Une machine à fabriquer des premiers

Patrick Teller

Résumé.

La fonction σ qui associe à tout entier la somme de ses diviseurs est bien connue; nous désignerons par f la fonction définie par $f(t)=\sigma(t)-1$, dont les points fixes sont les premiers.

Ainsi f(5)=5, f(6)=11.

L'expérience suggère que, quel que soit l'entier $x>1$, si on considère la suite récurrente définie par $\begin{cases} u_0=x \\ \forall n\in\mathbb{N}, u_{n+1}=f(u_n) \end{cases}$ il existe un rang n_0 tel que $f(u_{n_0+1})=f(u_{n_0})$.

La conjecture a été soumise sur le site Mathoverflow en septembre 2014 et on peut trouver cette suite sur le site OEIS sous le numéro A039654.

Devant la difficulté à démontrer ce résultat nous en proposons une démonstration probabiliste.

1. Exemples

J'ai pu vérifier empiriquement jusqu'à $x=2000000$ que, quel que soit x, la suite ainsi construite atteint 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).

Ci-dessous quelques exemples sous Maxima.

```
Maxima 5.41.0 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.
```

```
(%i5) conject(a,n):=block([b,k,L],b:a,L:[[a,0]],for k:1 thru n do (if
      primep(b)=false then (b:divsum(b)-1,L:endcons([factor(b),k],L))),
      return(L))$
(%i6) conject(8192,100);
```

(%o6) [[8192, 0], [2 8191, 1], [5^2 983, 2], [11 47 59, 3], [7 4937, 4], [39503, 5]]

```
(%i7) conject(701823,100);
```

(%o7) [[701823, 0], [7 37 3613, 1], [5 219731, 2], [19 69389, 3], [7 198257, 4], [19 83477, 5], [29 57571, 6], [7 137 1801, 7], [7 284201, 8], [5 454723, 9], [19 37 3881, 10], [41 227 317, 11], [59 51613, 12], [17 182167, 13], [11 298093, 14], [41 43 2029, 15], [61 89 691, 16], [883 4373, 17], [5 53 14591, 18], [7 43 113 139, 19], [1031 5449, 20], [11 17 19 1583, 21], [59 115981, 22], [11 632629, 23], [31 244889, 24], [7 701 1597, 25], [41 218887, 26], [5 1838659, 27], [269 41011, 28], [17 41 15887, 29], [61 196907, 30], [5 11^2 17 1187, 31], [47 67 5419, 32], [163 108533, 33], [5^2 711983, 34], [241 91583, 35], [151 146777, 36], [5 11 405641, 37], [47 109 5701, 38], [7 4300937, 39], [13 439 6029, 40], [743 49993, 41], [5 13 572239, 42], [2293 20963, 43], [5 43 223681, 44], [59052047, 45]]

```
(%i20) conject(1000000000,100);
```

(%o20) [[1000000000, 0], [41 727 83791, 1], [47 54511153, 2], [19 101 1363489, 3], [277 10041587, 4], [53 52670971, 5], [113 25170199, 6], [37 1613 48079, 7], [13 17 79 168901, 8], [29 47 2498213, 9], [13 53 5221231, 10], [32341 122051, 11], [271 523 27851, 12], [5 19 37 883 1279, 13], [7 737104457, 14], [1429 1931 2137, 15], [101 58482979, 16], [19 313961261, 17], [7 23^2 47 109 331, 18], [7755095039, 19]]

```
(%i21)
```

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 45 itérations pour atteindre le nombre premier 59052047.

Remarque 1.

On sait que, si $x = \prod_{i=1}^{r} p_i^{n_i}$, $\sigma(x) = \prod_{i=1}^{r} (\sum_{j=0}^{n_i+1} p_i^j)$ et $f(x) = \prod_{i=1}^{r} (\sum_{j=0}^{n_i+1} p_i^j) - 1$.

Cette expression, qui mêle aspects multiplicatifs et additifs, rend le problème difficile (courrier de Michel Mendes-France).

On sait que Paul Erdös s'est intéressé à la fonction f et à ses itérations mais le seul article où il en est fait mention n'apporte aucune information [1].

La conjecture a reçu des « preuves » heuristiques, tant sur le site Mathoverflow que par courriers personnels ; ces « preuves » sont toutes d'esprit probabiliste.

Devant la difficulté à exprimer les propriétés de l'entier $u_{n+1} = f(u_n)$ en fonction de u_n nous nous ne retiendrons que la caractéristique suivante: $u_n \leqslant u_{n+1} \leqslant e^{\gamma} u_n \mathrm{Ln}(\mathrm{Ln}(u_n))$ [2] et l'hypothèse d'indépendance des variables aléatoires 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 2. *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* $1 - \frac{1}{p}$.

Conséquence du Théorème Chinois la probabilité que z soit premier est égale à $\prod_{p \text{ premier}, p \leqslant \sqrt{z}} \left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma}}{\mathrm{Ln}(\sqrt{z})} \left(1 + O\left(\frac{1}{\mathrm{Ln}(\sqrt{z})}\right)\right)$ *(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. Une suite contrainte d'entiers naturels peut-elle ne pas contenir de premiers ?

Définition 3. *Une suite contrainte d'entiers naturels*

Une suite (u_n) *d'entiers naturels sera dite « contrainte » si* $u_0 > 1$ *et pour tout n* u_{n+1} *suit une loi uniforme sur l'intervalle* $[\![u_n + 1, e^{\gamma} u_n \mathrm{Ln}(\mathrm{Ln}(u_n))]\!]$ *et les* u_n *sont indépendantes.*

Théorème 4.

