Divisibilité dans la suite de Fibonacci

La suite de Fibonacci est la suite (F_n) définie par $F_0 = 0$, $F_1 = 1$, et la relation de récurrence $F_{n+2} = F_{n+1} + F_n$, pour tout n$\geq$ 0. Elle doit son succès à sa transversalité tous azimuts : elle peut être abordée tant par un enfant attiré par les nombres [1] que par un mathématicien confirmé [2]. Les formules qui la font intervenir, finalement très proches de la trigonométrie [3], émanent d'une puissance qui force le respect de l'ami des sciences formelles, et en même temps, son caractère discret l'oriente vers une arithmétique d'une délicatesse attendrissante. Mais la suite est connue bien au-delà des frontières académiques puisque celle-ci est associée à des images de lapins, d'ananas, et autres choux romanesco. Bref, elle semble encoder les secrets de la nature et porte de ce fait, depuis la haute antiquité, en passant par la renaissance, une magie d'un autre siècle liée à la divine proportion, ses rapports successifs convergeant vers le vénéré nombre d'or.

L'agrégatif ne sera pas en mal de transversalité dans l'étude de ces nombres. La suite de Fibonacci l'aura suivi dans toutes ses études, vu qu'elle peut illustrer divers apprentissages comme celui de l'addition, de la récurrence, des espaces vectoriels (des suites récurrentes linéaires), de l'étude du trinôme (équation caractéristique), des suites géométriques, de la réduction (grâce à la matrice compagnon), et enfin, ses propriétés arithmétiques, liées aux problèmes quadratiques inhérents à la suite, la font batifoler avec le symbole de Legendre et la réciprocité quadratique.

Ici, nous allons regarder la suite sous l'angle de l'arithmétique, c'est-à-dire que nous allons observer ses propriétés pour la divisibilité. Un quizz classique pose la question "quels sont les entiers n tels que F_n est multiple de 10^k ?", et pour ceux qui n'ont pas la fibre décimale ; on en posera une plus générale "quels sont les entiers n tels que F_n est multiple de m, pour un entier m fixé ?". Nous allons voir que les groupes finis de matrices sur un anneau interviennent avec grâce dans ces questions, et amène naturellement à la notion d'ordre d'apparition de m dans une suite récurrente linéaire entière. C'est ensuite le lemme chinois qui sera l'outil fondamental en ramenant le problème dans $\mathbb{Z}/m\mathbb{Z}$ à un problème dans l'anneau, dit local, $\mathbb{Z}/p^k\mathbb{Z}$, où p désigne un nombre premier.

1. Ça existe encore ?
2. Même question
3. On peut comprendre un bon nombre de formules en assimilant les nombres de Fibonacci à une normalisation du sinus et aux nombres de Lucas à celle d'un cosinus.

Exercice 0.1. [Ordre d'apparition dans la suite de Fibonacci]
On considère les matrices suivantes de $\mathcal{M}_2(\mathbb{Z})$:

$$A := \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \; B := -A^2.$$

1. Pour tout entier positif n, expliciter, en fonction de F_n, la matrice $A^n - (-1)^n A^{-n}$, et en déduire qu'un entier $m > 0$ divise F_n si et seulement si n est multiple de l'ordre de $\overline{B}$, réduite de B modulo m dans le groupe fini $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. On notera $\alpha(m)$ cet ordre, que l'on appelle communément *ordre d'apparition de m dans la suite (F_n)*.
2. Montrer que si a divise c, $\alpha(a)$ divise $\alpha(c)$. Montrer ensuite que, si a et b sont premiers entre eux, alors $\alpha(ab)$ est le ppcm de $\alpha(a)$ et $\alpha(b)$.
3. Soit p un nombre premier et $r \geq 1$.
   (a) Montrer que $\alpha(p^{r+1})$ divise $p\alpha(p^r)$ et déduire $\alpha(p^{r+1}) = p\alpha(p^r)$ ou $\alpha(p^r)$.
   (b) Ici, $p > 2$ ou $p = 2$, et dans ce cas $r \geq 2$. On suppose $\alpha(p^{r+1}) = p\alpha(p^r)$. Montrer qu'alors $\alpha(p^{s+1}) = p\alpha(p^s)$ pour tout $s \geq r$.
4. Application : quel est l'ensemble des entiers naturels n tels que F_n termine sur exactement k zéros dans son écriture décimale ?
5. Soit p un nombre premier impair, $p \neq 5$, et G le groupe $\mathbb{F}_p[A]^* \cap \mathrm{SL}_2(\mathbb{F}_p)$, où $\mathbb{F}_p[A]^*$ désigne le groupe multiplicatif des inversibles de $\mathbb{F}_p[A]$.
   (a) Montrer que le déterminant définit un morphisme surjectif de $\mathbb{F}_p[A]^*$ sur $\mathbb{F}_p^*$ de noyau G, et déduire que $\alpha(p)$ divise $p - \left(\frac{5}{p}\right)$.
   (b) Montrer pour finir que $\alpha(p^r)$ divise $p^{r-1}(p-1)$ si $p \equiv \pm 1$ [5], et $p^{r-1}(p+1)$ si $p \equiv \pm 2$ [5].

