UNIVERSITÉ de BORDEAUX

ANNÉE UNIVERSITAIRE 2015/2016

Session 1 d'Automne

Master Sciences et Technologies, Mention Mathématiques ou Informatique

Spécialité Cryptologie et Sécurité Informatique

UE M1MA7W01 : Arithmétique

Responsable : M. Jean-Paul Cerri

Date : 15/12/2015. Durée : 3h.

Exercice 1 – Soit p un nombre premier.

1) On se propose d'abord de démontrer que X^4+1 n'est pas irréductible dans $\mathbb{F}_p[X]$.

a) Examiner le cas $p=2$.

On suppose désormais que $p>2$.

b) Montrer que $8 \mid p^2-1$.

c) En déduire qu'il existe dans $\mathbb{F}_{p^2}^\times$ un élément d'ordre 8.

d) Établir que dans $\mathbb{F}_{p^2}[X]$, le polynôme X^8-1 est scindé à racines simples.

e) En déduire que X^4+1 a toutes ses racines dans $\mathbb{F}_{p^2}$ et conclure.

2) Cherchons à préciser les choses. En s'inspirant de ce qui précède, montrer que si $p=2$ ou $p \equiv 1 \bmod 8$, dans $\mathbb{F}_p[X]$ le polynôme X^4+1 est scindé (à racines simples si $p \neq 2$), et que sinon, il est produit de deux irréductibles de degré 2 de $\mathbb{F}_p[X]$.

3) Factoriser X^4+1 dans $\mathbb{F}_3[X]$ et dans $\mathbb{F}_{17}[X]$.

Soit maintenant p un premier *impair* et soit $P(X)$ un diviseur irréductible de X^4+1 dans $\mathbb{F}_p[X]$. Soit d son degré. On note K le corps $\mathbb{F}_p[X]/(P(X))$ et α la classe de X dans K.

4) Quelle est la caractéristique de K ? Quel est son cardinal ?

5) Montrer que $\alpha \in K^\times$ et que $(\alpha+\alpha^{-1})^2=2$.

6) Montrer que 2 est un carré dans $\mathbb{F}_p$, i.e. il existe $x \in \mathbb{F}_p$ tel que $2=x^2$, si et seulement si $\alpha+\alpha^{-1} \in \mathbb{F}_p$.

7) Montrer que $\alpha^3+\alpha^{-3} \neq \alpha+\alpha^{-1}$.

8) En déduire que 2 est un carré dans $\mathbb{F}_p$ si et seulement si $p \equiv \pm 1 \bmod 8$.

Exercice 2 –

1) Soit $P(X) \in \mathbb{F}_5[X]$ défini par $P(X)=X^3+X^2+2X+2$. Factoriser $P(X)$ dans $\mathbb{F}_5[X]$ et en déduire que l'anneau $A=\mathbb{F}_5[X]/(P(X))$ n'est pas un corps.

2) À l'aide du théorème chinois, déterminer le cardinal de $A^\times$.

3) Le groupe $A^\times$ est-il cyclique ?

4) Soit $Q(X) \in \mathbb{F}_5[X]$ défini par $Q(X)=X^3+X^2+2$. Montrer que l'anneau $B=\mathbb{F}_5[X]/(Q(X))$ est un corps.

5) Combien y a-t-il de polynômes unitaires irréductibles de degré 3 dans $\mathbb{F}_5[X]$?

6) Combien y a-t-il de polynômes unitaires irréductibles primitifs de degré 3 dans $\mathbb{F}_5[X]$?

7) Le polynôme $Q(X)$ est-il primitif ? *Indication* : si α est la classe de X dans B, on pourra calculer α^4 puis α^{62} en se servant de l'automorphisme de Frobenius.

8) Soit d un entier naturel divisant $|B^\times|$. Combien y a-t-il dans $B^\times$ d'éléments d'ordre d ? Exprimer ces éléments en fonction de α.