

FEUILLE D'EXERCICES n° 6

Exercice 1 – [ALGORITHME D'EUCLIDE ÉTENDU, INVERSE MODULAIRE]

- 1) Calculer $\text{pgcd}(312, 793)$ et trouver une relation de Bézout entre ces entiers.
- 2) 73 est-il inversible modulo 119 ? Si oui, calculer son inverse.

Exercice 2 – [ALGORITHME D'EUCLIDE ÉTENDU POUR LES POLYNÔMES]

On rappelle ici l'algorithme d'Euclide étendu appliqué à deux polynômes F et $G \in K[X]$ où K est un corps commutatif.

Algorithme 1. Algorithme d'Euclide étendu

Entrées: $F, G \in K[X]$

Sorties: $\text{pgcd}(F, G)$ et $A, B \in K[X]$ tels que $AF + BG = \text{pgcd}(F, G)$

1: $A_0 = 1, B_0 = 0, R_0 = F$

2: $A_1 = 0, B_1 = 1, R_1 = G$

3: $i = 1$ {initialisations}

4: **tantque** $R_i \neq 0$ **faire**

5: Division de R_{i-1} par $R_i \rightarrow$ quotient Q et reste R_{i+1}

6: $A_{i+1} = A_{i-1} - QA_i$

7: $B_{i+1} = B_{i-1} - QB_i$

8: $i = i + 1$

9: Retourner le dernier R_i non nul ainsi que les A_i et B_i correspondants

Pour tout i , on note $n_i = \deg R_i$.

1) Sur papier, appliquer cet algorithme aux polynômes $X^2 + X + 1$ et X^2 . Quel est l'inverse de $X^2 + X + 1 \bmod X^2$? Soit $P \in K[X]$. Montrer que P est inversible dans $K[X]/X^k$ pour tout $k \in \mathbb{N}$ si et seulement si $P(0) \neq 0$.

2) L'algorithme d'Euclide classique calcule le pgcd sans calculer les coefficients de Bézout. Montrer que la complexité algébrique de cet algorithme est en $O((\deg F + 1)(\deg G + 1))$.

3) Montrer les égalités suivantes.

(1) $\deg A_i = n_1 - n_{i-1}$ (pour $i > 1$)

(2) $\deg B_i = n_0 - n_{i-1}$ (pour $i > 0$)

4) Montrer que la complexité algébrique de l'algorithme d'Euclide étendu est en $O((\deg F + 1)(\deg G + 1))$.

Exercice 3 – [RESTES CHINOIS]

1) Sur papier, résoudre dans \mathbb{Z} les systèmes

$$\begin{cases} 12x - 12 \equiv 6 \pmod{33} \\ 7x + 6 \equiv 7 \pmod{13} \\ 6x - 21 \equiv 9 \pmod{54} \end{cases} \quad \begin{cases} 15x \equiv 7 \pmod{25} \\ 8x \equiv 1 \pmod{13} \\ 7x \equiv 4 \pmod{11} \end{cases}$$

$$\begin{cases} x \equiv 5 \pmod{21} \\ x \equiv 3 \pmod{28} \\ x \equiv 1 \pmod{5} \end{cases} \quad \begin{cases} x \equiv 3 \pmod{21} \\ x \equiv 17 \pmod{49} \\ x \equiv 1 \pmod{5} \end{cases} \quad \begin{cases} 3x + 1 \equiv 0 \pmod{5} \\ 4x + 2 \equiv 1 \pmod{7} \\ x - 1 \equiv 1 \pmod{4} \end{cases}$$

2) Reprendre l'exercice en utilisant la commande `crt` de sage.

On connaît bien l'algorithme correspondant dans le cas où les moduli sont deux à deux premiers entre eux. La question suivante porte sur le cas général.

3) Soient a et b deux entiers > 0 . On considère le système d'inconnue N

$$\begin{cases} N \equiv \alpha \pmod{a} \\ N \equiv \beta \pmod{b} \end{cases}$$

et on pose $\delta = \text{pgcd}(a, b)$, puis u et v deux entiers tels que $au + bv = \delta$.

a) Montrer que le système n'a pas de solution si $\alpha \not\equiv \beta \pmod{\delta}$.

b) Sinon, montrer que

$$N := \alpha + u \frac{a}{\delta} (\beta - \alpha) = \beta + v \frac{b}{\delta} (\alpha - \beta) = u \frac{a}{\delta} \beta + v \frac{b}{\delta} \alpha$$

convient. Montrer que cette solution est unique modulo $\frac{ab}{\delta}$ (c'est-à-dire, montrer que si N' est une autre solution, alors $N \equiv N' \pmod{\frac{ab}{\delta}}$).

