\left(3\times 5\right) = 3$$
$$56\times(-12) + 45\times 15 = 3$$

Ainsi, un couple solution est : $\left(x'\,;y'\right) = \left(-12\,;15\right)$.

Exercice 3855

Pour tout entier naturel n supérieur ou égal à 2, on pose :
$A(n) = n^4 + 1$

1. Etudier la parité de l'entier $A(11)$.

2. Montrer que, quel que soit l'entier n, $A(n)$ n'est pas un multiple de 3.

3. Montrer que tout entier d diviseur de $A(n)$ est premier avec n.

4. Montrer que, pour tout entier d diviseur de $A(n)$:
$n^8 \equiv 1 \pmod{d}$

Correction 3855

1. Le produit de deux nombres impairs est un nombre impair ; on en déduit successivement :
- 11 est un entier impair ;
- 11^2 est un entier impair ;
- 11^3 est un entier impair ;
- 11^4 est un entier impair.

On en déduit que :
$A(11) = 11^4 + 1$ est un nombre pair.

2. Faisons une étude de la propriété "*$A(n)$ n'est pas un multiple de 3*" par disjonction de cas sur le reste de la division euclidienne de n par 3 :

- $n\equiv 0 \pmod 3$:
$A(n) = n^4 + 1$
$\equiv 0^4 + 1 \equiv 1 \pmod 3$
$A(n)$ n'est pas un divisible par 3.
- $n\equiv 1 \pmod 3$:
$A(n) = n^4 + 1$
$\equiv 1^4 + 1 \equiv 2 \pmod 3$
$A(n)$ n'est pas un divisible par 3.
- $n\equiv 2 \pmod 3$:
$A(n) = n^4 + 1$
$\equiv 2^4 + 1 \equiv 16 + 1 \equiv 17 \equiv 2 \pmod 3$
$A(n)$ n'est pas un divisible par 3.

3. Soit d un diviseur de $A(n)$; il existe un entier $k\in\mathbb{Z}$ tel que :
$A(n) = k\cdot d$

On peut écrire les égalités successives :

$$k\cdot d = A(n)$$
$$k\cdot d = n^4 + 1$$
$$k\cdot d - n^4 = 1$$
$$k\cdot d - n^3\cdot n = 1$$

D'après le théorème de Bezout, on en déduit que les entiers d et n sont premiers entre eux.

4. Soit d est un diviseur de $A(n)$, on a :

$$\begin{aligned}
A(n) &\equiv 0 \pmod{d}\\
n^4+1 &\equiv 0 \pmod{d}\\
n^4\cdot\left(n^4+1\right) &\equiv n^4\cdot 0 \pmod{d}\\
n^8+n^4 &\equiv 0 \pmod{d}\\
n^8+n^4+1 &\equiv 0+1 \pmod{d}\\
n^8+A(n) &\equiv 1 \pmod{d}\\
n^8+0 &\equiv 1 \pmod{d}\\
n^8 &\equiv 1 \pmod{d}
\end{aligned}$$

17. Arithmétique et suite :

Exercice 3322

On considère la suite (u_n) d'entiers naturels définie par :

$$\begin{cases} u_0 = 14 \\ u_{n+1} = 5u_n - 6 \text{ pour tout entier naturel } n \end{cases}$$

1. Calculer u_1, u_2, u_3 et u_4.
Quelle conjecture peut-on émettre concernant les deux derniers chiffres de u_n ?

2. Montrer que, pour tout entier naturel n, $u_{n+2} \equiv u_n \pmod{4}$.
En déduire que pour tout entier naturel k, $u_{2k} \equiv 2 \pmod{4}$ et $u_{2k+1} \equiv 0 \pmod{4}$.

3. a. Montrer par récurrence que, pour tout entier naturel n, $2u_n = 5^{n+2}+3$.

b. En déduire que, pour tout entier naturel n, $2u_n \equiv 28 \pmod{100}$.

4. Déterminer les deux derniers chiffres de l'écriture décimale de u_n suivant les valeurs de n.

5. Montrer que le $PGCD$ de deux termes consécutifs de la suite (u_n) est constant. Préciser sa valeur.

Correction 3322

1. Voici les cinq premiers termes de la suite (u_n) :
- $u_0 = 14$
- $u_1 = 5\cdot u_0 - 6 = 5\cdot 14 - 6 = 70 - 6 = 64$
- $u_2 = 5\cdot u_1 - 6 = 5\cdot 64 - 6 = 320 - 6 = 314$
- $u_3 = 5\cdot u_2 - 6 = 5\cdot 314 - 6 = 1570 - 6 = 1564$
- $u_4 = 5\cdot u_3 - 6 = 5\cdot 1564 - 6 = 1570 - 6 = 7814$

On peut émettre la conjecture que les deux derniers chiffres de cette suite sont respectivement 14 et 64.

2. On a :

$$\begin{aligned}
u_{n+2} &= 5\cdot u_{n+1} - 6 = 5\cdot\left(5u_n - 6\right) - 6\\
&= 25\cdot u_n - 30 - 6 = 25\cdot u_n - 36\\
&\equiv 1\cdot u_n - 0 \pmod{4} \equiv u_n \pmod{4}
\end{aligned}$$

D'après la propriété précédemment établie et pour k un entier naturel, on a :

- $2\cdot k$ est toujours un entier naturel pair :
$u_{2k} \equiv u_0 \equiv 14 \equiv 2 \pmod{4}$
- $2\cdot k+1$ est toujours un entier naturel impair :
$u_{2k+1} \equiv u_1 \equiv 64 \equiv 0 \pmod{4}$

3. a. Etablissons par un raisonnement par récurrence, l'égalité suivante pour tout entier naturel n :
$2\cdot u_n = 5^{n+2}+3$
- *Initialisation :*
On a :
$2\cdot u_0 = 2\cdot 14 = 28 = 5^2+3$
Ce qui établit que la propriété est vraie au rang 1.
- *Hérédité :*
Supposons la propriété vraie au rang n ; on a :
$2\cdot u_n = 5^{n+2}+3$
On a :

$$\begin{aligned}
2\cdot u_{n+1} &= 2\cdot\left(5\cdot u_n - 6\right)\\
&= 5\cdot\left(2\cdot u_n\right) - 12 = 5\cdot\left(5^{n+2}+3\right) - 12\\
&= 5^{(n+1)+2} + 15 - 12 = 5^{(n+1)+2} + 3
\end{aligned}$$

Ainsi, la propriété est vraie au rang $(n+1)$.

b. Par récurrence, montrons que pour tout $n \in \mathbb{N}$, on a :
$5^{n+2} \equiv 25 \pmod{100}$
- *Initialisation :*
$5^{0+2} = 5^2 = 25$
- *Hérédité :*
Supposons que pour $n \in \mathbb{N}$, on a :
$5^{n+2} \equiv 25 \pmod{100}$.
On a :

$$\begin{aligned}
5^{(n+1)+2} &= 5\cdot 5^{n+2}\\
&\equiv 5\cdot 25 \equiv 125 \equiv 25 \pmod{100}
\end{aligned}$$

On en déduit, à l'aide de la question a. :

$$\begin{aligned}
2\cdot u_n &= 5^{n+2}+3\\
&\equiv 25+3 \pmod{100}\\
&\equiv 28 \pmod{100}
\end{aligned}$$

4. Pour n un entier naturel, on a :
$2\cdot u_n \equiv 28 \pmod{100}$
Il existe un entier naturel k tel que :
$2\cdot u_n = 28 + 100\cdot k$
$u_n = 14 + 50\cdot k$
On remarque facilement que si :
- k est pair : il existe k' tel que $k = 2\cdot k'$; on a :
$u_n = 14 + 50\cdot\left(2\cdot k'\right) = 14 + 100k'$
Le nombre u_n se termine par 14.
- $(k+1)$ est impair : il existe k' tel que $k = 2\cdot k'+1$; on a :

$$\begin{aligned}
u_n &= 14 + 50\cdot\left(2\cdot k'+1\right) = 14 + 100\cdot k' + 50\\
&= 64 + 100\cdot k'
\end{aligned}$$

Le nombre u_n se termine par 64.

5. Deux démonstrations semblent possibles pour cette question ; notons :
$d = PGCD(u_{n+1}\,;\,u_n)$

- On a l'égalité suivante :
$PGCD(u_{n+1}\,;\,u_n) = PGCD(5{\cdot}u_n - 6\,;\,u_n)$
Par soustractions successives et les propriétés du PGCD :
$= PGCD(u_n\,;\,-6)$
Ainsi, d divise -6 ; les valeurs possibles sont alors 1, 2, 3, 6 :
  - 1 est impossible car deux termes consécutifs ont leurs deux derniers chiffres qui terminent par 64 et 14 : entraînant qu'ils sont tous deux divisibles par 2.
  - 3 est également impossible car de l'égalité :
$2{\cdot}u_n = 5^{n+2} - 3$
On montre facilement que si u_n est divisible par 3 alors à fortiori 5^n est également divisible par 3 ce qui est faux car 3 et 5 sont deux nombres premiers entre eux.
  - Si u_n n'est pas divisible par 3 alors il ne peut être divisible par 6.

  Il ne reste qu'une possibilité $d = 2$.
- On a les égalités suivantes :
  - $PGCD(2{\cdot}u_n\,;\,2{\cdot}u_{n+1}) = 2{\cdot}PGCD(u_n\,;\,u_{n+1})$
$= 2{\cdot}d$
  - $PGCD(2{\cdot}u_n\,;\,2{\cdot}u_{n+1})$
$= PGCD(5^{n+2}+3\,;\,5^{n+3}+3)$

  On en déduit que d divise $5^{n+2}+3$ et $5^{n+3}+3$; il divise donc leur différence. Il existe $k \in \mathbb{Z}$ tel que :
$k{\cdot}2{\cdot}d = (5^{n+3}+3) - (5^{n+2}+3)$
$= 5^{n+3} - 5^{n+2} = 5^{n+2}{\cdot}(5-1)$
$= 4{\cdot}5^{n+2}$
$\Longrightarrow k{\cdot}d = 2{\cdot}5^{n+2}$
Le chiffre des unités de u_n et u_{n+1} est 4 *(voir question précédente)* : on en déduit que ces deux nombres ne sont pas divisbles par 5. d n'est pas un multiple de 5 ; 5 étant un nombre premier, d et 5 sont premiers entre eux.
d divisant $2{\cdot}5^{n+2}$, d'après le théorème de Gauss, on en déduit que d divise 2 :
$d = 1$ ou $d = 2$
Les deux nombres u_n et u_{n+1} étant pairs, on en déduit :
$d = 2$

On vient de montrer que le $PGCD$ de deux termes consécutifs vaut 2.

---

18. Premiers exercices de congruences :

Exercice 3468

Vérifier la véracité de chacune des égalités suivantes :

a. $15 \equiv 27 \pmod 3$
b. $17 \equiv 11 \pmod 4$
c. $153 \equiv 237 \pmod{12}$
d. $-5 \equiv 8 \pmod{13}$
e. $-81 \equiv 224 \pmod 6$
f. $37^4 \equiv 1 \pmod 4$

Correction 3468

On utilisera la propriété suivante :
$a \equiv b \pmod c \iff (a-b)$ multiple de c

a. $15 - 27 = -12$ qui est un multiple de 3 dans $\mathbb{Z}$.
On en déduit que la relation suivante est vraie :
$15 \equiv 27 \pmod 3$

b. $17 - 11 = 6$ n'est pas un multiple de 4.
La relation proposée est donc fausse.

c. On a :
$153 - 237 = -84 = (-7){\times}12$
On en déduit que $153 - 237$ est un multiple de 12 dans $\mathbb{Z}$; la relation suivante est donc vraie :
$153 \equiv 237 \pmod{12}$

d. On a $-5-8 = -13$; on en déduit que la relation proposée est vraie.

e. On a :
$-81 - 224 = -305 = (-51){\times}6 + 1$
On en déduit que -305 n'est pas un multiple de 6 ; la relation proposée est fausse.

f. On a :
$37 = 9{\times}4 + 1$
Ainsi, on en déduit :
$37 \equiv 1 \pmod 4$
$37^4 \equiv 1^4 \pmod 4$
$37^4 \equiv 1 \pmod 4$
La relation proposée est donc vraie.

Exercice 3472

Dans cet exercice on étudie la divisibilité par 11 en exploitant la congruence modulo 11 des puissances de 10

1. a. Vérifier que $100 \equiv 1 \pmod{11}$.
En déduire que $10^4 \equiv 1 \pmod{11}$.

   b. Vérifier que $10 \equiv -1 \pmod{11}$.
En déduire que :
   - $10^3 \equiv -1 \pmod{11}$
   - $10^5 \equiv -1 \pmod{11}$

2. a. En utilisant l'égalité $3729 = 37{\times}100 + 29$ et les résultats précédents, montrer que 3729 est divisible par 11.

   b. En utilisant la méthode précédente, étudier la divisibilité de 9240 par 11.

3. a. En utilisant l'égalité :
$3729 = 3{\times}1000 + 7{\times}100 + 2{\times}10 + 9$
et les résultats précédents, montrer que 3729 est divisible par 11.

   b. En utilisant cette méthode, étudier la divisibilité de 9240 par 11.

4. Etudier la divisibilité de 197 277 par 11.

Correction 3472

1. a. La division euclidienne de 100 par 11 donne :
$100 = 9\times11 + 1$.
On a donc : $100 \equiv 1 \pmod{11}$. On en déduit :
$10^4 \equiv 10\times10\times10\times10 \pmod{11}$
$\equiv 1\times1\times1\times1 \equiv 1 \pmod{11}$

b. La différence des deux nombres 10 et -1 donne :
$10 - (-1) = 11$.
On en déduit la congruence de ces deux nombres modulo 11.
$10 \equiv -1 \pmod{11}$
Voici les deux autres congruences demandées :
- $10^3 \equiv -1\times(-1)\times(-1) \equiv -1 \pmod{11}$
- $10^5 \equiv -1\times(-1)\times(-1)\times(-1)\times(-1) \pmod{11}$
$\equiv -1 \pmod{11}$

2. a. Etudions la congruence de chaque termes et facteurs de cette expression :
$37 \equiv 4 \pmod{11}$; $100 \equiv 1 \pmod{11}$; $29 \equiv 7 \pmod{11}$
Grâce à l'égalité $3729 = 37\times100 + 29$ et les propriétés algébriques de la congruence, on obtient :
$3729 \equiv 37\times100 + 29 \equiv 4\times1 + 7 \pmod{11}$
$\equiv 0 \pmod{11}$
3729 est divisible par 11.

b. On décompose de même le nombre 9240 :
$9240 = 92\times100 + 40$.
Chaque termes et facteurs ont pour congruence :
$92 \equiv 4 \pmod{11}$; $100 \equiv 1 \pmod{11}$; $40 \equiv 7 \pmod{11}$
On en déduit la congruence suivante :
$9240 \equiv 92\times10 + 40 \equiv 4 + 7 \pmod{11}$
$\equiv 0 \pmod{11}$
On en déduit que 9240 est divisible par 11.

3. a. Les propriétés algébriques de la congruence donne :
$3729 \equiv 3\times1000 + 7\times100 + 2\times10 + 9 \pmod{11}$
$\equiv 3\times(-1) + 7\times1 + 2\times -1 + 9 \pmod{11}$
$\equiv 11 \equiv 0 \pmod{11}$
On en déduit que 3729 est divisible par 11.

b. De même :
$9240 \equiv 9\times1000 + 2\times100 + 4\times10 \pmod{11}$
$\equiv 9\times(-1) + 2\times1 + 4\times(-1) \pmod{11}$
$\equiv -11 \equiv 0 \pmod{11}$
On en déduit que 9240 est divisible par 11.

4. On décompose le nombre 197 277 :
$197277 = 1\times10^5+9\times10^4+7\times10^3+2\times10^2+7\times10+7$
On en déduit la congruence :
$\equiv 1\times10^5 + 9\times10^4 + 7\times10^3 + 2\times10^2 + 7\times10 + 7 \pmod{11}$
$\equiv 1\times(-1) + 9\times1 + 7\times(-1) + 2\times1 + 7\times(-1) + 7 \pmod{11}$
$\equiv 3 \pmod{11}$
Donc, 197 277 n'est pas divisible par 11.

19. Théorème de Gauss :

Exercice 3625

On considère le système de congruence :
$$(S) : \begin{cases} n \equiv 2 \pmod{3} \\ n \equiv 1 \pmod{5} \end{cases}$$
où n désigne un entier relatif.

1. Montrer que 11 est solution de (S).

2. Montrer que si n est solution de (S) alors $n-11$ est divisible par 3.

3. Montrer que les solutions de (S) sont tous les entiers de la forme $11+15\cdot k$, où k désigne un entier relatif.

Correction 3625

1. On a : $11 = 3\times3 + 2 \equiv 2 \pmod{3}$ | $11 = 2\times5 + 1 \equiv 1 \pmod{3}$

2. Supposons que l'entier n soit solution de $(\mathcal{S})$. En particulier, on a :
$n \equiv 2 \pmod{3}$
$n - 11 \equiv 2 - 11 \pmod{3}$
$n - 11 \equiv -9 \pmod{3}$
$n - 11 \equiv 0 \pmod{3}$
On vient de montrer que $n-11$ sera alors divisible par 13.

3. D'après la question précédente, il existe un entier k tel que :
$n - 11 = 3\cdot k$
$n = 11 + 3\cdot k$
Puisque n vérifie le système, on a :
$n \equiv 1 \pmod{5}$
$11 + 3\cdot k \equiv 1 \pmod{5}$
$1 + 3\cdot k \equiv 1 \pmod{5}$
$3\cdot k \equiv 0 \pmod{5}$
Ainsi, le nombre $3\cdot k$ est divisible par 5 et les nombres 5 et 3 sont premier entre eux.
D'après le théorème de Gauss, on en déduit que le nombre 5 divise l'entier k.

Il existe un entier k' tel que $k = 5\cdot k'$. Ainsi, l'entier n admet l'expression :
$n = 11 + 3\cdot k = 11 + 3\cdot(5\cdot k') = 11 + 15\cdot k'$

Exercice 3782

On se propose d'étudier des couples $(a\,;b)$ d'entiers strictement positifs, tels que :
$a^2 = b^3$

Soit $(a\,;b)$ un tel couple. On note $d = \text{pgcd}\,(a\,;b)$ et u, v les deux entiers naturels vérifiant :
$a = d\cdot u$; $b = d\cdot v$.

1. Montrer que : $u^2{=}d{\cdot}v^3$.

2. En déduire que v divise u, puis que $v{=}1$.

3. Soit $(a\,;b)$ un couple d'entiers strictement positifs.
Démontrer que l'on a $a^2{=}b^3$ si, et seulement si, a et b sont respectivement le cube et le carré d'un même entier.

Correction 3782

1. On a l'égalité suivante :
$$a^2 = b^3$$
$$\left(d{\cdot}u\right)^2 = \left(d{\cdot}v\right)^3$$
$$d^2{\cdot}u^2 = d^3{\cdot}v^3$$
$$u^2 = d{\cdot}v^3$$

2. D'après la question précédente, on a :
$u^2 = d{\cdot}v^3$
$u^2 = \left(d{\cdot}v^2\right){\cdot}v$
On en déduit que l'entier v divise u^2.

D'après la définition des entiers u et v, ces deux entiers entiers sont premiers entre eux :
$\text{pgcd}\,(v\,;u) = 1$

Or :
- v divise $u{\times}u$;
- u et v sont deux nombres premiers entre eux.

D'après le théorème de Gauss, on en déduit que :
v divise u.
On en déduit :
$\text{pgcd}\,(v\,;u) = v$
$1 = v$

3. • $\Longrightarrow$: supposons que $a^2{=}b^3$.
A la question précédente, on vient de montrer :
$v{=}1 \quad\Longrightarrow\quad b{=}d$
Ainsi, on a :
$$a^2 = b^3$$
$$\left(d{\cdot}u\right)^2 = b^3$$
$$\left(b{\cdot}u\right)^2 = b^3$$
$$b^2{\cdot}u^2 = b^3$$
$$u^2 = b$$
On vient de montrer que b est le carré d'un entier.
On en déduit :
$$a^2 = b^3$$
$$a^2 = \left(u^2\right)^3$$
$$a^2 = u^6$$
$$a^2 = \left(u^3\right)^2$$
$$a = u^3$$
On vient de montrer que a est le cube d'un entier.

• $\Longleftarrow$: supposons que a et b soient respectivement le cube et le carré d'un même entier ; ainsi, il existe un entier k tel que :
$a = k^3 \quad ; \quad b = k^2$
Ainsi, on a les valeurs suivantes :
$a^2 = \left(k^3\right)^2 = k^6 \quad ; \quad b^3 = \left(k^2\right)^3 = k^6$
On a l'égalité suivante :
$a^2 = b^3$

Exercice 4375

On considère l'équation :
(F) : $11{\cdot}x^2 - 7{\cdot}y^2 = 5$ où x et y sont des entiers relatifs.

1. a. Démontrer que si le couple $(x\,;y)$ est solution de (F), alors :
$x^2 \equiv 2{\cdot}y^2 \pmod 5$

b. Soient x et y des entiers relatifs. Recopier et compléter les deux tableaux suivants :

Modulo 5, x est congru à	0	1	2	3	4
Modulo 5, x^2 est congru à					

Modulo 5, y est congru à	0	1	2	3	4
Modulo 5, $2y^2$ est congru à					

Quelles sont les valeurs possibles du reste de la division euclidienne de x^2 et de $2{\cdot}y^2$ par 5 ?

c. En déduire que si le couple $(x\,;y)$ est solution de (F), alors x et y sont des multiples de 5.

2. Démontrer que si x et y sont des multiples de 5, alors le couple $(x\,;y)$ n'est pas solution de (F).
Que peut-on en déduire pour l'équation (F) ?

Correction 4375

1. a. L'équation (F) est définie par la relation :
$11x^2 - 7y^2 = 5$
Cette égalité donne l'équivalence :
$1{\times}x^2 - 2{\times}y^2 \equiv 0 \pmod 5$
$x^2 - 2{\cdot}y^2 \equiv 0 \pmod 5$
$x^2 \equiv 2{\cdot}y^2 \pmod 5$

b. Voici les deux tableaux complétés :

Modulo 5, x est congru à	0	1	2	3	4
Modulo 5, x^2 est congru à	0	1	4	4	1

Modulo 5, y est congru à	0	1	2	3	4
Modulo 5, $2y^2$ est congru à	0	2	3	3	2

c. Supposons que le couple $(x\,;y)$ d'entiers relatifs est solution de l'équation (F). Ainsi, la question a., les entiers x et y vérifient l'équivalence :
$x^2 \equiv 2y^2 \pmod 5$
Or, d'après la question b., on a :
- x^2 modulo 5 appartient à $\{0\,;1\,;4\}$
- $2y^2$ modulo 5 appartient à $\{0\,;2\,;3\}$

La seule possibilité d'égalité implique que :
$x^2 \equiv 0 \pmod 5 \quad ; \quad 2y^2 \equiv 0 \pmod 5$
C'est à dire
- 5 divise x^2 donc 5 divise le produit $x{\times}x$.
5 étant un nombre premier, d'après le corollaire du théorème de Gauss alors 5 divise x :
x est un multiple de 5.
- 5 divise $2y^2$, donc 5 le produit de 2 et de y^2. Or, les nombres 5 et 2 étant premiers entre eux.
D'après le théorème de Gauss, on en déduit que 5

divise y^2.
Par un raisonnement équivalent sur le produit y^2, on en déduit que 5 divise y :
y est un multiple de 5.

