Université Bordeaux 1 **Algèbre et calcul formel – Master**
Mathématiques Année 2012–2013

FEUILLE D'EXERCICES n° 7

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

1) Calculer le pgcd d de 312 et 793, et trouver une relation de Bézout correspondante. Quel est l'ensemble des couples (u, v) tels que $312u + 793v = d$?

2) 73 est-il inversible modulo 119 ? Si oui, calculer son inverse.

Exercice 2 – [ALGORITHME DES RESTES CHINOIS SUR LES ENTIERS]
Résoudre dans $\mathbb{Z}$ les systèmes

$$\begin{cases} 3x + 1 \equiv 0 \bmod 5 \\ 4x + 2 \equiv 1 \bmod 7 \\ x - 1 \equiv 1 \bmod 4 \end{cases} \quad \begin{cases} 12x - 12 \equiv 6 \bmod 33 \\ 7x + 6 \equiv 7 \bmod 13 \\ 6x - 21 \equiv 9 \bmod 54 \end{cases} \quad \begin{cases} 15x \equiv 7 \bmod 25 \\ 8x \equiv 1 \bmod 13 \\ 7x \equiv 4 \bmod 11 \end{cases}$$

$$\begin{cases} x \equiv 5 \bmod 21 \\ x \equiv 3 \bmod 28 \\ x \equiv 1 \bmod 5 \end{cases} \quad \begin{cases} x \equiv 3 \bmod 21 \\ x \equiv 17 \bmod 49 \\ x \equiv 1 \bmod 5 \end{cases}$$

Exercice 3 – [RESTES CHINOIS ET INTERPOLATION]

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

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

2) Déterminer le polynôme P de $\mathbb{F}_7[x]$ de degré inférieur ou égal à 3 tel que

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

Exercice 4 – [EXPONENTIATION VIA FERMAT]
Calculer

$$2^{99960000006} \bmod 187 \quad \text{et} \quad 3^{123500000002} \bmod 385.$$

Exercice 5 – [Approximants de Padé - Applications]
On rappelle ici l'algorithme d'Euclide étendu appliqué à deux polynômes F et $G \in K[X]$ où K est un corp commutatif.

Algorithme 1. 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

---

On rappelle également qu'à chaque étape de l'algorithme, si $n_k =$deg R_k, on a

(1) $A_iF + B_iG = R_i$
(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 $F = f_0 + f_1X + f_2X^2 + \cdots \in K[[X]]$ 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

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

1) En posant $F' = f_0 + \cdots + f_{m+n}X^{m+n}$ 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 $\leqslant n$ 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 :

$$F = f_0 + f_1X + f_2X^2 + \cdots$$

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 qu'on a le problème suivant. On connaît un certains nombre s de termes consécutifs d'une suite (u_n) satisfaisant une relation de récurrence d'ordre k :

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

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

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

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 (nombre d'opérations dans K) 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

$$\left\{\begin{array}{lclcl} u_k & = & a_{k-1}u_{k-1} & + \cdots + & a_0 u_0 \\ u_{k+1} & = & a_{k-1}u_k & + \cdots + & a_0 u_1 \\ & \vdots & & & \\ u_{2k-1} & = & a_{k-1}u_{2k-2} & + \cdots + & a_0 u_{k-1}. \end{array}\right.$$