CORRECTION DU DEVOIR A LA MAISON N° 6

Exercice 1 :

1. (a) On applique l'algorithme d'Euclide : $226 = 109 \times 2 + 8$; $109 = 8 \times 13 + 5$; $8 = 5 \times 1 + 3$; $5 = 1 \times 3 + 2$; $3 = 2 \times 1 + 1$; $2 = 2 \times 1 + 0$. Le dernier reste non nul dans cette succession de divisions euclidiennes est 1 donc $PGCD(109\,;\,226) = 1$. D'après l'identité de Bézout, on peut en déduire qu'il existe un couple $(u\,;\,v) \in \mathbb{Z}^2$ tel que $109u + 226v = 1$. En posant $x = u$ et $y = -v$, cela nous donne un couple $(x\,;\,y)$ solution de (E). Autrement dit, l'équation (E) admet au moins une solution (en fait elle en admet alors une infinité).

   (b) Montrons que $(x_0\,;\,y_0) = (141\,;\,68)$ est une solution particulière de (E) (on devine qu'il s'agit d'une solution particulière de (E) d'après la forme donnée des solutions en choisissant $k = 0$). Comme $109x_0 - 226y_0 = 109 \times 141 - 226 \times 68 = 15369 - 15368 = 1$ alors $(x_0\,;\,y_0) = (141\,;\,68)$ est solution particulière de (E).
   Soit $(x\,;\,y)$ une solution de (E). Alors $109x - 226y = 1 = 109x_0 - 226y_0$ d'où $109(x - x_0) = 226(y - y_0)$. Comme $y - y_0 \in \mathbb{Z}$, alors 226 divise $109(x - x_0)$. Or, $PGCD(109\,;\,226) = 1$ donc 226 divise $x - x_0$ d'après le théorème de Gauss. Ainsi, il existe $k \in \mathbb{Z}$ tel que $x - x_0 = 226k$ soit $x = x_0 + 226k = 141 + 226k$. De plus, en remplaçant dans $109(x - x_0) = 226(y - y_0)$, on aboutit à $109 \times 226k = 226(y - y_0)$ soit $y - y_0 = 109k$ ou encore $y = y_0 + 109k = 68 + 109k$. On a ainsi montré que si $(x\,;\,y)$ est solution de (E) alors il existe $k \in \mathbb{Z}$ tel que $(x\,;\,y) = (141 + 226k\,;\,68 + 109k)$.
   Vérifions que tous ces couples sont effectivement solutions de (E) : pour tout $k \in \mathbb{Z}$,

   $$109(141+226k)-226(68+109k) = 109\times141+109\times226k-226\times68-226\times109k = 15369-15368 = 1$$

   L'ensemble des solutions de (E) et donc $\mathcal{S} = \{(141 + 226k\,;\,68 + 109k)\,;\,k \in \mathbb{Z}\}$.
   Dire que d et e vérifient la relation $109d = 1 + 226e$ signifie que $109d - 226e = 1$ donc que $(d\,;\,e)$ est solution de (E). Ainsi, il existe $k \in \mathbb{Z}$ tel que $d = 141 + 226k$ et $e = 68 + 109k$. Or $0 < d \leqslant 226 \Leftrightarrow 0 < 141 + 226k \leqslant 226 \Leftrightarrow -141 < 226k \leqslant 85$ soit $-1 < -\dfrac{141}{226} < k \leqslant \dfrac{85}{226} < 1$. L'unique entier k de cet encadrement est $k = 0$ d'où $d = 141$ et $e = 68 \in \mathbb{N}^*$.

