EISTI	**Cycle préparatoire 1$^{\text{ère}}$ année** **Devoir surveillé 3** *N. Arancibia, S. El Sayed, K. Fayad, J.-M. Masereel*	
	Matière : **Algèbre**	*Date* : **Vendredi 15 décembre 2017**
	Appareils électroniques et documents interdits	*Durée* : **2 heures**
		Nombre de pages : **1**

Il sera tenu compte de la qualité de la rédaction et de la précision des justifications.

Le sujet comporte quatre exercices. L'ordre dans lequel ceux-ci sont traités n'est pas imposé.
Le barème est donné à titre indicatif.

Exercice 1. (5 points)
Soit dans $\mathbb{R}[X]$ les deux polynômes $P(X) = X^4 + X^3 + aX^2 + bX + 2$ et $Q(X) = X^2 + 2$.

1. Trouver une condition nécessaire et suffisante sur a et b pour que Q divise P.
2. On suppose dans cette question que $a = 2$ et $b = 3$.
   (a) Trouver le PGCD de P et Q, noté $P \wedge Q$.
   (b) Trouver $(U, V) \in \mathbb{R}[X]^2$ tel que $PU + QV = P \wedge Q$.

Exercice 2. (6 points)
Les questions suivantes sont indépendantes.

1. Résoudre dans $\mathbb{Z} \times \mathbb{Z}$ l'équation $(x - 27)(y + 12) = xy$.
2. Résoudre dans $\mathbb{Z}$ l'équation $12x \equiv 9\ [51]$.
3. Trouver le reste de la division euclidienne de 100^{2017} par 17.
4. Montrer que $2^{36} + 5^{18}$ est divisible par 41.

Exercice 3. (6 points)
On rappelle le petit théorème de Fermat :

Si p est un nombre premier, alors pour tout entier a premier à p, on a $a^{p-1} \equiv 1[p]$.

Le but de cet exercice est de montrer que la réciproque est fausse, c.-à-d. qu'il existe des entiers n qui ne sont pas premiers et pour lesquels on a aussi : pour tout entier a premier à n, $a^{n-1} \equiv 1[n]$.
Ces nombres sont appelés pseudo-premiers ou aussi nombres de Carmichael.

1. Décomposer 561 en produit de facteurs premiers.
2. Montrer que si un entier a est premier à 561, alors

$$a^{560} \equiv 1[3]$$
$$a^{560} \equiv 1[11]$$
$$a^{560} \equiv 1[17]$$

3. Montrer que pour tout entier a premier à 561, on a $a^{560} \equiv 1[561]$.
   561 est le plus petit nombre de Carmichael.

Exercice 4. (3 points)
Soit $(a, b) \in \mathbb{Z}^2$. Exprimer, en le justifiant, $(15a + 4b) \wedge (11a + 3b)$ en fonction de $a \wedge b$.