

Le test de Lucas-Lehmer

Marc Lorenzi

17 décembre 2025

1 Introduction

Définition 1. Pour tout $n \in \mathbb{N}$, le n^e nombre de Mersenne est

$$M_n = 2^n - 1$$

Proposition 1. Soit $n \in \mathbb{N}$. Si M_n est premier, alors n est premier.

Démonstration. $M_0 = 0$ et $M_1 = 1$ ne sont pas premiers. Supposons donc $n \geq 2$. Supposons que $n = ab$ est composé, où $a, b \in \llbracket 2, n-1 \rrbracket$. On a

$$M_n = (2^a)^b - 1 = (2^a - 1) \sum_{k=0}^{b-1} 2^{ka}$$

Comme $a \neq 1$, $2^a - 1 \neq 1$. Comme $a < n$, $2^a - 1 \neq M_n$. Ainsi, $2^a - 1$ est un facteur de M_n qui est différent de 1 et M_n , donc M_n est composé. \square

La réciproque est fausse. Par exemple, $M_{11} = 23 \times 89$. Les nombres premiers inférieurs à 5000 pour lesquels M_p est premier sont 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253 et 4423.

Dans toute la suite, p désigne un nombre premier impair. Nous allons dans ce qui suit déterminer une condition nécessaire et suffisante pour que M_p soit un nombre premier. Cette condition exprimera qu'un certain terme d'une certaine suite d'éléments de $\mathbb{Z}/M_p\mathbb{Z}$ est nul. Il s'agit du *test de Lucas-Lehmer*.

Nous notons $\mathcal{M}_p = \mathbb{Z}/M_p\mathbb{Z}$ l'anneau des entiers modulo p . Si M_p est premier, cet anneau est un corps. Sinon, c'est un anneau non intègre. Pour tout entier relatif a , nous noterons simplement a , plutôt que $a + M_p\mathbb{Z}$, la classe de a modulo M_p . En cas de doute, nous préciserons que nous calculons dans \mathcal{M}_p et pas dans \mathbb{Z} .

2 Une extension de \mathcal{M}_p

2.1 3 n'est pas un carré

Lemme 2. *Le nombre 3 n'est pas un carré dans \mathcal{M}_p .*

Démonstration. Par la loi de réciprocité quadratique généralisée, les symboles de Jacobi $\left(\frac{3}{M_p}\right)$ et $\left(\frac{M_p}{3}\right)$ vérifient

$$\left(\frac{3}{M_p}\right) = (-1)^{\frac{3-1}{2} \frac{M_p-1}{2}} \left(\frac{M_p}{3}\right) = (-1)^{\frac{M_p-1}{2}} \left(\frac{M_p}{3}\right)$$

On a

$$(-1)^{(M_p-1)/2} = (-1)^{2^{p-1}-1} = -1$$

De plus,

$$M_p = 2^p - 1 \equiv (-1)^p - 1 = -2 \equiv 1 \pmod{3}$$

et donc

$$\left(\frac{M_p}{3}\right) = \left(\frac{1}{3}\right) = 1$$

Ainsi,

$$\left(\frac{3}{M_p}\right) = -1$$

donc 3 n'est pas un carré dans \mathcal{M}_p . \square

2.2 Un sur-anneau de \mathcal{M}_p

On considère l'anneau $\mathcal{A}_p = \mathcal{M}_p[X]/(X^2 - 3)$.

