Irréductibilité et factorisation de polynômes dans $\mathbb{F}_p$

1 Exercices

Ici, p est partout un nombre premier.

Exercice 1.1 (Recherche de racines)**.**
Soit $P \in \mathbb{F}_p[X]$.

(*a*) Rappeler pourquoi P a les mêmes racines dans $\mathbb{F}_p$ que $\gcd(P, X^p - X)$ (voir le TD PGCD si nécessaire)
(*b*) Donner les racines de P dans $\mathbb{F}_p$ avec $P = X^4 + X + 1$ et $p = 5$ ou 7.
(*c*) Quel est le coût du calcul dans le pire cas avec P de degré n dans $\mathbb{F}_p[X]$?

Exercice 1.2 (Irréductibilité d'un polynôme au cas par cas)**.**
Soit $P = X^4 + X + 2 \in \mathbb{Z}[X]$. P est-il irréductible modulo 3 ? modulo 5 ?

Exercice 1.3 (Coût moyen de recherche de polynôme irréductible)**.**
(*a*) En utilisant le cours, rappeler le coût d'un test d'irréductibilité de $P \in \mathbb{F}_p[X]$ unitaire en fonction de p et $n = \deg P$.
(*b*) Encore avec le cours, rappeler la proportion asymptotique de polynômes irréductibles unitaires parmi les polynômes unitaires de degré n.
(*c*) En déduire un algorithme probabiliste de recherche de polynôme irréductible de degré n dans $\mathbb{F}_p[X]$, et donner le coût moyen de cet algorithme.

Exercice 1.4 (Construction explicite de $\mathbb{F}_{16}$)**.**
(*a*) Déterminer un polynôme de degré 4 irréductible dans $\mathbb{F}_2[X]$. Utiliser ce polynôme pour générer la table d'addition d'un corps K de taille 16 (noté `GF(2,4)` dans Xcas).
(*b*) Déterminer un générateur g de K^*, et construire la table des puissances.
(*c*) Avec cette table, donner une méthode rapide pour multiplier, inverser, calculer une racine carrée dans le corps K.
(*d*) Résoudre dans K les équations $x^2 + x + 1 = 0$, $x^2 + gx + g^2 + g + 1 = 0$, $x^2 + gx + 1 = 0$.

Exercice 1.5 (Puissance p-ième dans les anneaux de polynômes en caractéristique p)**.**
(*a*) Rappeler pourquoi pour tout $x \in \mathbb{F}_p$, $x^p = x$.
(*b*) Dans tout anneau commutatif unitaire A tel que $p \cdot 1_A = 0$ (on parle d'anneau de caractéristique p), montrer que $\mathrm{Frob}_A : x \mapsto x^p$ est encore un morphisme d'anneaux
(*c*) Pour tout $P \in \mathbb{F}_p[X]$, montrer que $P^p = P(X^p)$.
(*d*) Réciproquement, montrer que si K est un corps fini de caractéristique p, avec les injections canoniques,

$$\mathbb{F}_p[X] = \{P \in K[X] \mid P(X^p) = \mathrm{Frob}_{K[X]}(P) = P^p\}.$$

Exercice 1.6 (Factorisation squarefree (SQF) dans les corps finis)**.**
L'algorithme de Yun vu pour $\mathbb{Q}[X]$ ne fonctionne pas tel quel en caractéristique p, mais voici comment néanmoins trouver la factorisation sqf (squarefree) d'un polynôme $P \in \mathbb{F}_p[X]$.

On pose $P = QR$ avec Q (resp. R) le produit des facteurs irréductibles de P de multiplicité multiple de p (resp. première à p), avec la même multiplicité que dans P, et on cherche d'abord à calculer Q et R connaissant P.

(*a*) Rappeler pourquoi P est sans facteurs carrés si et seulement si $\gcd(P, P') = 1$.