1. Tout d'abord, on montre par récurrence que $A^n = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix}$, $n \geq 1$. En effet, l'égalité est valable pour $n = 1$, puis, par récurrence par

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

   Comme $\det(A) = -1$, on en déduit

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

   et donc

$$A^n - (-1)^n A^{-n} = \begin{pmatrix} F_{n-1} - F_{n+1} & 2F_n \\ 2F_n & F_{n+1} - F_{n-1} \end{pmatrix} = \begin{pmatrix} -F_n & 2F_n \\ 2F_n & F_n \end{pmatrix}.$$

   On rappelle que $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ est l'ensemble des matrices inversibles de $\mathcal{M}_2(\mathbb{Z}/m\mathbb{Z})$. C'est clairement un groupe pour la multiplication matricielle, et il est fini ! Comme

$\det(B) = (-1)^2 \det(A)^2 = 1$, on a $\det(\overline{B}) = \overline{1}$ modulo m, et donc la transposée de la comatrice ${}^t\mathrm{com}(\overline{B})$ est l'inverse de $\overline{B}$. Donc, $\overline{B} \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

D'après le calcul précédent, m divise F_n si et seulement si $A^n - (-1)^n A^{-n} = 0$ modulo m et donc $\overline{B}^n = \mathrm{Id}$, en multipliant l'égalité par $(-A)^n$. Ceci est vrai si et seulement si n est multiple de l'ordre de $\overline{B}$.

2. On note ici $\overline{B}_m$ la réduction de B modulo m dans $\mathcal{M}_2(\mathbb{Z}/m\mathbb{Z})$. On rappelle que le morphisme (d'anneaux) de réduction $\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z}$ passe au quotient en un morphisme $\mathbb{Z}/c\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z}$, puisque a divise c. On peut donc, par extension, réduire une matrice de $\mathcal{M}_2(\mathbb{Z}/c\mathbb{Z})$ en une matrice de $\mathcal{M}_2(\mathbb{Z}/a\mathbb{Z})$, et construire ainsi un morphisme d'anneaux. Comme $\overline{B}_c^{\alpha(c)} = \mathrm{Id}$, il vient, par réduction, $\overline{B}_a^{\alpha(c)} = \mathrm{Id}$, et donc $\alpha(a)$ divise $\alpha(c)$.

   On va montrer l'égalité $\alpha(ab) = \mathrm{ppcm}\,(\alpha(a), \alpha(b))$ par double divisibilité.

   • $\mathrm{ppcm}\,(\alpha(a), \alpha(b))$ divise $\alpha(ab)$. Cela résulte clairement du fait que $\alpha(a)$ et $\alpha(b)$ divisent $\alpha(ab)$ (par ce qui précède) et de la propriété du ppcm.

   • $\alpha(ab)$ divise $\mathrm{ppcm}\,(\alpha(a), \alpha(b))$. Il suffit de montrer que, si t est un multiple quelconque de $\alpha(a)$ et de $\alpha(b)$, alors $\overline{B}_{ab}^t = \mathrm{Id}$, ce qui impliquera que t est multiple de $\alpha(ab)$. Or, comme t est multiple de $\alpha(a)$, la réduction de $\overline{B}_{ab}^t$ modulo a vaut $\overline{B}_a^t = \mathrm{Id}$, et de même pour la réduction modulo b. Conclusion, tous les coefficients de la matrice $\overline{B}_{ab}^t$ se réduisent en l'identité modulo a et modulo b. Comme a et b sont premiers entre eux, le lemme chinois fournit un isomorphisme, par réduction, entre $\mathbb{Z}/ab\mathbb{Z}$ et $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, ce qui prouve, par unicité, que $\overline{B}_{ab}^t = \mathrm{Id}$.

