1. On considère l'équation (E) : $109\,x - 226\,y = 1$ 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 : $(141 + 226\,k\,;\, 68 + 109\,k)$, où k appartient à $\mathbb{Z}$.

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 $109\,d = 1 + 226\,e$. (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 $g \circ f(0) = 0$.

On rappelle 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. $g \circ f(a) = a$. Que peut-on dire de $f[(g(a)] = a$?

CORRECTION

1. *a*. D'après l'algorithme d'Euclide :

$226 = 109 \times 2 + 8$ $\quad 109 = 8 \times 13 + 5$ $\quad 8 = 5 + 3$ $\quad 5 = 3 + 2$ $\quad 3 = 2 + 1$

donc 109 et 226 sont premiers entre eux donc d'après le théorème de Bézout l'équation (E) admet au moins une solution.

b. $109 \times 141 - 226 \times 68 = 15\,369 - 15\,368$ donc $109 \times 141 - 226 \times 68 = 1$

$\begin{cases} 109'x - 226\,y = 1 \\ 109' \times 141 - 226 \times 68 = 1 \end{cases}$ donc par différence membre à membre : $109\,(x - 141) - 226\,(y - 68) = 0$

soit $109\,(x - 141) = 226\,(y - 68)$ donc 109 divise $226\,(y - 68)$ or 109 et 226 sont premiers entre eux donc d'après le théorème de Gauss, 109 divise $y - 68$ donc il existe un entier relatif k tel que $y - 68 = 109\,k$

En remplaçant dans $109\,(x - 141) = 226\,(y - 68)$ on obtient $109\,(x - 141) = 226 \times 109\,k$ donc $x - 141 = 226\,k$

donc $x = 141 + 226\,k$ et $y = 68 + 109\,k$ où k appartient à $\mathbb{Z}$.

Vérification : si $x = 141 + 226\,k$ et $y = 68 + 109\,k$ alors $109\,x - 226\,y = 109 \times 141 + 226 \times 109\,k - 226 \times 38 - 226 \times 109\,k = 1$

L'ensemble de solutions de (E) est l'ensemble des couples de la forme : $(141 + 226\,k\,;\, 68 + 109\,k)$, où k appartient à $\mathbb{Z}$.

d et e sont solutions de (E) donc il existe un entier relatif k tel que $d = 141 + 226\,k$ et $e = 68 + 109\,k$

$0 < d \leq 226$ donc $0 < 141 + 226\,k \leq 226$ donc $k = 0$ et $d = 141$ alors $e = 68 + 109\,k = 68$

Il existe un unique entier naturel non nul d inférieur ou égal à 226 et un unique entier naturel non nul e tels que $109\,d = 1 + 226\,e$.

2. $15 < \sqrt{227} < 16$, cherchons s'il existe un nombre premier inférieur à $\sqrt{227}$ qui divise 227.

227 est impair donc n'est pas divisible par 2 ;

La somme de ses chiffres est 11 donc 227 n'est pas divisible par 3.

Son chiffre des unités n'est ni 0 ni 5 donc 227 n'est pas divisible par 5

$227 = 7 \times 32 + 3$ donc 227 n'est pas divisible par 7

$227 = 11 \times 20 + 7$ donc 227 n'est pas divisible par 11

$227 = 13 \times 17 + 6$ donc 227 n'est pas divisible par 13 donc 227 est un nombre premier.

3. *a*. $f(0)$ est le reste de la division euclidienne de 0^{109} par 227 or $0^{109} = 227 \times 0 + 0$ donc $f(0) = 0$

$g(0)$ est le reste de la division euclidienne de 0^{141} par 227 or $0^{141} = 227 \times 0 + 0$ donc $g(0) = 0$ donc $g \circ f(0) = 0$.

b. $0 < a \leq 226$ et 227 est un nombre premier donc a est un entier non divisible par 227 donc quel que soit l'entier non nul a de A, $a^{226} \equiv 1$ [modulo 227]. (petit théorème de Fermat).

c. $a^{226} \equiv 1$ [modulo 227]

$f(a)$ est le reste de la division euclidienne de a^{109} par 227 donc $a^{109} \equiv f(a)$ [modulo 227]

$f(a)^{141} \equiv a^{109 \times 141}$ [modulo 227] or $109 \times 141 = 1 + 226 \times 68$ donc $a^{109 \times 141} = a^{1 + 226 \times 68} = a \times (a^{226})^{68}$

$a^{226} \equiv 1$ [modulo 227] donc $(a^{226})^{68} \equiv 1$ [modulo 227] donc $a^{109 \times 141} \equiv a$ [modulo 227]

donc $f(a)^{141} \equiv a$ [modulo 227]

$0 \leq a \leq 226$ donc a est le reste de la division de $f(a)^{141}$ par 227 donc $g \circ f(a) = a$

$a(a)$ est le reste de la division euclidienne de a^{141} par 227 donc $a^{141} \equiv g(a)$ [modulo 227]

$g(a)^{109} \equiv a^{109 \times 141}$ [modulo 227] or $109 \times 141 = 1 + 226 \times 68$ donc $a^{109 \times 141} = a^{1 + 226 \times 68} = a \times (a^{226})^{68}$

$a^{226} \equiv 1$ [modulo 227] donc $(a^{226})^{68} \equiv 1$ [modulo 227] donc $a^{109 \times 141} \equiv a$ [modulo 227]

donc $g(a)^{109} \equiv a$ [modulo 227]

$0 \leq a \leq 226$ donc a est le reste de la division de $g(a)^{109}$ par 227 donc $f \circ g\,(a) = a$