Correction de l'examen du 16 décembre 2015

Exercice 1

1) On a $121 = 11^2$ et 123 (resp. 125) est divisible par 3 (resp. 5). On vérifie ensuite que 127 est premier, qui est donc l'entier cherché ; en effet, la racine carrée de 127 est plus petite que 12, donc si 127 n'était pas premier, il serait divisible par un nombre premier inférieur ou égal à 11, ce qui n'est pas.

2.1) L'entier a étant impair, il est congru à $\pm 1, \pm 3$ ou 5 modulo 10. Si a n'était pas premier avec 100, il serait donc congru à 5 modulo 10, ce qui par hypothèse est exclu.

2.2) Soit φ la fonction indicatrice d'Euler. Parce que a est premier avec 100, on a la congruence $a^{\varphi(100)} \equiv 1$ mod. 100 (théorème d'Euler). On a l'égalité $\varphi(100) = 40$, d'où $a^{40} \equiv 1$ mod. 100. Pour tout $k \in \mathbb{N}$, on obtient $a^{40k} \equiv 1$ mod. 100. Ainsi, 1 est le reste de la division euclidienne de a^{40k} par 100.

3.1) En utilisant l'algorithme d'Euclide, on obtient le tableau suivant :

	2	3	3	2	
53	23	7	2	1	0
1	0	1	-3	10	
0	1	-2	7	-23	

On en déduit l'égalité $-23^2 + 53 \times 10 = 1$, autrement dit, le couple $(u, v) = (-23, 10)$ convient.

3.2) Il résulte de la question précédente, avec le théorème chinois, que -529 est multiple de 23 et est congru à 1 modulo 53. Un tel entier est unique modulo 1219. On en déduit que l'on a $N = 1219 - 529 = 690$.

Exercice 2

1) Le polynôme $X^3 + X^2 + 2$ n'a pas de racines dans $\mathbb{F}_3$. Il est de degré 3, donc il est irréductible sur $\mathbb{F}_3$. Par suite, K est un corps.

2) Sa caractéristique est 3 et son cardinal est 27.

3) Les ordres possibles des éléments du groupe K^* sont les diviseurs de 26, autrement dit, ce sont 1, 2, 13 et 26.

4) On a $\alpha^3 + \alpha^2 + 2 = 0$, d'où les égalités $\alpha^2(\alpha + 1) = -2 = 1$. L'inverse de $1 + \alpha$ est donc α^2. Ses coordonnées dans $\mathcal{B}$ sont $(0, 0, 1)$.

5) On a $\alpha^6 = \alpha^4 + \alpha^2 + 1$ et $\alpha^4 = 2 + \alpha + \alpha^2$, d'où $\alpha^6 = \alpha + 2\alpha^2$, dont les coordonnées dans $\mathcal{B}$ sont $(0, 1, 2)$.

6) On déduit par exemple de la question précédente que l'on a $\alpha^{12} = \alpha+\alpha^2$, d'où $\alpha^{13} = 1$. Ainsi, α est d'ordre 13.

7) L'application de K^* à valeurs dans K^* qui à x associe x^2 est un homomorphisme de groupes, de noyau $\{\pm 1\}$, qui est d'ordre 2. Son image est H. Il en résulte que H est un groupe isomorphe à $K^*/\{\pm 1\}$, il est donc d'ordre 13.

8) Parce que K^* est un groupe cyclique, H est l'ensemble des éléments $x \in K^*$ tels que $x^{13} = 1$. D'après la question 6, α est donc dans H.

9) On déduit de la question 6 que l'on a

$$\left(\alpha^7\right)^2 = \alpha^{14} = \alpha.$$

Les racines du polynôme $Y^2 - \alpha$ sont donc α^7 et $-\alpha^7$. Leurs coordonnées dans $\mathcal{B}$ sont respectivement $(2, 0, 2)$ et $(1, 0, 1)$.

10) On a $(2\alpha)^{13} = -\alpha^{13} = -1$. Par suite, 2α est d'ordre 26, qui est ainsi un générateur de K^*.

11) On a $(2\alpha)^2 = \alpha^2$, d'où $n = 2$.

Exercice 3

1) Ce sont les polynômes X, $X + 1$ et $X^2 + X + 1$.

2) Le polynôme $X^{16} - X$ est le produit des polynômes irréductibles de $\mathbb{F}_2[X]$ de degré divisant 4. Si N est le nombre cherché, on a donc

$$2 + 2 + 4N = 16,$$

d'où $N = 3$.

3) Un polynôme de degré 4 de $\mathbb{F}_2[X]$ est irréductible sur $\mathbb{F}_2$ si et seulement si il n'a pas de racines dans $\mathbb{F}_2$ et n'est pas divisible par $X^2 + X + 1$. Compte tenu de l'égalité $(X^2 + X + 1)^2 = X^4 + X^2 + 1$, on vérifie alors que ces polynômes sont

$$X^4 + X + 1, \quad X^4 + X^3 + 1, \quad X^4 + X^3 + X^2 + X + 1.$$

4) On en déduit que la décomposition cherchée est

$$X^{16} - X = X(X+1)(X^2+X+1)(X^4+X+1)(X^4+X^3+1)(X^4+X^3+X^2+X+1).$$