

## Nombres de Mersenne premiers : test de Lucas Lehmer

d'après Mikael I. Rosen (1988) et John W. Bruce (1993)

Soit  $(a_n)_{n \geq 0}$  une suite de réels telle que  $\forall n \geq 0 \ a_{n+1} = a_n^2$ , avec  $a_0 \neq 0$ . Alors  $\forall n \geq 0 \ a_n = a_0^{2^n} \neq 0$ .

Soit  $S_n = a_n^{-1} + a_n$ . Alors  $\forall n \geq 0 \ S_{n+1} = S_n^2 - 2$  et  $S_n = a_0^{-2^n} + a_0^{2^n}$ .

Pour  $a_0 = 2 + \sqrt{3}$ , tel que  $a_0^{-1} = 2 - \sqrt{3}$ , on obtient la suite de Lucas  $(S_n)_{n \geq 0}$ , suite d'entiers définie par  $S_0 = 4$  et  $\forall n \geq 0 \ S_{n+1} = S_n^2 - 2$ . On a  $\forall n \geq 0 \ S_n = (2 + \sqrt{3})^{-2^n} + (2 - \sqrt{3})^{2^n}$ .

Soit  $M_p = 2^p - 1$  le nombre de Mersenne associé à  $p = 1 + 2n$  ( $n \in \mathbf{N}^*$ ). Le test de Lucas-Lehmer s'énonce

$$M_p \text{ premier} \iff S_{p-2} \equiv 0 \pmod{M_p}$$

Comme  $M_p$  premier  $\Rightarrow p$  premier (évident), on supposera  $p$  premier impair.

### Préliminaire :

Soit  $q$  un nombre premier. Soit  $A = \mathbf{Z} + \mathbf{Z}\sqrt{3}$  le sous anneau de  $\mathbf{R}$  engendré par 1 et  $\sqrt{3}$ . Soit  $B = A/qA$ .  $B$  est un anneau de caractéristique  $q$  car  $\sqrt{3}$  irrationnel. On note  $\alpha$  la classe dans  $B$  de  $\sqrt{3}$ ,  $\omega$  celle de  $2 + \sqrt{3}$  et  $s_n$  celle de  $S_n$ , et pour tout  $k \in \mathbf{Z}$  on note encore  $k$  sa classe dans  $B$  de sorte que, pour tout  $(k, \ell) \in \mathbf{Z}$ ,  $k \equiv \ell \pmod{q}$  équivaut à l'égalité  $k = \ell$  dans  $B$ . Les éléments  $k$  de  $B$  qui correspondent à  $k \in \mathbf{Z}$  forment un sous-corps de  $B$  isomorphe à  $\mathbf{F}_q = \mathbf{Z}/q\mathbf{Z}$ .  $B$  est ainsi une  $\mathbf{F}_q$ -algèbre ayant  $(1, \alpha)$  pour base. En particulier :

(1)  $\text{card } B = q^2$

On a par la surjection canonique  $A \rightarrow B$  (morphisme d'anneaux)

$$\omega = 2 + \alpha, \quad \omega \in B^* \text{ avec } \omega^{-1} = 2 - \alpha, \text{ et } s_n = \omega^{-2^n} + \omega^{2^n}$$

et on observe que :

(2)  $\omega = \frac{(1+\alpha)^2}{2}$

(3)  $(1 + \alpha)^q = 1 + \alpha^q$  (car  $x \rightarrow x^q$  est un endomorphisme de l'anneau  $B$  : endomorphisme de Frobenius)

(4)  $S_{p-2} \equiv 0 \pmod{q} \iff s_{p-2} = 0 \iff \omega^{-2^{p-2}} + \omega^{2^{p-2}} = 0 \iff 1 + \omega^{2^{p-1}} = 0 \iff \omega^{2^{p-1}} = -1$

### Preuve de $\implies$ :

Supposons  $M_p$  premier. Soit  $q = M_p$ . Alors  $2^{p-1} = \frac{q+1}{2}$ . D'après (4) il s'agit de vérifier que  $\omega^{\frac{q+1}{2}} = -1$ .

