ENS Lyon 2014 - 2015

Préparation à l'agrégation externe Option C

TD/TP sur les corps finis

Généralités sur les corps finis

Exercice 1. —

1. Ecrire une procédure qui calcule l'inverse d'un élement de $\mathbb{Z}/p\mathbb{Z}$ lorsque p est un entier premier.
2. Calculer l'inverse de -3 dans $\mathbb{Z}/307\mathbb{Z}$.

Exercice 2. — **Recherche de générateurs** —

1. Notons $q_1, \dots, q_r$ les facteurs premiers deux à deux distincts de $p-1$. Montrer que $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$ si et seulement si l'on a $x^{\frac{p-1}{q_i}} \neq 1$ pour tout $i \in \{1, \dots, r\}$.
2. Ecrire une procédure qui prend en entrée une paire (p, x) avec p entier premier et x entier, et qui vérifie si x est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$.
3. Lorsque p est de la forme $2r+1$ avec r entier impair, reformuler l'algorithme précédent à l'aide du symbole de Legendre. Cette manipulation est-elle pertinente ?
4. Quelle est la proportion théorique d'éléments générateurs dans $(\mathbb{Z}/p\mathbb{Z})^\times$?
5. Ecrire une procédure qui prend en entrée un entier premier p et renvoie un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$.
6. Sur un tirage aléatoire de $N \geq 1$ éléments de $(\mathbb{Z}/p\mathbb{Z})^\times$, combien trouvez-vous de générateurs ? Comparer ainsi le résultat obtenu avec celui de la Question 4.
7. Ecrire des procédures analogues lorsque l'on remplace $\mathbb{Z}/p\mathbb{Z}$ par une extension finie $\mathbb{F}_q$ de $\mathbb{Z}/p\mathbb{Z}$.

Exercice 3. —

1. Justifier l'existence de la suite exacte suivante :

$$1 \longrightarrow \{\pm 1\} \longrightarrow \mathbb{F}_p^\times \xrightarrow{f} \mathbb{F}_p^\times \xrightarrow{g} \{\pm 1\} \longrightarrow 1 \ ,$$

   où l'on pose $f(x) = x^2$ et $g(x) = x^{\frac{p-1}{2}}$ pour tout $x \in \mathbb{F}_p^\times$.
2. Existe-t-il un analogue de cette suite exacte pour les corps finis non premiers ?

Exercice 4. — **Le logarithme de Zech** — Cet exercice présente une autre manière de faire des calculs dans les corps finis de caractéristique paire. Soit $m \geq 1$ un entier : si g est un générateur du groupe $\mathbb{F}_{2^m}^\times$, on sait que l'on dispose d'une bijection $\mathbb{Z}/(2^m-1)\mathbb{Z} \simeq \mathbb{F}_{2^m}^\times$ qui envoie i sur g^i. On choisit en outre de poser $g^\infty = 0$.

1. Ecrire une procédure permettant de calculer le produit de deux éléments de $\mathbb{F}_2^m$ représentés comme ci-dessus à l'aide du générateur g.

   Passons maintenant au calcul de la somme de deux éléments. Puisque $g^i + g^j = g^i(1 + g^{j-i})$, il nous suffit de savoir calculer $1 + g^k$ pour $k \in \mathbb{Z}/(2^m-1)\mathbb{Z}$. On introduit alors l'application $z : \mathbb{Z}/(2^m-1)\mathbb{Z} \cup \{\infty\} \to \mathbb{Z}/(2^m-1)\mathbb{Z} \cup \{\infty\}$ définie par $1 + g^k =: g^{z(k)}$.
2. Montrer que z est une involution de $\mathbb{Z}/(2^m-1)\mathbb{Z} \cup \{\infty\}$ qui vérifie :

$$\forall\ k \in \mathbb{Z}/(2^m-1)\mathbb{Z} \cup \{\infty\},\ z(2k) = 2z(k) \ \text{ et } \ z(-k) = z(k) - k \ .$$

3. Choisir un générateur g de $\mathbb{F}_{16}^\times$ et construire la table donnant explicitement l'application z pour ce choix de générateur.
4. En déduire des fonctions permettant de calculer dans $\mathbb{F}_{16}$.
5. Modifier les procédures de la question précédente pour pouvoir calculer dans une extension finie arbitraire de $\mathbb{F}_2$.

