EXERCICE 5

Dans cet exercice, on pourra utiliser le résultat suivant :

"*Etant donnés deux entiers naturels, a et b non nuls, si $pgcd\,(a\,;b)=1$ alors $pgcd\,(a^2\,;b^2)=1$*"

Une suite (S_n) est définie pour $n>0$ par : $S_n=\sum_{p=1}^{n}p^3$.

On se propose de calculer, pour tout entier naturel non nul n, le plus grand commun diviseur de S_n et S_{n+1}.

1. Démontrer que, pour tout $n>0$, on a :
$$S_n=\left[\frac{n(n+1)}{2}\right]^2$$

2. Etude du cas où n est pair. Soit k l'entier naturel non nul tel que $n=2k$

   a. Démontrer que :
   $\text{pgcd}\,(S_{2k}\,;S_{2k+1})=(2k+1)^2\cdot\text{pgcd}\,\left(k^2\,;(k+1)^2\right)$.

   b. Calculer $\text{pgcd}\,(k\,;k+1)$.

   c. Calculer $\text{pgcd}\,(S_{2k}\,;S_{2k+1})$.

3. Etude du cas où n est impair. Soit k l'entier naturel non nul tel que $n=2k+1$.

   a. Démontrer que les entiers $2k+1$ et $2k+3$ sont premiers entre eux.

   b. Calculer $\text{pgcd}\,(S_{2k+1}\,;S_{2k+2})$.

4. Déduire des questions précédentes qu'il existe une unique valeur de n, que l'on déterminera, pour laquelle S_n et S_{n+1} sont premiers entre eux.

Correction

1. Montrons, à l'aide d'un raisonnement par récurrence, que pour tout entier naturel non-nul, on a la relation :
$$S_n=\left[\frac{n(n+1)}{2}\right]^2$$
   - **Initialisation :**
   Etudions la cas $n=1$:
   $S_n=\sum_{p=1}^{1}p^3=1^3$
   $\left[\frac{n(n+1)}{2}\right]^2=\left[\frac{1(1+1)}{2}\right]^2=\left(\frac{2}{2}\right)^2=1$
   - **Hérédité :**
   Supposons la relation vérifiée au rang n ; montrons que la relation est également vraie au rang $(n+1)$:
   Par définition, on a l'égalité :
$$S_{n+1}=\sum_{p=1}^{n+1}p^3=1^3+2^3+3^3+\cdots+n^3+(n+1)^3$$
$$=S_n+(n+1)^3=\left[\frac{n\cdot(n+1)}{2}\right]^2+(n+1)^3$$
$$=\frac{n^2\cdot(n+1)^2}{4}+(n+1)^3=\frac{n^2\cdot(n+1)^2+4\cdot(n+1)^3}{4}$$
$$=\frac{(n+1)^2\cdot\left[n^2+4(n+1)\right]}{4}=\frac{(n+1)^2\cdot(n^2+4n+4)}{4}$$
$$=\frac{(n+1)^2\cdot(n+2)^2}{4}=\left[\frac{(n+1)\cdot(n+2)}{2}\right]^2$$
   La relation est vérifiée au rang $(n+1)$.
   - **Conclusion :**
   La propriété s'initialise au rang 1 et elle vérifie la propriété d'hérédité. A l'aide du raisonnement par récurrence, on en déduit que la propriété est vrai pour tout entier naturel non-nul.

2. a. On remarque les deux égalités suivantes
   - $S_{2k}=\left[\frac{2k\cdot(2k+1)}{2}\right]^2=\left[k\cdot(2k+1)\right]^2$
   $=k^2\cdot(2k+1)^2$
   - $S_{2k+1}=\left[\frac{(2k+1)\cdot(2k+2)}{2}\right]^2=\left[\frac{(2k+1)\cdot2\cdot(k+1)}{2}\right]^2$
   $=\left[(2k+1)\cdot(k+1)\right]^2=(2k+1)^2\cdot(k+1)^2$

   Ainsi, on a :
   $\text{pgcd}\,(S_{2k}\,;S_{2k+1})$
   $=\text{pgcd}\,\left(k^2\cdot(2k+1)^2\,;(2k+1)^2\cdot(k+1)^2\right)$
   D'après les propriétés du PGCD, on a :
   $=(2k+1)^2\cdot\text{pgcd}\,\left(k^2\,;(k+1)^2\right)$

   b. k est un entier naturel non-nul ; notons :
   $d=\text{pgcd}\,(k\,;k+1)$
   d divisant les entiers k et $k+1$ alors il divise la différence de ces deux termes ; on en déduit que d divise 1.
   On en déduit :
   $d=1$

   c. D'après la question précédente, on a :
   $\text{pgcd}\,(k\,;k+1)=1$
   En utilisant la propriété citée dans l'énoncé, on en déduit :
   $\text{pgcd}\,\left(k^2\,;(k+1)^2\right)=1$
   En utilisant la question a. :
   $\text{pgcd}\,(S_{2k}\,;S_{2k+1})=(2k+1)^2\cdot\text{pgcd}\,\left(k^2\,;(k+1)^2\right)$
   $=(2k+1)^2\cdot1=(2k+1)^2$

3. a. Notons $d=\text{pgcd}\,(2k+1\,;2k+3)$. d divise les deux termes $2k+1$ et $2k+3$ alors il divise également leurs soustractions :
   d divise $(2k+3)-(2k+1)$
   Donc,
   d divise 2

   Ainsi, d vaut 1 ou 2 ; or, d divise $2k+1$ est impair : on en déduit $d=1$.

   b. On a les deux valeurs :
   - $S_{2k+1}=\left[\frac{(2k+1)(2k+2)}{2}\right]^2=\left[\frac{(2k+1)\cdot2\cdot(k+1)}{2}\right]^2$
   $=\left[(2k+1)(k+1)\right]^2=(2k+1)^2(k+1)^2$
   - $S_{2k+2}=\left[\frac{(2k+2)(2k+3)}{2}\right]^2=\left[\frac{2\cdot(k+1)\cdot(2k+3)}{2}\right]^2$
   $=\left[(k+1)(2k+3)\right]^2=(k+1)^2(2k+3)^2$

   On a les égalités suivantes :
   $\text{pgcd}\,(S_{2k+1}\,;S_{2k+2})$
   $=\text{pgcd}\,\left((2k+1)^2(k+1)^2\,;(k+1)^2(2k+3)^2\right)$
   A l'aide des propriétés du $PGCD$, on a :
   $=(k+1)^2\cdot\text{pgcd}\,\left((2k+1)^2\,;(2k+3)^2\right)$
   D'après la propriété de l'énoncé, on a l'implication :
   $\text{pgcd}\,(2k+1\,;2k+3)=1$
   $\text{pgcd}\,\left((2k+1)^2\,;(2k+3)^2\right)=1$

On en déduit la valeur suivante du $PGCD$:

$$\begin{aligned}&\text{pgcd}\left(S_{2k+1}\,;S_{2k+2}\right)\\&=(k+1)^2\cdot\text{pgcd}\left((2k+1)^2\,;(2k+3)^2\right)\\&=(k+1)^2\cdot 1=(k+1)^2\end{aligned}$$

4. • Si n est pair et non-nul, il existe k non-nul tel que $n=2\cdot k$:

$$\begin{aligned}&\text{pgcd}\left(S_n\,;S_{n+1}\right)=\text{pgcd}\left(S_{2k}\,;S_{2k+1}\right)\\&=(2k+1)^2\end{aligned}$$

Or, $k\geqslant 1$ entraîne que $(2k+1)^2$ est différent de 1.

• Si n est impair et non-nul, il existe k un entier naturel tel que $n=2\cdot k+1$:

$$\begin{aligned}&\text{pgcd}\left(S_n\,;S_{n+1}\right)=\text{pgcd}\left(S_{2k+1}\,;S_{2k+2}\right)\\&=(k+1)^2\end{aligned}$$

Pour $k=0$, $(k+1)^2$ vaut 1

On en déduit que seul les termes S_1 et S_2 sont premiers entre eux.

