Calcul Formel - Master 1 - Univ. Paris-Saclay
Chapitre 8 - Partie 1

I Transformée de Fourier discrète.

Soit $n \geq 1$ et A un anneau dans lequel n est inversible (i.e. caract de A doit être nulle ou première avec n). Soit $\omega \in A$ une racine primitive $n^{\text{ième}}$ de l'unité.

Si A corps : $\omega \in A^*$ d'ordre n.

Exemples : $A = \mathbb{C}$ ou $\mathbb{Q}(\exp(\frac{2i\pi}{n}))$, $\omega = \exp(\frac{2i\pi}{n}) \cdot \frac{q-1}{n}$ avec χ générateur de $\mathbb{F}_q^*$.

$A = \mathbb{F}_q$, $q = p^d$, $p \nmid n$, $n \mid q-1$, $\omega = \chi$

Déf : La transformée de Fourier discrète est l'application A-linéaire

$$TFD_\omega : A[X]_{<n} \longrightarrow A^n$$
$$P \longmapsto (P(1), P(\omega), P(\omega^2), \dots, P(\omega^{n-1})).$$

On identifie $A[X]_{<n}$ à A^n en identifiant $P(X) = a_0 + a_1 X + \dots + a_{n-1} X^{n-1}$ au n-uplet $(a_0, a_1, \dots, a_{n-1})$.

Alors $TFD_\omega : A^n \to A^n$.

Th : TFD_ω est bijective et $TFD_\omega^{-1} = \frac{1}{n} TFD_{\omega^{-1}}$.

Preuve : Matrice de TFD_ω dans les bases canoniques : Van Der Monde $(1, \omega, \dots, \omega^{n-1})$.

Corollaire Soient $P, Q \in A[X]$ tels que $\deg P + \deg Q < n$. Alors :

$$PQ = \frac{1}{n} TFD_{\omega^{-1}}\left(TFD_{\omega}(P) \cdot TFD_{\omega}(Q) \right).$$

produit dans A^n coordonnée par coordonnée

Preuve : $TFD_{\omega}(PQ) = TFD_{\omega}(P) \cdot TFD_{\omega}(Q)$.

Chapitre 8 - Partie 2.

II Transformée de Fourier rapide (FFT).

Soit $n = 2^k$, et A un anneau dans lequel 2 est inversible. (par ex. : $A = \mathbb{F}_q$, $q \equiv 1 \bmod 2^k$)
Notons $\omega \in A$ une racine primitive $n^{\text{ième}}$ de l'unité. Soit $P \in A[X]_{<n}$.

Th : On peut calculer $\mathrm{TFD}_\omega(P)$ en $O(n \log n)$ opérations arithmétiques dans A.
↳ sommes, soustractions, produits par des puissances de ω.

Preuve : Notons $n = 2m$ et $\omega_d = \omega^{n/d}$ pour tout diviseur d de n.
Notamment $\omega_n = \omega$ et $\omega_m = \omega^2$ racine primitive m-ième de l'unité dans A.
Notons $P(X) = Q_0(X^2) + X\,Q_1(X^2)$ avec $\deg Q_0, \deg Q_1 < m$.
Alors $\forall i \in [\![0, n-1]\!]$ $P(\omega_n^i) = Q_0(\omega_m^i) + \omega_n^i\, Q_1(\omega_m^i)$. On a $\omega_n^m = -1$ donc

$$\forall i \in [\![0, m-1]\!] \quad \begin{cases} P(\omega_n^i) = Q_0(\omega_m^i) + \omega_n^i\, Q_1(\omega_m^i) \\ P(\omega_n^{m+i}) = Q_0(\omega_m^i) - \omega_n^i\, Q_1(\omega_m^i) \end{cases}$$

Notons u_n le coût du calcul de l'image par TFD_{ω_n} d'un élément de $A[X]_{<n}$.
Alors $u_n \leq 2u_{n/2} + O(n)$ donc $u_n = O(n \log n)$.

Chapitre 8 - Partie 3.

III Multiplication rapide.

Th (Schönhage-Strassen, 1971) : On peut multiplier des entiers à n bits en $O(n \log n \log\log n)$ opérations élémentaires sur les bits.

But : calculer ab avec $a, b \in \mathbb{N}$ tels que $ab < 2^{64 \times 2^s}$ avec s fixé, $s \leq 61$.

Ex : $s=5$, $ab < 2^{2048}$; $s \approx 30$: stocker ab prend quelques Go.

On choisit a priori p_1, p_2, p_3 premiers distincts compris entre 2^{63} et 2^{64} tels que $p_i \equiv 1 [2^s]$.

On pré-calcule $\omega_1, \omega_2, \omega_3$ tels que ω_i soit une racine primitive 2^s-ième dans $\mathbb{F}_{p_i}$.

On écrit $a = a_0 + a_1 2^{64} + \dots + a_d 2^{64d} = P(2^{64})$ avec $P \in \mathbb{Z}[X]$ à coefficients a_i compris entre 0 et $2^{64}-1$.

De même $b = Q(2^{64})$. On a $a \geq 2^{64(\deg P)}$ donc $2^{64(\deg P + \deg Q)} \leq ab < 2^{64 \times (2^s)}$ donc $\deg(PQ) < 2^s$.

On calcule $\overline{PQ}$ (image de PQ dans $\mathbb{F}_{p_i}[X]$) par FFT.

Th Chinois donne $\overline{PQ}$ réduction modulo $p_1 p_2 p_3$

Notons $S \in \mathbb{Z}[X]$ à coefficients compris entre 0 et $p_1 p_2 p_3 - 1$ tel que $S \equiv PQ \bmod p_1 p_2 p_3$.

On les coeff. de PQ sont $\leq (2^{64})^2 \times 2^s = 2^{64 \times 2 + s} \leq 2^{3 \times 63} < p_1 p_2 p_3$. Donc $S = PQ$.

On a calculé $ab = S(2^{64})$.