2. Effectuons un raisonnement par l'absurde :
Supposons que x et y sont des multiples de 5 et qu'ils soient solution de léquation (F).

Etant multiples de 5, on a l'existence d'entiers k et k' vérifiant :
$x = 5\cdot k \quad ; \quad y = 5\cdot k'$

Etant solution de l'équation (F), on a :

$$\begin{aligned} 11\cdot x^2 - 7\cdot y^2 &= 5 \\ 11\cdot(5\cdot k)^2 - 7\cdot(5\cdot k')^2 &= 5 \\ 11\times 5^2\cdot k^2 - 7\times 5^2\cdot k'^2 &= 5 \\ 5^2\cdot\left(11\cdot k - 7\cdot k'\right) &= 5 \\ 5\cdot\left(11\cdot k - 7\cdot k'\right) &= 1 \end{aligned}$$

L'égalité précédente montre que 5 est un diviseur de 1 ce qui est absurde.

Ainsi, un couple $(x\,;y)$ d'entiers solutions de (F) ne peuvent être des multiples de 5.

Or, la question 1. montre que s'il existe un couple $(x\,;y)$ solution de (F) alors les entiers x et y sont des multiples de 5.

Ainsi, il ne peut y avoir de couple $(x\,;y)$ solution de (F). On en déduit que l'équation (F) n'admet pas de solution dans $\mathbb{Z}$.

Exercice 6018

Soit a et b deux entiers naturels dont la somme et le produit ont pour PGCD le carré d'un nombre premier p.

1. Montrer que p^2 divise a^2.
(on pourra remarquer que a^2=$a\cdot(a+b)-ab$).
En déduire que p divise a. Montrer que p divise b.

2. Démontrer que le PGCD de a et b est, soit p, soit p^2.

Correction 6018

1. • Les conditions initiales de l'énoncé donne deux entiers a et b tels que :
$\text{pgcd}\left(a+b\,;a\cdot b\right) = p^2$
Ainsi, p^2 divise toute combinaison linéaire des entiers a+b et $a\cdot b$. En particulier, on a :

$$\begin{aligned} a\cdot\left(a+b\right) + (-1)\cdot\left(a\cdot b\right) &\equiv 0 \pmod{p^2} \\ a^2 + a\cdot b - a\cdot b &\equiv 0 \pmod{p^2} \\ a^2 &\equiv 0 \pmod{p^2} \end{aligned}$$

On vient de montrer que p^2 divise a^2.

• Ainsi, il existe un entier k tel que :
$k\cdot p^2 = a^2$
$\left(k\cdot p\right)\cdot p = a^2$
On vient de montrer que p divise $a\times a$.
De plus, p étant un nombre premier, on en déduit que p et a sont premiers entre eux.
D'après le théorème de Gauss, on en déduit que p divise a.

• De même, on montre l'égalité :
$b^2 = b\cdot(b+a) - b\cdot a$
En suivant le même raisonnement que précédemment *(car a et b jouent des rôles symétriques)*, on en déduit que :
b divise p.

2. Notons d le *PGCD* de a et de b.
• Il existe deux entiers k et k' tels que :
$a = k\cdot d \quad ; \quad b = k'\cdot d$
D'après l'énoncé :

$$\begin{aligned} p^2 &= \text{pgcd}\left(a+b\,;a\cdot b\right) = \text{pgcd}\left(k\cdot d + k'\cdot d\,;(k\cdot d)\cdot(k'\cdot d)\right) \\ &= \text{pgcd}\left(d\cdot k + k'\right)\,;(d\cdot(k\cdot k'\cdot d)\right) \\ &= d\cdot\text{pgcd}\left(k+k'\,;k\cdot k'\cdot d\right) \end{aligned}$$

On en déduit que d divise p^2. p étant un nombre premier, on en déduit que l'entier d vérifie l'une des trois égalités suivantes :
$d = 1 \quad ; \quad d = p \quad ; \quad d = p^2$

• A la question précédente, on vient de montrer que p est un diviseur de a et de b. Ainsi, il existe deux entiers naturels vérifiant les égalités :
$a = k\cdot p \quad ; \quad b = k'\cdot p$
On obtient la relation :
$d = \text{pgcd}\left(a\,;b\right) = \text{pgcd}\left(k\cdot p\,;k'\cdot p\right) = p\cdot\text{pgcd}\left(k\,;k'\right)$
On vient de montrer que p divise d : ainsi, d est un multiple de p.

On en déduit que d vaut p ou p^2.

Exercice 5829

On pose u=$2+\sqrt{3}$ et v=$2-\sqrt{3}$

1. Démontrer par récurrence que, n désignant un entier positif, on peut écrire :

$$u^n = a_n + b_n\cdot\sqrt{3} \quad ; \quad v^n = a_n - b_n\cdot\sqrt{3}$$

où a_n et b_n sont des entiers positifs.
Exprimer a_{n+1} et b_{n+1} en fonction de a_n et b_n.

2. Etablir les égalités :

$$a_n{}^2 - 3\cdot b_n{}^2 = 1 \quad ; \quad a_n\cdot b_{n+1} - a_{n+1}\cdot b_n = 1$$

En déduire que les fractions $\dfrac{a_n}{b_n}$, $\dfrac{a_{n+1}}{a_n}$, $\dfrac{b_{n+1}}{b_n}$ sont irréductibles.

Correction 5829

1. Pour tout entier n positif, considérons la propriété $\mathcal{P}_n$ définie par la relation :
$\mathcal{P}_n$: "Il existe a_n et b_n tel que $u^n = a_n + b_n\cdot\sqrt{3}$; $v^n = a_n - b_n\cdot\sqrt{3}$"

Démontrons, à l'aide d'un raisonnement par récurrence, que la propriété $\mathcal{P}_n$ est vraie pour tout entier naturel non-nul.

• **Initialisation :**
On a :
➪ $u^1 = 2 + \sqrt{3}$
On doit choisir a_1=2 et b_1=1

$v^1 = 2-\sqrt{3}$

On doit choisir a_1=2 et b_1=1

Ainsi, $\mathcal{P}_1$ est vraie.

- **Hérédité :**

Supposons que la propriété $\mathcal{P}_n$ soit vérifiée pour un entier naturel n non-nul quelconque. C'est à dire qu'on a l'hypothèse de récurrence suivante :

"Il existe a_n et b_n tel que :

$u^n = a_n + b_n\cdot\sqrt{3}$; $v^n = a_n - b_n\cdot\sqrt{3}$"

Etudions les puissances $(n+1)$ième de u et de v :

$u^{n+1} = u^n\cdot u = \left(a_n + b_n\cdot\sqrt{3}\right)\cdot\left(2+\sqrt{3}\right)$

$= 2\cdot a_n + \sqrt{3}\cdot a_n + 2\sqrt{3}\cdot b_n + \left(\sqrt{3}\right)^2\cdot b_n$

$= 2\cdot a_n + \sqrt{3}\cdot\left(a_n + 2b_n\right) + 3\cdot b_n$

$= \left(2\cdot a_n + 3\cdot b_n\right) + \sqrt{3}\cdot\left(a_n + b_n\right)$

$v^{n+1} = v^n\cdot v = \left(a_n - b_n\cdot\sqrt{3}\right)\left(2-\sqrt{3}\right)$

$= 2\cdot a_n - a_n\cdot\sqrt{3} - 2\sqrt{3}\cdot b_n + b_n\cdot\left(\sqrt{3}\right)^2$

$= 2\cdot a_n - \sqrt{3}\cdot\left(a_n + 2b_n\right) + 3\cdot b_n$

$= \left(2\cdot a_n + 3\cdot b_n\right) - \sqrt{3}\cdot\left(a_n + 2b_n\right)$

On vient donc d'établir l'existence des entiers a_{n+1} et b_{n+1} définie par :

$a_{n+1} = 2\cdot a_n + 3\cdot b_n$; $b_{n+1} = a_n + 2\cdot b_n$

vérifions les égalités :

$u^{n+1} = a_{n+1} + b_{n+1}\cdot\sqrt{3}$; $v^{n+1} = a_{n+1} - b_{n+1}\cdot\sqrt{3}$

On vient d'établir que la propriété $\mathcal{P}_{n+1}$ est vraie.

- **Conclusion :**

La propriété $\mathcal{P}_n$ est initialisée au rang 1 et elle vérifie par propriété d'hérédité. On en déduit, à l'aide d'un raisonnement par récurrence, que la propriété $\mathcal{P}_n$ est vraie pour tout entier naturel n non-nul.

2. On remarque que :

$u\cdot v = \left(2+\sqrt{3}\right)\left(2-\sqrt{3}\right) = 2^2 - \left(\sqrt{3}\right)^2 = 4-3 = 1$

Ainsi, pour tout entier naturel n non-nul, on a :

$u^n\cdot v^n = \left(u\cdot v\right)^n = 1^n = 1$

Ainsi, on a l'égalité :

$$u^n\cdot v_n = 1$$
$$\left(a_n + b_n\cdot\sqrt{3}\right)\left(a_n - b_n\cdot\sqrt{3}\right) = 1$$
$$\left(a_n\right)^2 - \left(b_n\cdot\sqrt{3}\right)^2 = 1$$
$${a_n}^2 - 3\cdot{b_n}^2 = 1$$

Etudions l'expression :

$a_n\cdot b_{n+1} - a_{n+1}\cdot b_n = a_n\cdot\left(a_n + 2\cdot b_n\right) - \left(2\cdot a_n + 3\cdot b_n\right)\cdot b_n$

$= {a_n}^2 + 2\cdot a_n\cdot b_n - 2\cdot a_n\cdot b_n - 3\cdot{b_n}^2 = {a_n}^2 - 3\cdot{b_n}^2 = 1$

Utilisons à chaque fois le théorème de Bezout :

- De l'égalité : $a_n\cdot a_n + (-3b_n)\cdot b_n = 1$

On en déduit que les entiers a_n et b_n sont premiers entre eux.

Le quotient $\dfrac{a_n}{b_n}$ est irréductible.

- De l'égalité : $b_{n+1}\cdot a_n + (-b_n)\cdot a_{n+1} = 1$

On en déduit que les entiers a_n et a_{n+1} sont premiers entre eux.

Le quotient $\dfrac{a_{n+1}}{a_n}$ est irréductible.

- De l'égalité : $a_n\cdot b_{n+1} + (-a_{n+1})\cdot b_n = 1$

On en déduit que les entiers b_n et b_{n+1} sont premiers entre eux.

Le quotient $\dfrac{b_{n+1}}{b_n}$ est irréductible.

Exercice 4376

On souhaite déterminer l'ensemble des couples $(a\,;b)$ d'entiers naturels solutions de l'équation :

$a^2 - 3\cdot a\cdot b + b^2 = 0$

On suppose l'existence d'un couple $(a\,;b)$ solution de cette équation :

1. Justifier l'existence d'entiers naturels a' et b' premiers entre eux vérifiant l'égalité :
$a'^2 - 3\cdot a'\cdot b' + b'^2 = 0$
2. Montrer que a' divise b'^2, puis que a' divise b'.
3. Etablir que b' vérifie la relation : $1-3b'+b'^2 = 0$.
4. Conclure.

Correction 4376

1. En notant d le $PGCD$ des nombres a et b, on a l'existence de deux nombres a' et b' premiers entre eux vérifiant :

$a = a'\cdot d$; $b = b'\cdot d$

Le couple $(a\,;b)$ vérifie l'égalité :

$$a^2 - 3\cdot a\cdot b + b^2 = 0$$
$$(a'\cdot d)^2 - 3\cdot(a'\cdot d)\cdot(b'\cdot d) + (b'\cdot d)^2 = 0$$
$$d^2\cdot a'^2 - d^2\cdot 3\cdot a'\cdot b' + d^2\cdot b'^2 = 0$$
$$d^2\cdot\left(a'^2 - 3\cdot a'\cdot b' + b'^2\right) = 0$$

Or, le $PGCD$ de deux nombres relatifs non-nuls est un entier non-nul, on en déduit :

$a'^2 - 3\cdot a'\cdot b' + b'^2 = 0$

où a' et b' sont premiers entre eux.

2. De l'égalité précédente, on a :

$a'^2 - 3\cdot a'\cdot b' + b'^2 = 0$

$$b'^2 = -a'^2 + 3\cdot a'\cdot b'$$
$$b'^2 = a'\cdot\left(-a' + 3\cdot b'\right)$$

L'égalité précédente montre que a' divise b'^2.

Ainsi, a' divise le produit de $b'\times b'$. Or, a' et b' *(considérons le premier facteur)* étant premier entre eux, d'après le théorème de Gauss, on en déduit que a' divise b' *(ce sera alors le second facteur).*

3. On vient de montrer que a' divise b', on en déduit :

$\text{pgcd}\left(a'\,;b'\right) = a'$.

Or, les nombres a' et b' sont premiers entre eux : $\text{pgcd}\left(a'\,;b'\right) = 1$.

On en déduit : a'=1

L'équation vérifiée par le couple $\left(a'\,;b'\right)$ devient :

$a'^2 - 3\cdot a'\cdot b' + b'^2 = 0$

$1^2 - 3\times 1\cdot b' + b'^2 = 0$

$1 - 3\cdot b' + b'^2 = 0$

4. Etudions le polynôme x^2-3x+1. Ce polynome du second degré admet pour discriminant :

$\Delta = b^2 - 4\cdot a\cdot c = (-3)^2 - 4\times 1\times 1 = 9-4 = 5$.

Le discriminant étant strictement positif, le polynôme admet les deux racines suivantes :

$$x_1 = \frac{-b-\sqrt{\Delta}}{2\cdot a} = \frac{-(-3)-\sqrt{5}}{2\times 1} = \frac{3-\sqrt{5}}{2} \qquad x_2 = \frac{-b+\sqrt{\Delta}}{2\cdot a} = \frac{-(-3)+\sqrt{5}}{2\times 1} = \frac{3+\sqrt{5}}{2}$$

Or, aucune de ces racines n'est entière : il n'existe pas de nombre entier b' vérifiant les conditions précédente.

On conclut que l'équation de départ :
$a^2 - 3\cdot a\cdot b + b^2 = 0$
n'admet aucun couple de solutions de nombres relatifs.

20. Manipulation algébrique :

Exercice 3807

Soit n un entier relatif. Indiquer si la proposition suivante est vraie ou fausse et donner une justification de la réponse choisie :

$n^2+n+3 \equiv 0 \pmod 5$ si, et seulement si, $n \equiv 1 \pmod 5$.

Correction 3807

Prenons $n = 3$, on a :

- $n^2+n+3 = 3^2+3+3 = 9+3+3 = 15 \equiv 0 \pmod 5$
- $n \not\equiv 1 \pmod 5$

Cet entier montre que la relation d'équivalence proposée est fausse.

21. Corollaire du théorème de Gauss :

Exercice 4359

On considère l'équation (E) sur les triplets $(x\,;y\,;z)$ définie par :

$$x^2+y^2 = \frac{5}{2}\cdot z^2$$

Considérons un triplet $(x\,;y\,;z)$ d'entiers relatifs vérifiant l'équation (E) :

1. Vérifier que le triplet $A\,(1\,;3\,;2)$ est solution de (E).
2. Démontrer que z est divisible par 2 et x^2+y^2 est divisible par 10.
3. Supposons que y=3, montrer alors l'équivalence suivante :
   $x^2 \equiv 1 \pmod{10}$
4. Déterminer un triplet $(x\,;y\,;z)$ à valeur entières solutions de (E) où y est un nombre impair.

Correction 4359

1. Vérifions que le triplet A vérifie cette équation :
   - $x^2+y^2 = 1^2+3^2 = 1+9 = 10$
   - $\frac{5}{2}\cdot z^2 = \frac{5}{2}\times 2^2 = \frac{5}{2}\times 4 = 10$

   Le triplet A vérifie l'équation (E).

2. - L'équation permet d'écrire :
   $$x^2+y^2 = \frac{5}{2}\cdot z^2$$
   $$2\cdot\left(x^2+y^2\right) = 5\cdot z^2$$
   De la dernière égalité, on déduit que 2 divise le produit $5\cdot z^2$. Les entiers 2 et 5 sont premiers entre eux, d'après le théorème de Gauss, on en déduit que le nombre 2 divise z^2.
   2 est un nombre premier et il divise le produit $z\times z$. D'après le corollaire du théorème de Gauss, on en déduit qu'il divise un des deux facteurs : 2 divise l'entier z.
   - L'entier z est donc un nombre pair. Il existe un entier relatif k tel que :
     $z = 2\cdot k$
     L'équation (E) permet d'écrire :
     $$x^2+y^2 = \frac{5}{2}\cdot z^2$$
     $$x^2+y^2 = \frac{5}{2}\cdot(2\cdot k)^2$$
     $$x^2+y^2 = \frac{5}{2}\times 4\cdot k^2$$
     $$x^2+y^2 = 10\cdot k^2$$
     On en déduit que la somme x^2+y^2 est divisible par 10.

3. Supposons que y=3 :
   $$x^2+y^2 \equiv 0 \pmod{10}$$
   $$x^2+3^2 \equiv 0 \pmod{10}$$
   $$x^2+9 \equiv 0 \pmod{10}$$
   $$x^2+10 \equiv 1 \pmod{10}$$
   $$x^2 \equiv 1 \pmod{10}$$

4. Le triplet $B(9\,;\,3\,;\,6)$ vérifie l'équation (E) :
   - $x^2+y^2 = 9^2+3^2 = 81+9 = 90$
   - $\frac{5}{2}\cdot 6^2 = \frac{5}{2}\times 36 = 90$

22. Raisonnement par récurrence :

Exercice 696

Soit p une entier naturel supérieur ou égal à 2 et a un entier naturel non-nul

Montrer que si il existe un entier naturel n tel que $a^n \equiv 0 \pmod{p}$ alors pour tout entier naturel k, on a l'implication : $k \geqslant n \implies a^k \equiv 0 \pmod{p}$

Correction 696

Supposons l'existence d'un entier n vérifiant la congruence :
$a^n \equiv 0 \pmod{p}$.

Considérons un entier naturel k supérieur ou égal à n.

On a les égalités et congruences suivantes :
$a^k = a^n \cdot a^{k-n}$
D'après les propriétés algébriques de la congruence :

$$\equiv 0 \times a^{k-n} \equiv 0 \pmod{p}$$

Exercice 5469

1. Déterminer le plus petit entier k réalisant l'équivalence :
$6^k \equiv 0 \pmod{4}$

2. Pour tout entier naturel a, à l'aide d'un raisonnement par récurrence, établir la congruence ci-dessous pour tout entier naturel n non-nul :
$(a+6)^n \equiv a^n + 6 \cdot n \cdot a^{n-1} \pmod{4}$

Correction 5469

1. On remarque les deux congruences suivantes :
$6^1 \equiv 2 \pmod{4}$; $6^2 = 36 = 9 \times 4 \equiv 0 \pmod{4}$

Le plus petit entier k recherché a pour valeur k=2.

2. On note $\mathcal{P}_n$ la propriété définie par :
$(a+6)^n \equiv a^n + 6 \cdot n \cdot a^{n-1} \pmod{4}$

Montrons, à l'aide d'un raisonnement par récurrence, que la propriété $\mathcal{P}_n$ est vraie pour tout entier naturel n non-nul :

- **Initialisation :**
Pour $n = 1$, on a :
$(a+6)^1 = a + 6 \equiv a + 6 \pmod{4}$
$a^1 + 6 \times 1 \times a^0 = a + 6 \equiv a + 6 \pmod{4}$
On vient d'établir l'égalité recherchée au rang 1.

- **Hérédité :**
On suppose que la propriété $\mathcal{P}_n$ est vraie pour un entier naturel n non-nul quelconque. C'est à dire qu'on a la congruence suivante :
$(a+6)^n \equiv a^n + 6 \cdot n \cdot a^{n-1} \pmod{4}$
On a les égalités et congruences suivantes :
$(a+6)^{n+1} = (a+6)^n \cdot (a+6)$
D'après la relation de récurrence, on a :

$$\equiv (a^n + 6 \cdot n \cdot a^{n-1})(a+6) \pmod{4}$$
$$\equiv a^{n+1} + 6 \cdot a^n + 6 \cdot n \cdot a^n + 6^2 \pmod{4}$$
$$\equiv a^{n+1} + 6 \cdot a^n \cdot (n+1) + 0 \pmod{4}$$
$$\equiv a^{n+1} + 6 \cdot a^n \cdot (n+1) \pmod{4}$$

On vient d'établir que la propriété $\mathcal{P}_{n+1}$ est vraie.

- **Conclusion :**
La propriété $\mathcal{P}_n$ est initialisée au rang 1 et elle vérifie la propriété d'hérédité. Le raisonnement par récurrence permet d'affirmer que la propriété $\mathcal{P}_n$ est vraie pour tout entier naturel n non-nul.

24. Equation diophantienne :

Exercice 4361

Déterminer l'ensemble des couples $(x\,;y)$, où x et y sont deux entiers relatifs, solutions de l'équation :
(E) : $2 \cdot x + 11 \cdot y = 7$

Correction 4361

Le couple $(-2\,;1)$ est solution de l'équation (E) :
$2 \cdot x + 11 \cdot y = 2 \times (-2) + 11 \times 1 = -4 + 11 = 7$

Considérons $(x\,;y)$ une solution de l'équation. Ce couple vérifie l'équation :
$2 \cdot x + 11 \cdot y = 7$

En utilisant les deux égalités précédentes :
$2 \cdot x + 11 \cdot y = 2 \times (-2) + 11 \times 1$
$2 \cdot x - 2 \times (-2) = 11 \times 1 - 11 \cdot y$
$2 \cdot (x+2) = 11 \cdot (1-y)$

On vient d'établir que 2 divise le produit $11 \cdot (1-y)$. Or, les deux nombres 2 et 11 sont premiers entre eux.
D'après le théorème de Gauss, on en déduit que 2 divise le facteur $1-y$.