VERS L'EXERCICE 3

EXERCICE 3

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

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 transitivité 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. Montrons par récurrence qu'on a la propriété suivante pour tout entier naturel n :
$2 \cdot u_n = 5^{n+2} + 3$
- **Initialisation :**
On remarque que :
$\Rightarrow 2 \cdot u_0 = 2 \times 14 = 28$
$\Rightarrow 5^{0+2} + 3 = 5^2 + 3 = 28$
La propriété est vérifiée au rang 0.
- **Hérédité :**
On suppose la relation vraie au rang n, ainsi on a :
$2 \cdot u_n = 5^{n+2} + 3$
Montrons que la relation est également vraie au rang suivant :
$$\begin{aligned} 2 \cdot u_{n+1} &= 2 \cdot (5 \cdot u_n - 6) = 10 \cdot u_n - 12 \\ &= 5 \cdot (2 \cdot u_n) - 12 = 5 \cdot (5^{n+2} + 3) - 12 \\ &= 5 \times 5^{n+2} + 15 - 12 = 5^{n+3} + 3 \end{aligned}$$
- **Conclusion :**
La propriété est initialisée au rang 0 et elle vérifie la propriété d'hérédité. Par un raisonnement par récurrence, on vient de montrer que :
$u_n = 5^{n+2} + 3$

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 $(n + 1)$:
$$\begin{aligned} 2 \cdot u_{n+1} &= 5^2 \cdot (5^{n+1} - 1) \\ &= 5^2 \cdot (5^{n+1} - 5^n + 5^n - 1) \\ &= 25 \cdot \left[5^n \cdot (5 - 1) + 5^n - 1\right] \\ &= 25 \cdot \left[5^n \cdot (5 - 1)\right] + 25 \cdot (5^n - 1) \\ &= 25 \cdot 5^n \cdot 4 + 25 \cdot (5^n - 1) \\ &= 100 \times 5^n \cdot 4 + 25 \cdot (5^n - 1) \\ &\equiv 0 \times 5^n \cdot 4 + 25 \cdot (5^n - 1) \pmod{100} \\ &\equiv 25 \cdot (5^n - 1) \pmod{100} \end{aligned}$$
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 :
$2 \cdot u_n = 100 \cdot k + 28$
$u_n = 50 \cdot k + 14$
Or :
- si k est pair : $u_n = 100 \cdot k' + 14$
- si k est impair : $u_n = (50 + 100 \cdot k') + 14 = 100 \cdot k' + 64$

Ainsi, les deux derniers chiffres des termes de la suite (u_n) ne peuvent avoir comme valeur que 14 et 64

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

On a montré, à la question 2., que les termes de la suite (u_n) 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 (u_n) ; on utilisera la propriété suivante du $PGCD$ de deux entiers naturels a et b :

$\text{pgcd}(a\,;b) = \text{pgcd}(b\,;r)$

où r est le reste de la division euclidienne de a par b.

On a, pour tout entier naturel n :

$d = \text{pgcd}(5{\cdot}u_n - 6\,;u_n)$

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

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

Ainsi, d divise u_n et d divise $u_n - 6$. On en déduit que d divise :

$u_n - (u_n - 6) = 6$

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

$d = 2 \quad ; \quad d = 6$

Montrons par un raisonnement par l'absurde que $\text{pgcd}(u_{n+1}\,;u_n)$ 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

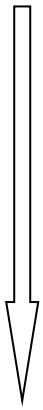
$\Longrightarrow 5^{n+2}$ est un multiple de 3

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 :

$d = 2$.

VERS L'EXERCICE 4



EXERCICE 4

Dans cet exercice, a et b désignent des entiers strictement positifs.

1. a. Démontrer que s'il existe deux entiers relatifs u et v tels que $au + bv = 1$ alors les nombres a et b sont premiers entre eux.

   b. En déduire que si $(a^2 + ab - b^2)^2 = 1$, alors a et b sont premiers entre eux.

2. On se propose de déterminer les couples d'entiers strictement positifs $(a\,;b)$ tels que $(a^2 + ab - b^2)^2 = 1$. Un tel couple sera appelé solution.

   a. Déterminer a lorsque $a = b$.

   b. Vérifier que $(1\,;1)$, $(2\,;3)$ et $(5\,;8)$ sont trois solutions particulières.

   c. Montrer que si $(a\,;b)$ est solution et si $a < b$, alors $a^2 - b^2 < 0$.

3. a. Montrer que si $(x\,;y)$ est une solution différente de $(1\,;1)$ alors $(y - x\,;x)$ et $(y\,;y + x)$ sont aussi des solutions.

   b. Déduire de 2. b. trois nouvelles solutions.

4. On considère la suite de nombres entiers strictement positifs $(a_n)_n$ définie par $a_0 = a_1 = 1$ et pour tout entier n, $n \geqslant 0$:
   $a_{n+2} = a_{n+1} + a_n$.
   Démontrer que pour tout entier $n \geqslant 0$, $(a_n\,;a_{n+1})$ est solution.
   En déduire que les nombres a_n et a_{n+1} sont premiers entre eux.

Correction

1. a. Supposons l'existence de deux entiers relatifs u et v tels que :
   $a\cdot u + b\cdot v = 1$
   Notons d le $PGCD$ des entiers a et b. On a :
   - d divise $a \Longrightarrow$ d divise $u\cdot a$;
   - d divise $b \Longrightarrow$ d divise $v\cdot b$.

   On en déduit que d divise la somme des deux termes $a\cdot u$ et $b\cdot v$: d divise $a\cdot u + b\cdot v$.
   Puisque $a\cdot u + b\cdot v = 1$, on en déduit que d divise 1 : les entiers a et b sont donc premiers entre eux.

   b. On a le développement suivant :

$$\begin{aligned}&(a^2 + a\cdot b - b^2)^2\\ &= (a^2 + a\cdot b - b^2)\cdot(a^2 + a\cdot b - b^2)\\ &= a^4 + a^3\cdot b - a^2\cdot b^2 + a^3\cdot b + a^2\cdot b^2 - a\cdot b^3 - a^2\cdot b^2 - a\cdot b^3 + b^4\\ &= a^4 + 2\cdot a^3\cdot b - a^2\cdot b^2 - 2\cdot a\cdot b^3 + b^4\\ &= a\cdot(a^3 + 2\cdot a^2\cdot b) + b\cdot(-a^2\cdot b - 2\cdot a\cdot b^2 + b^3)\end{aligned}$$

   De l'égalité :
   $(a^2 + a\cdot b - b^2)^2 = 1$
   On en déduit que :
   $a\cdot(a^3 + 2\cdot a^2\cdot b) + b\cdot(-a^2\cdot b - 2\cdot a\cdot b^2 + b^3) = 1$
   D'après le théorème de Bezout, on en déduit que les entiers a et b sont premiers entre eux.

