Calcul Formel - Master 1 - Univ. Paris-Saclay



Chapitre 2 - Partie 1

## I Coût de la division euclidienne dans $\mathbb{K}[X]$.

<u>NB</u> : dans $\mathbb{Z}$ on considère chaque opération élémentaire (somme, soustraction, produit, calcul d'une division euclidienne) comme prenant un temps 1.

$\mathbb{K}$ corps. Soit $A, B \in \mathbb{K}[X]$ avec $B \neq 0$.

<u>Effectuer</u> la division euclidienne de $A$ par $B$ c'est trouver $Q, R \in \mathbb{K}[X]$ tels que $\begin{cases} \deg R < \deg B \\ A = BQ + R \end{cases}$

<u>Th</u> On peut effectuer la division euclidienne de $A$ par $B$ en $O((\deg A+1)(\deg B+1))$ opérations arithmétiques dans $\mathbb{K}$ (additions, multiplications, divisions dans $\mathbb{K}$).
Plus <u>précisément</u> : si $\deg A > \deg B > 0$ alors $O(\deg B \cdot (\deg A - \deg B))$ opérations suffisent.

<u>NB</u> : Si $A$ et $B$ sont non constants, le nombre d'opérations arithmétiques dans $\mathbb{K}$ est $O((\deg A)(\deg B))$. En effet on a alors $\deg A \leq \deg A + 1 \leq 2 \deg A$.

**Preuve** : Supposons $a \geq b$ avec $a = \deg A$ et $b = \deg B$.
Notons $Q = \sum_{i=0}^{a-b} q_i X^i$. On pose $R_0 = A$.
Pour $i$ allant de $0$ à $a-b$ on calcule :

$$R_{i+1} = R_i - q_{a-b-i} X^{a-b-i} B$$

où $q_{a-b-i}$ est le ~~co~~ quotient du coefficient de $X^{a-i}$ dans $R_i$ par le coefficient dominant de $B$.

**A la fin** : $R = R_{a-b+1}$.

$\mathbb{K} = \mathbb{Q}$, $a = 3$, $b = 1$

$$
\begin{array}{rl|l}
R_0 = A = & X^3 - \frac{1}{2}X^2 + \frac{3}{2}X - 1 & 2X+5 = B \\
\hline
q_2 X^2 B = & X^3 + \frac{5}{2}X^2 & \underbrace{\tfrac{1}{2}}_{q_2} X^2 - \underbrace{\tfrac{3}{2}}_{q_1} X + \underbrace{\tfrac{9}{2}}_{q_0} = Q \\
\hline
R_1 = R_0 - q_2 X^2 B = & -3X^2 + \frac{3}{2}X - 1 & \\
q_1 X B = & -3X^2 - \frac{15}{2}X & \\
\hline
R_2 = R_1 - q_1 X B = & 9X - 1 & \\
q_0 B = & 9X + \frac{45}{2} & \\
\hline
R_3 = R_2 - q_0 B = & -\frac{47}{2} = R &
\end{array}
$$

**Coût de ce calcul** :

<u>$a-b+1$ étapes</u> ; à chaque étape :
- 1 quotient dans $\mathbb{K}$
- Multiplier par $q_{a-b-i}$ chaque coefficient de $X^{a-b-i}B$ : coûte $b+1$ multiplications.
- Calculer $R_{i+1}$ : coûte $b+1$ soustractions au maximum.

**Conclusion** : $O\left((a-b+1)(b+1)\right)$ opérations arithmétiques dans $\mathbb{K}$.

Chapitre 2 - Partie 2.

## II Algorithme d'Euclide étendu.

Anneau euclidien $A$ : anneau intègre muni d'une jauge $\nu : A \setminus \{0\} \to \mathbb{N}$ telle que $\forall (a,b) \in A \times (A \setminus \{0\})$ $\exists (q,r) \in A^2$ tel que $a = bq + r$ et $\nu(r) < \nu(b)$ (en posant $\nu(0) = -\infty$).

NB : $A$ euclidien $\Rightarrow$ $A$ principal (Bezout) $\Rightarrow$ $A$ factoriel (pgcd) $\Rightarrow$ $A$ intègre.

pgcd$(a,b) = d$ défini si l'idéal $(a,b) = aA + bA = \{\lambda a + \mu b,\ \lambda, \mu \in A\}$ est principal.

Rappel : $A^* = \{u \in A,\ \exists v \in A,\ uv = 1\}$ unités de $A$.