Polynômes sur les corps finis

Exercice 5. —

1. Comment faire représenter par Xcas un polynôme à coefficients dans $\mathbb{Z}/p\mathbb{Z}$? A coefficients dans une extension finie de $\mathbb{Z}/p\mathbb{Z}$?
2. Posons $P(X) = X^6 - 1$ et $Q(X) = 2X^3 + 5$.
   (a) Représenter $P(X)$ et $Q(X)$ dans $\mathbb{F}_7[X]$.
   (b) Calculer le pgcd de $P(X)$ et $Q(X)$ dans $\mathbb{F}_7[X]$.
   (c) Calculer le quotient et le reste de la division euclidienne de $P(X)$ par $Q(X)$ dans $\mathbb{F}_7[X]$.
3. Reprendre la question précédente en remplaçant $\mathbb{F}_7[X]$ par $\mathbb{F}_9[X]$.

Exercice 6. —

1. Déterminer un polynôme $P(X)$ de degré 2 irréductible sur $\mathbb{F}_9$ puis expliciter un isomorphisme entre les corps $\mathbb{F}_9[X]/(P(X))$ et $\mathbb{F}_{81}$.
2. Expliciter un isomorphisme de corps entre :
   (a) $\mathbb{F}_2[X]/(X^3 + X + 1)$ et $\mathbb{F}_2[X]/(X^3 + X^2 + 1)$;
   (b) $\mathbb{F}_3[X]/(X^3 - X + 1)$ et $\mathbb{F}_3[X]/(X^3 - X^2 + 1)$;
   (c) $\mathbb{F}_2[X]/(X^7 + X + 1)$ et $\mathbb{F}_2[X]/(X^7 + X^3 + 1)$.

Exercice 7. —

1. Montrer que pour tout entier $n \geq 1$, $X^{p^n} - X$ est le produit des polynômes irréductibles sur $\mathbb{F}_p$ dont le degré divise n.
2. Expliquer comment factoriser un polynôme à coefficients dans $\mathbb{F}_p$.
3. Ecrire une procédure permettant de tester l'irréductibilité sur $\mathbb{F}_p$ d'un polynôme.
4. Ecrire une procédure fournissant la liste des facteurs irréductibles sur $\mathbb{F}_p$ d'un polynôme à coefficients dans $\mathbb{F}_p$.
5. Déterminer le plus petit entier premier p tel que $X^4 - X^3 + X^2 - X + 1$ soit scindé à racines simples sur $\mathbb{F}_p$.
6. Factoriser le polynôme $X^9 - X \in \mathbb{F}_3[X]$ en produit de polynômes irréductibles sur $\mathbb{F}_3$.
7. Factoriser le polynôme $X^9 - X \in \mathbb{F}_9[X]$ en produit de polynômes irréductibles sur $\mathbb{F}_9$.
8. Exhiber un polynôme de degré 100 irréductible sur $\mathbb{F}_2$.
9. Expliquer comment modifier la procédure établie dans la Question 2 pour obtenir la liste des facteurs irréductibles sur $\mathbb{F}_{p^n}$ d'un polynôme à coefficients dans $\mathbb{F}_{p^m}$, avec m diviseur de n.
10. Estimer la complexité des procédures obtenues dans cet exercice.

Exercice 8. —

1. Ecrire une procédure prenant en entrée une paire (p, n), avec p entier premier et $n \geq 1$ entier, qui renvoie un polynôme unitaire de degré n à coefficients dans $\mathbb{F}_p$ par tirage aléatoire uniforme.
2. Ecrire une procédure prenant en entrée une paire (p, n), avec p entier premier et $n \geq 1$ entier, qui renvoie un polynôme unitaire de degré n irréductible sur $\mathbb{F}_p$.
3. Tester cette procédure pour des valeurs raisonnables de p et n, et évaluer son temps de calcul.

Exercice 9. —

1. Soit x le générateur de $\mathbb{F}_{16}^{\times}$ donné par Sage. Quel est son polynôme minimal sur $\mathbb{F}_4$?
2. Ecrire une procédure prenant en entrée un triplet (p, n, a), avec p entier premier, n entier naturel non nul et a élément de $\mathbb{F}_{p^n}$, qui renvoie le polynôme minimal de a sur $\mathbb{F}_p$.
3. Ecrire un algorithme prenant en entrée un quadruplet (p, n, m, a) avec p entier premier, n et m entiers naturels non nul et a élément de $\mathbb{F}_p^n$, qui renvoie, lorsque cela a un sens, le polynôme minimal de a sur $\mathbb{F}_{p^m}$.