On note $\sqrt{3}$ la classe de X dans \mathcal{A}_p . Les éléments de \mathcal{A}_p s'écrivent de façon unique $a + b\sqrt{3}$ où $a, b \in \mathcal{M}_p$. Il en résulte que \mathcal{A}_p est un anneau fini de cardinal M_p^2 . Les opérations dans \mathcal{A}_p s'écrivent, pour tous $a, b, c, d \in \mathcal{M}_p$,

$$\begin{aligned} (a + b\sqrt{3}) + (c + d\sqrt{3}) &= (a + c) + (b + d)\sqrt{3} \\ (a + b\sqrt{3}) \times (c + d\sqrt{3}) &= (ac + 3bd) + (ad + bc)\sqrt{3} \end{aligned}$$

L'ensemble des éléments de \mathcal{A}_p de la forme $a + 0\sqrt{3}$ est un sous-anneau de \mathcal{A}_p isomorphe à \mathcal{M}_p . Nous confondrons dorénavant ce sous-anneau avec \mathcal{M}_p , de sorte que, $\mathcal{M}_p \subset \mathcal{A}_p$.

Proposition 3. *Si M_p est premier, alors \mathcal{A}_p est un corps. Sinon, l'anneau \mathcal{A}_p n'est pas intègre.*

Démonstration. Supposons M_p est premier. Par la proposition 2, le polynôme $X^2 - 3$ est irréductible sur le corps \mathcal{M}_p , donc \mathcal{A}_p est un corps. Si M_p n'est pas premier alors \mathcal{M}_p n'est pas intègre. Comme $\mathcal{M}_p \subset \mathcal{A}_p$, l'anneau \mathcal{A}_p n'est pas non plus intègre. \square

Proposition 4. *On suppose M_p premier. Soit $\Phi : \mathcal{A}_p \longrightarrow \mathcal{A}_p$ définie par $\Phi(x) = x^{M_p}$. L'application Φ est un endomorphisme de l'anneau \mathcal{A}_p . Les points fixes de Φ sont les éléments de \mathcal{M}_p .*

L'application Φ est le *morphisme de Frobenius*.

Démonstration. Comme M_p est premier, les anneaux \mathcal{M}_p et \mathcal{A}_p sont des corps.

Les points fixes de Φ sont les racines du polynôme $P = X^{M_p} - X$. Par le petit théorème de Fermat, on a pour tout $x \in \mathcal{M}_p$, $x^{M_p} = x$ et donc x est racine de P . De plus, comme \mathcal{A}_p est un corps, le polynôme P , de degré M_p , a au plus M_p racines. Les racines de P sont donc les éléments de \mathcal{M}_p .

Soient $x, y \in \mathcal{A}_p$. On a

$$\Phi(xy) = (xy)^{M_p} = x^{M_p}y^{M_p} = \Phi(x)\Phi(y)$$

Par la formule du binôme,

$$\Phi(x + y) = (x + y)^{M_p} = \sum_{k=0}^{M_p} \binom{M_p}{k} x^k y^{M_p-k}$$

Comme M_p est premier, pour tout $k \in \llbracket 1, M_p - 1 \rrbracket$, M_p divise $\binom{M_p}{k}$ et donc, dans \mathcal{A}_p , $\binom{M_p}{k} = 0$. De là, tous les termes de la somme sont nuls sauf le premier et le dernier, d'où

$$\Phi(x + y) = x^{M_p} + y^{M_p} = \Phi(x) + \Phi(y)$$

Enfin, $\Phi(1) = 1$. Ainsi, Φ est un endomorphisme du corps \mathcal{A}_p . \square

Remarque. Plus généralement, soit \mathbb{K} un corps de caractéristique $q \neq 0$. L'entier q est un nombre premier et l'ensemble $\mathbb{K}_0 = \{n \times 1 : n \in \mathbb{Z}\}$ est un sous-corps de \mathbb{K} isomorphe à $\mathbb{Z}/q\mathbb{Z}$. L'application $\Phi : \mathbb{K} \longrightarrow \mathbb{K}$ définie par $\Phi(x) = x^q$ est un endomorphisme du corps \mathbb{K} et pour tout $x \in \mathbb{K}$, $\Phi(x) = x$ si et seulement si $x \in \mathbb{K}_0$. La preuve de ces résultats est analogue à ce que nous avons fait dans le cas particulier de \mathcal{A}_p .

