Devoir Surveillé 5, corrigé

PROBLÈME
Groupe des périodes

Partie I. Structure de G_f et exemples.

1) *Généralités.*

a) On a $0 \in G_f$ (car $\forall x \in \mathbb{R},\ f(x) = f(x)$). La loi $+$ est bien associative. Si $T_1, T_2 \in G_f$ alors pour $x \in \mathbb{R}$:

$$f(x + T_1 + T_2) = f(x + T_1) = f(x)$$

donc $T_1 + T_2 \in G_f$. Enfin, on a aussi pour $x \in \mathbb{R}$:

$$f(x - T_1) = f((x - T_1) + T_1) = f(x)$$

ce qui prouve que $-T_1 \in G_f$. On a donc bien un groupe pour la loi $+$.

b) Supposons $\alpha \in G_f$. Montrons par récurrence que $\forall n \in \mathbb{N},\ n\alpha \in G_f$. La propriété est vraie pour $n = 0$ car $0 \in G_f$.

Fixons $n \in \mathbb{N}$ et supposons que $n\alpha \in G_f$. Puisque G_f est un groupe et que $\alpha \in G_f$, on a $n\alpha + \alpha \in G_f$, soit $(n+1)\alpha \in G_f$. La propriété est donc vraie au rang $n + 1$.

On a donc par récurrence que $\forall n \in \mathbb{N},\ n\alpha \in G_f$. Puisque G_f est un groupe pour la loi $+$, il est stable par passage à l'opposé et on a donc $\forall n \in \mathbb{N},\ -n\alpha \in G_f$.

On a donc finalement $\alpha\mathbb{Z} \subset G_f$.

2) *Exemples.*

a)

i) Si f est constante, on a $G_f = \mathbb{R}$ (tous les réels sont des périodes de f).

ii) exp est strictement croissante sur $\mathbb{R}$ donc $\forall T \neq 0,\ \forall x \in \mathbb{R},\ f(x + T) \neq f(x)$. On en déduit que $G_f = \{0\}$ (car on a toujours $0 \in G_f$ puisque G_f est un groupe).

iii) On a $\sin(x) = 1 \Leftrightarrow x \equiv \frac{\pi}{2}\ [2\pi]$. On en déduit que si T est une période de sinus, on doit avoir $\sin\left(\frac{\pi}{2}\right) = \sin\left(\frac{\pi}{2} + T\right)$, ce qui implique que :

$$\frac{\pi}{2} + T \equiv \frac{\pi}{2}\ [2\pi] \Leftrightarrow T \equiv 0\ [2\pi].$$

iv) La question précédente prouve que $G_f \subset 2\pi\mathbb{Z}$ (puisque si T est dans G_f, alors T est un multiple de 2π). Pour la réciproque, on sait que $2\pi \in G_f$ (car sinus est 2π périodique). D'après la question 1.b, on a alors $2\pi\mathbb{Z} \subset G_f$. On a donc l'égalité demandée par double inclusion.

b)

i) Soit $T \in \mathbb{Q}$. Fixons $x \in \mathbb{R}$. On a alors deux cas :

- Si $x \in \mathbb{Q}$, on a alors $x + T \in \mathbb{Q}$ car $\mathbb{Q}$ est stable par somme (il suffit de mettre l'expression $x + T$ au même dénominateur). On a donc $f(x) = 1$ et $f(x + T) = 1$ d'où $f(x) = f(x + T)$.

- Si $x \notin \mathbb{Q}$, on a alors $x+T \notin \mathbb{Q}$. En effet, si par l'absurde on avait $x+T \in \mathbb{Q}$, alors $x = (x+T)-T$ serait rationnel comme différence de deux rationnels ce qui est absurde. On a donc $f(x) = 0$ et $f(x+T) = 0$ ce qui prouve bien que $f(x) = f(x+T)$.

