L3 - Math Info Année **2018-19**
Algorithmique mathématique 1 Université de Bordeaux

TD 2 : Coût, algorithme d'Euclide

Exercice 1. (DS, 11/2016)
On considère le pseudocode suivant :
Entrées : un élément a d'un anneau R et un entier $n \geq 1$.
1. $A = a$, $N = n$, $r = 1$.
2. Tant que $N > 0$:
   - si N est impair on fait $r = r \times A$,
   - $A = A \times A$,
   - $N =$ quotient dans la division euclidienne de N par 2.

Sortie : r.

1. Que calcule cet algorithme en fonction de l'entrée (a, n) ?
2. Déterminer le coût de cet algorithme en nombre d'opérations dans R en fonction de n.

Exercice 2. (DS, 11/2017)
On considère la suite $(h_n)_{n\geq 0}$ définie par $\begin{cases} h_0 = 0\,, \\ h_n = 5h_{n-1} + 3^n\,,\ n \geq 1\,. \end{cases}$

1. On considère la série génératrice $H(X) = \sum_{n\geq 0} h_n X^n$ associée à $(h_n)_{n\geq 0}$. Montrer que
$$H(X) = \frac{3X}{(1-5X)(1-3X)}\,.$$
2. Décomposer la fraction rationnelle $\dfrac{3X}{(1-5X)(1-3X)}$ en éléments simples.
3. Déduire l'expression de h_n en fonction de n pour tout $n \geq 0$.

Exercice 3.
On rappelle la définition de la suite de Fibonacci :
$$F_1 = F_2 = 1\,, \qquad F_{n+2} = F_{n+1} + F_n\,, n \geq 1\,.$$

1. En utilisant la série génératrice $F(X) := \sum_{n\geq 1} F_n X^n$, déterminer l'expression de F_n en fonction de n.
2. On fixe $n \geq 1$. Lorsque l'on applique l'algorithme d'Euclide au couple (a, b) avec $a = F_{n+1}$ et $b = F_n$, quel pgcd d obtient-on ? Quel est le nombre de divisions euclidiennes nécessaires à cet algorithme pour calculer d ?
3. Montrer que si $a > b$ sont des entiers naturels non-nuls tels que la détermination de pgcd(a, b) par l'algorithme d'Euclide nécessite n divisions euclidiennes, alors $b \geq F_{n+1}$. Déduire alors que $n/5$ est inférieur au nombre de décimales de b.

Exercice 4.
1. Calculer le pgcd dans $\mathbb{Q}[x]$ des polynômes
$$f = 2x^4 + 3x^3 - 19x^2 - 28x + 6\,, \qquad g = x^3 + 2x^2 - 9x - 18\,.$$
2. Soit $a = 1275$, $b = 68$. Déterminer le pgcd $d \in \mathbb{N}$ de a et b, et trouver des entiers u et v tels que $d = au + bv$.

Exercice 5. Sans avoir recours à un algorithme de factorisation en produit d'irréductibles, écrire un pseudocode pour une procédure prenant en entrée un polynôme $f \in \mathbb{Q}[X]$ et renvoyant en sortie le produit des polynômes irréductibles divisant f.