Corrigés Exercices classe PGCD , Bézout ,Gauss

Exercice 1

1. *Voir le cours.*

2. *On considère le nombre de Mersenne* $2^{33}-1$.

   (a) *Si 3 divise* $2^{33}-1$ *et 4 divise* $2^{33}-1$, *comme 3 et 4 sont premiers entre eux, d'après le* ***1.*** *12 devrait diviser* $2^{33}-1$ *ce qui est contradictoire avec ce que dit l'élève : il a donc tort.*

   (b) 2^{33} *est un naturel pair donc* $2^{33}-1$ *est impair donc 4 ne peut le diviser.*

   (c) $2 \equiv -1 \quad [3] \Rightarrow 2^3 \equiv (-1)^3 \quad [3] \iff 2^3 \equiv -1 \quad [3] \Rightarrow (2^3)^{11} \equiv (-1)^{11} \quad [3] \iff 2^{33} \equiv -1 \quad [3]$ *ce qui montre que 3 ne divise pas* $2^{33}-1$.

   (d) $S = 1 + 2^3 + (2^3)^2 + (2^3)^3 + \cdots + (2^3)^{10}$;
   $2^3 S = 2^3 + 2^4 + (2^3)^3 + (2^3)^3 + \cdots + (2^3)^{11}$, *d'où par différence :*
   $7S = (2^3)^{11} - 1 \iff S = \dfrac{(2^3)^{11}-1}{7}$.

   (e) *S est une somme d'entiers naturel donc est un entier naturel ; le résultat précédent montre que* $(2^3)^{11}-1$ *est donc un multiple de 7.*
   Finalement $2^{33}-1$ *est divisible par 7.*

3. $2^7 - 1 = 128 - 1 = 127$.

   Ce nombre n'est divisible ni par 2, ni par 3, ni par 5, ni par 7 (dans la division reste 1), ni par 11 (dans la division reste 7), ni par 13 (dans la division reste 10) et comme $13^2 = 169$, *il est inutile de continuer : 127 est premier.*

4. (a) *Comme on vient de le voir pour 127, l'algorithme cherche le reste de la division de* $2^{33}-1$ *par les naturels 2, 3, 4, etc.,* $k \leqslant \sqrt{2^n-1}$ *tant que le reste est non nul.*
   Or on a vu que le nombre $2^{33}-1$ *est divisible par 7, donc l'algorithme va afficher ce diviseur 7 et CAS 2 .*
   En effet $2^{33}-1$ *n'est pas multiple de 5 :*
   $2^{11} = 2048$ *et* $2048 \equiv 3 \quad [5] \Rightarrow (2^{11})^3 \equiv 3^3 \quad [5]$, *mais* $3^3 = 27 \equiv 2 \quad [5]$, *donc* $2^{33} \equiv 2 \quad [5] \Rightarrow 2^{33} - 1 \equiv 1 \quad [5]$.
   Si on entre $n = 7$, *l'algorithme affiche 12 et CAS 1 .*

   (b) *Le cas 2 concerne donc les nombres de Mersenne non premiers et le nombre k est le plus petit de ses diviseurs (différent de 1).*

   (c) *Le CAS 1 concerne les nombres Mersenne premier comme* 2^7-1.

Exercice 2

Partie A

1.

valeur de a	*26*	*9*	*8*
valeur de b	*9*	*8*	*1*
valeur de c	*8*	*1*	*0*
Affichage			*1*

2.

Variables :	*c est un entier naturel*
	a et b sont des entiers naturels non nuls
Entrées :	*Demander a*
	Demander b
Traitement:	*Affecter à c le nombre* $r(a,\ b)$
	Tant que $c \neq 0$
	Affecter à a le nombre b
	Affecter à b la valeur de c
	Affecter à c le nombre $r(a,\ b)$
	Fin Tant que
Sortie :	*Si* $b = 1$
	Afficher les nombres entrés sont premiers entre eux
	Sinon
	Afficher les nombres entrés ne sont pas premiers entre eux
	Fin de Si

Partie B

1. *Dans cette question, on choisit* $p = 9$ *et* $q = 2$.

   (a) *Dans le tableau V correspond à 21, or* $9\times21+2 = 189+2 = 191$ *et* $191 = 26\times7+9$ *; donc* $x' \equiv 9 \quad [26]$.

   Dans le tableau 9 correspond à la lettre J.

   (b) *9 et 26 étant premiers entre eux, le théorème de Bezout permet d'affirmer l'existence de deux entiers relatifs u et v tels que* $9u + 26v = 1$.

   Le couple $(3\ ;\ -1)$ *est un couple simple solution de cette équation.*

   (c) *On a* $x' \equiv 9x + 2 \quad [26] \iff$ *il existe* $k \in \mathbb{Z},\ x' = 26k + 9x + 2 \iff 3x' = 26k' + 27x + 6 \iff 3x' = 26k' + 26x + x + 6 \iff 3x' = 26r'' + x + 6 \iff x = 26(-r'') + 3x' - 6 \iff x = 26(-r'') + 3x' + 20$, *soit* $x \equiv 3x' + 20 \quad [26]$

   (d) *R correspond à* $x' = 17$, *donc* $3x' + 20 = 51 + 20 = 71$ *et*

   $71 = 26 \times 2 + 19$, *soit* $71 \equiv 19 \quad [26]$.

   On a donc $x = 19$ *qui correspond à la lettre T.*

2. *J correspond à* $x = 9$ *et D correspond à* $x' = 3$. *de plus* $q = 2$ *; on a donc :*

   $3 = 9p + 2 \quad [26] \iff 9p \equiv 1 \quad [26]$ *ou encore* $27p \equiv 3 \quad [26]$, *mais on sait que* $27 \equiv 1 \quad [26]$ *; il en résulte que* $p \equiv 3 \quad [26]$ *et comme p est compris entre 0 et 25, on a donc* $p = 3$.

3. *B correspond à* $x = 1$, *d'où* $x' = 13x + 2 \equiv 15 \quad [26]$ *et 15 correspond à la lettre P.*

   D correspond à $x = 3$, *d'où* $x' = 13x + 2 \equiv 41 \quad [26]$ *et* $41 \equiv 15 \quad [26]$ *et 15 correspond à la lettre P.*

Conclusion : deux lettres différentes sont codées par la même lettre. Ce codage n'est pas bon puisque le décryptage donnera plusieurs solutions.

Exercice 3

On considère l'algorithme suivant, où A et B sont des entiers naturels tels que $A < B$:

Entrées :	*A et B entiers naturels tels que $A < B$*
Variables :	*D est un entier* *Les variables d'entrées A et B*
Traitement :	*Affecter à D la valeur de $B - A$* *Tant que $D > 0$* *B prend la valeur de A* *A prend la valeur de D* *Si $B > A$ Alors* *D prend la valeur de $B - A$* *Sinon* *D prend la valeur de $A - B$* *Fin Si* *Fin Tant que*
Sortie :	*Afficher A*

1. *On entre $A = 12$ et $B = 14$. On remplit le tableau donné en* **annexe***; voir page* **??**.
   La valeur affichée par l'algorithme est 2.

2. *Cet algorithme calcule la valeur du PGCD des nombres A et B.*
   En entrant $A = 221$ et $B = 331$, l'algorithme affiche la valeur 1.

   (a) *On a fait tourner l'algorithme pour $A = 221$ et $B = 331$ donc le PGCD de 221 et 331 est 1; ces deux nombres sont donc premiers entre eux.*
   D'après le théorème de Bézout, on peut dire qu'il existe des entiers relatifs x et y tels que $221x - 331y = 1$ (équation (E)).

   (b) $221 \times 3 - 331 \times 2 = 663 - 662 = 1$ *donc le couple $(3\ ;\ 2)$ est une solution de (E).*

$$\begin{array}{rrcll} (E) & 221 \times x & - & 331 \times y & = 1 \\ & 221 \times 3 & - & 331 \times 2 & = 1 \\ \hline & 221(x-3) & - & 331(y-2) & = 0 \quad \textit{par soustraction} \end{array}$$

   Donc $221(x-3) = 331(y-2)$ et donc 221 divise $331(y-2)$. Or on sait que 221 et 331 sont premiers entre eux donc, d'après le théorème de Gauss, 221 divise $y - 2$.
   On peut donc dire que $y - 2 = 221k$ où $k \in \mathbb{Z}$ et donc que $y = 2 + 221k$.
   De $221(x-3) = 331(y-2)$ on déduit $221(x-3) = 331 \times 221k$ ce qui équivaut à $x - 3 = 331k$; donc $x = 3 + 331k$.
   L'ensemble solution de l'équation (E) est $\{(3 + 331k\,;\, 2 + 221k)\}_{k \in \mathbb{Z}}$

3. *On considère les suites d'entiers naturels (u_n) et (v_n) définies pour tout entier naturel n par*

$$u_n = 2 + 221n \text{ et } \begin{cases} v_0 = 3 \\ v_{n+1} = v_n + 331 \end{cases}$$

   (a) *La suite (v_n) est arithmétique de raison $r = 331$ et de premier terme $v_0 = 3$; donc, pour tout entier naturel n, $v_n = v_0 + n \times r = 3 + 331n$.*

   (b) $u_p = v_q \iff 2 + 221p = 3 + 331q \iff 221p - 331q = 1$

   D'après les questions précédentes, on a: $(p\,,\,q) = (3 + 331k\,,\,2 + 221k)_{k\in\mathbb{Z}}$

$$\left.\begin{array}{l} 0 \leq p \leq 500 \iff 0 \leq 3 + 331k \leq 500 \Longrightarrow k \in \{0\,,\,1\} \\ 0 \leq q \leq 500 \iff 0 \leq 2 + 221k \leq 500 \Longrightarrow k \in \{0\,,\,1\,,\,2\} \end{array}\right\} \Longrightarrow k \in \{0\,,\,1\}$$

   Pour $k = 0$, $(p\,,\,q) = (3\,,\,2)$ donc $u_3 = v_2 = 665$.

   Pour $k = 1$, $(p\,,\,q) = (334\,,\,223)$ donc $u_{334} = v_{223} = 73816$.

Exercice 4

Partie A Inverse de 23 modulo 26

1. $23 \times (-9) - 26 \times (-8) = -207 + 208 = 1$ *: le couple $(-9\,;\ -8)$ est solution de l'équation (E).*

2. $\left\{\begin{array}{lcl} 23x - 26y & = & 1 \\ 23 \times (-9) - 26 \times (-8) & = & 1 \end{array}\right. \Longrightarrow$ *(par différence membre à membre)*

   $23(x + 9) - 26(y + 8) = 0 \iff 23(x + 9) = 26(y + 8) \quad (1)$

   Donc 23 divise $26(y + 8)$ et comme il est premier avec 26; il divise $y + 8$ (théorème de Gauss) : il existe donc un entier k tel que $y + 8 = 23k \iff y = -8 + 23k$.

   En remplaçant dans (1) $y + 8$ par $23k$, on obtient :

   $23(x + 9) = 26 \times 23k \iff x + 9 = 26 \iff x = -9 + 26k$.

