Une machine à fabriquer des premiers

PAR PATRICK TELLER

Définition 1. *L'application f*

On note f l'application qui à tout entier x>1 associe la somme de ses diviseurs strictement supérieurs à 1; ainsi f(5)=5, f(6)=11, etc...il est immédiat que x premier <=>f(x)=x.

(traditionnellement on désigne par σ(x) la somme des diviseurs de l'entier x, et ainsi f(t)=$\sigma(t)$-1)

On notera $f^{\circ n}$ la composée n fois de f par f; ainsi $f^{\circ 3}(12)=f^{\circ 2}(39)=f(55)=67$.

Pour tout entier x>1 on considérera le système dynamique associé $\left\{ \begin{array}{l} u_0=x \\ \forall n\in\mathbb{N}, u_{n+1}=f(u_n) \end{array} \right.$.

J'ai pu vérifier empiriquement jusqu'à $x=2000000$ que, quel que soit x, la suite ainsi construite atteint « en un temps fini » (sic !) un point fixe, c'est à dire un nombre premier; des étudiants de l'EFREI ont fait la même constatation jusqu'à x=300000000; d'où la conjecture:

$\forall x\in\mathbb{N}\backslash\{0,1\}, \exists p\in\mathbb{N}$, $f^{\circ p}$(x) est premier, ou, ce qui revient au même, $\forall x\in\mathbb{N}\backslash\{0,1\}, \exists p\in\mathbb{N}$, $f^{\circ p}$(x)=$f^{\circ(p+1)}$(x).

1 Exemples

```
Maxima 5.37.2 http://maxima.sourceforge.net
using Lisp GNU Common Lisp (GCL) GCL 2.6.12
Distributed under the GNU Public License. See the file COPYING.
Dedicated to the memory of William Schelter.
The function bug_report() provides bug reporting information.
(%i1) conject(a,n):=block([b,k,L],b:a,L:[],for k:1 thru n do (if primep(b)=false
      then (b:divsum(b)-1,L:endcons(factor(b),L))),return(L))$
(%i2) conject(45,12);
```

(%o2) $[7\,11, 5\,19, 7\,17, 11\,13, 167]$

```
(%i3) conject(1234567,100);
```

(%o3) $[3\,5\,23\,3607, 2078207]$

```
(%i4) conject(701823,100);
```

(%o4) $[7\,37\,3613, 5\,219731, 19\,69389, 7\,198257, 19\,83477, 29\,57571, 7\,137\,1801, 7\,284201, 5\,454723, 19\,37\,3881, 41\,227\,317, 59\,51613, 17\,182167, 11\,298093, 41\,43\,2029, 61\,89\,691, 883\,4373, 5\,53\,14591, 7\,43\,113\,139, 1031\,5449, 11\,17\,19\,1583, 59\,115981, 11\,632629, 31\,244889, 7\,701\,1597, 41\,218887, 5\,1838659, 269\,41011, 17\,41\,15887, 61\,196907, 5\,11^2\,17\,1187, 47\,67\,5419, 163\,108533, 5^2\,711983, 241\,91583, 151\,146777, 5\,11\,405641, 47\,109\,5701, 7\,4300937, 13\,439\,6029, 743\,49993, 5\,13\,572239, 2293\,20963, 5\,43\,223681, 59052047]$

```
(%i5)
```

On remarquera que le processus est souvent très rapide, le record en nombre d'itérations (pour les entiers inférieurs à 1000000) est atteint pour $u_0=701823$ qui exige 46 itérations pour atteindre le nombre premier 59052047.

Remarque 2.

La conjecture a reçu des « preuves » heuristiques, tant sur le site Mathoverflow que par courriers personnels ; ces « preuves » sont probabilistes, ce qui s'explique par la difficulté du problème qui mêle des aspects multiplicatifs et additifs (Courrier de Michel Mendes-France).

L'ouvrage Unsolved Problems in Number Theory [1] précise que Erdös s'est intéressé à la fonction f et à ses itérations sans aboutir; c'est la raison pour laquelle au lieu de considérer explicitement la relation $u_{n+1} = f(u_n)$ nous ne retiendrons que la caractéristique suivante:

$1 < u_n < u_{n+1} \leqslant e^{\gamma} u_n \mathrm{Ln}(\mathrm{Ln}(u_n))$

Nous établirons que, sous cette seule condition, la probabilité qu'il existe n tel que u_n est premier est égale à 1.

