PGCD des nombres de Fibonacci et une généralisation

Jean-François Burnol, 23 septembre 2011

Définissons les nombres de Fibonacci par $F_0 = 0$, $F_1 = 1$, $F_2 = 1 + 0 = 1$, $F_3 = 1 + 1 = 2$, et plus généralement $F_{n+1} = F_n + F_{n-1}$. De plus, on définit les F_n pour $n < 0$ afin que la relation de récurrence soit valable pour tous les n, positifs comme négatifs. Ainsi $F_{-1} = 1$, $F_{-2} = -1$, etc…

Suivant la théorie générale on associe à cette récurrence linéaire d'ordre deux la matrice

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

qui a la propriété de donner la solution de $u_{n+1} = u_n + u_{n-1}$, $n \in \mathbb{Z}$, pour toute condition initiale u_0, u_1 par la formule :

$$\begin{pmatrix} u_n \\ u_{n+1} \end{pmatrix} = A^n \begin{pmatrix} u_0 \\ u_1 \end{pmatrix}$$

Les nombres de Fibonacci correspondent à $u_0 = 0$ et $u_1 = 1$ et par conséquent la deuxième colonne de la matrice A^n est $\left(\begin{smallmatrix} F_n \\ F_{n+1} \end{smallmatrix}\right)$. Sa première colonne est obtenue avec $u_0 = 1$ et $u_1 = 0$, or $1 = F_{-1}$ et $0 = F_0$, la solution de la récurrence avec cette condition initiale est $u_n = F_{n-1}$, donc la première colonne de A^n est $\left(\begin{smallmatrix} F_{n-1} \\ F_n \end{smallmatrix}\right)$. Ainsi, comme on peut aussi le deviner en calculant à la main les premières puissances de A, puis le prouver ensuite par récurrence, on a (aussi pour $n < 0$!) :

$$A^n = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix}$$

Nous allons établir purement sur la base de cette identité matricielle la fameuse formule, pour $n, m > 0$:

$$\boxed{\operatorname{pgcd}(F_n, F_m) = F_{\operatorname{pgcd}(n,m)}}$$

Montrons d'abord que F_n est multiple de F_m lorsque n est un multiple (positif ou négatif) km de m. Modulo F_m la matrice A^m est diagonale. Donc $A^n = (A^m)^k$ aussi, et ainsi l'entrée en haut à droite F_n est nulle modulo F_m, on a donc prouvé :

$$m \mid n \implies F_m \mid F_n$$

Par conséquent, en notant en général $d = \text{pgcd}(n, m)$, comme d divise à la fois n et m, cela impose que F_d divise et F_n et F_m donc $F_d \mid \text{pgcd}(F_n, F_m)$.

Il reste à prouver que $D = \text{pgcd}(F_n, F_m)$ divise F_d. Pour cela nous travaillons dans l'anneau $\mathbb{Z}/D\mathbb{Z}$, car modulo D, chacune des deux matrices A^n et A^m est diagonale. Utilisons une identité de Bezout $d = an + bm$, de sorte que $A^d = (A^n)^a(A^m)^b$ est elle aussi modulo D une matrice diagonale,[1] comme produit de matrices diagonales. Donc le nombre entier F_d qui apparaît en dehors de la diagonale dans la matrice A^d est nécessairement nul modulo D.

Et si l'on préfère ne pas travailler avec des matrices modulo D, on peut aussi extraire de $A^d = A^{an}A^{bm}$ l'identité $F_d = F_{an-1}F_{bm} + F_{an}F_{bm+1}$. D'où $D \mid F_d$ puisque $D \mid F_{bm}$ et $D \mid F_{an}$. C'est ce qu'il fallait prouver et nous avons terminé. Il était indispensable d'avoir à disposition les F_k pour $k < 0$!

Une généralisation

Soit maintenant plus généralement une matrice 2×2 à coefficients entiers et déterminant ± 1.

$$B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad a, b, c, d \in \mathbb{Z},\ ad - bc = \pm 1$$

Définissons (aussi pour $n < 0$) :

$$B^n = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix}$$

Par exemple $b_0 = 0$, $b_1 = b$, $b_2 = (a + d)b$, etc... Et $\forall n \in \mathbb{Z} \quad a_n, b_n, c_n, d_n \in \mathbb{Z}$.

Théorème. *La suite* (b_n) *vérifie*

$$\forall (n, m) \neq (0, 0) \qquad \text{pgcd}(b_n, b_m) = |b_{\text{pgcd}(n,m)}|$$

Plus précisément et pour tenir compte des cas possibles $b_n = b_m = 0$, $b_n\mathbb{Z} + b_m\mathbb{Z} = b_{\text{pgcd}(n,m)}\mathbb{Z}$. *De même la suite* (c_n) *vérifie*

$$\forall (n, m) \neq (0, 0) \qquad c_n\mathbb{Z} + c_m\mathbb{Z} = c_{\text{pgcd}(n,m)}\mathbb{Z}$$

1. Notez bien que les puissances négatives de A sont aussi à coefficients entiers, nous avons besoin de cela car dans notre identité de Bezout $d = an + bm$ il y aura en général soit a soit b strictement négatif.

