Division euclidienne - congruence

Exercice 1

Soit *n* et *a* deux entiers naturels non nuls.

1) On suppose que a divise (42n + 37) et a divise (7n + 4). Montrer que a divise 13.

2) En déduire les valeurs possibles de *a*.

Exercice 2

1) Ecrie la division euclidienne de 1 000 par 13.

Soit n un entier naturel.

2) Déterminer, suivant les valeurs de n, le reste de la division euclidienne de 10^{3n} par 13.

3) Déterminer, suivant les valeurs de n, le reste de la division euclidienne de $10^{3n+1}+10^{3n}$ par 13.

4) En déduire le reste de la division euclidienne par *13* de *11 000 000 000 000*.

5) Quel est le reste de la division euclidienne par 13 de $25\times10^{15}+1$.

Exercice 3

1) Montrer que $5^0\equiv1(13)$, $5^1\equiv5(13)$, $5^2\equiv-1(13)$, $5^3\equiv-5(13)$

2) En déduire que pour tout entier naturel *k* :

$5^{4k}\equiv1(13)$; $5^{4k+1}\equiv5(13)$; $5^{4k+2}\equiv-1(13)$; $5^{4k+3}\equiv-5(13)$.

3) Déterminer l'ensemble des entiers naturels n tels que: $5^{2n}+5^n\equiv0(13)$.

Inverse modulo

Exercice 4

1) On considère l'ensemble $A_7=\{1;2;3;4;5;6\}$.

a) Pour tout élément a de A_7 , écrire dans le tableau suivant (sans justifier) l'unique élément y de A_7 tel que $a\,y\equiv 1 \pmod 7$.

a	1	2	3	4	5	6
y						

b) Pour x entier relatif, démontrer que l'équation $3x\equiv 5 \pmod 7$ équivaut à $x\equiv 4 \pmod 7$.

c) Si a est un élément de A_7 , montrer que les seuls entiers relatifs x solutions de l'équation $a\,x\equiv 0 \pmod 7$ sont les multiples de 7.

2) Dans toute cette question, p est un nombre premier supérieur ou égal à 3.
On considère l'ensemble $A_p=\{1;2;...;p-1\}$ des entiers naturels non nuls et strictement inférieurs à p. Soit a un élément de A_p .

a) Vérifier que a^{p-2} est une solution de l'équation $a\,x\equiv 1 \pmod p$.

b) On note r le reste dans la division euclidienne de a^{p-2} par p. Démontrer que r est l'unique solution x dans A_p de l'équation $a\,x\equiv 1 \pmod p$.

c) Soient x et y deux entiers relatifs. Démontrer que $x\,y\equiv 0 \pmod p$ si et seulement si x est un multiple de p ou y est un multiple de p.

d) Application: $p=31$.

Résoudre dans A_{31} les équations $2x\equiv 1 \pmod{31}$ et $3x\equiv 1 \pmod{31}$.
A l'aide des résultats précédents, résoudre dans $\mathbb{Z}$ l'équation $6x^2-5x+1\equiv 0 \pmod{31}$.

Equation du type ax + by = c où a, b et c sont des entiers

Exercice 5

1. On considère l'équation (E_1) :
$$6x - 5y = 7$$
dont les inconnues x et y sont des entiers relatifs.
   (a) On suppose que le couple d'entiers (x, y) vérifie $6x - 5y = 7$.
   Démontrer que $x \equiv 2\ [5]$
   (b) En déduire tous les couples d'entiers, solutions de l'équation (E_1).

2. *Application* : dans le plan muni d'un repère $(O\,;\ \vec{i},\ \vec{j})$, on note Δ la droite d'équation
$$6x - 5y = 7$$
Déterminer le nombre de points de Δ dont les coordonnées sont des entiers naturels et dont l'abscisse est inférieure à 500.

3. On considère à présent l'équation (E_2) :
$$6x^2 - 5y^2 = 7$$
dont les inconnues x et y sont des entiers relatifs.
   (a) Vérifier que si le couple $(x\,;y)$ est solution de (E_2), alors
$$x^2 \equiv 2 \quad [5]$$
   (b) Démontrer que, pour tout entier α, α^2 est congru à 0, à 1 ou à 4 modulo 5.
   (c) Quel est l'ensemble solution de l'équation (E_2) ?

