ÉNS de Lyon
2018-2019

Agrégation
Option C

TD FFT

Exercice 1 — Soit A un anneau, et $n \geq 1$ un entier. On note $A[\mathbb{Z}/n\mathbb{Z}]$ la A-algèbre $(A^{\mathbb{Z}/n\mathbb{Z}}, +, *)$. Vérifier que l'application

$$\begin{aligned} \varphi : A[\mathbb{Z}/n\mathbb{Z}] &\to A[X]/(X^n - 1) \\ f &\mapsto \Big[\sum_{i=0}^{n-1} f(i)X^i\Big] \end{aligned}$$

est un isomorphisme de A-algèbres.

Exercice 2 — Dans cet exercice, on explique comment construire des entiers N tels que $\mathbb{Z}/N\mathbb{Z}$ possède une racine principale de l'unité d'ordre 2^k.

Soit $A = \mathbb{Z}/N\mathbb{Z}$ avec N impair, et soit $n = 2^k$ avec $k \geq 1$.

1. Montrer que $\omega \in A$ est une racine principale n-ième de l'unité si et seulement si $\omega^{2^{k-1}} = -1$.

   Indication : Pour $1 \leq i \leq n-1$, poser $\operatorname{pgcd}(i, 2^k) = 2^\ell$ et utiliser une relation de Bézout.

2. En déduire que A possède une racine principale n-ième de l'unité si et seulement si tous les facteurs premiers de N sont congrus à 1 modulo 2^k.

3. Comment trouver une racine principale 2^k-ième de l'unité lorsque $N = p \equiv 1 \bmod 2^k$ est premier ?

4. Même question pour $N = p_1 \cdots p_r$, où les p_i sont des nombres premiers distincts vérifiant $p_i \equiv 1 \bmod 2^k$.

5. On suppose maintenant $N = a^{2^{k-1}} + 1$ avec $a \geq 2$ pair. Montrer que $\bar{a}$ est une racine principale n-ième de l'unité dans A.

6. En déduire que si N est un nombre de Fermat $F_m = 2^{2^m} + 1$ avec $m \geq k - 1$, alors $\mathbb{Z}/N\mathbb{Z}$ possède un racine principale n-ième de l'unité.

Exercice 3 — Multiplication dans $\mathbb{Z}/N\mathbb{Z}[X]$ — On suppose donnés un entier N et une racine principale 2^k-ième de l'unité dans $\mathbb{Z}/N\mathbb{Z}$.

1. Soient $P, Q \in \mathbb{Z}/N\mathbb{Z}[X]$ des polynômes vérifiant $\deg P + \deg Q < 2^k$. Expliquer comment calculer PQ en utilisant la transformée de Fourier rapide.

2. Quel est le coût de ce calcul en termes des degrés de P et Q ?

Exercice 4 — Multiplication dans $\mathbb{Z}[X]$ — Soient $P, Q \in \mathbb{Z}[X]$ des polynômes de degré $\leq d$.

1. On suppose que tous les coefficients de P et Q sont dans $[-M, M]$. Montrer que les coefficients de PQ sont dans $[-(d+1)M^2, (d+1)M^2]$.
2. Donner un algorithme de calcul de PQ utilisant la transformée de Fourier rapide et l'exercice 3.
3. Estimer le coût de ce calcul (en nombres d'opérations sur les bits) en termes de d et M.

Exercice 5 — Multiplication de grands entiers — On se donne deux entiers $a, b \geq 0$, représentés dans une base $M \geq 2$ fixée :

$$a = \sum_{i=0}^{d} a_i M^i \qquad b = \sum_{i=0}^{d} b_i M^i.$$

On pose $c = ab$.

1. Expliciter un polynôme $C \in \mathbb{Z}[X]$ à coefficients dans $[0, (d+1)(M-1)^2]$ tel que $c = C(M)$.
2. Comment calculer alors la représentation de c en base M ?
3. Estimer le coût de ce calcul (en nombres d'opérations sur les bits) en termes de la taille de a et b.
4. On suppose que l'on travaille sur une machine à 32 bits, et l'on prend $M = 2^{16}$. Posons $N = p_1 p_2 p_3$ avec $p_1 = 3 \cdot 2^{12} + 1$, $p_2 = 10 \cdot 2^{12} + 1$ et $p_3 = 15 \cdot 2^{12} + 1$ (ce sont des nombres premiers $< 2^{16}$). Estimer la taille des entiers que l'on peut multiplier en utilisant $\mathbb{Z}/N\mathbb{Z}[X]$ comme expliqué précédemment.