Un critère de primalité pour les nombres de Mersenne

Clarence Kineider

Leçons : 120, 121, 123, 141

Référence(s) : Saux Picard, Rannou, *Cours de Calcul Formel, Corps finis, Systèmes polynomiaux, Applications.*

Définition : Soit $q \in \mathbf{N}^*$. Le q-ième nombre de Mersenne est $M_q = 2^q - 1$.

Remarque 1 :
Si q n'est pas premier, alors M_q n'est pas premier.
En effet, si q s'écrit $a \times b$ avec $a, b \geq 2$, alors $M_q = 2^{a \cdot b} - 1 = (2^a - 1)(1 + 2^a + 2^{2a} + \cdots + 2^{(b-1)a})$ et $2^a - 1 \neq 1$.
Puisque $M_2 = 3$ est premier, il reste à traiter le cas de M_q avec q premier impair.

Théorème : Soit q premier impair. Alors M_q est premier si et seulement si $(2 + \sqrt{3})^{2^{q-1}} \equiv -1 \ [\text{mod } M_q]$.

Remarque 2 :
Le $\sqrt{3}$ [mod M_q] n'est pas bien défini dans l'énoncé. Si 3 n'est pas un carré modulo M_q (et on va montrer que c'est toujours le cas), il faudra se placer dans une extension de $\mathbf{Z}/M_q\mathbf{Z}$ dans laquelle $X^2 - 3$ a une racine.

Démonstration : Soit q un nombre premier impair. On montre d'abord que 3 n'est jamais un carré modulo M_q. En effet, $M_q \equiv (-1)^q - 1 \equiv 1$ [mod 3], donc par la loi de réciprocité quadratique, on a :

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

Cette relation est également valable si M_q n'est pas premier, il suffit d'appliquer la loi de réciprocité quadratique pour le symbole de Jacobi défini de la manière suivante :

$$\left(\frac{a}{n}\right) = \prod \left(\frac{a}{p_i}\right) \text{ où } n = \prod p_i.$$

On pose alors $\mathcal{A} = \left(\mathbf{Z}/M_q\mathbf{Z}[X]\right)/(X^2 - 3)$ et on note $\sqrt{3}$ la classe de X dans $\mathcal{A}$.
$\Rightarrow$: On suppose que M_q est premier. On a $2(2^q - 1) \equiv 0$ [mod M_q], donc $2^{q+1} \equiv 2$ [mod M_q]. Comme $q+1$ est pair, 2 est un carré modulo M_q. On note alors $\sqrt{2}$ pour $2^{\frac{q+1}{2}}$.

Montrons que $(2+\sqrt{3})^{2^{q-1}} = -1$ dans $\mathcal{A}$. Pour cela, posons $\rho = \dfrac{1+\sqrt{3}}{\sqrt{2}}$ et $\overline{\rho} = \dfrac{1-\sqrt{3}}{\sqrt{2}}$. On a :

$$\begin{aligned}(2+\sqrt{3})^{2^{q-1}} &= (\rho^2)^{2^{q-1}} \\ &= \rho^{2^q} \\ &= \rho \cdot \rho^{M_q}\end{aligned}$$

Comme le polynôme X^2-3 est irréductible dans ${}^{\mathbf{Z}}\!/_{M_q\mathbf{Z}}[X]$, $\mathcal{A}$ est un corps et l'application $\begin{array}{ccc}\mathcal{A} & \to & \mathcal{A} \\ x & \mapsto & x^{M_q}\end{array}$ est un morphisme d'anneaux (c'est le morphisme de Frobenius car $\mathcal{A}$ est de caractéristique M_q). De plus, ρ et $\overline{\rho}$ sont les deux racines du polynôme $(\sqrt{2}X-1)^2-3 \in {}^{\mathbf{Z}}\!/_{M_q\mathbf{Z}}[X]$, et $\rho \notin {}^{\mathbf{Z}}\!/_{M_q\mathbf{Z}}$ donc n'est pas un point fixe du morphisme de Frobenius. Ainsi $\rho^{M_q} = \overline{\rho}$. D'où, $(2+\sqrt{3})^{2^{q-1}} = \rho \cdot \overline{\rho} = -1$ dans $\mathcal{A}$.

