
Corps finis

Exercice 1

Le but de cet exercice est l'étude et l'implantation de l'algorithme de Cipolla d'extraction de racines carrées modulo p . Soit p un nombre premier impair et D un résidu quadratique non nul (i.e. un carré non nul) modulo p . On cherche à déterminer une racine carrée de D dans $\mathbf{F}_p$.

1. Soit $u \in \mathbf{F}_p$. À quelle condition sur u et D le polynôme $P = X^2 - uX + D$ est-il irréductible sur $\mathbf{F}_p$?
2. Écrire une fonction `cherche_u(D,p)` qui à l'entrée (D,p) associe un $u \in \mathbf{F}_p$ tel que P est irréductible.
[Voir `kronecker` et `is_square`.]
3. (Sans **Sage**) Supposons P irréductible. Quelle est la dimension du quotient $\mathbf{F}_p[T]/(P(T))$ en tant que $\mathbf{F}_p$ -espace vectoriel ? Si t désigne la classe de T dans ce quotient, écrire la factorisation du polynôme $X^2 - uX + D$ en produit de facteurs linéaires ne faisant intervenir que l'indéterminée X et t . Exprimer alors D en fonction de t , puis une racine carrée de D en fonction de t .
4. Écrire une fonction `cipolla(D,p)` prenant (D,p) en entrée avec $\left(\frac{D}{p}\right) = 1$ et renvoyant une racine carrée de D modulo p en sortie.
[Voir la commande `K.<a>=k.extension(f(x))` permettant de définir l'extension K de k obtenue en quotientant $k[x]$ par la polynôme irréductible f . La syntaxe signifie que `a` est la classe de `x` dans le quotient.]
5. Évaluer le coût de cet algorithme.
6. Le temps permettant, étudier en fin de TP l'adaptation de l'algorithme au cas où le corps de base est un corps fini quelconque $\mathbf{F}_q$ avec q impair.
[Voir **GF** (pour « Galois Field ») ou **FiniteField** qui sont des commandes synonymes.]
7. Que dire du cas où q est une puissance de 2 ?

Exercice 2

1. Justifier, sans utiliser **Sage**, que $P = U^2 - 2 \in \mathbf{F}_5[U]$ est irréductible. On note $K = \mathbf{F}_5[U]/(P)$ l'extension de $\mathbf{F}_5$ correspondante.
2. Justifier de même que $Q = V^3 + V + 1 \in \mathbf{F}_5[V]$ est irréductible. On note $L = \mathbf{F}_5[V]/(Q)$ l'extension de $\mathbf{F}_5$ correspondante.
3. Montrer que Q est irréductible sur K :
 - (a) avec **Sage** (on pourra utiliser **GF**, ou **FiniteField**, et **PolynomialRing** et s'assurer que $V^3 + V + 1$ est bien vu comme polynôme à coefficients dans K),
 - (b) sans **Sage**.

On note M le corps $K[V]/(Q)$. C'est à la fois une extension de K et de L (en effet M est un corps contenant $\mathbf{F}_5$ et une racine de Q).
4. (Sans **Sage**) Quel est le degré de M sur $\mathbf{F}_5$, quel est son cardinal, quels sont ses sous-corps ?
5. Si u et v désignent respectivement les classes de U et V dans M , montrer, sans utiliser **Sage**, que $x = u + v$ engendre l'extension $M/\mathbf{F}_5$.

6. Calculer avec **Sage** le polynôme minimal de x sur $\mathbf{F}_5$ (une première étape consiste à donner une définition correcte de x sous **Sage**. Pour cela on pourra définir directement K en utilisant la commande `GF(5**2, name='...', modulus=...)`, puis quotienter l'anneau de polynômes en une variable sur K par l'idéal (Q) en utilisant `quotient`). Retrouver le fait que $M = \mathbf{F}_5(x)$.
7. Déterminer la matrice dont la i -ème colonne ($0 \leq i \leq 5$) donne les coordonnées de x^i dans la base $(1, v, v^2, u, uv, uv^2)$.
[On pourra utiliser **MatrixSpace** et trouver une façon astucieuse d'extraire les coefficients de x^i vu comme polynôme en u et v .]
8. En déduire une expression de u et v comme polynômes en x de degré < 6 .
9. Sans **Sage**, justifier que $x + x^{5^2} + x^{5^4} \in K$ et que $x + x^{125} \in L$.

Exercice 3

1. Écrire un test d'irréductibilité `test_irr(P,p)` prenant en entrée un polynôme $P \in (\mathbf{Z}/p\mathbf{Z})[X]$ de degré $n \geq 1$ et renvoyant **True** si P est irréductible sur $\mathbf{Z}/p\mathbf{Z}$ et **False** sinon.
2. Implanter un algorithme probabiliste `cherche_irr(n,p)` (l'algorithme de Ben Or par exemple, ou un algorithme utilisant le test de la question précédente) prenant en entrée un nombre premier p et un entier $n \geq 1$ et renvoyant un polynôme irréductible unitaire de degré n à coefficients dans $\mathbf{Z}/p\mathbf{Z}$ ainsi que le nombre N d'essais avant que le polynôme tiré uniformément au hasard ne soit irréductible.
3. Étudier la généralisation des fonctions ci-dessus au cas d'un corps fini $\mathbf{F}_q$ quelconque.
[Voir **GF** ou **FiniteField**.]

Exercice 4

Soit p un nombre premier impair et f un polynôme unitaire sans facteur carré de $\mathbf{F}_p[x]$ de degré $n = rd$. On suppose que f est produit de $r \geq 2$ polynômes irréductibles tous de degré d .

On considère le pseudocode suivant implantant un algorithme de recherche de facteur non trivial de f .

Entrée : (f, d) comme ci-dessus.

1. Choisir $h \in \mathbf{F}_p[x]$ de degré $< n$ uniformément au hasard.
2. Calculer $g := \gcd(f, h^{\frac{p^d-1}{2}} - 1)$.
3. Si $1 \leq \deg g \leq \deg f - 1$, on renvoie g , sinon on renvoie "échec".
 1. Quel est la probabilité de succès de l'algorithme ci-dessus.
 2. Implanter l'algorithme ci-dessus puis un algorithme de factorisation des polynômes de $\mathbf{F}_p[x]$ sans facteur carré et dont les facteurs irréductibles sont tous de même degré d (donné en entrée).
 3. Tester votre algorithme sur les polynômes cyclotomiques $\Phi_n(x)$ vus dans $\mathbf{F}_p[x]$ sous l'hypothèse $p \nmid n$.