

## Algorithmique Algébrique

### TD4 Exercice 2.

1) Soit  $k \geq 1$ , montrons que l'algorithme d'Euclide appliqué à  $(F_{k+2}, F_{k+1})$  nécessite  $k$  étapes. Notons que pour  $k \geq 2$  la division euclidienne de  $F_{k+2}$  par  $F_{k+1}$  est :

$$F_{k+2} = F_{k+1} + F_k.$$

Cette formule est vraie par définition et  $F_k < F_{k+1}$  donc c'est bien la division euclidienne de  $F_{k+2}$  par  $F_{k+1}$ . Cette formule n'est pas valide pour  $k = 1$  car  $F_{k+1} = F_2 = 1$  et la division euclidienne de  $F_3$  par  $F_2$  est donc  $F_3 = 2 \times F_2 + 0$ .

Montrons le résultat par récurrence :

1. Initialisation : pour  $k = 1$ , on a vu que  $F_3 = 2 \times F_2 + 0$ , ce qui nécessite donc 1 étape.
2. Hérédité : supposons qu'il faille en effet  $k$  étapes pour faire la division euclidienne de  $F_{k+2}$  par  $F_{k+1}$ . L'algorithme d'Euclide appliqué à  $F_{k+3}$  et  $F_{k+2}$  est :

$$\left. \begin{array}{l} F_{k+3} = F_{k+2} + F_{k+1} \\ F_{k+2} = F_{k+1} + F_k \\ \vdots \\ F_4 = F_3 + F_2 \\ F_3 = 2 \times F_2 + 0 \end{array} \right\} k \text{ étapes.}$$

Il y a donc  $k + 1$  étapes.

3. Conclusion : la propriété est vraie pour tout  $k$ .

Remarquons de plus que par ce qui précède, le pgcd de  $F_{k+2}$  et  $F_{k+1}$  est  $F_2 = 1$ .

2) Soient  $a > b > 0$  des entiers, montrons par récurrence sur  $k$  la proposition  $P(k)$  : "si l'algorithme d'Euclide appliqué à  $a$  et  $b$  nécessite  $k$  étapes alors  $a \geq F_{k+2}$ ".

1. Initialisation : pour  $k = 1$ , si il y a une seule étape, elle est de la forme :

$$a = qb + 0$$

or  $qb \geq 2$  car si  $a = qb = 1$  alors  $b = q = 1$  ce qui n'est pas possible puisque  $a > b$ . Donc  $a \geq 2 = F_3$ .

pour  $k = 2$ , il y a deux étapes :

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_2 + 0 \end{aligned}$$

Pour les mêmes raisons que précédemment,  $b \geq 2$  et comme  $r_1 \geq 1$  on a  $a \geq 2 + 1 \geq 3 = F_4$ .

2. Hérédité : Supposons que  $P(k)$  soit vraie pour  $k$  et  $k + 1$ . Supposons qu'il faille  $k + 2$  étapes pour appliquer l'algorithme d'Euclide à  $a$  et  $b$  :

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ r_2 &= q_4 r_3 + r_4 \\ &\vdots \end{aligned}$$

Il faut donc  $k + 1$  étapes pour appliquer l'algorithme à  $b$  et  $r_1$ , par hypothèse de récurrence,  $b \geq F_{k+3}$ . Il faut aussi  $k$  étapes pour appliquer l'algorithme à  $r_1$  et  $r_2$ , par hypothèse de récurrence,  $r_1 \geq F_{k+2}$ . Alors  $a = q_1 b + r_1 \geq F_{k+3} + F_{k+2} = F_{k+4}$ .