$\Leftarrow$: On suppose que $(2+\sqrt{3})^{2^{q-1}} = -1$ dans l'anneau $\mathcal{A}$. Pour montrer que M_q est premier, on va montrer que son seul diviseur distinct de 1 est lui-même. Soit donc $p > 1$ un facteur premier de M_q. Alors p est un diviseur de zéro dans $\mathcal{A}$ car $p \cdot \dfrac{M_q}{p} = M_q = 0$ dans $\mathcal{A}$. Ainsi, p n'est pas inversible dans $\mathcal{A}$. On peut donc considérer $\mathcal{M}$ un idéal maximal de $\mathcal{A}$ contenant p ($\mathcal{M}$ existe car $\mathcal{A}$ est fini).
On se place dans le corps $\mathcal{A}/\mathcal{M}$ qui est de caractéristique p car $p \in \mathcal{M}$ et donc $p \cdot 1 = 0$ dans le quotient.
On pose α (resp. β) la classe de $2+\sqrt{3}$ (resp. $2-\sqrt{3}$) dans $\mathcal{A}/\mathcal{M}$. On a $(2+\sqrt{3})^{2^{q-1}} = -1$ dans $\mathcal{A}$ donc $\alpha^{2^{q-1}} = -1$ dans $\mathcal{A}/\mathcal{M}$. L'ordre de α est donc 2^q.
On considère le polynôme $Q(X) = (X-\alpha)(X-\beta) = X^2 - 4X + 1$ dans $\mathcal{A}/\mathcal{M}$. Or $\mathcal{A}/\mathcal{M}$ est de caractéristique p, donc α^p est un zéro de Q car α l'est. Donc $\alpha^p = \alpha$ ou $\alpha^p = \beta$.
Dans le premier cas, $\alpha^p = \alpha$ et comme α est inversible d'inverse β, on a $\alpha^{p-1} = 1$ donc 2^q divise $p-1$. Or on sait que p divise $2^q - 1 = M_q$, ce qui est absurde. Dans le deuxième cas, $\alpha^p = \beta$, on a $\alpha^p = \beta = \alpha^{-1} = \alpha^{M_q}$. Donc 2^q divise $p+1$, ce qui implique que $p = M_q$. Ainsi M_q est bien premier. □

Remarque 3 :
Ce critère n'est pas directement utilisable en pratique car le calcul de $(2+\sqrt{3})^{2^{q-1}}$ demande beaucoup de temps lorsque la valeur de q est grande.
Cependant, ce résultat est utilisé dans le test de primalité suivant :

Théorème (Test de Lucas-Lehmer)**:** On définit par récurrence la suite $(x_n)_{n\in\mathbf{N}}$ par :

$$\begin{cases} x_0 = 4; \\ \forall n \geqslant 0,\ x_{n+1} = x_n^2 - 2. \end{cases}$$

Alors pour q premier impair, M_q est premier si et seulement si $x_{q-2} \equiv 0 \pmod{M_q}$.

Démonstration : La solution générale de cette équation de récurrence est $x_n = (2+\sqrt{3})^{2^n} + (2-\sqrt{3})^{2^n}$.

Alors par le théorème précédent, on a :

$$\begin{aligned} x_{q-2} \equiv 0 \ [\text{mod } M_q] &\Leftrightarrow (2+\sqrt{3})^{2^{q-2}} + (2-\sqrt{3})^{2^{q-2}} \equiv 0 \ [\text{mod } M_q] \\ &\Leftrightarrow (2+\sqrt{3})^{2^{q-1}} + 1 \equiv 0 \ [\text{mod } M_q] \\ &\Leftrightarrow (2+\sqrt{3})^{2^{q-1}} \equiv -1 \ [\text{mod } M_q] \\ &\Leftrightarrow M_q \text{ est premier} \end{aligned}$$

□