On a donc bien $\forall x \in \mathbb{R},\ f(x+T) = f(x)$ ce qui entraine que T est une période de f.

ii) D'après la question précédente, on a $\mathbb{Q} \subset G_f$. Il reste à justifier l'autre inclusion. Fixons donc $T \in G_f$. On a alors $f(0) = f(T)$. Puisque $0 \in \mathbb{Q}$, on a donc $f(0) = 1$, soit $f(T) = 1$. Ceci entraine par définition de f que $T \in \mathbb{Q}$. On a donc l'égalité voulue par double inclusion.

c) Fixons $x_0 \in \mathbb{R}$. Si $x_0 \in \mathbb{Q}$, alors puisque $\mathbb{R} \setminus \mathbb{Q}$ est dense dans $\mathbb{R}$, il existe une suite $(u_n) \in (\mathbb{R} \setminus \mathbb{Q})^{\mathbb{N}}$ telle que $\lim\limits_{n\to+\infty} u_n = x_0$. Or, on a $\forall n \in \mathbb{N},\ f(u_n) = 0$ donc $\lim\limits_{n\to+\infty} f(u_n) = 0 \neq f(x_0)$ car $f(x_0) = 1$.

On procède de la même façon si $x_0 \in \mathbb{R} \setminus \mathbb{Q}$ en utilisant le fait que $\mathbb{Q}$ est dense dans $\mathbb{R}$ et en construisant une suite $(v_n) \in \mathbb{Q}^{\mathbb{N}}$ telle que $\lim\limits_{n\to+\infty} v_n = x_0$ et on a $\lim\limits_{n\to+\infty} f(v_n) = 1 \neq f(x_0) = 0$.

3) G_f n'est en général pas stable par produit. Prenons $f = \sin$. On a $2\pi \in G_f$ mais on peut vérifier que $(2\pi)^2 = 4\pi^2 \notin G_f$. En effet, par l'absurde, si c'était le cas, il existerait $k \in \mathbb{Z}$ tel que $4\pi^2 = 2k\pi$, ce qui entraine que $\pi = \dfrac{k}{2} \in \mathbb{Q}$: absurde !

Partie II. Description de G_f quand f est continue.

4) *Borne inférieure de $G_f \cap \mathbb{R}_+^*$.*

a) $G_f \cap \mathbb{R}_+^*$ est non vide (il contient $T > 0$ par hypothèse) et est minoré par 0. Il admet donc une borne inférieure par propriété fondamentale de $\mathbb{R}$ et on a $\alpha \geq 0$ (car 0 minore $G_f \cap \mathbb{R}_+^*$ et α est le plus grand minorant.

b) Par caractérisation séquentielle de α, il existe $(\alpha_n)_{n\in\mathbb{N}} \in (G_f \cap \mathbb{R}_+^*)^{\mathbb{N}}$ telle que $\lim\limits_{n\to+\infty} \alpha_n = \alpha$.

Si $x \in \mathbb{R}$, on a alors $\forall n \in \mathbb{N},\ f(x+\alpha_n) = f(x)$. Puisque la fonction f est continue et que $\lim\limits_{n\to+\infty} x + \alpha_n = x + \alpha$, on en déduit par passage à la limite que :

$$f(x+\alpha) = f(x).$$

On a donc bien $\forall x \in \mathbb{R},\ f(x+\alpha) = f(x)$.

5) *Minoration des périodes.*

a) f est continue sur le segment $[0,T]$. Elle admet donc un minimum m et un maximum M sur $[0,T]$ d'après le théorème des bornes atteintes. Supposons par l'absurde que $m = M$. On a alors f constante sur $[0,T]$ et puisqu'elle est T-périodique, elle est alors constante sur $\mathbb{R}$ ce qui est absurde. On a donc bien $m < M$.

b) On a $0 \in [0,T]$ donc $m \leq f(0) \leq M$. Puisque $m < M$, on ne peut pas avoir à la fois $m = f(0)$ et $f(0) = M$. On en déduit que $m < f(0)$ ou que $f(0) < M$.