3 Le test de Lucas-Lehmer

Posons $\alpha = 2 + \sqrt{3}$ et $\beta = 2 - \sqrt{3}$. Remarquons que

$$\alpha\beta = (2 + \sqrt{3})(2 - \sqrt{3}) = 2^2 - \sqrt{3}^2 = 1$$

Ainsi, sans l'anneau \mathcal{A}_p , α est inversible et $\alpha^{-1} = \beta$.

3.1 Condition nécessaire

Proposition 5. *On suppose M_p premier. Alors, $\alpha^{2^{p-1}} = -1$.*

Démonstration. Soit $r = 2^{(p+1)/2} \in \mathcal{M}_p$. On a

$$r^2 = 2^{p+1} = 2 \times 2^p = 2(M_p + 1) = 2$$

Ainsi, 2 est un carré dans \mathcal{M}_p . Notons $\sqrt{2} = r$. Soient

$$\rho = \frac{1 + \sqrt{3}}{\sqrt{2}} \quad \text{et} \quad \bar{\rho} = \frac{1 - \sqrt{3}}{\sqrt{2}}$$

On a facilement $\rho^2 = \alpha$ et $\bar{\rho}^2 = \beta$. De là,

$$\alpha^{2^{p-1}} = (\rho^2)^{2^{p-1}} = \rho^{2^p} = \rho \rho^{M_p} = \rho \Phi(\rho)$$

Clairement, ρ et $\bar{\rho}$ sont des racines du polynôme $Q = (\sqrt{2}X - 1)^2 - 3$. Comme Q est de degré 2, ce sont *les* racines de Q (rappelons que comme M_p est premier, \mathcal{A}_p est un corps). De plus, comme Φ est un endomorphisme d'anneau,

$$Q(\Phi(\rho)) = \Phi(Q(\rho)) = \Phi(0) = 0$$

On a donc $\Phi(\rho) = \rho$ ou $\Phi(\rho) = \bar{\rho}$. Par la proposition 4, comme $\rho \notin \mathcal{M}_p$, $\Phi(\rho) \neq \rho$, donc $\Phi(\rho) = \bar{\rho}$. Ainsi,

$$\alpha^{2^{p-1}} = \rho \Phi(\rho) = \rho \bar{\rho} = -1$$

□

3.2 Condition suffisante

Proposition 6. *On suppose $\alpha^{2^{p-1}} = -1$. Alors, M_p est premier.*

Démonstration. Supposons, par l'absurde, que M_p n'est pas premier. Soit $q < M_p$ un diviseur premier de M_p . Dans l'anneau \mathcal{M}_p , on a $q(M_p/q) = M_p = 0$. Comme $M_p/q \neq 0$, on en déduit que q est un diviseur de zéro dans \mathcal{M}_p et donc aussi dans \mathcal{A}_p .

Comme q est un diviseur de zéro, q n'est pas inversible. Il appartient donc à un idéal maximal \mathcal{I} de \mathcal{A}_p . Notons $\mathbb{K} = \mathcal{A}_p/\mathcal{I}$. Comme \mathcal{I} est maximal, \mathbb{K} est un corps. De plus, comme $q \in \mathcal{I}$, on a dans le corps \mathbb{K} l'égalité $q \times 1 = 0$. Ainsi, \mathbb{K} est de caractéristique q .

Notons $\bar{\alpha}$ et $\bar{\beta}$ les classes de α et β dans \mathbb{K} . On a $\bar{\alpha}^{2^{p-1}} = -1$ dans \mathbb{K} . En élevant au carré, $\bar{\alpha}^{2^p} = 1$. On en déduit que $\bar{\alpha}$ est d'ordre 2^p dans le corps \mathbb{K} .

Soit $Q = (X - \bar{\alpha})(X - \bar{\beta}) = X^2 - 4X + 1 \in \mathbb{K}[X]$.