(*b*) Montrer que $\gcd(P, P') = P$ si et seulement si P est une puissance p-ième dans $\mathbb{F}_p[X]$.
(*c*) Montrer que $P' = QR'$, et en déduire que $\gcd(P, P') = Q \gcd(R, R')$.
(*d*) En déduire comment calculer successivement $R/\gcd(R, R')$, R, puis Q.
(*e*) Montrer que l'algorithme de Yun s'applique tel quel à R.
(*f*) Enfin, en écrivant $Q = A^p$ pour un certain $A \in \mathbb{F}_p[X]$, montrer qu'on peut donner la factorisation sqf sqf de P par récurrence sur le degré.
(*g*) Appliquer cet algorithme pour calculer la factorisation square-free de $X^7 + X^6 + X + 1$ modulo 2.

Exercice 1.7 (Factorisation à degrés distincts (DDF))**.**
Soit $P \in \mathbb{F}_p[X]$ de degré n, on cherche à écrire

$$P = \prod_{k=1}^{n} P_k$$

où P_k est le produit des facteurs irréductibles de P de degré exactement k (avec leur multiplicité).

(*a*) Montrer avec le cours que pour tout $k \leq n$, $\gcd(P, X^{p^k} - X) = \prod_{d|k} P_d$.
(*b*) Rappeler comment calculer efficacement ces pgcd, quel est le coût total ?
(*c*) En déduire comment calculer chacun des P_k.

Exercice 1.8 (PGCD de polynômes à coefficients entiers)**.**
Soit P et Q deux polynômes à coefficients entiers.

(*a*) Montrer que pour tout nombre premier p ne divisant pas les coefficients dominants de P et Q, le degré du pgcd de P et Q dans $\mathbb{Q}[X]$ est inférieur ou égal au degré du pgcd de P et Q dans $\mathbb{Z}/p\mathbb{Z}[X]$.
(*b*) En déduire le PGCD de $X^4 + X + 1$ et $X^3 + 7X^2 + 7X + 1$ dans $\mathbb{Z}[X]$.

Exercice 1.9 (Algorithme de Cantor-Zassenhaus)**.**
Ici, on suppose $p > 2$, on cherche à factoriser un polynôme $P \in \mathbb{F}_p[X]$ de degré n.

(*a*) Avec les exercices précédents, justifier qu'on peut se ramener à P sans facteur carré et dont tous les facteurs irréductibles partagent le même degré donné $d|n$.
(*b*) Montrer que pour tout $Q \in \mathbb{F}_p[X]$,

$$Q^{p^d} - Q = Q(Q^{(p^d-1)/2} - 1)(Q^{(p^d-1)/2} + 1)$$

et que $P | Q^{p^d} - Q$.
(*c*) En déduire que

$$P = \gcd(P, Q) \gcd(P, Q^{(p^d-1)/2} - 1) \gcd(P, Q^{(p^d-1)/2} + 1).$$

(*d*) Avec l'aide du théorème des restes chinois, montrer que si P est réductible, cette factorisation est non triviale pour au moins la moitié des $Q \in \mathbb{F}_p[X]$ de degré au plus $n - 1$.
(*e*) En déduire l'algorithme probabiliste (de Cantor-Zassenhaus) pour factoriser P, et donner une estimation de son coût.
(*f*) Quel est son avantage par rapport à l'algorithme de Berlekamp ?

Exercice 1.10 (Cantor-Zassenhaus pour les racines carrées)**.**
Ceci est une version simplifiée de l'exercice 1.9, avec encore $p > 2$ (on peut le faire avant ou après).

Soit $P = X^2 + aX + b \in \mathbb{F}_p[X]$.

(*a*) Rappeler un algorithme utilisant le pgcd pour savoir si P a deux racines ou non dans $\mathbb{F}_p$. On suppose pour la suite qu'on est bien dans ce cas, et on cherche à calculer les racines.

