UFR Sciences
M2 Calcul Formel

Martin WEIMANN

TP1 : addition, multiplication, écriture en base b

Exercice 1 (écriture binaire) Écrire une fonction `binaire`(n) qui renvoie (sous forme de liste) l'écriture binaire d'un entier naturel n. Voir aussi la procédure `bin` de Sage. Noter aussi la fonction `int('01101',base=2)` pour aller de l'écriture en base 2 vers les entiers.

Exercice 2 (exponentiation rapide) Implémenter deux algorithmes d'exponentiation rapide qui étant donnés x (a priori dans un anneau quelconque A) et $n \in \mathbb{N}$, calculent x^n. Le premier basé sur l'écriture binaire de n, le second en récursif.

Exercice 3 (addition et multiplication binaire) Ici, chaque entier est représenté par la liste de ses coefficients en base 2. Écrire les fonctions $a \mapsto a+1$, $(a,b) \mapsto (a+b)$, $a \mapsto 2a$ et $(a,b) \mapsto ab$.

Exercice 4 (écriture en base b rapide) On considère $a, b \in \mathbb{F}_7[X]$. Avec Sage, le corps fini $\mathbb{F}_p$ se déclare $GF(p)$ et l'anneau $\mathbb{F}_7[X]$ se déclare `F=GF(7)['X']`, suivi de `X=F.gen()` pour déclarer la variable. Autre option : écrire `F.<X>=PolynomialRing(GF(7))`.

1. Écrire une fonction `Baseb`(a,b) qui renvoie (sous forme de liste) l'écriture en base base b de $a \in \mathbb{F}_7[X]$.
2. Écrire une fonction récursive `BasebRapide`(a,b) basée sur l'exponentiation rapide et le principe "diviser pour régner" (cf CM).
3. Comparer les temps des 2 fonctions en considérant b unitaire de degré 3 et a un polynôme aléatoire de $\mathbb{F}_7[X]$ de degré 100, 1000, 10000 (utiliser `a=F.random_element(degree=100)`). Taper `%time` en début de ligne pour afficher un temps.
4. Ecrire une procédure `Developpe`(L,b) qui étant donnée la liste L des coefficients d'un polynôme a en base b, retourne le polynôme a.
5. Ecrire une procédure `DeveloppeRapide`(L,b) basée sur le principe "diviser pour régner".
6. Comparer les temps des 2 fonctions en reprenant les exemples obtenus à la question 3).

Exercice 5 (multiplication de Karatsuba)

1. Programmer un algorithme de multiplication naïve dans $K[X]$ (utiliser `A.list()` pour transformer un polynôme A en une liste), puis programmer l'algorithme de multiplication de Karatsuba.
2. Écrire une procédure qui calcule les temps nécessaires au calcul du produit de deux polynômes aléatoires de $\mathbb{F}_7[X]$ de degrés n avec vos deux algorithmes puis avec la multiplication implémentée dans Sage.
3. Comparer les temps des trois algorithmes pour $n = 100, 1000, 10000$.
4. En comparant les temps pour $n = 1000$ et $n = 10000$, vérifier que Karatsuba est en $O(n^{log_2(3)})$.