Exercice 6

1. On considère l'équation (E) : $109x - 226y = 1$ où x et y sont des entiers relatifs.

a. Déterminer le pgcd de 109 et 226. Que peut-on en conclure pour l'équation (E) ?
b. Montrer que l'ensemble de solutions de (E) est l'ensemble des couples de la forme

$(141+226k, 68+109k)$, où k appartient à **Z.**

En déduire qu'il existe un unique entier naturel non nul d inférieur ou égal à 226 et un unique entier naturel non nul e tels que $109d = 1+226e$. (On précisera les valeurs des entiers d et e.)

2. Démontrer que 227 est un nombre premier.

3. On note A l'ensemble des 227 entiers naturels a tels que $a \leq 226$.

On considère les deux fonctions f et g de A dans A définies de la manière suivante :

à tout entier de A, f associe le reste de la division euclidienne de a^{109} par 227,

à tout entier de A, g associe le reste de la division euclidienne de a^{141} par 227.

a. Vérifier que $g[f(0)] = 0$.

On rappele *le résultat* suivant *appelé* petit théorème *de Fermat :*

Si p est un nombre premier et a un entier non divisible par p alors $a^{p-1} \equiv 1$ modulo p.

b. Montrer que, quel que soit l'entier non nul a de A, $a^{226} \equiv 1$ [modulo 227].
c. En utilisant **1. b.,** en déduire que, quel que soit l'entier non nul a de A. $g[f(a)] = a$. Que peut-on dire de $f[(g(a)] = a$ *?*

Exercice7

1. On considère l'équation (E) : $17x - 6y = 2$, où x et y sont des entiers.

a) Résoudre dans $\mathbb{N}^2$ l'équation $17x = 6y$.

b) A l'aide de l'algorithme d'Euclide, déterminer une solution particulière de $17x - 6y = 1$.
Montrer que le couple $(-1 ; -3)$ est une solution particulière de l'équation $17x - 6y = 1$, en déduire une solution particulière de l'équation (E).

c) En déduire tous les couples de $\mathbb{Z}^2$ solution de (E).

d) Montrer que le pgcd des couples solution de (E) est 1 ou 2.

e) Déterminer les couples $(x ; y)$ solution de (E) dont le pgcd est 2.

f) Déterminer le couple $(x_0 ; y_0)$ solution de (E) tel que : $\text{pgcd}(x_0 ; y_0) = 2$ et $100 \leq y_0 \leq 150$.

Exercice 1

1) $a\,|\,(42n+37)$ *et* $a\,|\,(7n+4) \Rightarrow a\,|\,(42n+37)-6(7n+4)$ *soit* $a\,|\,13$.

2) L'ensemble des diviseurs de 13 est: $D_{13}=\{1,13\}$ donc $\boxed{a=1 \text{ ou } a=13}$

Exercice 2

Rappel des propriétés des congruences:

$a\equiv b(n)\Leftrightarrow a-b=k\times n$	$a\equiv b(n)$ *et* $a'\equiv b'(n)\Leftrightarrow a+a'\equiv b+b'(n)$
$a\equiv b(n)\Leftrightarrow a^p\equiv b^p(n)$ $(p\in\mathbb{N})$	$a\equiv b(n)$ *et* $a'\equiv b'(n)\Leftrightarrow a\times a'\equiv b\times b'(n)$

1) $1000=76\times13+12\Leftrightarrow 10^3\equiv 12(13)$

2) $10^3\equiv 12(13)\Leftrightarrow \boxed{10^3\equiv -1(13)}$ *car* $(10^3=76\times13+12=76\times13+13-1=77\times13-1)$.

si $a\equiv b(n)$ alors $a^p\equiv b^p(n)$:

$10^3\equiv -1(13)\Leftrightarrow \left(10^3\right)^n\equiv(-1)^n(13)\Leftrightarrow 10^{3n}\equiv(-1)^n(13)$

si n est pair alors $10^{3n}\equiv 1(13)$; si n est impair alors $10^{3n}\equiv -1(13)\equiv 12(13)$.

3) Le reste de la division de $10^{3n+1}+10^{3n}$ par 13 :

si n est pair: $10^{3n}\equiv 1(13)$ *et* $10^{3n+1}=10\times10^{3n}\Leftrightarrow 10^{3n+1}\equiv 10(13)$

d'où : $10^{3n+1}+10^{3n}\equiv 1+10(13)$ *soit* $\boxed{10^{3n+1}+10^{3n}\equiv 11(13)}$.

si n est impair: $10^{3n}\equiv -1(13)\equiv 12(13)$ *et* $10^{3n+1}=-10(13)$

donc $\boxed{10^{3n+1}+10^{3n}\equiv 2(13)}$.