Ainsi, il existe un entier k relatif tel que :

$1 - y = 2 \cdot k$
$-y = 2 \cdot k - 1$
$y = -2 \cdot k + 1$

Le couple $(x\,;y)$ étant une solution de l'équation. On a :
$2 \cdot x + 11 \cdot y = 7$
$2 \cdot x + 11 \cdot (-2 \cdot k + 1) = 7$
$2 \cdot x - 22 \cdot k + 11 = 7$
$2 \cdot x = 7 + 22 \cdot k - 11$
$2 \cdot x = 22 \cdot k - 4$
$x = \dfrac{22 \cdot k - 4}{2}$
$x = 11 \cdot k - 2$

On vient de montrer que tout couple solution de l'équation admet pour expression :
$(11 \cdot k - 2\,;\, -2 \cdot k + 1)$

Montrons que tout couple admettant cette expression est une solution de l'équation :
$2 \cdot x + 11 \cdot y = 2 \cdot (11 \cdot k - 2) + 11 \cdot (-2 \cdot k + 1)$
$= 22 \cdot k - 4 - 22 \cdot k + 11 = 7$

Ainsi, l'ensemble des solutions de cette équation est l'ensemble des couples :
$(11 \cdot k - 2\,;\, -2 \cdot k + 1)$ où $k \in \mathbb{Z}$

25. Equations :

Exercice 5058

1. Compléter le tableau de valeurs suivant :

n	0	1	2	3	4
Reste de 3^n par 5					

2. Justifier que pour tout entier naturel n, on a : $2008^{4\cdot n} \equiv 1 \pmod 5$

3. En déduire que $2008^{2008}-31$ est divisible par 5.

Correction 5058

1. Compléter le tableau de valeurs suivant :

n	0	1	2	3	4
3^n	1	3	9	27	81
Reste de 3^n par 5	1	3	4	2	1

2. La division euclidienne de 2008 par 5 donne l'égalité :
$2008 = 401\times 5 + 3$

Ainsi, on a les congruences suivantes :

$2008 \equiv 3 \pmod 5$

$2008^{4\cdot n} \equiv 3^{4\cdot n} \pmod 5$

$2008^{4\cdot n} \equiv \left(3^4\right)^n \pmod 5$

$2008^{4\cdot n} \equiv 1^n \pmod 5$

$2008^{4\cdot n} \equiv 1 \pmod 5$

3. On a les transformations suivantes :
$2008^{2008} - 31 = 2008^{4\times 502} - 31$
$= \left(2008^4\right)^{502} - 31$

On a les congruences :

$\equiv \left(3^4\right)^{502} - 31 \equiv 1^{502} - 31 \pmod 5$

$\equiv 1 - 1 \equiv 0 \pmod 5$

Le nombre 2008^{2008} est divisible par 5.

Exercice 3474

1. a. Déterminer les restes de la division euclidienne par 7 des nombres 3^n pour $n \in \mathbb{N}$, $n \leqslant 6$.
On complétera le tableau suivant :

Puissance de 3	3^0	3^1	3^2	3^3	3^4	3^5	3^6
Reste modulo 7							

b. En déduire que, pour tout $k\in\mathbb{N}$, 3^{6k} est congru à 1 modulo 7.

2. a. Déterminer le plus petit entier naturel congru à 1515 modulo 7.

b. Après avoir remarqué que $2004 = 6\times 334$, déduire de la question 1. le reste de la division euclidienne de 1515^{2004} par 7.

c. Montrer que dans la division euclidienne de 1515^{2006} par 7, le reste est 2.

Correction 3474

1. a. Voici le tableau donnant le reste de la division euclidienne des nombres 3^n, pour $n\in\mathbb{N}$ et $n\leqslant 6$:

n	0	1	2	3	4	5	6
3^n	1	3	9	27	81	243	729
$3^n \pmod 7$	1	3	2	6	4	5	1

b. $3^{6k} = \left(3^6\right)^k \equiv 1^k \equiv 1 \pmod 7$

3. a. La division euclidienne de 1515 par 7 donne :
$1515 = 216\times 7 + 3$
On en déduit que : $1515 \equiv 3 \pmod 7$

b. Calculons la classe d'équivalence de 1515^{2004} modulo 7 :

$1515^{2004} \equiv 3^{2004} \equiv 3^{6\times 334} \equiv \left(3^6\right)^{334} \pmod 7$

$\equiv 1^{334} \equiv 1 \pmod 7$

c. Les propriétés sur les puissances permettent d'écrire :
$1515^{2006} = 1515^{2004}\times 1515^2$
On en déduit les congruences :

$\equiv 1\times 3^2 \equiv 1\times 3^2 \pmod 7$

$\equiv 9 \equiv 2 \pmod 7$

Exercice 3555

1. On s'intéresse, pour tout entier naturel n, au reste de la division euclidienne de 2^n par 7.

a. compléter le tableau suivant :

n	0	1	2	3	4
Reste de la division de 2^n par 7					

b. On note r le reste de la division euclidienne de n par 3 ; justifier l'égalité suivante :
$2^n \equiv 2^r \pmod 7$

2. a. En déduire que pour tout entier naturel k, le nombre $\left(2^{3\cdot k}-1\right)$ est un multiple de 7.

b. Montrer que pour tout entier naturel k, le nombre $\left(2^{3\cdot k+1}-2\right)$ est un multiple de 7.

3. Déterminer le reste de la division euclidienne de $\left(17\,159\right)^{541}$ par 7.

Correction 3555

1. On a les calculs suivants :
- $2^0 = 1 \equiv 1 \pmod 7$
- $2^1 = 2 \equiv 2 \pmod 7$
- $2^2 = 4 \equiv 4 \pmod 7$
- $2^3 = 8 \equiv 1 \pmod 7$
- $2^4 = 16 \equiv 2 \pmod 7$

Ainsi, on a le tableau de résultats ci-dessous :

n	0	1	2	3	4
Reste de la division de 2^n par 7	1	2	4	1	2

2. a. Les propriétés sur les puissances permettent d'écrire
Pour tout entier naturel k :
$2^{3\cdot k}-1=\left(2^3\right)^k-1$

On en déduit les congruences :

$\equiv 1^k-1\equiv 1-1\equiv 0 \pmod 7$

Pour tout entier naturel k, $\left(2^{3\cdot k}-1\right)$ est un multiple de 7.

b. Pour tout entier naturel k, on a :
$2^{3\cdot k+1}-2=2^{3\cdot k}\times 2^1-2=\left(2^3\right)^k\times 2-2$

$\equiv 1^k\times 2-2\equiv 2-2\equiv 0 \pmod 7$

Pour tout entier naturel k, $\left(2^{3\cdot k+1}-2\right.$ est un multiple de 7.

3. La division euclidienne de 17 159 par 7 donne l'égalité :
$17\,159=2451\times 7+2$

La division euclidienne de 541 par 3 donne l'égalité :
$541=180\times 3+1$

Ainsi, on a les équivalences suivantes :
$\left(17\,159\right)^{541}\equiv 2^{541}\equiv 2^{180\times 3+1}\equiv 2^{180\times 3}\times 2^1 \pmod 7$

$\equiv \left(2^3\right)^{180}\times 2\equiv 1^{180}\times 2\equiv 2 \pmod 7$

Le reste de la division euclidienne de $\left(17\,159\right)^{541}$ par 7 est 2.

Exercice 3553

1. a. Déterminer le reste de la division euclidienne de 10^3 par 27.

b. En déduire le reste de la division euclidienne par 27 du nombre suivant :
$A=345\,948\,546\,421$

2. Déterminer le reste de la division euclidienne par 16 du nomre suivant :
$B=15\times 33^{51}-9\times 18^{152}+15^{37}$

Correction 3553

1. a. On a la division euclidienne suivante :
$10^3=37\times 27+1$
Ainsi, le reste de 10^3 par la division euclidienne par 27 a pour valeur 1.

b. On a :

$345\,948\,546\,421=345\times 10^{+}948\times 10^{+}546\times 10^{+}421$

$=345\times 10^9+948\times 10^6+546\times 10^3+421$

On a les classes d'équivalences suivantes :

$\equiv 345+948+546+421 \pmod{27}$

$\equiv 2260\equiv 83\times 27+19 \pmod{27}$

$\equiv 19 \pmod{27}$

2. On a les relations suivantes :

$15\times 33^{51}-9\times 18^{152}+15^{37}$

$=(16-1)\times(2\times 16+1)^{51}-9\times(16+2)^{152}+(16-1)^{37}$

$\equiv(-1)\times 1^{51}-9\times 2^{152}+(-1)^{37} \pmod{16}$

$\equiv -1-9\times 2^{4\times 38}-1\equiv -2-9\times\left(2^4\right)^{38} \pmod{16}$

$\equiv -2-9\times 16^{38}\equiv -2-9\times 0^{38} \pmod{16}$

$\equiv -2-0\equiv -2\equiv 14 \pmod{16}$

Exercice 4362

On considère l'entier N=11^{2011}. Montrer que l'entier N est congru à 4 modulo 7.

Correction 4362

Pour n un entier naturel non-nul, en notant r_n le reste de la division euclidienne de 11^n par 7, on obtient le tableau de congruence suivant :

n	1	2	3	4	5	6
r_n	4	2	1	4	2	1

On remarque du tableau l'équivalence suivante :
$11^3\equiv 1 \pmod{11}$

La division euclidienne de 2011 par 3 donne l'égalité :
$2011=670\times 3+1$

On a les transformations algébriques suivantes des puissances :
$11^{2011}=11^{670\times 3+1}=11^{670\times 3}\times 11^1=\left(11^3\right)^{670}\times 11^1$

On a la congruence suivante :

$\equiv 1^{670}\times 4\equiv 1\times 4\equiv 4 \pmod 7$

---

26. congruences :

Exercice 3212

Rappel :
Pour deux entiers relatifs a et b, on dit que a est congru à b modulo 7, et on écrit $a\equiv b \pmod 7$ lorsqu'il existe un entier relatif k tel que $a=b+7k$.

1. *Cette question constitue une restitution organisée de connaissances* :

a. Soient a, b, c et d des entiers relatifs.

Démontrer que :
Si $a\equiv b \pmod 7$ et $c\equiv d \pmod 7$
alors $ac\equiv bd \pmod 7$.

b. En déduire que : pour a et b entiers relatifs non nuls.
Si $a\equiv b \pmod 7$ alors pour tout entier naturel n, $a^n\equiv b^n \pmod 7$.

2. Pour $a=2$ puis pour $a=3$, déterminer un entier naturel n non nul tel que $a^n\equiv 1 \pmod 7$.

3. Soit a un entier naturel non divisible par 7.

a. Montrer que $a^6 \equiv 1 \pmod 7$.

b. On appelle *ordre* de $a \pmod 7$, et on désigne par k, le plus petit entier naturel non nul tel que $a^k \equiv 1 \pmod 7$. Montrer que le reste r de la division euclidienne de 6 par k vérifie $a^r \equiv 1 \pmod 7$.
En déduire que k divise 6.
Quelles sont les valeurs possibles de k ?

c. Donner l'ordre modulo 7 de tous les entiers a compris entre 2 et 6.

4. A tout entier naturel n, on associe le nombre :
$A_n = 2^n + 3^n + 4^n + 5^n + 6^n$.
Montrer que $A_{2006} \equiv 6 \pmod 7$

Correction 3212

1. a. Puisque $a \equiv b \pmod 7$, il existe $k \in \mathbb{Z}$ tel que :
$a = k\cdot 7 + b$
Puisque $c \equiv d \pmod 7$, il existe $k' \in \mathbb{Z}$ tel que :
$c = k'\cdot 7 + d$
Ainsi, on a l'égalité suivante :
$$\begin{aligned} a\cdot c &\quad \big(k\cdot 7 + b\big)\cdot\big(k'\cdot 7 + d\big) \\ &k\cdot k'\cdot 7^2 + k\cdot d\cdot 7 + b\cdot k'\cdot 7 + b\cdot d \\ &\Big(k\cdot k'\cdot 7 + k\cdot d + b\cdot k'\Big) + b\cdot d \end{aligned}$$
De l'égalité précédente, on en déduit :
$a\cdot c \equiv b\cdot d \pmod 7$

b. Soit a et b deux entiers relatifs non nuls tels que :
$a \equiv b \pmod 7$
Montrons par récurrence la propriété suivante :
Pour tout $n \in \mathbb{N}$, $a^n \equiv b^n \pmod 7$

- **Initialisation** :
Cette relation est vraie pour $n = 0$:
$a^0 = 1$ et $b^0 = 1 \Longrightarrow a^0 \equiv b^0 \pmod 7$
Remarquons que d'après les hypothèses sur a et b, cette relation est également vraie pour $n = 1$.

- **Hérédité** :
Supposons la relation vraie pour le rang n ; cela signifie qu'on a :
$a^n \equiv b^n \pmod 7 \Longrightarrow$ il existe $k \in \mathbb{N}$ tel que $a^n = k\cdot 7 + b^n$
D'après les hypothèses de départ, on a :
$a \equiv b \Longrightarrow$ il existe $k' \in \mathbb{N}$ tel que $a = k'\cdot 7 + b$
Etablissons cette relation pour $(n+1)$; on a les égalités suivantes :
$$\begin{aligned} a^{n+1} &= a\cdot a^n \\ &= \big(k'\cdot 7 + b\big)\cdot\big(k\cdot 7 + b^n\big) \\ &= k'\cdot k\cdot 7^2 + k'\cdot 7\cdot b^n + b\cdot k\cdot 7 + b\cdot k\cdot 7 + b^{n+1} \\ &= \Big(k'\cdot k\cdot 7 + k'\cdot b^n + b\cdot k + b\cdot k\Big) + b^{n+1} \end{aligned}$$
Cette dernière égalité permet d'obtenir l'équivalence suivante :
$a^{n+1} \equiv b^{n+1} \pmod 7$

- **Conclusion :**
Cette propriété s'initialise au rang 0 et vérifie la propriété d'hérédité. Cette propriété est vérifiée pour tout entier naturel n.

2. - $a = 2$:
Notons r_n le reste de la division euclidienne de a^n par 7 ; on a le tableau suivant :

n	1	2	3	4	5	6
r_n	2	4	1	2	4	1

On en d'eduit que pour $n = 3$, on a :
$a^n \equiv 1 \pmod 7$

- $a = 3$:
Notons r'_n le reste de la division euclidienne de a^n par 7 ; on a le tableau suivant :

n	1	2	3	4	5	6
r'_n	3	2	6	4	5	1

On en d'eduit que pour $n = 6$, on a :
$a^n \equiv 1 \pmod 7$

3. a. On a le tableau suivant :

a	1	2	3	4	5	6
a^6	1	64	729	4 096	15 625	46 656
Division de a^6 par 7	$\underset{0\times 7+1}{\underline{1}}$	$\underset{9\times 7+1}{\underline{64}}$	$\underset{104\times 7+1}{\underline{729}}$	$\underset{585\times 7+1}{\underline{4\,096}}$	$\underset{2232\times 7+1}{\underline{15\,625}}$	$\underset{6665\times 7+1}{\underline{46\,656}}$

D'après le tableau précédent, on montre que pour tout entier naturel a non-divisible par 7, on a :
$a^6 \equiv 1 \pmod 7$

b. Soit k l'ordre de a ; la division euclidienne de 6 par k donne l'existence du couple $(q\,;r)$ tel que :
$6 = k\cdot q + r$ où $0 \leqslant r < k$

On remarque :
$a^6 = a^{k\cdot q + r}$
$a^6 = a^{k\cdot q}\cdot a^r$
$a^6 = \big(a^k\big)^q\cdot a^r$

Cette égalité modulo 7 devient :
$1 \equiv 1^q\cdot a^r \pmod 7$
$1 \equiv 1\cdot a^r \pmod 7$
$1 \equiv a^r \pmod 7$
r étant le reste d'une division euclidienne par k, on a :
$0 \leqslant r < k$
Or, par définition, k est le plus petit entier **non nul** réalisant $a^k \equiv 1 \pmod 7$; on en déduit que r est nul.
On en déduit que k divise 6.

L'ordre d'un entier naturel non divisible par 7 est un diviseur de 6 dont cet ordre a pour valeur :
1 ; 2 ; 3 ; 6

c.

a	2	3	4	5	6
a^2	4	9	16	25	36
Reste a^2	4	2	2	4	1
a^3	8	27	64	124	216
Reste a^3	1	6	1	6	6
a^6	64	729	4096	15625	46656
Reste a^6	1	1	1	1	1
Ordre de a	3	6	3	6	2

4. On a les divisions euclidiennes suivantes du nombre 2006 :

- par 2 : $2006 = 1003\times 2$
- par 3 : $2006 = 668\times 3 + 2$
- par 6 : $2006 = 334\times 6 + 2$

A l'aide de la question 3. c., on utilise la transformation :

$$\begin{aligned}A_{2006} &= 2^{2006} + 3^{2006} + 4^{2006} + 5^{2006} + 6^{2006}\\ &= 2^{668\times 3+2} + 3^{334\times 6+2} + 4^{668\times 3+2} + 5^{334\times 6+2} + 6^{1003\times 2}\\ &= 2^{668\times 3}\cdot 2^2 + 3^{334\times 6}\cdot 3^2 + 4^{668\times 3}\cdot 4^2 + 5^{334\times 6}\cdot 5^2 + \left(6^2\right)^{1003}\\ &= \left(2^3\right)^{668}\cdot 4 + \left(3^6\right)^{334}\cdot 9 + \left(4^3\right)^{668}\cdot 16 + \left(5^3\right)^{334}\cdot 25 + \left(6^2\right)^{1003}\end{aligned}$$

Cette égalité modulo 7 devient :

$$\begin{aligned}&\equiv 1^{668}\cdot 4 + 1^{334}\cdot 9 + 1^{668}\cdot 16 + 1^{334}\cdot 25 + 1 \pmod 7\\ &\equiv 4 + 9 + 16 + 25 + 1 \pmod 7\\ &\equiv 55 \pmod 7\\ &\equiv 7\times 7 + 6 \equiv 6 \pmod 7\end{aligned}$$

Exercice 3255

Etant donné un entier naturel $n \geqslant 2$, on se propose d'étudier l'existence de trois entiers naturels x, y et z tels que :

$$x^2 + y^2 + z^2 \equiv 2^n - 1 \pmod{2^n}$$

Partie A : Etude de deux cas particuliers

1. Dans cette question, on suppose que $n = 2$. Montrer que 1, 3 et 5 satisfont à la question précédente.

2. Dans cette question, on suppose $n = 3$.

   a. Soit m un entier naturel. Reproduire et compléter le tableau ci-dessous donnant le reste r de la division euclidienne de m par 8 et le reste R de la division euclidienne de m^2 par 8.

r	0	1	2	3	4	5	6	7
R								

   b. Peut-on trouver trois entiers naturels x, y et z tels que :
   $x^2 + y^2 + z^2 \equiv 7 \pmod 8$?

Partie B : Etude du cas général où $n \geqslant 3$

Supposons qu'il existe trois entiers naturels x, y et z tels que :

$$x^2 + y^2 + z^2 \equiv 2^n - 1 \pmod{2^n}$$

1. Justifier le fait que les trois entiers naturels x, y et z sont tous impairs ou que deux d'entre eux sont pairs.

2. On suppose que x et y sont pairs et que z est impair. On pose alors :
   $x = 2q \quad ; \quad y = 2r \quad ; \quad z = 2s + 1$
   où q, r, s sont des entiers naturels.

   a. Montrer que $x^2 + y^2 + z^2 \equiv 1 \pmod 4$.

   b. En déduire une contradiction.

3. On suppose que x, y, z sont impairs.

   a. Prouver que, pour tout entier naturel k non nul, $k^2 + k$ est divisible par 2.

   b. En déduire que $x^2 + y^2 + z^2 \equiv 3 \pmod 8$.

   c. Conclure.

Correction 3255

Partie A

1. Supposons que $n = 2$, on a :
   $2^n - 1 = 4 - 1 = 3 \equiv 3 \pmod 4$
   Considérons le triplet $(1\,;\,3\,;\,5)$, on a :

$$\begin{aligned}x^2 + y^2 + z^2 &= 1^2 + 3^2 + 5^2 = 1 + 9 + 25\\ &= 35 = 8\times 4 + 3\\ &= 3 \pmod 4\end{aligned}$$

   Ainsi, on vient de montrer l'égalité suivante pour $n = 2$ et le triplet $(1\,;\,3\,;\,5)$

2. a. On a le tableau suivant :

r	0	1	2	3	4	5	6	7
R	0	1	4	1	0	1	4	1

   b. Il n'est pas possible avec trois nombres parmi 0, 1 et 4 d'obtenir une somme congru à 7 modulo 8.
   Ainsi, l'égalité $x^2 + y^2 + z^2 \equiv 7 \pmod 8$ ne peut être réalisée.

Partie B

1. Il est clair que pour tout entier n, le nombre 2^n est un nombre pair ; on en déduit que le nombre $2^n - 1$ est un nombre impair.

   Or, pour que la somme des trois nombres x^2, y^2, z^2 soit impaire, il est nécessaire que :
   - ces trois nombres soit impair ;
   - ou un nombre est impair et les deux autres sont pairs.

   Or :
   - le carré d'un nombre pair si, et seulement si, le nombre est pair ;
   - le carré d'un nombre est impair si, et seulement si, le nombre est impair.

   On en déduit que sur les trois nombres x, y et z, on a :
   - soit deux nombres sont pairs et le troisième est impair ;
   - soit les trois nombres sont impairs.

2. a. On a :

$$\begin{aligned}x^2 + y^2 + z^2 &= (2q)^2 + (2r)^2 + (2s+1)^2\\ &= 4q^2 + 4r^2 + 4s^2 + 4s + 1\\ &= 4q^2 + 4r^2 + 4s^2 + 4s + 1\\ &= 4\cdot\left(q^2 + r^2 + s^2 + s\right) + 1\\ &\equiv 1 \pmod 4\end{aligned}$$

   b. Dans les hypothèses de la question 2., les entiers x, y et z vérifient la relation :
   $x^2 + y^2 + z^2 \equiv 2^n - 1 \pmod{2^n}$
   Ainsi, il existe $k \in \mathbb{Z}$ tel que :

$$x^2+y^2+z^2 = k\cdot 2^n + 2^n - 1$$
$$= (k+1)\cdot 2^n - 1$$

Or, $n \geqslant 3$, on a :

$$= (k+1)\cdot 2^2 \cdot 2^{n-2} - 1$$
$$= 4\cdot(k+1)\cdot 2^{n-2} - 1$$
$$\equiv -1 \pmod 4$$

Ce qui est en contradiction avec le résultat de la question a. : on en déduit qu'il ne peut exister de triplet $(x\,;y\,;z)$ vérifiant les deux conditions simultanemment.

3. a. Etablissons ce résultat par disjonction de cas :

- Si k est un nombre pair, on a l'existence de $m \in \mathbb{Z}$ vérifiant :
  $k = 2\cdot m$
  Ainsi, on peut écrire :
  $$k^2+k = (2\cdot m)^2 + 2\cdot m$$
  $$= 4\cdot m^2 + 2\cdot m$$
  $$= 2\cdot\left(2\cdot m^2 + m\right)$$
  On remarque que k^2+k est un nombre pair, il est donc divisible par 2.
- Supposons le nombre k impair, on a l'existence d'un nombre $\mathbb{Z}$ vérifiant :
  $k = 2\cdot m + 1$
  Ainsi, on peut écrire :
  $$k^2+k = (2\cdot m+1)^2 + (2\cdot m+1)$$
  $$= 4\cdot m^2 + 2\cdot m + 1 + 2\cdot m + 1$$
  $$= 4\cdot m^2 + 4\cdot m + 2$$
  $$= 2\cdot(2\cdot m^2 + 2\cdot m + 1)$$
  Le nombre k^2+k est un nombre pair, il est divisible par 2.

b. Les nombres x, y et z étant impair, on en déduit l'existence de trois entiers relatifs k, k' et k'' tels que :
$x = 2\cdot k+1 \quad ; \quad y = 2\cdot k'+1 \quad ; \quad z = 2\cdot k''+1$
Ainsi, on a :
$$x^2+y^2+z^2 = (2\cdot k+1)^2 + (2\cdot k+1)^2 + (2\cdot k+1)^2$$
$$= 4\cdot k^2+4\cdot k+1+4\cdot k'^2+4\cdot k'+1+4\cdot k''^2+4\cdot k''+1$$
$$= 4\cdot\left(k^2+k+k'^2+k'+k''^2+k''\right)+3$$

Or, on a vu à la question a., que pour tout entier naturel k, k^2+k est divisible par 2. Relativement à cette question, il existe trois entiers s, s', s'' tels que :
$k^2+k = 2\cdot s \quad ; \quad k'^2+k' = 2\cdot s' \quad ; \quad k''^2+k'' = 2\cdot s''$
On a :
$$x^2+y^2+z^2$$
$$= 4\cdot\left[(k^2+k)+(k'^2+k')+(k''^2+k'')\right]+3$$
$$= 4\cdot\left[(2\cdot s)+(2\cdot s')+(2\cdot s'')\right]+3$$
$$= 8\cdot\left[s+s'+s''\right]+3$$
On en déduit :
$$\equiv 3 \pmod 8$$

c. Le triplet $(x\,;y\,;z)$ sont solutions de l'équation :
$x^2+y^2+z^2 \equiv 2^n - 1 \pmod{2^n}$
Or, on a supposé $n \geqslant 3$, ainsi, on a :
$$2^n - 1 = 2^3\cdot 2^{n-3} - 1$$
$$= 8\cdot 2^{n-3} - 1$$
$$= \equiv -1 \pmod 8$$
$$= \equiv 7 \pmod 8$$
Ainsi, on aboutit à une contradiction et on en déduit qu'il ne peut exister de triplet $(x\,;y\,;z)$ solution de cette équation.