Comme \mathbb{K} est de caractéristique q , l'application $\Psi : x \mapsto x^q$ est un endomorphisme du corps \mathbb{K} . On a donc

$$Q(\bar{\alpha}^q) = Q(\Psi(\bar{\alpha})) = \Psi(Q(\bar{\alpha})) = 0$$

Ainsi, $\bar{\alpha}^q$ est racine de Q . On en déduit que $\bar{\alpha}^q = \bar{\alpha}$ ou $\bar{\alpha}^q = \bar{\beta}$. Examinons chacun des deux cas.

- Cas 1, $\bar{\alpha}^q = \bar{\alpha}$. En multipliant par $\bar{\beta} = \bar{\alpha}^{-1}$, on obtient $\bar{\alpha}^{q-1} = 1$. De là, l'ordre de $\bar{\alpha}$, 2^p , divise $q - 1$ et donc $2^p \leq q - 1$. Or, $q < M_p = 2^p - 1$. Contradiction.
- Cas 2, $\bar{\alpha}^q = \bar{\beta} = \bar{\alpha}^{-1}$. On a donc $\bar{\alpha}^{q+1} = 1$. On en déduit que l'ordre de $\bar{\alpha}$ divise $q + 1$, c'est à dire 2^p divise $q + 1$. On a donc $2^p \leq q + 1$, d'où $M_p = 2^p - 1 \leq q$. Contradiction. □

3.3 La suite de Lucas-Lehmer

Le calcul de $\alpha^{2^{p-1}}$ peut être effectué en $p-1$ élévations au carré dans l'anneau \mathcal{A}_p . On dispose donc d'un algorithme en $O(p)$ pour décider de la primalité de M_p . Il est toutefois possible de se passer de l'anneau \mathcal{A}_p en effectuant uniquement des élévations au carré dans l'anneau \mathcal{M}_p . Pour cela, considérons la suite $(x_n)_{n \in \mathbb{N}}$ d'éléments de \mathcal{M}_p définie par

$$\begin{cases} x_0 = 4 \\ \text{pour tout } n \in \mathbb{N}, x_{n+1} = x_n^2 - 2 \end{cases}$$

Proposition 7. *Pour tout $n \in \mathbb{N}$,*

$$x_n = \alpha^{2^n} + \beta^{2^n}$$

Démonstration. Montrons ce résultat par récurrence sur n . Tout d'abord,

$$\alpha^{2^0} + \beta^{2^0} = \alpha + \beta = 4 = x_0$$

Soit $n \in \mathbb{N}$. Supposons la propriété vérifiée par n . On a alors

$$\begin{aligned} x_n^2 &= (\alpha^{2^n} + \beta^{2^n})^2 \\ &= \alpha^{2^{n+1}} + \beta^{2^{n+1}} + 2(\alpha\beta)^{2^n} \\ &= \alpha^{2^{n+1}} + \beta^{2^{n+1}} + 2 \end{aligned}$$

et donc

$$x_{n+1} = x_n^2 - 2 = \alpha^{2^{n+1}} + \beta^{2^{n+1}}$$

□

Proposition 8. *M_p est premier si et seulement si $x_{p-2} = 0$.*

Démonstration. Rappelons que α est inversible dans l'anneau \mathcal{A}_p . On a donc

$$\begin{aligned} x_{p-2} = 0 &\iff \alpha^{2^{p-2}} + \alpha^{-2^{p-2}} = 0 \\ &\iff \alpha^{-2^{p-2}}(\alpha^{2^{p-1}} + 1) = 0 \\ &\iff \alpha^{2^{p-1}} + 1 = 0 \\ &\iff \alpha^{2^{p-1}} = -1 \end{aligned}$$

d'où le résultat par les propositions 5 et 6. □

La proposition 8 fournit un algorithme efficace pour déterminer si un nombre de Mersenne est premier : pour déterminer si M_p est premier, il suffit d'effectuer $p-2$ élévations au carré et $p-2$ soustractions modulo M_p .