c) f est continue en 0 si et seulement si $\forall \varepsilon > 0,\ \exists eta > 0 \ /\ \forall x \in \mathbb{R},\ ((|x| \leq \eta) \Rightarrow (|f(x) - f(0)| \leq \varepsilon))$. En utilisant alors cette définition en $\varepsilon = \dfrac{M - f(0)}{2} > 0$, on en déduit qu'il existe $\eta > 0$ tel que en particulier, pour $x \in [0,\eta]$:

$$|f(x) - f(0)| \leq \varepsilon \Leftrightarrow f(0) - \varepsilon \leq f(x) \leq f(0) + \varepsilon.$$

En particulier, on a $f(x) \leq \dfrac{M + f(0)}{2} < M$ ce qui donne le résultat demandé.

d) Soit $0 < t \leq \eta$ et supposons que f est t-périodique. D'après la question précédente, puisque $[0,t] \subset [0,\eta]$, on a alors pour tout $x \in [0,t],\ f(x) < M$. Par t-périodicité de f, on en déduit que

$\forall x \in \mathbb{R},\ f(x) < M$ ce qui est absurde car M est le maximum de f sur $[0, T]$ et est donc atteint en au moins une valeur.

6) D'après la question 4, on a $\alpha \in G_f$ (puisque α est une période de f) et $\alpha \geq 0$. Or, d'après la question 5, η minore $G_f \cap \mathbb{R}_+^*$ (puisqu'il n'existe aucune période de f dans $]0, eta]$. On a donc par définition de la borne inférieure que $\eta \leq \alpha$, ce qui entraine $0 < \alpha$.

On a donc $\alpha \in G_f \cap \mathbb{R}_+^*$. α est donc un minorant qui appartient à l'ensemble qu'il minore. C'est donc le minimum de $G_f \cap \mathbb{R}_+^*$.

7) *La conclusion.*

a) Si on pose $n = \lfloor \dfrac{t}{\alpha} \rfloor \in \mathbb{Z}$, on a $n \leq \dfrac{t}{\alpha} < n+1$. Puisque $\alpha > 0$, on a alors $n\alpha \leq t < (n+1)\alpha$.

b) On a alors directement que $0 \leq t - n\alpha < \alpha$ donc $0 \leq t - n\alpha$. De plus, $\alpha \in G_f$ et $n \in \mathbb{Z}$ donc puisque G_f est un groupe, $n\alpha \in G_f$ et par différence, $t - n\alpha \in G_f$ (car $t \in G_f$). On a donc $t - n\alpha \in G_f \cap \mathbb{R}_+$.

Or, on a $t - n\alpha < \alpha = \min(G_f \cap \mathbb{R}_+^*)$. On a donc une absurdité si $t - n\alpha \in G_f \cap \mathbb{R}_+^*$, autrement dit si $0 < t - n\alpha$. On a donc $0 = t - n\alpha$, soit $t = n\alpha$.

c) On a montré dans la question précédente que $G_f \subset \alpha\mathbb{Z}$. Or, puisque $\alpha \in G_f$, la question 1 prouve que $\alpha\mathbb{Z} \subset G_f$. On a donc bien $G_f = \alpha\mathbb{Z}$.

8) *Application.*

a) Soit $n \in \mathbb{N}^*$. D'après la formule du binôme, on a :

$$(\sqrt{2} - 1)^n = \sum_{k=0}^{n} \binom{n}{k} (\sqrt{2})^k (-1)^{n-k}.$$

En séparant la somme entre les indices pairs et impairs, on a donc :

$$\begin{aligned}
(\sqrt{2} - 1)^n &= \sum_{\substack{0 \leq k \leq n \\ k \text{ pair}}} \binom{n}{k} (\sqrt{2})^k (-1)^{n-k} + \sum_{\substack{0 \leq k \leq n \\ k \text{ impair}}} \binom{n}{k} (\sqrt{2})^k (-1)^{n-k} \\
&= \sum_{0 \leq 2j \leq n} \binom{n}{2j} 2^j (-1)^{n-2j} + \sum_{0 \leq 2j+1 \leq n} \binom{n}{2j+1} (\sqrt{2})^{2j+1} (-1)^{n-(2j+1)} \\
&= \sum_{0 \leq 2j \leq n} \binom{n}{2j} 2^j (-1)^{n} + \sqrt{2} \sum_{0 \leq 2j+1 \leq n} \binom{n}{2j+1} 2^j (-1)^{n-1}.
\end{aligned}$$

