. Primalité des nombres de Mersenne : 120, 121, 125, 141

Nombres de Mersenne : $M_q = 2^q - 1$

Lemme : M^q premier $\Rightarrow$ q premier

preuve : si $q = mn$ avec $m, n \geq 2$ alors $M_q = 2^{mn} - 1$, divisible par $2^m - 1$

Théorème : pour tout premier impair q, on a

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

Rmq : on doit se placer dans un corps où 3 admet une racine carrée.

$\Rightarrow$) On utilise le lemme suivant

Lemme 1 : $\forall k \in \mathbb{N}^*$, $M_{2k+1} \equiv 7 \; [12]$

démo : par récurrence (ok si $k=1$) $2^{2(k+1)+1} - 1 \equiv 4 \times 2^{2k+1} - 1 \equiv (2^{2k+1} - 1) \times 4 + 3 \equiv 7 \times 4 + 3 \equiv 7 \; [12]$

Montrons que 3 n'est pas un résidu quadratique modulo M_q, on utilise le lemme suivant

Lemme 2 : si p est premier, 3 est résidu quadratique modulo p ssi $p \equiv \pm 1 \; [12]$

démo : on a $\left(\frac{p}{3}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}$ (réciprocité quadratique)

et donc par définition 3 est résidu quadratique modulo p ssi $\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}$

ssi $[p \equiv 1 \; [3]$ et $\frac{p-1}{2}$ pair$]$ ou $[p \equiv 2 \; [3]$ et $\frac{p-1}{2}$ impair$]$ (le seul carré de $\mathbb{F}_3$ est 1)

ssi $[p \equiv 1 \; [3]$ et $p \equiv 1 \; [4]]$ ou $[p \equiv 2 \; [3]$ et $p \equiv 3 \; [4]]$

ssi $p \equiv \pm 1 \; [12]$ (thm chinois).

Comme M_q n'est pas congru à ± 1 mod (12) (lemme 1), 3 n'est pas un carré modulo M_q (lemme 2). $X^2 - 3$ est donc irréductible sur $\mathbb{F}_{M_q}$: $A = \frac{\mathbb{F}_{M_q}[X]}{X^2 - 3}$ est un corps et on note $\sqrt{3}$ la classe de X dans le quotient.

De plus $2^{q+1} \equiv 2 \; [M_q]$ donc 2 admet une racine carrée : $\sqrt{2} := 2^{\frac{q+1}{2}}$

On définit les éléments $\ell, \bar{\ell} \in A$: $\ell = \frac{1+\sqrt{3}}{\sqrt{2}}$, $\bar{\ell} = \frac{1-\sqrt{3}}{\sqrt{2}}$

alors $\ell^2 = 2 + \sqrt{3}$ et $\ell\bar{\ell} = -1$. bien défini

De plus, $(\sqrt{3})^{M_q} = \sqrt{3}^{M_q - 1}\sqrt{3} = 3^{\frac{M_q - 1}{2}}\sqrt{3} = -\sqrt{3}$ dans $\mathbb{F}_{M_q}$ (Fermat)

Comme $\mathrm{Car}(A) = M_q$, on a $(a + b\sqrt{3})^{M_q} = a - b\sqrt{3}$ dans A, $\forall a, b \in \mathbb{F}_{M_q}$

De même, $\sqrt{2}^{M_q} = \sqrt{2}$ et $\ell^{M_q} = \bar{\ell}$

$\rightarrow (2+\sqrt{3})^{2^{q-1}} = (2+\sqrt{3})^{\frac{M_q+1}{2}} = (\ell^2)^{\frac{M_q+1}{2}} = \ell\bar{\ell} = -1$

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

$\Leftarrow$ Si $\mathbb{Z}/M_q\mathbb{Z}$ contient une racine de 3, on pose $\mathcal{A} = \mathbb{Z}/M_q\mathbb{Z}$, sinon on prend $\mathcal{A} = \mathbb{Z}/M_q\mathbb{Z}[X]/(X^2-3)$. En bref : 3 admet admet une racine dans l'extension d'anneaux $\mathcal{A}$.

Par l'absurde, supposons M_q non premier et soit p un diviseur premier de M_q.

p est un diviseur de 0 dans $\mathcal{A}$, donc n'y est pas inversible. Il existe donc un idéal maximal de $\mathcal{A}$ contenant p, notons le $\mathcal{M}$.

Alors $\mathcal{A}/\mathcal{M}$ est un <u>corps</u> de caractéristique p $(p \neq 0)$

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

Par hypothèse, on a $\alpha^{2^{q-1}} \equiv -1\ [M_q]$ et donc α est d'ordre 2^q dans $\mathcal{A}/\mathcal{M}$.

Posons $Q = (X-\alpha)(X-\beta) = X^2-4X+1 \in \mathcal{A}/\mathcal{M}[X]$ à priori, mais est à coefficients dans le sous-corps premier de $\mathcal{A}/\mathcal{M}$: $\mathbb{F}_p$.

Comme α est racine de Q, α^p l'est aussi dans $\mathcal{A}/\mathcal{M}$. Donc $\alpha^p = \alpha$ ou $\alpha^p = \beta$.

<u>si $\alpha^p = \alpha$</u> : comme α est d'ordre 2^q, on a $2^q \mid p-1$, or $p \mid M_q = 2^q-1$

donc $p < 2^q$: absurde.

<u>si $\alpha^p = \beta$</u> : alors $\alpha^p = \beta = \alpha^{-1} = \alpha^{M_q}$. Alors $p \equiv \underbrace{2^q-1}_{M_q}\ [2^q]$ car α est d'ordre 2^q

donc nécessairement $p = M_q$: absurde.
($M_q < 2^q$ et $p \mid M_q$)

donc <u>M_q est premier</u>

On a comme corollaire direct un algorithme de test de primalité :

<u>Théorème</u> : (Test de Lehmer-Lucas)

On définit la suite $(L_n)_{n \geq 0} \in (\mathbb{Z}/M_q\mathbb{Z})^{\mathbb{N}}$ par

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

alors M_q premier <u>ssi</u> $L_{q-2} \equiv 0\ [M_q]$