Les problèmes de l'APMEP

Les propositions de problèmes, solutions ou commentaires, sont à envoyer à

Max HOCHART
65, rue Blatin
63 000 CLERMONT-FERRAND
ou par courriel à
hochartmax@yahoo.fr

Énoncés des nouveaux problèmes

Les problèmes ci-dessous constituaient les épreuves des 50$^{\text{e}}$ olympiades internationales de mathématiques qui se sont déroulées à Brême, en Allemagne, du 10 au 22 Juillet 2009. Des compléments d'information et les résultats se trouvent aux adresses suivantes : www.imo2009.de et www.imo-official.org

Problème 485-1 (Olympiades internationales 2009)

Soit n un entier strictement positif et soit $a_1, \ldots, a_k$, avec $k \geq 2$, des entiers appartenant à l'ensemble $[[1, n]]$ tels que n divise $a_i(a_{i+1} - 1)$ pour $i \in [[1, k-1]]$. Montrer que n ne divise pas $a_k(a_1 - 1)$.

Problème 485-2 (Olympiades internationales 2009)

Soit ABC un triangle et O le centre de son cercle circonscrit. Les points P et Q sont des points intérieurs aux côtés CA et AB respectivement. Soit K, L et M les milieux respectifs des segments BP, CQ et PQ, et soit Γ le cercle passant par K, L et M. On suppose que la droite (PQ) est tangente au cercle Γ. Montrer que OP = OQ.

Problème 485-3 (Olympiades internationales 2009)

Soit $s_1, s_2, s_3, \ldots$ une suite strictement croissante d'entiers strictement positifs telle que les sous-suites $s_{s_1}, s_{s_2}, s_{s_3}, \ldots$ et $s_{s_1+1}, s_{s_2+1}, s_{s_3+1}, \ldots$ soient deux progressions arithmétiques. Montrer que la suite $s_1, s_2, s_3, \ldots$ est aussi une progression arithmétique.

Problème 485-4 (Olympiades internationales 2009)

Soit ABC un triangle tel que AB = AC. Les bissectrices de $\widehat{\text{CAB}}$ et $\widehat{\text{ABC}}$ rencontrent respectivement les côtés BC et CA en D et E. Soit K le centre du cercle circonscrit dans le triangle ADC. On suppose que $\widehat{\text{BEK}} = \dfrac{\pi}{4}$. Trouver toutes les valeurs possibles de $\widehat{\text{CAB}}$.

Problème 485-5 (Olympiades internationales 2009)

Déterminer toutes les fonctions $f : \mathbb{N}^* \to \mathbb{N}^*$ telles que. pour tous $a, b \in \mathbb{N}^*$, il existe un triangle non aplati dont les longueurs des côtes sont a, $f(b)$ et $f(b + f(a) - 1)$.

Problème 485-6 (Olympiades internationales 2009)

Soit a_1, a_2, …, a_n des entiers strictement positifs distincts et soit M un ensemble de $n - 1$ entiers strictement positifs ne contenant pas $s = a_1 + a_2 + \ldots + a_n$. Une sauterelle doit faire des sauts le long de l'axe réel ; partant du point 0, elle doit effectuer n sauts vers la droite de longueurs a_1, a_2, …, a_n dans l'ordre de son choix. Montrer que la sauterelle peut choisir l'ordre de ses sauts de façon à ne passer par aucun point de M.

Solutions des problèmes antérieurs

Problème 481-1

Étudier le comportement quand r tend vers $+\infty$ de la distance minimale entre un point du cercle de rayon $r > 0$ centré en l'origine et un point du réseau $\mathbb{Z}^2$.