Algorithme d'Euclide pour le calcul du pgcd de $a$ et $b$ :

Dans un anneau euclidien :
$$\begin{cases} \text{pgcd}(a,b) = \text{pgcd}(b,r) & \text{où } r \text{ est le reste dans la div. eucl. de } a \text{ par } b, \text{ si } b \neq 0 \\ & (\text{dans ce cas } \nu(r) < \nu(b)) \\ \text{pgcd}(a,0) = a. \end{cases}$$

Algorithme d'Euclide étendu : étant donné $a, b \in A$ avec $A$ anneau euclidien :

calcul simultané de pgcd$(a,b)$ et d'une relation de Bezout :
$$au + bv = \text{pgcd}(a,b) \quad \text{avec } u, v \in A.$$

$a = 26$
$b = 7$
dans $\mathbb{Z}$

$26 = 3\times 7 + 5$
$7 = 1\times 5 + 2$
$5 = 2\times 2 + 1$
$2 = 2\times 1 + 0$

$1 = 5 - 2\times 2$
$1 = 5 - 2\times(7 - 1\times 5)$
$1 = 3\times 5 - 2\times 7$
$1 = 3\times(26 - 3\times 7) - 2\times 7$
$1 = 3\times 26 - 11\times 7$

$5 = 1\times 26 - 3\times 7$
$2 = 7 - 1\times 5$
$= 7 - 1\times(1\times 26 - 3\times 7)$
$= -1\times 26 + 4\times 7$
$1 = (1\times 26 - 3\times 7) - 2\times(-1\times 26 + 4\times 7)$
$1 = 3\times 26 - 11\times 7.$

Algorithme d'Euclide étendu:

on part de $a_0 = a$, $b_0 = b$.

A chaque étape on maintient $a_i = x_i a + y_i b$ et $b_i = z_i a + t_i b$

A la fin : étape $i$ telle que $b_i = 0$ et $a_i = \text{pgcd}(a, b)$ donc $x_i$ et $y_i$ sont les $u, v$ cherchés.

Passage de l'étape $i$ à l'étape $i+1$ : [si $b_i \neq 0$] division eucl. de $a_i$ par $b_i$

$a_{i+1} = b_i$ et $b_{i+1}$ = reste dans la division où $q_i$ est le quotient

$b_{i+1} = a_i - q_i b_i$

$x_{i+1} = z_i$ $\qquad z_{i+1} = x_i - q_i z_i$

$y_{i+1} = t_i$ $\qquad t_{i+1} = y_i - q_i t_i$

Coût du passage de $i$ à $i+1$ : calculer 1 division euclidienne dans $A$

$O(1)$ opérations arithmétiques dans $A$ (produits, différences)

Coût en mémoire : $O(1)$ éléments de $A$

# Chapitre 2 - Partie 3

## III Coût de l'algorithme d'Euclide (étendu)

Suite de Fibonacci : $F_0 = 0$, $F_1 = 1$, et $\forall n \geq 0$ $F_{n+2} = F_{n+1} + F_n$.

### ① Dans $\mathbb{Z}$ :

**Th (Lamé)** : Soient $a, b \in \mathbb{N}^*$ tels que $a > b$. Soit $n \in \mathbb{N}^*$. Si l'algorithme d'Euclide pour le calcul de $\operatorname{pgcd}(a,b)$ nécessite au moins $n$ étapes alors $a \geq F_{n+2}$ et $b \geq F_{n+1}$.
En outre si $a = F_{n+2}$ et $b = F_{n+1}$ alors l'algorithme nécessite exactement $n$ étapes.

**Corollaire** : le coût de l'algorithme d'Euclide (étendu ou non) sur des entiers $a, b \in \mathbb{N}^*$ est : $O(\log(\min(a,b)))$ opérations arithmétiques dans $\mathbb{Z}$.
↳ sommes, produits, divisions euclidiennes.

**Preuve** : $F_n \approx \phi^n$ avec $\phi = \frac{1+\sqrt{5}}{2} \approx 1,618$.

### ② Dans $\mathbb{K}[X]$ (avec $\mathbb{K}$ corps)

**Th** : Soient $A, B \in \mathbb{K}[X]$ non constants. Alors le coût de l'algorithme d'Euclide (étendu ou non) appliqué à $A$ et $B$ est $O((\deg A)(\deg B))$ opérations arithmétiques dans $\mathbb{K}$.

**NB** : le nombre de divisions euclidiennes à effectuer est $O(\min(\deg A, \deg B))$.

Preuve : Notons $a = \deg A$, $b = \deg B$. Supposons $a > b > 0$. (6)

Notons $P_0 = A, P_1 = B, P_2, \ldots, P_e, P_{e+1} = 0$ les polynômes tels que $P_{i+2}$ soit le reste dans la division euclidienne de $P_i$ par $P_{i+1}$ (avec $P_e \neq 0$).

Notons $d_i = \deg P_i$ ; alors $d_0 = a > d_1 = b > d_2 > \ldots > d_e \geq 0$ donc $e \leq b+1$.

Coût du calcul de $P_{i+2}$ à partir de $P_i$ et $P_{i+1}$ : $\leq \underbrace{\lambda}_{\text{constante}} d_{i+1}(d_i - d_{i+1}) \leq \lambda \deg B (d_i - d_{i+1})$.

Coût du calcul de $\operatorname{pgcd}(A, B)$ : $\leq \lambda \deg B (\deg A - \deg P_e) \leq \lambda \deg A \deg B$.

