Primalité des nombres de Mersenne

Leçons : 120 ; 121 ; 123 ; 141

Références : SAUX PICART–RANNOU, *Cours de Calcul Formel, Corps finis, Systèmes polynomiaux Applications* (p.80)[?]

Prérequis :

- le symbole de Legendre et la propriété $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$
- la Loi de Réciprocité Quadratique (voir le développement)
- le théorème chinois
- le morphisme de Frobenius
- corps de rupture

Introduction :

Un nombre de Mersenne est un nombre de la forme $M_q = 2^q - 1$ avec $q \in \mathbb{N}^*$. On veut trouver les nombres de Mersenne qui sont premiers. Si q n'est pas premier, $q = ab$ et

$$2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1)$$

est divisible par $2^a - 1$ non inversible dans $\mathbb{Z}$ (ainsi le cas q non premier ne donnera jamais de M_q premier). Pour $q = 2$, $M_q = 2^2 - 1 = 3$ qui est premier. On se restreint donc à q premier impair.

Remarques :

Tous les nombres de Mersenne ne sont pas premiers, par exemple, $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$, et l'on ne sait pas aujourd'hui s'il existe une infinité de nombres de Mersenne qui sont premiers, ni s'il existe une infinité de nombres de Mersenne qui ne sont pas premiers. Aujourd'hui, les plus grands nombres premiers que l'on connaisse sont des nombres de Mersenne.

Le théorème ci-dessous nous donne donc un critère de primalité des nombres de Mersenne pour q premier impair.

Théorème 1. Pour q premier impair, on a

$$M_q \text{ est premier } \iff (2+\sqrt{3})^{2^{q-1}} \equiv -1 \ [M_q]$$

Remarques :

Tout d'abord, il faut comprendre où l'on se place pour dire cela, en effet il faut comprendre le sens de $\sqrt{3}$. Si 3 est un carré dans $\mathbb{Z}/M_q\mathbb{Z}$, on peut se placer dans $\mathbb{Z}/M_q\mathbb{Z}$, sinon on se placera dans une extension de corps de $\mathbb{Z}/M_q\mathbb{Z}$ qui contient une racine de 3, un corps de rupture de $X^2 - 3$ par exemple. Cela dit dans la première implication, on prouvera que 3 n'est jamais un carré dans $\mathbb{Z}/M_q\mathbb{Z}$ donc on se placera forcément dans $\mathbb{Z}/M_q\mathbb{Z}[X]/(X^2-3)$. De plus, le deuxième membre de l'équivalence n'a de sens que si on est dans $\mathbb{Z}/M_q\mathbb{Z}$, ainsi dans le cas où il faut se placer dans $\mathcal{A} = \mathbb{Z}/M_q\mathbb{Z}[X]/(X^2-3)$, il faut comprendre que l'on veut juste l'égalité dans $\mathcal{A}$.

Démonstration :

$\boxed{\Longrightarrow}$ Pour le sens direct :

Étape 1 : *Condition nécessaire pour que 3 soit un carré modulo p avec p premier.*

On utilise la loi de réciprocité quadratique [1] avec 3 et p.

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

On suppose que 3 est un carré modulo p. Donc $\left(\frac{3}{p}\right) = 1$.

Ainsi si $p \equiv 1\ [3]$, on a $\left(\frac{p}{3}\right) = 1$ donc nécessairement, on a $\frac{p-1}{2}$ qui doit être pair, d'où $p \equiv 1\ [4]$. Par le lemme chinois [2], on a $p \equiv 1\ [12]$.

Et si $p \equiv 2\ [3]$, on a $\left(\frac{p}{3}\right) = -1$ donc nécessairement, on a $\frac{p-1}{2}$ qui doit être impair, d'où $p \equiv 3\ [4]$. Par le lemme chinois [3], on a $p \equiv -1\ [12]$.

Donc si 3 est un carré modulo p, on a nécessairement $p \equiv \pm 1\ [12]$.

