# Dév. ⑤ – Test de primalité des nombres de Mersenne

Leçons 120 Anneaux $\mathbb{Z}/n\mathbb{Z}$
121 Nombres premiers
123 Corps finis
141 Polynômes irréd. Corps de rupture

Réf : Gaux-Picard
Corps finis, etc.

**Thm :** On note $M_q := 2^q - 1$. $M_q$, $q$ impair, est premier ssi

$$(2+\sqrt{3})^{2^{q-1}} \equiv -1 \quad [M_q]$$

Rqe : On se placera bien sûr dans une extension de $\mathbb{Z}/M_q\mathbb{Z}$ contenant une racine carrée de 3...

$\boxed{\Rightarrow}$ Supp. $M_q$ premier ($q$ impair)

(1) On se place dans l'extension qui va bien.

→ 3 est pas résidu quadratique mod $M_q$ :

Remarquons qu'un $M_q$ est $\equiv 7\ [12]$ :
$M_3 = 7$, $M_{2k+1} \equiv 7\ [12] \Rightarrow M_{2k+3} \equiv 4 \cdot 2^{2k+1} - 1 \equiv 4\cdot(2^{k+1}-1) + 3$
$\equiv 4\times 7 + 3 \equiv 7 \quad [12]$.

Or 3 est résidu quadratique mod $p$ ssi $p \equiv \pm 1\ [12]$ :
$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}$ d'où 3 résidu quad. mod $p$ ssi $\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}$

ssi $\begin{cases} p \equiv 1\ (3),\ \frac{p-1}{2} \text{ pair} \\ \text{ou} \\ p \equiv 2\ (3),\ \frac{p-1}{2} \text{ impair} \end{cases}$

ssi $\begin{cases} p \equiv 1\ [12] \\ \text{ou} \\ p \equiv -1\ [12] \end{cases}$

→ 2 est un résidu quadratique mod $M_q$ :
$2(\underbrace{2^q - 1}_{M_q}) \equiv 0\ [M_q]$, d'où $2^{q+1} \equiv 2\ [M_q]$,
on notera $\sqrt{2}$ pour $2^{\frac{q+1}{2}}$.

→ 3 n'est pas résidu quadratique

⇒ $x^2-3$ est irréductible

⇒ $\mathbb{k} = \mathbb{Z}/M_q\mathbb{Z}[X]/(X^2-3)$ est un corps.

$\overline{X} \in \mathbb{k}$ est une racine de 3, on la notera $\sqrt{3}$.

(2) On calcule $(2+\sqrt{3})^{2^{q-1}}$.

On pose $\rho = \frac{1+\sqrt{3}}{\sqrt{2}}$, $\overline{\rho} = \frac{1-\sqrt{3}}{\sqrt{2}} \in \mathbb{k}$.

$$(2+\sqrt{3})^{2^{q-1}} = (\rho^2)^{2^{q-1}} \quad \text{car } \rho^2 = 2+\sqrt{3}$$

$$= \rho \times \rho^{M_q}$$

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

$$= \rho \left(\left(\frac{1}{\sqrt{2}}\right)^{M_q} + \left(\frac{\sqrt{3}}{\sqrt{2}}\right)^{M_q}\right) \quad \text{car } \mathbb{k} \text{ est de caractéristique } M_q$$

$$= \rho \left(\frac{1}{\sqrt{2}} + \frac{-\sqrt{3}}{\sqrt{2}}\right) \quad \text{car } (\sqrt{2})^{M_q} = \sqrt{2}$$

$(\sqrt{3})^{M_q} = 3^{(M_q-1)/2} \times \sqrt{3}$ et comme $3^{M_q-1} = 1$, $3^{(M_q-1)/2} = \pm 1$ mais comme 3 n'est pas résidu quadratique, c'est $-1$

$= -\sqrt{3}$

$$= \rho\overline{\rho}$$

$$= -1 .$$

□