4) En déduire un algorithme pour résoudre un nombre quelconque de congruences simultanées.

Exercice 4 – [INTERPOLATION]

Dans cet exercice, les questions 1) et 2) seront faits sur papier, les autres pourront être faits en utilisant une machine.

1) Déterminer le polynôme P de $\mathbb{Q}[x]$ de degré inférieur ou égal à 2 tel que

$$P(0) = 2, \quad P(1) = 2, \quad P(2) = 1.$$

2) Déterminer le polynôme P de $\mathbb{Q}[x]$ de degré inférieur ou égal à 3 tel que

$$P(0) = 0, \quad P'(0) = 1, \quad P(1) = 1, \quad P'(1) = 0.$$

3) Déterminer le polynôme P de $\mathbb{Q}[x]$ de degré inférieur ou égal à 4 tel que

$$P(0) = -1, \quad P(1) = 1, \quad P(2) = 7, \quad P'(1) = 3, \quad P''(1) = 1.$$

4) Déterminer le polynôme P de $\mathbb{F}_7[x]$ de degré inférieur ou égal à 4 tel que

$$P(0) = 2, P(1) = 2, P(2) = -1, P(-1) = 1, P'(1) = 0.$$

Exercice 5 – [APPROXIMANTS DE PADÉ]

Cet exercice utilise l'algorithme d'Euclide étendu, rappelé dans l'exercice 2. Avec les notations de cet exercice, on utilisera notamment les égalités suivantes.

- (1) $A_i F + B_i G = R_i$ pour tout i
- (2) $\deg A_i = n_1 - n_{i-1}$ (pour $i > 1$)
- (3) $\deg B_i = n_0 - n_{i-1}$ (pour $i > 0$)

Soient $F = f_0 + f_1 X + f_2 X^2 + \dots \in K[[X]]$ et $m, n \in \mathbb{N}$.

On appelle *approximant de Padé de type (m, n)* de F la donnée de U et $V \in K[X]$ vérifiant

$$\begin{cases} V \neq 0, \deg U \leq m \text{ et } \deg V \leq n \\ VF - U = X^{m+n+1}R, \text{ où } R \in K[[X]]. \end{cases}$$

1) En posant $F' = f_0 + \dots + f_{m+n} X^{m+n}$ et en appliquant l'algorithme d'Euclide étendu à F' et X^{m+n+1} , montrer qu'un tel approximant existe et que la fraction U/V est unique.

2) Soit \mathcal{F} une fraction rationnelle de $K(X)$ quotient de deux polynômes U et V de $K[X]$ de degrés $\leq n$ et premiers entre eux mais que l'on ne connaît pas. Supposons que l'on connaisse en revanche un développement en série formelle de \mathcal{F} en 0 :

$$F = f_0 + f_1 X + f_2 X^2 + \dots$$

Comment à partir de F retrouver U et V à une constante multiplicative près (reconstruction rationnelle) ?

Indication : se servir d'un approximant de Padé de type (n, n) de F .

3) On suppose que l'on connaît un certain nombre s de termes consécutifs d'une suite (u_n) satisfaisant une relation de récurrence d'ordre k :

$$u_{n+k} = a_{k-1} u_{n+k-1} + \dots + a_0 u_n$$

dont les coefficients a_k nous sont inconnus. On supposera en outre que k est minimal et que $s = 2k$. Montrer comment on peut retrouver la relation de récurrence, et donc calculer un terme quelconque de la suite, en se servant de la méthode préconisée en 1).

Indication : chercher un approximant de Padé approprié de la série génératrice

$$F = \sum_{i \geq 0} u_i X^i.$$

4) Essayer avec :

- 1, 1, ... et $k = 1$;
- 3, 5, 8, 13, ... et $k = 2$;
- 12, 134, 222, 21, -3898, -40039, -347154, -2929918, ... et $k = 4$,

en cherchant à chaque fois le terme suivant.

5) Estimer la complexité algébrique de chacun des algorithmes de cet exercice.

6) Comparer l'algorithme utilisé pour répondre à la question **3)** avec la résolution directe (par le pivot de Gauss par exemple) du système

$$\begin{cases} u_k &= a_{k-1}u_{k-1} + \cdots + a_0u_0 \\ u_{k+1} &= a_{k-1}u_k + \cdots + a_0u_1 \\ &\vdots \\ u_{2k-1} &= a_{k-1}u_{2k-2} + \cdots + a_0u_{k-1}. \end{cases}$$