2 Un sous-produit du Théorème des nombres premiers

N'ayant trouvé nulle part d'expression utilisable de la probabilité qu'un entier soit premier:

Proposition 3. *La probabilité qu'un entier z>1 soit premier*

Il existe un réel A tel que, quel que soit $z \in \mathbb{N}^* \setminus \{1\}$, *la probabilité que z soit premier est supérieure ou égale à* $\frac{A}{\mathrm{Ln}(z)}$.

Démonstration.

Nous poserons que, si (z,p) sont deux entiers quelconques la probabilité que $z \equiv 0[p]$ *est* $\frac{1}{p}$, *d'où la probabilité que p ne divise pas z est* $1 - \frac{1}{p}$.

La probabilité que z soit premier est donc $\prod_{p\,\mathrm{premier}, p \leqslant \sqrt{z}} \left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma}}{\mathrm{Ln}(\sqrt{z})} \left(1 + O\left(\frac{1}{\mathrm{Ln}(\sqrt{z})}\right)\right)$*(3ème Théorème de Mertens) [3].*

D'où il existe un réel A tel que la probabilité que pour tout z>1 z soit premier est supérieure ou égale à $\frac{A}{\mathrm{Ln}(z)}$.

□

3 La suite des itérés

Théorème 4.

Soit un entier $u_0 > 1$ *et la suite définie par la relation* $\forall n, u_{n+1} = f(u_n)$, *la probabilité qu'il existe n tel que* u_n *est premier est égale à 1.*

Démonstration.

On considère l'entier u_0 et la suite (éventuellement finie) définie par la relation $\forall n, u_n \notin \mathcal{P} \Longrightarrow u_{n+1} = f(u_n)$.

Nous savons que, si $u_{k-1} \notin \mathcal{P}$, on calcule u_k et alors, d'après la proposition 3, P(u_{k} non premier/(u_{k-1}nonpremier) $\leqslant$ 1-A/Ln(u_k).

Alors la probabilité que $u_1, \ldots., u_n$ ne soient pas premiers est inférieure ou égale à $\prod_{k=1\ldots n} (1 - A/\mathrm{Ln}(u_k))$.

Pour établir le Théorème nous allons montrer que la probabilité qu'aucun u_n ne soit premier est nulle.

Rappelons le Théorème de Robin: $\forall n > 1, \sigma(n) < e^{\gamma} n \mathrm{Ln}(\mathrm{Ln}(n))$ [2].

Soit donc une suite d'entiers (u_n) telle que $\forall n \in \mathbb{N}, 1 < u_n < u_{n+1} \leqslant e^{\gamma} u_n \mathrm{Ln}(\mathrm{Ln}(u_n))$.

La suite $(\prod_{k=1\ldots n} (1 - A/\mathrm{Ln}(u_k)))$ tend vers 0 si et seulement la série (à termes positifs pour k assez grand) de terme général $\sum \frac{A}{\mathrm{Ln}(u_k)}$ diverge.

On a donc $\forall k \in \mathbb{N}$, $\mathrm{Ln}(u_k) < \mathrm{Ln}(\mathrm{u}_{k+1}) \leqslant \gamma + \mathrm{Ln}(u_k) + \mathrm{Ln}(\mathrm{Ln}(\mathrm{Ln}(u_k)))$, par suite $\frac{1}{\mathrm{Ln}(u_{k+1})} \geqslant \frac{1}{\mathrm{Ln}(u_k)} \times \frac{1}{1+\gamma/\mathrm{Ln}(u_k)+\mathrm{Ln}(\mathrm{Ln}(\mathrm{Ln}(u_k)))/\mathrm{Ln}(u_k)}$.

Posons $\mathrm{t}_k = 1/\mathrm{Ln}(\mathrm{u}_k)$, on a donc $\mathrm{t}_{k+1} \geqslant \mathrm{t}_\mathrm{k} \times \frac{1}{1+\gamma t_k + \mathrm{Ln}(\mathrm{Ln}(1/t_k))t_k}$.

Par la suite nous ne préciserons plus que les séries condidérées sont à termes positifs.

On en déduit d'abord $0 \leqslant \mathrm{Ln}(1/\mathrm{t}_{k+1})$-$\mathrm{Ln}(1/\mathrm{t}_k) \leqslant \mathrm{Ln}(1+\gamma t_k + \mathrm{Ln}(\mathrm{Ln}(1/t_k))t_k)$; or la série de tg $\mathrm{Ln}(1/\mathrm{t}_{k+1})$-$\mathrm{Ln}(1/\mathrm{t}_k)$ est divergente donc la série de tg $\mathrm{Ln}(1+\gamma t_k + \mathrm{Ln}(\mathrm{Ln}(1/t_k))t_k)$ aussi.

