Université Pierre et Marie Curie 2009-2010
Certificat MM067 Cryptologie, cryptographie algébrique

Partiel du 2 mars 2010

Durée 2 heures 30

Les documents, calculatrices et téléphones portables sont interdits.

Les trois exercices sont indépendants.

Exercice 1

Les cinq questions sont indépendantes.

1) Quels sont les nombres premiers impairs $p \neq 7$ tels que $7 + p\mathbb{Z}$ soit un carré dans $\mathbb{F}_p$?

2) Soit p un nombre premier impair. Dans l'anneau $\mathbb{F}_p[X]$ posons $F = X^4 + 4$.

   2.1) Supposons $p \equiv 3$ mod. 4. Montrer que F est le produit de deux polynômes irréductibles de degré 2 de $\mathbb{F}_p[X]$.

   2.2) Supposons $p \equiv 1$ mod. 4. Montrer que F a toutes ses racines dans $\mathbb{F}_p$.

   2.3) Si $p = 13$, expliciter les racines de F dans $\mathbb{F}_{13}$.

3) Dans l'anneau $\mathbb{Z}[X]$ posons $F = X^4 - X^2 + 1$. Soit p un nombre premier. On suppose qu'il existe un entier $n \in \mathbb{N}$ tel que p divise $F(n)$. On se propose d'établir que l'on a $p \equiv 1$ mod. 12.

   3.1) Montrer que p ne divise pas $6n$.

   3.2) Montrer que F divise $X^6 + 1$ et donc $X^{12} - 1$.

   3.3) Quel est le reste de la division euclidienne de $X^6 - 1$ par F ? Quel est celui de F par $X^2 + 1$?

   3.4) En déduire que p ne divise pas $(n^4 - 1)(n^6 - 1)$.

   3.5) En déduire l'ordre de la classe de n dans $\mathbb{F}_p^*$ et le fait que 12 divise $p - 1$.

4) Soit p un nombre premier congru à 1 modulo 4. Pour tout k compris entre 1 et $p-1$, l'expression $\left(\frac{k}{p}\right)$ désigne le symbole de Legendre. Montrer que l'on a

$$\sum_{k=1}^{p-1} k\left(\frac{k}{p}\right) = 0.$$

Indication : on pourra remarquer que l'application qui à k associe $p-k$ est une bijection de $\{1, \cdots, p-1\}$.

5) Rappeler la définition d'un entier pseudo-premier (ou pseudo-premier en base 2).

Soit p un nombre premier. Démontrer l'équivalence

$$p^2 \text{ est pseudo-premier} \iff 2^{p-1} \equiv 1 \text{ mod. } p^2.$$

Exercice 2

Soit K un corps fini de cardinal q. Étant donné un polynôme $F \in K[X]$, on note

$$\widetilde{F} : K \to K$$

la fonction polynôme qui lui est associée. Rappelons que si $F = \sum a_i X^i \in K[X]$, alors pour tout $x \in K$ on a $\widetilde{F}(x) = \sum a_i x^i \in K$.

1) Soient P et Q des polynômes de $K[X]$ de degrés strictement plus petits que q. Montrer que l'on a
$$P = Q \Longleftrightarrow \widetilde{P} = \widetilde{Q}.$$

2) Soit $f : K \to K$ une application. Montrer qu'il existe un unique polynôme $F \in K[X]$ de degré strictement plus petit que q tel que l'on ait $f = \widetilde{F}$.

3) En déduire le nombre de polynômes de $K[X]$ de degrés strictement plus petits que q qui n'ont aucune racine dans K.

Considérons un entier $n \geq q$.

4) Soit $R \in K[X]$ un polynôme de degré strictement plus petit que q. Quel est le nombre de polynômes $F \in K[X]$, unitaires de degré n, satisfaisant la condition suivante : le reste de la division euclidienne de F par $X^q - X$ est R.

5) En déduire le nombre de polynômes unitaires de degré n de $K[X]$ qui n'ont aucune racine dans K.

6) Expliciter les polynômes de degré 4 de $\mathbb{F}_2[X]$ qui n'ont aucune racine dans $\mathbb{F}_2$.

Exercice 3

1) Montrer $5 + 23\mathbb{Z}$ est une générateur du groupe $\mathbb{F}_{23}^*$.

2) Deux personnes, Alice et Bob souhaitent se construire une clé secrète commune pour chiffrer leur correspondance, avec le protocole de Diffie-Hellman, en utilisant le couple public
$$(\mathbb{F}_{23}, 5 + 23\mathbb{Z}).$$

Pour cela, Alice transmet à Bob l'élément $9 + 23\mathbb{Z}$ et Bob transmet à Alice l'élément $3 + 23\mathbb{Z}$. Quelle est leur clé secrète commune ?