Solution de Michel Lafond (Dijon), Jean Lefort (Wintzenheim), Emmanuel Moreau (Joigny), Pierre Renfer (Ostwald), Daniel Saada (Rambouillet) — Pour $r > 0$, on note $d(r)$ la distance minimale entre un point du cercle de rayon r centré en l'origine et un point du réseau $\mathbb{Z}^2$:

$$d(r) = \min\left\{\left|r - \sqrt{x^2 + y^2}\right| ; x, y \in \mathbb{Z}\right\}.$$

On introduit $p = [r]$ la partie entière de r, et également $q = \left[\sqrt{r^2 - p^2}\right]$. Le point (p,q) appartient au réseau $\mathbb{Z}^2$ et la distance de ce point au cercle de rayon r centré en l'origine est

$$\left|r - \sqrt{p^2 + q^2}\right|$$

Par définition,

$$p \leq r < p + 1$$

et

$$q^2 \leq r^2 - p^2 < (q+1)^2,$$

donc

$$0 \leq r^2 - p^2 - q^2 < 2q + 1 \leq 2\sqrt{r^2 - p^2} + 1 < 2\sqrt{2p+1} + 1 \leq 1 + 2\sqrt{2r+1}.$$

Ainsi,

$$0 \leq d(r) \leq \left|r - \sqrt{p^2 + q^2}\right| = \frac{r^2 - p^2 - q^2}{r + \sqrt{p^2 + q^2}} < \frac{1 + 2\sqrt{2r+1}}{r} \xrightarrow[r \to +\infty]{} 0,$$

ce qui montre que $d(r)$ tend vers 0 quand r tend vers $+\infty$.

Commentaires des lecteurs

1. L'inégalité ci-dessus établit la domination $d(r) \underset{r\to+\infty}{=} O\left(\frac{1}{\sqrt{r}}\right)$. Après une « exploration informatique », Michel Lafond pense que $d(r) \leq \frac{C}{\sqrt{r}}$ avec une constante $C \simeq 0{,}61$.
2. Daniel Saada remarque que le résultat de l'énoncé est manifestement faux dans $\mathbb{R}$ mais vrai pour $n \geq 2$ dans $\mathbb{R}^n$ muni de la distance euclidienne (considérer le point de coordonnées $(p, q, 0, \ldots, 0)$). Il pose ensuite la question d'un tel résultat dans d'autres espaces, par exemple $\mathbb{R}^{\mathbb{N}}$, mais ce dernier espace n'est pas – à ma connaissance – muni d'un produit scalaire « naturel ».

Problème 480-2

Pour $n \in \mathbb{N}^*$, S_n désigne le groupe des permutations de l'ensemble $[[1, n]]$. Pour chaque permutation $\sigma \in S_n$, on note $\omega(\sigma)$ le nombre d'orbites de σ. Factoriser le polynôme $P_n(X) = \sum_{\sigma \in S_n} X^{\omega(\sigma)}$.

Solution de Franck Gautier (Pérignat lès Sarlièves), Moubinool Omarjee (Paris), Pierre Renfer (Ostwald) — Pour $n \in \mathbb{N}^*$ et $k \in [[1, n]]$, on note $s(n, k)$ le nombre de permutations de $[[1, n]]$ ayant k orbites. Alors

$s(n, n) = 1$;
$s(n, k) = s(n-1, k-1) + (n-1)\, s(n-1, k) \qquad (2 \leq k < n-1)$;
$s(n, 1) = (n-1)!$.

En effet, les conditions aux bords sont obtenues respectivement pour l'identité et pour les cycles de longueur n. Pour démontrer la relation de récurrence, on fixe deux entiers k, n tels que $2 \leq k \leq n-1$ et une permutation $f \in S_n$ ayant k orbites. Si $f(1) = 1$, la restriction de f à $[[2, n]]$ possède $k-1$ orbites soit $s(n-1, k-1)$ choix. Sinon $f(1)$ est un entier $i \in [[2, n]]$ et la composée $(1, i) \circ f$ laisse fixe 1 et sa restriction à $[[2, n]]$ possède k orbites soit $n-1$ choix pour $f(1) = i$ et $s(n-1, k)$ choix pour $(1, i) \circ f$. D'où la relation.
Le polynôme P_n s'écrit

$$P_n = \sum_{k=1}^{n} s(n,k) X^k.$$

On va démontrer qu'il est égal au polynôme

$$Q_n = X(X+1)\ldots(X+n-1).$$

La relation

$$Q_n(X) = Q_{n-1}(X)(X+n-1) \quad (n \geq 2)$$

montre que les coefficients $a_{n,k}$ de Q_n vérifient la même relation de récurrence que les entiers $s(n, k)$. Et les conditions aux bords sont les mêmes :

$$a_{n,n} = 1 \text{ et } a_{n,1} = (n-1)!.$$

Les polynômes P_n et Q_n sont donc égaux.

