TD multiplication polynômes

October 19, 2020

Dans la suite $\mathbf{A}$ sera un anneau intègre et $\mathbf{k}$ un corps.
Exercice 1 : On définit sur $\mathbf{A}[[\mathbf{X}]]$ une distance par

$$d(f,g) = 2^{-\operatorname{val}(f-g)}.$$

Montrer que d est une distance sur $\mathbf{A}[[\mathbf{X}]]$ et montrer qu'il est complet pour cette distance.

Exercice 2 : Soit $\mathbf{k}$ un corps fini, on veut montrer que $\mathbf{k}^* := \mathbf{k} \setminus \{0\}$ est un groupe cyclique. Soit q le cardinal de $\mathbf{k}$, cela revient à montrer que $\mathbf{k}^*$ possède un élément d'ordre $q-1$.

1. Montrer que tout élément de $\mathbf{k}^*$ est d'ordre d pour d divisant $q-1$.
2. Montrer que $\mathbf{k}^*$ possède au plus d éléments d'ordre d.
3. Soit $x \in \mathbf{k}^*$ d'ordre d pour d divisant $q-1$ et H le sous-groupe engendré par x. Montrer que H est isomorphe à $\mathbf{Z}/d\mathbf{Z}$ et que tous les éléments d'ordre d sont dans H.
4. En déduire que $\mathbf{k}^*$ a au plus $\varphi(d)$ éléments d'ordre d avec φ l'indicatrice d'Euler et montrer que $\mathbf{k}^*$ est cyclique grace à la formule $n = \sum_{d|n} \varphi(d)$.

Exercice 3 : Si $(a,b) = (462, 104)$, calculer $d = pgcd(a,b)$ et un couple d'entiers u et v tels que $au + bv = d$. Même question (facultative) avec $(a,b) = (126, 69)$.

Exercice 4 :

1. Trouver un entier a compris entre 1 et 12 et égal à 27^{103} modulo 13.
2. Trouver un entier b compris entre 1 et 10 et égal à 27^{103} modulo 11.
3. En utilisant le théorème des restes chinois, trouver combien vaut 27^{103} modulo 143.

Exercice 5 : Trouver un entier x tel que

$$\begin{aligned} x &\equiv 3 \bmod 7 \\ x &\equiv 5 \bmod 11 \end{aligned}$$

Exercice 6 :

1. Écrire l'algorithme de Toom-Cook en pseudo-code.

2. On suppose que dans $\mathbf{A}$, les éléments $2, 3, 5$ sont inversibles. Soient f, g deux polynômes de degré 3, donner le nombre de multiplications nécessaires pour les multiplier dans l'algorithme de Karatsuba. Montrer que l'on peut s'en sortir avec seulement 7 multiplications.

3. En déduire un algorithme qui permet de multiplier 2 polynômes de degré $< N$ en $O(N^{\log_3 7})$.

4. Généraliser l'algorithme précédent pour obtenir un algorithme en $O(N^{\log_k(2k-1)})$ pour tout k entier et en déduire le résulat suivant:

   Pour tout $\varepsilon > 0$, il existe un algorithme qui multiplie deux polynômes de degré $< N$ en $O_\varepsilon(N^{1+\varepsilon})$

Exercice 7 : Dans cet exercice, on se place sur le corps $\mathbf{F}_{17}$ et on regarde les deux polynômes

$$f(x) = 5x^3 + 3x^2 - 4x + 3, \quad 2x^3 - 5x^2 + 7x - 2$$

On cherche à calculer le produit $h = fg$ à l'aide de la transormée de Fourier rapide. Puisque le polynôme h sera de degré 6, on choisit la puissance de 2 supérieure la plus proche, c'est à dire $2^3 = 8$. Ainsi $n = 8$ dans la suite de l'exercice.

1. Montrer que $\mathbf{F}_{17}$ admet une racine primitive 8-ième de l'unité.

2. Trouver une racine w primitive 8-ième de l'unité dans $\mathbf{F}_{17}$. On montrera que $t \in \mathbf{F}_{17}$ est un candidat si et seulement si t est un carré et $t^4 \neq 1$.

3. Calculer, à l'aide de la FFT, la transformée de Fourier en w de f et g.

   On se donne maintenant les valeurs de fg en $1, w, \cdots, w^7$: 14, 15, 0, 0, 5, 13, 5, 2.

4. Calculer w^{-1} dans $\mathbf{F}_{17}$.

5. Calculer à l'aide de la FFT, le coefficient constant et le coefficient en x^4 du polynôme produit h, résultats de la transformée de Fourier inverse utilisant w^{-1}.

6. Comparer avec le résultat obtenu en faisant le produit "à la main".

Exercice 8 : Montrer que l'algorithme naïf de multiplication de deux polynômes de degrés m et n requiert au plus $(n+1) \times (m+1)$ multiplications et mn additions dans $\mathbf{A}$.

Exercice 9 :

1. Ecrire 74 en binaire.

2. Calculer 2^{74} modulo 503 en utilisant l'algorithme "square-and-multiply" et en détaillant les étapes.

3. L'écriture binaire de 460 est 111001100. Détailler les étapes du calcul de g^{460} en utilisant l'algorithme de la fenêtre glissante avec une taille de fenêtre égale à 3.