Ref: Saux Picart, Cours de Calcul formel, corps finis, systèmes polynomiaux p. 80

Développement: Test de Lehmer-Lucas (nombres de Mersenne)

Leçons: 120, 121, 125, 141, 127

On appelle q-ième nombre de Mersenne le nombre $M_q = 2^q - 1$
On définit la suite $(L_n)_{n\in\mathbb{N}}$ par $\begin{cases} L_0 = 4 \\ L_{n+1} = L_n^2 - 2 \end{cases}$

Théorème (Test de Lehmer-Lucas)
Soit q un nombre premier impair. Alors M_q est premier si et seulement si $L_{q-2} \equiv 0 \bmod M_q$.

Preuve:

- rq: M_q premier $\Rightarrow q$ premier (si $q = mn$, alors $2^q - 1 = (2^m - 1)(2^{m(n-1)} + \dots)$) mais la réciproque est fausse : $M_{11} = 2047 = 23 \times 89$.

- $M_q \mid L_{q-2} = 0 \ [M] \iff (2+\sqrt{3})^{2^{q-1}} = -1 \ [M]$ (on note $M = M_q$)

Soit A une extension de $\mathbb{Z}/M\mathbb{Z}$ contenant une racine carrée de 3, notée $\sqrt{3}$ (si $\mathbb{Z}/M\mathbb{Z}$ contient une racine de 3, $A = \mathbb{Z}/M\mathbb{Z}$)

On pose $\alpha = 2 - \sqrt{3}$, $\beta = 2 + \sqrt{3}$ $\alpha, \beta \in A$ ($2 \neq 0$ car on est en car $q \geq 3$)
On a $\alpha + \beta = 4$, $\alpha\beta = 1$

* M_q $\forall n \in \mathbb{N}$ $L_n = \alpha^{2^n} + \beta^{2^n}$ par récurrence sur n.
- $L_0 = 4 = \alpha + \beta$ ok
- si ok en n, $\alpha^{2^{n+1}} + \beta^{2^{n+1}} = \left(\alpha^{2^n} + \beta^{2^n}\right)^2 - 2(\alpha\beta)^{2^n}$
$= (\alpha^{2^n} + \beta^{2^n})^2 - 2$
(on identifie L_n et $\bar{L}_n$ de $\mathbb{Z}/M\mathbb{Z}$) (HR) $= L_n^2 - 2$
$= L_{n+1}$

$* L_{q-2} \equiv 0 [M] \iff \alpha^{2^{q-2}} = -\beta^{2^{q-2}} [M]$

$\iff \alpha^{2^{q-1}} = -(\alpha\beta)^{2^{q-2}} = -1 [M]$

(multiplié par $\alpha^{2^{q-2}}$ et $\alpha\beta = 1$)

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

☑ M_q M premier $\Rightarrow (2+\sqrt{3})^{2^{q-1}} = -1 [M]$

i.e. $\alpha^{2^{q-1}} = -1 [M]$

$* M_q \equiv 7 [12]$ par récurrence q impair :

- $2^{2\times 1+1} - 1 = 7 \equiv 7 [12]$
- si ok pour M_{2k+1} $2^{2(k+1)+1} - 1 = 4\times 2^{2k+1} - 1$

$= 4(2^{k+1} - 1) + 3$ (HR)

$\equiv 4\times 7 + 3 [12]$

$= 7 [12]$

$* \left(\frac{3}{M}\right) = -1$ i.e. 3 n'est pas résidu quadratique mod M.

Soit p premier, $p \geq 5$ LRQ : $\left(\frac{p}{3}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}\frac{3-1}{2}} = (-1)^{\frac{p-1}{2}}$

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

$\iff$ $p \equiv 1 [3]$ → carré et $\left(\frac{p}{3}\right) = (-1)^{(p-1)/2}$ ou $p \equiv -1 [3]$ → non carré et $\left(\frac{p}{3}\right) = (-1)^{(p-1)/2}$

$\iff$ $p \equiv 1 [3]$ et $(p-1)/2$ pair ou $p \equiv -1 [3]$ et $(p-1)/2$ impair

$\iff$ $p \equiv 1 [3]$ et $p \equiv 1 [4]$ ou $p \equiv -1 [3]$ et $p \equiv -1 [4]$

$\iff p \equiv 1 \bmod 12$ ou $p \equiv -1 [12]$

Comme $M \equiv 7 [12]$, $M \not\equiv \pm 1 [12]$ donc 3 est non carré mod M.