4) $11000\,000\,000\,000=11\cdot10^{12}$ $10^{12}=10^{3\times4}$,$10^{12}\equiv-(1)^4(13)$ *soit* $10^{12}\equiv 1(13)$

donc $\boxed{11\cdot10^{12}\equiv 11(13)}$

5) $10^{15}=10^{3\times5}\equiv -1(13)$ et $25=12+13\Leftrightarrow 25\equiv 12(13)\Leftrightarrow 25\equiv -1(13)$

d'où: $25\times10^{15}\equiv 1(13)$ *ainsi* $\boxed{25\times10^{15}+1\equiv 2(13)}$

Exercice 3

1) En utilisant les propriétés rappelées dans l'exercice précédent on obtient:

$5^0 = 1+0\times 13 \Rightarrow \boxed{5^0 \equiv 1(13)}, 5^1 = 5+0\times 13 \Rightarrow \boxed{5^1 \equiv 5(13)}, 5^2 = 12+13 \Rightarrow 5^2 \equiv 12(13) \Leftrightarrow \boxed{5^2 \equiv -1(13)}.$

$5^3 = 5\times 5^2 \Rightarrow 5^3 \equiv 5\times -1(13)$ soit $\boxed{5^3 \equiv -5(13)}$.

2) Pour tout entier naturel *k*,

$5^{4k} = \left(5^4\right)^k \equiv (1)^k\ (13)$ soit $\boxed{5^{4k} \equiv 1(13)}$, $5^{4k+1} = 5\times 5^{4k} \Rightarrow \boxed{5^{4k+1} \equiv 5(13)}$.

$5^{4k+2} = 5^{4k}\times 5^2 \Leftrightarrow \boxed{5^{4k+2} \equiv -1(13)}$, $5^{4k+3} = 5^{4k}\times 5^3 \Leftrightarrow \boxed{5^{4k+3} \equiv -5(13)}$.

3) Ensemble des entiers naturels n tels que: $5^{2n} + 5^n \equiv 0(13)$

Tout entier naturel *n* s'écrit sous la forme: $n = 4k + r$ avec $0 \le r \le 3$

En utilisant les résultats précédents:

si $r = 0$: $5^{2n} + 5^n = \left(5^{4k}\right)^2 + 5^{4k}$ $5^{4k} \equiv 1(13)$ donc $\boxed{5^{2n} + 5^n \equiv 2(13)}$.

si $r = 1$: $5^{2n} + 5^n = \left(5^{4k+2}\right)^2 + 5^{4k+2}$, $5^{4k+2} \equiv -1(13)$ et $\left(5^{4k+2}\right)^2 \equiv 1(13)$ donc $\boxed{5^{2n} + 5^n \equiv 0(13)}$

si $r = 2$: $5^{2n} + 5^n = \left(5^{4k+3}\right)^2 + 5^{4k+3}$, $5^{4k+3} \equiv -5(13)$ et $\left(5^{4k+3}\right)^2 \equiv 5^2(13) \equiv -1(13)$

donc $5^{2n} + 5^n \equiv -1-5(13) \Leftrightarrow 5^{2n} + 5^n \equiv -6(13) \Leftrightarrow \boxed{5^{2n} + 5^n \equiv 7(13)}$.

Conclusion:

$\boxed{5^{2n} + 5^n \equiv 0(13) \text{ si } n = 4k+2}$.

Inverse modulo

Exercice 4

1) a)

x	1	2	3	4	5	6
y	1	4	5	2	3	6

1) b) *Remarque:* **on ne peut pas résoudre des congruences par équivalences, car on ne peut diviser chaque membre par un même nombre.**

Modulo 7:

- Si $3x \equiv 5$ alors $5\times 3x \equiv 5\times 5$ alors $x \equiv 4$
- Réciproque: Si $x \equiv 4$ alors $3\times x \equiv 3\times 4$ alors $3x \equiv 5$

Conclusion $\boxed{3x \equiv 5 \Leftrightarrow x \equiv 4 \quad (mod\ 7)}$

1) c) $ax \equiv 0 \quad (mod\ 7)$ alors 7 divise ax , or 7 est premier avec a (car 7 est premier, et $1 \leqslant a \leqslant 6$), alors d'après le th de GAUSS, 7 divise x . La réciproque est évidente: si *x* est multiple de 7 alors $ax \equiv 0 \quad (mod\ 7)$.

