DVP Primalité des nombres de Mersenne

Antoine Dequay

21 septembre 2022

Notes

— Prof : Lionel Fourquaux.

— Leçons : 120, 121, 123, 141.

— Références :

— Saux Picart–Rannou, Cours de Calcul Formel, Corps finis, Systèmes polynomiaux, Applications (p.80).

Définition 1 *Nombre de* MERSENNE. Pour $q \in \mathbb{N}$, on appelle nombre de MERSENNE le nombre :

$$M_q := 2^q - 1.$$

Remarque Pour $q \in \mathbb{N}\backslash\{0,1\}$, si M_q est premier, alors q est premier. En effet, si $q = pr$ et $2^q - 1$ est premier, on a $2^q - 1 = (2^p)^r - 1$, donc $2^p - 1$ divise $2^q - 1$ (car $X^n - 1 = (X-1)\sum_{k=0}^{n-1} X^k$, et on peut remplacer n par r et X par 2^p). Comme $2^q - 1$ est supposé premier, il vient $p = 1$ ou $p = q$, donc q est bien premier !

Notation On note $\mathcal{P}$ l'ensemble des nombres premiers.

Théorème 2 Pour tout nombre premier impair q, on a :

$$M_q \in \mathcal{P} \iff \left(2+\sqrt{3}\right)^{2^{q-1}} \equiv -1\,[M_q]\,.$$

Preuve. On procède par double implication.

Supposons M_q premier et voyons ce que l'on entend par $\sqrt{3}$. On définit

$$\mathcal{A} := \left(\mathbb{Z}/M_q\mathbb{Z}\,[X]\right)/\left\langle X^2 - 3\right\rangle\,.$$

Montrons que $\mathcal{A}$ est un corps. Pour cela, on va montrer que $X^2 - 3$ est irréductible sur $\mathbb{Z}/M_q\mathbb{Z}$, c'est à dire que 3 n'est pas un carré modulo M_q. Montrons dans un premier temps que 3 **est un carré modulo $p \in \mathcal{P}$ si et seulement si** $p \equiv \pm 1\,[12]$.

La loi de réciprocité quadratique permet d'écrire :

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

donc

$$3 \text{ est un carré modulo } p \iff \left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}.$$

Le seul carré non nul (car on veut p premier) modulo 3 étant 1, 3 est un carré modulo p si et seulement si :

— $p \equiv 1\,[3]$ et $\dfrac{p-1}{2} \equiv 0\,[2]$, donc $\begin{cases} p \equiv 1\,[3] \\ p \equiv 1\,[4] \end{cases}$, donc $p \equiv 1\,[12]$ par le théorème des restes chinois ;

— **ou** $p \equiv 2\,[3]$ et $\dfrac{p-1}{2} \equiv 1\,[2]$, donc $\begin{cases} p \equiv 2\,[3] \equiv -1\,[3] \\ p \equiv 3\,[4] \equiv -1\,[3] \end{cases}$, donc $p \equiv -1\,[12]$ par le théorème des restes chinois.

Examinons maintenant M_q **modulo** 12 pour q nombre premier (d'après la remarque) impair. On a $2^{2\times1+1}-1=7$, puis, par récurrence :

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

On a donc $M_{2r+1}\equiv 7\,[12]$ pour $r\in\mathbb{N}^*$, donc $M_q\equiv 7\,[12]$ pour $q\in\mathcal{P}\backslash\{2\}$.

Ainsi, 3 n'est pas un carré modulo M_q, ce qui montre que $\mathcal{A}$ est un corps. La classe de X dans $\mathcal{A}$ est alors une racine de 3, que l'on note $\sqrt{3}$.

On a $2M_q\equiv 0\,[M_q]$, donc $2^{q+1}\equiv 2\,[M_q]$, donc $2^{\frac{q+1}{2}}$ (q est bien impair) est une racine de 2 dans $\mathbb{Z}/M_q\mathbb{Z}$, que l'on note $\sqrt{2}$.

On peut donc définir dans $\mathcal{A}$:

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

Comme 3 n'est pas un carré modulo M_q, on a dans $\mathcal{A}$:

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

Ainsi, $\mathcal{A}$ étant de caractéristique M_q, pour tout $(a,b)\in\mathbb{Z}/M_q\mathbb{Z}$, on a :

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

C'est en particulier le cas pour $a\in\{\sqrt{2},1\}$ et $b\in\{0,1\}$, donc :

$$\rho^{M_q}=\overline{\rho}.$$

On remarque que $\rho^2=2+\sqrt{3}$ et que $\rho\overline{\rho}=-1$. Il vient donc :

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

On a donc bien le sens direct.

Supposons à présent $\left(2+\sqrt{3}\right)^{2^{q-1}}\equiv -1\,[M_q]$, où on se place dans une extension $\mathcal{A}$ de $\mathbb{Z}/M_q\mathbb{Z}$ contenant une racine de 3, notée $\sqrt{3}$. Si 3 est un carré modulo M_q, on prend $\mathcal{A}=\mathbb{Z}/M_q\mathbb{Z}$, sinon, on reprends $\mathcal{A}=(\mathbb{Z}/M_q\mathbb{Z})/\langle X^2-3\rangle$.

Par l'absurde, supposons $M_q\notin\mathcal{P}$ et donnons-nous $p\in\mathcal{P}$ un de ses diviseurs (on a $p\neq 2$). C'est donc un diviseur de 0 dans $\mathcal{A}$ donc p n'est pas inversible. Il est donc contenu dans un idéal maximal $\mathcal{M}$ de $\mathcal{A}$ (En effet, p est non-inversible, donc l'idéal engendré par p est propre. On peut conclure par le théorème de KRULL (équivalent à l'axiome du choix, se démontre en

prenant l'union de chaînes (pour l'inclusion) d'idéaux propres, et par utilisation du lemme de Zorn)). Ainsi, $\mathcal{A}/\mathcal{M}$ est un corps de caractéristique divisant p (car $p \in \mathcal{M}$), donc égale à p (car p est premier), donc $\mathcal{A}/\mathcal{M}$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Soient α et β les classes de $2+\sqrt{3}$ et $2-\sqrt{3}$. On a $\alpha^{2^{q-1}} \equiv -1\,[M_q]$, donc α est d'ordre 2^q dans $\mathcal{A}/\mathcal{M} \cong \mathbb{Z}/p\mathbb{Z}$ (car p est impair).

On a $Q = (Y-\alpha)(Y-\beta) = Y^2 - 4Y + 1 \in \mathcal{A}/\mathcal{M}[Y] \cong \mathbb{Z}/p\mathbb{Z}\,[Y]$. Ainsi, α est racine de Q, donc α^p aussi, donc $\alpha^p = \alpha$ ou $\alpha^p = \beta$.

Si $\alpha^p = \alpha$, alors $2^q | \, p-1$. Comme $p \,| M_q$, $p < M_q$, donc c'est absurde. On a donc $\alpha^p = \beta = \alpha^{-1} = \alpha^{M_q}$. Donc $p \equiv 2^q - 1\,[2^q]$, donc $p = 2^q - 1 = M_q$, ce qui est absurde. Donc M_q est premier, ce qui termine la preuve.

□