Or, les deux sommes précédentes sont entières (on ne fait que des sommes/produits d'entiers). On en déduit que $(\sqrt{2} - 1)^n = a + b\sqrt{2}$ avec $a, b \in \mathbb{Z}$. Puisque f est 1-périodique et $\sqrt{2}$-périodique et que G_f est un groupe pour la loi $+$ (et donc stable par somme/différence), on en déduit que $(\sqrt{2} - 1)^n$ est une période de f.

b) On a $0 < \sqrt{2} - 1 < 1$. On a donc par limite de suite géométrique $\lim\limits_{n \to +\infty} (\sqrt{2} - 1)^n = 0$.

c) Puisque $\forall n \in \mathbb{N}^*$, $(\sqrt{2} - 1)^n \in G_f \cap \mathbb{R}_+^*$, on a aussi $0 \leq \alpha \leq (\sqrt{2} - 1)^n$ (toujours en considérant α la borne inférieure de $G_f \cap \mathbb{R}_+^*$). Par théorème des gendarmes, on en déduit que $\alpha = 0$.

Or, d'après la question précédente, si f est continue non constante et périodique, on a $\alpha > 0$. Puisqu'ici f est continue, périodique et que $\alpha = 0$, on en déduit que f est constante.

PROBLÈME
LES CARRÉS DE LA SUITE DE LUCAS

Partie I. Généralités et le cas n pair.

1) Posons pour $n \in \mathbb{N}$, $\mathcal{P}(n)$: « $L_n \in \mathbb{N}^*$ ».

La propriété est vraie au rang 0 et au rang 1 puisque $L_0 = 2$ et que $L_1 = 1$.

Soit $n \in \mathbb{N}$. Supposons $\mathcal{P}(n)$ et $\mathcal{P}(n+1)$. On a alors $L_{n+2} = L_{n+1} + L_n$ qui est dans $\mathbb{N}^*$ par somme d'entiers strictement positifs.

Par récurrence double, on a donc que $\forall n \in \mathbb{N},\ L_n \in \mathbb{N}^*$.

2) Pour $n \in \mathbb{N}$, posons $\mathcal{P}(n)$: « $L_n \wedge L_{n+1} = 1$ ».

La propriété est vraie au rang 0 puisque $L_0 \wedge L_1 = 2 \wedge 1 = 1$. Soit $n \in \mathbb{N}$. Supposons $\mathcal{P}(n)$. On a alors en utilisant le lemme d'Euclide :

$$\begin{array}{rcl} L_{n+1} \wedge L_{n+2} & = & L_{n+1} \wedge (L_{n+1} + L_n) \\ & = & L_{n+1} \wedge (L_{n+1} + L_n - L_{n+1}) \\ & = & L_{n+1} \wedge L_n. \end{array}$$

En utilisant l'hypothèse de récurrence, on a donc $L_{n+1} \wedge L_{n+2} = 1$ ce qui prouve $\mathcal{P}(n+1)$. Par récurrence, la propriété est donc vraie à tout rang.

3) *Périodicité de L_n [4].*

a) Pour $n \in [\![0, 7]\!]$, on a (pour obtenir un terme, on additionne les deux précédents) :

n	0	1	2	3	4	5	6	7
L_n	2	1	3	4	7	11	18	29

On a $L_6 = 18 \equiv 2$ [4] et $L_7 = 29 \equiv\ 1[4]$ ce qui donne le résultat voulu puisque $L_0 = 2$ et $L_1 = 1$.

b) On peut procéder par récurrence double. La propriété demandée est vraie au rang 0 et 1. Soit $n \in \mathbb{N}$ tel que $L_{n+6} \equiv L_n$ [4] et $L_{n+7} \equiv L_{n+1}$ [4]. On a alors par définition de la suite de Lucas et par hypothèse de récurrence :

$$L_{n+8} = L_{n+7} + L_{n+6} \equiv L_{n+1} + L_n \ [4].$$

Puisque $L_{n+1} + L_n = L_{n+2}$, on a alors $L_{n+8} \equiv L_{n+2}$ [4] ce qui prouve l'hypothèse au rang $n+2$. Par récurrence double, on a donc la propriété vraie à tout rang.