Soit une suite contrainte d'entiers naturels la probabilité que, quel que soit n, u_n *ne soit pas premier est nulle.*

Démonstration.

D'après la proposition 2, $\mathrm{P}(u_k \text{ non premier}) \leqslant 1\text{-}A/\mathrm{Ln}(u_k)$, par suite la probabilité que $u_1, \ldots.$, u_n ne soient pas premiers est inférieure ou égale à $\prod_{k=1\ldots n} (1 - A/\mathrm{Ln}(u_k))$.

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 $\frac{A}{\mathrm{Ln}(u_k)}$ diverge.

De l'hypothèse sur la suite (u_n) on déduit $\forall k \in \mathbb{N}$, $\mathrm{Ln}(u_k) < \mathrm{Ln}(u_{k+1}) \leqslant \gamma + \mathrm{Ln}(u_k) + \mathrm{Ln}(\mathrm{Ln}(\mathrm{Ln}(u_k)))$, 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 t_k=1/Ln(u_k), (t_k) tend vers 0 et on a $t_{k+1} \geqslant t_k \times \frac{1}{1+\gamma t_k + \mathrm{Ln}(\mathrm{Ln}(1/t_k))t_k}$.

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

On en déduit d'abord $0 \leqslant \mathrm{Ln}(1/t_{k+1}) - \mathrm{Ln}(1/t_k) \leqslant \mathrm{Ln}(1 + \gamma t_k + \mathrm{Ln}(\mathrm{Ln}(1/t_k))t_k)$; or la suite $(\mathrm{Ln}(1/t_k))$ tend vers $+\infty$, d'où la série de tg $\mathrm{Ln}(1/t_{k+1}) - \mathrm{Ln}(1/t_k)$ 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 $(t_k) = o(\mathrm{Ln}(\mathrm{Ln}(1/t_k))t_k)$, 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 $\mathrm{Ln}(\mathrm{Ln}(1/t_k))t_k$.

Par ailleurs $\mathrm{Ln}(1+\gamma t_k + \mathrm{Ln}(\mathrm{Ln}(1/t_k))t_k) \leqslant \gamma t_k + \mathrm{Ln}(\mathrm{Ln}(1/t_k))t_k = O(\mathrm{Ln}(\mathrm{Ln}(1/t_k))t_k)$.

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

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

Or $t_{k+1} < t_k < 1$ 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.

Par suite la probabilité qu'aucun des termes de la suite ne soit premier est nulle.

□

Théorème 5.

Soit f l'application qui à tout entier x>1 associe la somme de ses diviseurs strictement supérieurs à 1; pour tout entier x>1 on considère le système dynamique $\begin{cases} u_0 = x \\ \forall n \in \mathbb{N}, u_{n+1} = f(u_n) \end{cases}$.

La probabilité que la suite (u_n) soit stationnaire est égale à 1.

Démonstration.

Soit $\sigma(x)$ la somme des diviseurs de x, le Théorème de Robin donne la majoration $\sigma(x) < e^{\gamma} x \mathrm{Ln}(\mathrm{Ln}(x))$ [2]; d'où $\forall n \in \mathbb{N}, 1 < u_n \leqslant u_{n+1} \leqslant e^{\gamma} u_n \mathrm{Ln}(\mathrm{Ln}(u_n))$.

Si on suppose que la suite ne contient pas de premier alors $\forall n \in \mathbb{N}, 1 < u_n < u_{n+1} \leqslant e^{\gamma} u_n \mathrm{Ln}(\mathrm{Ln}(u_n))$ et le Théorème précédent nous dit que la probabilité en est nulle. □

4. Commentaires

Ceci constitue un preuve probabiliste complète de la conjecture.

Il y a un certain paradoxe entre la beauté de la conjecture (quel que soit x>1 la suite (u_n) atteint un point fixe) et la généralité de l'hypothèse utilisée ($\forall n \in \mathbb{N}, 1 < u_n \leqslant u_{n+1} \leqslant e^{\gamma} u_n \mathrm{Ln}(\mathrm{Ln}(u_n))$*).

Par ailleurs

Le résultat ne dépendant que des inégalités *, il s'en suit que si on remplaçait $f(t) = \sigma(t) - 1$ par $f(t) = \sigma(t) + 1$, ou même $\sigma(t) + a$ (quitte à remplacer γ par une autre constante) , la probabilité d'atteindre un premier serait aussi égale à 1.

Cependant le caractère probabiliste du résultat n'interdit pas les cas particuliers:

par exemple, si on pose $f(t) = \sigma(t) + 1$ 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 $f(t) = \sigma(t) + 1$; c'est à dire que le système dynamique associé possède 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.

Remarquons aussi que si on remplace l'hypothèse « $\forall n \in \mathbb{N}, 1 < u_n \leqslant u_{n+1} \leqslant e^{\gamma} u_n \mathrm{Ln}(\mathrm{Ln}(u_n))$ » par « $\forall n \in \mathbb{N}, 1 < u_n \leqslant u_{n+1} \leqslant \mathrm{Ku}_n \mathrm{Ln}(u_n)$ », moins contraignante, la conclusion reste la même.

5. Un souhait

Ce procédé pourrait permettre de trouver de nouveaux nombres premiers qui ne seraient pas des nombres de Mersenne; sa lourdeur réside dans la nécessité de factoriser à chaque itération.

Bibliographie:

[1] Paul **Erdos**, Andrew **Granville**, Carl **Pomerance** and Claudia **Spiro**, On the normal behavior of the iterates of some arithmetic functions, Analytic number theory, Birkhäuser Boston, 1990, pp. 165-204.

[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] G.Tenenbaum, M.Mendes France, Les Nombres premiers, Que sais-je ?, P.U.F., 1997;pp.32-40.