2. a. Supposons que $(a\,;b)$ est solution et que $a = b$, on a :
   $(a^2 + a\cdot b - b^2)^2 = 1$
   On a : $a = b$
   $(a^2 + a\cdot a - a^2)^2 = 1$
   $(a^2)^2 = 1$
   $a^4 = 1$
   Ainsi, l'entier a a pour valeur 1 ou -1 ; l'énoncé précise que $(a\,;b)$ est un couple d'entiers positifs ; on en déduit :
   $a = b = 1$.

   b. • Vérifions que $(1\,;1)$ est solution :
   $(a^2 + a\cdot b - b^2)^2 = (1^2 + 1\cdot 1 - 1^2)^2$
   $= 1^2 = 1$
   • Vérifions que $(2\,;3)$ est solution :
   $(a^2 + a\cdot b - b^2)^2 = (2^2 + 2\cdot 3 - 3^2)^2$
   $= (4 + 6 - 9)^2 = 1^2 = 1$
   • Vérifions que $(5\,;8)$ est solution :
   $(a^2 + a\cdot b - b^2)^2 = (5^2 + 5\cdot 8 - 8^2)^2$
   $= (25 + 40 - 64)^2 = 1^2 = 1$

   c. On a :
   $a < b$
   Ces deux entiers sont strictement positifs :
   $0 < a < b$
   La fonction carré est strictement croissante sur $\mathbb{R}$:
   $a^2 < b^2$

3. a. Soit $(x\,;y)$ un couple de solution :
   • Vérifions que le couple $(y - x\,;x)$ est solution :

$$(a^2 + a\cdot b - b^2)^2 = \left[(y - x)^2 + (y - x)\cdot x - x^2\right]^2$$
$$= (y^2 - 2\cdot y\cdot x + x^2 + y\cdot x - x^2 - x^2)^2 = (y^2 - y\cdot x - x^2)^2$$
$$= \left[-(x^2 + y\cdot x - y^2)\right]^2 = (x^2 + y\cdot x - y^2)^2 = 1$$

   • Vérifions que le couple $(y\,;y + x)$ est solution :

$$(a^2 + a\cdot b - b^2)^2 = \left[y^2 + y\cdot(y + x) - (y + x)^2\right]^2$$
$$= (y^2 + y^2 + y\cdot x - y^2 - 2\cdot y\cdot x - x^2)^2 = (y^2 - y\cdot x - x^2)^2$$
$$= \left[-(y^2 - y\cdot x - x^2)\right]^2 = (y^2 - y\cdot x - x^2)$$

   b. • Du fait que le couple $(2\,;3)$ est solution, on en déduit que les couples suivants sont également solutions :
   ⇨ $(3 - 2\,;2) = (1\,;2)$
   ⇨ $(3\,;2 + 3) = (3\,;5)$
   • Du fait que le couple $(5\,;8)$ est solution, d'après la question précédente, les deux couples suivants sont également solutions :
   ⇨ $(8 - 5\,;5) = (3\,;5)$
   ⇨ $(8\,;8 + 5) = (8\,;13)$

4. Montrons, à l'aide d'un raisonnement par récurrence, que pour tout entier naturel n, on a la propriété :
   $(a_n\,;a_{n+1})$ est solution.
   • *Initialisation :*
   Pour $n = 0$, $(a_0\,;a_1) = (1\,;1)$ est solution.
   La relation est vérifiée au rang n.
   • *Hérédité :*
   Supposons que la relation est vraie au rang n ; mon-

trons que cette relation est vraie au rang n :

Au rang $(n+1)$, on considère le couple $(a_{n+1}\,;a_{n+2})$.

On a :

$$(a^2+a\cdot b-b^2)^2=(a_{n+1}^2+a_{n+1}\cdot a_{n+2}-a_{n+2}^2)^2$$

$$=\left[a_{n+1}^2+a_{n+1}\cdot(a_{n+1}+a_n)-(a_{n+1}+a_n)^2\right]^2$$

$$=(a_{n+1}^2+a_{n+1}^2+a_{n+1}\cdot a_n-a_{n+1}^2-2\cdot a_{n+1}\cdot a_n-a_n^2)^2$$

$$=(a_{n+1}^2-a_{n+1}\cdot a_n-a_n^2)^2$$

$$=\left[-(a_n^2+a_{n+1}\cdot a_n-a_{n+1}^2)\right]^2$$

$$=(a_n^2+a_n\cdot a_{n+1}-a_{n+1}^2)^2$$

Par hypothèse de récurrence : $(a_n\,;a_{n+1})$ est solution :

$=1$

On vient de montrer que $(a_{n+1}\,;a_{n+2})$ est solution ; la relation est vraie au rang $(n+1)$.

On bient de montrer entre que pour tout entier n, le couple $(a_n\,;a_{n+1})$ est solution.

D'après la question 1. b. , tout couple d'entiers solution sont premiers entre eux.

VERS L'EXERCICE 9

EXERCICE 9

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

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. $2003 = 16\times123 + 35$

   ii. $123 = 3\times35 + 18$

   iii. $35 = 1\times18 + 17$

   iv. $18 = 1\times17 + 1$

   v. $17 = 17\times1 + 0$

   En notant $a = 2003$ et $b = 123$:

   i. $2003 = 16\times123 + 35$
   $a = 16\cdot b + 35$
   $a - 16\cdot b = 35$
   $35 = a - 16\cdot b$

   ii. $123 = 3\times35 + 18$
   $b = 3\times(a - 16\cdot b) + 18$
   $b = 3\cdot a - 48\cdot b + 18$
   $-3\cdot a + 49\cdot b = 18$
   $18 = -3\cdot a + 49\cdot b$

   iii. $35 = 1\times18 + 17$
   $(a - 16\cdot b) = 1\times(-3\cdot a + 49\cdot b) + 17$
   $a - 16\cdot b = -3\cdot a + 49\cdot b + 17$
   $4\cdot a - 65\cdot b = 17$
   $17 = 4\cdot a - 65\cdot b$

   iv. $18 = 1\times17 + 1$
   $-3\cdot a + 49\cdot b = 1\times(4\cdot a - 65\cdot b) + 1$
   $-3\cdot a + 49\cdot b = 4\cdot a - 65\cdot b + 1$
   $-7\cdot a + 114\cdot b = 1$
   $1 = -7\cdot a + 114\cdot b$

   Ainsi, le couple $(114\,;\,-7)$ est une solution de l'équation :
   $123\cdot u + 2003\cdot v = 1$

   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. • $\Leftarrow$: supposons que $x \equiv 456\cdot k_0 \pmod{2003}$
   On a :
   $x \equiv 456\cdot k_0 \pmod{2003}$
   $123\cdot x \equiv 123\cdot456\cdot k_0 \pmod{2003}$
   $123\cdot x \equiv 456\cdot(123\cdot k_0) \pmod{2003}$
   $123\cdot x \equiv 456\cdot1 \pmod{2003}$
   $123\cdot x \equiv 456 \pmod{2003}$

   • $\Longrightarrow$: supposons que $123\cdot x \equiv 456 \pmod{2003}$
   On a :
   $123\cdot x \equiv 456 \pmod{2003}$
   $k_0\cdot123\cdot x \equiv k_0\cdot456 \pmod{2003}$
   $(123\cdot k_0)\cdot x \equiv k_0\cdot456 \pmod{2003}$
   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 :
   $1 \leqslant n \leqslant 2002$; $123\cdot n \equiv 456 \pmod{2003}$
   $1 \leqslant n' \leqslant 2002$; $123\cdot n' \equiv 456 \pmod{2003}$
   En effectuant membre à membre les inégalités et les équivalences, on obtient :
   $-2001 \leqslant n - n' \leqslant 2001$; $123\cdot(n - n') \equiv 0 \pmod{2003}$
   De la dernière équivalence, on en déduit que le produit $123\cdot(n - n')$ 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, $(n - n') \in [-2001\,;\,2001]$ 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 :
   $PGCD(a\,;\,2003) = 1$
   D'après le théorème de Bezout, il existe un couple d'entiers $(u\,;v)$ tels que :
   $u\cdot a + v\cdot2003 = 1$
   La congruence permet d'écrire :
   $u\cdot a + v\cdot2003 \equiv 1 \pmod{2003}$
   $u\cdot a + v\cdot0 \equiv 1 \pmod{2003}$
   $u\cdot a \equiv 1 \pmod{2003}$
   On vient de montrer l'existence d'un entier m tel que :
   $a\cdot m \equiv 1 \pmod{2003}$

   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 $y = b\cdot m$:
   $a\cdot y \equiv b \pmod{2003}$

EXERCICE 11

Soit l'équation (1) d'inconnue rationnelle x :

$$78x^3 + ux^2 + vx - 14 = 0$$

où u et v sont des entiers relatifs.