Exercice 3308

Partie A

Soit N un entier naturel, impair non premier.
On suppose que $N = a^2 - b^2$ où a et b sont deux entiers naturels.

1. Montrer que a et b n'ont pas la même parité.
2. Montrer que N peut s'écrire comme produit de deux entiers naturels p et q.
3. Quelle est la parité de p et de q ?

Partie B

On admet que 250 507 n'est pas premier.
On se propose de chercher des couples d'entiers naturels $(a\,;b)$ vérifiant la relation :

$$(E) : \; a^2 - 250\,507 = b^2$$

1. Soit X un entier naturel.
   a. Donner dans un tableau, les restes possibles de X modulo 9 ; puis ceux de X^2 modulo 9.
   b. Sachant que $a^2 - 250\,507 = b^2$, déterminer les restes possibles modulo 9 de $a^2 - 250\,507$; en déduire les restes possibles modulo 9 de a^2.
   c. Montrer que les restes possibles modulo 9 de a sont 1 et 8.
2. Justifier que si le couple $(a\,;b)$ vérifie la relation (E), alors $a \geqslant 501$. Montrer qu'il n'existe pas de solution du type $(501\,;b)$.
3. On suppose que le couple $(a\,;b)$ vérifie la relation (E).
   a. Démontrer que a est congru à 503 ou à 505 modulo 9.
   b. Déterminer le plus petit entier naturel k tel que le couple $(505+9k\,;b)$ soit solution de (E), puis donner le couple solution correspodant.

Partie C

1. Déduire des parties précédentes une écriture de 250 507 en un produit deux facteurs.
2. Les deux facteurs sont-ils premiers entre eux ?
3. Cette écriture est-elle unique ?

Correction 3308

Partie A

1. L'entier N est impair et non premier.
   - Effectuons un raisonnement par l'absurde ; supposons que les deux entier s a et b sont pairs ; il existe k et k' tels que :
     $a = 2\cdot k \quad ; \quad b = 2\cdot k'$
     Ainsi, on a :

$$a^2-b^2=\left(2\cdot k\right)^2-\left(2\cdot k'\right)^2$$
$$=4\cdot k^2-4\cdot k'^2$$
$$=2\cdot\left(2\cdot k^2-2\cdot k'^2\right)$$

On obtient ainsi que le nombre N est pair ce qui contredit l'hypothèse de départ : les entiers a et b ne peuvent pas être tous les deux pairs.

- Effectuons un raisonnement par l'absurde ; supposons que les deux entier s a et b sont impairs ; il existe k et k' tels que :

$a=2\cdot k+1\quad ;\quad b=2\cdot k'+1$

Ainsi, on a :

$$a^2-b^2=\left(2\cdot k+1\right)^2-\left(2\cdot k'+1\right)^2$$
$$=4\cdot k^2\cdot k+1-\left(4\cdot k'^2+2\cdot k'+1\right)$$
$$=2\cdot\left(2\cdot k^2+k-2\cdot k'^2-k'\right)$$

On obtient ainsi que le nombre N est pair ce qui contredit l'hypothèse de départ : les entiers a et b ne peuvent pas être tous les deux impairs.

On en déduit que les deux entiers a et b ne peuvent pas être de même parité

2. On a la factorisation :

$N=a^2-b^2=\left(a+b\right)\cdot\left(a-b\right)$

Ainsi, on vient de montrer que le nombre N peut s'écrire comme le produit de deux nombres entiers.

3. Le nombre N est impair et N est le produit de deux entiers p et q ; or, le produit de deux entiers est impair si, et seulement si, les deux entiers sont impairs.

Partie B

1. a. Voici le tableau représentant les valeurs possibles de X modulo 9 et ceux de X^2 :

X	0	1	2	3	4	5	6	7	8
X^2	0	1	4	0	7	7	0	4	1

b. D'après l'égalité $a^2-250\,507=b^2$, on en déduit que $a^2-250\,507$ est le carré d'un nombre. D'après la question précédente, le reste d'un carrée par la division euclidienne par 9 a une des valeurs suivantes :

$0\quad ;\quad 1\quad ;\quad 4\quad ;\quad 7$

Voici la division euclidienne de 250 507 :

$250\,507=27\,834\times 9+1$

Voici un tableau présentant les restes de $a^2-250\,507$ et de a^2 :

$a^2-250\,507$	0	1	4	7
a^2	1	2	5	8

Or, la question a. nous assure que les restes possibles du carré d'un nombre sont 0, 1, 4, 7 ; ainsi, avec le résultat précédent, on en déduit que le reste de a^2 par la division euclidienne par 9 a pour valeur 1

c. On vient de voir que le a^2 est égal à 1 modulo 9 ; le tableau obtenu à la question a. permet de dire que le nombre a a pour reste 1 et 8.

2. Si $\left(a\,;b\right)$ vérifie la relation (E) alors :

$a^2-250\,507=b^2$

Or, b^2 étant positif, on en déduit que :

$$a^2-250\,507\geqslant 0$$
$$a^2\geqslant 250\,507$$
$$a\geqslant\sqrt{250\,507}$$
$$a\geqslant 501$$

Supposons que $a=501$, alors on a :

$$b^2=a^2-250\,507$$
$$=501^2-250\,507$$
$$=251\,001-250\,507$$
$$=494$$

Or, 494 n'est pas un carré parfait ce qui entraîne l'impossibilité que $a=501$.

3. a. On a vu à la question 1. c. que a est égal à 1 ou 8 modulo 9 ; or, on remarque que 503 et 505 ont pour reste respectif 8 et 1 modulo 9.

Ainsi, a est congru à 503 ou 505 modulo 9.

b. Recherchons les valeurs de k pour lesquelles $a^2-250\,507$ soit le carré d'un entier :

k	0	1	2	3	4	5	6
b	×	117	×	×	×	×	×

Ainsi, le couple $\left(514\,;117\right)$ est solution de la relation (E).

Partie C

1. On a vu à la question 3. b. de la partie **B** que le couple $\left(514\,;117\right)$ est solution de (E) ; ainsi, on peut écrire :

$$514^2-250\,507=117^2$$
$$514^2-117^2=250\,507$$
$$250\,507=\left(514+117\right)\cdot\left(514-117\right)$$
$$250\,507=631\cdot 397$$

2. On a les deux valeurs approchées suivantes :

$\sqrt{631}\simeq 25{,}12\quad ;\quad \sqrt{397}\simeq 19{,}92$

La recherche de diviseurs premiers des nombres 631 et 397 respectivement sur les intervalles $\left[2\,;25\right]$ et $\left[2\,;19\right]$ montrent que ces deux nombres sont premiers.

3. Cette écriture est unique car une autre écriture sous la forme d'un produit de deux nombres *(distincts de 1)* contredirait qu'au moins un des facteurs dans le produit ci-dessous est des nombres premiers :

$250\,507=631\times 397$

Exercice 3387

1. a. Déterminer suivant les valeurs de l'entier naturel non nul n le reste dans la division euclidienne par 9 de 7^n.

b. Démontrer alors que $\left(2005\right)^{2005}\equiv 7\pmod 9$.

2. a. Démontrer que pour tout entier naturel non nul n : $\left(10\right)^n\equiv 1\pmod 9$.

b. On désigne par N un entier naturel écrit en base dix, on appelle S la somme de ses chiffres. Démontrer la relation suivante :

$N\equiv S\pmod 9$.

c. En déduire que N est divisible par 9 si, et seulement si, S est divisible par 9.

3. On suppose que $A=\left(2005\right)^{2005}$; on désigne par :

- B la somme des chiffres de A ;
- C la somme des chiffres de B ;
- D la somme des chiffres de C.

a. Démontrer la relation suivante : $A \equiv D \pmod 9$.

b. Sachant que $2005 < 10000$, démontrer que A s'écrit en numération décimale avec au plus 8020 chiffres. En déduire que $B \leqslant 72180$.

c. Démontrer que $C \leqslant 45$.

d. En étudiant la liste des entiers inférieurs à 45, déterminer un majorant de D plus petit que 15.

e. Démontrer que $D = 7$.

Correction 3387

1. a. Voici un tableau indiquant le reste de la division euclidienne de 7^n par 9 :

n	01	2	3	4	5	6
$7^n \equiv \ldots \pmod 9$	1	7	4	1	7	4

Le tableau précédent nous emmène à remarquer que :
$7^3 = 343 = 38\times 9 + 1 \equiv 1 \pmod 9$
Ainsi, pour tout entier naturel n, par la division euclidienne de n par 3, il existe un entier naturel k tel que :
$n = 3\cdot k + r$
Ainsi, on a les équivalences suivantes :
$7^n = 7^{3k+r} = 7^{3k}\cdot 7^r = \left(7^3\right)^k \cdot 7^r$
$\equiv 1^k \cdot 7^r \equiv 1\cdot 7^r \equiv 7^r \pmod 9$
Ainsi, suivant le reste r de la division euclidienne de n par 3, on a :

r	01	2	3
$7^n \equiv \ldots \pmod 9$	1	7	4

b. La division euclidienne de 2 005 par 9 donne la relation :
$2\,005 = 222\times 9 + 7$
La division euclidienne de 2 005 par 3 donne :
$2\,005 = 668\times 3 + 1$
Ainsi, on a les équivalences suivantes :
$\left(2\,005\right)^{2\,005} = \left(222\times 9 + 7\right)^{668\times 3+1}$
$\equiv \left(222\times 0 + 7\right)^{668\times 3+1} \pmod 9$
$\equiv 7^{668\times 3+1} \equiv \left(7^3\right)^{668}\times 7^1 \pmod 9$
D'après la question précédente :
$\equiv 7 \pmod 9$

2. a. Démontrons la relation suivante par récurrence :
$\left(10\right)^n \equiv 1 \pmod 9$
- Initialisation :
Pour $n = 0$, on a :
$10^0 = 1 \equiv 1 \pmod 9$.
La relation est vraie au rang 1.
- Hérédité :
Supposons la relation vraie au rang n ; étudions le nombre 10^{n+1} :
$10^{n+1} = 10\cdot 10^n$
$\equiv 10\cdot 1 \equiv 10 \equiv 1 + 9 \equiv 1 \pmod 9$
La propriété est donc vraie pour tout entier naturel n.

b. Soit N un entier naturel ; afin d'écrire ce nombre en base dix, on a l'existence de $m \in \mathbb{N}$ et de $a_1, a_2, \ldots, a_m$ des chiffres de la base dix *(des entiers compris entre 0 et 9)* afin d'avoir l'écriture :
$N = a_m\cdot 10^m + a_{m-1}\cdot 10^{m-1} + \cdots + a_1\cdot 10 + a_0$
D'après la question précédente, on a :
$\equiv a_m\cdot 1 + a_{m-1}\cdot 1 + \cdots + a_1 + a_0 \pmod 9$
On vient donc de montrer que la N est congru à la somme de ses chiffres *(en base dix)* modulo 9.

c. - $\Longrightarrow$:
Supposons que le nombre N soit divisible par 9, alors on a :
$N \equiv 0 \pmod 9$
Or, d'après la question précédente : $N \equiv S \pmod 9$, on en déduit que le nombre S vérifie :
$S \equiv 0 \pmod 9$
S est également divisible par 9.
- $\Longleftarrow$:
De même, si S est divisible par 9 alors $S \equiv 0 \pmod 9$.
De l'égalité de la question b., on en déduit que $N \equiv 0 \pmod 9$
Ainsi, le nombre N est divisible par 9.

3. a. D'après la question 2. b. et du fait que la somme des chiffres du nombres A vaut B, on a :
$A \equiv B \pmod 9$
D'après la question 2. b. et du fait que la somme des chiffres du nombres B vaut C, on a :
$B \equiv C \pmod 9$
D'après la question 2. b. et du fait que la somme des chiffres du nombres C vaut D, on a :
$C \equiv D \pmod 9$
Par transitivité de la congruence d'un nombre pour un même modulo, on a :
$A \equiv D \pmod 9$

b. On a :
$2\,005 < 10\,000$
$2\,005 < 10^4$
$2\,005^{2\,005} < \left(10^4\right)^{2\,005}$
$2\,005^{2\,005} < 10^{4\cdot 2\,005}$
$2\,005^{2\,005} < 10^{8\,020}$
Or, le nombre $10^{8\,020}$ s'écrit avec exactement 8 021 chiffres ; le nombre $2\,005^{2\,005}$ lui étant strictement inférieure, ce nombre s'écrit avec au plus 8 020 chiffres.
Supposons que chacun des chiffres de A soit 9, on en déduit que la somme de ses chiffres vaut :
$8\,020\times 9 = 72\,180$
Ainsi, la valeur de B est inférieur ou égale à cette valeur :
$B \leqslant 72\,180$

c. Ainsi, le nombre B comprend au maximum 5 chiffres et chacun de ces chiffres peuvent avoir pour plus grande valeur 9 ; ainsi, en suppososant que tous ses chiffres valent 9, la somme des chiffres du nombre B ne peut dépasser la valeur :
$9\times 5 = 45$
On en déduit que $C \leqslant 45$

d. - Sur l'intervalle $\left[40\,;\,45\right]$, l'entier ayant la plus grande somme de ses chiffres est 45 et cette somme vaut 9
- Sur l'intervalle $\left[0\,;\,39\right]$, la plus grande somme de chiffre est obtenu avec 39 et cette somme vaut 12

Ainsi, on en déduit que 12 est un majorant de D.

e. Or, on a montré que à la question 1. b. , on a :
$2\,005^{2\,005} \equiv 7 \pmod 9$

Par rapport, à la question 3. a. , on en déduit que :
$D \equiv 2\,005^{2\,005} \equiv 7 \pmod 9$

A la question d. , on vient de montrer que le nombre D appartient à l'intervalle $[0\,;\,12]$.
Ainsi le seul entier vérifiant les deux conditions est :
$D = 7$.

Exercice 3623

1. Démontrer que, pour tout entier naturel n, $2^{3n}-1$ est un multiple de 7 *(on pourra utiliser un raisonnement par récurrence)*.
En déduire $2^{3n+1}-2$ est un multiple de 7 et que $2^{3n+2}-4$ est un multiple de 7.

2. Déterminer les restes de la division par 7 des puissances de 2.

3. Le nombre p étant un entier naturel, on considère le nombre entier :
$A_p = 2^p + 2^{2p} + 2^{3p}$

a. Si p=$3n$, quel est le reste de la division de A_p par 7 ?

b. Démontrer que si p=$3n$+1 alors A_p est divisible par 7.

c. Etudier le cas où p=$3n$+2.

Correction 3623

1. Considérons la propriété $\mathcal{P}_n$ définie pour tout entier naturel n par :
$\mathcal{P}_n$: "$2^{3n}-1$ est un multiple de 7"

Montrons, à l'aide d'un raisonnement par récurrence, que la propriété $\mathcal{P}_n$ est vraie pour tout entier naturel n :

- **Initialisation :**
Pour $n=0$, on a :
$2^{3\times 0}-1 = 2^0-1 = 1-1 = 0$
Ainsi, $2^{3\times 0}-1$ est un multiple de 7.
$\mathcal{P}_0$ est vraie.

- **Hérédité :**
Supposons que la propriété $\mathcal{P}_n$ est vraie un entier naturel n quelconque. On a l'hypothèse de récurrence suivante :
$2^{3n}-1$ est un multiple de 7 $\implies$ $2^{3n}-1 \equiv 0 \pmod 7$
On a :
$2^{3\cdot(n+1)}-1 = 2^{3\cdot n+3}-1 = 2^{3\cdot n}\times 2^3 - 1$
$= 2^{3\cdot n}\times 8 - 1$
Etudions la congruence modulo 7 :
$\equiv 2^{3\cdot n}\times 1 - 1 \pmod 7 \equiv 2^{3\cdot n}-1 \pmod 7$
D'après l'hypothèse par récurrence :
$\equiv 1-1 \equiv 0 \pmod 7$
On vient de montrer que la relation $\mathcal{P}_{n+1}$ est vérifiée.

- **Conclusion :**
La propriété $\mathcal{P}_n$ est initialisée au rang 0 et elle vérifie la propriété d'hérédité. A l'aide d'un raisonnement par récurrence, on vient d'établir que la propriété $\mathcal{P}_n$ est vraie pour tout entier naturel n.

Etudions les deux entiers demandés :
- $2^{3n+1}-2 = 2\times 2^{3n}-2 = 2\cdot\left(2^{3n}-1\right)$
En utilisant la relation précédente, on a :
$\equiv 2\times 0 \equiv 0 \pmod 7$
Ainsi, pour tout entier naturel n, $2^{3n+1}-2$ est un multiple de 7.

- $2^{3n+2}-4 = 2^2\times 2^{3n}-2^2 = 2^2\cdot\left(2^{3n}-1\right)$
En utilisant la relation précédente, on a :
$\equiv 4\times 0 \equiv 0 \pmod 7$
Ainsi, pour tout entier naturel n, $2^{3n+2}-4$ est un multiple de 7.

2. Soit n un entier naturel. La division euclidienne de n par 3, nous donne l'existence du couple $(q\,;r)$ d'entiers tel que :
$n = 3\cdot q + r$ où $0 \leqslant r < 3$

Ainsi, trois cas se présentent à nous :
- r=0 :
$2^n = \left(2^{3\cdot q}-1\right)+1$
D'après la question précédente, on a :
$\equiv 0+1 \equiv 1 \pmod 7$
- r=1 :
$2^n = \left(2^{3\cdot q+1}-2\right)+2$
D'après la question précédente, on a :
$\equiv 0+2 \equiv 2 \pmod 7$
- r=2 :
$2^n = \left(2^{3\cdot q+2}-4\right)+4$
D'après la question précédente, on a :
$\equiv 0+4 \equiv 4 \pmod 7$

3. a. Si p est un multiple de 3, alors il existe un entier naturel n tel que $p = 3\cdot n$
Ainsi, on a :
$A_p = 2^p + 2^{2p} + 2^{3p} = 2^{3n} + 2^{2\cdot(3n)} + 2^{3\cdot(3n)}$
$= 2^{3n} + \left(2^{3n}\right)^2 + \left(2^{3n}\right)^3 = 2^{3n} + \left(2^{3n}\right)^2 + \left(2^{3n}\right)^3$
Par passage à la congruence et grâce à la question précédente :
$\equiv 1+1+1 \equiv 3 \pmod 7$

b. Supposons que le reste de la division euclidienne de p par 3 soit 1, on a : $p = 3\cdot n+1$
On a :
$A_p = 2^p + 2^{2p} + 2^{3p} = 2^{3n+1} + 2^{2\cdot(3n+1)} + 2^{3\cdot(3n+1)}$
$= 2^{3n+1} + 2^{6n+2} + 2^{9n+3}$
$= 2^{3n+1} + 2^{3\cdot(2n)+2} + 2^{3\cdot(3n+1)}$
D'après la question 2., on a la congruence :
$\equiv 2+4+1 \equiv 7 \equiv 0 \pmod 7$
Ce qui montre que le nombre A_p est un entier divisible par 7.

c. Supposons que le reste de la division euclidienne de p par 3 soit 1, on a : p=$3\cdot n$+2
On a :
$A_p = 2^p + 2^{2p} + 2^{3p} = 2^{3n+2} + 2^{2\cdot(3n+2)} + 2^{3\cdot(3n+2)}$
$= 2^{3n+2} + 2^{6n+4} + 2^{9n+6}$
$= 2^{3n+2} + 2^{3\cdot(2n+1)+1} + 2^{3\cdot(3n+)}$
D'après la question 2., on a les équivalences :
$\equiv 4+2+1 \equiv 7 \equiv 0 \pmod 7$
Le nombre A_p est divisible par 7.

Exercice 3694

On appelle (E) l'ensemble des entiers naturels qui peuvent s'écrire sous la forme $9+a^2$ où a est un entier naturel non nul ; par exemple :

$10=9+1^2$; $13=9+2^2$; ...

On se propose dans cet exercice d'étudier l'existence d'éléments de (E) qui sont des puissances de 2, 3 ou 5.

1. Etude de l'équation d'inconnue a :
$a^2+9=2^n$ où $a\in\mathbb{N}$, $n\in\mathbb{N}$, $n\geqslant 4$.

a. Montrer que si a existe, a est impair.

b. En raisonnant modulo 4, montrer que l'équation proposée n'a pas de solution.

2. Etude de l'équation d'inconnue a :
$a^2+9=3^n$ où $a\in\mathbb{N}$, $n\in\mathbb{N}$, $n\geqslant 3$.

a. Montrer que si $n\geqslant 3$, 3^n est congru à 1 ou à 3 modulo 4.

b. Montrer que si a existe, il est pair et en déduire que nécessairement n est pair.

c. On pose $n=2p$ où p est un entier naturel, $p\geqslant 2$. Déduire d'une factorisation de 3^n-a^2, que l'équation proposée n'a pas de solution.

3. Etude de l'équation d'inconnue a :
$a^2+9=5^n$ où $a\in\mathbb{N}$, $n\in\mathbb{N}$, $n\geqslant 2$.

a. En raisonnant modulo 3, montrer que l'équation n'a pas de solution si n est impair.

b. On pose $n=2p$, en s'inspirant de 2. c. démontrer qu'il existe un unique entier naturel a tel que a^2+9 soit une puissance entière de 5.

Correction 3694

1. a. Soit n un entier naturel tel que $n\geqslant 4$. Soit a un entier naturel vérifiant l'égalité :
$a^2+9=2^n$
On a l'équivalence suivante :
$a^2+9=2^n$
$a^2+9\equiv 2^n \pmod 2$
$a^2+1\equiv 0 \pmod 2$
Ainsi, le nombre a^2+1 est pair ; on en déduit que a^2 est un entier impair. Seul les nombres impairs ont un carré impair.

b. On a les équivalences suivantes :
$$\begin{aligned} a^2+9&=2^n\\ a^2+9&\equiv 2^2\cdot 2^{n-2} \pmod 4\\ a^2+9&\equiv 4\cdot 2^{n-2} \pmod 4\\ a^2+1&\equiv 0 \pmod 4\end{aligned}$$
La division euclidienne de a par 4 donne :
$$\begin{aligned} (4\cdot q+r)^2+1&\equiv 0 \pmod 4\\ 16\cdot q^2+8\cdot q\cdot r+r^2+1&\equiv 0 \pmod 4\\ r^2+1&\equiv 0 \pmod 4\end{aligned}$$
Le reste r vérifie l'encadrement $0\leqslant r\leqslant 3$; voyons dans le tableau suivant quelles valeurs vérifient l'équivalence ci-dessus :

r	0	1	2	3
r^2+1	1	2	5	10
$r^2+1 \pmod 4$	1	2	1	2

On montre ainsi qu'aucun nombre a n'est solution de cette équation.

