Université de Bordeaux
Mathématiques
Année 2015-2016

Master CSI
M1MA7W01
Arithmétique

Devoir Surveillé, 3 novembre 2015

Durée 2h00, documents interdits

Exercice 1 – Soit p un nombre premier.

1) Soit a un nombre premier. Combien y a-t-il dans $\mathbb{F}_p[X]$ de polynômes unitaires irréductibles de degré a ? *Indication* : se servir de la décomposition en produit d'irréductibles unitaires du polynôme $X^{p^a} - X$ dans $\mathbb{F}_p[X]$.

2) Soient a et b deux nombres premiers distincts.

Montrer que dans $\mathbb{F}_p[X]$, il y a $\dfrac{p^{ab} - p^a - p^b + p}{ab}$ polynômes irréductibles unitaires de degré ab.

3) Ce résultat montre que dans $\mathbb{Z}$, $ab \mid p^{ab} - p^a - p^b + p$. Retrouver cette relation de divisiblité en utilisant le petit théorème de Fermat.

4) Soient a, b et c trois nombres premiers deux à deux distincts. Combien y a-t-il dans $\mathbb{F}_p[X]$ de polynômes unitaires irréductibles de degré abc ?

5) La formule établie dans la question 2 montre qu'il y a 9 polynômes irréductibles de degré 6 dans $\mathbb{F}_2[X]$. On se propose de retrouver ce résultat de façon élémentaire.

a) Dans $\mathbb{F}_2[X]$, combien y a-t-il de polynômes irréductibles de degré 2, de degré 3 et de degré 4 ? Dresser leur liste.

b) Soit $P(X) = X^6 + a_5X^5 + a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 \in \mathbb{F}_2[X]$. Montrer que $P(X)$ n'a pas de racine dans $\mathbb{F}_2[X]$ si et seulement si $a_0 = 1$ et $|\{1 \leqslant i \leqslant 5;\ a_i = 1\}|$ est impair.

c) Combien y a-t-il dans $\mathbb{F}_2[X]$ de polynômes de degré 6 sans racine dans $\mathbb{F}_2$?

d) Parmi ceux-ci, combien y en a-t-il qui sont réductibles dans $\mathbb{F}_2[X]$? *Indication* : les dénombrer en observant les décompositions possibles en produits d'au moins deux irréductibles de degré $\geqslant 2$.

e) Conclure.

Exercice 2 –

1) Soit p un nombre premier. Quels sont les sous-corps de $\mathbb{F}_{p^4}$?

2) Soit $x \in \mathbb{F}_{p^4}$. Quel est le degré de $P_x(X)$, le polynôme minimal de x sur $\mathbb{F}_p$? On distinguera les cas suivant l'appartenance de x à tel ou tel sous-corps de $\mathbb{F}_{p^4}$.

3) On pose $Q_x(X) = (X - x)(X - x^p)(X - x^{p^2})(X - x^{p^3})$. Quelle relation y a-t-il entre $Q_x(X)$ et $P_x(X)$?

4) Établir la liste des polynômes unitaires irréductibles de degré 2 de $\mathbb{F}_3[X]$.

5) En déduire que le polynôme $P(X) = X^4 - X^3 - 1 \in \mathbb{F}_3[X]$ est irréductible.

6) Combien y a-t-il dans $\mathbb{F}_3[X]$ de polynômes unitaires irréductibles de degré 4 ?

7) On identifie $\mathbb{F}_{81}$ à $\mathbb{F}_3[X]/(P(X))$ et on note α la classe de X dans $\mathbb{F}_{81}$. Quels sont les ordres possibles de α dans $\mathbb{F}_{81}^{\times}$?

8) Calculer de façon économique α^{16} et α^{40}. Le polynôme $P(X)$ est-il primitif ?

9) Combien y a-t-il dans $\mathbb{F}_3(X)$ de polynômes unitaires irréductibles primitifs de degré 4 ?

10) Montrer que $\beta = \alpha^3 + \alpha^2 + 1$ appartient à un sous-corps strict de $\mathbb{F}_{81}$ que l'on précisera.

11) Déterminer $P_\beta(X)$.

Exercice 3 –

1) Montrer que dans $\mathbb{F}_2[X]$, le polynôme $\sum_{k=0}^{10} X^k$ est irréductible.

2) Montrer que dans $\mathbb{F}_2[X]$, le polynôme $\sum_{k=0}^{20} X^k$ est produit de tous les irréductibles de degré 2 et 3 et de 2 irréductibles de degré 6.

3) Montrer que dans $\mathbb{F}_2[X]$, le polynôme $Q(X) = \sum_{k=0}^{30} X^k$ est produit de 6 irréductibles de degré 5, que l'on notera $P_i(X)$ $(1 \leqslant i \leqslant 6)$.

4) Montrer que pour tout i, $P_i(X)$ est primitif.

5) Soit $P(X) = X^5 + X^2 + 1 \in \mathbb{F}_2[X]$. Montrer (sans faire le quotient de $Q(X)$ par $P(X)$) qu'il existe i tel que $P(X) = P_i(X)$.

6) On considère la suite $(s_i)_{i \geqslant 0} \in \mathbb{F}_2^{\mathbb{N}}$ définie par $s_0 = s_1 = s_2 = s_3 = s_4 = 1$ et par la relation de récurrence linéaire $s_{i+5} = s_{i+2} + s_i$ (pour tout $i \geqslant 0$). Montrer que $(s_i)_{i \geqslant 0}$ est périodique. Déterminer sa période sans calculer les premiers termes de la suite.

7) On identifie $\mathbb{F}_{32}$ à $\mathbb{F}_2[X]/(P(X))$. On note α la classe de X dans $\mathbb{F}_{32}$. Calculer $\mathrm{Tr}(1)$, $\mathrm{Tr}(\alpha)$, $\mathrm{Tr}(\alpha^2)$, $\mathrm{Tr}(\alpha^3)$ et $\mathrm{Tr}(\alpha^4)$.

8) En déduire un entier $k \geqslant 0$ tel que $s_i = \mathrm{Tr}(\alpha^{k+i})$ pour tout $i \geqslant 0$.