# Primalité des nombres de Mersenne : test de Lucas

Gilles Auriol
auriolg@free.fr — http://auriolg.free.fr

**Théorème.** — Soit $(y_k)$ la suite définie par $y_0 = 2$ et $y_{k+1} = 2y_k^2 - 1$ pour $k \geqslant 0$. Alors pour tout $k \geqslant 3$, l'entier $2^k - 1$ est premier si et seulement s'il divise $y_{k-2}$.

**Preuve.** — 1) Dans la première partie de la preuve, on fixe $p \geqslant 5$ un nombre premier. On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et $M_2(\mathbb{Z})$ (resp. $M_2(\mathbb{F}_p)$) les matrices carrées de taille $2 \times 2$ oefficients dans $\mathbb{Z}$ (resp. $\mathbb{F}_p$). Soit

$$M = \begin{pmatrix} 4 & 1 \\ -1 & 0 \end{pmatrix} \in M_2(\mathbb{Z}) \quad \text{et} \quad M_p = \begin{pmatrix} 4 & 1 \\ -1 & 0 \end{pmatrix} \in M_2(\mathbb{F}_p).$$

Le polynôme minimal de $M_p$ est $X^2 - 4X + 1$, donc la $\mathbb{F}_p$-algèbre $K_p = \mathbb{F}_p[M_p]$ engendrée par $M_p$ dans $M_2(\mathbb{F}_p)$ est de dimension 2 et commutative. En désignant par $I_2$ la matrice identité, on a

$$K_p = \{aM_p + bI_2,\ (a,b) \in \mathbb{F}_p^2\}.$$

Soit $B_p = \{A \in K_p,\ \det A = 1\}$ et montrons que c'est un groupe multiplicatif. Le seul point qui n'est pas immédiat est le fait que si $A$ est une matrice inversible de $K_p$, alors son inverse est encore dans $K_p$. En écrivant que le polynôme caractéristique de $A$ annule $A$ et que son terme constant est non nul (c'est $\det A$), on exprime $A^{-1}$ comme un polynôme en $A$, d'où $A^{-1} \in K_p$.

2) Montrons par récurrence que $2y_k = \mathrm{Tr}(M^{2^k})$. Pour $k = 0$ c'est clair, et l'hérédité provient de la formule $\mathrm{Tr}(A^2) = (\mathrm{Tr}(A))^2 - 2\det(A)$ qui montre alors que

$$2y_{k+1} = 4y_k^2 - 2 = (2y_k)^2 - 2 = (\mathrm{Tr}(M^{2^k}))^2 - 2\det(M^{2^k}) = \mathrm{Tr}(M^{2^{k+1}}).$$

3) Montrons maintenant le résultat suivant (où les fractions désignent le symbole de Legendre)

- si $\left(\dfrac{3}{p}\right) = -1$, alors $K_p$ est un corps commutatif et $|B_p| = p + 1$ ;
- si $\left(\dfrac{3}{p}\right) = 1$, alors $|B_p| = p - 1$.

Posons $C_{a,b} = aM_p + bI_2$ pour $a, b \in \mathbb{F}_p$. On a $\det C_{a,b} = a^2 + 4ab + b^2$.
Si $a = 0$, alors $\det C_{a,b} = 0 \iff b = 0$.
Si $a \neq 0$, alors $\det C_{a,b} = 0 \iff (b + 2a)^2 = 3a^2 \iff (ba^{-1} + 2)^2 = 3$.
Ceci conduit iscuter selon que 3 est ou non résidu quadratique modulo $p$. Supposons qu'on ait $\left(\dfrac{3}{p}\right) = -1$, alors $\det C_{a,b} = 0 \iff a = b = 0$, donc $K_p$ est un corps. Considérons le morphisme de groupe multiplicatif $\det : K_p^* \longrightarrow \mathbb{F}_p^*$. Son noyau est $B_p$, de plus $|K_p^*| = p^2 - 1$ et $|\mathbb{F}_p^*| = p - 1$. Le théorème d'isomorphisme donne $K^*/B_p \simeq \mathrm{Im}(\det)$, d'où l'on déduit que $p+1$ divise $|B_p|$. Mais d'autre part, étant donné $a \in \mathbb{F}_p$, il existe au plus deux valeurs de $b \in \mathbb{F}_p$ telles que $\det(C_{a,b}) = 1$, donc $|B_p| \leqslant 2p$ (et bien sûr $|B_p| \geqslant 1$), d'où l'égalité $|B_p| = p + 1$.