Conclusion: Les solutions de l'équation $ax \equiv 0 \quad (mod\ 7)$ sont les multiples de 7.

Autre méthode: En reprenant les notations de la question 1) a): Pour tout *a* de A_p , il existe *y* dans A_p tel que $ay \equiv 1 \quad (mod\ 7)$. Si $ax \equiv 0 \quad (mod\ 7)$ alors $yax \equiv 0 \quad (mod\ 7)$, c'est-à-dire $x \equiv 0 \quad (mod\ 7)$.

Réciproque ... Conclusion ...

2) a) $a\cdot a^{p-2}\equiv a^{p-1} \pmod p$ or p est premier, et p est premier avec a (car $0<a<p$), alors d'après le petit théorème de FERMAT, $\boxed{a^{p-1}\equiv 1 \pmod p}$.

2) b) On note r le reste dans la division euclidienne de a^{p-2} par p, alors d'après le th de la division euclidienne, il existe un entier naturel q tel que $a^{p-2}=pq+r$ avec $0\leqslant r<p$.

- $\begin{aligned} a^{p-1}\equiv 1 &\Leftrightarrow a\cdot a^{p-2}\equiv 1 \pmod p \\ &\Leftrightarrow a(pq+r)\equiv 1 \pmod p \\ &\Leftrightarrow a\cdot p\cdot q+a\cdot r\equiv 1 \pmod p \\ &\Leftrightarrow a\cdot r\equiv 1 \pmod p \end{aligned}$.

  Ainsi r est une solution de l'équation $a^{p-1}\equiv 1 \pmod p$.
- De plus r est un élément de A_p , car par définition de la division euclidienne $0\leqslant r<p$, et $p\neq 0$ (car sinon $a\cdot r\equiv 0 \pmod p$).
- Il reste à démontrer que r est l'unique solution dans A_p de cette équation. Démonstration par l'absurde:
  Supposons qu'il existe un entier s de A_p tel que $a\cdot s\equiv 1 \pmod p$.
  Par soustraction membre à membre des congruences $a\cdot r\equiv 1 \pmod p$ et $a\cdot s\equiv 1 \pmod p$, il vient $a(r-s)\equiv 0 \pmod p$, c'est-à-dire p divise $a(r-s)$. Or p est premier avec a (car p est premier et $0<a<p$), alors d'après le th de GAUSS, p divise $r-s$.
  Mais $\begin{cases}0<r<p\\0<s<p\end{cases}$ alors $\begin{cases}0<r<p\\-p<-s<0\end{cases}$ alors par somme memmbre à membre $-p<r-s<p$.
  Ainsi $r-s$ est un multiple de p et est élément de $]-p\,;p[$, d'où $r-s=0$; d'où $r=s$.

2) c) Si $xy\equiv 0 \pmod p$, alors p divise xy ; or p est premier, donc p divise x ou p divise y . (En effet, comme p divise xy, ou bien p divise x, ou bien p ne divise pas x et alors il est premier avec x; par application du théorème de GAUSS, p divise alors y).

La réciproque est évidente: si x est multiple de p ou si y est multiple de p alors $xy\equiv 0 \pmod p$.
Conclusion: $\boxed{xy\equiv 0 \pmod p}$ si et seulement si x est multiple de p ou y est multiple de p

2) d) Application: p=31 31 étant premier, on peut appliquer les résultats des questions 2)a) à 2)c).

- D'après 2)b), l'unique solution dans A_{31} de l'équation $2x\equiv 1 \pmod 7$ est le reste dans la division euclidienne de 2^{29} par 31 . Or $2^5\equiv 1 \pmod{31}$ donc $2^{29}\equiv(2^5)^5\times 2^4\equiv 2^4\equiv 16$. Et $0\leqslant 16<31$. Donc 16 est le reste cherché. D'où $\boxed{\text{l'unique solution dans } A_{31} \text{ est 16.}}$

