

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) 15 est-il inversible modulo 38 ? Si oui, calculer son inverse.

Exercice 2 – [COMPLEXITÉ DE L'ALGORITHME D'EUCLIDE ÉTENDU POUR LES ENTIERS]

On rappelle l'algorithme d'Euclide étendu.

Algorithme 1. Algorithme d'Euclide étendu pour les entiers

Entrées: $a, b \in \mathbb{N}$, $(a, b) \neq (0, 0)$

Sorties: $\text{pgcd}(a, b)$ et $u, v \in \mathbb{Z}$ tels que $au + bv = \text{pgcd}(a, b)$

1: $u_0 = 1, v_0 = 0, r_0 = a$

2: $u_1 = 0, v_1 = 1, r_1 = b$

3: $i = 1$ {initialisations}

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

5: Division de r_{i-1} par $r_i \rightarrow$ quotient q_i et reste r_{i+1}

6: $u_{i+1} = u_{i-1} - q_i u_i$

7: $v_{i+1} = v_{i-1} - q_i v_i$

8: $i = i + 1$

9: Retourner le dernier r_i non nul ainsi que les u_i et v_i correspondants

- 1) Soit $U_i = \begin{pmatrix} u_i & v_i \\ u_{i+1} & v_{i+1} \end{pmatrix}$. Vérifier que pour tout i ,

$$U_i = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = U_i \begin{pmatrix} a \\ b \end{pmatrix}$$

- 2) Montrer que $U_i^{-1} = \begin{pmatrix} |v_{i+1}| & |v_i| \\ |u_{i+1}| & |u_i| \end{pmatrix}$.

3) En déduire que pour tout $i > 0$, $|u_i| \leq b/r_{i-1}$ et $|v_i| \leq a/r_{i-1}$.

4) Montrer que la complexité binaire de cet algorithme est quadratique.

Exercice 3 – [ALGORITHME D'EUCLIDE ÉTENDU POUR LES POLYNÔMES]

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

Algorithme 2. 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) Soit $P \in \mathbb{Q}[X]$ tel que $P(0) \neq 0$. Montrer que P est premier à X^k pour tout entier naturel k . Calculer deux polynômes U et V de $\mathbb{Q}[X]$ tels que

$$U(X)(X-1)^2 + V(X)X^2 = 1.$$

En déduire l'inverse de $(X-1)^2 \bmod X^2$.

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 4 – [INVERSION RAPIDE MODULO x^n] Soit K un corps. Soient $F \in K[x]$ et n un entier naturel non nul. On suppose que $F(0) = 1$. On sait que dans ce cas, la classe de F dans $K[x]/(x^n)$ est inversible. Cet exercice porte sur un algorithme rapide pour calculer son inverse.

Soit (A_i) la suite définie de la manière suivante.

$$A_0 = 1 \quad , \quad A_{i+1} = 2A_i - FA_i^2 \quad \forall i \geq 0.$$

1) Montrer que $FA_i \equiv 1 \pmod{x^{2^i}}$ pour tout $i \geq 0$.

2) En déduire un algorithme **Inverse(n, F)** pour calculer l'inverse de F modulo x^n . On s'efforcera d'optimiser la complexité de cette fonction.

3) On suppose que la complexité algébrique de la multiplication de deux polynômes de $K[x]$ de degrés inférieurs à un entier N est en $O(N \log N)$. On rappelle que prendre le reste de la division d'un polynôme par x^N revient à tronquer

le polynôme : on ne prend pas cette opération en compte dans le calcul de la complexité algébrique.

Soient $C(n)$ la complexité algébrique de $\text{Inverse}(n, F)$ et $r = \lceil \log n \rceil$ le plus petit entier supérieur ou égal à $\log n$. Montrer que $C(n)$ est en $O(r2^r)$. En déduire que $C(n)$ est en $O(n \log n)$.

Exercice 5 – [DIVISION EUCLIDIENNE RAPIDE]

Soit K un corps. pour tout polynôme $F \in K[x]$, et tout entier k , on note

$$\text{rev}_k(F)(x) = x^k F\left(\frac{1}{x}\right).$$

- 1) Montrer que si $k \geq \deg F$, alors $\text{rev}_k(F) \in K[x]$ et $\text{rev}_k(\text{rev}_k(F)) = F$.
- 2) Soient F et G deux polynômes non nuls de $K[x]$ de degrés respectifs m et n tels que $m \geq n$. Soient Q et R le quotient et le reste de la division euclidienne de F par G . Montrer que

$$\text{rev}_m(F) = \text{rev}_{m-n}(Q)\text{rev}_n(G) + x^{m-n+1}\text{rev}_{n-1}(R).$$

- 3) Montrer que la classe de $\text{rev}_n(G)$ dans $K[x]/(x^{m-n+1})$ est inversible.
- 4) On suppose que les multiplications de polynômes de $K[x]$ de degrés inférieurs à N peuvent se faire en $O(n \log n)$. Déduire de l'exercice 4 un algorithme de complexité quasi-linéaire pour la division euclidienne dans $K[x]$.

Exercice 6 – [RESTES CHINOIS]

- 1) Résoudre dans \mathbb{Z} les systèmes

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

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

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.

- 2) 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 $N \equiv N' \pmod{\frac{ab}{\delta}}$).

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

Exercice 7 – [INTERPOLATION]

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

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

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

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

3) Écrire les contraintes suivantes en termes de congruences.

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

4) Écrire les contraintes suivantes en termes de congruences.

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