UNIVERSITÉ DE RENNES 1

Algèbre et Arithmétique 3

Examen (seconde session)

Documents, notes de cours ou de TD, téléphones portables, calculatrices sont interdits. ***Justifiez toutes vos réponses.*** *Il est bon de relire sa copie...*

Durée : 2 heures

Le barème est donné à titre indicatif.

Exercice 1 (5 points)

1 Enoncer le théorème de la division euclidienne dans $k[X]$.
2 Enoncer le théorème de la division euclidienne dans $\mathbf{Z}[i]$.
3 Soit G un groupe et a un élément de G d'ordre n. Soit k un entier naturel.
Donner sans justification l'ordre de a^k ?
4 Démontrer que tout groupe d'ordre 13 est commutatif.
5 Donner l'exemple d'un nombre premier qui ne peut pas s'écrire comme somme de deux carrés.

Exercice 2 (3 points)

1 Les groupes $\mathbf{Z}/9\mathbf{Z}$ et $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ sont-ils isomorphes ? Justifier.
2 Les groupes $\mathbb{F}_7$ et $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ sont-ils isomorphes ? Justifier.
3 Les groupes $(\mathbb{F}_7)^\star$ et $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ sont-ils isomorphes ? Justifier.

Exercice 3 (7 points)

1 On rappelle que le seul polynôme irréductible de degré 2 sur $\mathbb{F}_2$ est $X^2 + X + 1$. Montrer que le polynôme $X^4 + X^3 + 1$ est irréductible dans $\mathbb{F}_2[X]$. (On pourra admettre le résultat de cette question et continuer)
2 On note $A := \mathbb{F}_2[X]/ < X^4 + X^3 + 1 >$ l'anneau quotient de $\mathbb{F}_2[X]$ par l'idéal engendré par P. L'anneau A est-il un corps ? Comment obtenir dans chaque classe un représentant de degré minimal ? Combien a-t-il d'éléments ?
3 On note α la classe du polynôme X dans A. Déterminer α^4 et α^{15} comme polynômes de degré au plus 3 en α.
4 Déterminer toutes les puissances de α, α jusqu'à α^{15}, comme polynômes de degré au plus 3 en α.
5 Déterminer $\alpha^7 + \alpha^8 + \alpha^9$ comme polynômes de degré au plus 3 en α.
6 Ecrire l'inverse de $1 + \alpha + \alpha^3$ comme puissance de α.

Exercice 4 (5 points)

Alice et Bernard décident d'utiliser l'algorithme d'El Gamal. Ils utilisent le corps $\mathbb{F}_{19}$ avec l'élément $G = 2$.

1 Quels sont les ordres possibles des éléments de $\mathbb{F}_{19}^{\times}$. Déterminer l'ordre de 2 dans $\mathbb{F}_{19}^{\times}$.

2 Bernard choisit sa clé privée $c = 3$. Déterminer sa clé publique $C = G^c$.

3 Alice choisit une clé temporaire privée $d = 7$. Quelle est sa clé publique D ? Elle souhaite envoyer le message $m = 11$. Elle le chiffre en utilisant la clé publique C de Bernard par $(M_1, M_2) = (D, mC^d)$. Expliciter ce message chiffré.

4 Comment Bernard retrouve-t-il le message m ?

5 Dans un second envoi, Bernard reçoit $(8, 3)$. Quel est le message m envoyé cette fois par Alice ? Quelle clé privée a-t-elle utilisé cette fois ?

Un corrigé sera disponible sur internet.