**Université de Toulon**
**U.F.R. de Sciences**
**Mathématiques**

**Année 2014-2015**
07 janvier 2015

**Examen de Master 2 de Mathématiques**

**Corps finis et leurs applications**

Durée : 3h00

## Exercice 1.

**1.** Déterminer l'ordre de 2 dans $(\mathbb{Z}/15\mathbb{Z})^*$. En déduire quelle est la plus petite extension de $\mathbb{F}_2$ qui contienne toutes les racines du polynôme

$$P(X) = X^{15} - 1.$$

Factoriser $P(X)$, d'une part par $X^5 - 1$, et d'autre part par $X^3 - 1$.

**2.** Déterminer les classes cyclotomiques binaires modulo 15. En déduire le nombre de facteurs irréductibles de $P(X)$ dans $\mathbb{F}_2[X]$ ainsi que leurs degrés.

**3.** Montrer que la décomposition en produit de facteurs irréductibles dans $\mathbb{F}_2[X]$ du polynôme $Q(X) = X^8 + X^7 + X^5 + X^4 + X^3 + X + 1$ est la suivante :

$$Q(X) = (X^4 + X + 1)(X^4 + X^3 + 1).$$

En déduire la décomposition en produit de facteurs irréductibles dans $\mathbb{F}_2[X]$ du polynôme $P(X)$. Quelle est celle du polynôme $X^{30} - 1$ ?

**5.** On rappelle qu'un code linéaire cyclique $q$-aire de longueur $n$ est un idéal de l'anneau $A = \mathbb{F}_q[X]/(X^n - 1)$. Déterminer le nombre de codes linéaires cycliques binaires de longueur 30.

## Exercice 2.

On s'intéresse à l'existence de solutions dans $\mathbb{Z}/717\mathbb{Z}$ à l'équation

$$x^2 = 185. \tag{1}$$

**1.** Calculer le symbole de Jacobi suivant :

$$\Big(\frac{185}{717}\Big).$$

**2.** Que peut-on en déduire quant à l'existence de solutions à l'équation (1) ?

**3.** On remarque que $717 = 3 \times 239$. Si $x$ est solution de la congruence $x^2 \equiv 185 \pmod{717}$, que peut-on en déduire de $x^2$ modulo 3 ? Conclure.

**Exercice 3.**

Soit $q$ une puissance d'un nombre premier et $\mathbb{F}_{q^2}$ le corps fini à $q^2$ éléments. On considère le polynôme irréductible :

$$F(X,Y) = X^{q+1} + Y^{q+1} - 1 \in \mathbb{F}_{q^2}[X,Y]$$

et son homogénéisé $F^*(X,Y,Z)$.

On considère la courbe algébrique projective $\mathcal{C}$, appelée courbe Hermitienne, définie sur $\mathbb{F}_{q^2}$ par :

$$\mathcal{C} = \{(x:y:z) \in \mathbb{P}^2(\overline{\mathbb{F}}_{q^2}) \ \mid \ x^{q+1} + y^{q+1} - z^{q+1} = 0\}.$$

**1.** Montrer que la courbe $\mathcal{C}$ est lisse et déterminer son genre.

**2.** Afin de déterminer les points à l'infini de $\mathcal{C}$, on est amené à considérer sur $\mathbb{F}_{q^2}$ l'équation

$$X^{q+1} + 1 = 0.$$

**2.1.** Montrer que cette équation admet $(q+1)$ solutions dans la clôture algébrique $\overline{\mathbb{F}}_{q^2}$ de $\mathbb{F}_{q^2}$.

**2.2.** Montrer que les racines de cette équation sont toutes dans $\mathbb{F}_{q^2}$.

**3.** On s'intéresse ici au nombre de points à distance finie de $\mathcal{C}$.

**3.1.** De la même manière que dans la question 2), montrer que l'équation $Y^{q+1} = a$ avec $a \in \mathbb{F}_{q^2}^*$, possède $(q+1)$ solutions dans $\mathbb{F}_{q^2}$.

**3.2.** En déduire que le nombre de points (rationnels sur $\mathbb{F}_{q^2}$) à distance finie de $\mathcal{C}$ est égal à :

$$(q^2 - (q+1))(q+1) + (q+1).$$

**4.** Montrer que le nombre de points rationnels sur $\mathbb{F}_{q^2}$ de la courbe Hermitienne $\mathcal{C}$ atteint la borne supérieure de la borne de Weil.

**5.** Déterminer la fonction zêta de $\mathcal{C}$ sur $\mathbb{F}_{q^2}$.

* * *