Autre solution — Si X est un ensemble, on note S_X l'ensemble des permutations de X. Dans le cas où $X = [[1, n]]$, on note $S_n = S_X$. On fixe $n \in \mathbb{N}$ et l'on cherche une relation entre P_{n+1} et P_n. Pour $\sigma \in S_{n+1}$, on note U_σ l'orbite sous σ de l'élément $n+1$ et $V_\sigma = [[1, n+1]] - U_\sigma$. Le cardinal de V_σ peut valoir 0, 1, …,n. Déterminer $\sigma \in S_{n+1}$, c'est se donner

1. k, un entier de $[[0, n]]$, qui sera le cardinal de V_σ,
2. A_k, une partie à k éléments de $[[1, n]]$, qui sera la partie V_σ,
3. δ, une permutation de A_k, restriction de σ à A_k,
4. u, l'orbite sous σ de $n+1$.

Ayant fixé $k \in [[0, n]]$, il y a $\binom{n}{k}$ choix pour A_k. L'orbite sous σ de $n+1$ est un cycle de longueur $n+1-k$:

$$u = (n+1) \mapsto \sigma(n+1) \mapsto \ldots \mapsto \sigma^{n+1-k}(n+1).$$

Pour l'élément $\sigma(n+1)$ qui appartient à $[[1, n]] - A_k$, on a $n-k$ choix, puis $(n-k-1)$ choix pour $\sigma^2(n+1)$ et ainsi de suite, soit au total $(n-k)!$ choix pour le cycle u. La permutation δ parcourt S_{A_k}. Enfin, puisque $\sigma = u \circ \delta$ et que u est un cycle de σ, on a $\omega(\sigma) = 1 + \omega(\delta)$. On peut alors écrire

$$P_{n+1}(X) = \sum_{k=0}^{n} \binom{n}{k} (n-k)! \sum_{\delta \in S_{A_k}} X^{\omega(\delta)+1} = X \sum_{k=0}^{n} \frac{n!}{k!} P_k(X),$$

en identifiant S_{A_k} à S_k et où il faut convenir que $S_{A_0} = \{\mathrm{id}\} = S_0$ et que $P_0 = 1$. En isolant le dernier terme,

$$P_{n+1}(X) = XP_n(X) + nX \sum_{k=0}^{n-1} \frac{(n-1)!}{k!} P_k(X) = XP_n(X) + nP_n(X).$$

La relation $P_{n+1}(X) = (X+n)P_n(X)$ permet alors de montrer par récurrence que pour tout $n \in \mathbb{N}^*$,

$$\sum_{\sigma \in S_n} X^{\omega(\sigma)} = P_n(X) = \prod_{j=0}^{n-1} (X+j).$$

Problème 480-3 (question de Fernand Canonico).

Soit $k, n \in \mathbb{N}$. Est-il vrai que le n-ième terme de la suite de Fibonacci (définie par $F_0 = 0$, $F_1 = 1$, $F_{n+2} = F_{n+1} + F_n$ est divisible par 5^k si et seulement si n l'est ?

Commentaires — Les notations suivantes sont communes aux différentes solutions proposées. On introduit le nombre d'or et son conjugué

$$\varphi = \frac{1+\sqrt{5}}{2} \quad \text{et} \quad \psi = \frac{1-\sqrt{5}}{2}.$$

On rappelle les relations $\varphi + \psi = 1$ et $\varphi\psi = -1$ et la formule de Binet : pour tout $n \in \mathbb{N}$,

$$\mathrm{F}_n = \frac{\varphi^n - \psi^n}{\varphi - \psi}.$$

Enfin, pour $x \in \mathbb{R}$, on note $[x]$ sa partie entière.