2. $\sqrt{227} \simeq 15,07$ donc pour montrer que 227 est premier on vérifie qu'il n'est divisible par aucun nombre premier inférieur à 15. Les nombres premiers inférieurs à 15 sont : 2, 3, 5, 7, 11 et 13.
   - Comme 227 est impair, il n'est pas divisible par 2.
   - La somme des chiffres de 227 est $2 + 2 + 7 = 11$, ce n'est pas un multiple de 3 donc 227 n'est pas divisible par 3.
   - 227 ne se termine ni par 0 ni par 5 donc ce n'est pas un multiple de 5.
   - $227 = 7 \times 32 + 3$ (avec $0 \leqslant 3 < 7$) donc le reste de la division euclidienne de 227 par 7 n'est pas nul, ce qui signifie que 227 n'est pas divisible par 7.
   - $227 = 11 \times 20 + 7$ (avec $0 \leqslant 7 < 11$) donc reste de la division euclidienne de 227 par 11 n'est pas nul, ce qui signifie que 227 n'est pas divisible par 11.
   - $227 = 13 \times 17 + 6$ (avec $0 \leqslant 6 < 13$) donc reste de la division euclidienne de 227 par 13 n'est pas nul, ce qui signifie que 227 n'est pas divisible par 13.

   Le nombre 227 n'est divisible par aucun nombre premier inférieur à $\sqrt{227}$ donc il est premier.

3. (a) $f(0)$ est le reste de la division euclidienne de 0^{109} par 227. Or, $0^{109} = 0$ donc le reste de 0 dans la division euclidienne par 227 est 0 ($0 = 227 \times 0 + 0$). Ainsi, $f(0) = 0$ et $g[f(0)] = g(0)$. De même, le reste de $0^{141} = 0$ dans la division euclidienne par 227 est 0 donc $g(0) = 0$ et $g[f(0)] = 0$.

   (b) Comme 227 est un nombre premier et que 226 n'est pas un multiple de 227 (en effet, $226 < 227$), alors $PGCD(226\,;\,227) = 1$. On peut donc appliquer le petit théorème de Fermat : $a^{227-1} \equiv 1\ [227]$ soit $a^{226} \equiv 1\ [227]$.

   (c) Comme $f(a)$ est le reste de la division euclidienne de a^{109} par 227 alors $f(a) \equiv a^{109}\ [227]$. Comme $g[f(a)]$ est le reste de la division euclidenne de $[f(a)]^{141}$ par 227 alors $g[f(a)] \equiv [f(a)]^{141}\ [227]$. Or, $[f(a)]^{141} \equiv \left(a^{109}\right)^{141}\ [227]$. Dans la question 1.b) on a prouvé que $d = 141$ et $109d = 1 + 226e$ avec $e \in \mathbb{N}^*$. Ainsi, par transitivité, $g[f(a)] \equiv a^{109d}\ [227]$ soit $g[f(a)] \equiv a^{1+226e}\ [227]$, ce qui s'écrit

également $g[f(a)] \equiv a \times \left(a^{226}\right)^e$ [227]. D'après la question précédente, $a^{226} \equiv 1$ [227] et comme $e \in \mathbb{N}^*$, alors $\left(a^{226}\right)^e \equiv 1^e$ [227] soit $\left(a^{226}\right)^e \equiv 1$ [227]. Finalement $g[f(a)] \equiv a$ [227]. Comme a et $g[f(a)]$ sont tous les deux des nombres de l'ensemble A (compris entre 0 et 226), alors $g[f(a)] = a$. Par définition de f et g, $g(a) \equiv a^{141}$ [227] et $f[g(a)] \equiv g(a)^{109}$ [227]. Ainsi, $f[g(a)] \equiv \left(a^{141}\right)^{109}$ [227] soit $f[g(a)] \equiv a^{109d}$ [227]. On peut conclure comme précédemment que $a^{109d} \equiv a$ [227] d'où $f[g(a)] \equiv a$ [227]. Or, $f[g(a)]$ et a sont dans A d'où $f[g(a)] = a$ est vraie.