   Réciproquement les couples $(-9 + 26k\ ;\ -8 + 23k)$ vérifient (E) car

   $23(-9 + 26k) - 26(-8 + 23k) = -207 + 23 \times 26k + 208 - 26 \times 23k = 1$.

   Les couples solutions de (E) sont donc de la forme : $(-9 + 26k\ ;\ -8 + 23k)$, $k \in \mathbb{Z}$.

3. *Il faut trouver un (ou des) couple(s) de premier terme a tel que $0 \leqslant a \leqslant 25$, donc vérifiant :*

   $0 \leqslant -9 + 26k \leqslant 25 \iff 9 \leqslant 26k \leqslant 34$. *La solution $k = 1$ est évidente ce qui donne $a = -9 + 26 = 17$.*

   Donc comme $26b \equiv 0 \pmod{26}$, on a $23 \times 17 \equiv 1 \pmod{26}$.

Partie B Chiffrement de Hill

1. $\underbrace{ST}_{\text{mot en clair}} \overset{\text{étape1}}{\Longrightarrow} (18,\ 19) \overset{\text{étape 2}}{\Longrightarrow} (21,\ 20) \overset{\text{étape 3}}{\Longrightarrow} \underbrace{VU}_{\text{mot codé}}$

2. *(a)* $(S_1)\ \begin{cases} y_1 \equiv 11x_1 + 3x_2 \pmod{26} \\ y_2 \equiv 7x_1 + 4x_2 \pmod{26} \end{cases} \Longrightarrow$

$\begin{cases} -44x_1 - 12x_2 = -4y_1 \pmod{26} \\ 21x_1 + 12x_2 = 3y_2 \pmod{26} \end{cases} \Rightarrow$ *(par somme)*

$-23x_1 = -4y_1 + 3y_2 \pmod{26}$.

De même :

$(S_1)\ \begin{cases} y_1 \equiv 11x_1 + 3x_2 \pmod{26} \\ y_2 \equiv 7x_1 + 4x_2 \pmod{26} \end{cases} \Longrightarrow$

$\begin{cases} -77x_1 - 21x_2 = -7y_1 \pmod{26} \\ 77x_1 + 44x_2 = 11y_2 \pmod{26} \end{cases} \Longrightarrow$ *(par somme)*

$23x_2 = -7y_1 + 11y_2 \pmod{26}$ *ou encore puisque*

$-7 \equiv 19 \pmod{26}$ *:*

$23x_2 = 19y_1 + 11y_2 \pmod{26}$.

Donc, tout couple $(x_1\ ;\ x_2)$ *vérifiant les équations du système* (S_1)*, vérifie les équations du système :*

$$(S_2)\ \begin{cases} 23x_1 \equiv 4y_1 + 23y_2 \pmod{26} \\ 23x_2 \equiv 19y_1 + 11y_2 \pmod{26} \end{cases}$$

(b) On a vu à la partie B que $23 \times 17 \equiv 1 \pmod{26}$ *(23 a pour inverse 17 modulo 26), donc en multipliant chaque membre du système* (S_2) *par 17, on obtient*

$(S_2) \iff \begin{cases} 23x_1 \times 17 \equiv 4y_1 \times 17 + 23y_2 \times 17 \pmod{26} \\ 23x_2 \times 17 \equiv 19y_1 \times 17 + 11y_2 \times 17 \pmod{26} \end{cases} \Longrightarrow$

$\begin{cases} x_1 \equiv 68y_1 + 391y_2 \pmod{26} \\ x_2 \equiv 323y_1 + 187y_2 \pmod{26} \end{cases}$

Or $68 \equiv 16 \pmod{26}$, $391 \equiv 1 \pmod{26}$, $323 \equiv 11 \pmod{26}$,

$187 \equiv 5 \pmod{26}$*, donc finalement tout couple* $(x_1\ ;\ x_2)$ *vérifiant les équations du système* (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) On calcule $11x_1 + 3x_2 = 11\,(16y_1 + y_2) + 3\,(11y_1 + 5y_2) = 176y_1 + 11y_2 + 33y_1 + 15y_2 = 209y_1 + 26y_2$.

Or $209 \equiv 1 \pmod{26}$ *et* $26 \equiv 0 \pmod{26}$*, donc*

$11x_1 + 3x_2 \equiv 1y_1 + 0y_2 \pmod{26}$.

De même $7x_1 + 4x_2 = 7\,(16y_1 + y_2) + 4\,(11y_1 + 5y_2) = 112y_1 + 7y_2 + 44y_1 + 20y_2 = 156y_1 + 27y_2$.

Or $146 \equiv 0 \pmod{26}$ *et* $27 \equiv 1 \pmod{26}$*, donc*

$7x_1 + 4x_2 \equiv 0y_1 + 1y_2 \pmod{26}$.

Conclusion : tout couple $(x_1\ ;\ x_2)$ *vérifiant les équations du système* (S_3)*, vérifie les équations du système* (S_1)*.*

Finalement les systèmes (S_1) *et* (S_3) *sont équivalents.*

(d) *Pour YJ le couple* $(y_1\ ;\ y_2) = (24\ ;\ 9)$. *En appliquant les équations de* (S_3) *on obtient :*

$$\begin{cases} x_1 \equiv 16 \times 24 + 9 \pmod{26} \\ x_2 \equiv 11 \times 24 + 5 \times 9 \pmod{26} \end{cases} \iff \begin{cases} x_1 \equiv 393 \pmod{26} \\ x_2 \equiv 309 \pmod{26} \end{cases}$$

Or $393 = 26 \times 15 + 3$, *donc* $393 \equiv 3 \pmod{26}$;

$309 = 26 \times 11 + 23$, *donc* $269 \equiv 23 \pmod{26}$.

On a donc $(x_1\ ;\ x_2) = (3\ ;\ 23)$ *et en utilisant le tableau le mot décodé est donc* ***DX***.

Exercice 5

Partie A

On considère l'équation (E) : $25x - 108y = 1$ *où* x *et* y *sont des entiers relatifs.*

1. $25 \times 13 - 108 \times 3 = 325 - 224 = 1$, *le couple* $(13\ ;\ 3)$ *est bien solution de l'équation* $25x - 108y = 1$.

2. $(x_0; y_0) = (13\ ;\ 3)$ *est une solution particulière de l'équation (E).*

   $(x\ ;\ y)$ *est solution de (E) équivaut à* $25(x - x_0) = 108(y - y_0)$ *avec 25 et 108 premier entre eux donc 108 divise* $x - x_0$

   On a donc $x - x_0 = 108k$ *avec* k *entier relatif d'où alors* $y - y_0 = 25k$.

   L'ensemble des couples d'entiers relatifs solutions de l'équation (E) est $\{(13 + 108k\ ;\ 3 + 25k) / k \in$

Partie B

Dans cette partie, a désigne un entier naturel et les nombres c et g sont des entiers naturels vérifiant la relation $25g - 108c = 1$.

1. *Soit* x *un entier naturel.*
   Si $x \equiv a$ [7] *alors* $x - a$ *est divisible par 7. De même* $x \equiv a$ [19] *entraîne* $x - a$ *divisible par 19.*

   Or 7 et 19 sont premiers entre eux donc $x - a$ *divisible par* $7 \times 19 = 133$. *Ce qui s'écrit encore* $x \equiv a$ [133].

   Donc si $x \equiv a$ [7] *et* $x \equiv a$ [19], *alors* $x \equiv a$ [133].

2. (a) *On suppose que a n'est pas un multiple de 7.*
   7 est premier et a n'est pas un multiple de 7 donc d'après le petit théorème de Fermat on a $a^6 \equiv 1$ [7].
   De plus $108 = 6 \times 18$ *donc* $a^{108} = (a^6)^{18} \equiv 1^{18}$ [7] $\equiv 1$ [7].
   On a donc $(a^{25})^g = a^{25g} = a^{1+108c} a \times (a^{108})^c \equiv a \times 1^c$ [7] $\equiv a$ [7].

   (b) *On suppose que a est un multiple de 7.*
   On a alors $a \equiv 0$ [7] *et* $a^{25g} = (a^{25})^g \equiv 0$ (7] *donc* $(a^{25})^g \equiv a$ [7].

(c) *On admet que pour tout entier naturel* a, $(a^{25})^g \equiv a$ [19].

D'après les questions a. et b. on sait que l'on a aussi $(a^{25})^g \equiv a$ [7] *on peut donc en appliquant le résultat de la question 1. à* $x = (a^2 5)^g$ *démontrer que* $(a^{25})^g \equiv a$ [133].

Partie C *On note A l'ensemble des entiers naturels a tels que :* $1 \leqslant a \leqslant 26$.

Un message, constitué d'entiers appartenant à A, est codé puis décodé.
La phase de codage consiste à associer, à chaque entier a de A, l'entier r tel que $a^{25} \equiv r$ [133] *avec* $0 \leqslant r < 133$.

La phase de décodage consiste à associer à r , l'entier r_1 *tel que* $r^{13} \equiv r_1$ [133] *avec* $0 \leqslant r_1 < 133$.

1. $r_1 \equiv r^{13}$ [133] $\equiv (a^{25})^{13}$ [133] *avec* $(g\ ;\ c) = (13\ ;\ 3)$ *vérifiant la relation* $25g - 108c = 1$ *d'après la partie A.*

   D'où d'après la question 2.c. de la partie B, $(a^{25})^{13}$ [133] $\equiv a$ [133] *donc finallement on bien* $r_1 \equiv a$ [133].

2. $128 \equiv -5$ [133] *donc* $128^{13} \equiv -5^{13}$ [133] $\equiv -131$ [133] $\equiv 2$ [133]

   $59^4 \equiv 130$ [133] $\equiv -3$ [133] *donc* $59^{13} = (59^4)^3 \times 59 \equiv -3^3 \times 59$ [133] $\equiv -130$ [133] $\equiv 3$ [133]

   Le message initiale était donc : 2 3.

Exercice 6
PARTIE B

On se propose de déterminer l'ensemble $\mathcal{S}$ *des entiers relatifs n vérifiant le système :*

$$\begin{cases} n & \equiv & 9 & [17] \\ n & \equiv & 3 & [5] \end{cases}$$

1. *Recherche d'un élément de* $\mathcal{S}$.

   On désigne par $(u\ ;\ v)$ *un couple d'entiers relatifs tel que* $17u + 5v = 1$.

   (a) *17 et 5 sont premiers entre eux, donc, d'après le théorème de Bézout, il existe u et v entiers relatifs tels que* $17u + 5v = 1$.

   (b) *On pose* $n_0 = 3 \times 17u + 9 \times 5v$.

   Soit $(u\ ;\ v)$ *un couple solution, donc* $17u + 5v = 1$. *On en déduit que* $17u \equiv 1$ [5] *et* $5v \equiv 1$ [17].
   Alors $n_0 = 3 \times 17u + 9 \times 5v \equiv 9 \times 5v$ [17] $\equiv 9 \times 1$ [17] $\equiv 9$ [17].
   De même : $n_0 = 3 \times 17u + 9 \times 5v \equiv 3 \times 17u$ [5] $\equiv 3 \times 1$ [5] $\equiv 3$ [5].
   Par conséquent, $n_0 \in \mathcal{S}$.

