TD 5 : PGCD rapide

Exercice 1. *Restes choisis*

Soit A et B deux polynômes de degrés n et $< n$ respectivement, et $\ell < n$ un entier. On cherche à calculer R_j, U_j et V_j tels que $AU_j + BV_j = R_j$ et R_j est le premier reste de degré $< \ell$ dans l'algorithme d'Euclide.

1. Comment faire si on utilise l'algorithme d'Euclide étendu ? Quelle est la complexité ?

On veut maintenant faire le même calcul, plus rapidement, en utilisant l'algorithme DEMIPGCD.

2. On suppose d'abord que $\ell \geq n/2$. Montrer que R_j, U_j et V_j peuvent s'obtenir *via* le calcul du demi-PGCD de $A \operatorname{quo} X^t$ et $B \operatorname{quo} X^t$ pour un t bien choisi.
3. On suppose maintenant que $\ell < n/2$. On calcule la matrice D de demi-PGCD de A et B.
   i. Que vaut $D\left(\begin{smallmatrix} A \\ B \end{smallmatrix}\right)$?
   ii. Comment peut-on obtenir R_j, U_j et V_j à partir de A, B et D ?
4. Écrire formellement l'algorithme complet et analyser sa complexité.

Exercice 2. *Preuve du lemme de correction*

Soit $(R_i)_{i\geq 0}$ la suite des restes associée à R_0 et R_1, et $n_i = \deg(R_i)$ pour tout i. On suppose qu'il existe deux entiers $t, d > 0$ tels que $t + 2d \geq n_0 > n_1 \geq t + d$. On note $R_0^\star = R_0 \operatorname{quo} X^t$ et $R_1^\star = R_1 \operatorname{quo} X^t$ et $(R_i^\star)_{i\geq 0}$ la suite des restes associée à $R_0^\star$ et $R_1^\star$. On note j l'indice tel que $\deg(R_j^\star) \geq d > \deg(R_{j+1}^\star)$.
On veut montrer par récurrence que pour $0 \leq i \leq j$,

$$R_i = R_i^\star X^t + R_i^- \text{ avec } \begin{cases} \deg(R_i^\star) = n_i - t & \text{et} \\ \deg(R_i^-) < t + n_0 - n_{i-1} \end{cases}$$

avec la convention $n_{-1} = n_0$.

1. Montrer que le résultat est correct pour $i = 0$ et $i = 1$.

On fixe $0 \leq i < j - 1$, et on suppose le résultat correct jusqu'au rang $i + 1$.

2. On note $Q_i^\star$ le quotient dans la division euclidienne de $R_i^\star$ par $R_{i+1}^\star$.
   i. Montrer que $R_i = R_{i+1}^\star Q_i^\star X^t + R_{i+2}^\star X^t + R_i^-$.
   ii. En déduire que $R_i = R_{i+1} Q_i^\star - R_{i+1}^- Q_i^\star + R_{i+2}^\star X^t + R_i^-$.
3. On pose $R_{i+2}^- = R_i^- - Q_i^\star R_{i+1}^-$.
   i. Montrer que $\deg(R_{i+1}^- Q_i^\star) < t + n_0 - n_{i+1}$.
   ii. En déduire que $\deg(R_{i+2}^-) < t + n_0 - n_{i+1}$.
4. i. Montrer que $t + n_0 - n_{i+1} < n_{i+1}$.
   ii. En déduire que $R_{i+2} = R_{i+2}^\star X^t + R_{i+2}^-$ et que le quotient de R_i par R_{i+1} est $Q_i^\star$.
5. Montrer que $\deg(R_{i+2}^\star) = n_{i+2} - t$ et conclure la récurrence.
6. En déduire que si $D^\star = \text{DEMIPGCD}(R_0^\star, R_1^\star)$, alors $D^\star\left(\begin{smallmatrix} R_0 \\ R_1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} R_j \\ R_{j+1} \end{smallmatrix}\right)$.