ENS de Lyon
2017-2018

Option C

Corps finis

Dans toute la feuille p désigne un nombre premier.

1 Calculs dans $\mathbf{Z}/p\mathbf{Z}$

Exercice 1 (Opérations de base) On se place dans $\mathbf{Z}/307\mathbf{Z}$. Que vaut 154×78 ? Quel est l'inverse de -3 ?

Exercice 2 (Recherche d'un générateur) Soit p un nombre premier. On rappelle qu'un élément $g \in (\mathbf{Z}/p\mathbf{Z})^\times$ engendre $(\mathbf{Z}/p\mathbf{Z})^\times$ si et seulement si pour tout facteur premier q de $p-1$, on a $g^{(p-1)/q} \neq 1$.

1. Écrire une procédure qui prend en entrée un nombre premier p et un élément $x \in (\mathbf{Z}/p\mathbf{Z})^\times$, et qui dit si x est un générateur de $(\mathbf{Z}/p\mathbf{Z})^\times$.
2. Écrire une procédure qui prend en entrée un nombre premier p et renvoie un générateur de $(\mathbf{Z}/p\mathbf{Z})^\times$.

Exercice 3 (Représentation des polynômes) Soit $P(x) = x^6 - 1$ et $Q(x) = 2x^3 + 5$ des polynômes à coefficients dans $\mathbf{Z}/7\mathbf{Z}$. Comment les faire représenter par Sage ? Calculer leur pgcd, le quotient et le reste de la division euclidienne de P par Q.

Exercice 4 (Factorisation de polynômes) Comment factoriser un polynôme dans $\mathbf{Z}/p\mathbf{Z}[X]$? Comment obtenir la liste de ses facteurs irréductibles ?

Application : quel est le plus petit nombre premier p tel que $x^4 - x^3 + x^2 - x + 1$ est scindé à racines simples dans $\mathbf{Z}/p\mathbf{Z}$?

Exercice 5 (Recherche de polynômes irréductibles)

1. Étant donné un premier p et un entier n, écrire une procédure qui renvoie un polynôme unitaire de degré n à coefficients dans $\mathbf{Z}/p\mathbf{Z}$ par un tirage aléatoire uniforme.
2. Étant donné un premier p et un entier n, écrire une procédure qui renvoie un polynôme de degré n irréductible à coefficients dans $\mathbf{Z}/p\mathbf{Z}$.
3. Tester sur des valeurs de p et n pas trop grandes. (On rappelle qu'environ $1/n$ parmi les polynômes de degré n sont irréductibles.)

Exercice 6 (Une famille de polynômes)

1. Déterminer tous les entiers n compris entre 2 et 100 tels que le polynôme $P_n = X^n + X + 1$ est irréductible dans $\mathbf{Z}/2\mathbf{Z}[X]$.
2. Cela est-il cohérent avec ce que vous savez sur la probabilité qu'un polynôme de degré donné soit irréductible ?

2 Calcul dans les $\mathbf{F}_{p^n}$ avec $n > 1$

On travaille maintenant dans les extensions finies de $\mathbf{F}_p$ (commande `GF`).

Exercice 7 Créer le corps $\mathbf{F}_9$ et afficher tous ses éléments. Comment obtenir l'ordre d'un élément de $\mathbf{F}_9^\times$?

Exercice 8 (Polynômes primitifs) On rappelle que tout polynôme P irréductible de degré n sur $\mathbf{F}_p$ est scindé à racines simples dans $\mathbf{F}_{p^n}$, et si $\alpha \in \mathbf{F}_{p^n}$ est une racine de P, alors les racines de P sont de la forme α^{p^k} avec $0 \leq k \leq n-1$. On dit que P est *primitif* si de plus l'une quelconque de ses racines engendre le groupe $\mathbf{F}_{p^n}^*$.

1. Montrer que P est primitif si et seulement si P divise Φ_{p^n-1} dans $\mathbf{F}_p[X]$.
2. Écrire une procédure qui fournit un polynôme primitif de degré n.

Exercice 9
1. Construire le corps $\mathbf{F}_{16}$ puis, avec la méthode `subfields`, définir le corps $\mathbf{F}_4$ et un plongement $\iota : \mathbf{F}_4 \to \mathbf{F}_{16}$.
2. Soit x le générateur de $\mathbf{F}_{16}^\times$ donné par Sage. Quel est son polynôme minimal sur $\mathbf{F}_4$?
3. Expliciter un isomorphisme de corps dans les cas suivants :
   (a) $\mathbf{F}_2[X]/(X^3+X+1) \cong \mathbf{F}_2[X]/(X^3+X^2+1)$.
   (b) $\mathbf{F}_3[X]/(X^3-X+1) \cong \mathbf{F}_3[X]/(X^3-X^2+1)$.
   (c) $\mathbf{F}_2[X]/(X^7+X+1) \cong \mathbf{F}_2[X]/(X^7+X^3+1)$.

Exercice 10
1. Écrire une procédure qui prend en entrée un élément a de $\mathbf{F}_{p^n}$, et renvoie le polynôme minimal de a sur $\mathbf{F}_p$.
2. Si m divise n, alors $\mathbf{F}_{p^m}$ est un sous-corps de $\mathbf{F}_{p^n}$. Modifier la procédure précédente pour qu'elle renvoie le polynôme minimal de a sur $\mathbf{F}_{p^m}$.

3 Logarithme de Zech

Dans cette section, on décrit une manière alternative de calculer dans le corps fini $\mathbf{F}_{2^m}$. Soit g un générateur de $\mathbf{F}_{2^m}^\times$. On a une bijection $\mathbf{Z}/(2^m-1)\mathbf{Z} \cong \mathbf{F}_{2^m}^\times$ donnée par $i \mapsto g^i$. On convient également que $g^\infty = 0$.

Exercice 11 Écrire une procédure donnant le produit de deux éléments de $\mathbf{F}_{2^m}^\times$ représentés sous la forme précédente.

Pour l'addition, on utilise la remarque suivante : $g^i + g^j = g^i(1+g^{j-i})$. Il suffit donc de savoir calculer $1+g^i$ pour tout $i \in \mathbf{Z}/(2^m-1)\mathbf{Z}$. On définit une application $z : \mathbf{Z}/(2^m-1)\mathbf{Z} \cup \{\infty\} \to \mathbf{Z}/(2^m-1)\mathbf{Z} \cup \{\infty\}$ par $1+g^i = g^{z(i)}$.

Exercice 12 Montrer que z est une involution sans point fixe qui vérifie $z(2i) = 2z(i)$ et $z(-i) = z(i) - i$ pour tout $i \in \mathbf{Z}/(2^m-1)\mathbf{Z} \cup \{\infty\}$.

Exercice 13
1. Choisir un générateur de $\mathbf{F}_{16}^\times$ puis construire la *table de Zech* donnant explicitement l'application z pour ce générateur.
2. En déduire des fonctions permettant de calculer dans $\mathbf{F}_{16}$.
3. Faire de même pour les corps $\mathbf{F}_{32}$ et $\mathbf{F}_{64}$.

Exercice 14 Modifier les programmes précédents pour pouvoir calculer dans $\mathbf{F}_{2^m}$ avec m quelconque.