On en déduit que la suite $(L_n\ [4])_{n\in\mathbb{N}}$ est 6 périodique.

4) *Expression explicite de L_n.*

a) L'équation caractéristique associée à $(L_n)_{n\in\mathbb{N}}$ (qui est une suite récurrence linéaire d'ordre 2 à coefficients constants) est $X^2 - X - 1 = 0$. Son discriminant vaut 5 et les racines sont donc ω_1 et ω_2. On en déduit qu'il existe des constantes réelles λ, μ telles que pour tout $n \in \mathbb{N}$:

$$L_n = \lambda \omega_1^n + \mu \omega_2^n.$$

On trouve alors les constantes en évaluant en $n = 0$ et $n = 1$. On trouve le système :

$$\begin{array}{cl} & \left\{ \begin{array}{l} \lambda + \mu = 2 \\ \lambda\omega_1 + \mu\omega_2 = 1 \end{array} \right. \\ \Leftrightarrow & \left\{ \begin{array}{l} \lambda + \mu = 2 \\ \lambda(1 - \sqrt{5}) + \mu(1 + \sqrt{5}) = 2 \end{array} \right. \\ \Leftrightarrow & \left\{ \begin{array}{l} \lambda + \mu = 2 \\ (-\lambda + \mu)\sqrt{5} = 0 \end{array} \right. . \end{array}$$

On en déduit que $\lambda = \mu = 1$. On a donc :

$$\forall n \in \mathbb{N},\ L_n = \omega_1^n + \omega_2^n.$$

b) D'après la question précédente, on a :

$$\begin{array}{rcl} L_{2n} - L_n^2 & = & \omega_1^{2n} + \omega_2^{2n} - (\omega_1^n + \omega_2^n)^2 \\ & = & -2\omega_1^n \omega_2^n \\ & = & -2\left(\dfrac{1-\sqrt{5}}{2} \times \dfrac{1+\sqrt{5}}{2}\right)^n \\ & = & -2 \times \left(\dfrac{1-5}{4}\right)^n \\ & = & 2(-1)^{n+1}. \end{array}$$

5) *Le cas n pair.*

a) Les deux inégalités non évidentes sont $(x-1)^2 < x^2-2$ et $x^2+2 < (x+1)^2$. Pour la première, on a $(x-1)^2 = x^2-2x+1$. Or, on a $-2x+1 < -2$ si et seulement si $-2x < -3$ si et seulement si $x > \dfrac{3}{2}$ ce qui est vrai pour $x \geq 2$.

Pour la seconde, on a $(x+1)^2 = x^2+2x+1 \geq x^2+5 > x^2+2$ puisque $x \geq 2$. On a donc bien l'encadrement demandé.

b) On a $L_{2n} = L_n^2 + 2(-1)^{n+1}$. Si on note $x = L_n \in \mathbb{N}^*$ (d'après la question 1), on a donc $L_{2n} = x^2 \pm 2$. Supposons alors $x \geq 2$. D'après la question précédente, on a alors L_{2n} strictement compris entre deux carrés consécutifs. Autrement dit, L_{2n} ne peut pas être un carré d'entier.

Il reste à traiter le cas où $x = 1$. On aurait alors dans ce cas que $L_{2n} = 1 \pm 2$, soit $L_{2n} = -1$ ou $L_{2n} = 3$. Dans les deux cas, L_{2n} n'est pas un carré d'entier.

On en déduit que les indices pairs de la suite de Lucas ne sont jamais des carrés d'entier.

Partie II. Étude des carrés modulo n.