2. a. Soit n un entier supérieur à 3, la division euclidienne de n par 2 donne l'existence d'un quotient q et r vérifiant :
$n=2\cdot q+r$ où $0\leqslant r<2$
On a :
$$\begin{aligned} 3^n=3^{2\cdot q+r}&=3^{2\cdot q}\cdot 3^r=\left(3^2\right)^q\cdot 3^r\\ &=9^q\cdot 3^r\\ &\equiv 1^q\cdot 3^r \pmod 2\\ &\equiv 3^r \pmod 2\end{aligned}$$
Ainsi :
- Si $r=0$ alors $3^n\equiv 1 \pmod 4$;
- Si $r=1$ alors $3^n\equiv 3 \pmod 4$;

b. D'après la question précédente, on déduit pour tout entier naturel n :
$3^n\equiv 1 \pmod 2$
On en déduit l'équivalence suivante :
$$\begin{aligned} a^2+9&\equiv 3^n \pmod 2\\ a^2+1&\equiv 1 \pmod 2\\ a^2&\equiv 0 \pmod 2\end{aligned}$$
Le carré de a étant pair, on en déduit que a est également pair.
Puisque a est pair, il existe un entier k naturel tel que :
$a=2\cdot k$
L'équation s'écrit :
$$\begin{aligned} a^2+9&=3^n\\ (2\cdot k)^2+9&=3^n\\ 4\cdot k^2+9&=3^n\end{aligned}$$
On a les équivalences suivantes :
$$\begin{aligned} 0\cdot k^2+1&\equiv 3^n \pmod 4\\ 1&\equiv 3^n \pmod 4\end{aligned}$$
Or, d'après la question a., puisque $3^n\equiv 1 \pmod 4$, on en déduit que n est pair.

c. On a la factorisation suivante :
$$\begin{aligned} 3^n-a^2=3^{2\cdot p}-a^2&=\left(3^p\right)^2-a^2\\ &=\left(3^p-a\right)\left(3^p+a\right)\end{aligned}$$
On obtient l'équation suivante :
$$\begin{aligned} a^2+9&=3^n\\ 9&=3^n-a^2\\ 9&=\left(3^p-a\right)\left(3^p+a\right)\end{aligned}$$
Par hypothèse, on a $n\leqslant 3$; on vient de montrer que n est pair, on en déduit que $n\leqslant 4$. Dans l'écriture $n=2\cdot p$, on en déduit que :
$$\begin{aligned} p&\geqslant 2\\ 3^p&\geqslant 3^2\\ 3^p&\geqslant 9\\ 3^p+a&\geqslant 9+a\end{aligned}$$
De l'égalité :
$\left(3^p-a\right)\left(3^p+a\right)=9$
On en déduit que $a=0$ et $p=2$ afin que le second fac-

teur du membre de gauche vale 9. Mais alors l'égalité n'est pas vérifiée.

Cette équation n'a pas de solution.

3. a. En effectuant la division euclidienne de n par 2, on a l'existence de deux entiers naturels tels que :

$n = 2{\cdot}q + r$ où $0 \leqslant r \leqslant 1$

On en déduit l'équivalence suivante :

$$\begin{aligned} 5^n = 5^{2{\cdot}q+r} = 5^{2{\cdot}q} \cdot 5^r &= \left(5^2\right)^q \cdot 5^r \\ &= 25^q \cdot 5^r \\ &\equiv 1^q \cdot 5^r \pmod 3 \\ &\equiv 5^r \pmod 3 \end{aligned}$$

On en déduit :

- $5^n \equiv 1 \pmod 3$ si n est pair.
- $5^n \equiv 2 \pmod 3$ si n est impair.

La division euclidienne de a par 3 donne l'existence de deux entiers q et r tels que :

$a = 3{\cdot}q + r$ où $0 \leqslant r < 3$

On a les transformations suivantes :

$$\begin{aligned} a^2 + 9 &= 5^n \\ (3{\cdot}q + r)^2 + 9 &= 5^n \\ (3{\cdot}q)^2 + 2{\cdot}3{\cdot}q{\cdot}r + r^2 + 9 &= 5^n \end{aligned}$$

On a les équivalences suivantes :

$$\begin{aligned} (0{\cdot}q)^2 + 2{\cdot}0{\cdot}q{\cdot}r + r^2 + 0 &\equiv 5^n \pmod 3 \\ r^2 &\equiv 5^n \pmod 3 \end{aligned}$$

Supposons n impair, on a :

$$r^2 \equiv 2 \pmod 3$$

Vérifions si une valeur de r vérifie cette équivalence :

r	0	1	2
r^2	0	1	4
$r^2 \pmod 3$	0	1	1

Ainsi, il n'y a pas de solution lorsque n est impair.

b. On a la factorisation suivante :

$$\begin{aligned} a^2 + 9 &= 5^n \\ 9 &= 5^n - a^2 \\ 9 &= 5^{2{\cdot}p} - a^2 \\ 9 &= \left(5^p\right)^2 - a^2 \\ 9 &= \left(5^p + a\right)\left(5^p - a\right) \end{aligned}$$

Dans le membre de droite, le premier facteur est positif ; cela entraîne que le second est également positif.
Or, $n \geqslant 2$, on en déduit que $p \geqslant 1$.
Ainsi, le premier facteur vérifie :

- $5^p + a \geqslant 5$
- $5^p + a$ divise 9

On en déduit $5^p + a = 9$ entraînant nécessairement :

$p = 1$; $a = 4$

Vérifions que ce couple d'entiers est solution :

$4^2 + 9 = 25$; $5^{2\times 1} = 5^2 = 25$

Exercice 5862

On note E l'ensemble des vingt-sept nombres entiers compris entre 0 et 26.
On note A l'ensemble dont les éléments sont les vingt-six lettres de l'alphabet et un séparateur entre deux mots, noté "$\star$" considéré comme un caractère.
Pour coder les éléments de A, on procède de la façon suivante :

- *Premièrement* : on associe à chacune des lettres de l'alphabet, rangées par ordre alphabétique, un nombre entier naturel compris entre 0 et 25, rangés par ordre croissant. On a donc :

  $a \longmapsto 0$; $b \longmapsto 1$; $\ldots$; $z \longmapsto 25$.

  On associe au séparateur "$\star$" le nombre 26.

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13

o	p	q	r	s	t	u	v	w	x	y	z	$\star$
14	15	16	17	18	19	20	21	22	23	24	25	26

  On dit que a a pour rang 0, b a pour rang 1,..., z a pour rang 25 et le séparateur "$\star$" a pour rang 26.

- *Deuxièmement :* à chaque élément x de E, l'application g associe le reste de la division euclidienne de $4x+3$ par 27.
  On remarquera que, pour tout x de E, $g(x)$ appartient à E.

- *Troisièmement :* le caractère initial est alors remplacé par le caractère de rang $g(x)$.

Exemple :

$s \longmapsto 18$; $g(18) = 21$; $21 \longmapsto v$.

Donc, la lettre s est remplacée lors du codage par la lettre v.

1. Trouver tous les entiers x de E tel que $g(x) = x$, c'est à dire invariants par l'application g.
   En déduire tous les caractères invariants dans ce codage.

2. Démontrer que, pour tout entier naturel x appartenant à E et tout entier naturel y appartenant à E :

   Si $y \equiv 4x + 3 \pmod{27}$ alors $x \equiv 7y + 6 \pmod{27}$

   En déduire que deux caractères distincts sont codés par deux caractères distincts.

3. Proposer une méthode de décodage.

4. Décoder le mot "vfv".

Correction 5862

1. Considérons un nombre x tel que :

   $g(x) = x$

   Ainsi, un tel nombre x doit vérifier :

   $$\begin{aligned} g(x) &= x \\ 4{\cdot}x + 3 &\equiv x \pmod{27} \\ 4{\cdot}x - x &\equiv -3 \pmod{27} \\ 3{\cdot}x &\equiv 24 \pmod{27} \end{aligned}$$

   Puisque x vérifie l'encadrement :

   $0 \leqslant x \leqslant 26 \implies 0 \leqslant 3{\cdot}x \leqslant 78$

   Ainsi, le nombre x peut vérifier l'une des équations ci-dessous :

$3{\cdot}x = 24$	$3x = 51$	$3x = 78$
$x = 8$	$x = 17$	$x = 26$

   On en déduit que les lettres suivantes sont invariantes par ce codage :

i ; r ; $\star$

2. Supposons que x et y sont deux entier naturel de E vérifiant la congruence :

$$\begin{aligned} y &\equiv 4x+3 && (\text{mod. } 27)\\ 7{\cdot}y &\equiv 7{\cdot}(4x+3) && (\text{mod. } 27)\\ 7{\cdot}y &\equiv 28{\cdot}x+21 && (\text{mod. } 27)\\ 7{\cdot}y-21 &\equiv x && (\text{mod. } 27)\\ x &\equiv 7{\cdot}y-21+27 && (\text{mod. } 27)\\ x &\equiv 7{\cdot}y+6 && (\text{mod. } 27) \end{aligned}$$

Effectuons un raisonnement par l'absurde : supposons deux caractès, associée dans le tableau par les nombres x et x', codés par le même caractère associé dans le tableau par le nombre y Ainsi, on a :

$y \equiv 4{\cdot}x+3 \pmod{27}$; $y \equiv 4{\cdot}x'+3 \pmod{27}$

On en déduit l'égalité :

$$\begin{aligned} 4{\cdot}x+3 &\equiv 4{\cdot}x'+3 && (\text{mod. } 27)\\ (4{\cdot}x+3)-(4{\cdot}x'+3) &\equiv 0 && (\text{mod. } 27)\\ 4{\cdot}x-4{\cdot}x' &\equiv 0 && (\text{mod. } 27)\\ 4{\cdot}(x-x') &\equiv 0 && (\text{mod. } 27) \end{aligned}$$

On vient d'établir que $4{\cdot}(x-x')$ est un multiple de 27. Ainsi :

- 27 divise $4{\cdot}(x-x')$;
- les entiers 27 et 4 sont premiers entre eux.

D'après le théorème de Gauss, on en déuit que 27 divise $x-x'$. Or, les deux nombres appartenant à E, on en déduit :

$0 \leqslant x \leqslant 26$ | $0 \leqslant x' \leqslant 26$

$-26 \leqslant x' \leqslant 0$

On en déduit l'encadrement :

$-26 \leqslant x-x' \leqslant 26$

Or, 27 divisant $x-x'$, on en déduit :

$x-x'=0$.

$x=x'$

Ce qui est absurde.

On vient de montrer que si deux lettres acceptent le même codage alors elles sont égales.

3. Voici la "*m'éthode*" de décodage :

- *Premièrement :* à chacune des lettres, on associe un nombre à l'aide du tableau de l'exercice ;
- *Deuxièmement :* à chaque nombre y de E, on associe le reste de la division euclidienne de $7{\cdot}y+6$ par 27
- *Troisièmement :* le nombre obtenu est remplacé par une lettre à l'aide du tableau.

4. Appliquons la méthode précédente aux deux lettres du mot à décoder :

- Pour la lettre "v" :
  - La lettre v est associée au nombre 21.
  - On a : $7{\times}21+6 = 147+6 = 153 = 5{\times}27+18 \equiv 18 \pmod{27}$
  - La lettre associée au nombre 18 est S.
- Pour la lettre "f" :
  - La lettre f est associée au nombre 5.
  - On a : $7{\times}5+6 = 35+6 = 41 = 1{\times}27+14 \equiv 14 \pmod{27}$
  - La lettre associée au nombre 14 est o.

Ainsi, le mot "*vfv*" est *sos*.

Exercice 5863

Partie A

On considère l'algorithme suivant :

```
Variables : a est un entier naturel
            b est un entier naturel
            c est un entier naturel
Initialisation : Affecter à c la valeur 0
            Demander la valeur de a
            Demander la valeur de b
Traitement  Tant que a > b
              Affecter à c la valeur c + 1
              Affecter à a la valeur de a − b
            Fin de Tant que
Sortie :    Afficher c
            Afficher a
```

1. Faire fonctionner cet algorithme avec $a=13$ et $b=4$ en indiquant les valeurs des variables à chaque étape.

2. Que permet de calculer cet algorithme ?

Partie B

A chaque lettre de l'alphabet, on associe, grâce au tableau ci-dessous, un nombre entier compris entre 0 et 25.

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

On définit un procédé de codage de la façon suivante :

Etape 1 : A la lettre que l'on veut coder, on associe le nombre m correspond dans le tableau.

Etape 2 : On calcule le reste de la division euclidienne de $9m+5$ par 26 et on le note p.

Etape 3 : Au nombre p, on associe la lettre correspondante dans le tableau.

1. Coder la lettre U.

2. Modifier l'algorithme de la partie A pour qu'à une valeur de m entrée par l'utilisateur, il affiche la valeur de p, calculée à l'aide du procédé de codage précédent.

Partie C

1. Trouver un nombre entier x tel que $9x \equiv 1 \pmod{26}$.

2. Démontrer alors l'équivalence :

$9m+5 \equiv p \pmod{26} \iff m \equiv 3p-15 \pmod{26}$

3. Décoder alors la lettre B.

Correction 5863

Partie A

1. Voici les valeurs des différentes variables lors de l'exécution de l'algorithme "*Tant que*" :

- A la fin de l'initialisation :

$a=13$; $b=4$; $c=0$

- A la fin du 1er passage :
  $a=9$; $b=4$; $c=1$
- A la fin du 1er passage :
  $a=5$; $b=4$; $c=2$
- A la fin du 1er passage :
  $a=1$; $b=4$; $c=3$

A la sortie de la boucle, l'algorithme affichera les deux valeurs :
3, puis 1

2. Cet algorithme permet d'afficher le quotient et le reste de la division euclidienne de a par b.

Partie B

1. Voici les étapes du codage de la lettre U :
   - La lettre U est associée au nombre 20 ;
   - Le nombre 20 subit la transformation suivante :
     $9\times20+5=185$
     La division euclidienne de 185 par 26 donne l'égalité :
     $185=7\times25+10$
     Ainsi, la valeur de p est associée au nombre 10.
   - La lettre associée au nombre 10 est la lettre K.

2. Voici l'algorithme modifié permettant d'afficher le nombre p :

Variables :	a est un entier naturel
	b est un entier naturel
	c est un entier naturel
Initialisation :	Affecter à c la valeur 0
	Affecter à b la valeur 26
	Demander la valeur de a
	Affecter à a la valeur $9*a+5$
Traitement	Tant que $a>b$
	Affecter à c la valeur $c+1$
	Affecter à a la valeur de $a-b$
	Fin de Tant que
Sortie :	Afficher a

Partie C

1. On remarque que pour x=3, on a :
   $9\times3=27=26+1\equiv0+1\equiv1 \pmod{26}$

2. Pour montrer l'équivalence, nous allons montrer les deux implications suivantes :
   - Supposons que $m\equiv3p-15 \pmod{26}$
     On a les congruences suivantes :
     $$\begin{aligned} m &\equiv 3p-15 && (\text{mod. }26)\\ 9\cdot m &\equiv 9\cdot(3p-15) && (\text{mod. }26)\\ 9\cdot m &\equiv 27\cdot p-135 && (\text{mod. }26)\\ 9\cdot m+5 &\equiv 27\cdot p-135+5 && (\text{mod. }26)\\ 9\cdot m+5 &\equiv 27\cdot p-130 && (\text{mod. }26)\\ 9\cdot m+5 &\equiv (26+1)\cdot p-26\times5 && (\text{mod. }26)\\ 9\cdot m+5 &\equiv p && (\text{mod. }26) \end{aligned}$$
   - Supposons que $9\cdot m+5\equiv p \pmod{26}$
     On a les congruences suivantes :
     $9\cdot m+5\equiv p \pmod{26}$
     D'après la question 1., on a :
     $$\begin{aligned} 3\cdot(9\cdot m+5) &\equiv 3\cdot p && (\text{mod. }26)\\ 27\cdot m+15 &\equiv 3\cdot p && (\text{mod. }26)\\ 27\cdot m &\equiv 3\cdot p-15 && (\text{mod. }26)\\ (26+1)\cdot m &\equiv 3\cdot p-15 && (\text{mod. }26)\\ m &\equiv 3\cdot p-15 && (\text{mod. }26) \end{aligned}$$
     On vient d'établir l'équivalence.

3. Notons m le code associé à la lettre qui codée, donne la lettre B. C'est à dire que le nombre p associé au nombre m a pour valeur 1.
   D'après la question précédente, on a :
   $$\begin{aligned} m &\equiv 3\times1-15 && (\text{mod. }26)\\ m &\equiv 3-15 && (\text{mod. }26)\\ m &\equiv -12 && (\text{mod. }26)\\ m &\equiv -12+26 && (\text{mod. }26)\\ m &\equiv 14 && (\text{mod. }26) \end{aligned}$$
   Ainsi, la lettre décodée donne O.

---

27. Problèmes sur la congruence :

Exercice 3662

Partie A

1. Déterminer le reste de la division euclidienne de $2\,009^2$ par 16.

2. En déduire que $2\,009^{8\,001}\equiv2\,009 \pmod{16}$

Partie B

On considère la suite (u_n) définie sur $\mathbb{N}$ par $u_0=2\,009^2-1$ et, pour tout entier naturel n, $u_{n+1}=(u_n+1)^5-1$.

1. a. Démontrer que u_0 est divisible par 5.

   b. Démontrer, en utilisant la formule du binôme de Newton, que pour tout entier naturel n :
   $u_{n+1}=u_n\cdot\left[u_n^4+5\cdot(u_n^3+2\cdot u_n^2+2\cdot u_n+1)\right]$

   c. Démontrer par récurrence que, pour tout entier naturel n, u_n est divisible par 5^{n+1}.

2. a. Vérifier que $u_3=2\,009^{250}-1$ puis en déduire que $2\,009^{250}\equiv1 \pmod{625}$.

   b. Démontrer alors que $2\,009^{8\,001}\equiv2\,009 \pmod{625}$

Correction 3662

Partie A

1. La division euclidienne de 2 009 par 16 donne :
   $2\,009=125\times16+9$

   Ainsi, on a :

$$2\,009 \equiv 9 \pmod{16}$$
$$2\,009^2 \equiv 9^2 \pmod{16}$$
$$2\,009^2 \equiv 81 \pmod{16}$$
$$2\,009^2 \equiv 5\times 16+1 \pmod{16}$$
$$2\,009^2 \equiv 1 \pmod{16}$$

2. On a :

$$2\,009^{8\,001} = 2\,009^{4\,000\times 2+1} = \left(2\,009^2\right)^{4\,000}\cdot 2\,009$$
$$\equiv 1^{4\,000}\times 2\,009 \equiv 2\,009 \pmod{16}$$

Partie B

1. a. La division euclidienne de 2 009 par 5 permet d'écrire :

$$2\,009 = 401\times 5+4$$

On obtient ainsi les classes d'équivalences suivantes :

$$u_0 = 2\,009^2-1$$
$$\equiv 4^2-1 \equiv 16-1 \equiv 15 \pmod{5}$$
$$\equiv 0 \pmod{5}$$

b. Par développement, on obtient :

$$u_{n+1} = \left(u_n+1\right)^5-1$$
$$= \left(u_n+1\right)^2\cdot\left(u_n+1\right)^2\cdot\left(u_n+1\right)-1$$
$$= \left(u_n^2+2\cdot u_n+1\right)\cdot\left(u_n^2+2\cdot u_n+1\right)\cdot\left(u_n+1\right)-1$$
$$= \left(u_n^4+2\cdot u_n^3+u_n^2+2\cdot u_n^3+4\cdot u_n^2+2\cdot u_n+u_n^2+2\cdot u_n+1\right)\cdot\left(u_n+1\right)-1$$
$$= \left(u_n^4+4\cdot u_n^3+6\cdot u_n^2+4\cdot u_n+1\right)\cdot\left(u_n+1\right)-1$$
$$= \left(u_n^5+4\cdot u_n^4+6\cdot u_n^3+4\cdot u_n^2+u_n\right)+\left(u_n^4+4\cdot u_n^3+6\cdot u_n^2+4\cdot u_n+1\right)-1$$
$$= u_n^5+5\cdot u_n^4+10\cdot u_n^3+10\cdot u_n^2+5u_n$$
$$= u_n\cdot\left(u_n^4+5\cdot u_n^3+10\cdot u_n^2+10\cdot u_n+5\right)$$
$$= u_n\cdot\left[u_n^4+5\cdot\left(u_n^3+2\cdot u_n^2+2\cdot u_n+1\right)\right]$$

c. Considérons la propriété $\mathcal{P}_n$ définie pour tout entier naturel n par :

$\mathcal{P}_n$: "u_n est divisible par 5^{n+1}"

Montrons, à l'aide d'un raisonnement par récurrence, que la propriété $\mathcal{P}_n$ est vraie pour tout entier naturel n.

- **Initialisation :**
  D'après la question a., u_0 est divisible par 5 donc divisible par 5^{0+1}.
  On vient de montrer que $\mathcal{P}_0$ est vraie.
- **Hérédité :**
  Supposons que la propriété $\mathcal{P}_n$ est vraie pour un entier naturel n quelconque. C'est à dire qu'on a :
  u_n est divisible par 5^{n+1}.
  Il existe un entier k vérifiant : $u_n = 5^{n+1}\times k$
  D'après la relation obtenue à la question b. :

$$u_{n+1} = u_n\cdot\left[u_n^4+5\cdot\left(u_n^3+2\cdot u_n^2+2\cdot u_n+1\right)\right]$$
$$= \left(5^{n+1}\cdot k\right)\cdot\left[\left(5^{n+1}\cdot k\right)^4+5\cdot\left(u_n^3+2\cdot u_n^2+2\cdot u_n+1\right)\right]$$
$$= 5^{n+1}\cdot k\cdot\left[5^{4n+4}\cdot k^4+5\cdot\left(u_n^3+2\cdot u_n^2+2\cdot u_n+1\right)\right]$$
$$= 5^{n+1}\cdot k\cdot\left[5\cdot\left(5^{4n+3}\cdot k^4+u_n^3+2\cdot u_n^2+2\cdot u_n+1\right)\right]$$
$$= 5^{n+2}\cdot k\cdot\left[5^{4n+3}\cdot k^4+u_n^3+2\cdot u_n^2+2\cdot u_n+1\right]$$

- **Conclusion :**
  La propriété s'initialise au rang 0 et elle vérifie la propriété d'hérédité. D'après le raisonnement par récurrence, on montre que la propriété est vraie pour tout entier naturel n.

