Nombres de Mersenne et test de Lucas-Lehmer

Introduction

Cette version contient un raccourci (voir la remarque I.0.2) permettant de présenter l'application qui est le test de Lehmer-Lucas. Il semble possible de tout faire à part le lemme I.0.1 et la complexité (qui ne sont pas très importants, peuvent aller avant et après dans le plan).

Dans cette version, je prends également le temps de définir proprement ce qu'on va signifier par $\sqrt{3}$. C'est presque toujours mal fait (même dans le Saux-Picard-Rannou), et il est temps que ça change.

À partir de maintenant, $\boxed{\text{que } M_q \text{ soit premier ou non}}$, on va poser $\mathcal{A}_q = (\mathbb{Z}/M_q\mathbb{Z})[T]/(T^2-3)$. On écrit $\sqrt{3}$ la classe de T. On veut donc prouver le :

Théorème .0.1.
Si $q \geqslant 3$ impair, alors M_q est premier si et seulement si $(2+\sqrt{3})^{2^{q-1}} = -1$ dans $\mathcal{A}_q$.

I. L'entier 3 n'est pas un carré modulo un nombre premier de Mersenne

Lemme I.0.1. Ne fait pas partie du développement
Si $M_q = 2^q - 1$ est premier, alors q aussi.

Preuve. Si $d \mid q$, alors $2^d - 1 \mid 2^q - 1$. □

On peut ne s'intéresser qu'à $q \geqslant 3$ impair. Comme q est impair, $(-1)^q = -1$ donc $2^q = 2[3]$. Donc $M_q = 1[3]$ est un carré donc, en écrivant $p = M_q$, on a $\left(\frac{p}{3}\right) = 1$. Or, par le théorème de la réciprocité quadratique, $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{3-1}{2}\frac{M_q-1}{2}}$. Or, $\frac{M_q-1}{2} = \frac{2^q-2}{2} = 2^{q-1} - 1$ est impair donc $\left(\frac{3}{p}\right) = -1$.

On note la conséquence qui est que, si $p = M_q$ est premier, alors $3^{\frac{p-1}{2}} = -1$ d'où $\boxed{\sqrt{3}^{p-1} = -1}$.

Remarque I.0.2. On peut carrément caractériser les nombres premiers p tels que 3 est un carré mod p. C'est si et seulement si $p = \pm 1[12]$ (utiliser résidus et lemme chinois). En outre, si q est impair, une récurrence immédiate montre que $M_q \equiv 7[12]$. Cela prouve que 3 n'est jamais carré modulo M_q (quand il est premier). Ce passage ne fait pas partie du développement sauf si on veut insister dessus par rapport à la leçon (pour la leçon 120 à l'extrême limite). Je déconseille de faire ce passage car il est un peu chronophage et empêche de faire le test de Lucas-Lehmer.

Remarque : *Si M_q est premier, $\mathcal{A}_q$ est donc strictement plus gros que $\mathbb{Z}/M_q\mathbb{Z}$, et c'est une extension de corps de degré 2.*

II. L'entier 2 est carré modulo tout nombre de Mersenne

Bah alors là c'est juste $M_q = 0[M_q]$, donc $2^{q+1} = 2[M_q]$, et sous l'hypothèse que q est impair... On écrit $\sqrt{2}$ une racine de 2 dans $\mathbb{Z}/M_q\mathbb{Z}$.

Une conséquence est que, quand $M_q = p$ est premier, on a $\boxed{\sqrt{2}^{M_q} = \sqrt{2}}$.

III. Condition nécessaire à la primalité

Si $p = M_q$ est premier, alors $\mathcal{A}_q$ est un corps donc on peut poser $\rho = \frac{1+\sqrt{3}}{\sqrt{2}}$ et ρ' son $\mathbb{F}_{M_q}$-conjugué. Alors $\rho^2 = 2+\sqrt{3}$ et $\rho\rho' = -1$. Alors on est armés pour calculer ce qu'on voulait calculer : $(2+\sqrt{3})^{2^{q-1}} = \rho^{2^q} = \rho^{M_q}\rho = \rho\frac{1}{\sqrt{2}^{M_q}}\left(\sqrt{3}^{M_q}+1\right)$. Mais $\sqrt{3}^{M_q} = -\sqrt{3}$, donc $(2+\sqrt{3})^{2^{q-1}} = \rho\frac{1-\sqrt{3}}{\sqrt{2}} = \rho\rho' = -1$.