6) Puisque $p \in \mathbb{P}$, le petit théorème de Fermat donne que $\forall x \in \mathbb{Z},\ x^p \equiv x\ [p]$. Supposons à présent $x \wedge p = 1$. D'après le petit théorème de Fermat, on a $x^p - x \equiv 0\ [p]$ ce qui entraine que :

$$p | x(x^{p-1} - 1).$$

Or, $p \wedge x = 1$ donc d'après le théorème de Gauss, $p | (x^{p-1} - 1)$, ce qui entraine $x^{p-1} - 1 \equiv 0\ [p]$, soit $x^{p-1} \equiv 1\ [p]$.

7) Soit $p \in \mathbb{P}$ un nombre premier tel que $p \equiv 3\ [4]$. On suppose par l'absurde qu'il existe $x \in \mathbb{Z}$ tel que $x^2 \equiv -1\ [p]$.

a) Puisque $x^2 \equiv -1\ [p]$, on a qu'il existe $k \in \mathbb{Z}$ tel que $x^2 = -1 + kp$, soit que $1 = kp - x \times x$. Puisque $(k, -x) \in \mathbb{Z}^2$, d'après le théorème de Bézout, on a $p \wedge x = 1$.

De plus, puisque $p \equiv 3\ [4]$, on a p impair (plus grand que 3 car p est premier). On a donc $p-1$ pair plus grand que 2 et donc $\dfrac{p-1}{2}$ entier strictement positif.

b) On part de $x^2 \equiv -1\ [p]$ et on élève cette égalité à la puissance $\dfrac{p-1}{2}$ qui est bien un entier. On en déduit, puisque $p = 2 \times \dfrac{p-1}{2}$ que :

$$x^{p-1} \equiv (-1)^{\frac{p-1}{2}}\ [p].$$

On en déduit d'après la question 6 (toutes les hypothèses sont réunies) que $1 \equiv (-1)^{\frac{p-1}{2}}$ $[p]$. Or, on a $p \equiv 3$ $[4]$ donc $p-1 \equiv 2$ $[4]$. En divisant par 2, on en déduit que $\dfrac{p-1}{2} \equiv 1$ $[2]$, autrement dit que $\dfrac{p-1}{2}$ est impair. On a donc :

$$1 \equiv -1 \ [p] \Leftrightarrow 2 \equiv 0 \ [p].$$

Ceci est absurde puisque l'on aurait alors $p|2$ alors que p est un nombre premier impair.

On en déduit que $\forall x \in \mathbb{Z}$, $x^2 \not\equiv -1$ $[p]$.

c) Puisque $n \equiv 3$ $[4]$, n est impair. Dans sa décomposition en produit de facteurs premiers, il ne peut donc apparaitre que des nombres impairs (sinon n serait pair). De plus modulo 4, un nombre impair ne peut être égal qu'à 1 ou 3 (puisque s'il était égal à 0 ou 2 modulo 4, il serait pair).

Supposons par l'absurde que tous les nombres premiers qui apparaissent dans la décomposition de n en produit de facteurs premiers soient congrus à 1 modulo 4. Alors, par produit/puissance dans les modulos, leur produit (avec les p_k élevés à la puissance α_k) serait congru à 1 modulo 4 (puisque $1 \times 1 = 1$ $[4]$). Puisque $n \equiv 3$ $[4]$, c'est absurde ! Il existe donc au moins un nombre premier p impair tel que $p|n$ et $p \equiv 3$ $[4]$.
Justifier que tous les nombres premiers $p_1, \ldots, p_k$ sont impairs, puis qu'ils sont tous congrus à 1 ou 3 modulo 4 et enfin qu'il en existe au moins un congru à 3 modulo 4, que l'on notera p dans la suite.

d) Supposons par l'absurde qu'il existe $x \in \mathbb{Z}$ tel que $x^2 \equiv -1$ $[n]$. Il existe donc $k \in \mathbb{Z}$ tel que $x^2 = -1 + kn$. Puisque p divise n, on en déduit que $x^2 \equiv -1$ $[p]$. Or, puisque $p \equiv 3$ $[4]$, ceci est absurde d'après la question 7. On a donc bien le résultat voulu.