3. (a) D'après la question 2, $\alpha(p^r)$ divise $\alpha(p^{r+1})$, et donc, si l'on montre que $\alpha(p^{r+1})$ divise $p\alpha(p^r)$, on obtient bien $\alpha(p^{r+1}) = p\alpha(p^r)$ ou $\alpha(p^r)$, puisqu'il n'y a pas de diviseur intermédiaire non trivial entre $\alpha(p^r)$ et $p\alpha(p^r)$.

   On veut donc montrer que $\overline{B}_{p^{r+1}}^{p\alpha(p^r)} = \mathrm{Id}$. Or, par hypothèse, $B^{\alpha(p^r)} = \mathrm{Id} + p^r C$, avec $C \in \mathcal{M}_2(\mathbb{Z})$. En appliquant le binôme de Newton, il vient

$$B^{p\alpha(p^r)} = \mathrm{Id} + p^{r+1} C + \sum_{t=2}^{p} \binom{p}{t} p^{tr} C^t.$$

   Si $t \geq 2$, $tr \geq 2r \geq r+1$, et donc $\overline{B}_{p^{r+1}}^{p\alpha(p^r)} = \mathrm{Id}$, comme désiré.

   (b) Montrons l'assertion par récurrence sur $s \geq r$. Pour $s = r$, c'est juste l'hypothèse. On suppose donc $\alpha(p^{s+1}) = p\alpha(p^s)$, et on veut montrer $\alpha(p^{s+2}) = p\alpha(p^{s+1})$, c'est-à-dire, d'après ce qui précède $\alpha(p^{s+2}) \neq \alpha(p^{s+1})$.

   On a $B^{\alpha(p^s)} = \mathrm{Id} + p^s C$, avec $C \in \mathcal{M}_2(\mathbb{Z})$ et, de plus, $C \notin p\mathcal{M}_2(\mathbb{Z})$, sinon, on aurait $\alpha(p^{s+1}) = \alpha(p^s)$, ce qui est contraire à l'hypothèse de récurrence. Elevons l'égalité à la puissance p, et appliquons le binôme de Newton. Comme $p\alpha(p^s) = \alpha(p^{s+1})$, il vient

$$B^{\alpha(p^{s+1})} = \mathrm{Id} + p^{s+1} C + \sum_{t=2}^{p-1} \binom{p}{t} p^{ts} C^t + p^{ps} C^p.$$

On sait que, p étant premier, il divise $\binom{p}{t}$ pour tout $1 \leq t \leq p-1$, donc la somme $\sum_{t=2}^{p-1} \binom{p}{t} p^{ts} C^t$ est nulle modulo p^{1+ts}, avec $1+ts \geq 1+2s \geq s+2$.

Reste le dernier terme. Si $p > 2$, alors $ps \geq 3s \geq s+2$ et donc le dernier terme est nul modulo p^{s+2}. Si $p = 2$, alors $s \geq r \geq 2$ par hypothèse, et donc $ps = 2s \geq s+2$.

On obtient au final que $B^{\alpha(p^{s+1})} = \mathrm{Id} + p^{s+1}C$ modulo p^{s+2}. Or, $p^{s+1}C$ est non nul modulo p^{s+2}, sinon, C serait dans $p\mathcal{M}_2(\mathbb{Z})$, et on a vu ci-dessus que c'était faux. On a bien prouvé que $B^{\alpha(p^{s+1})}$ est différent de Id modulo p^{s+2}, et donc que $\alpha(p^{s+2}) \neq \alpha(p^{s+1})$.

4. On l'aura compris. Cette petite application n'est là que pour nous rassurer, en demandant de résoudre un problème élégant, qui nous distingue des autres mammifères, et surtout, des toons [4], qui, n'ayant que 8 doigts, sont restés insensibles au système décimal.

   On traduit donc la question en : trouver les entiers naturels n tels que $\alpha(10^k)$ divise n et $\alpha(10^{k+1})$ ne le divise pas.

   Commençons par calculer $\alpha(10^k)$. Par la question 2, il s'agit du ppcm de $\alpha(2^k)$ et $\alpha(5^k)$.

   Les premiers termes de la suite de Fibonacci sont $F_2 = 1$, $F_3 = 2$, $F_4 = 3$, $F_5 = 5$, $F_6 = 8$. Ceci nous donne $\alpha(5) = 5$, et $\alpha(25) = 25$, puisque $\alpha(25) \neq 5$. Pour le plus petit et le plus rebelle [5] des nombres premiers $p = 2$, l'étude est plus retorse : $\alpha(2) = 3$, $\alpha(4) = 6$, $\alpha(8) = 6$, et enfin, $\alpha(16) = 12$, sans calcul supplémentaire, puisque $\alpha(16) \neq 6$.

