Primalité des nombres de Mersenne

Référence : Cours de calcul formel. Corps finis, systèmes polynomiaux, applications.
Philippe Saux Picart, Éric Rannou

2011-2012

On appelle *nombres de Mersenne* les

$$M_q = 2^q - 1$$

pour $q \in \mathbb{N}$

On a d'abord le lemme :

Lemme 1
Si M_q est un nombre premier, alors q est premier.

Démonstration. Si q n'est pas premier, $q = mn$, avec $m, n > 2$.
Et alors $M_q = 2^{mn} - 1$ qui est divisible par $2^n - 1$. □

On a une caractérisation :

Théorème 2
Pour tout nombre premier impair q :

$$M_q \text{ est premier} \iff \left(2+\sqrt{3}\right)^{2^{q-1}} \equiv -1 \mod M_q.$$

On remarque qu'il faut se placer dans un corps où 3 admet une racine carrée. Dans la suite, on explicitera : on prendra $\mathbb{F}_{M_q}$ ou une de ses extensions.

Démonstration du sens direct.

Lemme 3
Pour tout entier k non nul, M_{2k+1} est congru à 7 modulo 12.

Démonstration. Par récurrence :
$(k = 1)$: On a bien $2^{2\times 1+1} = 7$.

$(k \to k+1)$: On a modulo 12 :

$$\begin{aligned} 2^{2(k+1)+1} - 1 &\equiv 4 \times 2^{2k+1} - 1 \\ &\equiv \left(2^{2k+1} - 1\right) \times 4 + 3 \\ &\equiv 7 \times 4 + 3 \\ &\equiv 7 \end{aligned}$$

$\Diamond$

Donc, pour tout q impair, $M_q \equiv 7 \mod 12$.

Montrons maintenant que 3 n'est pas résidu quadratique modulo M_q.

Pour cela, on montre le

Lemme 4
3 est résidu quadratique modulo un entier premier p si, et seulement si $p \equiv \pm 1 \mod 12$.

Démonstration. Par la loi de réciprocité quadratique, on a :

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

Ainsi, par définition du symbole de Legendre :

$$3 \text{ résidu modulo } p \Leftrightarrow \left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}.$$

On remarque que le seul carré non nul de $\mathbb{F}_3$ est 1, et donc 3 est résidu quadratique modulo p *si, et seulement si* l'une des conditions est vérifiée :

(i) $p \equiv 1 \mod 3$ et $\frac{p-1}{2}$ est pair.

(ii) $p \equiv 2 \mod 3$ et $\frac{p-1}{2}$ est impair.

Dans le premier cas, p est congru à 1 modulo 3 et 4, et donc modulo 12.

Dans le second cas, p est congru à 2 modulo 3, et 3 modulo 4, et donc par théorème chinois, à -1 modulo 12. $\Diamond$

Comme M_q n'est congru ni à 1, ni à -1 modulo 12, 3 n'est pas résidu quadratique modulo M_q. $X^2 - 3$ est donc irréductible sur $\mathbb{F}_{M_q}$, et donc $\mathscr{A} = \mathbb{F}_{M_q}[X]/(X^2 - 3)$ est un corps, et on note la classe de X dans $\mathscr{A}$ $\sqrt{3}$.

On remarque de plus que $2^{q+1} \equiv 2 \mod M_q$, et donc 2 admet une racine carrée $\sqrt{2} := 2^{\frac{q+1}{2}}$.

On définit les quantités

$$\rho = \frac{1+\sqrt{3}}{\sqrt{2}} \text{ et } \overline{\rho} = \frac{1-\sqrt{3}}{\sqrt{2}}.$$

On montre facilement que $\rho^2 = 2 + \sqrt{3}$ et $\overline{\rho}\rho = -1$.

De plus, on remarque que comme $\sqrt{3}$ n'est pas résidu quadratique modulo M_q, par petit théorème de Fermat :

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

Comme $\mathscr{A}$ est de caractéristique M_q, on a par morphisme de Frobénius :

$$\left(a + b\sqrt{3}\right)^{M_q} = a - b\sqrt{3}.$$

De même, on a $\rho^{M_q} = \overline{\rho}$ Comme $\mathscr{A}$ est de caractéristique M_q, on a par morphisme de Frobénius :

$$\left(a + b\sqrt{3}\right)^{M_q} = a - b\sqrt{3}.$$

De même, on a $\sqrt{2}^{M_q} = \sqrt{2}$, et donc $\rho^{M_q} = \overline{\rho}$.

On multiplie à gauche et à droite, et on obtient :

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

□

Démonstration du sens réciproque. On note dans la suite $\mathbb{Z}_n$ l'anneau $\mathbb{Z}/n\mathbb{Z}$.

On note encore $\mathscr{A}$ une extension de $\mathbb{Z}_{M_q}$ contenant une racine de 3 : plus précisemment, si $\mathbb{Z}_{M_q}$ contient une racine de 3, on prend $\mathscr{A} = \mathbb{Z}_{M_q}$, et sinon on prend $\mathscr{A} = \mathbb{Z}_{M_q}[X]/(X^2 - 3)$.

On suppose M_q non premier, et on appelle p un de ses diviseurs premiers.

p est donc un diviseur de 0 dans $\mathscr{A}$, et a fortiori n'est pas inversible. Il est donc contenu dans un idéal maximal $\mathscr{M}$ de $\mathscr{A}$.

Alors $\mathscr{A}/\mathscr{M}$ est un corps, de caractéristique p (p non nul dans $\mathscr{M}$).

On appelle α (resp. β) la classe de $2 + \sqrt{3}$ (resp. $2 - \sqrt{3}$) dans $\mathscr{A}/\mathscr{M}$.

Notre hypothèse s'écrit donc $\alpha^{2^{q-1}} \equiv -1 \mod M_q$, et on en déduit que α est d'ordre 2^q dans $\mathscr{A}/\mathscr{M}$.

On pose maintenant $Q = (X - \alpha)(X - \beta) = X^2 - 4X + 1$. C'est un polynôme à coefficient dans le corps premier de $\mathscr{A}/\mathscr{M}$, $\mathbb{F}_p$.

Donc, comme α est racine de Q, α^p aussi, et donc $\alpha^p = \alpha$ ou $\alpha^p = \beta$.

Dans le premier cas, comme l'ordre de α est 2^q, 2^q divise $p - 1$. Or p divise $M_q = 2^q - 1$, donc $p < 2^q$. D'où une contradiction.

Dans le second cas, $\alpha^p = \beta = \alpha^{-1} = \alpha^{M_q}$. On a alors $p \equiv 2^q - 1 \mod 2^q$, et ceci impose $p = M_q$. Encore une contradiction.

□

Remarque – On peut citer un corollaire direct de ce théorème :

Théorème 5 : Test de Lehmer-Lucas
On définit la suite $(L_n) \in \mathbb{Z}_{M_q}^{\mathbb{N}}$ *par*

$$L_0 = 4 \text{ et } L_{n+1} = L_n^2 - 2 \mod M_q.$$

Alors on a :

$$M_q \text{ premier} \iff L_{q-2} \equiv 0 \mod M_q.$$

Cet algorithme permet de calculer directement dans $\mathbb{Z}_{M_q}$ plutôt que dans une extension. Au final, il est de complexité $\mathcal{O}(q^3)$ (on peut accélerer un peu avec la transformée de Fourier discrète).