Étape 2 : *3 n'est pas un carré modulo M_q.*

On va prouver par récurrence sur les q impairs (pour $q \geqslant 3$) que $M_q \equiv 7\ [12]$.

Initialisation : pour $q = 3$, on a $M_3 = 2^3 - 1 = 7 \equiv 7\ [12]$

Hérédité : on suppose que $M_{2k+1} \equiv 7\ [12]$, on veut prouver que $M_{2(k+1)+1} \equiv 7\ [12]$.

$M_{2(k+1)+1} = 2^{2k+3} - 1 = 4 \times 2^{2k+1} - 1 = 4(2^{2k+1} - 1) + 3 \equiv 4 \times 7 + 3 \equiv 24 + 7 \equiv 7\ [12]$.

Donc pour tout q impair premier, on a $M_q \equiv 7\ [12]$, ainsi par l'étape 1, on sait que 3 n'est pas un carré modulo M_q.

Étape 3 : *2 est un carré modulo M_q.*

Il suffit de faire un court calcul : $2(2^q - 1) \equiv 0\ [M_q]$ d'où $2^{q+1} \equiv 2\ [M_q]$, donc comme $q+1$ est pair, on a $(2^{\frac{q+1}{2}})^2 \equiv 2\ [M_q]$. Donc 2 est bien un carré modulo M_q. On notera désormais $\sqrt{2}$ pour $2^{\frac{q+1}{2}}$.

Étape 4 : *Calcul de $(2+\sqrt{3})^{2^{q-1}}$ dans un corps approprié.*

Comme 3 n'est pas un carré modulo M_q, le polynôme $X^2 - 3$ est irréductible sur $\mathbb{Z}/M_q\mathbb{Z}$. Donc on peut se placer dans le corps $\mathcal{A} = \mathbb{Z}/M_q\mathbb{Z}[X]/(X^2-3)$. On notera désormais $\sqrt{3}$ pour la classe de X dans $\mathcal{A}$. On pose $\rho = \dfrac{1+\sqrt{3}}{\sqrt{2}}$ et $\bar{\rho} = \dfrac{1-\sqrt{3}}{\sqrt{2}}$. On veut prouver que $(2+\sqrt{3})^{2^{q-1}} = -1$ dans $\mathcal{A}$.

$$\begin{aligned}(2+\sqrt{3})^{2^{q-1}} &= (\rho^2)^{2^{q-1}} = \rho^{2^q} \\ &= \rho\Big(\frac{1+\sqrt{3}}{\sqrt{2}}\Big)^{M_q} \\ &= \rho\Big(\Big(\frac{1}{\sqrt{2}}\Big)^{M_q} + \Big(\frac{\sqrt{3}}{\sqrt{2}}\Big)^{M_q}\Big) \text{ car } \mathcal{A} \text{ est de caractéristique } M_q\end{aligned}$$

Or $\sqrt{2}^{M_q} = \sqrt{2}$ dans $\mathcal{A}$ car 2 est un carré modulo M_q. Et $\sqrt{3}^{M_q} = \sqrt{3} \times (\sqrt{3})^{M_q-1} = \sqrt{3}.3^{\frac{M_q-1}{2}} = -\sqrt{3}$ car 3 n'est pas un carré modulo M_q [4].

Donc $(2+\sqrt{3})^{2^{q-1}} = \rho\Big(\Big(\frac{1}{\sqrt{2}}\Big) - \Big(\frac{\sqrt{3}}{\sqrt{2}}\Big)\Big) = \rho\bar{\rho} = -1$ dans $\mathcal{A}$.

1. Connaitre la loi de réciprocité quadratique, c'est un développement classique donc ça peut aider.
2. Savoir expliquer rapidement comment trouver que $p \equiv 1\ [12]$
3. Même chose avec $p \equiv -1\ [12]$.
4. Savoir que pour x un carré modulo p, $x^{\frac{p-1}{2}} \equiv 1\ [p]$ et pour un non carré, $x^{\frac{p-1}{2}} \equiv -1\ [p]$.