(c) *Appliquons l'algorithme d'Euclide :*
$17 = 3 \times 5+2$ *et* $5 = 2 \times 2 + 1$, *d'où* $1 = 5 - 2 \times 2$
$= 5 - (17 - 5 \times 3) \times 2 = 17 \times (-2) + 5 \times 7$.
On peut prendre $(u\ ;\ v) = (-2\ ;\ 7)$.
On obtient alors $n_0 = 213$ *(ce n'est évidemment pas la seule valeur !)*

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

(a) *Soit* n *un entier relatif appartenant à* $\mathcal{S}$.
$n \equiv 9\ [17]$ *et* $n_0 \equiv 9\ [17]$ *donc* $n - n_0 \equiv 0\ [17]$.
De même, $n \equiv 3\ [5]$ *et* $n_0 \equiv 3\ [5]$ *donc* $n - n_0 \equiv 0\ [5]$.
17 et 5 sont premiers entre eux, donc d'après la partie A, $n - n_0 \equiv 0\ [85]$ *(car* $5 \times 17 = 85$*).*

(b) *On en déduit que, si* $n \in \mathcal{S}$, $n \equiv n_0\ [85]$ *donc* $n \equiv 213\ [85]$.
Or $213 = 170 + 43 = 2 \times 85 + 43 \equiv 43\ [85]$ *donc* $213 \equiv 43\ [85]$.
Par conséquent : $n \in \mathcal{S} \iff n \equiv 43\ [85]$ *donc* $n = 43 + 85k$, $k \in \mathbb{Z}$.
Réciproquement, si $n \equiv 43 + 85k$, $k \in \mathbb{Z}$ *, il est clair que* $n \equiv 9\ [17]$ *et* $n \equiv 3\ [5]$.

3. *Application :*

Soit n *le nombre de jetons. On a :* $n \equiv 9\ [17]$ *et* $n \equiv 3\ [5]$.

D'après ce qui précède, on a : $n = 43 + 85k$.

On sait que $300 \leqslant n \leqslant 400$, *donc* $300 \leqslant 43 + 85k \leqslant 400$. *On en déduit que* $k = 4$ *et que Zoé a* 383 *jetons.*

Exercice 7

1. (a) *Les entiers 11 et 7 sont premiers entre eux, donc, d'après le théorème de Bézout, il existe un couple* $(u\ ;\ v)$ *d'entiers relatifs tels que* $11u - 7v = 1$. *Par ailleurs* $11 \times 2 - 7 \times 3 = 1$, *le couple* $(2\ ;\ 3)$ *répond alors à la question.*

(b) *On a, en multipliant chaque membre de la dernière égalité par 5,*
$11 \times 10 - 7 \times 15 = 5$. *Le couple* $(10\ ;\ 15)$ *est donc une solution particulière de (E).*

(c) *Soit* $(x\ ;\ y)$ *une solution de (E), alors* $11x - 7y = 11 \times 10 - 7 \times 15$, *d'où:*

$$11(x - 10) = 7(y - 15). \qquad (1)$$

7 divise $11(x - 10)$ *et est premier avec 11, donc, d'après le théorème de Gauss, 7 divise* $x - 10$*: il existe donc un entier relatif* k *tel que* $x - 10 = 7k$. *En remplaçant* $x - 10$ *par* $7k$ *dans (1), puis en simplifiant, on en déduit que* $y - 15 = 11k$. *Ainsi, si* $(x\ ;\ y)$ *est solution de (E), alors nécessairement* $(x\ ;\ y)$ *est de la forme* $(10 + 7k\ ;\ 15 + 11k)$ *avec* $k \in \mathbb{Z}$. *Réciproquement, on vérifie aisément que de tels couples sont bien solutions de (E).*

(d) *Un point de D à coordonnées entières appartient à* $\mathcal{C}$ *si et seulement si* $\begin{cases} x \in \mathbb{Z} \ ; \ y \in \mathbb{Z} \\ 11x - 7y = 5 \\ 0 \leqslant x \leqslant 50 \ ; \ 0 \leqslant y \leqslant \end{cases}$

$\begin{cases} (x \ ; \ y) \text{ solution de (E)} \\ 0 \leqslant x \leqslant 50 \ ; \ 0 \leqslant y \leqslant 50 \end{cases}$ *On cherche donc tous les entiers relatifs* k *tels que* $0 \leqslant 10 + 7k \leqslant 50$ *et* $0 \leqslant 15 + 11k \leqslant 50$, *ce qui équivaut à* $-\dfrac{10}{7} \leqslant k \leqslant \dfrac{50}{7}$ *et* $-\dfrac{15}{11} \leqslant k \leqslant \dfrac{35}{11}$. *Les seules valeurs possibles de* k *sont* -1, 0, 1, 2 *et* 3. *Il y a donc cinq points de* $\mathcal{C}$ *donc les coordonnées sont entières:*

$$A(3 \ ; \ 4) \quad B(10 \ ; \ 15) \quad C(17 \ ; \ 26) \quad D(24 \ ; \ 37) \quad E(31 \ ; \ 48).$$

2. (a) *On a* $11 \equiv 1 \ (5)$, $7 \equiv 2 \ (5)$ *et* $5 \equiv 0 \ (5)$, *par conséquent, si le couple* $(x \ ; \ y)$ *est solution de (F), en passant aux congruences:* $11x^2 - 7y^2 = 5$ *devient* $x^2 - 2y^2 \equiv 0 \ (5)$, *c'est-à-dire* $x^2 \equiv 2y^2 \ (5)$.

(b) *On calcule aisément:*

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*

Les valeurs possibles du reste de la division euclidienne de x^2 *par 5 sont donc 0, 1 et 4. De même, les valeurs possibles du reste de la division euclidienne de* $2y^2$ *par 5 sont 0, 2 et 3.*

(c) *Si* $(x \ ; \ y)$ *est solution de (F), alors* $x^2 \equiv 2y^2 \ (5)$ *ce qui n'est possible, d'après les tableaux précédents, que si* $x \equiv 0 \ (5)$ *et* $y \equiv 0 \ (5)$, *c'est-à-dire si* x *et* y *sont des multiples de 5.*

3. *Supposons que* x *et* y *sont deux entiers multiples de 5. Alors il existe des entiers* a *et* b *tels que* $x = 5a$ *et* $y = 5b$. *En réinjectant cela dans l'équation (F) on a alors:* $11 \times 25a^2 - 7 \times 25b^2 = 5$, *c'est-à-dire* $25(11a^2 - 7b^2) = 5$, *ce qui est impossible (5 n'est pas multiple de 25 !). L'équation (F) ne possède donc aucune solution.*

Exercice 8

1. *On calcule :* $u_1 = 2 + 3 + 6 - 1 = 10$;

$u_2 = 4 + 9 + 36 - 1 = 48$;

$u_3 = 8 + 27 + 216 - 1 = 250$;

$u_4 = 16 + 81 + 1296 - 1 = 1392$;

$u_5 = 32 + 243 + 7776 - 1 = 8050$;

$u_6 = 64 + 729 + 46656 - 1 = 47448.$

2. *On a :* $2 \equiv 0 \mod 2 \Rightarrow 2^n \equiv 0 \mod 2$;

   $3 \equiv 1 \mod 2 \Rightarrow 3^n \equiv 1 \mod 2$;

   $6 \equiv 0 \mod 2 \Rightarrow 6^n \equiv 0 \mod 2$.

   Donc $u_n = 2^n + 3^n + 6^n - 1 \equiv 0 + 1 + 0 - 1 \equiv 0 \mod 2$

   u_n *est donc pair.*

   Ou encore 2^n *et* 6^n *sont pairs ;* 3^n *et 1 sont impairs, donc leur différence est paire et par somme* u_n *est pair.*

3. n *est pair : il existe donc* $k \in \mathbb{N}^*$ *tel que* $n = 2k$.

   On peut donc écrire : $u_n = u_{2k} = 2^{2k} + 3^{2k} + 6^{2k} - 1 = 4^k + 9^k + 2^{2k} \times 3^{2k} - 1 = 4^k + 4^k \times 9^k + 9^k - 1$.

   Comme $4 \equiv 0 \mod 4$, $4^k \equiv 0 \mod 4$;

   $4^k \times 9^k \equiv 0 \mod 4$;

   $9 \equiv 1 \mod 4$, *donc* $9^k \equiv 1 \mod 4$, *d'où par somme :*

   $u_{2k} \equiv 0 + 0 + 1 - 1 = 0 \mod 4$, *c'est-à-dire que* u_{2k} *est un multiple de 4.*

4. *On a vu que 2 divise* u_1, *que 3 divise* u_2, *que 5 divise* u_3 *et 7 divise* u_5.

   Donc 2, 3, 5 et 7 appartiennent à l'ensemble (E)

5. (a) *D'après le théorème de Fermat, 2 étant premier avec p, on a* $2^{p-1} \equiv 1 \mod p$.
   Donc $6 \times 2^{p-2} = 3 \times 2^{p-1} \iff 3 \mod p$.
   D'autre part 3 étant premier avec p, $3^{p-1} \equiv 1 \mod p$.
   Donc $6 \times 3^{p-2} = 2 \times 3^{p-1} \equiv 2 \mod p$.

   (b) *Par définition :* $6u_{p-2} = 6\left(2^{p-2} + 3^{p-2} + 6^{p-2} - 1\right) =$
   $6 \times 2^{p-2} + 6 \times 3^{p-2} + 6^{p-1} - 6$.
   On a vu que $6 \times 2^{p-2} \equiv 3 \mod p$, *que* $6 \times 3^{p-2} \equiv 2 \mod p$ *et on a* $6^{p-1} \equiv 1 \mod p$ *car p premier avec 2 et 3 est premier avec 6.*
   Donc $6 \times u_{p-2} \equiv 3 + 2 + 1 - 6 \mod p$ *soit* $6 \times u_{p-2} \equiv 0 \mod p$.

   (c) *On vient de démontrer que* $6 \times u_{p-2} \equiv 0 \mod p$ *: donc p divise* $6 \times u_{p-2}$, *mais p et 6 sont premiers entre eux, donc d'après le théorème de Gauss p divise* u_{p-2}.
   Conclusion : tout entier p premier appartient à l'ensemble (E)

Exercice 9

1. (a) *Si n est impair,* n^4 *l'est aussi, donc* $n^4 + 1$ *est pair.*
   Si n est pair, n^4 *l'est aussi, donc* $n^4 + 1$ *est impair.*

   (b) *Soit n un entier supérieur ou égal à 2.*

   - *Si* $n \equiv 0 \mod 3$, $n^4 \equiv 0 \mod 3$, $A(n) \equiv 1 \mod 3$.
   - *Si* $n \equiv 1 \mod 3$, $n^4 \equiv 1 \mod 3$, $A(n) \equiv 2 \mod 3$.