   On déduit donc, par la question 3, que $\alpha(5^k) = 5^k$, puis que $\alpha(2^k) = 3 \times 2^{k-2}$, pour $k \geq 3$.

   Donc, $\alpha(10) = 15$, $\alpha(100) = 150$ et $\alpha(10^k) = 75 \times 10^{k-2}$ pour $k \geq 3$.

   Par exemple, pour $k \geq 3$, F_n se termine par exactement k zéros dans son écriture décimale si et seulement si n est multiple de $75 \times 10^{k-2}$ sans être multiple de $75 \times 10^{k-1}$, c'est-à-dire $n = 75 \times 10^{k-2} z$, avec $z \notin 10\mathbb{Z}$. Le reste ($k = 1, 2$) est à l'avenant.

5. (a) Tout d'abord, on note que G est bien un groupe multiplicatif comme intersection de deux sous-groupes. Le déterminant définit bien un morphisme de $\mathbb{F}_p[A]^*$ dans $\mathbb{F}_p^*$, de noyau G.

   La surjectivité se fait de façon classique par un dénombrement sur le corps fini $\mathbb{F}_p$. Précisons. Un élément de $\mathbb{F}_p[A]$ s'écrit comme un polynôme $P(A)$ en A, et, quitte à diviser P par le polynôme caractéristique $\chi_A = X^2 - X - 1$ de A, qui annule A comme chacun sait, on peut se ramener au cas où $P := aX + b$, $a, b \in \mathbb{F}_p$, est de degré 1. On a donc

$$P(A) = aA + b = \begin{pmatrix} b & a \\ a & a+b \end{pmatrix}, \det P(A) = b^2 + ab - a^2 = x^2 - 5y^2,$$

   avec $x = b + 2^{-1}a$ et $y = 2^{-1}a$ (on rappelle que p est impair ; 2 est donc inversible modulo p). Soit c dans $\mathbb{F}_p^*$. Comme le changement de variables linéaire

4. Et des Na'vis !
5. 2 est aux nombres premiers ce que Joe est à la fratrie des Dalton.

$(a,b) \mapsto (x,y)$ est bijectif sur $\mathbb{F}_p^2$, il suffit de montrer qu'il existe un couple $(x,y) \in \mathbb{F}_p^2$, tel que $x^2 = 5y^2 + c$. Par [Carnets de Voyage en Algébrie, Exercice 4.2.36], on sait qu'il existe $\frac{p+1}{2}$ carrés dans $\mathbb{F}_p$ (car $p \neq 2$), donc autant de nombres de la forme x^2. Comme 5 est non nul (car $p \neq 5$), $z \mapsto 5z + c$ définit une bijection, et il y a donc $\frac{p+1}{2}$ éléments de la forme $5y^2 + c$. Comme $\frac{p+1}{2} + \frac{p+1}{2} = p + 1 > p$, il existe forcément au moins un élément qui se mette sous la forme x^2 et $5y^2 + c$. Ceci conclut la surjectivité.

Calculons maintenant l'ordre de $\mathbb{F}_p[A]^*$. Cela revient à chercher le nombre de couples (x,y) de $\mathbb{F}_p^2$ tels que $x^2 - 5y^2 \neq 0$. Deux cas s'imposent.

• 5 n'est pas un carré modulo p, *i.e.* $\left(\frac{5}{p}\right) = -1$. Dans ce cas, $x^2 - 5y^2 = 0$ est impossible dès que x (et donc) y sont inversibles. La seule possibilité est alors $(x,y) = (0,0)$. On en déduit que $|\mathbb{F}_p[A]^*| = p^2 - 1$, et donc, par surjectivité,

$$|G| = |\mathrm{Ker}\det| = \frac{p^2-1}{|\mathrm{Im}\det|} = \frac{p^2-1}{p-1} = p+1.$$

• 5 est un carré modulo p, *i.e.* $\left(\frac{5}{p}\right) = 1$. Dans ce cas, $x^2 - 5y^2 = 0$ implique $(x-\delta y)(x+\delta y) = 0$. Il faut donc retirer à $\mathbb{F}_p^2$ l'union de deux droites vectorielles distinctes (qui ont donc un seul point en commun, le vecteur nul). On en déduit que $|\mathbb{F}_p[A]^*| = p^2 - (p+p-1) = (p-1)^2$, et donc, par surjectivité,

$$|G| = |\mathrm{Ker}\det| = \frac{(p-1)^2}{|\mathrm{Im}\det|} = \frac{(p-1)^2}{p-1} = p-1.$$

On obtient bien le résultat annoncé.