- D'après 2)b), l'unique solution dans A_{31} de l'équation $3x\equiv 1 \pmod 7$ est le reste dans la division euclidienne de 3^{29} par 31 . Or $3^2\equiv 9$ $3^3\equiv -4$, d'où
  $3^{29}\equiv 3^{3\times 9+2}\equiv(3^3)^9\times 3^2\equiv(-4)^9\times 3^2\equiv -2^{18}\times 3^2\equiv -2^{15}\times 2^3\times 3^2\equiv -1\times 8\times 9\equiv -72\equiv 21$
  Et $0\leqslant 21<31$. Donc 21 est le reste cherché. D'où $\boxed{\text{l'unique solution dans } A_{31} \text{ est 21.}}$

- $\begin{aligned} 6x^2-5x+1\equiv 0 \pmod{31} &\Leftrightarrow (2x-1)(3x-1)\equiv 0 \pmod{31} \\ &\Leftrightarrow 2x-1\equiv 0 \text{ ou } 3x-1\equiv 0 \pmod{31} \quad \text{d'après 2) c)} \\ &\Leftrightarrow x\equiv 16 \text{ ou } x\equiv 21 \pmod{31} \end{aligned}$

  Conclusion: $\boxed{S=\{31k+16\,;31k+21 \text{ avec } k\in\mathbb{Z}\}}$

Exercice 5

1. (a) **Analyse** : on suppose que le couple d'entiers (x, y) vérifie $6x - 5y = 7$.
Alors $6x = 7 + 5y$ donc $6x \equiv 7\ [5]$. Or $6 \equiv 1\ [5]$ car $6 = 1 + 5 \times 1$.
Donc $6x \equiv x\ [5]$. De plus $7 \equiv 2\ [5]$ car $7 = 2 + 5 \times 1$.
En conséquence $x \equiv 2\ [5]$.

(b) On déduit de la question précédente qu'il existe un entier relatif k tel que $\boxed{x = 2 + 5k}$. Or $6x - 5y = 7$.
Donc $5y = 6x - 7 = 6(2 + 5k) - 7 = 12 + 30k - 7 = 5 + 30k = 5(1 + 6k)$.
Ainsi $\boxed{y = 1 + 6k}$.

Vérification : posons $x = 2 + 5k$ et $y = 1 + 6k$ avec $k \in \mathbb{Z}$.
Alors $6x - 5y = 6(2 + 5k) - 5(1 + 6k) = 12 + 30k - 5 - 30k = 12 - 5 = 7$.

Conclusion : l'équation (E_1) admet pour ensemble solution :

$$\mathcal{S} = \{(2 + 5k\,;\, 1 + 6k) \quad \text{avec } k \in \mathbb{Z}\}$$

2. Chercher les points de Δ dont les coordonnées sont des entiers naturels et dont l'abscisse est inférieure à 500 revient à chercher les couples d'entiers $(x; y)$ solutions de (E_1) tels que $0 \leq x \leq 500$ et $0 \leq y$.
On est amené à déterminer le nombre de solutions du système :

$$\begin{cases} x = 2 + 5k\ (k \in \mathbb{Z}) \\ y = 1 + 6k \\ 0 \leq x \leq 500 \\ 0 \leq y \end{cases} \iff \begin{cases} x = 2 + 5k\ (k \in \mathbb{Z}) \\ y = 1 + 6k \\ 0 \leq 2 + 5k \leq 500 \\ 0 \leq 1 + 3k \end{cases}$$

Or

$$\begin{cases} k \in \mathbb{Z} \\ 0 \leq 2 + 5k \leq 500 \\ 0 \leq 1 + 3k \end{cases} \iff \begin{cases} k \in \mathbb{Z} \\ -2/5 \leq k \leq 498/5 \\ -1/3 \leq k \end{cases} \iff \begin{cases} k \in \mathbb{Z} \\ 0 \leq k \leq 99 \end{cases}$$

Il y a donc exactement $\boxed{\text{100 points qui conviennent}}$

3. (a) Si le couple $(x\,;y)$ est solution de (E_2), alors $6x^2 = 7 + 5y^2$ avec $y^2 \in \mathbb{N}$ donc $6x^2 \equiv 7\ [5]$. Or $6 \equiv 1\ [5]$. Donc $6x^2 \equiv x^2\ [5]$. De plus $7 \equiv 2\ [5]$.
Ainsi $x^2 \equiv 2\ [5]$.