Contactez-moi en cas de coquille s'il vous plaît ! prenom.nom@ens-lyon.fr

IV. Condition suffisante à la primalité

Si $p \mid M_q$ est un facteur premier de M_q, alors p divise 0 dans $\mathcal{A}_q$ donc il existe un idéal maximal de $\mathcal{A}_q$ contenant p noté m.[1] $p \in m$ donc $p = 0$ dans $\Bbbk := \mathcal{A}_q/m$ donc $\Bbbk$ est un corps de caractéristique p.[2] On pose $\alpha = 2 + \sqrt{3}$, $\beta = 2 - \sqrt{3}$. On a $\alpha\beta = 1$. Or, $\alpha^{2^{q-1}} = -1 \neq 1$ car p est impair car M_q l'est. Donc l'ordre de α dans $\Bbbk^*$ est exactement $2^q = M_q + 1$.[3]

On pose, dans $\Bbbk[X]$, $Q(X) = (X - \alpha)(X - \beta) = X^2 - 4X + 1$ qui est donc à coefficients dans $\mathbb{F}_p \hookrightarrow \Bbbk$. Donc Q est invariant par le morphisme de Frobenius dans $\Bbbk$ donc ses racines sont permutées par celui-ci, donc $\alpha^p = \alpha$ ou β. Dans le cas où $\alpha^p = \alpha$, on trouve que $2^q \mid p - 1$ vu son ordre ce qui est contradictoire car $p - 1 < 2^q$. Ainsi, $\alpha^p = \beta = \alpha^{-1}$ donc $2^q \mid p + 1 = 2^q$ d'où l'égalité donc M_q est premier.

V. Test de Lucas-Lehmer

Soit $q \geqslant 3$ impair fixé.

Définition V.0.1. On pose $L_0 = 4 \in \mathbb{Z}/M_q\mathbb{Z}$ et, pour $n \geqslant 0$, $L_{n+1} = L_n^2 - 2$.

Théorème V.0.2.
M_q est premier si et seulement si $L_{q-2} = 0$.

Preuve. Comme éléments de $\mathcal{A}_q$, on pose $\alpha = 2 + \sqrt{3}$, $\beta = 2 - \sqrt{3}$, $\alpha\beta = 1$. On montre par récurrence que $L_n = \alpha^{2^n} + \alpha^{-2^n}$. $n = 0$: $L_0 = 4$ et $\alpha^1 + \beta^1 = 4$. Si $n \geqslant 0$, si $L_n = \alpha^{2^n} + \alpha^{-2^n}$, alors $L_{n+1} = \alpha^{2^{n+1}} + \alpha^{-2^{n+1}} + 2 - 2$. Donc à présent : $L_{q-2} = 0$ si et seulement si $\alpha^{2^{q-2}} = -\alpha^{-2^{q-2}}$ si et seulement si $\alpha^{2^{q-1}} = -1$. □

Remarque V.0.3. Le test peut donc se faire en $O(q^3)$: chaque mise au carré prend $O(\log(M_q)^2)$ soit $O(q^2)$, et il faut faire ça q fois.

1. m existe car c'est un anneau fini ! Je vous recommande de quand même connaître le théorème de Krull (lemme de Zorn).
2. Dès qu'un nombre premier est nul dans un corps, ça veut dire que ce corps l'a pour caractéristique.
3. En effet, en mettant au carré, on voit que l'ordre est une puissance de 2, et COMME $-1 \neq 1$!!! ça ne peut pas être une puissance inférieure.

Contactez-moi en cas de coquille s'il vous plaît ! prenom.nom@ens-lyon.fr