* 2 est carré mod M $0 \bmod M = 2M = 2(2^q - 1) = 2^{q+1} - 2$

donc $2^{q+1} = 2 [M]$ et donc $2^{(q+1)/2}$ racine carrée de 2 dans $\mathbb{Z}/M\mathbb{Z}$, noté $\sqrt{2}$.

On note $A = \mathbb{F}_M[X]/(X^2-3)$, c'est un corps ($X^2-3$ est irréductible sur A (d°2, sans racines ds le corps $\mathbb{F}_M$) donc (X^2-3) est maximal) et contient $\sqrt{3}$ une racine carré de 3.

On pose $\rho = \frac{1+\sqrt{3}}{\sqrt{2}}$, $\bar{\rho} = \frac{1-\sqrt{3}}{\sqrt{2}}$ éléments de A.

On a $\boxed{\rho^2 = \alpha \text{ et } \rho\bar{\rho} = -1}$

$$\alpha^{2^{q-1}} = \alpha^{(M+1)/2} = (\rho^2)^{(M+1)/2} = \rho^{M+1} = \rho\rho^M$$

On $\rho^M = \frac{(1+\sqrt{3})^M}{\sqrt{2}^M} = \frac{1+\sqrt{3}^M}{\sqrt{2}}$ ($\sqrt{2} \in \mathbb{F}_M$ donc $\sqrt{2}^M = \sqrt{2}$, $x \mapsto x^M$ est le Frob)

et $(\sqrt{3})^M = (\sqrt{3})^{M-1}\sqrt{3} = (\sqrt{3}^2)^{(M-1)/2}\sqrt{3} = 3^{(M-1)/2}\sqrt{3} = \left(\frac{3}{M}\right)\sqrt{3}$

$= -\sqrt{3}$

Donc $\rho^M = \bar{\rho}$. Finalement $\alpha^{2^{q-1}} = \rho\rho^M = \rho\bar{\rho} = -1$

On a bien $(2+\sqrt{3})^{2^{q-1}} = -1$ ds A. En particulier, $\alpha^{2^{q-1}} \in \mathbb{F}_M$ et $(2+\sqrt{3})^{2^{q-1}}$ est congru à -1 mod M.

■ M_q $(2+\sqrt{3})^{2^{q-1}} = -1 [M] \Rightarrow$ M premier

Comme au début A est une extension (finie) de $\mathbb{Z}/M\mathbb{Z}$ contenant une racine carrée de 3 notée $\sqrt{3}$. Si M n'est pas premier, soit $p \mid M$,

rq: A est fini, c'est $\mathbb{Z}/M\mathbb{Z}$ ou $\mathbb{Z}/M\mathbb{Z}[X]/(X^2-3)$

(impair)

p premier. p est un diviseur de zéro dans $\mathbb{Z}/M\mathbb{Z}$ donc dans A aussi donc $p \notin A^\times$ (et $p \neq 0$ ds A car $\neq 0$ ds $\mathbb{Z}/M\mathbb{Z}$).

Soit $M \subset A$ un idéal maximal contenant p (cf rq pour la preuve de l'existence de M)

A/M est un corps et $\mathrm{car}(A/M) = p$ (elle div. p car $p = 0$ ds A/M ~~elle est $\neq 0$ car A/M fini (A fini)~~ et $p\,1^{(m)}$)

On note encore α, β les classes de $\alpha\ 2+\sqrt{3}, 2-\sqrt{3}$ dans A/M.

Puisque $\alpha^{2^{q-1}} = -1\ [M]$, α est d'ordre exactement 2^q dans $(A/M)^*$ ($1 \neq -1$ car caract. impaire)

Soit $Q = (X-\alpha)(X-\beta) = X^2 - 4X + 1 \in$ sous-corps 1^{er} de A/M, qui est isom à $\mathbb{F}_p$.

