

CORRECTION DU DEVOIR MAISON N° 9

*Théorème de Gauss et
petit théorème de Fermat*

Pour le 5 février 2008

Liban, juin 2005

1) a) Par la méthode l'algorithme d'Euclide, on obtient :

a	b	reste
226	109	8
109	8	5
8	5	3
5	3	2
3	2	1
2	1	0

On en déduit que $\text{PGCD}(226; 109) = 1$.

Comme 226 et 109 sont premiers entre eux, d'après le théorème de Bézout, il existe des entiers x et y tels que $109x - 226y = 1$. **L'équation diophantienne (E) admet donc des couples solutions.**

b) • En remontant, on a :

$$1 = 3 - 2.$$

Or $2 = 5 - 3$; alors :

$$1 = 3 - (5 - 3) = 3 \times 2 - 5.$$

Or $3 = 8 - 5$; alors :

$$1 = 2 \times (8 - 5) - 5 = 2 \times 8 - 3 \times 5.$$

Or $5 = 109 - 13 \times 8$; alors :

$$1 = 2 \times 8 - 3 \times (109 - 13 \times 8) = 41 \times 8 - 3 \times 109.$$

Or $8 = 226 - 2 \times 109$; alors :

$$1 = 41 \times (226 - 2 \times 109) - 3 \times 109 = 41 \times 226 - 85 \times 109.$$

Par conséquent, **le couple $(-85 \quad -41)$ est un couple solution de (E).**

D'après la question précédente, $109x - 226y = 1$ équivaut à

$$109x - 226y = 109 \times (-85) - 226 \times (-41), \text{ ou encore à } 109(x + 85) = 226(y + 41).$$

On en déduit que 226 divise $109(x + 85)$, et comme 226 et 109 sont premiers entre eux, d'après le théorème de Gauss, 226 divise $x + 85$. Il existe donc un entier q tel que $x + 85 = 226q$, c'est-à-dire $x = -85 + 226q$. En remplaçant x par $-85 + 226q$ dans l'égalité $109(x + 85) = 226(y + 41)$, on a : $109 \times 226q = 226(y + 41)$, soit $y + 41 = 109q$, c'est-à-dire $y = -41 + 109q$.

Prenons $q = k + 1$; on obtient alors : $x = 141 + 226k$ et $y = 68 + 109k$.

Réciproquement, on vérifie que tous les couples de la forme $(141 + 226k ; 68 + 109k)$, où k appartient à \mathbf{Z} , sont solutions de l'équation (E).

$109(141 + 226k) - 226(68 + 109k) = 15369 - 15368 = 1$. Ce qui vérifie ce que l'on souhaite.

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

• Recherchons la valeur d de $x = 141 + 226k$ telle que d appartienne à $[0 ; 226]$.

$$0 \leq d \leq 226 \Leftrightarrow 0 \leq 141 + 226k \leq 226$$

$$\Leftrightarrow -141 \leq 226k \leq 85$$

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

Comme k est un entier, alors $k = 0$. D'où : $d = 141$ et la valeur de y pour $k = 0$ est égale à 68. De plus, $109 \times 141 - 226 \times 68 = 1$.

Par conséquent, **$109d = 1 + 226e$ avec d inférieur ou égal à 226 (et égal à 141) et e égal à 68.**

2) Vérifions si 227 est divisible par les nombres premiers inférieurs à $\sqrt{227}$.

227 n'est divisible ni par 2, ni par 3, ni par 5, ni par 7, ni par 11, ni par 13 ; **227 est donc un nombre premier.**

3) a) $0^{109} = 0$, et le reste de la division euclidienne de 0 par 227 est 0 ; alors $f(0) = 0$.

$0^{141} = 0$, d'où le reste de la division euclidienne de 0^{141} par 227 est 0 ; alors $g(0) = 0$.

Par conséquent, **$g[f(0)] = 0$.**

b) Soit a un entier non nul de \mathcal{A} . Comme a est un entier naturel compris entre 1 et 226, il ne peut pas être divisible par 227.

D'après la question 2), 227 est un nombre premier, alors, d'après le petit théorème de Fermat, $a^{227-1} \equiv 1 \pmod{227}$, c'est-à-dire $a^{226} \equiv 1 \pmod{227}$.

Par conséquent, **quel que soit l'entier non nul a de \mathcal{A} , $a^{226} \equiv 1 \pmod{227}$.**

c) Soit a un entier non nul de \mathcal{A} . $f(a) \equiv a^{109} \pmod{227}$ et $g[f(a)] \equiv (f(a))^{141} \pmod{227}$, alors $g[f(a)] \equiv a^{109 \times 141} \pmod{227}$, d'après les propriétés des congruences.

Or, d'après la question 1) b), $109 \times 141 = 1 + 226 \times 68$.

On en déduit que $g[f(a)] \equiv a \times a^{226 \times 68} \pmod{227}$.

D'après la question 3) b), $a^{226} \equiv 1 \pmod{227}$, d'où $a \times a^{226} \equiv a \pmod{227}$.

Par conséquent, $g[f(a)] \equiv a \pmod{227}$

Comme $g[f(a)]$ et a sont deux entiers inférieurs à 227, on en déduit que $g[f(a)] = a$.

Donc, **quel que soit l'entier non nul a de \mathcal{A} , $g[f(a)] = a$.**

$f[g(a)] \equiv g(a)^{109} \pmod{227} \equiv (a^{109})^{141} \pmod{227} \equiv a^{109 \times 141} \pmod{227} \equiv g[f(a)] \pmod{227}$.

Par conséquent, **pour tout entier non nul a de \mathcal{A} , $f[g(a)] = a$.**