Le test de Lucas

Daniel PERRIN

1 Énoncé

Voici le théorème de Lucas-Lehmer (voir [3] et [1]) :

1.1 Théorème. *Soit p un nombre premier impair et M_p (ou M) le nombre de Mersenne $2^p - 1$. On considère la suite L_n définie par récurrence par $L_0 = 4$ et $L_{n+1} = L_n^2 - 2$. Alors M est premier si et seulement si L_{p-2} est multiple de M.*

1.2 Commentaire. Ce test est d'une efficacité extraordinaire pour déterminer si un nombre de Mersenne est premier ou non. Il est très facile d'écrire un programme dans ce but. En voici un sur *xcas* :

```
Lucas(p):={
local n,M, u;
u:=4;
M:=2^p-1;
pour n de 1 jusque p-2 faire
u:=irem(u^2-2,M);
fpour
si u==0 alors Disp "premier"
sinon Disp "pas premier"
fsi
}:;
```

Avec ce programme, *xcas* montre que $2^{44497} - 1$ est premier en moins de 95 secondes. C'est tout de même un nombre de 13395 chiffres. C'est avec ce test que l'actuel record du plus grand nombre premier (connu !) a été battu en décembre 2017. Il s'agit de $M_{77232917}$ qui a plus de 23 millions de chiffres.

2 La suite (L_n)

2.1 Son origine

La suite mystérieuse (L_n) est issue d'une suite récurrente double ordinaire : $u_{n+1} = 4u_n - u_{n-1}$, avec les valeurs initiales $u_0 = 2$ et $u_1 = 4$. Dans les articles originaux de Lucas (1878), voir [2] et [3], il étudie systématiquement la divisibilité des termes de ce type de suite par des nombres premiers.

On sait calculer les termes d'une telle suite : on introduit l'équation caractéristique $X^2 - 4X + 1 = 0$ dont les racines sont $\alpha = 2 + \sqrt{3}$ et

$\beta = \alpha^{-1} = 2 - \sqrt{3}$. On a alors $u_n = \alpha^n + \beta^n$. La suite (L_n) n'est autre que la sous-suite de (u_n) formée des termes d'indice une puissance de 2 :

2.1 Proposition. *1) Pour tout $n \geq 0$ on a la formule :*

$$L_n = (2+\sqrt{3})^{2^n} + (2-\sqrt{3})^{2^n}.$$

2) En particulier, on a $L_{p-2} = (2-\sqrt{3})^{2^{p-2}}\left[(2+\sqrt{3})^{2^{p-1}} + 1\right]$.

Démonstration. C'est immédiat par récurrence, le point crucial est la remarque $(2+\sqrt{3})(2-\sqrt{3}) = 1$.

2.2 *Remarque.* Cette formule vaut dans tout anneau commutatif contenant $\sqrt{3}$ (c'est-à-dire un élément de carré 3). On notera qu'un tel anneau contient aussi les entiers $n = 1 + 1 + \cdots + 1$ (n fois), ces entiers pouvant être nuls si la caractéristique est positive.

3 Démonstration du théorème

3.1 Rappels sur Frobenius

Soit q un nombre premier et $\mathbf{F}_q = \mathbf{Z}/q\mathbf{Z}$ le corps à q éléments. Rappelons que dans tout anneau A contenant $\mathbf{F}_q$, donc de caractéristique q, on a l'application de Frobenius $F : x \mapsto x^q$ dont on rappelle les propriétés :

1) C'est un homomorphisme d'anneaux de A, en particulier on a $(xy)^q = x^q y^q$, ce qui est banal, et $(x+y)^q = x^q + y^q$, ce qui l'est moins.

2) Si A est un corps fini F est un isomorphisme.

3) L'homomorphisme F fixe les éléments de $\mathbf{F}_q$ et, réciproquement, si A est un corps, les points fixes de F sont exactement les éléments de $\mathbf{F}_q$.

3.2 Le sens direct

On suppose que $M = 2^p - 1$ est premier.

3.2.1 Les carrés

On a un premier lemme :

3.1 Lemme. *Soit p un nombre premier impair et $M = 2^p - 1$. On suppose M premier. Alors, 3 n'est pas un carré modulo M.*

Démonstration. On peut évidemment montrer ce lemme en utilisant la loi de réciprocité quadratique. La preuve ci-dessous évite le recours à ce théorème et n'utilise que les notions élémentaires sur les carrés d'un corps fini qu'on peut trouver dans [4]. Comme M est congru à -1 modulo 4, -1 n'est pas un carré de $\mathbf{F}_M$. Dire que 3 n'est pas un carré est alors équivalent à dire que -3 en est un. Mais ceci revient à dire que la racine cubique de l'unité $j = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$ est dans $\mathbf{F}_M$, ou encore que 3 divise $M - 1 = 2(2^{p-1} - 1)$ donc que $2^{p-1} \equiv 1 \pmod 3$. Comme on a $2 \equiv -1 \pmod 3$ et que $p - 1$ est pair, c'est bien vrai.

3.2 *Remarque.* En revanche, 2 est un carré dans $\mathbf{F}_M$. En effet, comme $M = 2^p - 1$, on a $2 = 2^{p+1}$ et 2 est le carré de $2^{(p+1)/2}$. On peut aussi, si l'on est plus savant, utiliser le fait que 2 est un carré car M est congru à -1 modulo 8, voir [5].