(b) Soit α un entier fixé. D'après le théorème de la division euclidienne, il existe un unique couple $(q; r)$ d'entiers tel que $\alpha = 5q + r$ avec $0 \leq r < 5$.
Donc $\alpha \equiv r\ [5]$ avec $r \in \{0; 1; 2; 3; 4\}$ puis $\alpha^2 \equiv r^2\ [5]$

- Si $r = 0$ alors $\alpha^2 \equiv 0^2\ [5]$ donc $\alpha^2 \equiv 0\ [5]$.
- Si $r = 1$ alors $\alpha^2 \equiv 1^2\ [5]$ donc $\alpha^2 \equiv 1\ [5]$.
- Si $r = 2$ alors $\alpha^2 \equiv 2^2\ [5]$ donc $\alpha^2 \equiv 4\ [5]$.
- Si $r = 3$ alors $\alpha^2 \equiv 9\ [5]$ or $9 = 4 + 5 \times 1$ donc $\alpha^2 \equiv 4\ [5]$.
- Si $r = 4$ alors $\alpha^2 \equiv 16\ [5]$ or $16 = 1 + 5 \times 3$ donc $\alpha^2 \equiv 1\ [5]$.

(c) On suppose l'équation (E_2) admet un couple solution $(x; y)$. Alors, d'après 3.(a), $x^2 \equiv 2\ [5]$ ce qui est impossible d'après 3.(b) puisque le carré d'un entier est congru soit à 0, soit à 1, soit à 4 modulo 5.
Par conséquent l'équation $\boxed{(E_2) \text{ n'admet aucune solution}}$

Exercice 6

1. .

a. Effectuons l'algorithme d'Euclide appliqué à 226 et 109

$226 = 2 \times 109 + 8$

$109 = 13 \times 8 + 5$

$8 = 1 \times 5 + 3$

$5 = 1 \times 3 + 2$

$3 = 1 \times 2 + 1$

$2 = 2 \times 1 + 0$

Le PGCD est le dernier reste non nul donc : PGCD(226 ; 109) = 1

L'équation Diophantienne $ax + by = c$ admet des solutions si et seulement si le PGCD(a, b) divise c.

C'est bien le cas ici, donc (E) admet des solutions entières.

b. On recherche une solution particulière (u, v) de (E).

On a : $141 \times 109 - 68 \times 226 = 1$

Le couple (u, v) = (141 ; 68) est une solution particulière de l'équation $109x - 226y = 1$.

Soit maintenant $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ une solution quelconque de (E).

On a : $109\,u - 226\,v = 1$ et $109\,x - 226\,y = 1$

En soustrayant membre à membre :

$109\,u - 226\,v = 1$

$109(x - u) = 226(y - v)$

Donc 226 divise $109(x - u)$ et comme PGCD(109,226) = 1.

On en déduit que 226 divise $(x - u)$ d'après le théorème de Gauss.

Il existe donc un entier k tel que : $x - u = 226k$ c'est-à-dire $x = u + 226k = 141 + 226k$

En remplaçant $x - u$ par $226k$, il vient : $109 \times 226k = 226(y - v)$

$y = v + 109k = 68 + 109k$.

Ainsi : $x = 141 + 226k$ *et* $y = 68 + 109k$

Réciproquement, on vérifie bien que tous les couples (x, y) de la forme $(141 + 226k, 68 + 109k)$, où $k \in \mathbb{Z}$,

sont des solutions de (E).

Montrons qu'il existe une unique valeur d de $x = 141 + 226k$ qui soit élément de $[\![0;226]\!]$

$$0 \leq 141 + 226k \leq 226 \iff -141 \leq 226k \leq 85$$

$$\iff -\frac{141}{226} \leq k \leq \frac{85}{226}$$

Et comme k est entier, la seule possibilité est : $k = 0$

D'où : $d = 141$ et $e = 68$

Ainsi, on a bien : $109d = 1 + 226e$ avec $d \in [\![0;226]\!]$

2. 227 n'est pas divisible par 2, ni par 3, ni par 5, ni par 7, ni par 11 et ni par 13 (inutile de tester au delà, si 227 admettait un diviseur premier, il serait nécessaire inférieur à $E(\sqrt{227}) = 15$).

C'est donc un nombre premier.

3. En fait : $A = [\![0;226]\!]$

On a, par définition de f et g : $a^{109} \equiv f(a)\ [227]$ et $a^{141} \equiv g(a)\ [227]$

a. Le reste de la division euclidienne de 0^{109} par 227 est bien sûr 0 donc : $f(0) = 0$

De même $g(0) = 0$ donc : $g(f(0)) = 0$

b. Comme 227 est premier, d'après le petit théorème de Fermat, on a pour tout entier a non nul $a^{226} \equiv 1\ [227]$

c. Supposons a non nul.