Supposons résent $\left(\dfrac{3}{p}\right) = 1$. Alors en désignant par $\mu$ une racine carrée de 3, le polynôme caractéristique de $M_p$ est $(X - 2 - \mu)(X - 2 + \mu)$, dont les racines sont distinces (car $p \geqslant 5$). Ainsi il existe une matrice $P$ inversible telle que pour tout $(a,b) \in \mathbb{F}_p^2$

$$C_{a,b} = P \begin{pmatrix} a(2+\mu) + b & 0 \\ 0 & a(2-\mu) + b \end{pmatrix} P^{-1}.$$

Réciproquement, étant donné $(\alpha, \beta) \in \mathbb{F}_p^2$, il existe un unique couple $(a, b) \in \mathbb{F}_p^2$ tel que $(a(2+\mu)+b, a(2-\mu)+b) = (\alpha, \beta)$. Ainsi l'application $(\alpha, \beta) \longmapsto P \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} P^{-1}$ est une bijection de $\mathbb{F}_p^2$ dans $K_p$ et il y autant d'éléments dans $B_p$ que de couples $(\alpha, \beta) \in \mathbb{F}_p^2$ tels que $\alpha\beta = 1$. Ainsi $|B_p| = p - 1$.

4) Passons a preuve du théorème proprement dite. Soit $p$ un nombre premier de la forme $2^k - 1$, où $k \geqslant 3$. Remarquons que $k$ est impair, sinon ou pourrait écrire $p = (2^{k'} - 1)(2^{k'} + 1)$ avec $k' = k/2 \geqslant 2$, contredisant $p$ premier. Par conséquent $2^k - 1 \equiv (-1)^k - 1 \equiv 1 \bmod 3$ et la loi de réciprocité quadratique montre que

$$\left(\frac{3}{p}\right) = (-1)^{\frac{3-1}{2}\frac{2^k-2}{2}} \left(\frac{p}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

Donc $K_p$ est un corps commutatif, et $B_p$ en est un sous-groupe multiplicatif de cardinal $2^k$ dont les éléments sont les racines du polynôme $X^{2^k} - I_2$ (en effet ce polynôme a au plus $2^k$ racines, donc exactement $2^k$ racines d'après le théorème de Lagrange appliqué au groupe $B_p$).

Montrons que $M_p$ est d'ordre $2^k$. Il suffit pour cela de montrer que $M_p^{2^{k-1}} \neq I_2$. Soit $\lambda = 2^{\frac{k+1}{2}}$. On a $\lambda^2 = 2^{k+1} = 2(2^k - 1) + 2 \equiv 2 \bmod p$. En posant $X = \lambda^{-1}(M_p - I_2)$, on constate que $X^2 = M_p$. Supposons alors que $M_p^{2^{k-1}} = I_2$, on aurait donc

$$X^{2^k} = (X^2)^{2^{k-1}} = M_p^{2^{k-1}} = I_2,$$

d'où $X \in B_p$, ce qui est absurde car $\det X = \lambda^{-2} \det(M_p - I_2) = 2^{-1}(-2) = -1$.

Soit $S = M_p^{2^{k-2}}$. Par ce qui précède, $S$ est d'ordre 4, donc $S^4 - I_2 = 0$, d'où l'on déduit $S^2 + I_2 = 0$ (car $S$ n'est pas d'ordre 2 et $K_p$ est intègre). Mais par Cayley-Hamilton, $S^2 - \mathrm{Tr(S)}S + I_2 = 0$, d'où en soustrayant, $\mathrm{Tr}(S) = 0$, ce qui d'après la partie 2 montre que $p$ divise $2y_{k-2}$ et enfin que $p$ divise $y_{k-2}$ puisque 2 et $p$ sont premiers entre eux.

5) Réciproquement, soit $n = 2^k - 1$ un entier qui divise $y_{k-2}$, avec $k \geqslant 3$. Supposons $n$ composé. Dans un premier temps, supposons en plus que $n$ admette un diviseur premier $q \geqslant 5$. (donc $q < n$ car $n$ composé). D'après la partie 1, on a que $n$, donc $q$, divise $\mathrm{Tr}(M^{2^{k-2}})$, donc $\mathrm{Tr}(S) = 0$ où $S = M_q^{2^{k-2}}$. Par Cayley-Hamilton, il vient que $S^2 + I_2 = 0$, donc $S$ est d'ordre 4 et $M_q$ d'ordre $2^k$. Mais l'ordre de $M_q$ divise l'ordre du groupe $B_q$ auquel elle appartient, qui est de cardinal $q - 1$ ou $q + 1$ d'après la partie 3. Ainsi $2^k \leqslant q + 1$, donc $n \leqslant q$, absurde.

C'est donc qu'il existe $r \geqslant 2$ tel que $2^k - 1 = 3^r$. Si $k$ est impair cette égalité ne peut avoir lieu car alors $2^k - 1 \equiv 1 \bmod 3$. On en déduit donc que $k = 2k'$ avec $k' \geqslant 2$, d'où

$$3^r = 2^k - 1 = (2^{k'} - 1)(2^{k'} + 1).$$

Chacun de ces deux facteurs étant égal au moins , on en déduit qu'ils sont tous les deux divisibles par 3, donc leur différence aussi, ce qui est absurde car celle-ci vaut 2.

Ainsi l'entier $n$ est premier, et le théorème est prouvé. ∎

**Référence.** — *Algèbre linéaire*, Michel Cognet. Bréal.