Université Paris 7
U.F.R. de Mathématiques

21 janvier 1997
B. Keller

**D.E.U.G. Mathématiques : MT 282**

**Corrigé du devoir à la maison de janvier 1997**

1) **Comprendre le critère.**

a) Pour $s = 5$, on trouve la suite $4, 14, 8, 0, -2, 2, 2, 2, \ldots$. En particulier $L_4 = 0$ en accord avec le fait que $2^5 - 1 = 31$ est premier. Pour $s = 11$, on trouve la suite $4, 14, 194, 788, 701, 119, 1877, 240, 282, 1736, \ldots$. En particulier, $L_{10} = 1736 \neq 0$ en accord avec le fait que $2^{11} - 1 = 2047 = 23 \times 89$ n'est pas premier.

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 $x + x^{-1} = 4$.* Dans $A$, on a $x^2 - 4x + 1 = 0$. Donc $x(4 - x) = 1$ dans $A$ et $x$ est inversible d'inverse $x^{-1} = 4 - x$ dans $A$. Il s'ensuit aussi que $x + x^{-1} = x + (4 - x) = 4$.

b) *Montrer que $L_i = x^{(2^{i-1})} + x^{-(2^{i-1})}$, $i \geq 1$.* Nous procédons par récurrence sur $i$. Nous avons bien $L_1 = 4 = x + x^{-1}$ d'après a). Supposons l'affirmation vraie au cran $i$. Alors nous avons

$$\begin{aligned} L_{i+1} &= L_i^2 - 2 = (x^{(2^{i-1})} + x^{-(2^{i-1})})^2 - 2 \\ &= x^{2^i} + x^{-2^i} + 2 - 2 = x^{2^i} + x^{-2^i}. \end{aligned}$$

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'après b), nous avons

$$x^{2^{s-1}} + x^{-2^{s-1}} = L_s.$$

Or $L_s = L_{s-1}^2 - 2 = -2$ d'après l'hypothèse. Comme $n$ est impair, nous avons $p \neq 2$ et donc $L_s = -2 \neq 2$. Finalement, nous avons

$$x^{2^s} + x^{-2^s} = L_{s+1} = L_s^2 - 2 = 4 - 2 = 2.$$

d) *Montrer que pour $a \in A$, on a $a^2 = 0$ ssi $a = 0$.* 1er cas : supposons que $X^2 - 4X + 1$ est irréductible. Alors $A$ est un corps. Donc $A$ est intègre, c'est-à-dire que $uv = 0$ implique $u = 0$ ou $v = 0$ dans $A$. En particulier $a^2 = 0$ implique $a = 0$ dans $A$.

2e cas : supposons que $X^2 - 4X + 1$ est réductible et qu'il admet deux racines distinctes $\alpha$ et $\beta$. Alors $X - \alpha$ et $X - \beta$ sont premiers entre eux et d'après le théorème chinois, nous avons un isomorphisme

$$A \xrightarrow{\sim} \mathbf{F}_p[X]/(X - \alpha) \times \mathbf{F}_p[X]/(X - \beta).$$

Nous savons aussi que $\mathbf{F}_p[X]/(X-\alpha)$ est isomorphe à $\mathbf{F}_p$ par l'application qui à la classe de $P$ associe $P(\alpha)$. Nous obtenons donc un isomorphisme

$$A \tilde{\to} \mathbf{F}_p \times \mathbf{F}_p.$$

Soit $(a_1, a_2)$ l'image de $a$ par cet isomorphisme. Comme $a^2 = 0$, nous avons $(a_1, a_2)^2 = 0$ ce qui veut dire que $a_1^2 = 0$ et $a_2^2 = 0$. Comme $\mathbf{F}_p$ est un corps, il s'ensuit que $a_1 = 0$ et $a_2 = 0$ et donc $a = 0$.