On a donc $Q(\alpha^p) = Q(\alpha)^p = 0$ (Frobenius)

α^p est racine de Q donc soit $\alpha^p = \alpha$ soit $\alpha^p = \beta$

- si $\alpha^p = \alpha$, $\alpha^{p-1} = 1$ donc $2^q \mid p-1$ mais $p \mid 2^q - 1$ donc $p < 2^q$ ↯
- si $\alpha^p = \beta$, $\alpha^p = \beta = \alpha^{-1} = \alpha^{2^q - 1} = \alpha^{M_q}$ donc

$p \equiv M_q \bmod (2^q)$.

$\equiv 2^q - 1 \bmod (2^q)$

$= -1\ [2^q]$ i.e. $2^q \mid p+1$

$2^q \leq p+1$ donc $M = 2^q - 1 \leq p$

On $p \mid M$ donc $p = M$ ↯

C'est donc que M est premier.

(cf verso)

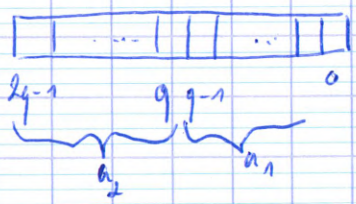
Remarques :

- Soit A un anneau (commutatif unitaire), $I \subset A$ un idéal propre (i.e. $I \neq \{0\}$, $I \neq A$). Alors si A/I est fini, il existe un idéal maximal J de A contenant I.
En effet les idéaux de A contenant sont en bijection avec ceux de A/I qui sont en nombre fini. Soit J l'idéal engendré par l'union (finie) des idéaux de A contenant I.
$J \supset I$ (clair) et J ~~maximal~~ : si $J \subsetneq L \subsetneq A$ (L idéal), $L \supset I$ donc $L \subset J$ et $L = J$ ↳ on a pas forcément $J \neq A$!!!

- Cette propriété reste vraie si A/I n'est pas fini (c'est le théorème de Krull), la preuve fait alors appel à l'axiome du choix.

- La réduction modulo $2^q - 1$ est facile en machine : si $a = \sum_{i=0}^{k} \varepsilon_i 2^i$ où $\varepsilon_i \in \{0,1\}$ $\forall i$. Prenons $k = 2q-1$ pour simplifier. $a = \underbrace{\sum_{i=0}^{q-1} \varepsilon_i 2^i}_{a_1} + 2^q \underbrace{\sum_{i=0}^{q-1} \varepsilon_{i+q} 2^i}_{a_2}$. Comme $2^q \equiv 1 \,[2^q - 1]$,

$a \equiv a_1 + a_2 \bmod (2^q - 1)$. Pour réduire a, il suffit de couper son écriture en blocs de longueur q et de faire la somme bit à bit.



$a = a_1 + a_2 \,[2^q - 1]$ (c'est facile)

- Le test consiste à calculer itérativement les valeurs de $(L_n)_{n \in \mathbb{N}}$ jusqu'à L_{q-2}. Les calculs se font dans $\mathbb{Z}/M\mathbb{Z}$.

Il faut de l'ordre de $O(q)$ opérations dans $\mathbb{Z}/M\mathbb{Z}$ (il y a une mise au carré et 1 soustraction par étape). Une op. dans $\mathbb{Z}/M\mathbb{Z}$ coûte $O((\log M)^2) = O(q^2)$. Le test est donc en $O(q^3)$

Si A anneau, $I \subset A$ idéal. Si A/I fini, $\exists$ J idéal max. de A tq $I \subseteq J$.

$\mathcal{E} = \{ J \text{ idéal de } A \mid I \subseteq J, J \neq A \} \xrightarrow[\text{bij}]{} \{ K \text{ idéal de } A/I \}$ → fini

$|\mathcal{E}|$ fini, $\mathcal{E}$ ordonné donc admet un plus grand élément, noté J. J est maximal.

⚠⚠ introduire $A = \mathbb{Z}/m\mathbb{Z}[X]/(X^2-3)$ au début de la preuve et ne faire que des calculs dans A.