2. a. On a les valeurs suivantes pour les termes de la suite $\left(u_n\right)$:

- $u_0 = 2\,009^2-1$
- $u_1 = \left[\left(2\,009^2-1\right)+1\right]^5-1 = \left(2\,009^2\right)^5-1$
  $= 2\,009^{10}-1$
- $u_2 = \left[\left(2\,009^{10}-1\right)+1\right]^5-1 = \left(2\,009^{10}\right)^5-1$
  $= 2\,009^{50}-1$
- $u_3 = \left[\left(2\,009^{50}-1\right)+1\right]^5-1 = \left(2\,009^{50}\right)^5-1$
  $= 2\,009^{250}-1$

D'après la propriété obtenue à la question 1. a. , u_3 est divisible par $5^{3+1} = 5^4 = 625$; ainsi, on a :

$$u_3 \equiv 0 \pmod{625}$$
$$2\,009^{250}-1 \equiv 0 \pmod{625}$$
$$2\,009^{250} \equiv 1 \pmod{625}$$

b. On peut écrire :

$$2\,009^{8\,001} = 2\,009^{4\times 250+1} = \left(2\,009^{250}\right)^4\times 2\,009^1$$
$$\equiv 1^4\times 2\,009^1 \equiv 2\,009 \pmod{625}$$

28. Annales :

Exercice 3361

On considère la suite $\left(u_n\right)$ d'entiers naturels définie par :

$u_0 = 14$; $u_{n+1} = 5u_n-6$ pour tout $n\in\mathbb{N}$

Montrer que, pour tout entier naturel n, $u_{n+2} \equiv u_n \pmod{4}$.

Correction 3361

On a la relation :

$$u_{n+2} = 5\cdot u_{n+1}-6 = 5\cdot\left(5\cdot u_n-6\right)-6$$
$$= 25\cdot u_n-30-6 = 25\cdot u_n-36$$

On a la relation de congruence modulo 4 :

$$\equiv 1\cdot u_n-0 \equiv u_n \pmod{4}$$

Exercice 5704

Une frise est constituée de carrés, triangles, cercles et trapèzes se succédant régulièrement. Ces élèments sont successivement peints en blanc, avec des rayures ou en noir.

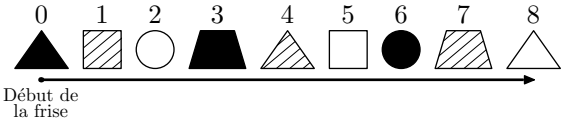
Le début de la frise est représenté ci-dessous :

1. Donner les caractéristiques du 113$^{\text{ième}}$ élément de cette frise.

2. Quel est l'élément suivant le 113$^{\text{ième}}$ élément et ayant les mêmes caractéristiques.

Correction 5704

1. Numérotons les éléments de la frise en partant de 0 :



On peut faire les remarques suivantes :

- Pour la couleur, on remarque que le coloriage de l'objet est cyclique de période 3. Notons r le reste de la division euclidienne du rang de l'objet par 3 :
  - si $r=0$: l'objet est noir ;
  - si $r=1$: l'objet est hachuré ;
  - si $r=2$: l'objet est blanc.
- Pour la forme, on remarque que la forme de l'objet est cyclique de période 4. Notons r' le reste de la division euclidienne du rang de l'objet par 4 :
  - si $r'=0$: l'objet est un triangle ;
  - si $r'=1$: l'objet est un carré ;
  - si $r'=2$: l'objet est un cercle ;
  - si $r'=3$: l'objet est un trapèze ;

Dans cet modélisation, le 113$^{\text{ième}}$ élément de cette frise aura pour rang 112. Voici les divisions euclidiennes de 112 respectivement par 3 et par 4 :
$112 = 37\times3+1$; $112 = 28\times4+0$

On en déduit que l'objet est un triangle hachuré.

2. Les prochains objet hachurés seront les objets :
115 ; 118 ; 121 ; 124 ; 127

Les prochains objet de forme triangulaire seront les objets :
116 ; 120 ; 124 ; 128 ; 132

Ainsi, le prochain objet ayant les mêmes caractéristiques que l'objet 113$^{\text{ième}}$ sera le 125$^{\text{ième}}$ objet.

Exercice 5727

Montrer que la somme de trois entiers consécutifs est divisible par 3.

Correction 5727

Notons n le premier de ces trois entiers consécutifs. Alors les deux autres entiers admettent pour expression :
$n+1$; $n+2$

Ainsi, la somme de ces trois entiers consécutfis admet pour expression :
$n+(n+1)+(n+2) = 3\cdot n+3 = 3\cdot(n+1)$

On vient de montrer que la somme de ces trois entiers est un multiple de 3 : elle est donc divisible par 3.

Exercice 3363

Montrer, à l'aide d'un raisonnement par récurrence, que, pour tout entier naturel n, on a :

$5^{n+2} \equiv 25 \pmod{100}$

Correction 3363

Considérons la propriété $\mathcal{P}_n$ définie pour tout entier naturel n par la relation :
$\mathcal{P}_n$: "$5^{n+2} \equiv 25 \pmod{100}$"

Montrons, à l'aide d'un raisonnement par récurrence, que la propriété $\mathcal{P}_n$ est vraie pour tout entier naturel n.

- **Initialisation :**

Pour $n=0$, on a :
$5^{0+2} = 5^2 = 25$
$\equiv 25 \pmod{100}$

La propriété $\mathcal{P}_0$ est vraie.

- **Hérédité :**

Supposons que la propriété $\mathcal{P}_n$ est vraie pour un entier naturel n quelconque. C'est à dire qu'on a l'hypothèse de récurrence :
$5^{n+2} \equiv 25 \pmod{100}$

Considérons la valeur :
$5^{(n+1)+2} = 5^{n+3} = 5^{(n+2)+1} = 5^{n+2}\times5$

D'après l'hypothèse de récurrence :
$\equiv 25\times5 \equiv 125 \equiv 25 \pmod{100}$

On vient d'établir que la propriété $\mathcal{P}_{n+1}$ est vraie.

- **Conclusion :**

La propriété $\mathcal{P}_{n+1}$ est initialisée au rang 0 et elle vérifie la propriété d'hérédité. A l'aide d'un raisonnement par récurrence, on vient d'établir que la propriété $\mathcal{P}_n$ est vraie pour tout entier naturel n.

Exercice 3665

On considère l'ensemble $A_7 = \{1\,;\,2\,;\,3\,;\,4\,;\,5\,;\,6\}$

1. Pour tout élément a de A_7, écrire dans le tableau ci-dessous l'unique élément y de A_7 tel que $ay \equiv 1 \pmod{7}$.

a	1	2	3	4	5	6
y						6

2. Pour x entier relatif, démontrer que l'équation :
$3x \equiv 5 \pmod{7}$ équivaut à $x \equiv 4 \pmod{7}$.

3. Soit a un élèment de A_7, montrer que les seuls entiers relatifs x solutions de l'équation $a\cdot x \equiv 0 \pmod{7}$ sont les multiples de 7.

Correction 3665

1. Voici le tableau complété :

a	1	2	3	4	5	6
y	1	4	5	2	3	6

2. On a :

$$3\cdot x \equiv 5 \pmod 7$$
$$5\times 3\cdot x \equiv 5\times 5 \pmod 7$$
$$15\cdot x \equiv 25 \pmod 7$$
$$x \equiv 4 \pmod 7$$

3. Soit a un élèment de A_7.
D'après la question 1., pour élèment a de A_7, il existe un unique $b\in A_7$ tel que :
$a\cdot b \equiv 1 \pmod 7$

Résolvons l'équation demandée :
$$a\cdot x \equiv 0 \pmod 7$$
$$b\cdot(a\cdot x) \equiv b\cdot 0 \pmod 7$$
$$(b\cdot a)\cdot x \equiv 0 \pmod 7$$
$$1\cdot x \equiv 0 \pmod 7$$
$$x \equiv 0 \pmod 7$$

Ainsi, les solutions de l'équation sont les entiers multiples de 7.

Exercice 5703

Un système de codage permet de transformer toute lettre d'un texte en un autre rendant ainsi le texte illisible.

Pour cela, il numérote les lettres de l'alphabet en commençant par 0. Une transformation sur le nombre permet alors de changer la lettre.

Voici le tableau de correspondance de ce codage :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
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
C	F	I	L	O	R	U	X	A	D	G															

Quelle a-été la transformation utilisée sur les nombres ?

Correction 5703

Voici le tableau de correspondance de ce codage partiellement compléé :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
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
2	5	8	11	14	17	20	23	0	3	6															
C	F	I	L	O	R	U	X	A	D	G															

Apparemment pour obtenir le codage, on utilise la transformation suivante entre les nombres :
$n \longmapsto 2+3\times n$

Or, cette transformation donne des nombres supérieurs à 25 :
$9 \longmapsto 29$ Pour pouvoir ensuite associer une lettre à ce nombre, il faut prendre le reste de la division euclidienne par 26. Ainsi, on a le schéma suivante :

$6 \longmapsto 20 \longmapsto 20$
$7 \longmapsto 23 \longmapsto 23$
$8 \longmapsto 26 \longmapsto 0$
$9 \longmapsto 29 \longmapsto 3$
$10 \longmapsto 32 \longmapsto 6$

Exercice 3523

Montrer par un raisonnement par récurrence que pour tout entier naturel n, l'entier 5^n-1 est un multiple de 4.

Correction 3523

On considère la propriété $\mathcal{P}_n$ définie par :
$\mathcal{P}_n$: "5^n-1 est un multiple de 4"

Etablissons, à l'aide d'un raisonnement par récurrence, que la propriété $\mathcal{P}_n$ est vraie pour tout entier naturel n,

- **Initialisation :**
Pour $n=0$, on a : $5^n-1=1-1=0$
Le nombre 0 est un multiple de 4. On vient de montrer que la propriété $\mathcal{P}_0$ est vraie.
- **Hérédité :**
Supposons que la propriété $\mathcal{P}_n$ est vraie pour un entier naturel n quelconque. C'est à dire que le nombre 5^n-1 est un multiple de 4.
Ainsi, il existe un entier $k\in\mathbb{N}$ tel que :
$5^n-1=4\cdot k$

On a :
$$5^{n+1}-1=5^{n+1}-5^n+5^n-1=5^{n+1}-5^n+5^n-1$$
$$=5^n\cdot(5-1)+5^n-1=4\times 5^n+(5^n-1)$$

D'après l'hypothèse par récurrence :
$$=4\times 5^n+4\cdot k=4\times(5^n+k)$$

On vient d'établir que la propriété $\mathcal{P}_{n+1}$ est vraie.

- **Conclusion :**
La propriété $\mathcal{P}_n$ est initialisée au rang 0 et elle vérifie la propriété d'hérédité. A l'aide d'un raisonnement par récurrence, on vient de montrer que la propriété $\mathcal{P}_n$ est vraie pour tout entier naturel n.

Exercice 5470

Soit x un entier relatif.

1. En étudiant les restes possibles de la division euclidienne d'un entier x par 7, résoudre dans $\mathbb{Z}$ les équations suivantes :
a. $4\cdot x \equiv 1 \pmod 7$ b. $6\cdot x \equiv 3 \pmod 7$

2. En étudiant les restes possibles de la division euclidienne de x par 6, résoudre dans $\mathbb{Z}$ les équations suivantes :
a. $5\cdot x \equiv 2 \pmod 6$ b. $2\cdot x \equiv 3 \pmod 6$

Correction 5470

1. a. Par la division euclidienne par 7, tout nombre a un reste compris entre 0 et 6. Etudions chacun de ces cas :

Reste de x par 7	0	1	2	3	4	5	6
Reste de $4\cdot x$ par 7	0	4	1	5	2	6	3

On en déduit que l'ensemble des solutions de l'équation est l'ensemble des entiers relatifs ayant un reste de 2 par la division euclidienne par 7 :
$\mathcal{S}=\{2+7\cdot k \mid k\in\mathbb{Z}\}$

b. Par la division euclidienne par 7, tout nombre a un reste compris entre 0 et 6. Etudions chacun de ces cas :

Reste de x par 7	0	1	2	3	4	5	6
Reste de $6{\cdot}x$ par 7	0	6	5	4	3	2	1

On en déduit que l'ensemble des solutions de l'équation est l'ensemble des entiers relatifs ayant un reste égal à 4 par la division euclidienne par 7 :

$\mathcal{S} = \{4 + 7{\cdot}k \mid k \in \mathbb{Z}\}$

2. a. Par la division euclidienne par 6, tout nombre a un reste compris entre 0 et 5. Etudions chacun de ces cas :

Reste de x par 6	0	1	2	3	4	5
Reste de $5{\cdot}x$ par 6	0	5	4	3	2	1

On en déduit que l'ensemble des solutions de l'équation est l'esenmble des entiers relatifs ayant un reste égal à 2 par la division euclidienne par 6 :

$\mathcal{S} = \{4 + 6{\cdot}k \mid k \in \mathbb{Z}\}$

b. Par la division euclidienne par 6, tout nombre a un reste compris entre 0 et 5. Etudions chacun de ces cas :

Reste de x par 6	0	1	2	3	4	5
Reste de $2{\cdot}x$ par 6	0	2	4	0	2	4

Aucune valeur de x ne permet de réaliser la congruence $2{\cdot}x \equiv 3 \pmod 6$: on en déduit que l'ensemble des solutions de l'équation est vide :

$\mathcal{S} = \varnothing$

Exercice 5729

1. De l'égalité : $456\,164 = 65\,164{\times}7 + 16$, en déduire la divisione euclidienne de 456 164 par 7.

2. La division euclidienne du nombre 7^{17} par 4 a pour reste 3. On répondra aux questions suivantes en justifiant votre réponse.

   a. Déterminer le reste de la division euclienne de 7^{17} par 2.

   b. Déterminer le reste de la division euclidienne 7^{34} par 4.

Correction 5729

1. De l'égalité :

$456\,164 = 65\,164{\times}7 + 16$

$456\,164 = 65\,164{\times}7 + 14 + 2$

$456\,164 = 65\,164{\times}7 + 2{\times}7 + 2$

$456\,164 = 65\,166{\times}7 + 2$

On en déduit que le reste de la division euclidienne de 456 164 par 7 a pour valeur 2.

2. Le reste de la division euclidienne de 7^{17} par 4 a pour valeur 3. Ainsi, il existe un entier naturel k réalisant l'égalité suivante :

$7^{17} = k{\times}4 + 3$

a. De l'égalité précédente :

$7^{17} = k{\times}4 + 3$

On en déduit :

$7^{17} = (2k){\cdot}2 + 2 + 1$

$7^{17} = (2k+1){\cdot}2 + 1$

L'écriture ci-dessous donne le reste de la division euclidienne de 7^{17} par 2 : son reste vaut 2.

b. De l'égalité précédente :

$7^{17} = k{\times}4 + 3$

On en déduit :

$\left(7^{17}\right)^2 = \left(k{\cdot}7 + 3\right)^2$

$7^{17\times 2} = 49{\cdot}k^2 + 42{\cdot}k + 9$

$7^{34} = 7{\cdot}\left(7{\cdot}k^2 + 6{\cdot}k\right) + 9$

$7^{34} = 7{\cdot}\left(7{\cdot}k^2 + 6{\cdot}k\right) + 7 + 2$

$7^{34} = 7{\cdot}\left(7{\cdot}k^2 + 6{\cdot}k + 1\right) + 2$

L'expression précédente donne la division euclidienne de l'entier 7^{34} par 7 : son reste a pour valeur 2.

Exercice 3524

On considère la suite (u_n) d'entiers naturels définie par :

$u_0 = 14 \quad ; \quad u_{n+1} = 5{\cdot}u_n - 6$ pour tout $n \in \mathbb{N}$

1. Montrer par récurrence que, pour tout entier naturel : $2{\cdot}u_n = 5^{n+2} + 3$

2. a. Justifier que pour tout entier naturel n, $2{\cdot}u_n$ est un multiple de 4.

   b. Montrer que pour tout entier naturel n, on a : $2{\cdot}u_n \equiv 28 \pmod{100}$

Correction 3524

1. Considérons la propriété $\mathcal{P}_n$ définie pour tout entier naturel n par :

$\mathcal{P}_n$: "$2{\cdot}u_n = 5^{n+2} + 3$"

Montrons, à l'aide d'un raisonnement par récurrence, que la propriété $\mathcal{P}_n$ est vraie pour tout entier naturel n.

- **Initialisation :**

Pour $n = 0$, on a :

- $2{\cdot}u_0 = 2{\times}14 = 28$
- $5^{0+2} + 3 = 5^2 + 3 = 28 + 3 = 28$

On vient de montrer que la propriété $\mathcal{P}_0$ est vraie.

- **Hérédité :**

Supposons que la propriété $\mathcal{P}_n$ est vraie pour un entier naturel n quelconque. C'est à dire qu'on a la relation :

$2{\cdot}u_n = 5^{n+2} + 3$

La définition des termes de la suite (u_n) permet d'écrire :

$2{\cdot}u_{n+1} = 2{\cdot}\left(5{\cdot}u_n - 6\right) = 10{\cdot}u_n - 12 = 5{\cdot}\left(2{\cdot}u_n\right) - 12$

En utilisant l'hypothèse par récurrence :

$= 5{\cdot}\left(5^{n+2} + 3\right) - 12 = 5^{n+2+1} + 15 - 12$

$= 5^{(n+1)+2} + 3$

On vient de montrer que la propriété $\mathcal{P}_{n+1}$.

- **Conclusion :**

La propriété $\mathcal{P}_n$ est initialisée au rang 0 et elle vérifie la propriété d'hérédité. A l'aide d'un raisonnement par récurrence, on a établi que la propriété $\mathcal{P}_n$ est vraie pour tout entier naturel n.

2. a. Pour tout entier naturel n, on a la relation :

$2{\cdot}u_n = 5^{n+2} + 3$

En passant à la congruence modulo 4, cette relation devient :

$\equiv 1^{n+2} + 3 \equiv 1 + 3 \pmod 4$

$\equiv 4 \equiv 0 \pmod 4$

On en déduit que le nombre $2{\cdot}u_n$ est un multiple de 4.

b. Considérons la propriété $\mathcal{P}_n$ définie pour tout entier naturel n par :

$\mathcal{P}_n$: "$2{\cdot}u_n \equiv 28 \pmod{100}$"

Montrons, à l'aide d'un raisonnement par récurrence, que la propriété $\mathcal{P}_n$ est vraie pour tout entier naturel n.

- **Intialisation :**
  Pour $n = 0$, on a :
  $2{\cdot}u_0 = 2{\times}14 = 28 \equiv 28 \pmod{100}$
  La propriété $\mathcal{P}_0$ est vraie.
- **Hérédité :**
  Supposons que la propriété $\mathcal{P}_n$ est vérifiée pour un entier naturel n quelconque. C'est à dire qu'on a la congruence :
  $2{\cdot}u_n \equiv 28 \pmod{100}$
  La définition des termes de la suite (u_n) permet d'écrire :
  $2{\cdot}u_{n+1} = 2{\cdot}\big(5{\cdot}u_n - 6\big) = 10{\cdot}u_n - 12$
  $= 5{\cdot}\big(2{\cdot}u_n\big) - 12$
  En utilisant l'hypothèse de récurrence :
  $\equiv 5{\times}28 - 12 \equiv 140 - 12 \pmod{100}$
  $\equiv 128 \equiv 28 \pmod{100}$
  On vient de montrer que la propriété $\mathcal{P}_{n+1}$ est vraie.
- **Conclusion :**
  La propriété $\mathcal{P}_n$ est initialisée au rang 0 et elle vérifie la propriété d'hérédité. A l'aide d'un raisonnement par récurrence, on vient de montrer que cette propriété est vraie pour tout entier naturel n.

Exercice 5730

On considère les deux nombres $A = 10n + 7$ et $B = 2n + 1$.

1. Déterminer les nombres réels a et b vérifiant l'égalité :
$$\frac{10n+7}{2n+1} = a + \frac{b}{2n+1}$$

2. Justifier que les nombres A et B sont premiers entre eux.

Correction 5730

1. Effectuons les manipulations algébriques suivantes :
$$a + \frac{b}{2n+1} = \frac{a{\cdot}(2n+1)+b}{2n+1} = \frac{2a{\cdot}n + a + b}{2n+1}$$
$$= \frac{2a{\cdot}n + (a+b)}{2n+1}$$
Les deux quotients $\dfrac{10n+7}{2n+1}$ et $\dfrac{2a{\cdot}n+(a+b)}{2n+1}$ ayant le même dénominateur, il est nécessaire d'avoir l'égalité des numérateurs pour tout entier naturel n. Par identification, on obtient le système :
$$\begin{cases} 2a = 10 \\ a + b = 7 \end{cases}$$
Ce système admet pour solution : $a = 5$ et $b = 2$.

2. De la question précédente, on a obtenu l'égalité :
$$\frac{10n+7}{2n+1} = 5 + \frac{2}{2n+1}$$
qui permet d'obtenir l'égalité :
$$10n + 7 = 5{\cdot}(2n+1) + 2$$
Pour n supérieur à 1, on a l'encadrement $0 \leqslant 2 \leqslant 2n+1$, ce qui permet d'affirmer que la division euclidienne de l'entier $10n{+}7$ par $2n{+}1$ a toujours pour valeur 2.

En utilisant l'algorithme d'Euclide pour déterminer le pgcd de ces deux entiers, on obtient le tableau ci-dessous :

Dividende	Diviseur	Reste
10n+7	2n+1	2
2n+1	2	1
2	1	0

On en déduit : $\text{pgcd}\big(10n+7\,;2n+1\big) = 1$

Exercice 3558

Démontrer à l'aide d'un raisonnement par récurrence, que pour tout entier naturel n non-nul, on a :
$$x^n - 1 = (x-1)\big(1 + x + x^2 + \cdots + x^{n-1}\big)$$

Correction 3558

Montrons, à l'aide d'un raisonnement par récurrence, que pour tout entier naturel n non-nul, on a :
$x^n - 1 = (x-1)\big(1 + x + \cdots + x^{n-1}\big)$

- *Inialisation :*
  Au rang 1, on a :
  $x^1 - 1 = x - 1$
  $(x-1)(1) = x - 1$
  La relation est vraie au rang 1.
- *Hérédité :*
  Supposons la relation vraie au rang n.
  On a :
$$x^{n+1} - 1 = x^{n+1} - x^n + x^n - 1$$
$$= x^{n+1} - x^n + (x-1)\big(1 + x + x^2 + \cdots + x^{n-1}\big)$$
$$= x^n{\cdot}(x-1) + (x-1)\big(1 + x + x^2 + \cdots + x^{n-1}\big)$$
$$= (x-1)\Big[x^n + \big(1 + x + x^2 + \cdots + x^{n-1}\big)\Big]$$
$$= (x-1)\big(1 + x + x^2 + \cdots + x^{n-1} + x^n\big)$$
  La relation est vraie au rang $(n{+}1)$.

Exercice 5731

Montrer que pour tout entier nature n, l'expression $3n^2{+}n{+}2$ est divisible par 2.

Correction 5731

Etudions cette propriété par disjonction de cas. Plus particulièrement en deux cas : lorsque l'entier n est pair et lorsqu'il est impair.

- Lorsque n est pair :
  Il existe un entier k tel que $n = 2{\cdot}k$.
  Ainsi, l'expression à étudier devient :
$$3n^2 + n + 2 = 3{\cdot}\big(2k\big)^2 + \big(2k\big) + 2 = 3{\times}4k^2 + 2k + 2$$
$$= 12k^2 + 2k + 2 = 2{\cdot}\big(6k^2 + k + 1\big)$$

Ainsi, pour tout entier naturel n pair, l'expression $3n^2+n+2$ définit un nombre divisible par 2.

