Université Paris 7
U.F.R. de Mathématiques

8 décembre 1996
B. Keller

D.E.U.G. Mathématiques : MT 282

Devoir à la maison

(à rendre a semaine du 13 janvier)

Soit s un entier impair > 1, $n = 2^s - 1$ et L_i, $i \geq 1$, la suite d'entiers modulo n définie par

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

Le *critère de Lucas-Lehmer* affirme que

$$2^s - 1 \textit{ est premier si et seulement si } L_{s-1} \equiv 0\ (n).$$

Dans ce cas, le nombre $2^s - 1$ est appelé un *nombre premier de Mersenne*. Actuellement (décembre 1996), le plus grand nombre premier connu est le nombre premier de Mersenne

$$2^{1398269} - 1.$$

1) **Comprendre le critère.**

   a) Calculer la suite des L_i pour $s = 5$ et $s = 11$. Conclusion ?

   b) (facultatif) Quelle est la classe de L_{s-1} modulo $2^s - 1$ obtenue à l'aide de votre calculette pour $s = 13, 17, 19, 31, 61, 89, 107$? Si votre calculette est assez performante, vous trouvez 0 pour toutes ces valeurs de s. Comment s'expliquent les résultats différents de 0 obtenus sur des calculettes moins performantes ?

2) **Suffisance de la condition.** Supposons que $L_{s-1} \equiv 0\ (n)$. Nous voulons montrer que n est premier. Soit p un facteur premier de n. Notons A l'anneau quotient de $\mathbf{F}_p[X]$ par l'idéal engendré par $X^2 - 4X + 1$ et x l'image de X dans A.

   a) Montrer que x est inversible dans A et qu'on a $x + x^{-1} = 4$.

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

   c) Montrer que $x^{(2^{s-1})} + x^{-(2^{s-1})} \neq 2$, et que $x^{(2^s)} + x^{-(2^s)} = 2$ dans A.

   d) Montrer que pour $a \in A$, on a $a^2 = 0$ ssi $a = 0$. Indication : on distinguera deux cas suivant que $X^2 - 4X + 1$ est irréductible ou non.

   e) Soit $m \in \mathbf{N}$. Montrer qu'on a $x^m + x^{-m} = 2$ ssi $x^m = 1$. Indication : Considérer $a = x^m - 1$.

   f) Montrer que x est d'ordre 2^s dans le groupe A^*.

   g) Supposons le polynôme $X^2 - 4X + 1$ réductible sur $\mathbf{F}_p$. Montrer qu'on a $x^{p-1} = 1$.

h) Supposons le polynôme $X^2 - 4X + 1$ irréductible sur $\mathbf{F}_p$. Montrer qu'on a $x^p + x^{-p} = 4$. En déduire qu'on a $x^{p-1} = 1$ ou $x^{p+1} = 1$.

i) Montrer que $p = 2^s - 1$.

3) **Sur les carrés de $\mathbf{F}_p$.** Soit p un nombre premier impair.

a) Soit $a \in \mathbf{F}_p^*$. Montrer que $a^{(p-1)/2} = \pm 1$ Indication : considérer $u = a^{(p-1)/2}$ et son carré.

b) Montrer qu'un élément $a \in \mathbf{F}_p^*$ est le carré d'un élément de $\mathbf{F}_p^*$ ssi $a^{(p-1)/2} = 1$ et que $a^{(p-1)/2} = -1$ si a n'est pas un carré.

La 'loi de réciprocité quadratique' permet de montrer que 2 est un carré dans $\mathbf{F}_p$ ssi $p \equiv \pm 1$ (8) et que 3 est un carré dans $\mathbf{F}_p$ ssi $p \equiv \pm 1$ (12). On admettra ce fait qui sera utilisé dans 4).

4) **Nécessité de la condition.** Supposons que $p = 2^s - 1$ est premier. Gardons les notations A et x de la partie 2).

a) Montrer à l'aide de 3) b) et c) qu'on a $2^{(p-1)/2} = 1$ et $3^{(p-1)/2} = -1$ dans $\mathbf{F}_p$.

b) Posons $y = x - 2$. Montrer qu'on a $y^2 = 3$, $2x = (1 + y)^2$, $2x^{-1} = (1 - y)^2$ et

$$2^{(p+1)/2} L_s = (1 + y)^{p+1} + (1 - y)^{p+1} = 2(1 + y^{p+1}) = 2(1 + 3^{(p+1)/2}).$$

Indication : on utilisera que $(a + b)^{p+1} = (a + b)^p (a + b) = (a^p + b^p)(a + b)$ dans A.

c) Conclure qu'on a $L_s \equiv -2$ (p) et $L_{s-1} \equiv 0$ (p).