Remarquons que (t_k) et $(\mathrm{Ln}(\mathrm{Ln}(1/t_k))t_k)$ tendent vers 0 et $(t_k) = \mathrm{o}(\mathrm{Ln}(\mathrm{Ln}(1/t_k))t_k)$, d'où $\mathrm{Ln}(1+\gamma t_k + \mathrm{Ln}(\mathrm{Ln}(1/t_k))t_k) \sim \gamma t_k + \mathrm{Ln}(\mathrm{Ln}(1/t_k))t_k \sim \mathrm{Ln}(\mathrm{Ln}(1/t_k))t_k$ d'où la divergence de la série de tg $\mathrm{Ln}(\mathrm{Ln}(1/t_k))t_k$.

On peut aussi comparer $\mathrm{Ln}(1+\gamma t_k + \mathrm{Ln}(\mathrm{Ln}(1/t_k))t_k) \leqslant \gamma t_k + \mathrm{Ln}(\mathrm{Ln}(1/t_k))t_k \leqslant 2\mathrm{Ln}(\mathrm{Ln}(1/t_k))t_k$

De ce qui précède on déduit par sommation des relations de comparaison $\mathrm{Ln}(1/\mathrm{t}_n) < \mathrm{Ln}(1/t_{n+1}) = O(\sum_{k=1}^n \mathrm{Ln}(\mathrm{Ln}(1/t_k))t_k)$. (*)

Appliquons la transformation d'Abel pour obtenir $\sum_{k=1}^n \mathrm{Ln}(\mathrm{Ln}(1/t_k))t_k = \mathrm{Ln}(\mathrm{Ln}(1/t_n))\sum_{k=1}^n t_k - \sum_{k=1}^{n-1}\left\{\mathrm{Ln}\left(\frac{\mathrm{Ln}(1/t_{k+1})}{\mathrm{Ln}(1/t_k)}\right)\sum_{i=1}^k t_i\right\}$.

Or $\mathrm{t}_{k+1} < \mathrm{t}_k < 1$ d'où $\sum_{k=1}^{n-1}\left\{\mathrm{Ln}\left(\frac{\mathrm{Ln}(1/t_{k+1})}{\mathrm{Ln}(1/t_k)}\right)\sum_{i=1}^k t_i\right\} > 0$ d'où on déduit de (*) la relation

$\mathrm{Ln}(1/t_n) = O(\mathrm{Ln}(\mathrm{Ln}(1/t_n))\sum_{k=1}^n t_k)$, qui, compte tenu de la négligeabilité de $\mathrm{Ln}(x)$ devant x en $+\infty$, impose la divergence de la série de tg t_k.

D'où $\sum \frac{A}{\mathrm{Ln}(u_k)} = +\infty$ d'où $\prod_{k=1\ldots n}(1 - A/\mathrm{Ln}(u_k))$ tend vers 0.

$\square$

Ce qui constitue un preuve probabiliste complète de la conjecture et, en même temps, la mise en évidence que le fait d'atteindre nécessairement un premier n'est pas lié spécifiquement à la fonction f mais plutôt aux inégalités $\forall n \in \mathbb{N}, 1 < u_n < u_{n+1} \leqslant e^\gamma u_n \mathrm{Ln}(\mathrm{Ln}(u_n))$; on en déduit que si on remplaçait f(x) par g(x)=$\sigma(x) + a$ la probabilité d'atteindre un premier sera aussi égale à 1; cependant le caractère probabiliste du résultat n'interdit pas les cas particuliers:

si on pose $g(x) = \sigma(x) + 1$ et $u_k = 2^{k'}$ la suite obtenue à partir du rang k sera $(2^{n-k+k'})$ qui ne compte aucun nombre premier.

De nombreux essais suggèrent qu 'il s'agit du seul cas particulier pour g(x)=$\sigma(x)$+1; c'est à dire soit une orbite sans premiers incluse à partir d'un certain rang dans la suite des puissances de 2, soit une orbite qui atteint « en un rang fini » un entier premier.

Bibliographie:

[1] Richard K.Guy, Unsolved Problems in Number Theory, Problem Books in Mathematics Springer, 2000; spécialement pp. 149.

[2] *Robin Guy (1984), "Grandes valeurs de la fonction somme des diviseurs et hypothèse de Riemann", Journal de Mathématiques Pures et Appliquées, Neuvième Série, **63** (2): 187–213, ISSN 0021-7824, MR 0774171*

[3] https://fr.wikipedia.org/wiki/Theoreme_deMertens

Nimes-Paris septembre 2018