On a : $g(f(a)) \equiv (f(a))^{141} \equiv a^{109\times141}\ [227]$

Mais d'après la question 1.b. : $109 \times 141 = 1 + 226 \times 68$

D'où : $g(f(a)) \equiv a^{109\times141} \equiv a \times a^{226\times68}\ [227]$

Et d'après la question 3.b. on sait que $a^{226} \equiv 1$ [227] donc : $g(f(a)) \equiv a\ [227]$

Enfin, comme on a vu que $g(f(0)) = 0$, on a bien pour tout a de A : $g(f(a)) = a$

Les fonctions f et g commutent ; en effet, pour tout entier a : .

$f(g(a)) \equiv (g(a))^{109} \equiv a^{109\times141} \equiv g(f(a)) \equiv a\ [227]$

On a donc également, pour tout a de A : $f(g(a)) = a$.

Exercice7

1°) a) On considère l'équation : $17x = 6y$.

6 et 17 étant premiers entre eux (car 17 est premier et ne divise pas 6),

6 divise $17x$ donc d'après le théorème de Gauss 6 divise x.

Il existe donc un entier k tel que $x = 6k$, et donc $6y = 17 \times 6k$ et $y = 17k$.

Réciproquement, on a $17 \times 6k = 17 \times 6k$

Donc tous les couples $(6k ; 17k)$ sont solutions.

Les solutions dans $\mathbb{N}^2$ de cette équation sont donc $S_1 = \{(6k ; 17 k) , k \in \mathbb{N}\}$.

b) On a $17 = 6 \times 2 + 5 \Rightarrow 5 = 17 - 6 \times 2$

$6 = 5 \times 1 + 1 \Rightarrow 1 = 6 - 5 \times 1 = 6 - 1 \times (17 - 6 \times 2) = 17 \times (- 1) + 6 \times(- 3)$

$\Rightarrow 17\times(-1) - 6\times(-3) = -17 + 18 = 1$, donc $(-1 ; -3)$ est solution de l'équation $17x - 6y = 1$.

On obtient facilement que $(-2 ; -6)$ est une solution de (E).

c) (E) est donc équivalente à $17x - 6y = 17 \times (-2) - 6 \times (- 6)$, donc aussi à $17(x + 2) = 6(y + 6)$ (1)

- 1ère Méthode : nous connaissons d'après le a) les solutions de cette dernière : $x + 2 = 6k$ et $y + 6 = 17k$, où k est un entier quelconque.

  Les solutions de (E) sont donc $S_2 = \{(6k - 2 ; 17k - 6), k \in \mathbb{Z}\}$.

- 2ème Méthode : 6 et 17 étant premiers entre eux (car 17 est premier et ne divise pas 6),

  donc d'après le théorème de Gauss 17 divise $y + 6$.

  $\Rightarrow$ il existe un entier relatif k tel que $y + 6 = 17k$, c'est-à-dire $y = 17k - 6$.

  en reportant dans l'équation (1) on a : $17(x + 2) = 6 \times 17k$

  c'est à dire $x = 6k - 2$.

Réciproquement, on a $17 \times (6k - 2) - 6 (17k - 6) = 2$.

Donc tous les couples $(6k - 2 ; 17k - 2)$ avec $k \in \mathbb{Z}$ sont solutions.

d) Tout diviseur commun à x et y solution de (E) divise aussi $17x - 6y$, c'est à dire 2.

Le pgcd de x et y est donc un diviseur positif de 2, ce ne peut être que 1 ou 2.

e) Il résulte du d) que le pgcd d'un couple $(x ; y)$ solution de (E) est égal à 2 si et seulement si 2 divise x et y.

Or 2 divise $6k$ et 2, donc 2 divise $6k - 2$, donc 2 divise toujours x.

En revanche, 2 divise 6, donc 2 divise y $= 17k - 6$ si et seulement si 2 divise $17k$.

Comme 2 est premier avec 17, 2 divise $17k$ si et seulement si 2 divise k d'après le théorème de Gauss, c'est à dire $k = 2p$, $p \in \mathbb{Z}$.

Les solution de (E) de pgcd 2 sont donc $(12 p - 2 ; 34 p - 6)$.

f) On veut donc avoir $y = 34p - 6$ et $100 \leq y \leq 150$, la seule valeur entière possible de p est 4.

La solution recherchée est donc (46 ; 130).