Université de Bordeaux
Mathématiques

Algèbre et calcul formel – Master
2025–2026

FEUILLE D'EXERCICES n° 6

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

1) Calculer $\mathrm{pgcd}(312, 793)$ 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: $\mathrm{pgcd}(a, b)$ et u, $v \in \mathbb{Z}$ tels que $au + bv = \mathrm{pgcd}(a, b)$

$u_0 = 1$, $v_0 = 0$, $r_0 = a$
$u_1 = 0$, $v_1 = 1$, $r_1 = b$
$i = 1$ $\{$*initialisation*$\}$
tantque $r_i \neq 0$ **faire**
  Division de r_{i-1} par r_i $\to$ quotient q_i et reste r_{i+1}
  $u_{i+1} = u_{i-1} - q_i u_i$
  $v_{i+1} = v_{i-1} - q_i v_i$
  $i = i + 1$
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 $i > 0$, $|u_i| \leqslant b/r_{i-1}$ et $|v_i| \leqslant a/r_{i-1}$.

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

$A_0 = 1$, $B_0 = 0$, $R_0 = F$
$A_1 = 0$, $B_1 = 1$, $R_1 = G$
$i = 1$ $\quad$ {*initialisations*}
tantque $R_i \neq 0$ **faire**
 Division de R_{i-1} par $R_i \to$ quotient Q et reste R_{i+1}
 $A_{i+1} = A_{i-1} - QA_i$
 $B_{i+1} = B_{i-1} - QB_i$
 $i = i + 1$
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 – [Restes chinois]

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

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

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

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 $\delta = \mathrm{pgcd}(a, b)$, 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 $\dfrac{ab}{\delta}$ (c'est-à-dire, montrer que si N' est une autre solution, alors $N \equiv N' \mod \dfrac{ab}{\delta}$).

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

Exercice 5 – [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.

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