- Lorsque n est impair :
  Il existe un entier k tel que $n=2\cdot k+1$.

  Ainsi, l'expression à étudier devient :

$$\begin{aligned}3n^2+n+2 &= 3\cdot(2k+1)^2+(2k+1)+2\\ &= 3\cdot(4k^2+4k+1)+(2k+1)+2\\ &= 12k^2+12k+3+2k+1+2 = 12k^2+14k+6\\ &= 2\cdot(6k^2+7k+3)\end{aligned}$$

Ainsi, pour tout entier naturel n impair, l'expression $3n^2+n+2$ est un entier divisible par 2.

On vient de montrer que quelque soit l'entier naturel n, l'expression $3n^2+n+2$ définit un entier divisible par 2.

Exercice 5821

On considère l'algorithme suivant :

```
A et X sont des nombres entiers.
Saisir un entier positif A.
Affecter à X la valeur de A.
Tant que X supérieur ou égal à 26
    Affecter à X la valeur X−26.
Fin du tant que.
Afficher X.
```

1. Qu'affiche cet algorithme quand on saisit le nombre 3 ?
2. Qu'affiche cet algorithme quand on saisit le nombre 55 ?
3. Pour un nombre entier saisi quelconque, que représente le résultat fourni par cet algorithme ?

Correction 5821

1. 3 étant strictement inférieur à 26, la boucle conditionnelle ne sera pas évaluée : la valeur affichée par l'algorithme est 3.
2. Le nomnbre 55 étant supérieur ou égal à 26, la boucle sera exécuté une première fois.
   - A la fin de la première exécution de la boucle, la valeur de la variable X est :
     $X=55-26=29$
   - Le nombre 29 étant aussi supérieur ou égal à 26, la boucle est exécutée une seconde fois. A la fin de cette exécution, la variable X aura pour valeur :
     $X=29-26=3$

   La boucle ne sera plus exécutée et la valeur affichée par l'algorithme est 3.
3. Pour toute valeur de A saisie, cet algorithme affiche le reste de la division euclidienne de A par 26.

Exercice 5827

Utiliser les congruences pour calculer les restes de la division euclidienne par 7 des nombres suivants :

a. 5^6 b. 5^{6p}, pour $p\in\mathbb{N}^*$ c. 33^{38}

Correction 5827

a. $5^6=(5^2)^3=25^3=(3\times7+4)^3$
$\equiv 4^3\equiv 64\equiv 9\times7+1\equiv 1 \pmod 7$

b. $5^{6p}=(5^6)^p$
$\equiv 1^p\equiv 1 \pmod 7$

c. $33^{38}=(4\times7+5)^{36+2}$
$\equiv 5^{36}\times5^2\equiv 1^{36}\times25\equiv 1\times(3\times7+4)\equiv 4 \pmod 7$

Exercice 5841

On considère l'algorithme suivant :

```
Variables :      a est un entier naturel
                 b est un entier naturel
                 c est un entier naturel
Initialisation : Affecter à c la valeur 0
                 Demander la valeur de a
                 Demander la valeur de b
Traitement       Tant que a>b
                    Affecter à c la valeur c+1
                    Affecter à a la valeur de a−b
                 Fin de Tant que
Sortie :         Afficher c
                 Afficher a
```

1. Faire fonctionner cet algorithme avec $a=13$ et $b=4$ en indiquant les valeurs des variables à chaque étape.
2. Que permet de calculer cet algorithme ?

Correction 5841

1. Le tableau ci-dessous représente le fonctionnement de cet algorithme :

a	13	9	5	1
b	4	4	4	4
b	0	1	2	3
$a>b$	Vraie	Vraie	Vraie	Fausse

   A la sortie de la boucle, voici les valeurs des variables :
   $a=1$; $b=4$; $c=3$
2. Cet algorithme permet de calculer le quotient *(variable c)* et le reste *(variable a)* de la division euclidienne de la valeur initiale de a par celle de b.

Exercice 3390

Partie A : Question de cours

Quelles sont les propriétés de compatibilité de la relation de congruence avec l'addition, la multiplication et les puissances ?
Démontrer la propriété de compatibilité avec la multiplication.

Partie B

On note 0, 1, 2, ..., 9, α, β les chiffres de l'écriture d'un

nombre en base 12. Par exemple :
$\overline{\beta\alpha}^{12} = \beta\times12^2+\alpha\times12+7 = 11\times12^2+10\times12+7$
$= 1711$ en base 10

1. a. Soit N_1 le nombre s'écrivant en base 12 :
$N_1 = \overline{\beta1\alpha}^{12}$
Déterminer l'écriture de N_1 en base 10.

b. Soit N_2 le nombre s'écrivant en base 10 :
$N_2 = 1131 = 1\times10^3+1\times10^2+3\times10+1$
Déterminer l'écriture de N_2 en base 12.

Dans toute la suite, un entier naturel N s'écrira de manière générale en base 12 :
$N = \overline{a_n\cdots a_1a_0}^{12}$

2. a. Démontrer que $N \equiv a_0 \pmod 3$. En déduire un critère de divisibilité par 3 d'un nombre écrit en base 12.

b. A l'aide de son écriture en base 12, déterminer si N_2 est divisible par 3. Confirmer avec son écriture en base 10.

3. a. Démontrer que $N \equiv a_n+\cdots+a_1+a_0 \pmod{11}$. En déduire un critère de divisibilité par 11 d'un nombre écrit en base 12.

b. A l'aide de son écriture en base 12, déterminer si N_1 est divisible par 11. Confirmer avec son écriture en base 10.

4. Un nombre N s'écrit $\overline{x4y}^{12}$. Déterminer les valeurs de x et de y pour lesquelles N est divisible par 33.

Correction 3390

1. a. On a l'égalité suivante :
$N_1 = \overline{\beta1\alpha}^{12}$
$= 11\times12^2+1\times12+10$
$= 11\times144+12+10$
$= 1606$

b. On a les divisions euclidiennes suivantes :
$1131 = 94\times12+3$
$94 = 7\times12+10$
Ainsi, on a l'égalité suivante :
$1131 = (7\times12+10)\times12+3$
$= 7\times12^2+10\times12+3$
$= \overline{7\alpha3}^{12}$

2. a. On a l'égalité suivante :
$N = \overline{a_n\cdots a_1a_0}^{12}$
$= a_n\times12^n+\cdots+a_1\times12+a_0$
On a l'équivalence suivante :
$\equiv a_n\times0^n+\cdots+a_1\times0+a_0 \pmod 3$
$\equiv a_0 \pmod 3$
En base 12, un nombre est divisible par 3 si, et seulement si, son chiffre des unités est un multiple de 3.

b. Le chiffre des unités de N_2 en base 12 est 3 qui est divisible par 3. A l'aide de son écriture en base 12, N_2 est divisible par 3.

3. a. On a l'équivalence suivante :
$N = \overline{a_n\cdots a_1a_0}$
$= a_n\times12^n+\cdots+a_1\times12+a_0$
On a l'équivalence : $12 = 1 \pmod{11}$
$\equiv a_n\times1^n+\cdots+a_1\times1+a_0 \pmod{11}$
$\equiv a_n+\cdots+a_1+a_0 \pmod{11}$
On en déduit qu'un nombre $N = \overline{a_n\cdots a_1a_0}^{12}$ est divisible par 11 si, et seulement si, la somme de ses chiffres est divisible par 11.

b. En base 12, la somme des chiffres de N_1 a pour valeur :
$\beta+1+\alpha = 11+1+10 = 22$
Ainsi, le nombre N_1 est divisible par 12.

c. En base 10, on a l'égalité suivante :
$N_2 = 1606 = 146\times11$

4. Si N est divisible par 33 alors N est divisible par 3 et par 11.
En base 12, son écriture doit vérifier les deux conditions suivantes :
- y est divisible par 3 :
Ainsi, il doit avoir les valeurs :
0 ; 3 ; 6 ; 9
- La somme de ses chiffres doit être divisible par 11 :
  - Si $y = 0$, le nombre N s'écrit :
  $N = \overline{740}^{12}$
  - Si $y = 3$, le nombre N s'écrit :
  $N = \overline{443}^{12}$
  - Si $y = 6$, le nombre N s'écrit :
  $N = \overline{146}^{12}$
  - Si $y = 9$, le nombre N s'écrit :
  $N = \overline{949}^{12}$

Exercice 3696

Les trois parties I, II, III peuvent être traitées indépendamment les unes des autres.

Partie I

Soit $E = \{1\,;\,2\,;\,3\,;\,4\,;\,5\,;\,6\,;\,7\,;\,8\,;\,9\,;\,10\}$.
Déterminer les paires $\{a\,;\,b\}$ d'entiers distincts de E tels que le reste de la division euclidienne de ab par 11 soit 1.

Partie II

Soit n un entier naturel supérieur ou égal à 3.

1. L'entier $(n-1)!$ est-il pair ?

2. L'entier $(n-1)!+1$ est-il divisible par un entier naturel pair ?

3. Prouver que l'entier $(15-1)!+1$ n'est pas divisible par 15.

4. L'entier $(11-1)!+1$ est-il divisible par 11 ?

Partie III

Soit p un entier naturel non premier $(p\geqslant2)$.

1. Prouver que p admet un diviseur q $(1<q<p)$ qui divise $(p-1)!$

2. L'entier q divise-t-il l'entier $(p-1)!+1$?

3. L'entier p divise-t-il l'entier $(p-1)!+1$?

Correction 3696

Partie A

On a :

- $a=1$:
  ~~$\{1;1\}$~~ ; ~~$\{1;2\}$~~ ; ~~$\{1;3\}$~~ ; ~~$\{1;4\}$~~ ; ~~$\{1;5\}$~~
  ~~$\{1;6\}$~~ ; ~~$\{1;7\}$~~ ; ~~$\{1;8\}$~~ ; ~~$\{1;9\}$~~ ; $\{1;10\}$
- $a=2$:
  ~~$\{2;2\}$~~ ; ~~$\{2;3\}$~~ ; ~~$\{2;4\}$~~ ; ~~$\{2;5\}$~~ ; $\{2;6\}$
  ~~$\{2;7\}$~~ ; ~~$\{2;8\}$~~ ; ~~$\{2;9\}$~~ ; $\{2;10\}$
- $a=3$:
  ~~$\{3;3\}$~~ ; $\{3;4\}$; ~~$\{3;5\}$~~ ; ~~$\{3;6\}$~~ ; ~~$\{3;7\}$~~
  $\{3;8\}$; ~~$\{3;9\}$~~ ; $\{3;10\}$
- $a=4$:
  ~~$\{4;4\}$~~ ; ~~$\{4;5\}$~~ ; ~~$\{4;6\}$~~ ; ~~$\{4;7\}$~~ ; ~~$\{4;8\}$~~
  ~~$\{4;9\}$~~ ; $\{4;10\}$
- $a=5$:
  ~~$\{5;5\}$~~ ; ~~$\{5;6\}$~~ ; ~~$\{5;7\}$~~ ; ~~$\{5;8\}$~~ ; $\{5;9\}$
  ~~$\{5;10\}$~~
- $a=6$:
  ~~$\{6;6\}$~~ ; ~~$\{6;7\}$~~ ; ~~$\{6;8\}$~~ ; ~~$\{6;9\}$~~ ; $\{6;10\}$
- $a=7$:
  ~~$\{7;7\}$~~ ; $\{7;8\}$; ~~$\{7;9\}$~~ ; $\{7;10\}$
- $a=8$:
  ~~$\{8;8\}$~~ ; ~~$\{8;9\}$~~ ; $\{8;10\}$
- $a=9$:
  ~~$\{9;9\}$~~ ; $\{9;10\}$
- $a=10$:
  $\{10;10\}$

La méthode exhaustive a été choisie mais ce n'est pas la seule.

Partie B

1. L'entier $(n-1)!$ s'écrit :
   $(n-1)! = 2\times3\times\cdots\times(n-1)$

   2 est un des facteurs définissant le produit $(n-1)!$ pour n supérieur ou égal à n : $(n-1)!$ est pair.

2. On déduit de la question précédente que $(n-1)!+1$ est un entier impair ; il n'est pas divisible par un entier pair.

3. 3 et 5 sont des facteurs de $(15-1)!$; ainsi, 15 divise $(15-1)!$.

   Supposons que 15 divise $(15-1)!+1$; comme il divise $(15-1)!$, il divise également leur différence :
   $\big[(15-1)!+1\big]-(15-1)!=1$
   Ce qui absurde car 1 n'est pas divisible par 15.

4. Deux méthodes étaient ici possible :
   - On a :
     $(11-1)!+1 = 3\,628\,801$
     On a la division euclidienne suivante :
     $3\,628\,801 = 329\,891\times11+0$
     Le nombre $(11-1)!+1$ est divisible par 11.
   - On a le nombre $(11-1)!$ qui s'ecrit :
     $(11-1)!+1 = 1\times2\times3\times4\times5\times6\times7\times8\times9\times10+1$
     $= (2\times6)\times(3\times4)\times(5\times9)\times(7\times8)\times10+1$
     D'après la question 1. :
     $= 1\times1\times1\times1\times10+1$
     $= 10+1 = 11\equiv0 \pmod{11}$

Partie C

1. p est un nombre non premier ; on en déduit qu'il existe un diviseur q de p tel que :
   $2\leqslant q\leqslant\sqrt{p}$

   On en déduit que $q\in\big[2\,;p-1\big]$; ainsi, q appartient au produit $(p-1)!$.

2. On vient de montrer que q divise $(p-1)!$; ainsi, il existe k tel que :
   $(p-1)! = q\cdot k$

   Ainsi, on peut écrire :
   $(p-1)!+1 = q\cdot k+1$

   Supposons que q divise $(p-1)!+1$, cela signifie que q divise $q\cdot k+1$, or, q divise également leur différence : q divisant 1, on en déduit que $q=1$
   Ce qui est absurde car $q\geqslant2$: $(p+1)!+1$ n'est pas divisible par q.

3. Supposons que p divise $(p-1)!+1$. On a l'existence de r tel que :
   $$\frac{(p-1)!+1}{p} = r$$
   Or p admet la décomposition suivante :
   $p = q\cdot s$
   On a :
   $$\frac{(p-1)!+1}{q\cdot s} = r$$
   $$s\cdot\frac{(p-1)!+1}{q\cdot s} = s\cdot r$$
   $$\frac{(p-1)!+1}{q} = s\cdot r$$
   Ainsi, l'entier q divise $(p-1)!+1$; ceci est en contradiction avec la question 2..

Exercice 5836

On considère l'algorithme suivant où $\text{Ent}\left(\frac{A}{N}\right)$ désigne la partie entière de $\frac{A}{N}$.

```
A et N sont des entiers naturels.
Saisir A.
N prend la valeur 1.
Tant que N≤√A
    Si  A/N − Ent(A/N) = 0  alors
        Afficher N et A/N
    Fin si
N prend la valeur N+1
Fin Tant que.
```

1. Quels résultats affiche cet algorithme pour $A=12$?
2. Que donne cet algorithme dans le cas général ?

Correction 5836

1. Voici les résultats affichées par l'algorithme :
   - `1` et `12` ;
   - `2` et `6` ;
   - `3` et `4`.
2. Cet algorithme permet d'obtenir tous les diviseurs du nombre saisi.

Exercice 3785

Partie A

On admet que 1 999 est un nombre premier. Déterminer l'ensemble des couples $(a\,;b)$ d'entiers naturels admettant pour somme 11 994 et pour $PGCD$ 1 999.

Partie B

On considère l'équation (E) d'inconnu n appartenant à $\mathbb{N}$:

(E) : $n^2 - S{\cdot}n + 11\,994 = 0$ où S est un entier naturel.

On s'intéresse à des valeurs de S telle que (E) admette deux solutions dans $\mathbb{N}$.

1. Peut-on déterminer un entier S tel que 3 soit solution de (E) ?
   Si oui, préciser la deuxième solution.

2. Peut-on déterminer un entier S tel que 5 soit solution de (E) ?

3. Montrer que tout entier n solution de (E) est un diviseur de 11 994.
   En déduire toutes les valeurs possibles de S telles que (E) admette deux solutions entières.

Partie C

Comment montrerait-on que 1 999 est un nombre premier ? Préciser le raisonnement employé ?
La liste de tous les entiers premiers inférieurs à 100 est précisée ci-dessous :

2	;	3	;	5	;	7	;	11	;
13	;	17	;	19	;	23	;	29	;
31	;	37	;	41	;	43	;	47	;
53	;	59	;	61	;	67	;	71	;
73	;	79	;	83	;	89	;	97	

Correction 3785

Partie A

Les entiers a et b admettent pour $PGCD$ l'entier 1 999 ; ainsi, il existe deux entiers k et k', premiers entre eux, tels que :
$a = k \cdot 1\,999$; $b = k' \cdot 1\,999$

Puisque la somme des deux entiers a et b vaut 11 994, on a :

$$\begin{aligned} a + b &= 11\,994 \\ k{\cdot}1\,999 + k'{\cdot}1\,999 &= 11\,994 \\ 1\,999{\cdot}(k + k') &= 11\,994 \\ k + k' &= \frac{11\,994}{1\,999} \\ k + k' &= 6 \end{aligned}$$

Ainsi, les couples $(k\,;k')$ d'entiers premiers entre eux et tels que k+k'=6 sont : $(1\,;5)$; $(5\,;1)$

Les couples $(a\,;b)$ d'entiers naturels admettant pour somme 11 994 et ayant pour $PGCD$ 1 999, on a :
$(1\,999\,;9\,995)$; $(9\,995\,;1\,999)$

Partie B

1. Supposons que 3 est solution, l'entier S vérifie alors l'égalité :

$$\begin{aligned} 3^2 - 3{\cdot}S + 11\,994 &= 0 \\ -3{\cdot}S + 12\,003 &= 0 \\ -3{\cdot}S &= -12\,003 \\ S &= 4\,001 \end{aligned}$$

L'équation (E) s'écrit alors :
(E) : $n^2 - 4\,001{\cdot}n + 11\,994 = 0$
Ce polynôme admet pour discriminant :
$\Delta = b^2 - 4{\cdot}a{\cdot}c = (4\,001)^2 - 4{\times}1{\times}11\,994 = 15\,960\,025$
On a la simplification : $\sqrt{\Delta} = \sqrt{15\,960\,025} = 3\,995$

Le discriminant étant strictement positif, l'équation (E) admet deux racines données par :

$$\begin{aligned} x_1 &= \frac{-b - \sqrt{\Delta}}{2{\cdot}a} \\ &= \frac{-(-4\,001) - 3\,995}{2{\times}1} \\ &= \frac{4\,001 - 3\,995}{2} \\ &= \frac{6}{2} \\ &= 3 \end{aligned} \qquad \begin{aligned} x_2 &= \frac{-b + \sqrt{\Delta}}{2{\cdot}a} \\ &= \frac{-(-4\,001) + 3\,995}{2{\times}1} \\ &= \frac{4\,001 + 3\,995}{2} \\ &= \frac{7996}{2} \\ &= 3998 \end{aligned}$$

La seconde solution de cette équation a pour valeur 3998.

2. Supposons que 5 soit solution de (E) ; ainsi, on a l'égalité suivante :

$$\begin{aligned} 5^2 - S{\cdot}5 + 11\,994 &= 0 \\ 25 - 5{\cdot}S + 11\,994 &= 0 \\ -5{\cdot}S + 12\,019 &= 0 \\ 5{\cdot}S &= 12\,019 \\ S &= \frac{12\,019}{5} \end{aligned}$$

S n'est pas un entier.

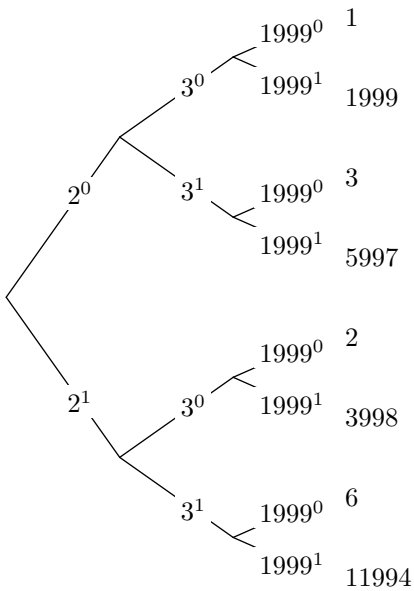
3. Soit n un entier naturel solution de (E), on a l'égalité suivante :

$$\begin{aligned} n^2 - S{\cdot}n + 11\,994 &= 0 \\ n^2 - S{\cdot}n &= -11\,994 \\ n{\cdot}(n - S) &= -11\,994 \end{aligned}$$

Ainsi, un entier n est solution de (E) si, et seulement si, il divise 11 994.

Voici la décomposition en produits de facteurs premiers de l'entier 11 944 :
$11\,994 = 2{\times}3{\times}1\,999$

Ainsi, l'ensemble des diviseurs de 11 994 est donné par l'arbre de choix suivant :



Les valeurs possibles de S sont :
- $n = 1$:

$$1\cdot(1-S) = -11\,994$$
$$-S = -11\,995$$
$$S = 11\,995$$

- $n = 2$:
$$2\cdot(2-S) = -11\,994$$
$$2-S = -5\,997$$
$$S = 5\,999$$

- $n = 3$:
$$3\cdot(3-S) = -11\,994$$
$$3-S = -3\,998$$
$$S = 4\,001$$

- $n = 6$:
$$6\cdot(6-S) = -11\,994$$
$$6-S = -1\,999$$
$$S = 2\,005$$

- $n = 1\,999$:
$$1\,999\cdot(1\,999-S) = -11\,994$$
$$1\,999-S = -6$$
$$S = 2\,005$$

- $n = 3\,998$:
$$3\,998\cdot(3\,998-S) = -11\,994$$
$$3\,998-S = -3$$
$$S = 4\,001$$

- $n = 5\,997$:
$$5\,997\cdot(5\,997-S) = -11\,994$$
$$5\,997-S = -2$$
$$S = 5\,999$$

- $n = 11\,994$:
$$11\,994\cdot(11\,994-S) = -11\,994$$
$$11\,994-S = -1$$
$$S = 11\,995$$

Ainsi, les possibilités pour S sont :
$2\,005$; $4\,001$; $5\,999$; $11\,995$

Partie C

Si $1\,999$ est non-premier, il admet un diviseur premier dans l'intervalle :
$[2\,;\,\sqrt{1\,999}] \subset [2\,;\,45]$

Ainsi, il suffit de tester la divisibilité de $1\,999$ parmi les entiers premiers :
2 ; 3 ; 5 ; 7 ; 11 ; 13 ; 17 ; 19
23 ; 31 ; 37 ; 41 ; 43

Et aucun de ces entiers n'est un diviseur de $1\,999$.