e) n est impair donc $2 \wedge n = 1$. D'après le théorème de Bezout, il existe $u, v \in \mathbb{Z}$ tel que $2u + nv = 1$. En prenant cette égalité modulo n, on en déduit que $2u \equiv 1$ $[n]$.

f) Supposons par l'absurde l'existence d'un tel x. On a alors en multipliant par u^2 que $u^2x^2 \equiv -(2u)^2$ $[n]$, soit que $(ux)^2 \equiv -1$ $[n]$. Puisque $ux \in \mathbb{Z}$, ceci contredit la question 8.b. On a donc bien qu'il n'existe pas de $x \in \mathbb{Z}$ tels que $x^2 \equiv -4$ $[n]$.

Partie III. Le cas n impair et la conclusion.

On note $(F_n)_{n\in\mathbb{N}}$ la suite de Fibonacci définie par $F_0 = 0$, $F_1 = 1$ et $\forall n \in \mathbb{N},\ F_{n+2} = F_{n+1} + F_n$. On montre, de la même manière que pour la suite de Lucas que $\forall n \in \mathbb{N},\ F_n \in \mathbb{N}$ et que $\forall n \in \mathbb{N},\ F_n = \dfrac{1}{\sqrt{5}}(\omega_2^n - \omega_1^n)$.

8) Soit $k \in \mathbb{N}$.

a) Pour $m \in \mathbb{N}$, on a :

$$\begin{aligned} 5F_mF_kL_k + L_mL_{2k} &= (\omega_2^m - \omega_1^m)(\omega_2^k - \omega_1^k)(\omega_2^k + \omega_1^k) + (\omega_2^m + \omega_1^m)(\omega_2^{2k} + \omega_1^{2k}) \\ &= (\omega_2^m - \omega_1^m)(\omega_2^{2k} - \omega_1^{2k}) + (\omega_2^m + \omega_1^m)(\omega_2^{2k} + \omega_1^{2k}) \\ &= 2\omega_2^{m+2k} + 2\omega_1^{m+2k} \\ &= 2L_{2k+m}. \end{aligned}$$

b) Tous les nombres considérés sont entiers. On a L_k qui divise $5F_mF_kL_k$ donc $5F_mF_kL_k \equiv 0$ $[L_k]$. Pour montrer le résultat annoncé, il reste donc à vérifier que $L_{2k} \equiv 2(-1)^{k+1}$ $[L_k]$. Or, d'après la question 3.b, on a $L_{2k} = 2(-1)^{k+1} + L_k$, ce qui en prenant cette égalité modulo L_k donne le résultat voulu.

c) En utilisant la propriété en $m = k$, on obtient, puisque $L_k \equiv 0$ $[L_k]$, que $L_{3k} \equiv 0$ $[L_k]$ d'où L_k divise $2L_{3k}$.

On peut ensuite montrer le résultat voulu par récurrence sur α. La propriété est vraie au rang $\alpha = 0$ (rien à montrer) et $\alpha = 1$ (on vient de le vérifier).

Si elle est vrai au rang $\alpha \in \mathbb{N}$ fixé, alors, en utilisant le fait que L_k divise $2L_{3k}$ en $3^\alpha k$ à la place de k, on obtient que $L_{3^\alpha k}$ divise $2L_{3^{\alpha+1}k}$. Ceci entraine que $2^\alpha L_{3^\alpha k}$ divise $2^{\alpha+1}L_{3^{\alpha+1}k}$. En utilisant l'hypothèse de récurrence, on en déduit que L_k divise $2^{\alpha+1}L_{3^{\alpha+1}k}$. La propriété étant initialisée et héréditaire, elle est vrai à tout rang.