3. On conclut par récurrence que la propriété est vraie pour tout  $k \geq 1$ .

**3)** La formule est vraie pour  $n = 1$  car  $F_2 = F_1 = 1$  et  $F_0 = 0$  donc

$$\begin{pmatrix} F_2 & F_1 \\ F_1 & F_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^1.$$

On peut facilement montrer par récurrence que la formule est valable pour tout  $n \geq 1$ , l'hérédité réside dans le fait suivant :

$$\begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} F_{n+1} + F_n & F_{n+1} \\ F_n + F_{n-1} & F_n \end{pmatrix} = \begin{pmatrix} F_{n+2} & F_{n+1} \\ F_{n+1} & F_n \end{pmatrix}$$

**4)** Diagonalisons la matrice suivante :

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

Son polynôme caractéristique est  $X^2 - X - 1$ . Ce polynôme a deux racines :  $\phi$  et  $\phi' = 1 - \phi$ , avec  $\phi = \frac{1+\sqrt{5}}{2}$ . Le polynôme caractéristique est scindé à racine simple donc la matrice est diagonalisable. Les espaces propres sont de dimensions 1, on peut vérifier que  $\begin{pmatrix} \phi \\ 1 \end{pmatrix}$  et  $\begin{pmatrix} 1 - \phi \\ 1 \end{pmatrix}$  sont des vecteurs propres pour les valeurs propres respectives  $\phi$  et  $1 - \phi$ .

Soit  $P$  la matrice  $\begin{pmatrix} \phi & 1 - \phi \\ 1 & 1 \end{pmatrix}$ , on a  $\det(P) = \phi - (1 - \phi) = \sqrt{5}$  et

$$P^{-1} = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & \phi - 1 \\ -1 & \phi \end{pmatrix}$$

On sait que :  $P^{-1} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} P = \begin{pmatrix} \phi & 0 \\ 0 & 1 - \phi \end{pmatrix}$ , on en déduit que :

$$\begin{aligned} \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = P \begin{pmatrix} \phi^n & 0 \\ 0 & (1 - \phi)^n \end{pmatrix} P^{-1} \\ &= \frac{1}{\sqrt{5}} \begin{pmatrix} \phi & 1 - \phi \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \phi^n & 0 \\ 0 & (1 - \phi)^n \end{pmatrix} \begin{pmatrix} 1 & \phi - 1 \\ -1 & \phi \end{pmatrix} \\ &= \frac{1}{\sqrt{5}} \begin{pmatrix} \phi & 1 - \phi \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \phi^n & \phi^{n+1} - \phi^n \\ -(1 - \phi)^n & \phi(1 - \phi)^n \end{pmatrix} \end{aligned}$$

D'où  $F_n = \frac{1}{\sqrt{5}}(\phi^n - (1 - \phi)^n)$ .

5) Si  $k$  est le nombre d'étapes nécessaires pour appliquer l'algorithme à  $a$  et  $b$  alors par les questions précédentes,  $a \geq F_{k+2} = \frac{1}{\sqrt{5}}(\phi^{k+2} - (1 - \phi)^{k+2})$ , en notant  $\epsilon_k = (1 - \phi)^{k+2} \leq 1$  on a :

$$\begin{aligned} a\sqrt{5} + \epsilon_k &\geq \phi^{k+2} \\ \implies \log_2(a\sqrt{5} + \epsilon_k) &\geq (k + 2) \log_2(\phi) \\ \implies k &\leq \frac{\log_2(a\sqrt{5} + \epsilon_k)}{\log_2(\phi)} - 2 \\ \implies k &\leq \frac{1}{\log_2(\phi)} (\log_2(a\sqrt{5} + \epsilon_k) - \log_2(\phi^2)) \\ \implies k &\leq \frac{1}{\log_2(\phi)} \log_2 \left( \frac{a\sqrt{5} + \epsilon_k}{\phi^2} \right) \end{aligned}$$

Or pour tout  $k$ ,  $\epsilon_k \leq (1 - \phi)^2$  car  $(1 - \phi) < 1$  et on peut vérifier numériquement que pour tout  $a \geq 2$ ,  $\frac{a\sqrt{5} + (1 - \phi)^2}{\phi^2} < a$ . Ici  $a \geq 2$ , on obtient alors comme estimation :

$$k < \frac{\log_2(a)}{\log_2(\phi)} \simeq 1.44042 \times \log_2(a).$$

La majoration dans le cours était  $k \leq 2 \log_2(a)$ , celle ci est donc plus intéressante.