Complexité de l'algorithme d'Euclide

Même si la complexité algorithmique est un domaine qui a connu un essor considérable principalement au cours des dernières décennies, il est intéressant d'observer que certains résultats dans ce domaine remontent au milieu du XIX$^\text{e}$ siècle. On doit en effet au mathématicien français Gabriel Lamé (1795–1870) le théorème suivant, paru dans les *Comptes rendus de l'Académie des sciences* en 1844.

Théorème *Le nombre de divisions à effectuer pour trouver le* PGCD *de deux entiers naturels à l'aide de l'algorithme d'Euclide ne dépasse pas cinq fois le nombre de chiffres dans l'écriture décimale du plus petit des deux nombres.*

Mais avant de plonger dans cette démonstration, on peut noter au passage un lien révélateur entre l'algorithme d'Euclide et la célèbre suite des *nombres de Fibonacci* $(1, 1, 2, 3, 5, 8, 13, \ldots)$, définie récursivement par

$$F_1 = F_2 = 1, \quad F_n = F_{n-1} + F_{n-2} \quad \text{pour} \quad n = 3, 4, \ldots$$

En appliquant cet algorithme à deux nombres de Fibonacci consécutifs, F_{n+2} et F_{n+1} avec $n \geq 1$, on obtient :

$$\begin{aligned} F_{n+2} &= 1 \cdot F_{n+1} + F_n \\ F_{n+1} &= 1 \cdot F_n + F_{n-1} \\ &\vdots \\ F_4 &= 1 \cdot F_3 + F_2 \\ F_3 &= 2 \cdot F_2, \end{aligned}$$

montrant ainsi que $\text{PGCD}(F_{n+2}, F_{n+1}) = F_2 = 1$, c'est-à-dire que ces deux nombres sont premiers entre eux. Or le point intéressant, et c'est là le coeur de l'observation de Lamé, [1] est qu'on se trouve ici en présence d'une « longue » suite de divisions euclidiennes, en ce sens que les quotients, sauf le dernier, sont tous égaux à 1. Il s'agit donc en quelque sorte du *pire cas* pour ce qui est de l'efficacité de la procédure d'Euclide et les nombres de Fibonacci serviront pour ainsi dire de « baromètres » dans l'analyse de l'efficacité de cet algorithme. (On aura noté que le calcul a été effectué ici en précisément n étapes, c'est-à-dire qu'il a nécessité n divisions euclidiennes.)

Voici donc la démonstration du théorème de Lamé.

DÉMONSTRATION : Soit deux naturels a et b, avec $a > b$, dont le PGCD r_j a été trouvé

1. Le texte de Lamé ne parle pas de « nombres de Fibonacci », tournure qui n'est devenue l'expression consacrée que plus tard au XIX$^\text{e}$ siècle, sous l'influence d'Édouard Lucas (1842–1891).

via l'algorithme d'Euclide à l'aide de $j+1$ divisions euclidiennes :

$$\begin{array}{rcll} a & = & q_1 \cdot b + r_1 & 0 < r_1 < b \\ b & = & q_2 \cdot r_1 + r_2 & 0 < r_2 < r_1 \\ r_1 & = & q_3 \cdot r_2 + r_3 & 0 < r_3 < r_2 \\ & \vdots & & \\ r_{j-2} & = & q_j \cdot r_{j-1} + r_j & 0 < r_j < r_{j-1} \\ r_{j-1} & = & q_{j+1} \cdot r_j. & \end{array}$$

Observons tout d'abord que tous les nombres intervenant dans ce calcul sont des naturels non nuls. On a donc en particulier que tous les quotients satisfont $q_i \geq 1$. De plus $q_{j+1} > 1$, car sinon on aurait $r_{j-1} = r_j$, ce qui contredirait la dernière condition $0 < r_j < r_{j-1}$.

En remontant la chaîne de divisions euclidiennes, de bas en haut, on trouve alors

$$\begin{array}{rcllcccc} r_j & \geq & 1 & & & = & 1 & = F_2 \\ r_{j-1} & = & q_{j+1} \cdot r_j & \geq & 2 \cdot 1 & = & 2 & = F_3 \\ r_{j-2} & = & q_j \cdot r_{j-1} + r_j & \geq & 1 \cdot 2 + 1 & = & 3 & = F_4 \\ r_{j-3} & = & q_{j-1} \cdot r_{j-2} + r_{j-1} & \geq & 1 \cdot 3 + 2 & = & 5 & = F_5 \\ r_{j-4} & = & q_{j-2} \cdot r_{j-3} + r_{j-2} & \geq & 1 \cdot 5 + 3 & = & 8 & = F_6 \\ & & & \vdots & & & & \\ b & = & q_2 \cdot r_1 + r_2 & \geq & 1 \cdot F_{j+1} + F_j & & & = F_{j+2}. \end{array}$$

Autrement dit, pour qu'il y ait eu $j+1$ divisions dans l'application de l'algorithme euclidien, il faut que

$$b \geq F_{j+2}, \qquad (*)$$

où b est le plus petit des deux nombres dont on cherche le PGCD. (C'est par le biais de cette inégalité que les nombres de Fibonacci jouent ici le rôle de baromètres dont je parlais plus haut.)

Nous proposons maintenant deux façons (en soi essentiellement équivalentes) de conclure la démonstration du théorème de Lamé à partir de cette dernière inégalité.

