Projet de Mathématiques
L3NEW - Semestre de Mobilité
2019-2020

Autour d'une conjecture

Enseignants référents : Federico Zalamea[1] et Patrick Teller[2]

1. Rappel de la conjecture PT

La fonction σ qui associe à tout entier la somme de ses diviseurs est bien connue ; nous désignons par f la fonction définie sur $\mathbb{N}^*$ par $f(t) = \sigma(t) - 1$, dont les points fixes sont les nombres premiers. Par exemple, on a

$$f(2) = 2,\ \ f(3) = 3,\ \ f(4) = 6,\ \ f(5) = 5,\ \ f(6) = 11,\ \ f(7) = 7.$$

L'expérience suggère que, quel que soit l'entier $x > 1$, si l'on considère la suite 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 $f(u_{n_0}) = u_{n_0}$.

Autrement dit, quel que soit l'entier à partir duquel la suite démarre, on arrive toujours en un temps fini à un nombre premier.

2. Les premiers sauvages

On conviendra des notations suivantes : si u_0 est le premier terme d'une telle suite de premier terme et si n_0 est le premier indice tel que u_{n_0} est un nombre premier, alors on dira que u_{n_0} est "*l'image première*" de u_0, ce que l'on notera $\mathcal{P}(u_0) = u_{n_0}$. Inversement, on dira que et que u_0 est "*un ancêtre*" de u_{n_0}.

Dans le tableau ci-dessous, nous donnons quelques exemples en fonction de la valeur du premier terme de la suite. Nous arrêtons d'écrire la suite dès qu'elle atteint un nombre premier :

u_0	u_1	u_2	u_3	u_4	u_5
2	...		...		...
3	...		...		...
4	6	11	...		...
5	...		...		...
6	11		...		...
7	...		...		...
8	14	23	...		...
9	12	27	39	55	71
10	17		...		...
11	...		...		...
12	71		...		...

[1]federico.zalamea@efrei.fr
[2]teller@free.fr

5 est premier et n'admet que 5 comme ancêtre. Par contre, 71 admet plusieurs ancêtres parmi lesquels 9 et 12 (et aussi 39, 55, ...).

On dira qu'un nombre premier est "*sauvage*" s'il n'admet aucun ancêtre à part lui-même. Le projet a pour but la constitution d'une liste des nombres premiers sauvages aussi longue que possible (idéalement jusqu'à $10^{2}0$).

3. Les outils

A chaque itération, il est nécessaire de factoriser en facteurs premiers. La méthode banale est trop lente, c'est pourquoi il sera exigé que la factorisation emploie au moins deux des trois méthodes suivantes :

- ♣ Algorithme rho de Pollard (voir une première description ici),
- ♣ Algorithme p-1 de Pollard (voir une première description ici),
- ♣ Factorisation de Lenstra par les courbes elliptiques (description ici).

4. Le projet

D'abord, vous fournirez le test de la conjecture PT le plus long possible (idéalement jusqu'à $10^{2}0$).

Ensuite, vous fournirez la liste la plus longue possible de premiers sauvages, avec les codes que vous avez utilisé pour faire les calculs et toutes les explications nécessaires.

Enfin, vous êtes encouragés à décrire le plus en détail possible le temps que prennent ces calculs : trouver la borne supérieure du nombre d'itérations nécessaires pour atteindre l'image première, le nombre moyen d'opérations nécessaires, etc.

5. Bibliographie

- P. Zimmermann, *The elliptic curve method*, téléchargeable ici.
- A.S. Charest, *Pollard's p-1 and Lenstra's factoring algorithms*, téléchargeable ici.
- S. Wagstaff, *The Joy of Factoring*, AMS, 2014.