- *Si* $n \equiv 2 \mod 3$, $n^4 \equiv 1 \mod 3$, $A(n) \equiv 2 \mod 3$.

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

(c) *Soit* d *un diviseur de* $A(n)$ *: il existe un entier* k *tel que* $n^4 + 1 = kd$, *i.e. tel que :*

$$kd - n^3 \times n = 1.$$

On en déduit, d'après le théorème de Bezout, que d *et* n *sont premiers entre eux. Donc, tout entier* d *diviseur de* $A(n)$ *est premier avec* n.

(d) *Soit* d *un diviseur de* $A(n)$. *On a alors :* $n^4 + 1 \equiv 0 \mod d$.
D'où : $n^4 \equiv -1 \mod d$, *et donc :* $n^8 \equiv 1 \mod d$.
Donc, pour tout entier d *diviseur de* $A(n)$ *:*

$$n^8 \equiv 1 \mod d.$$

2. (a) *Soit* k *un entier tel que* $n^k \equiv 1 \mod d$.
Effectuons la division euclidienne de k *par* s *(l'existence de* s *est assurée d'après* **1.d***) :*
Il existe un unique couple d'entiers (q, r) *tel que* $k = sq + r$ *avec* $0 \leqslant r < s$.
D'où : $n^k = (n^s)^q \times n^r$. *Or :* $n^s \equiv 1 \mod d$. *Donc :* $(n^s)^q \equiv 1 \mod d$.
Et comme $n^k \equiv 1 \mod d$, *il en résulte :* $n^r \equiv 1 \mod d$.
Or $r < s$ *et* s *est le plus petit entier naturel non nul ayant cette propriété. Donc* $r = 0$ *et donc* s *divise* k.

(b) *On a vu au* **1.d** *que :* $n^8 \equiv 1 \mod d$. *Donc d'après* **a**, s *est un diviseur de* $k = 8$.

(c) *D'après* **1.c**, *l'entier* d *est premier avec* n. *Si, de plus,* d *est premier, alors il découle du petit théorème de Fermat que :*

$$n^{d-1} \equiv 1 \mod d.$$

Comme $d \geqslant 2$ *(car premier) alors* $k = d - 1$ *est un entier naturel non nul. D'où, d'après* **a**, s *divise* k, *i.e.* s *divise* $d - 1$.

On a donc montré que :

Si d *est un diviseur premier de* $A(n)$, *alors* s *est un diviseur de* $d - 1$.

3. *Recherche des diviseurs premiers de* $A(n)$ *dans le cas où* n *est un entier pair.*

Soit p *un diviseur premier de* $A(n)$ *et soit* s *le plus petit des entiers naturels non nuls* k *tels que* $n^k \equiv 1 \mod d$.

D'après **2.b** s *est un diviseur de* 8, *donc* $s \in \{1, 2, 4, 8\}$.

Si $s \in \{1, 2, 4\}$, *i.e. si* s *est un diviseur de 4, alors de :* $n^s \equiv 1 \mod p$ *on déduit :*

$$n^4 \equiv 1 \mod p.$$

D'où :

$$A(n) \equiv 2 \mod p.$$

Or on a $\boxed{p > 2}$, *puisque* n *étant un entier pair alors* $A(n)$ *est un entier impair.*

Donc $A(n)$ *n'est pas un multiple de* p, *contrairement à l'hypothèse.*

Donc s *ne divise pas 4 : donc* $s = 8$, *et, d'après* **2.c**, *8 est un diviseur de* $p - 1$, *i.e.* $p - 1 \equiv 0 \mod 8$, *et donc* $p \equiv 1 \mod 8$.

On a donc montré que, dans le cas où n *est un entier pair :*

Si p *est un diviseur premier de* $A(n)$, *alors* p *est congru à 1 modulo* 8.

4. *Recherche des diviseurs premiers de* $A(12)$.

   $A(12) = 20737$. *En effectuant les divisions successives de 20737 par les nombres de la liste donnée, on constate que* $20737 = 89 \times 233$.

   Or $\sqrt{233} \approx 15,3$ *donc* $\sqrt{233} < 17$. *Et comme, dans la liste, il n'y a pas d'autres nombres avant 17, cela signifie que 233 fait partie de la liste des nombres premiers congrus à 1 modulo 8.*

   Donc les diviseurs premiers de $A(12)$ *sont 89 et 233.*

Exercice 10

1. $1 + x + x^2 + \cdots + x^{k-1}$ *est la somme des* k *premiers termes de la suite géométrique de premier terme* 1 *et de raison* x *: elle est donc égale à :* $\dfrac{x^k - 1}{x - 1}$ *(pour* $x \neq 1$*).*

   Donc $(x - 1)\left(1 + x + x^2 + \cdots + x^{k-1}\right) = (x - 1) \times \dfrac{x^k - 1}{x - 1} = x^k - 1$.

   Pour $x = 1$ *: l'égalité est évidente.*

2. (a) $n \in N$, $n = dk$.

   D'après la question ***1.*** $a^n - 1 = (a - 1)\left(1 + a + a^2 + \cdots + a^{n-1}\right) = a^{dk} - 1 = \left(a^d\right)^k - 1 = \left(a^d - 1\right)(\cdots + \cdots)$, *la parenthèse étant une somme d'entiers donc un entier.*

   Conclusion : $a^n - 1 = \left(a^d - 1\right)(\cdots + \cdots)$, *ce qui signifie que* $\left(a^d - 1\right)$ *est un diviseur de* $a^n - 1$.

   (b) *On a donc*

   - *2,004 est multiple de 3, donc d'après le* **a.** $2^{2,004} - 1$ *est divisible par* $2^3 - 1 = 7$ *;*
   - *2,004 est multiple de 3 et de de 2, donc de 6 ; d'où* $2^{2,004} - 1$ *est divisible par* $2^6 - 1 = 63$ *:*

- *On vient de voir que* $2^{2,004} - 1 = 63k = 9 \times (7k)$, *donc* $2^{2,004} - 1$ *est divisible par* 9.

3. (a) $m = dm'$ *et* $n = dn'$. *Puisque* d *est le plus grand diviseur commun à* m *et* n, *on sait que* m' *et* n' *sont premiers entre eux. D'après Bezout il existe* $(u,\ v) \in \mathbb{Z}^2$ *tel que*
$$m'u - n'v = 1 \iff m'ud - n'vd = d \iff mu - nv = d$$

   (b) *Avec* u *et* v *positifs, l'égalité précédente peut s'écrire* $mu = nv + d$.
   D'où : $(a^{mu} - 1) - (a^{nv} - 1)\, a^d = \left(a^{nv+d} - 1\right) - (a^{nv} - 1)\, a^d = \left(a^{nv} \times a^d - 1\right) - (a^{nv} - 1)\, a^d = \left(a^{nv} \times a^d\right) - 1 - \left(a^{nv} \times a^d\right) + a^d = a^d - 1$.
   Le PGCD de $a^{mu} - 1$ *et* $a^{nv} - 1$ *divise aussi toute combinaison linéaire donc* $a^d - 1$.
   Or par 2a) , $a^d - 1$ *divise* $(a^{mu} - 1)$ *et* $(a^{nv} - 1)$ *donc leur PGCD .*
   Conclusion :le PGCD de $a^{mu} - 1$ *et* $a^{nv} - 1$ *est égal à* $a^d - 1$.

   (c) *Application :* $m = 63,\ n = 60$.
   $63 = 3^2 \times 7$ *et* $60 = 2 \times 3 \times 5$. *Donc PGCD*$(63\ ;\ 60) = 3$.
   On a $m = 63 = 3 \times 21 = 3m'$ *et* $n = 60 = 3 \times 20 = 3n'$.
   D'autre part 21 et 20 sont premiers et on trouve facilement
   $u = 1,\ v = 1$ *tels que* $21 \times 1 - 20 \times 1 = 1$.
   Donc $mu - nv = 63 - 60 = 3 =$ *PGCD*$(63\ ;\ 60)$. *En appliquant le résultat de la question précédente :*
   PGCD$(2^{63} - 1\ ;\ 2^{60} - 1) = 2^3 - 1 = 7$.

Exercice 11
Dans cet exercice, a *et* b *désignent des entiers strictement positifs.*

1. (a) *Supposons qu'il existe un diviseur commun* d *à* a *et à* b. *Il existe donc* a' *et* b' *tels que* $a = da'$ *et* $b = db'$.
   L'égalité $au + bv = 1$ *peut s'écrire* $da'u + db'v = 1 \iff d(a'u + b'v) = 1$.
   Ceci montre que d *divise 1, donc* $d = 1$, *ce qui montre que* a *et* b *sont premiers entre eux.*

   (b) $(a^2 + ab - b^2)^2 = 1$ *peut s'écrire* $a \times a + b(a - b) = 1$. *Avec* $u = a$ *et* $v = b - a$, *ceci montre d'après le cours que* a *et* b *sont premiers entre eux.*

2. (a) *Lorsque* $a = b$, *l'égalité s'écrit* $\left(a^2 + a^2 - a^2\right)^2 = 1 \iff a^4 = 1 \iff a = 1$.

   (b) *On vient de voir que (1 ; 1) est un couple solution.*
   Si $a = 2,\ b = 3$, *alors* $(4 + 6 - 9)^2 = 1^2 = 1$, *donc (2 ; 3) est un couple solution.*
   Si $a = 5, b = 8$, *alors* $(25 + 40 - 64)^2 = 1^2 = 1$, *donc (5 ; 8) est un couple solution..*

   (c) $(a\ ;\ b)$ *est solution donc* $(a^2 + ab - b^2)^2 = 1$ *et si* $a < b \iff a - b < 0$, *alors* $a^2 - b^2 = (a + b)(a - b) < 0$ *car* $a + b$ *somme de deux positifs est positif.*

3. (a) *Si* $(x\ ;\ y)$ *est une solution avec* $xy \neq 1$ *alors* $\left(x^2+xy-y^2\right)^2 = 1 \iff x^4+x^2y^2+y^4+2x^3y-2x^2y^2-2xy^3 = 1$.
Calculons $\left[(y-x)^2+x(y-x)-x^2\right]^2 = \left(y^2+x^2-2xy+xy-x^2-x^2\right)^2 = \left(y^2-x^2-xy\right)^2 = y^4+x^2y^2+x^4-2xy^3-2x^2y^2+x^3y = 1$ *(d'après l'égalité ci-dessus.*
De même calculons $\left(y^2+y(y+x)-(y+x)^2\right)^2 = \left(y^2+xy-x^2-2xy\right)^2 = \left(y^2-x^2-xy\right)^2$ *que l'on vient de calculer et qui est égal à* 1.
Si $(x\ ;\ y$ *est un couple solution, alors* $(y-x\ ;\ x)$ *et* $(y\ ;\ y+x)$ *en sont deux autres*

   (b) *De de* ***2. b.*** *et* ***3. a.*** *on en déduit que le couple (2 ; 3) fournit les couples (1 ; 2) et (3 ; 5) et que le couple solution (5 ; 8) donne les couples (3 ; 5) (déjà trouvé) et (8 ; 13) solutions.*

4. *Démonstration par récurrence :*

   - *Initialisation : le couple* $(a_0\ ;\ a_1) = (1\ ;\ 1)$ *est solution ;*
   - *Hérédité : supposons que le couple de rang* n, $(a_n\ ;\ a_{n+1})$ *soit solution.*

   De la question ***3. a.*** *il résulte que le couple* $(a_{n+1}\ ;\ a_{n+1}+a_n) = (a_{n+1}\ ;\ a_{n+2})$ *est aussi solution.*
   On a donc démontré par récurrence que pour tout $n \geqslant 0$, *les couples* $(a_n\ ;\ a_{n+1})$ *sont des couples solutions.*
   D'après la question ***1. b.*** *les nombres* a_n *et* a_{n+1} *sont premiers entre eux.*

   Les premiers nombres de la suite (de Fibonacci) sont 1 ; 1 ; 2 ; 3 ; 5 ; 8 13 ; 21 ; . . . : deux termes consécutifs sont premiers entre eux.