1. On suppose dans cette question que $\frac{14}{39}$ est solution de l'équation (1).

   a. Prouver que les entiers relatifs u et v sont liés par la relation :
   $14u + 39v = 1129$

   b. Utiliser l'algorithme d'Euclide, en détaillant les diverses étapes du calcul, pour trouver un couple $(x\,;y)$ d'entiers relatifs vérifiant l'équation :
   $14x + 39y = 1$
   Vérifier que le couple $(-25\,;9)$ est solution de cette équation.

   c. En déduire un couple $(u_0\,;v_0)$ solution particulière de l'équation :
   $14u + 39v = 1129$
   Donner la solution générale de cette équation, c'est à dire l'ensemble des couples $(u\,;v)$ d'entiers relatifs qui la vérifient.

   d. Déterminer, parmi les couples $(u\,;v)$ précédents, celui pour lequel le nombre u est l'entier naturel le plus petit possible.

2. a. Décomposer 78 et 14 en facteurs premiers.
   En déduire, dans $\mathbb{N}$, l'ensemble des diviseurs de 78 et l'ensemble des diviseurs de 14.

   b. Soit $\frac{P}{Q}$ une solution rationnelle de l'équation (1) d'inconnue x :
   $78x^3 + ux^2 + vx - 14 = 0$ où u et v sont des entiers relatifs.
   Montrer que si P et Q sont des entiers relatifs premiers entre eux, alors P divise 14 et Q divise 78.

   c. En déduire le nombre de rationnels, non entiers, pouvant être solutions de l'équation (1) et écrire, parmi ces rationnels, l'ensemble de ceux qui sont positifs.

Correction

1. a. En supposons que la fraction $\frac{14}{39}$ est solution de l'équation (1), on obtient la relation suivante sur u et sur v :

$$78\cdot x^3 + u\cdot x^2 + v\cdot x - 14 = 0$$
$$78\cdot\left(\frac{14}{39}\right)^3 + u\cdot\left(\frac{14}{39}\right)^2 + v\cdot\frac{14}{39} - 14 = 0$$

En multipliant les deux membres par 39^3 :

$$78\times14^3 + 14^2\times39\times u + 14\times39^2\times v - 14\times39^3 = 0$$

Divivsons les deux membres par 39×14 :

$$2\times14^2 + 14\times u + 39\times v - 14\times39^2 = 0$$
$$14\times u + 39\times v = 39^2 - 2\times14^2$$
$$14\times u + 39\times v = 1129$$

b. L'algorithme d'Euclide permet d'écrire :

- $39 = 2\times14 + 11$
- $14 = 1\times11 + 3$
- $11 = 3\times3 + 2$
- $3 = 1\times2 + 1$
- $2 = 2\times1 + 0$

On en déduit :
$PGCD(39\,;14) = 1$

En notant $a = 39$ et $b = 14$, on a :

- $39 = 2\times14 + 11$
  $a = 2\cdot b + 11$
  $11 = a - 2\cdot b$
- $14 = 1\times11 + 3$
  $b = 1\cdot(a - 2\cdot b) + 3$
  $3 = b - (a - 2\cdot b)$
  $3 = 3\cdot b - a$
- $11 = 3\times3 + 2$
  $a - 2\cdot b = 3\cdot(3\cdot b - a) + 2$
  $a - 2\cdot b = 9\cdot b - 3\cdot a + 2$
  $2 = 4\cdot a - 11\cdot b$
- $3 = 1\times2 + 1$
  $3\cdot b - a = 1\times(4\cdot a - 11\cdot b) + 1$
  $3\cdot b - a = 4\cdot a - 11\cdot b + 1$
  $1 = 14\cdot b - 5\cdot a$

Cette dernière égalité permet d'écrire :

$$14\cdot b - 5\cdot a = 1$$
$$14\cdot14 - 5\cdot39 = 1$$
$$14\cdot14 + (-5)\cdot39 = 1$$

On en éduit que le couple $(14\,;-5)$ est solution de l'équation :
$(14\,;-5)$

Vérifions que le couple $(-25\,;9)$ est solution de l'équation : $14\cdot u + 39\cdot v = 14\cdot(-25) + 39\cdot9$
$= 1$

c. Montrons que le couple suivant :
$(-25\times1\,129\,;9\times1\,129) = (-28\,225\,;10\,161)$
est solution de l'équation car :

$$14\cdot u + 39\cdot v = 14\cdot28\,225 + 39\cdot10\,161$$
$$= 14\cdot(-25\times1\,129) + 39\cdot9\times1\,129$$
$$= 1\,129\cdot\big(14\cdot(-25) + 39\cdot9\big)$$

Cherchons l'ensemble des solutions de l'équation :
$14\cdot x + 39\cdot y = 1\,129$
Or, on sait que $(-28\,225\,;10\,161)$ est solution de cette équation :
$14\times(-28\,225) + 39\times10\,161 = 1$
On en déduit l'égalité :

$$14\cdot x + 39\cdot y = 14\times(-28\,225) + 39\times10\,161$$
$$14\cdot x + 14\times28\,225 = 39\times10\,161 - 39\cdot y$$
$$14\cdot(x + 28\,225) = 39\cdot(10\,161 - y)$$

Rappelons que l'égalité $14\cdot x + 39\cdot y = 1$ montre que les nombres x et y sont premiers entre eux.

- Le nombre 14 divisant le produit $39\cdot(10\,161 - y)$ et 14 et 39 sont premiers entre eux ; d'après le théorème de Gauss, on en déduit que 14 divise le facteur $10{,}161 - y$.
  On en déduit l'existence d'un entier relatif k' tel que :
  $10{,}161 - y = 14\cdot k'$
  $-y = 14\cdot k' - 10{,}161$
  $y = 10\,161 - 14\cdot k'$
- Le nombre 39 divisant le produit $14\cdot(x+25)$ et 14 et 39 sont premiers entre eux ; d'après le théorème de Gauss, on en déduit que 14 divise le facteur $x + 25$.

On en déduit l'existence d'un entier relatif k tel que :

$$x + 28\,225 = 39\cdot k$$

$$x = 39\cdot k - 28\,225$$

Ainsi, les solutions de l'équation $14\cdot u + 39\cdot v = 1\,129$ sont des couples d'entiers relatifs de la forme :

$\left(39\cdot k - 28\,225\,;10\,161 - 14\cdot k'\right)$

Parmi ces couples regardons ceux qui sont solutions de l'équation :

$$14\cdot u + 39\cdot v = 1$$

$$14\cdot(39\cdot k - 28\,225) + 39\cdot(10\,161 - 14\cdot k') = 1$$

$$14\times39\cdot k - 14\times28\,225 + 39\times10\,161 - 39\times14\cdot k' = 1$$

$$14\times39\cdot k + \left[14\times(-28\,225) + 39\times10\,161\right] - 39\times14\cdot k' = 1$$

$$14\times39\cdot k + 1 - 39\times14\cdot k' = 1$$

$$14\times39\cdot k - 39\times14\cdot k' = 0$$

$$14\times39\cdot(k - k') = 0$$

On en déduit l'égalité :

$$k = k'$$

Ainsi, les couples d'entiers relatifs sont les couples d'entiers :

$\left(39\cdot k - 28\,225\,;10\,161 - 14\cdot k\right)$ où k est un entier relatif

d. Résolvons l'inéquation :

$$39\cdot k - 28\,225 \geqslant 0$$

$$39\cdot k \geqslant 28\,225$$

$$k \geqslant \frac{28\,225}{39}$$

On en déduit que la valeur de k recherchée est 724 ; ce couple est :

$(11\,;25)$

2. a. On a les deux décompositions suivantes :