Exercice 3969

Pour chacune des cinq propositions suivantes, indiquer si elle est vraie ou fausse et donner une démonstration de la réponse choisie. Une réponse non démontrée ne rapporte aucun point,

Proposition 1 : Pour tout entier naturel n, 3 divise le nombre $2^{2n}-1$

Proposition 2 : Si un entier relatif x est solution de l'équation $x^2+x \equiv 0 \pmod 6$ alors $x \equiv 0 \pmod 3$

Proposition 3 : L'ensemble des couples d'entiers relatifs $(x\,;y)$ solutions de l'équation $12\cdot x-5\cdot y=3$ est l'ensemble des couples $(4+10\cdot k\,;9+24\cdot k)$ où $k \in \mathbb{Z}$

Proposition 4 : Il existe un seul couple $(a\,;b)$ de nombres entiers naturels, tel que $a<b$ et $PPCM(a\,;b)-PGCD(a\,;b)=1$

Deux entiers naturesl M et N sont tels que M a pour écriture abc en base dix et N a pour écriture bca en base dix.

Proposition 5 : Si l'entier M est divisible par 27 alors l'entier $M-N$ est aussi divisible par 27.

Correction 3969

1. **Vraie :**
On a les égalités et les équivalences suivantes :
$$2^{2n}-1 = \left(2^2\right)^n - 14^n - 1$$
$$\equiv 1^n - 1 \equiv 1-1 \equiv 0 \pmod 3$$

2. **Faux :**
Il suffit de prendre $x=2$:
- x vérifie l'égalité :
$$x^2+x = 2^2+2 = 6 \equiv 0 \pmod 6$$
- Mais, on a :
$$x \equiv 2 \not\equiv 0 \pmod 3$$

Ainsi, $x=2$ est un contre exemple à cette proposition.

3. **Faux :**
Vérifions que le couple $(9\,;21)$ est solution de l'équation :
$$12\cdot x-5\cdot y = 12\times 9-5\times 21$$
$$= 108-105$$
$$= 3$$
Mais, il n'existe pas de $k \in \mathbb{Z}$ tel que :
$$(9\,;21) = (4+10\cdot k\,;9+24\cdot k)$$
Résolvons l'équation :
$$4+10\cdot k = 9$$
$$10\cdot k = 9-4$$
$$10\cdot k = 5$$
$$k = \frac{1}{2}$$
Cette équation n'a donc pas de solution dans $\mathbb{Z}$.

4. **Vrai :**
Notons d le $PGCD$ de a et de b ; on a l'existence de deux entiers k et k' tels que :
$$a = k\cdot d \quad ; \quad b = k'\cdot d$$
On a les deux égalités suivantes :
$$PPCM(a\,;b) = k\cdot k'\cdot d \quad ; \quad PGCD(a\,;b) = d$$
Etudions l'égalité suivante :
$$PPCM(a\,;b) - PGCD(a\,;b) = 1$$
$$k\cdot k'\cdot d - d = 1$$
$$d\cdot(k\cdot k'-1) = 1$$
La dernière égalité nécessite :
- $d=1$
- $k\cdot k'-1=1 \Longrightarrow k\cdot k'=2$

On a $k<k'$, on en déduit nécessairement :
$$k=1 \quad ; \quad k'=2$$
Le seul couple solution de cette égalité est $(1\,;2)$

5. **Vraie :**
Supposons que l'entier M vérifie la relation :

$$M \equiv 0 \pmod{27}$$
$$\overline{abc}^{10} \equiv 0 \pmod{27}$$
$$a\times 10^2 + b\times 10 + c \equiv 0 \pmod{27}$$
$$19\cdot a + 10\cdot b + c \equiv 0 \pmod{27}$$

On a l'égalité suivante :

$$N = \overline{bca}^{10}$$
$$N = b\cdot 10^2 + c\cdot 10 + a$$
$$19\cdot N = 19\cdot\left(b\cdot 10^2 + c\cdot 10 + a\right)$$
$$19\cdot N = 19\cdot\left(b\cdot 19 + c\cdot 10 + a\right)$$
$$19\cdot N = 361\cdot b + 190\cdot c + 19\cdot a$$
$$19\cdot N \equiv 361\cdot b + 190\cdot c + 19\cdot a \pmod{27}$$
$$19\cdot N \equiv 10\cdot b + 1\cdot c + 19\cdot a \pmod{27}$$
$$19\cdot N \equiv 19\cdot a + 10\cdot b + c \pmod{27}$$
$$19\cdot N \equiv M \pmod{27}$$
$$19\cdot N \equiv 0 \pmod{27}$$

On en déduit que le produit $19\cdot N$ est divisible par 27 ; or, les nombres 19 et 27 sont premiers entre eux : d'après le théorème de Gauss,on en déduit que n est divisble par 27.

Exercice 3970

1. Montrer que, pour tout entier naturel non nul k et pour tout entier naturel x :

$$(x-1)\cdot\left(1 + x + x^2 + \cdots + x^{k-1}\right) = x^k - 1$$

Dans toute la suite de l'exercice, on consière un nombre entier a supérieur ou égal à 2.

2. a. Soit n un entier naturel non nul et d un diviseur positif de n :
$n = d\cdot k$
Montrer que $a^d - 1$ est un diviseur de $a^n - 1$.

b. Déduire de la question précédente que $2^{2004} - 1$ est divisible par 7, par 63 puis par 9.

3. Soient m et n deux entiers naturels non nuls et d leur *pgcd*.

a. On définit m' et n' par $m = d\cdot m'$ et $n = d\cdot n'$. En appliquant le théorème de Bezout à m' et n', montrer qu'il existe des entiers relatifs u et v tels que :
$m\cdot u - n\cdot v = d$.

b. On suppose u et v strictement positifs.
Montrer que : $\left(a^{m\cdot u} - 1\right) - \left(a^{n\cdot v} - 1\right)\cdot a^d = a^d - 1$
Montrer ensuite que $a^d - 1$ est le *pgcd* de :
$a^{m\cdot u} - 1$ et $a^{n\cdot v} - 1$

c. Calculer, en utilisant le résultat précédent le *pgcd* de :
$2^{63} - 1$ et $2^{60} - 1$

Correction 3970

1. Démontrons, à l'aide d'un raisonnement par récurrence, que pour tout entier naturel k non nul, on a :
$(x-1)\cdot\left(1 + x + x^2 + \cdots + x^{k-1}\right) = x^k - 1$

- *Initialisation :*
Pour $k = 1$, on a :
- $x^k - 1 = x - 1$
- $(x-1)\cdot\left(1 + x + x^2 + \cdots + x^{k-1}\right) = (x-1)\times 1$

- *Hérédité :*
Supposons la relation vérifiée au rang n. Etablissons cette relation pour le rang suivant :

$$(x-1)\cdot\left(1 + x + x^2 + \cdots + x^{k-1} + x^k\right)$$
$$= (x-1)\cdot\left(1 + x + x^2 + \cdots + x^{k-1}\right) + (x-1)\cdot x^k$$

D'après la relation de récurrence :

$$= \left(x^k - 1\right) + (x-1)\cdot x^k$$
$$= \left(x^k - 1\right) + x^{k+1} - x^k$$
$$= x^{k+1} - 1$$

2. a. On a les égalités suivantes :

$$a^n - 1 = a^{d\cdot k} - 1$$
$$= \left[a^d\right]^k - 1$$

D'après la formule de la question 1. :

$$\left(a^d - 1\right)\cdot\left[1 + a^d + (a^d)^2 + \cdots + (a^d)^{k-1}\right]$$

On vient de voir que $a^n - 1$ est un multiple de $a^d - 1$.

b. La décomposition en facteurs premiers de 2004 donne :

$$\begin{array}{r|l} 2004 & 2 \\ 1002 & 2 \\ 501 & 3 \\ 167 & 167 \\ 1 & \end{array}$$

On a :
$2004 = 2^2\times 3\times 167$

D'après la question précédente, puisque 3 et 6 sont des diviseurs de 2004, on en déduit que les deux nombres suivants sont des diviseurs de $2^{2004} - 1$:

- $2^3 - 1 = 8 - 1 = 7$
- $2^6 - 1 = 64 - 1 = 63$

Ainsi, les nombres 7 et 63 sont des diviseurs de $2^{2004} - 1$. Or, le nombre 9 est un diviseur, on en déduit que 9 est également un diviseur de $2^{2004} - 1$.

3. a. Les nombres m' et n' sont premieres entre eux ; on en déduit d'après le théorème de Bezout, l'existence de deux entiers u et v tels que :

$$u\cdot m' - v\cdot n' = 1$$

On en déduit :

$$d\cdot\left[u\cdot m' - v\cdot n'\right] = d\times 1$$
$$d\cdot u\cdot m' - d\cdot v\cdot n'\big] = d$$
$$u\cdot\left[d\cdot m'\right] - v\cdot\left[d\cdot n'\right] = d$$
$$u\cdot m - v\cdot n = d$$

b. On a le développement suivant :

$$\begin{aligned}&\left(a^{m\cdot u}-1\right)-\left(a^{n\cdot v}-1\right)\cdot a^d\\&=a^{m\cdot u}-1-a^{n\cdot v}\cdot a^d+1\cdot a^d\\&=a^{m\cdot u}-1-a^{n\cdot v+d}+a^d\end{aligned}$$

D'après la question précédente :

$$\begin{aligned}&=a^{m\cdot u}-1-a^{m\cdot u+a^d}\\&=a^d-1\end{aligned}$$

Notons D le *pgcd* de $a^{m\cdot u}-1$ et $a^{n\cdot v}-1$.

D'après la question 2., puisque d est le *pgcd* de m et de n, à fortiori, il divise $u\cdot m$ et $v\cdot n$.

On en déduit que a^d-1 divise $a^{m\cdot u}-1$ et $a^{n\cdot v}-1$; étant un diviseur commun, on en déduit que a^d-1 divise D.

D divisant les deux termes $a^{m\cdot u}-1$ et $a^{n\cdot v}-1$, on en déduit qu'il divise la différence :

$$\left(a^{m\cdot u}-1\right)-\left(a^{n\cdot v}-1\right)\cdot a^d$$

on en déduit que D divise a^d-1.

c. Les nombres 60 et 63 admettent 3 comme *pgcd* et on a la relation :

$$1\times 63-1\times 60=3$$

Ainsi, en utilisant la propriété de la question précédente, on obtient que le *pgcd* de ces deux nombres a pour valeur :

$$2^d-1=2^3-1=8-1=7.$$

Exercice 5471

Partie A : Restitution organisée de connaissance

Soit a, b, c, d des entiers relatifs et n un entier naturel non nul.

Montrer que si $a\equiv b \pmod{n}$ et si $c\equiv d \pmod{n}$ alors $ac\equiv bd \pmod{n}$.

Partie B : Inverse de 23 modulo 26

On considère l'équation : (E) : $23x-26y=1$ où x et y désignent deux entiers relatifs.

1. Vérifier que le couple $(-9\,;-8)$ est solution de l'équation (E).
2. Résoudre alors l'équation (E).
3. En déduire un entier a tel que :
$0\leqslant a\leqslant 25$; $23a\equiv 1 \pmod{26}$

Partie C : Chiffrement de Hill

On veut coder un mot de deux lettres selon la procédure suivante :

- **Etape 1** Chaque lettre du mot est remplacé par un entier en utilisant le tableau ci-dessous :

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

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

On obtient un couple d'entiers $(x_1\,;x_2)$ où x_1 correspond à la première lettre du mot et x_2 correspond à la deuxième lettre du mot.

- **Etape 2** $(x_1\,;x_2)$ est transformé en $(y_1\,;y_2)$ tel que :

$$(\mathcal{S}_1):\begin{cases}y_1\equiv 11x_1+3x_2 \pmod{26}\\ y_2\equiv 7x_1+4x_2 \pmod{26}\end{cases}$$

avec $0\leqslant y_1\leqslant 25$ et $0\leqslant y_2\leqslant 25$

- **Etape 3** $(y_1\,;y_2)$ est transformé en un mot de deux lettres en utilisant le tableau de correspondance donné dans l'étape 1.

Exemple :

$$\underbrace{\text{TE}}_{\text{mot en clair}} \overset{\text{étape 1}}{\Longrightarrow} (19\,;4) \overset{\text{étape 2}}{\Longrightarrow} (13\,;19) \overset{\text{étape 3}}{\Longrightarrow} \underbrace{\text{NT}}_{\text{mot codé}}$$

1. Coder le mot ST.
2. On veut maintenant déterminer la procédure de décodage :

a. Montrer que tout couple $(x_1\,;x_2)$ vérifiant les équations du système $(\mathcal{S}_1)$, vérifie les équations du système :

$$(\mathcal{S}_2):\begin{cases}23x_1\equiv 4y_1+23y_2 \pmod{26}\\ 23x_2\equiv 19y_1+11y_2 \pmod{26}\end{cases}$$

b. A l'aide de la partie **B**, montrer que tout couple $(x_1\,;x_2)$ vérifiant les équations du système $(\mathcal{S}_2)$, vérifie les équations du système :

$$(S_3):\begin{cases}x_1\equiv 16y_1+y_2 \pmod{26}\\ x_2\equiv 11y_1+5y_2 \pmod{26}\end{cases}$$

c. Montrer que tout couple $(x_1\,;x_2)$ vérifiant les équations du système $(\mathcal{S}_3)$, vérifie les équations du système $(\mathcal{S}_1)$.

d. Décoder le mot YJ

Correction 5471

Partie A

Considérons quatre entiers a, b, c et d vérifiant les deux relations suivantes :

$$a\equiv b \pmod{n} \quad ; \quad c\equiv d \pmod{n}$$

Des relations de congruences précédentes, on en déduit l'existence de deux entiers relatifs k et k' vérifiant les égalités suivantes :

$$a=b+k\cdot n \quad ; \quad c=d+k'\cdot n$$

Déterminons une expression du produit de a par c :

$$\begin{aligned}a\cdot c&=\left(b+k\cdot n\right)\left(d+k'\cdot n\right)=b\cdot d+b\cdot k'\cdot n+d\cdot k\cdot n+k\cdot k'\cdot n^2\\&=b\cdot d+n\cdot\left(b\cdot k'+d\cdot k+k\cdot k'\cdot n\right)\equiv b\cdot d \pmod{n}\end{aligned}$$

Partie B

1. Vérifions que le couple $(-9\,;-8)$ est solution de l'équation :

$$\begin{aligned}23x-26y&=23\times(-9)-26\times(-8)=-207-(-208)\\&=-207+208=1\end{aligned}$$

2. Considérons $(x\,;y)$ un couple solution de l'équation (E). On a les deux égalités :

$$23x-26y=1 \quad ; \quad 23\times(-9)-26\times(-8).$$

On en déduit l'égalité :

$$\begin{aligned}23x-26y&=23\times(-9)-26\times(-8)\\23x-26y&=-23\times 9+26\times 8\\23x+23\times 9&=26y+26\times 8\\23(x+9)&=26(y+8)\end{aligned}$$

On en déduit que 23 est un diviseur du produit $26(y+8)$. Or, le nombre 23 étant un nombre premier, on en déduit que les nombres 23 et 26 sont premiers entre eux.

D'après le corollaire du théorème de Gauss, on en déduit que 23 est un diviseur de $y+8$. On en déduit l'existence d'un nombre k vérifiant :

$$y+8 = 23{\cdot}k$$
$$y = 23{\cdot}k - 8$$

En utilisant l'équation (E), on obtient l'expression de x :

$$\begin{aligned}
23x - 26y &= 1\\
23x - 26{\cdot}\big(23{\cdot}k - 8\big) &= 1\\
23x - 26{\times}23{\cdot}k + 26{\times}8 &= 1\\
23x - 26{\times}23{\cdot}k + 208 &= 1\\
23\big(x - 26{\cdot}k\big) &= 1 - 208\\
23\big(x - 26{\cdot}k\big) &= -207\\
x - 26{\cdot}k &= \frac{-207}{23}\\
x - 26{\cdot}k &= -9\\
x &= -9 + 26{\cdot}k
\end{aligned}$$

On vient de montrer que tout couple solution de l'équation (E) admet pour expression $\big(-9+26{\cdot}k\,;\,-8+23{\cdot}k\big)$

Vérifions maintenant que tout couple de cette forme est solution de (E) :

$$\begin{aligned}
&23{\cdot}\big(-9+26{\cdot}k\big) - 26{\cdot}\big(-8+23{\cdot}k\big)\\
&= -207 + 598{\cdot}k + 208 - 598{\cdot}k = 1
\end{aligned}$$

3. Soit a un entier vérifiant la relation de congruence :

$$23a \equiv 1 \pmod{26}$$

Ainsi, il existe un entier relatif k tel que :

$$23a = 1 + k{\cdot}26$$
$$23a - k{\cdot}26 = 1$$

Ainsi, le couple $\big(a\,;k\big)$ est solution de l'équation (E). On en déduit l'existence d'un entier k' tel que :

$$a = -9 + k'{\cdot}26.$$

On remarque que pour k'=1, on a :

$$a = -9 + 1{\times}26 = -9 + 26 = 17$$

17 est la valeur recherchée.

Partie C

1. La lettre S est codée par le nombre 18 et la lettre T est codée par le nombre 20.
Ainsi, dans le codage du mot ST, on a les valeurs suivantes de x_1 et x_2 :

$$x_1 = 18 \quad ; \quad x_2 = 20$$

Ainsi, le système (S_1) donne les valeurs de y_1 et y_2 :

$$\begin{cases} y_1 \equiv 11x_1{+}3x_2 \pmod{26}\\ y_2 \equiv 7x_1{+}4x_2 \pmod{26}\end{cases} \Longrightarrow \begin{cases} y_1 \equiv 11{\times}18{+}3{\times}20 \pmod{26}\\ y_2 \equiv 7{\times}18{+}4{\times}20 \pmod{26}\end{cases}$$

$$\Longrightarrow \begin{cases} y_1 \equiv 198+60 \pmod{26}\\ y_2 \equiv 126+80 \pmod{26}\end{cases} \Longrightarrow \begin{cases} y_1 \equiv 258 \pmod{26}\\ y_2 \equiv 246 \pmod{26}\end{cases}$$

$$\Longrightarrow \begin{cases} y_1 \equiv 9{\times}26+24 \pmod{26}\\ y_2 \equiv 9{\times}26+12 \pmod{26}\end{cases}$$

On a : $y_1 = 24 \quad ; \quad y_2 = 12$
Ces deux nombres codent respectivement les deux lettres Y et M.

2. a. Considérons deux couples $(x_1\,;x_2)$ et $(y_1\,;y_2)$ vérifiant le système $(\mathcal{S}_1)$:

- $\begin{cases} y_1 \equiv 11x_1 + 3x_2 \pmod{26}\\ y_2 \equiv 7x_1 + 4x_2 \pmod{26}\end{cases}$

$$\Longrightarrow \begin{cases} 4y_1 \equiv 44x_1 + 12x_2 \pmod{26}\\ 3y_2 \equiv 21x_1 + 12x_2 \pmod{26}\end{cases}$$

Par soustraction de la première ligne par la seconde :

$$4y_1 - 3y_2 \equiv 23{\cdot}x_1 \pmod{26}$$
$$23{\cdot}x_1 \equiv 4y_1 - 3y_2 \pmod{26}$$

- $\begin{cases} y_1 \equiv 11x_1 + 3x_2 \pmod{26}\\ y_2 \equiv 7x_1 + 4x_2 \pmod{26}\end{cases}$

$$\Longrightarrow \begin{cases} 7y_1 \equiv 77x_1 + 21x_2 \pmod{26}\\ 11y_2 \equiv 77x_1 + 44x_2 \pmod{26}\end{cases}$$

Par soustraction de la première ligne par la seconde :

$$7y_1 - 11y_2 \equiv 21x_2 - 44x_2 \pmod{26}$$
$$7y_1 - 11y_2 \equiv -23x_2 \pmod{26}$$
$$23x_2 \equiv -7y_1 + 11y_2 \pmod{26}$$
$$23x_2 \equiv 19y_1 + 11y_2 \pmod{26}$$

On en déduit l'existence du système suivant :

$$(\mathcal{S}_2) : \begin{cases} 23x_1 \equiv 4y_1 + 23y_2 \pmod{26}\\ 23x_2 \equiv 19y_1 + 11y_2 \pmod{26}\end{cases}$$

b. Lors de la partie **B**, on a trouvé le nombre 17 vérifiant :

$$17{\times}23 = \equiv 1 \pmod{26}$$

Le système $(\mathcal{S}_2)$ admet pour expression :

$$\begin{cases} 23x_1 \equiv 4y_1 + 23y_2 \pmod{26}\\ 23x_2 \equiv 19y_1 + 11y_2 \pmod{26}\end{cases}$$

Multiplions chaque équation par 17 :

$$\Longrightarrow \begin{cases} 17{\times}23x_1 \equiv 17{\times}(4y_1 + 23y_2) \pmod{26}\\ 17{\times}23x_2 \equiv 17{\times}(19y_1 + 11y_2) \pmod{26}\end{cases}$$

$$\Longrightarrow \begin{cases} 17{\times}23x_1 \equiv 68y_1 + 17{\times}23y_2 \pmod{26}\\ 17{\times}23x_2 \equiv 323y_1 + 187y_2 \pmod{26}\end{cases}$$

Par congruence des coefficients :

$$\Longrightarrow \begin{cases} x_1 \equiv 16y_1 + y_2 \pmod{26}\\ x_2 \equiv 11y_1 + 5y_2 \pmod{26}\end{cases}$$

On obtient le système $(\mathcal{S}_3)$ recherchée.

c. Considérons un couple $(x_1\,;x_2)$ solution du système $(\mathcal{S}_3)$. On a les deux équivalences suivantes :
$x_1 \equiv 16y_1 + y_2 \pmod{26}$; $x_2 \equiv 11y_1 + 5y_2 \pmod{26}$
Montrons que ce couple est solution du système :

- $$\begin{aligned} 11{\cdot}x_1 + 3{\cdot}x_2 &\equiv 11{\cdot}\big(16y_1 + y_2\big) + 3{\cdot}\big(11y_1 + 5y_2\big)\\ &\equiv 176y_1 + 11y_2 + 33y_1 + 15y_2 \equiv 209y_1 + 26y_2\\ &\equiv y_1 \pmod{26}\end{aligned}$$
- $$\begin{aligned} 7{\cdot}x_1 + 4{\cdot}x_2 &\equiv 7{\cdot}\big(16y_1 + y_2\big) + 4{\cdot}\big(11y_1 + 5y_2\big)\\ &\equiv 112y_1 + 7y_2 + 44y_1 + 20y_2 \equiv 156y_1 + 27y_2\\ &\equiv y_2 \pmod{26}\end{aligned}$$

On vient de montrer que un couple solution du système $(\mathcal{S}_3$ est aussi solution du système $(\mathcal{S}_2)$.

d. Les lettres Y et J sont codés respectivement par les nombres 24 et 9. Pour décoder le mot YJ prenant les valeurs suivantes :

$$y_1 = 24 \quad ; \quad y_2 = 9$$

Déterminons les valeurs de x_1 et x_2 solutions de $(\mathcal{S}_3)$:

- $$\begin{aligned} x_1 &\equiv 16y_1 + y_2 \equiv 16{\times}24 + 9 \equiv 384 + 9\\ &\equiv 393 \equiv 19 \pmod{26}\end{aligned}$$
- $$\begin{aligned} x_2 &\equiv 11y_1 + 5y_2 \equiv 11{\times}24 + 5{\times}9 \equiv 264 + 45\\ &\equiv 309 \equiv 23 \pmod{26}\end{aligned}$$

Ainsi, le couple $\big(19\,;23\big)$ est solution du système $(\mathcal{S}_3)$. D'après la question précédente, ce couple est également solution de $(\mathcal{S}_1)$. Ainsi, le mot YJ se décode en TX.