Exercice 12
$S_n = \sum_{p=1} p^3$. *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. *Démonstration par récurrence :*

   - Initialisation *: pour* $n = 1,\ S_1 = 1^3 = 1$ *et* $\left[\dfrac{1(1+1)}{2}\right]^2 = 1$.
   - Hérédité *: soit un naturel* $n \geqslant 1$ *et supposons que* $n,\ S_n = \left[\dfrac{n(n+1)}{2}\right]^2$.

     Alors $S_{n+1} = S_n + (n+1)^3 = \left[\dfrac{n(n+1)}{2}\right]^2 + (n+1)^3 = (n+1)^2\left[\dfrac{n^2}{4}+(n+1)\right] = \dfrac{(n+1)^2}{4}\left(n^2+4n+4\right) = \dfrac{(n+1)^2}{4}(n+2)^2 = \left[\dfrac{(n+1)(n+2)}{2}\right]^2$. *La formule est vraie au rang* $n+1$.

La formule est vraie au rang 1,et selle est vraie au rang n supérieur ou égal à 1, elle l'est au rang $n+1$, on a donc démontré par récurrence que pour tout $n>0$, $\sum_{p=1}^{n} p^3 = \left[\frac{n(n+1)}{2}\right]^2$.

2. *Si n est pair, alors $n=2k,\ k\in\mathbb{N}$.*

   (a) *D'après la question précédente :* $S_{2k} = \left[\frac{2k(2k+1)}{2}\right]^2 = k^2(2k+1)^2$ *et* $S_{2k+1} = \left[\frac{(2k+1)(2k+2)}{2}\right]^2 = (k+1)^2(2k+1)^2$. *Les deux sommes ont donc au moins comme diviseur commun $(2k+1)^2$.*
   Donc $PGCD(S_{2k}\ ;\ S_{2k+1}) = (2k+1)^2 PGCD(k^2\ ;\ (k+1)^2)$.

   (b) *$PGCD\ (k\ ;\ k+1)$. Comme $(k+1)-k=1$, on sait que tout diviseur commun à deux nombres divise n'importe quelle combinaison linéaire de ces deux nombres. Donc le $PGCD(k\ ;\ k+1)$ divise 1, donc puisque les nombres sont positifs, $PGCD\ (k\ ;\ k+1)=1$.*

   (c) *Calculer $PGCD(S_{2k}\ ;\ S_{2k+1})$. On vient de voir que $PGCD\ (k\ ;\ k+1)=1$, donc en utilisant la propriété admise au début, $PGCD\ (k^2\ ;\ (k+1)^2)=1$.*
   Donc en reprenant le résultat de ***2. a.****, $PGCD(S_{2k}\ ;\ S_{2k+1}) = (2k+1)^2$.*

3. *Si n est impair, alors $n=2k+1$.*

   (a) *Tout diviseur de $2k+1$ et $2k+3$ est un diviseur de leur différence 2. Donc les seuls diviseurs de $2k+1$ et $2k+3$ sont 1 ou 2. Or ces deux nombres sont impairs : le seul diviseur possible est 1.*
   $PGCD(2k+1;2k+3)=1$. Ces deux nombres sont premiers entre eux.

   (b) *De façon analogue à la résolution précédente :* $S_{2k+1} = (k+1)^2(2k+1)^2$ *et* $S_{2k+2} = (k+1)^2(2k+3)^2$.
   Donc $PGCD(S_{2k+1}\ ;\ S_{2k+2}) = (k+1)^2 PGCD\left((2k+1)^2\ ;\ (2k+3)^2\right)$.
   Or $PGCD(2k+1;2k+3)=1$ implique que $PGCD((2k+1)^2;(2k+3)^2)=1$.
   Donc finalement : $PGCD(S_{2k+1}\ ;\ S_{2k+2}) = (k+1)^2$.

4. *Si $n=2k$ le $PGCD\ (k+1)^2=1 \iff k=0$. Ceci est impossible puisque S_0 n'existe pas.*

   Si $n=2k+1$ le $PGCD\ (k+1)^2=1 \iff k=0$: il existe donc un seul couple solution $(S_1\ ;\ S_2)$ ou encore les entiers 1 et 9.

Exercice 13

$(\mathcal{E})$: $17x-24y=9$

1. (a) *On a $17\times 9-24\times 6=9$ qui est vraie.*

(b) *De* $\left\{\begin{array}{rcl} 17x-24y & = & 9 \\ 17\times 9-24\times 6 & = & 9 \end{array}\right.$ *, on déduit par différence :*
$17(x-9)-24(y-6)=0 \iff 17(x-9)=24(y-6) \quad (1)$.
Donc 24 *divise* $17(x-9)$*, mais étant premier avec* 17*, divise* $x-9$*. Il existe donc* $k\in\mathbb{Z}$ *tel que* $x-9=24k \iff x=9+24k$.
En reportant dans (1), $17\times 24k=24(y-6) \iff 17k=y-6 \iff$
$y=6+17k$.
L'ensemble des solutions de l'équation $(\mathcal{E})$ *est donc :*

$$\{(9+24k\ ;\ 6+17k)\},\ k\in\mathbb{Z}.$$

On vérifie que pour tout $k\in\mathbb{Z}$, $17(9+24k)-24(6+17k)=153+17\times 24k-144-24\times 17k=9$.

2. (a) *Si Jean a effectué* y *tours avant d'attraper le pompon à l'instant* t*, alors que le pompon a effectué* x *tours, alors* $t=17x$ *(le pompon), et comme Jean met* $\frac{3}{8}\times 24=9$ *secondes pour aller de H à A, alors pour lui* $t=9+24y$*, soit en égalant :* $17x=9+24y \iff 17x-24y=9, x\in\mathbb{N},\ y\in\mathbb{N}$.
Le couple $(x\ ;\ y)$ *doit donc être une solution de l'équation résolue à la question 1.*
Or d'après l'ensemble des solutions, le plus petit couple de nombres positifs vérifiant cette équation est le couple (9 ; 6). Donc le temps nécessaire à Jean pour attraper le pompon est $t=17\times 9=9+24\times 6=153$ *secondes soit 2 minutes et 33 secondes.*

(b) *En deux minutes Jean n'a pas le temps d'attraper le pompon.*

(c) *En raisonnant comme au a.*

- *Si Jean attrape le pompon au point B, on doit avoir* $t=\frac{17}{4}+17x=\frac{5}{8}\times 24+24y \iff 68x=43+96y \iff 68x-96y=43$.
Or le PGCD de 68 et 96 est 4 qui ne divise pas 43, donc cette équation n'a pas de solutions entières.
- *Si Jean attrape le pompon au point C, on doit avoir* $t=\frac{17}{2}+17x=\frac{7}{8}\times 24+24y \iff 34x=25+48y \iff 34x-48y=25$.
Le PGCD de 34 et 48 est 2 qui ne divise pas 25, donc cette équation n'a pas de solutions entières.
- *Si Jean attrape le pompon au point D, on doit avoir* $t=\frac{51}{4}+17x=\frac{1}{8}\times 24+24y \iff 68x=-39+96y \iff 68x-96y=-39$.
Le PGCD de 68 et 96 est 4 qui ne divise pas 39, donc cette équation n'a pas de solutions entières.
Conclusion : Jean ne peut attraper le pompon qu'au point A.

(d) *Si Jean part de E, on a toujours* $t=17x$ *et pour Jean* $t=\frac{1}{8}\times 24+24y=3+24y$*, d'où* $17x=3+24y \iff 17x-24y=3$.
Or $17\times 3-24\times 2=3$*, donc le couple* $(3\ ;\ 2)$ *est solution de cette équation.*

Le temps nécessaire à Jean pour attraper le pompon est $t = 17 \times 3 = 51$ *secondes qui sont bien inférieures aux deux minutes payées.*

Exercice 14

1. a. *Le couple* $(x, y) = (1, 1)$ *est une solution particulière évidente. L'équation* (E) *est donc équivalente à l'équation* (E') *:* $8(x-1) = 5(y-1)$.

• *Soit* (x, y) *une solution de* (E). $5 \mid 5(y-1)$ *donc* $5 \mid 8(x-1)$. *Or* $5 \wedge 8 = 1$ *donc d'après le théorème de Gauss,* $5 \mid x-1$. *Soit donc* k *dans* $\mathbb{Z}$ *tel que* $x - 1 = 5k$. *Alors* $\boxed{x = 1 + 5k}$. *L'équation* (E') *donne alors* $8(5k) = 5(y-1)$ *donc* $8k = y - 1$ *et* $\boxed{y = 1 + 8k}$. *Ainsi,* (x, y) *est solution de* (E)*, s'il existe* k *dans* $\mathbb{Z}$ *tel que* $x = 1 + 5k$ *et* $y = 1 + 8k$.

• *Conclusion :* $\boxed{S_{(E)} = \{(1 + 5k\ ,\ 1 + 8k), \quad k \in \mathbb{Z}\}}$

1. b. $8p - 5q = (m-1) - (m-4) = 3$ *donc* $\boxed{(p, q) \text{ est une solution de } (E)}$. *Par suite, il existe* k *dans* $\mathbb{Z}$ *tel que* $p = 1 + 5k$, *et donc* $m = 8p + 1 = 40k + 9$ *donc on a bien* $\boxed{m \equiv 9 \pmod{40}}$

1. c. *Ce nombre est bien sûr* $\boxed{m_0 = 2009}$, *pour lequel* $p_0 = 251$ *et* $q_0 = 401$.

2. a. $2^3 = 8 \equiv 1 \pmod 7$ *donc* $2^{3k} = (2^3)^k \equiv 1^k \equiv 1 \pmod 7$ *:* $\boxed{2^{3k} \equiv 1 \pmod 7}$

2. b. *Procédons à la division euclidienne de* 2009 *par* 3 *:* $2009 = 669 \times 3 + 2$ *donc* $2^{2009} = (2^3)^{669} \times 2^2 \equiv 1 \times 4 \equiv 4 \pmod 7$ *donc le reste dans la division euclidienne de* 2^{2009} *par* 7 *est* $\boxed{4}$.