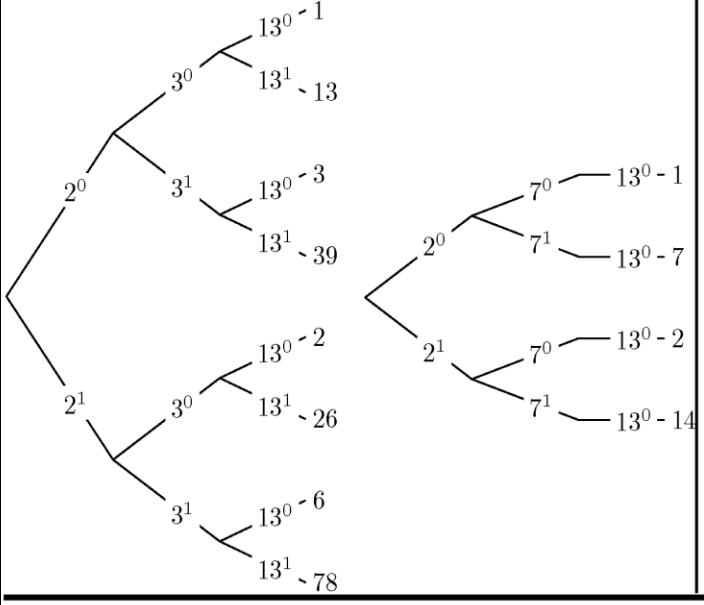
78	2
39	3
13	13
1	

$78 = 2\times3\times13$

14	2
7	7
1	

$14 = 2\times7$

On a les deux arbres de choix suivants :



b. Supposons que $\dfrac{P}{Q}$ est une solution rationnelle de l'équation (1) :

$$78\cdot x^3 + u\cdot x^2 + v\cdot x - 14 = 0$$

$$78\cdot\left(\frac{P}{Q}\right)^3 + u\cdot\left(\frac{P}{Q}\right)^2 + v\cdot\left(\frac{P}{Q}\right) - 14 = 0$$

$$78\cdot P^3 + u\cdot P^2\cdot Q + v\cdot P\cdot Q^2 - 14\cdot Q^3 = 0$$

Cette équation peut s'écrire des deux manières suivantes :

- $78\cdot P^3 + u\cdot P^2\cdot Q + v\cdot P\cdot Q^2 - 14\cdot Q^3 = 0$

$$78\cdot P^3 + u\cdot P^2\cdot Q + v\cdot P\cdot Q^2 = 14\cdot Q^3$$

$$P\cdot\left(78\cdot P^2 + u\cdot P\cdot Q + v\cdot Q^2 = 14\cdot Q^3\right.$$

En supposant que les entiers P et Q sont premiers entre eux et d'après le théorème de Gauss, on en déduit que P divise 14.

- $78\cdot P^3 + u\cdot P^2\cdot Q + v\cdot P\cdot Q^2 - 14\cdot Q^3 = 0$

$$u\cdot P^2\cdot Q + v\cdot P\cdot Q^2 - 14\cdot Q^3 = 78\cdot P^3$$

$$Q\cdot\left(u\cdot P^2 + v\cdot P\cdot Q - 14\cdot Q^2\right) = 78\cdot P^3$$

En supposant que les entiers P et Q sont premiers entre eux et d'après le théorème de Gauss, on en déduit que Q divise 78.

c. "***Remarque personnelle :*** *l'énoncé de cette question précise "*`les rationnels pouvant être solutions`*" car la question b. donne un critère nécessaire aux entiers P et Q pour être solution de (1) mais cette condition ne suffit peut être pas*".

Sachant que P est un diviseur de 14 et Q est un diviseur de 78, voici l'ensemble des diviseurs pouvant être solution de (1) :

	1	2	3	6	13	26	39	78
1	1	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{6}$	$\frac{1}{13}$	$\frac{1}{26}$	$\frac{1}{39}$	$\frac{1}{78}$
2	2	1	$\frac{2}{3}$	$\frac{1}{3}$	$\frac{2}{13}$	$\frac{1}{13}$	$\frac{2}{39}$	$\frac{1}{39}$
7	7	$\frac{7}{2}$	$\frac{7}{3}$	$\frac{7}{6}$	$\frac{7}{13}$	$\frac{7}{26}$	$\frac{7}{39}$	$\frac{7}{78}$
14	14	7	$\frac{14}{3}$	$\frac{7}{3}$	$\frac{14}{13}$	$\frac{7}{13}$	$\frac{14}{39}$	$\frac{7}{39}$

Voici les rationnels positifs succeptibles d'être solutions de l'équation (1) :

$$1\ ;\ \frac{1}{2}\ ;\ \frac{1}{3}\ ;\ \frac{1}{6}\ ;\ \frac{1}{13}\ ;\ \frac{1}{26}\ ;\ \frac{1}{39}$$

$$\frac{1}{78}\ ;\ 2\ ;\ \frac{2}{3}\ ;\ \frac{2}{13}\ ;\ \frac{2}{39}\ ;\ 7\ ;\ \frac{7}{2}$$

$$\frac{7}{3}\ ;\ \frac{7}{6}\ ;\ \frac{7}{13}\ ;\ \frac{7}{26}\ ;\ \frac{7}{39}\ ;\ \frac{7}{78}\ ;\ 14$$

$$\frac{14}{3}\ ;\ \frac{14}{13}\ ;\ \frac{14}{39}$$

On en déduit qu'il existe 24 rationnels positifs pouvant être solution de l'équation (1) ; par symétrie, il existe 48 rationnels pouvant être solution de l'équation (1).

EXERCICE 13

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 :
$7^n - 3\times 2^m = 1$ (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

Partie A :

1. Le couple $(1\,;1)$ est une solution de l'équation :
   $7\cdot x - 6\cdot y = 7\times 1 - 6\times 1 = 1$
2. Soit $(x\,;y)$ une couple solution de l'équation (E) ; on a légalité :
   $$\begin{aligned} 7\cdot x - 6\cdot y &= 1 \\ 7\cdot x - 6\cdot y &= 7\times 1 - 6\times 1 \\ 7\cdot x - 7\times 1 &= 6\cdot y - 6\times 1 \\ 7\cdot(x-1) &= 6\cdot(y-1) \end{aligned}$$
   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 $m = 1$:
     $7^n - 3\times 2^m = 1$newline On en déduit que le couple
     $$\begin{aligned} 7^n - 3\times 2^1 &= 1 \\ 7^n - 6 &= 1 \\ 7^n &= 7 \end{aligned}$$
     $(1\,;1)$ est solution de l'équatino (F).
   - Pour $m = 2$:
     On cherche n afin de vérifier l'égalité suivante :
     $$\begin{aligned} 7^n - 3\times 2^m &= 1 \\ 7^n - 3\times 2^2 &= 1 \\ 7^n - 3\times 4 &= 1 \\ 7^n - 12 &= 1 \\ 7^n &= 13 \end{aligned}$$
     Il n'existe pas de couple $(n\,;2)$ vérifiant l'égalité (F).
   - Pour $m = 3$:
     On cherche n afin de vérifier l'égalité suivante :
     $$\begin{aligned} 7^n - 3\times 2^m &= 1 \\ 7^n - 3\times 2^6 &= 1 \\ 7^n - 3\times 8 &= 1 \\ 7^n - 24 &= 1 \\ 7^n &= 25 \end{aligned}$$
     Il n'existe pas de couple $(n\,;3)$ vérifiant l'égalité (F).
   - Pour $m = 4$:
     $$\begin{aligned} 7^n - 3\times 2^m &= 1 \\ 7^n - 3\times 2^4 &= 1 \\ 7^n - 3\times 16 &= 1 \\ 7^n - 48 &= 1 \\ 7^n &= 49 \end{aligned}$$
     On en déduit que le couple $(2\,;4)$

