Master1, mathématiques
Algèbre 1

Devoir à la maison n° 2
à rendre la semaine du 18 novembre 2003

Soient s un entier impair ≥ 1 et L_i, $i \geq 1$, la suite d'entiers définie par

$$L_1 = 4\,,\; L_{i+1} = L_i^2 - 2\,,\; i \geq 1\,.$$

On propose de montrer le *critère de Lucas–Lehmer* qui affirme que le nombre de Mersenne $M_s = 2^s - 1$ est premier si et seulement si on a $L_{s-1} \equiv 0\,(M_s)$.

1. Calculer la suite des L_i modulo M_s $(i < s)$ pour $s = 7$ et $s = 11$. Vérifier le critère dans ces cas.

2. On considère le sous–anneau $A = \mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \,|\, a, b \in \mathbb{Z}\}$ de $\mathbb{R}$. On note $x = 2 + \sqrt{3}$.

a) Montrer que x est inversible dans A, d'inverse $x^{-1} = 2 - \sqrt{3}$.

b) Montrer que $\forall i \geq 1\,,\; L_i = x^{(2^{i-1})} + x^{-(2^{i-1})}$.

3. Suffisance de la condition On suppose que $L_{s-1} \equiv 0\,(M_s)$ et que M_s n'est pas premier. On note p un facteur premier de M_s inférieur ou égal à $\sqrt{M_s}$. L'entier p engendre un idéal propre (p) de A.

a) Montrer que $x^{(2^{s-1})} \equiv -1 \bmod (p)$.

b) On note G le groupe des éléments inversibles de l'anneau quotient $A/(p)$. Montrer que la classe $\overline{x}$ de x dans G est d'ordre 2^s.

c) Majorer l'ordre de G de manière à aboutir à une contradiction.

4. Nécessité de la condition On garde les notations de l'introduction et de 2) et on suppose que l'entier $p = M_s = 2^s - 1$ est premier.

a) Etudier la classe de p modulo 8 et modulo 12 et en déduire les valeurs de $2^{(p-1)/2}$ et $3^{(p-1)/2}$ modulo p.

b) Vérifier que $2x = (1+\sqrt{3})^2$, $2x^{-1} = (1-\sqrt{3})^2$, et montrer que *dans* A

$$2^{(p+1)/2} L_s = (1+\sqrt{3})^{p+1} + (1-\sqrt{3})^{p+1} \equiv 2[1 + (\sqrt{3})^{p+1}] = 2[1 + 3^{(p+1)/2}] \bmod (p).$$

c) Conclure qu'on a $L_s \equiv -2\,(p)$ et $L_{s-1} \equiv 0\,(p)$ (congruences *dans* $\mathbb{Z}$).

******