(*b*) Montrer qu'alors $P|X^p - X$ et identifier $A = \mathbb{F}_p[X]/(P)$.
(*c*) Montrer que pour tout polynôme linéaire $L(X) = mX + Y \in \mathbb{F}_p[X]$, $P|L^p - L$ (calculer dans A).
(*d*) En déduire que pour au moins $p^2/2$ polynômes linéaires L, $1 \neq \text{pgcd}(P, L^{(p-1)/2} - 1) \neq P$.
(*e*) Donner un algorithme probabiliste pour calculer les racines de P qui évite une recherche exhaustive.

Exercice 1.11 (Calcul de produit par FFT)**.**
Effectuer le produit de $X^2 + 2X - 1$ et $2X + 1$ par FFT dans $\mathbb{F}_5[X]$.

Exercice 1.12 (Généralisation à $\mathbb{F}_q$)**.**
Ici, q est une puissance de p et $\mathbb{F}_q$ un corps fini de caractéristique p. Reprendre les énoncés théoriques des exercices précédents sur $\mathbb{F}_p[X]$ et les adapter à $\mathbb{F}_q[X]$.

2 TP

Exercice 2.1.
Vérifier/faire les parties calculatoires des exercices de TD.

Exercice 2.2 (Algorithme de Hörner et facteurs de degré 1)**.**
Implémenter l'algorithme de Hörner pour évaluer un polynome en un point. Modifier l'algorithme pour calculer le quotient. Écrire une fonction qui renvoie les facteurs de degré 1 d'un polynôme dans $\mathbb{Z}/p\mathbb{Z}$ pour p premier.

Exercice 2.3 (Test d'irréductibilité)**.**
(*a*) Écrire une fonction testant si un polynôme est irréductible modulo p.
(*b*) L'utiliser pour écrire un algorithme qui à n et p associe un polynôme irréductible unitiare de degré n dans $\mathbb{F}_p[X]$ puis une représentation du corps fini $\text{GF}(p, n)$.

Exercice 2.4 (Polynômes et factorisation SQF)**.**
(*a*) Écrire une fonction déterminant si un polynôme est squarefree dans $\mathbb{F}_p[X]$.
(*b*) Prolongement : écrire l'algorithme suggéré dans l'exercice 1.6 et le tester sur des exemples du TD.

Exercice 2.5 (Exemple de factorisation DDF)**.**
(*a*) En se basant sur les idées de l'exercice 1.7 (pas besoin d'écrire l'algorithme complet), déterminer les degrés des facteurs irréductibles de $X^7 + X^5 + 2X^4 + X^3 + X^2 + 2X + 1$ modulo 5 et 7.
(*b*) Quelle est la factorisation sur $\mathbb{Q}$ de ce polynôme ?
(*c*) Plus généralement, écrire l'algorithme de factorisation DDF et le tester sur cet exemple

Exercice 2.6 (Corps $\mathbb{F}_{256}$ (`GF(2,8)`))**.**
Implémenter le corps à 256 éléments de manière efficace (en utilisant un entier 8 bits et une table).

Exercice 2.7 (FFT)**.**

(*a*) Trouver un nombre premier $p < 2^{31}$ de la forme $1 + 2^{25}k$, $k \in \mathbb{Z}$, on le fixe pour la suite.

(*b*) Déterminer une racine primitive 2^{25}-ième de l'unité pour p.

(*c*) A quelle condition peut-on calculer le produit de deux polynômes à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ par FFT ?

(*d*) Le faire sur un exemple en utilisant l'instruction `fft` avec 3 arguments.

(*e*) Soit $n < 2^{31}$. Montrer qu'on peut effectuer un produit de polynômes de $\mathbb{Z}/n\mathbb{Z}[X]$ dont la somme des degrés est $< 2^{25}$ en utilisant au plus 3 nombres premiers p de ce type et 3 produits par FFT.

(*f*) En déduire une méthode de multiplication de polynômes à coefficients entiers par FFT.