TD 10 : Pgcd et résultant

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 HGCD.

2. On suppose d'abord que $\ell \geq n/2$. Montrer que R_j, U_j et V_j peuvent s'obtenir comme le demi-PGCD de $A \operatorname{div} X^t$ et $B \operatorname{div} X^t$ 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 $D \cdot \binom{A}{B}$?
   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. *Résultant de polynômes*

Soit F et G deux polynômes de degrés m et n, respectivement, à coefficients dans un corps K. On note $x_1, \dots, x_m$ les racines de F et $y_1, \dots, y_n$ celles de G, dans la *clôture algébrique*[1] $\bar{\mathsf{K}}$ de K. Le *résultant* de F et G est défini[2] par

$$\operatorname{res}(F, G) = f_m^n g_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (x_i - y_j)$$

où f_m est le coefficient dominant de F et g_n celui de G, avec la convention que $\operatorname{res}(F, 0) = 0$.

1. **Propriétés de base.**
   i. Donner la valeur de $\operatorname{res}(F, \lambda)$ où λ est une constante.
   ii. Montrer que $\operatorname{res}(F, G) = (-1)^{mn} \operatorname{res}(G, F)$.
   iii. Montrer que $\operatorname{res}(F, G) = (-1)^{mn} g_n^m \prod_{j=1}^{n} F(y_j) = f_m^n \prod_{i=1}^{m} G(x_i)$.
   iv. Soit $F = QG + R$ la division euclidienne de F par G ($\deg(R) < \deg(G)$). Montrer que $\operatorname{res}(F, G) = (-1)^{mn} g_n^{m-r} \operatorname{res}(G, R)$ où $r = \deg(R)$.
2. **Algorithmes.**
   i. Déduire des questions précédentes un algorithme de type Euclide pour calculer le résultant de deux polynômes.
   ii. En généralisant l'algorithme précédent à un algorithme de type « Euclide étendu », montrer que pour tout F et G, il existe deux polynômes U et V tels que $\operatorname{res}(F, G) = FU + GV$.
   iii. Déduire des algorithmes précédents que $\operatorname{res}(F, G) \in \mathsf{K}$.
   iv. *(Bonus)* Adapter l'algorithme du demi-PGCD au résultant.
3. **Autres propriétés.**
   i. Montrer que $\operatorname{res}(F, G) = 0$ si et seulement si $\deg(\operatorname{pgcd}(F, G)) > 0$.
   ii. On définit le *discriminant* d'un polynôme F de degré m par $\operatorname{disc}(F) = ((-1)^{m(m-1)/2} / f_m) \operatorname{res}(F, F')$ où F' est la dérivée de F et f_m son coefficient dominant. Calculer le discriminant de $F = aX^2 + bX + c$.

1. D'après le *théorème fondamental de l'algèbre*, tout corps K possède une clôture algébrique $\bar{\mathsf{K}} \supseteq \mathsf{K}$ telle que tout polynôme de degré m à coefficients dans K possède exactement m racines dans $\bar{\mathsf{K}}$. Exemple : $\mathbb{C}$ est la clôture algébrique de $\mathbb{R}$.
2. On définit habituellement le résultant comme déterminant de la matrice de Sylvester associée à F et G (pour ceux qui connaissent !). La définition donnée ici est strictement équivalente.