3e cas : finalement, supposons que $X^2 - 4X + 1$ est réductible avec une racine double $\alpha$. Alors

$$X^2 - 4X + 1 = (X-\alpha)^2 = X^2 - 2\alpha X + \alpha^2$$

et $2\alpha = 4$. Comme $p \neq 2$, il s'ensuit que $\alpha = 2$. Donc 2 est racine de $X^2 - 4X + 1$, c'est-à-dire que $-3 = 0$ dans $A$ et donc dans $\mathbf{F}_p$. Donc $p = 3$. Mais $2^s - 1 = (-1)^s - 1 = -2$ dans $\mathbf{F}_3$ car $s$ est impair. Donc $p \neq 3$ est ce cas est impossible.

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

Si $x^m = 1$ alors clairement $x^m + x^{-m} = 1 + 1 = 2$. Réciproquement, si $x^m + x^{-m} = 2$, alors pour $a = x^m - 1$, nous avons $a^2 = x^{2m} - 2x^m + 1 = x^m(x^m - 2 + x^{-m}) = 0$. Donc $a = 0$ d'après d), et $x^m = 1$.

f) *Montrer que $x$ est d'ordre $2^s$ dans le groupe $A^*$.* D'après c) et e) nous avons $x^{2^s} = 1$ et $x^{2^{s-1}} \neq 1$. La première condition montre que l'ordre de $x$ est un diviseur de $2^s$. La deuxième montre que l'ordre de $x$ ne peut pas être un diviseur propre de $2^s$. Donc l'ordre de $x$ est égal à $2^s$.

g) *Supposons le polynôme $X^2 - 4X + 1$ réductible sur $\mathbf{F}_p$. Montrer qu'on a $x^{p-1} = 1$.* Nous avons vu dans d), que si $X^2 - 4X + 1$ est réductible, il admet deux racines distinctes et nous avons l'isomorphisme

$$A \tilde{\to} \mathbf{F}_p \times \mathbf{F}_p.$$

Soit $(x_1, x_2)$ l'élément qui correspond à $x$ par cet isomorphisme. Alors comme $x$ est inversible, il en va de même pour $x_1$ et $x_2$ et nous avons $(x_1, x_2)^{p-1} = (1, 1)$. Il s'ensuit que $x^{p-1} = 1$.

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 $x^{p+1} = 1$.*

D'après a), nous avons $x + x^{-1} = 4$. Donc $x^p + x^{-p} = (x + x^{-1})^p = 4^p = 4$, d'après le petit théorème de Fermat. Nous obtenons donc

$$x^p + x^{-p} = x + x^{-1}$$

et

$$(x^{p+1} - 1)(x^{p-1} - 1) = (x^{2p} + x^{p+1} + x^{p-1} + 1) = x^p\,(x^p - x - x^{-1} + x^{-p}) = 0.$$

Comme $A$ est un corps, il s'ensuit que $x^{p+1} = 1$ ou $x^{p-1} = 1$.

i) *Montrer que* $p = 2^s - 1$. D'après g) et h) nous avons $x^{p-1} = 1$ ou $x^{p+1} = 1$. Or l'ordre de $x$ dans $A^*$ est $2^s$ d'après f). Dans le premier cas, $2^s$ doit être un diviseur de $p-1$ et donc $2^s \leq p-1$, $2^s - 1 \leq p-2$ ce qui est impossible puisque $p$ divise $2^s - 1$. Donc $x^{p+1} = 1$ et $p+1$ est un multiple de $2^s$. Donc $2^s \leq p+1$ et $2^s - 1 \leq p$. De l'autre côté, $p$ divise $2^s - 1$. Donc $p = 2^s - 1$.

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

a) *Soit* $a \in \mathbf{F}_p^*$. *Montrer que* $a^{(p-1)/2} = \pm 1$. Considérons $u = a^{(p-1)/2}$. Nous avons $u^2 = a^{p-1} = 1$ d'après le petit théorème de Fermat. Donc $(u-1)(u+1) = 0$ et $u = \pm 1$ car $\mathbf{F}_p$ est un corps.

