Université de Rennes

ARIC - Arithmétique pour la Cybersécurité

Feuille de TD n°Feuille n°2 :
Corps finis et logarithmes discrets

1. Division euclidienne des polynômes

Exercice 1 (Division de polynômes à coefficients dans un corps fini)

1 Effectuer la division euclidienne de $X^3 + 2X^2 - 5X + 8$ par $X^2 - 1$ dans $\mathbb{Z}/5\mathbb{Z}[X]$.
2 Effectuer la division euclidienne de $X^3 + 2X^2 - 5X + 8$ par $2X^2 - 1$ dans $\mathbb{Z}/5\mathbb{Z}[X]$.

Exercice 2 (Calcul de *pgcd* de polynômes)

Déterminer le pgcd des polynômes $X^5 - 3X^4 + X^3 + 2X^2 - 6X + 2$ et $X^4 - 3X^3 + 3X - 1$, éléments de $\mathbb{Q}[X]$.

Exercice 3 (Inverse)

1 Déterminer le *pgcd* des polynômes $X^2 + X + 1$ et $X^3 + X + 1$ dans $\mathbb{R}[X]$ et écrire une relation de Bezout entre eux.
2 La classe du polynôme $X^2 + X + 1$ est-elle inversible dans l'anneau quotient $\mathbb{R}[X]/(X^3 + X + 1)$?
3 Si oui, donner son inverse.

Exercice 4 (Système d'équations)

Résoudre dans $\mathbb{R}[X]$ le système de congruences

$$\begin{cases} P &= X & [X^2 + X + 1] \\ P &= 3 & [X^2 + X] \end{cases}$$

2. Irréductibilité des polynômes

Exercice 5 (En degré 3)

1 L'équation $x^3 + x + 1 = 0$ a-t-elle des solutions dans $\mathbb{F}_2$.
2 Le polynôme $x^3 + x + 1$ est-il irréductible dans $\mathbb{F}_2[X]$.
3 L'équation $x^3 + x + 1 = 0$ a-t-elle des solutions dans $\mathbb{Z}$?

Exercice 6 (Sur le nombre de racines d'un polynôme)

Déterminer les racines de $X^2 - 1$ dans $\mathbb{Z}/8\mathbb{Z}$. Comparer leur nombre au degré du polynôme. Comment expliquer ce phénomène ?

Exercice 7 (Polynômes irréductibles de $\mathbb{F}_2[X]$)

1 Le polynôme $(X^2 + X + 1)^3$ est-il irréductible dans $\mathbb{F}_2[X]$?
2 Donner la liste des polynômes irréductibles de $\mathbb{F}_2[X]$ de degré 2 et 3.
3 Donner un polynôme irréductible de degré 4 de $\mathbb{F}_2[X]$.
4 Ecrire dans $\mathbb{F}_2[X]$, une relation de Bezout pour $X^3 + X^2 + 1$ et $X^2 + X + 1$.

Exercice 8 (Construction d'un corps fini)

1 L'anneau $A = \mathbb{F}_2[X]/(X^2 + X + 1)$ est-il un corps ?
2 Combien A a-t-il d'éléments ?
3 Déterminer la liste des éléments et la table de multiplication de A.
4 Multiplier $[X^5 + X^4 + 6X]$ par $[X^4 + 7X^5 + 9X^3 + 4X^2]$ dans A et donner le résultat avec un représentant de la liste précédente.
5 Déterminer un inverse de $[X^3 + X^2 + 1]$ dans A

3. Sur le groupe multiplicatif des corps finis

Exercice 9 (le groupe $\mathbb{F}_{11}^\times$)

On note $\mathbb{F}_{11}$ le corps fini $\mathbb{Z}/11\mathbb{Z}$. Considérons le groupe $(\mathbb{F}_{11}^\times, \times)$. Quels sont les ordres possibles d'un élément de ce groupe ? Montrer que 2 est un générateur de $\mathbb{F}_{11}^\times$ et expliciter la fonction logarithme associée.

Exercice 10 (Calcul dans $\mathbb{F}_9$)

1 Le polynôme $X^2 + 1$ est-il irréductible dans $\mathbb{F}_3[X]$?
2 Quelle est alors la structure de l'ensemble quotient $A = \mathbb{F}_3[X]/(X^2 + 1)$?
3 Quelle relation vérifie la classe α du polynôme X dans ce quotient ?
4 Donner la liste des éléments de A.
5 Déterminer l'ordre multiplicatif de α dans $A^\times$.
6 Déterminer l'ordre multiplicatif de $a := \alpha + 2$ dans $A^\times$.
7 Etablir la table des puissances de a.
8 Calculer $(2 + a)(2 + 2a)$.
9 Calculer $a^3 + a^2$ comme puissance de a.
10 Calculer $(1 + 2a)^{-1}$.

Exercice 11 (Calculs dans $\mathbb{F}_{25}$)

On rappelle que $\mathbb{F}_5$ désigne le corps $\mathbb{Z}/5\mathbb{Z}$ à cinq éléments.

1 Montrer que l'anneau quotient $\mathbb{F}_{25} := \mathbb{F}_5[X]/(X^2+2X+1)$ est un corps. Combien a-t-il d'éléments ?

2 Si a est un élément non nul de $\mathbb{F}_{25}$, que valent $5a$, a^2+2a+1 et a^{24} ?

3 Soit x un élément de $\mathbb{F}_{25}$ tel que $x^2+3x+3=0$. Quel est l'ordre multiplicatif de x ?

Exercice 12 (Calculs dans $\mathbb{F}_{16}$)

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+1 est irréductible dans $\mathbb{F}_2[X]$.

2 On note $A := \mathbb{F}_2[X]/ < X^4+X+1 >$ l'anneau quotient de $\mathbb{F}_2[X]$ par l'idéal engendré par P. La classe de $3X^5+X^2+X+7$ est-elle nulle dans A ? L'anneau A est-il un corps ? Combien a-t-il d'éléments ?

3 On note α la classe du polynôme X dans A. Montrer que $\alpha^4 = \alpha+1 = 0$ et $\alpha^3 \neq 1$ et $\alpha^5 \neq 1$.

4 En déduire que α est un générateur de $A^\times$.

4. Sur la cryptographie

Exercice 13 (Le protocole de Diffie-Hellman)

On reprend l'exercice précédent. On utilise la clé publique (A, α). Alice et Bernard vont utiliser le protocole de Diffie-Hellman pour créer une clé secrète commune C.

1 Alice choisit $a=9$ et transmet α^9 à Bernard. Bernard choisit $b=5$ et transmet α^5. Quelle est leur clé secrète commune C ?

2 Ils décident maintenant de chiffrer les informations m en des messages $M = Cm$. Alice veut envoyer l'information $m = \alpha^3$. Quel message M envoit-elle ? Expliquer comment Bernard parvient à retrouver l'information m à partir du message reçu M.

Exercice 14 (l'algorithme d'El Gamal)

Alice et Bernard décident d'utiliser l'algorithme d'El Gamal. Il utilise 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 ?