$\boxed{\Longleftarrow}$ Pour le sens indirect : De nouveau, il faut comprendre comment interpréter $\sqrt{3}$ dans l'hypothèse, donc on se place

— soit dans $\mathcal{A} = \mathbb{Z}/M_q\mathbb{Z}$ si 3 est un carré dans $\mathbb{Z}/M_q\mathbb{Z}$,

— soit dans $\mathcal{A} = \mathbb{Z}/M_q\mathbb{Z}[X]/(X^2-3)$ si 3 n'est pas un carré dans $\mathbb{Z}/M_q\mathbb{Z}$.

On prend $p > 1$ un facteur premier de M_q. Donc p est un diviseur de zéro dans $\mathcal{A}$, car $p \times \frac{M_q}{p} = 0$ dans $\mathcal{A}$. Ainsi p n'est pas inversible. Donc on peut considérer $\mathcal{M}$ un idéal maximal de $\mathcal{A}$ qui contient p [5].

On se place dans $\mathcal{A}/\mathcal{M}$ qui est un corps (car $\mathcal{M}$ est maximal) de caractéristique p car p est premier et $\underbrace{1+\cdots+1}_{p \text{ fois}} = 0$ dans $\mathcal{A}/\mathcal{M}$.

On pose α (resp. β) la classe de $2+\sqrt{3}$ (resp. $2-\sqrt{3}$), $\alpha^{2^{q-1}} = -1$ dans $\mathcal{A}/\mathcal{M}$ donc l'ordre de α est 2^q comme expliqué dans la note [6].

On considère le polynôme $Q(X) = (X-\alpha)(X-\beta) = X^2 - 4X + 1$ dans $\mathcal{A}/\mathcal{M}$. Or puisque $\mathcal{A}/\mathcal{M}$ est de caractéristique p, α^p est aussi zéro de Q [7] car α l'est. Donc $\alpha^p = \alpha$ ou $\alpha^p = \beta$.

Dans le premier cas, $\alpha^p = \alpha$, comme α est inversible car $\alpha^{2^q} = 1$, on a alors $\alpha^{p-1} = 1$ donc 2^q divise $p-1$ or on sait que p divise $2^q - 1$ ce qui est absurde.

Dans le deuxième cas, $\alpha^p = \beta$, or $\alpha^p = \beta = \alpha^{-1} = \alpha^{M_q}$ [8]. Donc 2^q divise $M_q - p$, ce qui implique que $p = M_q$ [9]. Ainsi M_q est bien premier.

□

Remarques :

En pratique cette méthode n'est pas applicable directement car pour chercher des nombres premiers extrêmement grand, on va avoir un q très grand et donc le calcul $(2+\sqrt{3})^{2^{q-1}}$ est difficilement faisable. Cependant, on se sert de ce résultat pour le test de Lehmer–Lucas :
On définit la suite $(L_n) \in (\mathbb{Z}/M_q\mathbb{Z})^{\mathbb{N}}$ par $L_0 = 4$ et $L_{n+1} \equiv L_n^2 - 2\ [M_q]$, on a alors M_q premier $\iff L_{q-2} \equiv 0\ [M_q]$
Complexité en $\mathcal{O}(q^3)$.

Théorème 2 (Test de Lehmer–Lucas)**.** Soit la suite $(L_n) \in (\mathbb{Z}/M_q\mathbb{Z})^{\mathbb{N}}$ définie par

$$L_0 = 4 \quad \text{et} \quad L_{n+1} \equiv L_n^2 - 2\ [M_q]$$

On a alors :

$$M_q \text{ est premier} \iff L_{q-2} \equiv 0\ [M_q]$$

Démonstration. On pose $\omega = 2+\sqrt{3}$ et $\tilde{\omega} = 2-\sqrt{3}$. On a $\omega^{2^n} + \tilde{\omega}^{2^n} \in \mathbb{Z}/M_q\mathbb{Z}$ car les parties en $\sqrt{3}$ se compensent et $\omega^{2^n} + \tilde{\omega}^{2^n} = L_n$ (par récurrence).
Initialisation : $n = 0$, $\omega^{2^0} + \tilde{\omega}^{2^0} = \omega + \tilde{\omega} = 4 = L_0 \in \mathbb{Z}/M_q\mathbb{Z}$.
Hérédité : On suppose que le résultat est vrai pour $k \in \mathbb{N}$, on veut prouver le résultat au rang $k+1$.