3. a. $10 \equiv 3 \pmod 7$ *donc* $10^2 \equiv 9 \equiv 2 \pmod 7$ *donc* $\boxed{10^3 \equiv 6 \equiv -1 \pmod 7}$.

3.b. N *est divisible par* 7 *ssi* $N \equiv 0 \pmod 7$. *Cette équation est équivalente à* $a \times 10^3 + b \equiv 0 \pmod 7$, *elle-même équivalente à* $-a + b \equiv 0 \pmod 7$, *soit* $\boxed{a \equiv b \pmod 7}$

$a = 1$ *: la condition* $b \equiv 1 \pmod 7$ *avec* $b \in [0, 9]$ *donne* $b = 1$ *ou* $b = 8$. *D'où* $\boxed{N = 1001}$ *et* $\boxed{N = 1008}$.

$a = 2$ *: la condition* $b \equiv 2 \pmod 7$ *avec* $b \in [0, 9]$ *donne* $b = 2$ *ou* $b = 9$. *D'où* $\boxed{N = 2002}$ *et* $\boxed{N = 2009}$.

$a = 3$ *: la condition* $b \equiv 3 \pmod 7$ *avec* $b \in [0, 9]$ *donne* $b = 3$. *D'où* $\boxed{N = 3003}$.

$a = 4$ *: la condition* $b \equiv 4 \pmod 7$ *avec* $b \in [0, 9]$ *donne* $b = 4$. *D'où* $\boxed{N = 4004}$.

$a = 5$ *: la condition* $b \equiv 5 \pmod 7$ *avec* $b \in [0, 9]$ *donne* $b = 5$. *D'où* $\boxed{N = 5005}$.

$a = 6$ *: la condition* $b \equiv 6 \pmod 7$ *avec* $b \in [0, 9]$ *donne* $b = 6$. *D'où* $\boxed{N = 6006}$.

$a = 7$ *: la condition* $b \equiv 7 \pmod 7$ *avec* $b \in [0, 9]$ *donne* $b = 0$ *ou* $b = 7$. *D'où* $\boxed{N = 7000}$ *et* $\boxed{N = 7007}$.

$a = 8$ *: la condition* $b \equiv 8 \pmod 7$ *avec* $b \in [0, 9]$ *donne* $b = 1$ *ou* $b = 8$. *D'où* $\boxed{N = 8001}$ *et* $\boxed{N = 8008}$.

$a = 9$: la condition $b \equiv 9 \pmod 7$ avec $b \in [0, 9]$ donne $b = 2$ ou $b = 9$. D'où $\boxed{N = 9002}$ *et* $\boxed{N = 9009}$.

Exercice 15

1. (a) $239 = 13 \times 18 + 5 \iff 239 \equiv 5 \quad (13)$
   $239 = 17 \times 14 + 1 \iff 239 \equiv 1 \quad (17)$
   Donc 239 est solution du système.

   (b) $N \equiv 5 \quad (13)$ *signifie : il existe* $y \in \mathbb{Z}$ *tel que* $N = 13y + 5$;
   De même $N \equiv 1 \quad (17)$ *signifie : il existe* $x \in \mathbb{Z}$ *tel que* $N = 17x + 1$.
   Toute solution N du système peut donc s'écrire de deux façons :
   $13y + 5 = 17x + 1$. *Il en résulte que* $17x + 1 - 13y - 5 = 0 \iff 17x - 13y = 4$, *avec* $x \in \mathbb{Z},\ y \in \mathbb{Z}$.

   (c) *Une solution évidente saute aux yeux : le couple (1 ; 1)*
   On a donc le système :
   $\begin{cases} 17x - 13y & = & 4 \\ 17 \times 1 - 13 \times 1 & = & 4 \end{cases} \Rightarrow$ (*par différence*)
   $17(x-1) - 13(y-1) = 0 \iff 17(x-1) = 13(y-1) \quad (1)$.
   17 étant premier avec 13, il divise d'après le théorème de Gauss, $(y-1)$ *; il existe donc* $k \in \mathbb{Z}$ *tel que* $y - 1 = 17k \iff y = 17k + 1$.
   En reportant dans l'équation (1), on obtient $17(x-1) = 13 \times 17k \iff$
   $x - 1 = 3k \iff x = 13k + 1$.
   Les couples solutions s'écrivent sous la forme $(13k + 1\ ;\ 17k + 1),\ k \in \mathbb{Z}$.

   (d) *On a vu que* $N = 17x + 1 = 17(13k + 1) + 1 = 221k + 17 + 1 = 221k + 18$.

   (e) *On a déjà démontré ci-dessus que* $\begin{cases} N & \equiv & 5 & (13) \\ N & \equiv & 1 & (17) \end{cases} \Rightarrow N \equiv 18 \quad (221)$.
   Inversement : $N \equiv 18 \quad (221) \iff N = 221q + 18 = 17 \times 13q + 18 =$
   $17 \times 13q + 17 + 1 \iff N = 17(13q + 1) + 1 \iff N \equiv 1 \quad 17$.
   De même on peut écrire $N = 221q + 18 = 17 \times 13q + 18 = 17 \times 13q + 13 + 5 =$
   $13(17q + 1) + 5 \iff N \equiv 5 \quad [13]$.

2. (a) *La réponse est oui s'il existe un nombre N de la forme* 10^k.
   D'après le petit théorème de Fermat :
   17 est premier et 10 est un entier non divisible par 17.
   On sait qu'alors $10^{17-1} \equiv 1 \quad [17] \iff 10^{16} \equiv 1 \quad [17]$.

   (b) *On a vu que* $10^\ell \equiv 18 \quad [221] \Longrightarrow \begin{cases} 10^\ell & \equiv & 5 & [13] \\ 10^\ell & \equiv & 1 & [17] \end{cases}$
   Or
   - $10 \equiv -3 \quad [13]$
   - $10^2 \equiv 9 \quad [13]$
   - $10^3 \equiv -1 \quad [13]$

- $10^4 \equiv 3 \quad [13]$
- $10^5 \equiv 4 \quad [13]$
- $10^6 \equiv 1 \quad [13]$

Dans la division par 13, tous les nombres 10^ℓ ont donc comme reste : -3 ; -1 ; 3 ; 4 ; 9, mais jamais 5.

Conclusion : il n'existe pas d'entier ℓ tel que $10^\ell \equiv 18 \quad [221]$.

Exercice 16

Soit A l'ensemble des entiers naturels de l'intervalle $[1\ ;\ 46]$.

1. *On considère l'équation*
$$(E) : \quad 23x + 47y = 1$$
où x et y sont des entiers relatifs.

   (a) *$(-2; 1)$ est une solution de (E) car $-2 \times 23 + 1 \times 47 = 1$.*

   (b) *$(x\ ;\ y)$ solution de $(E) \Rightarrow 23x + 47y = 1$*
   $\begin{cases} 23x + 47y & = & 1 \\ -2 \times 23 + 1 \times 47 & = & 1 \end{cases} \overset{\text{par soustraction}}{\Rightarrow} 23(x+2) + 47(y-1) = 0 \Rightarrow 23(x+2) = 47(1-y)$
   Donc 23 divise $47(1-y)$, mais 47 et 23 sont premiers entre eux, d'après le théorème de Gauss, 23 divise $1 - y$.
   Donc il existe un entier relatif k tel que $1 - y = 23k$ soit $y = 1 - 23k$
   On a donc aussi, $23(x + 2) = 47 \times 23k \iff x = 47k - 2$
   On vérifie que, réciproquement, pour tout entier relatif k, $(47k - 2; 1 - 23k)$ est bien solution de (E).
   L'ensemble des solutions de (E) est l'ensemble des couples $(47k - 2; 1 - 23k)$ où $k \in \mathbb{Z}$.

   (c) $23x \equiv 1 \quad (47) \Leftrightarrow$ *il existe $y \in \mathbb{Z}$, $23x = 1 - 47y \Leftrightarrow$ il existe $k \in \mathbb{Z}$, $x = 47k - 2$ et $y = 1 - 23k$*
   De plus $x \in A \Leftrightarrow 1 \leqslant 47k - 2 \leqslant 46 \Leftrightarrow 3 \leqslant 47k \leqslant 48$.
   Or un seul multiple de 47 se trouve dans cet encadrement, c'est 47. Donc $k = 1$ et $x = 45$.
   Le seul entier x appartenant à A tel que $23x \equiv 1 \quad (47)$ est 45.

2. *Soient a et b deux entiers relatifs.*

   (a) $ab \equiv 0 \quad (47) \Leftrightarrow 47$ *divise ab.*
   Or 47 est un nombre premier, il apparait donc au moins dans l'une des deux décompositions de a ou de b. D'où le résultat.

   (b) $a^2 \equiv 1 \quad (47) \Leftrightarrow a^2 - 1 \equiv 0 \quad (47) \Leftrightarrow (a-1)(a+1) \equiv 0 \quad (47) \overset{2a}{\Rightarrow} a - 1 \equiv 0 \quad (47)$ *ou* $a + 1 \equiv 0 \quad (47) \cdots$

3. (a) *Tout entier p de A est premier avec 47, donc le théorème de Bezout assure l'existence de $(q,\ s)$ entiers relatifs tels que $qp + 47s = 1$.*
   On a alors $p \times q \equiv 1 \quad (47)$.

   (b) $p = \text{inv}(p) \Rightarrow p^2 \equiv 1 \quad (47) \overset{2b}{\Rightarrow} p \equiv -1 \quad (47)$ *ou* $p \equiv 1 \quad (47) \overset{p\in A}{\Rightarrow} p = 46$ *ou* $p = 1$
   Réciproquement 1 et 46 conviennent bien.

   (c) *Pour tout entier p de A compris entre 2 et 45, il existe (d'après 3a) un entier de A* ***distinct*** *(d'après 3b)* $\text{inv}(p)$ *tel que* $p\times\ \text{inv}(p) \equiv 1 \quad (47)$, *donc* $45! \equiv 1 \quad (47)$.
   On en déduit $46! \equiv 46 \quad (47)$ *soit enfin* $46! \equiv -1 \quad (47)$.