(b) Tout d'abord, la loi de réciprocité quadratique implique $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$; et il est clair que p est un carré modulo 5, resp. non carré modulo 5, si et seulement si $p = \pm 1$, resp. $p = \pm 2$, modulo 5.

De plus, comme $\overline{B}_p \in G$, l'ordre de B divise celui de G par Lagrange. Donc $\alpha(p)$ divise $p-1$, resp. $p+1$. Puis, par la question 3, on déduit que $\alpha(p^r)$ divise $p^{r-1}(p-1)$, resp. $p^{r-1}(p+1)$.

Remarque 0.2. Au final, on a montré que si $m = \prod_i p_i^{k_i}$, alors pour tout n multiple de $\pi(m) := \prod_i p_i^{k_i-1}\mathrm{ppcm_i}(p_i - \epsilon(p_i))$, avec $\epsilon(p_i) = \left(\frac{p_i}{5}\right)$, alors $B^{\pi(m)} = \mathrm{Id}$ modulo m, et donc F_n est multiple de m. Il semble difficile de faire mieux que ce majorant. En utilisant l'égalité $B = -A^2$, on voit que si l'on pose $\pi'(m) = 4\pi(m)$ si $\pi(m)$ est impair et $2\pi(m)$ si $\pi(m)$ est pair, alors $A^{\pi'(m)} = \mathrm{Id}$ modulo m. Ceci prouve que toute suite récurrente sur $\mathbb{Z}$ dont la récurrence est donnée par $u_{n+2} = u_{n+1} + u_n$ est périodique modulo m et que la période divise $\pi'(m)$. Dans le même ordre d'idée, on peut montrer que toute suite récurrente $\mathbb{Z}$-linéaire d'ordre 2 est périodique modulo m à partir d'un certain rang [6], avec une période qui divise l'ordre de $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

6. Le temps de se débarrasser des termes nilpotents dans les puissances de la matrice compagnon.

Remarque 0.3. On a élagué la solution de grandes généralités afin de rendre la lecture plus digeste, mais il serait dommage de ne pas dégager les principes généraux derrière la preuve. Le problème de récurrence linéaire modulo m nous amène naturellement à travailler dans un groupe de type $\mathrm{GL}_d(\mathbb{Z}/m\mathbb{Z})$. Dans un premier temps, c'est le lemme chinois qui nous permet de se ramener à une étude sur des anneaux plus simples : si $m = \prod_i p_i^{k_i}$ est la décomposition de m en facteurs premiers, on a un isomorphisme naturel (par réduction modulaire) de groupes $\mathrm{GL}_d(\mathbb{Z}/m\mathbb{Z}) \simeq \prod_i \mathrm{GL}_d(\mathbb{Z}/p_i^{k_i}\mathbb{Z})$. Les anneaux $\mathbb{Z}/p_i^{k_i}$ possèdent la jolie propriété d'être locaux, c'est-à-dire qu'ils n'ont qu'un unique idéal maximal [7] M_i, engendré ici par p^{k_i-1}. Le sous-groupe $\mathrm{Id} + \mathcal{M}_d(M_i)$ de $\mathrm{GL}_d(\mathbb{Z}/p_i^{k_i}\mathbb{Z})$ est distingué : c'est le noyau du morphisme surjectif naturel (par réduction modulaire) $\mathrm{GL}_d(\mathbb{Z}/p_i^{k_i}\mathbb{Z}) \to \mathrm{GL}_d(\mathbb{Z}/p_i\mathbb{Z})$, nous rapportant à un groupe mieux compris, nommément $\mathrm{GL}_d(\mathbb{Z}/p_i\mathbb{Z})$.

Pour finir, signalons une conjecture de Wall sur laquelle les arithméticiens se sont cassé les dents depuis cinquante ans, qui stipule que $\alpha(p) \neq \alpha(p^2)$ pour tout p impair, ce qui impliquerait donc $\alpha(p^k) = p^{k-1}\alpha(p)$.

7. Un seul idéal maximal pour un anneau local contre zéro pour un corps. Ceci implique que l'anneau local est l'anneau le plus proche du corps. Cet adage est précisé par le lemme de Nakayama.