$\omega^{2^{k+1}} + \tilde{\omega}^{2^{k+1}} \equiv (\omega^{2^k} + \tilde{\omega}^{2^k})^2 - 2\omega^{2^k}\tilde{\omega}^{2^k} \equiv L_n^2 - 2\ [M_q]$ par hypothèse de récurrence et car $a^2+b^2 = (a+b)^2 - 2ab$ et $\omega^{2^k}\tilde{\omega}^{2^k} = 1$ puisque $\omega\tilde{\omega} = 1$.
Conclusion : Donc $\omega^{2^n} + \tilde{\omega}^{2^n} = L_n$ pour tout $n \in \mathbb{N}$.

5. car $\mathcal{A}$ est fini, donc on peut ajouter des éléments dans l'idéal tant que l'idéal n'est pas $\mathcal{A}$ tout entier
6. Bien comprendre pourquoi, l'ordre est forcément une puissance de 2 par hypothèse, puis par la même hypothèse, on a forcément que 2^q est l'ordre car $\alpha^{2^{q-1}} = -1$ puisque la caractéristique p est impaire donc $1 \neq -1$
7. Comprendre pourquoi (morphisme de Frobenius)
8. Bien comprendre d'où vient chaque égalité
9. Car $2^q - 1 - p = 2_q k$ implique en fait que $k = 0$ d'où le résultat

Ainsi on a

$$\begin{aligned} L_{q-2} \equiv 0\ [M_q] &\iff \omega^{2^{q-2}} + \tilde{\omega}^{2^{q-2}} \equiv 0\ [M_q] \\ &\iff \omega^{2^{q-2}} \equiv -\tilde{\omega}^{2^{q-2}}\ [M_q] \\ &\iff (\omega^{2^{q-2}})^2 \equiv -1\ [M_q] \text{ toujours car } \omega^{2^k}\tilde{\omega}^{2^k} = 1 \\ &\iff (\omega^{2^{q-1}}) \equiv -1\ [M_q] \\ &\iff M_q \text{ est premier, par le théorème précédent} \end{aligned}$$

□

Astuces de l'agrégatif :

Pour les différentes leçons, je ne fais pas toujours la même chose,

- pour la 120, j'utilise la notation $\mathbb{Z}/M_q\mathbb{Z}$, je mets en lumière le lemme chinois
- pour la 123, j'utilise la notation $\mathbb{F}_{M_q}$, je parle de corps fini, je mets en lumière la loi de réciprocité quadratique
- pour la 141, je mets en lumière la construction du corps de rupture.
- pour la 121, j'utilise un moyen plus court pour prouver que 3 n'est pas un carré dans $\mathbb{Z}/M_q\mathbb{Z}$ et je fais la réciproque qui est la partie plus intéressante car cela nous donne une caractérisation des nombres de Mersenne qui sont premiers.

Moyen plus court pour prouver que 3 n'est pas un carré dans $\mathbb{Z}/M_q\mathbb{Z}$:

$$\begin{aligned} \left(\frac{3}{M_q}\right) &\overset{(1)}{=} \left(\frac{M_q}{3}\right)(-1)^{\frac{M_q-1}{2}} = \left(\frac{2^q-1}{3}\right)(-1)^{\frac{2^q-2}{2}} \\ &\overset{(2)}{=} \left(\frac{(-1)^q-1}{3}\right)(-1)^{2^{q-1}-1} \overset{(3)}{=} -\left(\frac{(-1-1}{3}\right) = -\left(\frac{1}{3}\right) = -1 \end{aligned}$$

(1) Loi de réciprocité quadratique

(2) car $2 \equiv -1\ [3]$

(3) car $2^{q-1} - 1$ est impair et car q est impair