Exercice 17

1. (a) $2{,}009 = 11 \times 182 + 7$. *Le reste est donc égal à 7.*

   (b) *On a* $2^5 = 32 = 11 \times 2 + 10$, *donc* $2^5 \equiv 10 \mod 11$, *ou* $2^5 \equiv -1 \mod 11$ *donc* $\left(2^5\right)^2 \equiv (-1)^2 \mod 11 \iff 2^{10} \equiv 1 \mod 11$.
   Le reste dans la division euclidienne de 2^{10} *par 11 est égal à 1.*

   (c) *On a* $2^{2,009} = 2^{10\times200+9} = 2^{10\times100} \times 2^9 = \left(2^{10}\right)^{100} \times 2^9$.
   Or $2^{10} \equiv 1 \mod 11$, *donc* $\left(2^{10}\right)^{100} \equiv 1^{100} \mod 11$;
   D'autre part $2^9 = 2^5 \times 2^4$. *On a vu que* $2^5 \equiv -1 \mod 11$ *et* $2^4 = 16 \equiv 5 mod 11$, *donc par produit* $2^9 = 2^5 \times 2^4 \equiv -5 \mod 11$.
   Finalement $2^{2,009} \equiv 1 \times (-5) \mod 11$ *ou* $2^{2,009} \equiv -5 \mod 11$ *et comme* $2{,}009 \equiv 7 \mod 11$, *par somme on obtient finalement :*
   $2^{2,009} + 2{,}009 \equiv -5 + 7 \mod 11$ *ou encore* $2^{2,009} + 2{,}009 \equiv 2 \mod 11$.
   Le reste dans la division euclidienne de $2^{2,009} + 2{,}009$ *par 11 est égal à 2.*

2. (a) $A_{n+1} = 2^{n+1} + p$.
   Tout diviseur de A_n et A_{n+1} divise leur différence $2^{n+1} + p - (2^n + p) = 2^{n+1} - 2^n = 2^n(2-1) = 2^n$.
   En particulier d_n divise 2^n.

   (b) *n étant supérieur à zéro,* 2^n *est pair, donc* $A_n = 2^n + p$ *a la même parité que p.*

   (c) *D'après la question précédente A_n et A_{n+1} ont la parité de p. Donc*
   si p est pair A_n et A_{n+1} et par conséquent leur P. G. C. D. le sont aussi ;
   si p est impair A_n et A_{n+1} et par conséquent leur P. G. C. D. le sont aussi ; D'après le résultat précédent $A_{2,009}$ et $A_{2,010}$ sont impairs car 2,009 l'est et leur P. G. C. D. l'est aussi.
   Or on a vu que ce P. G. C. D., d_n divisait 2^n. *Or tous les diviseurs de* 2^n *sont pairs sauf 1 seul diviseur impair.*
   Conclusion : le P. G. C. D. de $2^{2,009} + 2{,}009$ *et* $2^{2,010} + 2{,}009$ *est égal à 1 : ils sont premiers entre eux.*

Exercice 18

1. (a) *Comme* $7 = 3\times2+1 \iff -3\times2+7\times1 = 1$, *le couple* $(-2\ ;\ 1)$ *vérifie l'équation* $3u + 7v = 1$. $3 \times (-2) + 7 \times 1 = 1$ *donne en multipliant par* 10^{2n}, $3 \times (2 \times 10^{2n}) + 7 \times 10^{2n} = 10^{2n}$.
   Le couple $(-2 \times 10^{2n}\ ;\ 10^{2n})$ *est donc une solution particulière de l'équation (E).*

(b) $\begin{cases} 3x+7y & = & 10^{2n} \\ 3\times(-2)+7\times 1 & = & 1 \end{cases} \iff \begin{cases} 3x+7y & = & 10^{2n} \\ 3\times(-2\times 10^{2n})+7\times 10^{2n} & = & 10^{2n} \end{cases}$

$\Rightarrow$ (*par différence*) $3\left(x+2\times 10^{2n}\right)+7\left(y-10^{2n}\right)=0 \iff 3\left(x+2\times 10^{2n}\right)=7\left(10^{2n}-y\right)$ (1).

3 divise $7\left(10^{2n}-y\right)$ *et est premier avec 7 : il divise donc* $10^{2n}-y$. *Il existe donc* $k\in\mathbb{Z}$ *tel que* $10^{2n}-y=3k \iff y=10^{2n}-3k$.

En reportant dans l'égalité (1) : $3\left(x+2\times 10^{2n}\right)=7\left(10^{2n}-10^{2n}+3k\right) \iff x+2\times 10^{2n}=7k \iff x=7k-2\times 10^{2n}$.

2. (a) $100=7\times 14+2 \iff 100\equiv 2 \mod 7$.

(x ; y) solution de (G) signifie $3x^2+7y^2=10^{2n} \iff 3x^2+7y^2=(10^2)^n \iff 3x^2+7y^2=100^n$.

Or $100\equiv 2 \mod 7 \Rightarrow 100^n\equiv 2^n \mod 7$.

Donc $3x^2+7y^2\equiv 2^n \mod 7$.

Mais $7y^2\equiv 0 \mod 7$, *donc finalement* $3x^2\equiv 2^n \mod 7$.

(b)

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.*	*0*	*3*	*5*	*6*	*6*	*5*	*3*

(c) *De trois choses l'une :*

- $n=3p, p\in N$; *alors* $2^{3p}=(2^3)^p=8^p$. *Or* $8\equiv 1 \mod 7 \Rightarrow 8^p\equiv 1 \mod 7$;
- $n=3p+1$; *alors* $2^{3p+1}=2^{3p}\times 2=8^p\times 2$. *Or* $8\equiv 1 \mod 7 \Rightarrow 8^p\equiv 1 \mod 7 \Rightarrow 2^{3p}\times 2\equiv 2 \mod 7$;
- $n=3p+2$; *alors* $2^{3p+2}=2^{3p}\times 2^2=4\times 2^{3p}=4\times 8^p$. *Comme* $8^p\equiv 1 \mod 7, 4\times 8^p\equiv 4 \mod 7$.

Conclusion : 2^n *est congru à 1, 2 ou 4 modulo 7.*

On vient de voir que les restes dans la division par 7 de 2^n *ne sont pas les mêmes que ceux de la division de* $3x^2$ *par 7. Donc* $3x^2$ *et* 2^n *ne peuvent être congrus modulo 7. D'après le 2. a. il n'y a donc pas de solution pour l'équation (G).*

Exercice 19
Partie A

1. *Soit* $(a,\ b)$ *un tel couple et* $d=PGCD(a,\ b)$. *Il existe deux entiers u et v premiers entre eux tels que* $a=du$ *et* $b=dv$.

Donc en remplaçant : $(du)^2=(dv)^3$ *soit* $d^2u^2=d^3v3$ *et comme*

$d\neq 0,\ u^2=dv^3$.

2. $u^2 = dv^3$ *donc* v *divise* u^2, *soit* v *divise* $u \times u$; *d'après le théorème de Gauss,* v *divise* $u \times u$ *et* v *et* u *sont premiers entre eux, donc* v *divise* u.

   $PGCD(u\ ;\ v) = 1$ *or si* v *divise* u, $PGCD(u\ ;\ v) = v$ *donc* $v = 1$.

3. *si* $a^2 = b^3$, *d'après la question précédente* $v = 1$ *donc en remplaçant dans* $b = dv$ *et* $u^2 = dv^3$, *on obtient* $b = d$ *et* $u^2 = d$ *donc* $a = du = u^3$ *et* $b = u^2$ *donc* a *et* b *sont respectivement le cube et le carré d'un même entier.*

   Réciproquement :

   Si a *et* b *sont respectivement le cube et le carré d'un même entier* d, *alors* $a = d^3$ *et* $b = d^2$ *donc* $a^2 = (d^3)^2 = d^6$ *et* $b^3 = (d^2)^3 = d^6$ *donc* $a^2 = b^3$.

   Conclusion : $a^2 = b^3$ *si et seulement si* a *et* b *sont respectivement le cube et le carré d'un même entier.*

4. *Montrer que si* n *est le carré d'un nombre entier naturel et le cube d'un autre entier, alors* $n \equiv 0 \quad [7]$ *ou* $n \equiv 1 \quad [7]$.

   S'il existe deux entiers a *et* b *tels que* $n = a^2 = b^3$ *alors d'après la question précédente il existe un entier* d *tel que* $a = d^3$ *et* $b = k^2$ *donc tel que*

   $n = d^6$.

d	0	1	2	3	4	5	6
d^6	0	1	64	729	4,096	15,625	46,656
$d^6 \equiv \ldots \quad [7]$	0	1	1	1	1	1	1

   donc $n \equiv 0 \quad [7]$ *ou* $n \equiv 1 \quad [7]$.

   Remarque : *On peut également dire :*

   - *si* $d = 0$, *alors* $n \equiv 0 \quad [7]$;
   - *si* $d = 1$, *alors* $n \equiv 1 \quad [7]$;
   - *si* $d > 1$ *et* n *multiple de 7, alors* $n \equiv 0 \quad [7]$;
   - *si* $d > 1$ *et* d *non multiple de* 7, *donc* d *premier, alors d'après le petit théorème de Fermat :*
     $d^{7-1} \equiv 1 \quad [7]$ *ou encore* $d^6 = n \equiv 1 \quad [7]$.

Partie B

Dans l'espace muni d'un repère orthonormal $(O; \overrightarrow{i}; \overrightarrow{j}; \overrightarrow{k})$ *on considère 1a surface* S *d'équation* $x^2 \times y^2 = z^3$.

Pour tout réel λ, *on note* $\mathcal{C}_\lambda$ *la section de* S *par le plan d'équation* $z = \lambda$.

1. $\mathcal{C}_\lambda$ *a pour équations :* $x^2 \times y^2 = \lambda^3$ *et* $z = \lambda$.

   Si $\lambda < 0$ *il est impossible que* $x^2 \times y^2$ *qui est positif ou nul, soit égal à* λ *donc* $\mathcal{C}_\lambda$ *est le graphique 2.*

Si $\lambda = 0$ alors $x^2 \times y^2 = 0 \iff x = 0$ ou $y = 0$ donc $\mathcal{C}_\lambda = \mathcal{C}_0$ est le graphique 1, $\mathcal{C}_\lambda$ est la réunion des deux axes dans le plan d'équation $z = \lambda = 0$.

Si $\lambda > 0$ par élimination, le graphique 3 représente la courbe $\mathcal{C}_\lambda$.

Si $\lambda > 0$, $\mathcal{C}_\lambda$ est l'ensemble des points du plan d'équation $z = \lambda$ tels que $x^2 \times y^2 = \lambda^3$ ce qui se décompose en deux parties : $xy = \sqrt{\lambda^3}$ et $xy = -\sqrt{\lambda^3}$ soit $y = \dfrac{\sqrt{\lambda^3}}{x}$ et $y = -\dfrac{\sqrt{\lambda^3}}{x}$.

$\mathcal{C}_\lambda$, quand $\lambda > 0$, est donc la réunion de deux hyperboles équilatères.

2. (a) *$\mathcal{C}_{25}$ a pour équations : soit $y = \dfrac{\sqrt{25^3}}{x}$ soit $y = -\dfrac{\sqrt{25^3}}{x}$ dans le plan d'équation $z = 25$.*

   Donc $\mathcal{C}_{25}$ a pour équations : soit $y = \dfrac{125}{x}$ soit $y = -\dfrac{125}{x}$ dans le plan d'équation $z = 25$.

   Si les coordonnées des points de $\mathcal{C}_{25}$ sont des nombres entiers strictement positifs alors $y > 0$ et $\dfrac{125}{x}$ est un entier strictement positif donc x est un entier strictement positif qui divise 125, soit $x = 1$ ou $x = 5$ ou $x = 25$ ou $x = 125$.