   Il y a exactement 4 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 :
   $$\begin{aligned} 7^n - 3\times 2^m &= 1 \\ 7^n - 3\times 2^5\times 2^{5-m} &= 1 \\ 7^n - 3\times 32\times 2^{5-m} &= 1 \end{aligned}$$
   On en déduit l'équivalence :
   $$\begin{aligned} 7^n - 3\times 0\times 2^{5-m} &\equiv 1 \pmod{32} \\ 7^n &\equiv 1 \pmod{32} \end{aligned}$$
   b. On remarque que :
   $7^4 = 2401 = 75\times 32 + 1 \equiv 32 \pmod{32}$
   Le reste de la division euclidienne de n par 4 donne

l'existence d'un couple $(q\,;r)$ vérifiant :

$n = q\times 4 + r$ où $0 \leqslant r < 4$

On a les trois posibilités suivantes :

- $r = 0$:

$7^{q\times 4+r} = 7^{q\times 4+0} = \left(7^4\right)^q$

$\equiv 1^q \equiv 1 \pmod{32}$

- $r = 1$:

$7^{q\times 4+r} = 7^{q\times 4+1} = \left(7^4\right)^q \times 7^1$

$\equiv 1^q \times 7 \equiv 7 \pmod{32}$

- $r = 2$:

$7^{q\times 4+r} = 7^{q\times 4+2} = \left(7^4\right)^q \times 7^2$

$\equiv 1^q \times 7^2 \equiv 49 \equiv 17 \pmod{32}$

- $r = 2$:

$7^{q\times 4+r} = 7^{q\times 4+3} = \left(7^4\right)^q \times 7^3$

$\equiv 1^q \times 343 \equiv 23 \pmod{32}$

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 :

$7^n - 3\times 2^m = 1$

$7^n - 3\times 2^m \equiv 1 \pmod{5}$

$1 - 3\times 2^m \equiv 1 \pmod{5}$

$-3\times 2^m \equiv 0 \pmod{5}$

$3\times 2^m \equiv 0 \pmod{5}$

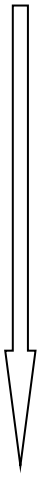
Cela signifie que 5 divise le produit 3×2^m ; or, les nombres 3 et 5 sont premiers entre eux, d'après le théorème de Gauss, on en déduit que 5 divise le facteur 2^m ce qui est une absurdité.

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 :

$\mathcal{S} = \left\{ (1\,;1)\ ;\ (2\,;4) \right)$

VERS L'EXERCICE 15



EXERCICE 15

Les questions 1. et 2. sont indépendantes.

Soit n un entier naturel non nul.

1. On considère l'équation notée (E) :
$3x+7y=10^{2n}$ où x et y sont des entiers relatifs.

a. Déterminer un couple $(u\,;v)$ d'entiers relatifs tels que :
$3\cdot u+7\cdot v=1$
En déduire une solution particulière $(x_0\,;y_0)$ de l'équation (E).

b. Déterminer l'ensemble des couples d'entiers relatifs $(x\,;y)$ solutions de (E).

2. On considère l'équation notée (G) :
$3x^2+7y^2=10^{2n}$ où x et y sont des entiers relatifs.

a. Montrer que : $100\equiv 2 \pmod 7$.
Démontrer que si $(x\,;y)$ est solution de (G) alors $3x^2\equiv 2^n \pmod 7$.

b. Reproduire et compléter le tableau suivant :

Reste de la division euclidienne de x par 7	0	1	2	3	4	5	6
Reste de la division euclidienne de $3x^2$ par 7							

c. Démontrer que 2^n est congru à 1, 2 ou 4 modulo 7.
En déduire que l'équation (G) n'admet pas de solution.

Correction :

1. a. Le couple $(-2\,;1)$ est une solution de l'équation proposée :
$3\cdot u+7\cdot v=3\cdot(-2)+7\cdot 1=1$
On en déduit que le couple $\left(-2\times 10^{2n}\,;10^{2n}\right)$ est solution de l'équation (E) :
$3\cdot x_0+7\cdot y_0=1=3\cdot(-2\times 10^{2n})+7\cdot 10^{2n}=10^{2n}\cdot(-6+7)=10^{2n}$

b. Soit $(x\,;y)$ une solution de l'équation (E) ; on en déduit :
$$3\cdot x+7\cdot y=10^{2n}$$
$(x_0\,;y_0)$ est solution de (E) :
$$3\cdot x+7\cdot y=3\cdot x_0+7\cdot y_0$$
$$3\cdot x-3\cdot x_0=7\cdot y_0-7\cdot y$$
$$3\cdot(x-x_0)=7\cdot(y_0-y)$$
$$3\cdot\left(x+2\times 10^{2n}\right)=7\cdot\left(10^{2n}-y\right)$$
De l'égalité précédente, on en déduit :

- 3 divise le produit $7\cdot\left(10^{2n}-y\right)$; or, les deux entiers 3 et 7 sont premiers entre eux, on en déduit que, à l'aide du théorème de Gauss, que l'entier 3 divise le facteur $10^{2n}-y$.
On en déduit l'existence d'un entier k' vérifiant :
$$10^{2n}-y=3\cdot k'$$
$$-y=3\cdot k'-10^{2n}$$
$$y=10^{2n}-3\cdot k'$$
- 7 divise le produit $3\cdot\left(x+2\times 10^{2n}\right)$; or, les deux entiers 3 et 7 sont premiers entre eux, on en déduit que, à l'aide du théorème de Gauss, que l'entier 7 divise le facteur $x+2\times 10^{2n}$.
On en déduit l'existence d'un entier k vérifiant :
$$x+2\times 10^{2n}=7\cdot k$$
$$x=7\cdot k-2\times 10^{2n}$$

Ainsi, l'ensemble des solutions de l'équation (E) sont les couples d'entiers de la forme :
$\left(7\cdot k-2\times 10^{2n}\,;10^{2n}-3\cdot k'\right)$ où $k\in\mathbb{N}$, $k'\in\mathbb{N}$
Vérifions maintenant quels couples de cette forme sont solutions de l'équation (E) ; soit $\left(7\cdot k-2\times 10^{2n}\,;10^{2n}-3\cdot k'\right)$ solution de (E) :
$$3\cdot\left(7\cdot k-2\times 10^{2n}\right)+7\cdot\left(10^{2n}-3\cdot k'\right)=1$$
$$3\cdot 7\cdot k-3\cdot 2\times 10^{2n}+7\cdot 10^{2n}-7\cdot 3\cdot k'=1$$
$$21\cdot(k-k')+\left[3\cdot(-2\times 10^{2n})+7\cdot 10^{2n}\right]=1$$
$$21\cdot(k-k')+1=1$$
$$21\cdot(k-k')=0$$
$$k-k'=0$$
$$k=k'$$
Ainsi, l'ensemble des solutions sont l'ensemble des couples d'entiers s'écrivant sous la forme :
$\left(7\cdot k-2\times 10^{2n}\,;10^{2n}-3\cdot k'\right)$ où $k\in\mathbb{N}$

2. a. La division euclidienne de 100 par 7 donne :
$100=14\times 7+2$
On en déduit l'équivalence suivante :
$100\equiv 2 \pmod 7$
Soit $(x\,;y)$ une solution de l'équation (G) ; on a les égalités et les équivalences suivantes :
$$3\cdot x^2+7\cdot y^2=10^{2n}$$
$$3\cdot x^2+0\cdot y^2\equiv\left(10^2\right)^n \pmod 7$$
$$3\cdot x^2\equiv 100^n \pmod 7$$
$$3\cdot x^2\equiv 2^n \pmod 7$$

b. On a le tableau suivant :

x	0	1	2	3	4	5	6
$3x^2$	0	3	12	27	48	75	108
Reste de la division euclidienne de $3x^2$ par 7	0	3	5	6	6	5	3

c. Soit n un entier naturel non-nul ; la division euclidienne de n par 3 donne l'existence du couple d'entiers $(q\,;r)$:
$n=3\cdot q+r$
On a l'équivalence suivante :
$$2^n\equiv 2^{3\cdot q+r}\equiv 2^{3\cdot q}\times 2^r \pmod 7$$
$$\equiv\left(2^3\right)^q\times 2^r\equiv 8^q\times 2^r \pmod 7$$
$$\equiv 1^q\times 2^r\equiv 2^r \pmod 7$$
Ainsi, 2^n peut avoir pour reste :