3.2.2 Le corps $\mathbf{F}_{M^2}$

Comme 3 n'est pas un carré de $\mathbf{F}_M$, le polynôme X^2-3 est irréductible sur $\mathbf{F}_M$ et on considère son corps de rupture $\mathbf{F}_M[X]/(X^2-3)$ qui n'est autre que le corps $\mathbf{F}_{M^2}$. Dans ce corps, on choisit une racine de 3, par exemple l'image de X, qu'on note $\sqrt{3}$, et les éléments de $\mathbf{F}_{M^2}$ sont de la forme $a + b\sqrt{3}$ avec $a, b \in \mathbf{F}_M$. On commence par un lemme :

3.3 Lemme. *L'automorphisme de Frobenius $F : x \mapsto x^M$ de $\mathbf{F}_{M^2}$ n'est autre que la conjugaison : $(a + b\sqrt{3})^M = a - b\sqrt{3}$.*

Démonstration. En effet, il suffit de montrer qu'on a $F(\sqrt{3}) = -\sqrt{3}$ car F fixe les éléments de $\mathbf{F}_M$. Posons $x = \sqrt{3}$. On a $x^2 = 3 \in \mathbf{F}_M$ donc $F(x)^2 = F(x^2) = F(3) = 3$. Comme $\mathbf{F}_{M^2}$ est un corps, on a donc $F(x) = \sqrt{3}$ ou $F(x) = -\sqrt{3}$ mais le premier cas est impossible car $\sqrt{3}$ n'est pas dans $\mathbf{F}_M$ en vertu de 3.1.

3.2.3 Le lemme crucial

Vu le point 2) de 2.1, il suffit de prouver le lemme suivant :

3.4 Lemme. *On suppose que M est premier. On a $(2 + \sqrt{3})^{2^{p-1}} = -1$ dans $\mathbf{F}_{M^2}$.*

Démonstration. Expliquons l'idée de la preuve. Ce qu'on sait bien calculer dans $\mathbf{F}_{M^2}$ ce sont les puissances M-ièmes avec $M = 2^p-1$. On s'en approchera donc si $\alpha = 2 + \sqrt{3}$ est un carré car on aura alors à calculer la puissance

2^p-ième de α. On montre que c'est bien le cas en cherchant une racine carrée de $2+\sqrt{3}$ dans $\mathbf{F}_{M^2}$ sous la forme $\rho = a + b\sqrt{3}$. On a $b = \frac{1}{2a}$ et on en déduit que a vérifie $4a^4 - 8a^2 + 3 = 0$, d'où, par exemple, $a^2 = 1/2$ (2 est un carré dans $\mathbf{F}_M$ par 3.2). Une racine de $\alpha = 2+\sqrt{3}$ est donc $\rho = \dfrac{1}{\sqrt{2}}(1+\sqrt{3})$.

On peut maintenant calculer :

$$(2+\sqrt{3})^{2^{p-1}} = \alpha^{2^{p-1}} = \rho^{2^p} = (\frac{1}{\sqrt{2}})^{M+1} \times (1+\sqrt{3})^{M+1}.$$

Mais, comme $x = \sqrt{2}$ est dans $\mathbf{F}_M$ on a $x^M = x$, donc le premier terme donne $\frac{1}{2}$. On a aussi $(1+\sqrt{3})^M = 1 + (\sqrt{3})^M = 1 - \sqrt{3}$ par la remarque 3.3. En définitive, on a $(2+\sqrt{3})^{2^{p-1}} = -\frac{2}{2} = -1$ comme annoncé.

3.3 Le sens réciproque

On suppose que L_{p-2} est multiple de M. Supposons que $M = 2^p - 1$ n'est pas premier et soit q son plus petit facteur premier, de sorte qu'on a $q^2 \leq M$. On considère l'anneau $A = (\mathbf{Z}/q\mathbf{Z})(\sqrt{3})$, c'est-à-dire $(\mathbf{Z}/q\mathbf{Z})[X]/(X^2-3)$, $\sqrt{3}$ désignant l'image [1] de X. L'anneau A est de cardinal q^2 et les éléments $\alpha = 2+\sqrt{3}$ et $\beta = 2-\sqrt{3}$ sont inversibles dans A à cause de la formule $\alpha\beta = 1$.

On a $L_{p-2} = (2-\sqrt{3})^{2^{p-2}}\left[(2+\sqrt{3})^{2^{p-1}} + 1\right]$ et cet élément est nul dans A (car q divise M). Comme $2-\sqrt{3}$ y est inversible, on a $(2+\sqrt{3})^{2^{p-1}} = -1$ dans A, de sorte que $2+\sqrt{3}$ est d'ordre 2^p dans le groupe multiplicatif de A. Mais, ce groupe est de cardinal $\leq q^2 - 1 < M = 2^p - 1 < 2^p$: c'est absurde !

Références

[1] Lehmer D.H., *An extended Theory of Lucas' functions*, Annals of Mathematics, Vol. 31, N° 3 (1930), p. 419-448.

[2] Lucas Édouard *Théorie des fonctions numériques simplement périodiques* American Journal of Mathematics, Vol. 1, N° 2 (1878), p. 184-196.

[3] Lucas Édouard *Théorie des fonctions numériques simplement périodiques* American Journal of Mathematics, Vol. 1, N° 4 (1878), p. 289-321.

[4] Perrin Daniel, *Cours d'algèbre*, Ellipses, 1996.

[5] Serre Jean-Pierre, *Cours d'arithmétique*, PUF, 1970.

1. On ne sait pas si 3 est un carré modulo q, mais peu importe.