D'après la loi de réciprocité quadratique rappelée plus loin,  $2^{\frac{q-1}{2}} \equiv 1 \pmod{q}$  et  $3^{\frac{q-1}{2}} \equiv -1 \pmod{q}$ , i.e. dans  $B$

(5)  $2^{\frac{q-1}{2}} = 1$  et  $3^{\frac{q-1}{2}} = -1$

À partir de (2), (3) et (5),  $\omega^{\frac{(q+1)}{2}} = \frac{(1+\alpha)^{q+1}}{2^{\frac{q+1}{2}}} = \frac{(1+\alpha^q)(1+\alpha)}{2} = \frac{(1+3^{\frac{q-1}{2}}\alpha)(1+\alpha)}{2} = \frac{(1-\alpha)(1+\alpha)}{2} = -1$ .

On obtient donc bien  $S_{p-2} \equiv 0 \pmod{q}$

### Preuve de $\impliedby$ :

Supposons  $M_p$  non premier : soit  $q$  un facteur premier de  $M_p$  tel que  $q^2 \leq M_p$ , i.e.  $\text{card } B \leq M_p$  d'après (1).

Par hypothèse,  $S_{p-2}$  est multiple de  $M_p$  donc de  $q$  :  $S_{p-2} \equiv 0 \pmod{q}$ . Donc d'après (4)  $\omega^{2^{p-1}} = -1$  puis, en élevant au carré,  $\omega^{2^p} = 1$ . Donc le sous-groupe  $G_\omega$  de  $B^*$  engendré par  $\omega$  a pour cardinal  $2^p$  (car pour  $k \in \mathbf{Z}$ ,  $\omega^k = 1 \iff \text{card } G_\omega \mid k$ ). Donc, puisque  $0 \notin B^*$ ,  $2^p < \text{card } B \leq M_p = 2^p - 1$  (contradiction).

### Loi de réciprocité quadratique :

On définit, pour tout  $q$  premier et tout  $a \in \mathbf{Z} \setminus q\mathbf{Z}$ ,  $\left(\frac{a}{q}\right) = \pm 1 \in \mathbf{Z}$  par  $\left(\frac{a}{q}\right) = 1 \iff \exists b \in \mathbf{Z} \ a \equiv b^2 \pmod{q}$

Alors, pour tous nombres premiers impair  $b$  et  $q$  et tout  $a \in \mathbf{Z} \setminus q\mathbf{Z}$ ,  $\left(\frac{b}{q}\right) = (-1)^{\frac{(b-1)(q-1)}{4}} \left(\frac{q}{b}\right)$  et  $\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}$

et  $a^{\frac{q-1}{2}} \equiv \left(\frac{a}{q}\right) \pmod{q}$

On obtient (5) pour  $b = 3$ ,  $q = M_p = 2^{1+2n} - 1$  et  $a = 2$  ou  $3$  :

$$\frac{q-1}{2} = 2^{2n} - 1 \text{ est impair}$$

$$\frac{q^2-1}{8} = \frac{q+1}{4} \frac{q-1}{2} = 2^{2n-1}(2^{2n} - 1) \text{ est pair. Donc } \left(\frac{2}{q}\right) = 1. \text{ Donc } 2^{\frac{q-1}{2}} \equiv 1 \pmod{q}$$

$$3^{\frac{q-1}{2}} \equiv (-1)^{\frac{(3-1)(q-1)}{4}} \left(\frac{q}{3}\right) = (-1)^{\frac{q-1}{2}} \left(\frac{q}{3}\right) = -\left(\frac{q}{3}\right) \pmod{q}.$$

Or  $q = 2^{1+2n} - 1 \equiv (-1)^{1+2n} - 1 = -2 \equiv 1 \pmod{3}$ . Donc  $\left(\frac{q}{3}\right) = 1$ . Donc  $3^{\frac{q-1}{2}} \equiv -1 \pmod{q}$ .