9)

a) Puisque n est impair et que $n = 4q + r$, on a r impair. Puisque $0 \leq r < 4$, on a donc $r \in \{1, 3\}$. De plus, on a $4q = 2 \times 2q$. On peut considérer la factorisation de $2q$ en produit de facteurs premiers. On a alors :

$$2q = 2 \times 3^\alpha \times n'$$

où n' ne contient différent nombres premiers mais aucun 3 (si on a mis tous les 3 dans le 3^α en prenant $\alpha = v_3(2q)$ la valuation 3 adique de $2q$). En posant $k = 2n'$, on a donc :

$$4q = 2 \times k \times 3^\alpha$$

avec $\alpha \in \mathbb{N}$ et $k \in \mathbb{N}^*$. On a de plus k pair car $k = 2n'$ et k non divisible par 3 car n' n'est pas divisible par 3 et 2 non plus et donc 3 n'apparait pas dans la décomposition en produit de facteurs premiers de k.

b) Puisque k est pair, k est congru modulo 6 à 0, 2 ou 4. Or, k n'est pas divisible par 3. Il n'est donc pas divisible par 6 et donc $k \not\equiv 0$ [6]. On a donc bien que $k \equiv 2$ [6] ou $k \equiv 4$ [6].

c) D'après la question 3, on a la suite $(L_n\ [4])_{n\in\mathbb{N}}$ qui est 6 périodique. Puisque $k \equiv 2$ [6] ou $k \equiv 4$ [6], on a donc $L_k \equiv L_2$ [4] ou $L_k \equiv L_4$ [4]. Puisque $L_2 = 3$ et $L_4 = 7$, on a bien dans les deux cas $L_k \equiv 3$ [4].

d) On a donc L_k de la forme $4n' + 3$ avec $n' \in \mathbb{Z}$ donc L_k est impair. On a donc $L_k \wedge 2 = 1$ (puisque 2 n'apparait pas dans la décomposition en produits de facteurs premiers de L_k). On a alors $L_k \wedge 2^\alpha = 1$ (puisque les seuls diviseurs de 2^α sont des puissances de 2 et que 2 ne divise pas L_k.

Puisque d'après la question 9.c, on a L_k qui divise $2^\alpha L_{3^\alpha k}$, alors d'après le théorème de Gauss, puisque $L_k \wedge 2^\alpha = 1$, on a alors L_k qui divise $L_{3^\alpha k}$.

e) On utilise alors la question 9.b en $k' = k3^\alpha$ et $m = r$ pour avoir $n = 2k' + m$. On a k' pair (car k est pair) donc $(-1)^{k'+1} = -1$. On a donc :

$$2L_n \equiv -2L_r\ [L_{k3^\alpha}].$$

Ceci entraine qu'il existe $u \in \mathbb{Z}$ tel que $2L_n = -2L_r + uL_{k3^\alpha}$. Puisque L_k divise $L_{3^\alpha k}$, on en déduit donc L_k divise $2(L_n + L_r)$. Or, L_k est impair donc $2 \wedge L_k = 1$. D'après le théorème de Gauss, on a alors L_k qui divise $L_n + L_r$. On a donc finalement :

$$L_n \equiv -L_r\ [L_k].$$

Puisque $r = 1$ ou $r = 3$ et que $L_1 = 1$ et $L_3 = 4$, on a donc bien que :

$$L_n \equiv -1\ [L_k] \text{ ou } L_n \equiv -4\ [L_k].$$

10) On a déjà d'après la partie I que les indices impairs de la suite de Lucas ne sont pas des carrés. Puisque $L_1 = 1$ et $L_3 = 4$, les indices 1 et 3 sont des carrés. Considérons à présent un entier n impair avec $n \geq 5$. D'après la question précédente (avec les mêmes notations), on a alors $L_n \equiv -1$ $[L_k]$ ou $L_n \equiv -4$ $[L_k]$. Or, d'après la question 10.c, on a $L_k \equiv 3$ [4]. D'après la partie II, il n'existe pas d'entiers tels que $x^2 \equiv -1$ $[L_k]$ ou tels que $x^2 \equiv -4$ $[L_k]$. On en déduit que L_n ne peut pas être un carré d'entier ! Le théorème de Cohn est démontré !