Notons $P_{i+2} = P_i - Q_i P_{i+1}$ et $\begin{matrix} U_0 = 1 \\ V_0 = 0 \end{matrix}$ $\begin{matrix} U_1 = 0 \\ V_1 = 1 \end{matrix}$ $\left.\begin{matrix} U_{i+2} = U_i - Q_i U_{i+1} \\ V_{i+2} = V_i - Q_i V_{i+1} \end{matrix}\right\} P_i = AU_i + BV_i$

$$\begin{cases} \deg U_{i+2} = \sum_{k=1}^{i} \deg Q_k = d_1 - d_{i+1} \leq \deg B - \deg P_{e-1} < \deg B & \text{pour } i \leq e-2 \\ \deg V_{i+2} = \sum_{k=0}^{i} \deg Q_k = d_0 - d_{i+1} \leq \deg A - \deg P_{e-1} < \deg A & \text{pour } i \leq e-2 \end{cases}$$

$$\boxed{\begin{matrix} \deg Q_i = d_i - d_{i+1} \\ > 0 \end{matrix}}$$

Coût du calcul de $U_{i+2}$ à partir de $U_i, U_{i+1}$ et $Q_i$ : $O((d_i - d_{i+1}) \deg B)$

Coût du calcul de $U_2, U_3, \ldots, U_e$ : $O\left(\sum_{i=0}^{e-2} (d_i - d_{i+1}) \deg B\right) = O((\deg A)(\deg B))$.

# IV Calculs dans $\mathbb{Z}/_{n\mathbb{Z}}$ ou $\mathbb{K}[X]/_{(P)}$.

① Dans $\mathbb{Z}/_{n\mathbb{Z}}$ avec $n \geq 2$ : Représenter une classe modulo $n$ par son représentant $\in [\![0, n-1]\!]$.

Somme : $a, b \in [\![0, n-1]\!] \rightsquigarrow \begin{cases} a+b & \text{si } a+b \leq n-1 \\ a+b-n & \text{sinon} \end{cases}$

Produit : $a, b \in [\![0, n-1]\!] \rightsquigarrow$ reste dans la div. eucl. de $ab$ par $n$

] $O(1)$ opérations arithmétiques dans $\mathbb{Z}$

$O(\log n)$ opérations arithmétiques dans $\mathbb{Z}$

[ Déterminer si $a \in [\![0, n-1]\!]$ est inversible modulo $n$ :
[ Si oui, calculer l'inverse de $a$ modulo $n$ : c'est $u \in [\![0, n-1]\!]$ tel que $au \equiv 1 \; [n]$ c'est-à-dire tel que $\exists v \in \mathbb{Z}$ $au + vn = 1$.

] $O(\log n)$ opérations

② Dans $\mathbb{K}[X]/_{(P)}$ avec $d = \deg P \geq 1$ : représenter une classe mod $P$ par un polynôme de degré $< d$.

Somme, produit de $Q_1, Q_2 \in \mathbb{K}[X]_{<d}$ : calculer $Q_1 + Q_2$ ou $Q_1 Q_2$
prendre le reste dans la div. eucl. par $P$.

Pour la somme : inutile de prendre le reste : $O(d)$ opérations arith. dans $\mathbb{K}$.
Pour le produit : $O(d^2)$ opérations arith. dans $\mathbb{K}$.

Déterminer si $Q \in \mathbb{K}[X]_{<d}$ est inversible modulo $P$
et si oui calculer son inverse

] $O(d^2)$ opérations arith. dans $\mathbb{K}$.

# V Théorème chinois

**Th** Soit $A$ un anneau et $a, b \in A$. Si $(a,b) = A$ alors $(a) \cap (b) = (ab)$ et le morphisme

$$\varphi : A/(ab) \to A/(a) \times A/(b) \qquad \text{est un isomorphisme.}$$
$$x \bmod (ab) \mapsto (x \bmod (a),\ x \bmod (b))$$

Dans $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{K}[X]/(P)$ (si $a, b \in \mathbb{N}^* \setminus \{1\}$ ou si $a, b \in \mathbb{K}[X]$ non constants) :

Dans $\mathbb{K}[X]$ : $x \bmod (ab)$ : $x$ polynôme de degré $< \deg(ab)$

Calcul de $\varphi(x)$ : prendre le reste dans les div. eucl. de $x$ par $a$ et par $b$

$O(d^2)$ avec $d = \deg A + \deg B$

Dans $\mathbb{Z}$ : $O(1)$ opérations.

Calcul de $\varphi^{-1}$ : Soient $x, y \in A$. Alors $\varphi^{-1}(x \bmod (a), y \bmod (b)) = (xbv + yau \bmod (ab))$

avec $u, v \in A$ tels que $au + bv = 1$.

Si $u$ et $v$ sont connus : dans $\mathbb{Z}$ : $O(1)$ opérations.

dans $\mathbb{K}[X]$ : $O(d^2)$ opérations arithmétiques dans $\mathbb{K}$ avec $d = \deg A + \deg B$

Calcul de $u$ et $v$ : dans $\mathbb{Z}$ : $O(\min(\log a, \log b))$ opérations

dans $\mathbb{K}[X]$ : $O(\deg A \deg B)$ opérations dans $\mathbb{K}$