Exercice 2 :

- **Horizontalement pour 2** : on cherche un nombre entier de trois chiffres tel que le produit de ses chiffres est égal à 1, c'est nécessairement le nombre 111.
- **Horizontalement pour 5** : le nombre cherché est $2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030$.
- **Verticalement pour B, 2ème mot** : on cherche un mutliple de 3 et 4 donc un multiple de 12 car $PGCD(3\,;\,4) = 1$. Il doit se terminer par 0 donc être aussi mutliple de 5. Or, $PGCD(12\,;\,5) = 1$ (car 5 est premier et 12 n'est pas un multiple de 5). On cherche donc un multiple de $12 \times 5 = 60$. Le seul de ces mutliples possédant deux chiffres est 60.
- **Horizontalement pour 4, 1er mot** : on cherche un carré parfait se terminant par 6 et ayant deux chiffres. Les carrés parfaits avec deux chiffres sont 16, 25, 36, 49, 64 et 81. Le seul se terminant par un 6 est 36. La somme de ses chiffres vaut $3 + 6 = 9$, ce n'est pas un nombre premier.
- **Verticalement pour A** : le nombre cherché possède 5 chiffres et la somme de ces chiffres doit valoir 8. On sait déjà qu'il y a dans ces 5 chiffres un 1 et deux 3, dont la somme fait 7. IL reste donc à placer un 1 et un 0. Les nombres ne doivent pas débuter par 0 donc en première place on met le 1 et en troisième place le 0.
- **Verticalement pour E** : Le nombre se termine par 0, pour que les chiffres soient consécutifs il faut donc que le nombre soit 43210.
- **Horizontalement pour 4, 2ème mot** : Les couples d'entiers naturels $(a\,;\,b)$ tels que $a + b = 10$ sont $(1\,;\,9)$, $(2\,;\,8)$, $(3\,;\,7)$, $(4\,;\,6)$, $(5\,;\,5)$ ainsi que leurs symétriques. Si on élimine les couples de nombres qui ne sont pas formés uniquement de nombres premiers, il reste : $(3\,;\,7)$, $(5\,;\,5)$ et leurs symétriques. Les produits formés par ces couples sont 21 ou 25. On cherche un nombre se terminant par 1 donc il s'agit de 21.
- **Verticalement pour D** : Un nombre est multiple de 9 si la somme de ses chiffres est divisible par 9. La somme des deux chiffres parmi les 3 composant le nombre cherché fait déjà 5. Pour qu'il s'agisse d'un multiple de 9, il faut donc ajouter le nombre 4. Le nombre cherché est donc 423.
- **Horizontalement pour 1** : on remarque que $2^{13} = 8192$, $2^{14} = 16384$, $2^{15} = 32768$. Comme multiplier par 2 augmente la valeur du résultat, la seule puissance de 2 comportant 5 chiffres et un 1 en première place est $2^{14} = 16384$.
- **Verticalement pour C** : on cherche un multiple de 5, il doit se terminer par 0 ou 5. Comme un des nombres cherché ne peut pas commencer par 0, le dernier chiffre de C ne peut pas valoir 0 puisque sinon, le premier chiffre du 3 horizontal serait égal à 0. Ainsi, le résultat du C est 315.
- **Horizontalement pour 3** : On vérifie que la somme des chiffres de 542 est premier : $5 + 4 + 2 = 11$ est bien un nombre premier.
- **Verticalement pour B, 1er mot** : on vérifie que le nombre 61 est premier et que la somme de ses chiffres est premier : $\sqrt{61} \simeq 7{,}8$ et 61 n'est ni divisible par 2 (impair), ni divisible par 3 (la somme de ses chiffres est 7, ce n'est pas un multiple de 3), ni divisible par 5 (se termine par 1), ni divisible par 7 : $61 = 7 \times 8 + 5$. Ainsi, 61 est premier et la somme de ses chiffres (7) également.

	A	B	C	D	E
1	1	6	3	8	4
2	1	1	1	■	3
3	0	■	5	4	2
4	3	6	■	2	1
5	3	0	0	3	0