UNIVERSITÉ DE RENNES 1

Algèbre et Arithmétique 3

Feuille de révision

Exercice 1

1 L'entier 256 appartient-il à $115 + 247\mathbf{Z}$?
2 L'entier -601 est-il un représentant de la classe $[-738]_{28}$ de $\mathbf{Z}/28\mathbf{Z}$?
3 Calculer l'élément 589 dans $\mathbf{Z}/23\mathbf{Z}$. Le résultat doit être représenté par un nombre compris entre 0 et 22.
4 Calculer l'élément 13^{923} dans $\mathbf{Z}/11\mathbf{Z}$. Le résultat doit être représenté par un nombre compris entre 0 et 10.

Exercice 2

Voici la table d'un groupe G.

$*$	a	b	c	d	e	f	g	h	i	j	k	l
a	d	j	g		h	i		e	f	b		k
b		g	j		l	e	d	i	k	a	h	
c	b	a	d			k	j	l	e	g	f	h
d			c	d				h	i			l
e		f		e	d	b	l	j	c	h	a	g
f	i	l	h			d	e	c	a	k	j	b
g	j	d		g	f	l		k	h	c	i	e
h	l	i		h	a	j	k	b		e	d	c
i	f		e	i	c	a	h		d	l	b	j
j		c	b	j	k		a	f	l	d	e	i
k	e	h	l	k	j	c	i	d			g	a
l		e	k	l	b	g		a	j	i	c	d

1 La compléter.
2 Le groupe est-il commutatif ?
3 Déterminer l'ordre de b.

Exercice 3

Considérons le groupe $(\mathbb{F}_{53})^\times$. Quels sont les ordres possibles d'un élément de ce groupe ? Combien d'éléments de chaque ordre ce groupe possède -t-il ? Déterminer en le justifiant un générateur de ce groupe.

Exercice 4

1. Montrer que le polynôme $X^3 + 2X + 1$ est irréductible dans $\mathbb{F}_3[X]$.
2. Quelle est alors la structure de l'ensemble quotient $A = \mathbb{F}_3[X]/(X^3 + 2X + 1)$?
3. Quel est le cardinal de A ? Soit α la classe du polynôme X dans ce quotient A. Donner la liste des éléments de A.

4. Sans calculs, mais en justifiant votre réponse, dire ce que valent les quantités suivantes

$$\alpha+\alpha+\alpha, \quad \alpha^3+2\alpha+1, \quad \alpha^{26}.$$

5. Déterminer l'ordre multiplicatif de α dans $A^\times$.
6. Etablir la table des puissances de α, jusqu'à α^{13}.
7. Calculer $(\alpha^2+2\alpha)(2\alpha^2+\alpha+2)$. Calculer $\alpha^4+\alpha^5$ comme puissance de α. Calculer $(2+\alpha)^{-1}$.

Exercice 5

1 Le polynôme X^3+X^2+X-1 est-il irréductible dans $\mathbb{F}_5$.
2 On considère l'anneau $A=\mathbb{F}_5[X]/<P>$. Est-ce un corps ?
3 Déterminer l'ordre de 2 dans le groupe des inversibles de A.
4 Déterminer l'ordre de $\alpha=[X]$ dans le groupe des inversibles de A.
5 Déterminer l'ordre de 2α dans le groupe des inversibles de A.

Exercice 6

Alice et Bernard décident d'utiliser l'algorithme d'El Gamal. Il utilise le corps $\mathbb{F}_{19}$ avec l'élément $G=15$.
1 Déterminer l'ordre de 15 dans $\mathbb{F}_{19}^\times$.
2 Bernard choisit sa clé privée $c=4$. Déterminer sa clé publique $C=G^c$.
3 Alice choisit une clé temporaire privée $d=5$. Quelle est sa clé publique D ? Elle souhaite envoyer le message $m=17$. Elle le chiffre en utilisant la clé publique C de Bernard par $(M_1,M_2)=(D,mC^d)$. Calculer 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 ?

Exercice 7

1 Montrer que le polynôme X^9-1 de $\mathbb{F}_3[X]$ vaut $(X-1)^9$. On considère le code ternaire C de longueur 9 associé au polynôme $g=(X-1)^5$
2 Déterminer l'alphabet, la longueur des mots, la dimension du code, le nombre de mots de code. Le code est-il cyclique ?
3 Donner une matrice génératrice de C.
4 Déterminer un élément de poids 3 du code.
5 Déterminer une matrice de contrôle H de ce code.
6 Déterminer la distance de ce code. Combien d'erreurs ce code peut-il détecter ? combien d'erreurs peut-il corriger ?
7 On a reçu le mot $r=121102210$. Calculer son image par H. Le mot r est-il un mot du code ?
8 Corriger le mot r en supposant qu'il n'y a eu au plus qu'une seule erreur de transmission.

Exercice 8

1 Le nombre 101 est-il premier ? Peut-il s'écrire comme somme de deux carrés.
2 Déterminer une racine c de -1 modulo 101.
3 Calculer le $pgcd(101, c-i)$ dans $\mathbf{Z}[i]$.
4 Ecrire 101 comme somme de deux carrés.