- Si le reste de n par 3 vaut 0 :
$2^n\equiv 2^0\equiv 1 \pmod 7$
- Si le reste de n par 3 vaut 1 :
$2^n\equiv 2^1\equiv 2 \pmod 7$
- Si le reste de n par 3 vaut 2 :
$2^n\equiv 2^2\equiv 4 \pmod 7$

Ainsi, on vient de montrer que les deux expressions $3\cdot x^2$ et 2^n ne peuvent avoir le même reste par la division euclidienne par 7.
De même, les deux expressions $3\cdot x^2+7\cdot y^2$ et 10^{2n} ne peuvent avoir le même reste par la division euclidienne par 7 ; A fortiori, ces deux nombres ne peuvent jamais être égaux : l'équation (G) n'admet aucune solution.

EXERCICE 16

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 :

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 : $\text{pgcd}\,(a\,;b)=1$.
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 :
$$\begin{aligned} a\cdot u+b\cdot v&=1\\ a\cdot u+b\cdot v&=1\\ c\cdot(a\cdot u+b\cdot v)&=c\\ a\cdot(u\cdot c)+(b\cdot c)\cdot v&=c \end{aligned}$$
   D'après la première remarque :
$$\begin{aligned} a\cdot(u\cdot c)+(k\cdot v)\cdot v&=c\\ a\cdot(u\cdot c+v)&=c \end{aligned}$$
   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 :
     $17\cdot u+5\cdot v=17\times(-2)+5\times 7=-34+35=1$
   - 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 :
   - $\begin{aligned} n_0&=3\times 17u+9\times 5v=3\times 17u+9\times(1-17u)\\ &=3\times 17u+9-9\times 17u\\ &\equiv 3\times 0\times u+9-9\times 0\times u \pmod{17}\\ &\equiv 0+9-0 \pmod{17}\\ &\equiv 9 \pmod{17} \end{aligned}$
   - $\begin{aligned} n_0&=3\times 17u+9\times 5v=3\times(1-5v)+9\times 5v\\ &=3-3\times 5v+9\times 5v\\ &\equiv 3-3\times 0\times v+9\times 0\times v \pmod{5}\\ &\equiv 3-0+0 \pmod{5}\\ &\equiv 3 \pmod{5} \end{aligned}$

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

   c. En utilisant le couple obtenu à la question a., on a :
   $n_0=3\times 17u+9\times 5v=3\times 17\times(-2)+9\times 5\times 7=213$

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 :

$$\begin{aligned} n - n_0 &= 85{\cdot}k \\ n &= n_0 + 85{\cdot}k \\ n &= 213 + 85{\cdot}k \\ n &= 45 + 2{\times}85 + 85{\cdot}k \\ n &= 45 + 85{\cdot}(k+2) \end{aligned}$$

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 :

- $$\begin{aligned} n = 43 + 85{\cdot}k &= 3 + 8{\times}5 + 5{\times}17{\cdot}k \\ &\equiv 3 + 8{\times}0 + 0{\times}17{\cdot}k \pmod{5} \\ &\equiv 3 + 0 + 0 \pmod{5} \\ &\equiv 3 \pmod{5} \end{aligned}$$
- $$\begin{aligned} n = 43 + 85{\cdot}k &= 9 + 2{\times}17 + 5{\times}17{\cdot}k \\ &\equiv 9 + 2{\times}0 + 0{\times}17{\cdot}k \pmod{5} \\ &\equiv 9 + 0 + 0 \pmod{5} \\ &\equiv 9 \pmod{5} \end{aligned}$$

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 :

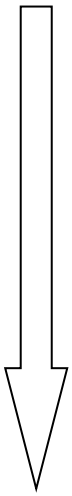
$$\begin{aligned} 300 &\leqslant 43 + 85{\cdot}k \leqslant 400 \\ 300 - 43 &\leqslant 85{\cdot}k \leqslant 400 - 43 \\ 257 &\leqslant 85{\cdot}k \leqslant 357 \\ \frac{257}{85} &\leqslant k \leqslant \frac{357}{85} \\ 3{,}02 &\leqslant k \leqslant 4{,}2 \end{aligned}$$

k étant un entier relatif, de l'encadrement précédent, on en déduit que $k = 4$.

Ainsi, Zoé possède exactement :

$n = 43 + 85{\times}4 = 43 + 340 = 383$

VERS L'EXERCICE 18



EXERCICE 18

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

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 :
$$\begin{aligned} 2{\cdot}u_{n+1} &= 2 \cdot (5{\cdot}u_n - 6) \\ &= 5 \cdot (2{\cdot}u_n) - 12 = 5 \cdot (5^{n+2} + 3) - 12 \\ &= 5^{(n+1)+2} + 15 - 12 = 5^{(n+1)+2} + 3 \end{aligned}$$
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 :
$$\begin{aligned} 2{\cdot}u_n &= 28 + 100{\cdot}k \\ u_n &= 14 + 50{\cdot}k \end{aligned}$$
On remarque facilement que si :
- k est pair : il existe k' tel que $k = 2{\cdot}k'$; on a :
$u_n = 14 + 50{\cdot}(2{\cdot}k') = 14 + 100k'$
Le nombre u_n se termine par 14.
- $(k+1)$ est impair : il existe k' tel que $k = 2{\cdot}k' + 1$; on a :
$$\begin{aligned} u_n &= 14 + 50{\cdot}(2{\cdot}k' + 1) = 14 + 100{\cdot}k' + 50 \\ &= 64 + 100{\cdot}k' \end{aligned}$$
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 :

$k\cdot 2\cdot d = \left(5^{n+3}+3\right) - \left(5^{n+2}+3\right)$

$= 5^{n+3} - 5^{n+2} = 5^{n+2}\cdot\left(5-1\right)$

$= 4\cdot 5^{n+2}$

$\Longrightarrow k\cdot d = 2\cdot 5^{n+2}$

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 :

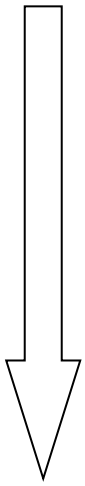
$d = 1$ ou $d = 2$

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.

VERS L'EXERCICE 20



EXERCICE 20

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	;	31	;
37	;	41	;	43	;	47	;	53	;
59	;	61	;	67	;	71	;	73	;
79	;	83	;	89	;	97			

Correction

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.

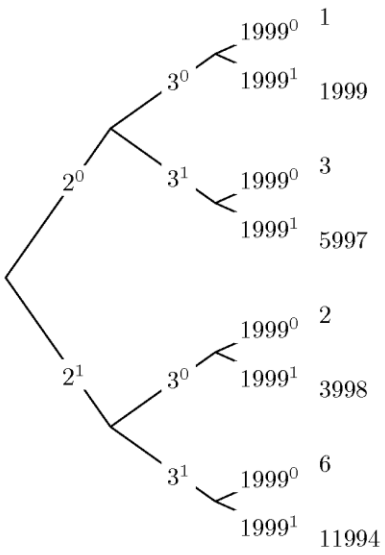
3. Soit n un entier naturel solution de (E), on a l'égalité suivante :

$$\begin{aligned} n^2 - S{\cdot}n + 11\,994 &= 0 \\ n^2 - S{\cdot}n &= -11\,994 \\ n{\cdot}(n - S) &= -11\,994 \end{aligned}$$

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 :

$[2\,;\sqrt{1\,999}]\subset[2\,;45]$

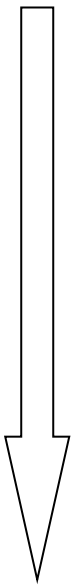
Ainsi, il suffit de tester la divisibilité de $1\,999$ parmi les entiers premiers :

2 ; 3 ; 5 ; 7 ; 11 ; 13 ; 17 ; 19

23 ; 31 ; 37 ; 41 ; 43

Et aucun de ces entiers n'est un diviseur de $1\,999$.