Exercice 10. — On rappelle qu'un élément de $\mathbb{F}_p[X]$ de degré $n \geq 1$ est dit *primitif* lorsqu'il est irréductible sur $\mathbb{F}_p$ et que ses racines engendrent le groupe $\mathbb{F}_{p^n}^\times$.

1. Comment tester si un polynôme est primitif en ne faisant que des calculs sur $\mathbb{F}_p$?
2. Ecrire une procédure prenant en entrée une paire (p, n), avec p entier premier et $n \geq 1$ entier, qui renvoie un polynôme primitif sur $\mathbb{F}_p$ de degré n.

Exercice 11. —

1. Déterminer l'ensemble des entiers naturels $n \leq 100$ tels que le polynôme $P_n(X) = X^n + X + 1$ soit irréductible sur $\mathbb{F}_2$.
2. Soit $k \geq 1$ un entier. Déterminer le nombre d'entiers naturels $n \leq 10^k$ tels que $P_n(X)$ soit irréductible sur $\mathbb{F}_2$.
3. Le résultat de la question précédente est-il compatible avec vos connaissances sur la probabilité qu'un polynôme de degré donné soit irréductible sur $\mathbb{F}_2$? *On rappelle que la proportion de polynômes irréductibles sur $\mathbb{F}_p$ parmi les polynômes de degré n est environ de $\frac{1}{n}$.*

Cyclotomie dans les corps finis et réduction modulo p

Exercice 12. —

1. Faire afficher par Sage les 20 premiers polynômes cyclotomiques à coefficients dans $\mathbb{F}_7$.
2. Quel est le plus petit entier $n \geq 1$ tel qu'il existe un coefficient du n-ième polynôme cyclotomique sur $\mathbb{F}_7$ différent de $0, 1$ ou -1 ?
3. Démontrer que si n est premier ou produit de deux entiers premiers distincts, alors tous les coefficients non nuls du n-ième polynôme cyclotomique valent ± 1. Ce résultat dépend-il du choix du corps (fini) des coefficients ?

Exercice 13. — Soit p un entier premier. Si $P \in \mathbb{Z}[X]$ un polynôme de degré $n \geq 1$, on note $\overline{P} \in \mathbb{F}_p[X]$ le polynôme obtenu après réduction modulo p des coefficients de P.

1. Supposons que P et $\overline{P}$ aient même degré. Démontrer que si $\overline{P}$ est irréductible sur $\mathbb{F}_p$, alors P est irréductible sur $\mathbb{Q}$. L'est-il nécessairement sur $\mathbb{Z}$?
2. En déduire que les polynômes $X^4 - 17X^3 + 7$ et $X^5 - 7$ sont irréductibles sur $\mathbb{Q}$.
3. Considérons maintenant le polynôme $P(X) = X^4 + 1$.
   (a) Montrer que $\overline{P}$ n'est pas irréductible sur $\mathbb{F}_2$.
   (b) Supposons que p est impair.
      i) Montrer que l'on a $p^2 \equiv 1 \bmod 8$ puis que le polynôme $X^8 - 1$ divise le polynôme $X^{p^2-1} - 1$.
      ii) Fixons une racine α de $\overline{P}$ dans une extension de $\mathbb{F}_p$. Montrer que le degré de l'extension $\mathbb{F}_p[\alpha]/\mathbb{F}_p$ est majoré par 2, puis que le polynôme P n'est pas irréductible modulo p.
   (c) Enoncer le résultat que nous avons ainsi démontré.
4. Plus généralement, vérifier numériquement puis démontrer le résultat suivant.

   Lemme 1. *Soit k un corps fini à q éléments et soit n un entier naturel premier à q. Si r désigne l'ordre de q dans le groupe cyclique $(\mathbb{Z}/n\mathbb{Z})^\times$, alors le n-ième polynôme cyclotomique à coefficients dans k se décompose dans $k[X]$ en un produit de facteurs irréductibles unitaires deux à deux distincts et tous de même degré r.*