Preuve. La preuve donnée plus haut pour les nombres de Fibonacci fonctionne à l'identique en remplaçant « diagonale » par « triangulaire inférieure » (pour (b_n)), resp. « triangulaire supérieure » (pour (c_n)). Notez bien que l'inverse d'une matrice triangulaire inférieure (resp. supérieure) l'est aussi. Par ailleurs $\operatorname{pgcd}(k, l)$ est > 0 et n'est pas défini lorsque $(k, l) = (0, 0)$. On vérifie que la formulation de l'énoncé fonctionne dans tous les cas. □

Ceci s'applique donc à une suite (x_n) lorsqu'il y a des récurrences croisées $x_{n+1} = ax_n + by_n$, $y_{n+1} = cx_n + dy_n$, et la condition initiale $x_0 = 0$, $y_0 = 1$. Si la condition initiale est $x_0 = 1$, $y_0 = 0$, c'est la suite (y_n) qui vérifiera les formules de pgcd.

D'autres congruences portant sur les entrées des B^n peuvent se déduire des relations fondamentales $B^{n+m} = B^n B^m$, $B^{dn} = (B^d)^n$, je me suis contenté ici du plus simple.

On considère la même situation mais avec maintenant $\delta = \det B$ différent de ± 1 (tout en restant non nul). Les entrées de la matrice B^n seront toujours entières pour $n \geqslant 0$ mais elles ne le seront plus pour $n < 0$.

Le fait que $b_d \mid \operatorname{pgcd}(b_n, b_m)$ avec $d = \operatorname{pgcd}(n, m)$ (ici on fait attention de vraiment se restreindre à $n, m > 0$) se prouve comme avant mais à la fin de la preuve lorsque l'on écrit $B^d = (B^n)^a (B^m)^b$, supposons par exemple $a < 0$, alors $(B^n)^a$ est l'inverse de la matrice $B^{n|a|}$, et

$$\delta^{n|a|} B^d = {}^t\mathrm{comat.}\,(B^{n|a|})\, B^{mb}$$

montre que $\delta^{n|a|} b_d$ est nul modulo $D = \operatorname{pgcd}(b_n, b_m)$.

On n'a donc plus ici le résultat $D = b_d$ mais seulement que D est un multiple de b_d et que le quotient D/b_d divise une puissance de δ :

$$\exists K \geqslant 0 \quad b_{\operatorname{pgcd}(n,m)} \mid \operatorname{pgcd}(b_n, b_m) \mid \delta^K b_{\operatorname{pgcd}(n,m)}$$

Jusqu'à présent nous avons travaillé avec des nombres entiers, mais nous pouvons aussi bien le faire avec un anneau commutatif (unitaire, factoriel). Ainsi et par exemple on a la formule de matrices à coefficients dans $\mathbb{Z}[X]$, facilement prouvée par récurrence :

$$\begin{pmatrix} X & X-1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} X^n & X^n - 1 \\ 0 & 1 \end{pmatrix}$$

Le déterminant est ici $\delta = X$, et on obtient donc de notre résultat général que $\operatorname{pgcd}(X^n - 1, X^m - 1) = (X^{\operatorname{pgcd}(n,m)} - 1)T$ avec T un diviseur d'une puissance

de X. Donc T = 1 car il n'y a pas de diviseur commun non constant à un X^k et un $X^n - 1$ ($n \geqslant 1$). Ce résultat

$$\operatorname{pgcd}(X^n - 1, X^m - 1) = X^{\operatorname{pgcd}(n,m)} - 1$$

est donc ici établi par **quasiment la même méthode** que pour Fibonacci !

> Cette convergence des méthodes apparaît à l'auteur de ces lignes comme particulièrement plaisante. La loi de multiplication des matrices et sa compatibilité à l'arithmétique modulaire à la Gauss fournissent dans les deux cas l'explication sous-jacente à des calculs de pgcd ! Ce n'est pas si surprenant lorsque l'on se rappelle que même l'algorithme d'Euclide est vu avec profit [2] sous la forme de la multiplication de matrices de taille 2×2 !

Construire un exercice

Il est bon de faire faire des calculs concrets aux élèves. Par exemple, 30 et 49 sont premiers entre eux, le professeur calcule chez lui une identité de Bezout, ce qui lui permet d'exhiber une matrice 2×2 de déterminant 1 : [3]

$$M = \begin{pmatrix} 30 & 49 \\ 11 & 18 \end{pmatrix}$$

Il calcule à la main au moins M^2 et M^3, et même plus de puissances s'il (elle) voulait,

$$M^2 = \begin{pmatrix} 1439 & 2352 \\ 528 & 863 \end{pmatrix} \qquad M^3 = \begin{pmatrix} 69042 & 112847 \\ 25333 & 41406 \end{pmatrix}$$

Il (elle) peut alors demander aux élèves d'appliquer l'algorithme d'Euclide au calcul de $\operatorname{pgcd}(112847, 2352)$ car il sait à l'avance, sans faire de calcul, que le résultat sera 49 ! De même $\operatorname{pgcd}(25333, 528) = 11$. Bon j'ai essayé, l'algorithme d'Euclide aboutit d'ailleurs rapidement pour ces exemples. En tout cas, ça marche.

2. `http://jf.burnol.free.fr/agregeuclide_fibo.pdf`

3. On peut aussi, pour construire des matrices de déterminant ± 1, et donc des identités de Bezout, prendre un produit quelconque de matrices de la forme $\left(\begin{smallmatrix} k & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$, etc…