VERS L'EXERCICE N°21



EXERCICE 21

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 $\left(4+10\cdot k\,;9+24\cdot k\right)$ 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

1. Vraie :

On a les égalités et les équivalences suivantes :

$$\begin{aligned}2^{2n}-1&=\left(2^2\right)^n-14^n-1\\&\equiv 1^n-1\equiv 1-1\equiv 0 \pmod 3\end{aligned}$$

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 :

$$\begin{aligned}12\cdot x-5\cdot y&=12\times 9-5\times 21\\&=108-105\\&=3\end{aligned}$$

Mais, il n'existe pas de $k\in\mathbb{Z}$ tel que :

$$(9\,;21)=\left(4+10\cdot k\,;9+24\cdot k\right)$$

Résolvons l'équation :

$$\begin{aligned}4+10\cdot k&=9\\10\cdot k&=9-4\\10\cdot k&=5\\k&=\frac{1}{2}\end{aligned}$$

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 :

$$\begin{aligned}PPCM(a\,;b)-PGCD(a\,;b)&=1\\k\cdot k'\cdot d-d&=1\\d\cdot\left(k\cdot k'-1\right)&=1\end{aligned}$$

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 :

$$\begin{aligned}M&\equiv 0 \pmod{27}\\\overline{abc}^{10}&\equiv 0 \pmod{27}\\a\times 10^2+b\times 10+c&\equiv 0 \pmod{27}\\19\cdot a+10\cdot b+c&\equiv 0 \pmod{27}\end{aligned}$$

On a l'égalité suivante :

$$\begin{aligned}N&=\overline{bca}^{10}\\N&=b\cdot 10^2+c\cdot 10+a\\19\cdot N&=19\cdot\left(b\cdot 10^2+c\cdot 10+a\right)\\19\cdot N&=19\cdot\left(b\cdot 19+c\cdot 10+a\right)\\19\cdot N&=361\cdot b+190\cdot c+19\cdot a\\19\cdot N&\equiv 361\cdot b+190\cdot c+19\cdot a \pmod{27}\\19\cdot N&\equiv 10\cdot b+1\cdot c+19\cdot a \pmod{27}\\19\cdot N&\equiv 19\cdot a+10\cdot b+c \pmod{27}\\19\cdot N&\equiv M \pmod{27}\\19\cdot N&\equiv 0 \pmod{27}\end{aligned}$$

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 22

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

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 :

$$\begin{aligned}&(x-1)\cdot\left(1+x+x^2+\cdots+x^{k-1}+x^k\right)\\&=(x-1)\cdot\left(1+x+x^2+\cdots+x^{k-1}\right)+(x-1)\cdot x^k\end{aligned}$$

D'après la relation de récurrence :

$$\begin{aligned}&=\left(x^k-1\right)+(x-1)\cdot x^k\\&=\left(x^k-1\right)+x^{k+1}-x^k\\&=x^{k+1}-1\end{aligned}$$

2. a. On a les égalités suivantes :

$$\begin{aligned}a^n-1&=a^{d\cdot k}-1\\&=\left[a^d\right]^k-1\end{aligned}$$

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 :

$$\begin{aligned}d\cdot\left[u\cdot m'-v\cdot n'\right]&=d\times 1\\d\cdot u\cdot m'-d\cdot v\cdot n'\right]&=d\\u\cdot\left[d\cdot m'\right]-v\cdot\left[d\cdot n'\right]&=d\\u\cdot m-v\cdot n&=d\end{aligned}$$

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 23

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

Partie A

Considérons quatre entiers a, b, c et d vérifiant les deux relations suivantes :
$a \equiv b \pmod{n}$; $c \equiv d \pmod{n}$

Des relations de congruences précédentes, on en déduit l'existence de deux entiers relatifs k et k' vérifiant les égalités suivantes :
$a = b + k\cdot n$; $c = d + k'\cdot n$

Déterminons une expression du produit de a par c :
$$a\cdot c = (b + k\cdot n)(d + k'\cdot n) = b\cdot d + b\cdot k'\cdot n + d\cdot k\cdot n + k\cdot k'\cdot n^2$$
$$= b\cdot d + n\cdot(b\cdot k' + d\cdot k + k\cdot k'\cdot n) \equiv b\cdot d \pmod{n}$$

Partie B

1. Vérifions que le couple $(-9\,;\,-8)$ est solution de l'équation :
$$23x - 26y = 23\times(-9) - 26\times(-8) = -207 - (-208)$$
$$= -207 + 208 = 1$$
2. Considérons $(x\,;y)$ un couple solution de l'équation (E).
On a les deux égalités :
$23x - 26y = 1$; $23\times(-9) - 26\times(-8)$.
On en déduit l'égalité :
$$23x - 26y = 23\times(-9) - 26\times(-8)$$
$$23x - 26y = -23\times 9 + 26\times 8$$
$$23x + 23\times 9 = 26y + 26\times 8$$
$$23(x + 9) = 26(y + 8)$$
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 :
$$23x - 26y = 1$$
$$23x - 26\cdot(23\cdot k - 8) = 1$$
$$23x - 26\times 23\cdot k + 26\times 8 = 1$$
$$23x - 26\times 23\cdot k + 208 = 1$$
$$23(x - 26\cdot k) = 1 - 208$$
$$23(x - 26\cdot k) = -207$$
$$x - 26\cdot k = \frac{-207}{23}$$
$$x - 26\cdot k = -9$$
$$x = -9 + 26\cdot k$$
On vient de montrer que tout couple solution de l'équation (E) admet pour expression $(-9 + 26\cdot k\,;\,-8 + 23\cdot k)$
Vérifions maintenant que tout couple de cette forme est solution de (E) :
$$23\cdot(-9 + 26\cdot k) - 26\cdot(-8 + 23\cdot k)$$
$$= -207 + 598\cdot k + 208 - 598\cdot k = 1$$
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 $(a\,;k)$ 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 (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 :
$x_1 \equiv 16y_1 + y_2 \pmod{26} \quad ; \quad x_2 \equiv 11y_1 + 5y_2 \pmod{26}$
Montrons que ce couple est solution du système :

- $11\cdot x_1 + 3\cdot x_2 \equiv 11\cdot(16y_1 + y_2) + 3\cdot(11y_1 + 5y_2)$
$\equiv 176y_1 + 11y_2 + 33y_1 + 15y_2 \equiv 209y_1 + 26y_2$
$\equiv y_1 \pmod{26}$
- $7\cdot x_1 + 4\cdot x_2 \equiv 7\cdot(16y_1 + y_2) + 4\cdot(11y_1 + 5y_2)$
$\equiv 112y_1 + 7y_2 + 44y_1 + 20y_2 \equiv 156y_1 + 27y_2$
$\equiv y_2 \pmod{26}$

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 $(\mathcal{S}_3)$:

- $x_1 \equiv 16y_1 + y_2 \equiv 16\times 24 + 9 \equiv 384 + 9$
$\equiv 393 \equiv 19 \pmod{26}$
- $x_2 \equiv 11y_1 + 5y_2 \equiv 11\times 24 + 5\times 9 \equiv 264 + 45$
$\equiv 309 \equiv 23 \pmod{26}$

Ainsi, le couple $(19\,;23)$ 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.