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.* Supposons que $a = b^2$. Alors $a^{(p-1)/2} = b^{p-1} = 1$ d'après le petit théorème de Fermat. Supposons maintenant que $a^{(p-1)/2} = 1$. Soit $g$ un générateur du groupe cyclique $\mathbf{F}_p^*$. Soit $l \in \mathbf{Z}$ tel que $g^l = a$. Alors $a^{(p-1)/2} = g^{l(p-1)/2} = 1$. Comme $g$ est d'ordre $p-1$, il s'ensuit que $l(p-1)/2$ est divisible par $p-1$ et que $l/2$ est un entier. Si nous posons $b = g^{l/2}$, nous avons $a = b^2$.

D'après a), nous savons que $a^{(p-1)/2} = \pm 1$. Donc si $a$ n'est pas un carré et donc $a^{(p-1)/2} \neq 1$, on doit avoir $a^{(p-1)/2} = -1$.

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 de la réciprocité quadratique qu'on a* $2^{(p-1)/2} = 1$ *et* $3^{(p-1)/2} = -1$ *dans* $\mathbf{F}_p$.

D'après 3 b) et la réciprocité quadratique, il suffit de montrer que $p \equiv \pm 1$ (8). Or $p = 2^s - 1$ et $s$ est un entier impair $\geq 3$. Donc $p \equiv -1$ (8). Pour calculer la classe de $p$ modulo 12, d'après le lemme chinois, il suffit de calculer les classes modulo 3 et 4. Nous avons $p \equiv -1$ (4) car nous avons même $p \equiv -1$ (8). En outre $p \equiv (-1)^s - 1 \equiv -2$ (3). Il s'ensuit que $p \equiv 7$ (12). Donc $p \not\equiv \pm 1$ (12) et l'affirmation s'ensuit d'après 3 b) et la réciprocité quadratique.

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

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

On a

$$\begin{aligned} y^2 &= (x-2)^2 = x^2 - 4x + 4 = (x^2 - 4x + 1) + 3 = 3\,, \\ (1+y)^2 &= 1 + 2y + y^2 = 2x - 4 + 1 + 3 = 2x\,, \\ (1-y)^2 &= 1 - 2y + y^2 = -2x + 4 + 1 + 3 = 2(4-x) = 2x^{-1}. \end{aligned}$$

Donc

$$\begin{aligned} 2^{(p+1)/2}L_s &= 2^{(p+1)/2}(x^{2^{s-1}} + x^{-2^{s-1}}) \\ &= 2^{2^{s-1}}(x^{2^{s-1}} + x^{-2^{s-1}}) = (2x)^{2^{s-1}} + (2x^{-1})^{2^{s-1}} \\ &= (1+y)^{2^s} + (1-y)^{2^s} = (1+y)^{p+1} + (1-y)^{p+1}. \end{aligned}$$

En utilisant que $(a+b)^{p+1} = (a+b)^p(a+b) = (a^p+b^p)(a+b)$ dans $A$ nous obtenons

$$\begin{aligned} (1+y)^{p+1} &= (1+y^p)(1+y) = 1+y^p+y+y^{p+1}\,, \\ (1-y)^{p+1} &= (1-y^p)(1-y) = 1-y^p-y+y^{p+1}. \end{aligned}$$

Donc

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

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

$$\begin{aligned} 2^{(p+1)/2} &= 2 \times 2^{(p-1)/2} = 2\,, \\ 3^{(p+1)/2} &= 3 \times 3^{(p-1)/2} = -3. \end{aligned}$$

D'après b), on obtient $2L_s = 2\,(1-3) = 2\,(-2)$. Donc $L_s = -2 = L_{s-1}^2 - 2$. Il s'ensuit que $L_{s-1}^2 = 0$ et $L_{s-1} = 0$.