Université Paris-Sud
Année universitaire 2015–2016

M1 MFA
MAO Calcul formel

TP 3

Exercice I

On considère l'algorithme suivant, définissant récursivement une fonction f prenant en argument deux entiers naturels non nuls a et b :

(i) Si $a = b$, renvoyer a ;
(ii) Si a et b sont tous les deux pairs, renvoyer $2 \cdot f(\frac{a}{2}, \frac{b}{2})$;
(iii) Si a est pair et b impair, renvoyer $f(\frac{a}{2}, b)$;
(iii') Si b est pair et a impair, renvoyer $f(a, \frac{b}{2})$;
(iv) Si a et b sont impairs, et que $a > b$, renvoyer $f(\frac{a-b}{2}, b)$;
(iv') Si a et b sont impairs, et que $a < b$, renvoyer $f(\frac{b-a}{2}, a)$.

(1) Montrer que le calcul de $f(a, b)$ termine pour tout couple $(a, b) \in (\mathbf{N} - \{0\})^2$.

Pour tout $n \in \mathbf{N}$, notons X_n le sous-ensemble de $(\mathbf{N} - \{0\})^2$ formé des couples d'entiers naturels non nuls (a, b) tels que $ab \leq 2^n$.

(2) Montrer que pour tout $n \in \mathbf{N}$, pour tout $(a, b) \in X_n$, le calcul de $f(a, b)$ nécessite au plus n appels récursifs.

(3) En déduire que le coût de f (en nombre d'appels récursifs) est un $O(\log_2(ab))$. Décrire en outre, pour chaque entier $n \geq 1$, un élément $(a_n, b_n) \in X_n$ tel que le nombre d'étapes de calcul de $f(a_n, b_n)$ soit exactement n.

(4) Montrer que pour tout $(a, b) \in (\mathbf{N} - \{0\})^2$, $f(a, b)$ est le pgcd de a et de b.

(5) Écrire une implémentation de l'algorithme ci-dessus calculant la fonction f dans Sage.

(6) Déterminer le pgcd de 7657 et 4340 *en utilisant cet algorithme.* (On indiquera les résultats intermédiaires.)

Exercice II

On fixe des entiers x_0, x_1, a, b et on considère la suite $(x_n)_{n \geq 0}$ définie par ses deux premières valeurs x_0, x_1 et la relation de récurrence $x_{n+2} = ax_n + bx_{n+1}$ pour tout $n \geq 0$.

(1) Construire une matrice $M \in M_2(\mathbf{Z})$ telle que pour tout $n \geq 0$, on ait :

$$\begin{pmatrix} x_{n+1} \\ x_{n+2} \end{pmatrix} = M \begin{pmatrix} x_n \\ x_{n+1} \end{pmatrix}$$

(2) Montrer que pour tout $n \geq 0$, on a :

$$\begin{pmatrix} x_n \\ x_{n+1} \end{pmatrix} = M^n \begin{pmatrix} x_0 \\ x_1 \end{pmatrix}$$

(3) En déduire un algorithme, étant donné un entier $n \geq 0$, pour calculer x_n. On indiquera les algorithmes fondamentaux qui interviennent.

(4) Donner une estimation en fonction de n du nombre d'opérations arithmétiques dans $\mathbf{Z}$ (additions, multiplications, soustractions).

(5) Implémenter votre algorithme sous la forme d'une fonction prenant en arguments x_0, x_1, a, b, n, c'est-à-dire commençant par :

```
def suite(x0,x1,a,b,n):
    ...
```

On fixe un nombre premier p différent de 2. En conservant les notations précédentes, on définit $(\overline{x_n})_{n\geq 0}$ la suite de $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ formée des classes modulo p des termes de la suite $(x_n)_{n\geq 0}$. On note de même $\overline{a}, \overline{b}$ les classes de a et b modulo p, et $\overline{M}$ l'image de M dans $M_2(\mathbf{F}_p)$. On suppose que $\overline{a} \neq 0$.

(6) Soit $u \in \mathbf{F}_p^2 - \{0\}$ un vecteur non nul du $\mathbf{F}_p$-espace vectoriel $\mathbf{F}_p^2$ de dimension 2. Combien existe-t-il de vecteurs v tels que la famille (u, v) soit liée ? Combien existe-t-il de vecteurs v tels que la famille (u, v) soit une $\mathbf{F}_p$-base de $\mathbf{F}_p^2$.

(7) En déduire le cardinal de $\mathrm{GL}_2(\mathbf{F}_p)$.

On note $N := \#\,\mathrm{GL}_2(\mathbf{F}_p)$ ce cardinal.

(8) Montrer que la suite $(\overline{x_n})_{n\geq 0}$ est N-périodique, c'est-à-dire que $x_{n+N} = x_n$ pour tout $n \geq 0$.

On note $\overline{P} = X^2 - \overline{b}X - \overline{a} \in \mathbf{F}_p[X]$. Dans les questions suivantes, on suppose que $\overline{P} \in \mathbf{F}_p[X]$ est irréductible. On note K le corps de rupture de $\overline{P}$ sur $\mathbf{F}_p$ et on note $\lambda \in K$ la racine priviliégiée de P dans K, c'est-à-dire que l'on pose $K := \mathbf{F}_p[T]/(\overline{P}(T))$ et $\lambda := [T] \in K$.

(9) Montrer que $\lambda^{p^2-1} = 1$.

(10) En déduire que l'on a la congruence de polynômes $X^{p^2-1} \equiv 1 \mod \overline{P}$.

(11) Est-il vrai que $\overline{M}^2 - \overline{b} \cdot \overline{M} - \overline{a} = 0$ dans $M_2(\mathbf{F}_p)$?

(12) Montrer que $\overline{M}^{p^2-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

(13) En déduire que la suite $(\overline{x_n})_{n\geq 0}$ est $p^2 - 1$-périodique.

(14) En déduire une méthode pour calculer $\overline{x_n}$ quand n est grand.

À partir de maintenant, on suppose que $p = 7$, $\overline{a} = \overline{b} = 2$, $x_0 = 0$, $x_1 = 1$.

(15) Déterminer un entier $k \geq 1$ tel que $x_{n+k} = x_n$ pour tout $n \geq 0$.

(16) Calculer $\overline{x_n}$ pour $n = 5^{10000}$.

(17) L'entier k est-il le plus petit entier qui convienne ?