   Les points cherchés ont donc pour coordonnées $(1\ ;\ 125\ ;\ 25)$, $(5\ ;\ 25\ ;\ 25)$, $(25\ ;\ 5\ ;\ 25)$ *et* $(125\ ;\ 1\ ;\ 25)$

   (b) *$\mathcal{C}_{2{,}010}$ a pour équations : $(xy)^2 = z^3$ avec $z = 2{,}010$.*

   D'après la question 3. a. : $a^2 = b^3$ si et seulement si a et b sont respectivement le cube et le carré d'un même entier, avec ici $a = xy$ et $b = z$; or 2,010 n'est pas le carré d'un nombre entier

   (2,010 $= 2 \times 3 \times 5 \times 67$) donc l'équation $(xy)^2 = 2010^3$ n'a pas de solutions entières.

Exercice 20

Un bit est un symbole informatique élémentaire valant soit 0, soit 1.

Partie A : ligne de transmission

Une ligne de transmission transporte des bits de données selon le modèle suivant :

- *elle transmet le bit de façon correcte avec une probabilité p ;*
- *elle transmet le bit de façon erronée (en changeant le 1 en 0 ou le 0 en 1) avec une probabilité $1 - p$.*

On assemble bout à bout plusieurs lignes de ce type, et on suppose qu'elles introduisent des erreurs de façon indépendante les unes des autres.

On étudie la transmission d'un seul bit, ayant pour valeur 1 au début de la transmission. Après avoir traversé n lignes de transmission, on note :

- p_n *la probabilité que le bit reçu ait pour valeur* 1 ;
- q_n *la probabilité que le bit reçu ait pour valeur* 0.

On a donc $p_0 = 1$ *et* $q_0 = 0$.
On définit les matrices suivantes : $A = \begin{pmatrix} p & 1-p \\ 1-p & p \end{pmatrix}$ $X_n = \begin{pmatrix} p_n \\ q_n \end{pmatrix}$ $P = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.
On admet que, pour tout entier n, *on a :* $X_{n+1} = AX_n$ *et donc,* $X_n = A^n X_0$.

1. (a) *Si on trouve une matrice inverse à la matrice* P, *on prouve ainsi que la matrice* P *est inversible.*
   La calculatrice donne $P^{-1} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} \end{pmatrix}$ *donc la matrice* P *est inversible de matrice inverse* P^{-1}.
   Remarques
   - *On peut démontrer que la matrice* P *est inversible en utilisant son déterminant: le déterminant de la matrice* P *est* $1 \times (-1) - 1 \times 1 = -2 \neq 0$ *donc la matrice* P *est inversible.*
   - *On peut aussi chercher une matrice* $Q = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *telle que* $P \times Q = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ *et vérifier ensuite que* $Q \times P = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. *Cela prouve que* P *est inversible et a pour inverse* Q.

   (b) *On pose :* $D = \begin{pmatrix} 1 & 0 \\ 0 & 2p-1 \end{pmatrix}$.
   $PD = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & 2p-1 \end{pmatrix} = \begin{pmatrix} 1 & 2p-1 \\ 1 & -2p+1 \end{pmatrix}$
   $PDP^{-1} = \begin{pmatrix} 1 & 2p-1 \\ 1 & -2p+1 \end{pmatrix} \times \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{2}+p-\frac{1}{2} & \frac{1}{2}-p+\frac{1}{2} \\ \frac{1}{2}-p+\frac{1}{2} & \frac{1}{2}+p-\frac{1}{2} \end{pmatrix} = \begin{pmatrix} p & 1-p \\ 1-p & p \end{pmatrix} =$
   A

   (c) *Soit* $\mathcal{P}_n$ *la propriété* $A^n = PD^nP^{-1}$.
   - ***Initialisation***
     Pour $n = 1$, *on sait que* $A = PDP^{-1}$ *donc la propriété est vraie au rang 1.*
   - ***Hérédité***
     Soit n *un réel quelconque supérieur ou égal à 1 tel que* $\mathcal{P}_n$ *soit vraie, c'est-à-dire* $A^n = PD^nP^{-1}$.
     $A^{n+1} = A^n \times A = (PD^nP^{-1}) \times (PDP^{-1}) = PD^n\left(P^{-1}P\right)DP^{-1} = P\left(D^nD\right)P^{-1} = PD^{n+1}P^{-1}$
     Donc la propriété est vraie au rang $n+1$.
   - ***Conclusion***
     La propriété est vraie pour $n = 1$ *et elle est héréditaire pour tout* $n < 1$; *d'après le principe de récurrence, la propriété est vraie pour tout* $n < 1$.

On a donc démontré, que pour tout entier naturel $n < 1$, on a $A^n = PD^nP^{-1}$.

(d) On a vu successivement que $X_n = \begin{pmatrix} p_n \\ q_n \end{pmatrix}$, que $X_n = A^nX_0$, et que $A^n = PD^nP^{-1}$.

Le logiciel de calcul formel donne $PD^nP^{-1}X_0 = \begin{pmatrix} \dfrac{(2p-1)^n+1}{2} \\ \dfrac{-(2p-1)^n+1}{2} \end{pmatrix}$ soit $\begin{pmatrix} p_n \\ q_n \end{pmatrix} = \begin{pmatrix} \dfrac{(2p-1)^n+1}{2} \\ \dfrac{-(2p-1)^n+1}{2} \end{pmatrix}$.

On peut donc en déduire que $q_n = \dfrac{-(2p-1)^n+1}{2}$.

2. *On suppose dans cette question que p vaut $0,98$. On souhaite que la probabilité que le bit reçu ait pour valeur 0 soit inférieure ou égale à $0,25$.*

On cherche donc n tel que $q_n < 0,25$ avec $p = 0,98$ donc $2p - 1 = 0,96$. On résout l'inéquation:

$q_n < 0,25 \iff \dfrac{-0,96^n+1}{2} < 0,25 \iff -0,96^n + 1 < 0,5 \iff 0,5 < 0,96^n \iff \ln(0,5) < \ln(0,96^n)$

$\iff \ln(0,5) < n\ln(0,96) \iff \dfrac{\ln(0,5)}{\ln(0,96)} > n$

$\dfrac{\ln(0,5)}{\ln(0,96)} \approx 16,98$ *donc on peut aligner au maximum 16 lignes de transmission pour que la probabilité que le bit reçu ait pour valeur 0 soit inférieure ou égale à $0,25$.*

Partie B : étude d'un code correcteur, le code de Hamming (7, 4)

On considère un mot formé de 4 bits que l'on note b_1, b_2, b_3 et b_4.

On ajoute à cette liste une clé de contrôle *$c_1c_2c_3$ formée de trois bits :*

- *c_1 est le reste de la division euclidienne de $b_2 + b_3 + b_4$ par 2 ;*
- *c_2 est le reste de la division euclidienne de $b_1 + b_3 + b_4$ par 2 ;*
- *c_3 est le reste de la di vision euclidienne de $b_1 + b_2 + b_4$ par 2.*

On appelle alors message la suite de 7 bits formée des 4 bits du mot et des 3 bits de contrôle.

1. *Préliminaires*

   (a) *c_1, c_2 et c_3 sont des restes dans une division par 2 donc ils ne peuvent être égaux qu'à 0 ou à 1.*

(b) *Soit le mot* 1001*; on a donc* $b_1 = 1$, $b_2 = 0$, $b_3 = 0$ *et* $b_4 = 1$.

- c_1 *est le reste de la division euclidienne de* $b_2 + b_3 + b_4 = 1$ *par 2 donc* $c_1 = 1$*;*
- c_2 *est le reste de la division euclidienne de* $b_1 + b_3 + b_4 = 2$ *par 2 donc* $c_2 = 0$*;*
- c_3 *est le reste de la di vision euclidienne de* $b_1 + b_2 + b_4 = 2$ *par 2 donc* $c_3 = 0$.

La clé de contrôle du mot 1001 est 100.

2. *Soit* $b_1b_2b_3b_4$ *un mot de 4 bits et* $c_1c_2c_3$ *la clé associée.*

   Si on change la valeur de b_1 *en* b'_1*, on aura* $b'_1 \equiv b_1 + 1 \pmod 2$.

   - *la valeur de* c_1 *ne dépend pas de* b_1 *donc est inchangée;*
   - $b'_1 + b_3 + b_4 \equiv b_1 + b_3 + b_4 + 1 \pmod 2$ *donc* c_2 *est modifiée;*
   - $b'_1 + b_2 + b_4 \equiv b_1 + b_2 + b_4 + 1 \pmod 2$ *donc* c_3 *est modifiée.*

3. *On suppose que, durant la transmission du message, au plus un des 7 bits a été transmis de façon erronée. À partir des quatre premiers bits du message reçu, on recalcule les 3 bits de contrôle, et on les compare avec les bits de contrôle reçus.*

   On complète le tableau ci-dessous:

Bit erroné / *Bit de contrôle calculé*	b_1	b_2	b_3	b_4	c_1	c_2	c_3	*Aucun*
c_1	J	F	F	F	F	J	J	J
c_2	F	J	F	F	J	F	J	J
c_3	F	F	J	F	J	J	F	J

4. *Les huit triplets du tableau* $(J\ ;\ F\ ;\ F)$, $(F\ ;\ J\ ;\ F)$, …, $(J\ ;\ J\ ;\ J)$, *sont tous différents. Quand on reçoit un message, on calcule les codes de contrôle et on les compare avec ceux qu'on a reçus. Selon le triplet obtenu, on sait donc quel est le bit erroné, s'il y en a un.*

5. *Voici deux messages de 7 bits :* $A = 0100010$ *et* $B = 1101001$.

   On admet que chacun d'eux comporte au plus une erreur de transmission.

   - *Pour le message* $A = 0100010$*:*
     - $b_2 + b_3 + b_4 = 1 + 0 + 0 = 1$ *a pour reste 1 dans la division par 2.*
     - $b_1 + b_3 + b_4 = 0 + 0 + 0 = 0$ *a pour reste 0 dans la division par 2.*
     - $b_1 + b_2 + b_4 = 0 + 1 + 0 = 1$ *a pour reste 1 dans la division par 2.*

   Donc le code correct est 101 alors que le code reçu est 010; la différence entre les deux codes correspond au triplet $(F\ ;\ F\ ;\ F)$.

   D'après le tableau, c'est donc b_4 *qui est erroné et le bon message est* 0101010.

- *Pour le message* $B = 1101001$*:*
  - $b_2 + b_3 + b_4 = 1 + 0 + 1 = 2$ *a pour reste 0 dans la division par 2.*
  - $b_1 + b_3 + b_4 = 1 + 0 + 1 = 2$ *a pour reste 0 dans la division par 2.*
  - $b_1 + b_2 + b_4 = 1 + 1 + 2 = 3$ *a pour reste 1 dans la division par 2.*

  Donc le code correct est 001 et est identique au code reçu; le message B *ne contient pas d'erreur.*