Variante 1 : Cette première preuve repose sur le résultat préliminaire suivant :

$$F_{n+5} > 10F_n \quad \text{pour} \quad n \geq 2. \qquad (**)$$

On vérifie facilement que cette inégalité est vérifiée pour $n = 2$. Par ailleurs, pour $n \geq 3$, on a

$$\begin{array}{rcl} F_{n+5} & = & F_{n+4} + F_{n+3} \\ & = & 2F_{n+3} + F_{n+2} \\ & = & 3F_{n+2} + 2F_{n+1} \\ & = & 5F_{n+1} + 3F_n \\ & = & 8F_n + 5F_{n-1}. \end{array}$$

De plus, la suite de Fibonacci n'étant pas décroissante, on a $F_n = F_{n-1} + F_{n-2} \leq 2F_{n-1}$, d'où l'on tire $2F_n \leq 4F_{n-1}$. Il s'ensuit alors $F_{n+5} = 8F_n + 5F_{n-1} > 8F_n + 4F_{n-1} \geq 10F_n$, et donc $F_{n+5} > 10F_n$, tel que demandé.

L'inégalité $(**)$ nous dit donc que pour $n \geq 2$, F_{n+5} a au moins un chiffre de plus que F_n dans sa représentation décimale. On peut alors en dégager une borne sur le nombre de chiffres des nombres de Fibonacci, lorsqu'écrits en base dix, en égrenant ceux-ci par tranches de cinq. Partant du fait que pour $2 \leq n \leq 6$, F_n est un nombre à un chiffre, on en tire que

$$\begin{array}{lll} \text{pour} & 5+1 < n \leq 2\cdot 5+1, & F_n \text{ s'écrit avec au moins 2 chiffres} \\ \text{pour} & 2\cdot 5+1 < n \leq 3\cdot 5+1, & F_n \text{ s'écrit avec au moins 3 chiffres} \\ \text{pour} & 3\cdot 5+1 < n \leq 4\cdot 5+1, & F_n \text{ s'écrit avec au moins 4 chiffres} \\ & \vdots & \\ \text{pour} & k\cdot 5+1 < n \leq (k+1)\cdot 5+1, & F_n \text{ s'écrit avec au moins } (k+1) \text{ chiffres.} \end{array}$$

Soit maintenant k, le nombre de chiffres dans le développement décimal de b. On a donc $b < 10^k$, et il faut montrer, pour conclure la preuve du théorème de Lamé, que $j+1 \leq 5k$, où, rappelons-le, $j+1$ est le nombre d'étapes dans l'application de l'algorithme d'Euclide à a et b (avec $a > b$). Supposons au contraire que $j+1 > 5k$. On a donc $j+2 > 5k+1$, d'où il suit, par les considérations précédentes sur le nombre de chiffres des nombres de Fibonacci écrits en base dix, que F_{j+2} s'écrit avec au moins $(k+1)$ chiffres. Or par l'inégalité $(*)$, il en serait de même pour b, ce qui contredit le fait que b a précisément k chiffres dans son écriture décimale. ■

Variante 2 : Voici une autre façon de conclure la démonstration du théorème de Lamé. Elle utilise le fait bien connu que le n^{e} nombre de Fibonacci satisfait l'inégalité

$$F_n \geq \alpha^{n-2}, \qquad (***)$$

où $\alpha = \frac{1+\sqrt{5}}{2}$ désigne le *nombre d'or*, solution de l'équation $\alpha^2 = \alpha + 1$.[2]

Combinant les inégalités $(***)$ et $(*)$, on en tire que $b \geq F_{j+2} \geq \alpha^j$. Comme on s'intéresse au nombre de chiffres décimaux de b, il est naturel de passer au logarithme base dix. On a donc $\log_{10} b \geq j \cdot \log_{10}\alpha$. Or on peut se convaincre facilement du fait[3] que $\log_{10}\alpha > \frac{1}{5}$, de sorte que $\log_{10} b > \frac{j}{5}$.

Soit maintenant k, le nombre de chiffres dans le développement décimal de b. On a alors $b < 10^k$, donc $\log_{10} b < k$. On en conclut que $\frac{j}{5} < k$, donc que $j < 5k$ et enfin, j et k étant des entiers, $j+1 \leq 5k$, ce qu'il fallait démontrer. ■

Le théorème de Lamé affirme donc que l'algorithme d'Euclide appliqué à des entiers a et b ($a > b$) arrête après $O(\log_{10} b)$ divisions euclidiennes. Pas mal efficace, somme toute !

2. L'inégalité $(***)$ se vérifie aisément par récurrence. Elle est immédiatement vraie pour $n = 1$ et 2. Supposant $F_{k-1} \geq \alpha^{k-3}$ et $F_{k-2} \geq \alpha^{k-4}$, on a alors $F_k = F_{k-1} + F_{k-2} \geq \alpha^{k-3} + \alpha^{k-4} = (\alpha+1)\alpha^{k-4} = \alpha^2\alpha^{k-4} = \alpha^{k-2}$.

3. L'inégalité $\log_{10}\alpha > \frac{1}{5}$ peut se vérifier par une simple évaluation numérique, car $\log_{10}\alpha \approx 0{,}208987\cdots$. On peut aussi justifier cette inégalité en bornant $\log_{10}\alpha$ de la manière suivante :

$$\left(\frac{1+\sqrt{5}}{2}\right)^5 = \left(\frac{5+\sqrt{125}}{10}\right)^5 > \left(\frac{5+11}{10}\right)^5 = \frac{16^5}{10^5} = \frac{1024^2}{10^5} > \frac{1000^2}{10^5} = 10.$$

Le résultat suit en prenant le $\log_{10}$ des expressions extrêmes. Je remercie mon collègue Jérémie Rostand de m'avoir proposé cette astucieuse minoration.