Solution de Fernand Canonico (Clermont-Ferrand) — On note $v_5(n)$ la valuation 5-adique de l'entier $n \neq 0$, quantité définie par

$$v_5(n) = \max\left\{k \in \mathbb{N} \,/\, 5^k \text{ divise } n\right\}.$$

Si $x = \dfrac{a}{b}$ est un rationnel non nul, l'entier relatif $v_5(x) = v_5(a) - v_5(b)$ est indépendant des représentants a et b choisis. Pour des rationnels non nuls $x_1, \ldots, x_n$, on montre facilement que

$$v_5\left(\sum_{k=1}^{n} x_k\right) \geq \min\left\{v_5\left(x_k\right) / \, k \in [[1,n]]\right\}.$$

Dans le cas où un seul x_k réalise le minimum, l'inégalité précédente est une égalité. La formule de Binet et la formule du binôme donnent

$$2^{n-1}\mathrm{F}_n = \sum_{k=0}^{\left[\frac{n-1}{2}\right]} \binom{n}{2k+1} 5^k = n(1+q),$$

où le rationnel q est défini par

$$q = \sum_{k=0}^{\left[\frac{n-1}{2}\right]} \binom{n-1}{2k} \frac{5^k}{2k+1}.$$

Pour $k \in \mathbb{N}^*$, $v_5(2k+1) \leq k - 1$ (sinon, 5^k diviserait $2k + 1$, ce qui imposerait $5^k \leq 2k + 1$ et un calcul montre que cela est faux). Ainsi, pour $k \in \mathbb{N}^*$,

$$v_5\left(\binom{n-1}{2k}\frac{5^k}{2k+1}\right) = v_5\left(\binom{n-1}{2k}\right) + v_5\left(\frac{5^k}{2k+1}\right) \geq 1.$$

On en déduit que $v_5(1 + q) = 0$, puis que $v_5(\mathrm{F}_n) = v_5(n)$. Le résultat en découle.

Emmanuel Moreau (Joigny) propose une belle solution à mi-chemin entre celle de Fernand Canonico ci-dessus (calcul de la valuation 5-adiquc de F_n) et celle de Franck et Patricia Gautier (utilisation do la suite de Lucas) exposée ci-dessous.

Solution de Franck et Patricia Gautier (Pérignat lès Sarliève) — On commence par établir un lemme qui correspond au cas particulier $k = 1$.

Lemme 1. *Pour $n \in \mathbb{N}$, 5 divise F_n si et seulement si 5 divise n.*

Preuve — Si $n = 0$, c'est évident. Pour $n \in \mathbb{N}^*$, on écrit

$$F_n = \frac{1}{\sqrt{5}}\left(\varphi^n - \psi^n\right) = \sum_{i=0}^{\left[\frac{n-1}{2}\right]} \binom{n}{2i+1} 5^i = \frac{1}{2^{n-1}}\left(n + \sum_{i=0}^{\left[\frac{n-1}{2}\right]} \binom{n}{2i+1} 5^i\right).$$

Comme 5 est premier avec 2 et que 5 divise la somme $\sum_{i=0}^{\left[\frac{n-1}{2}\right]} \binom{n}{2i+1} 5^i$, alors 5 divise F_n si et seulement si 5 divise n.

On introduit (L_n), la suite de Lucas, définie par les conditions $L_0 = 2$, $L_1 = 1$, $L_{n+2} = L_{n+1} + L_n$. Par les méthodes usuelles, on montre que pour tout $n \in \mathbb{N}$,

$$L_n = \varphi^n + \psi^n.$$

Lemme 2. *Pour tout $n \in \mathbb{N}$,* $F_{5n} = F_n \times \left(L_{4n} + (-1)^n L_{2n} + 1\right)$.

Preuve — Pour $n \in \mathbb{N}$,

$$\begin{aligned} F_{5n} &= \frac{1}{\sqrt{5}}\left(\left(\varphi^n\right)^5 - \left(\psi^n\right)^5\right) \\ &= \frac{1}{\sqrt{5}}\left(\varphi^n - \psi^n\right)\left(\varphi^{4n} + \varphi^{3n}\psi^n + \varphi^{2n}\psi^{2n} + \varphi^n\psi^{3n} + \psi^{4n}\right) \\ &= F_n \times \left(L_{4n} + (-1)^n L_{2n} + 1\right), \end{aligned}$$

en utilisant la relation $\varphi\psi = -1$.

On pose désormais, pour $n \in \mathbb{N}$, $U_n = L_{4n} + (-1)^n L_{2n} + 1$, donc $F_{5n} = F_n \times U_n$.

Lemme 3. *Pour tout $n \in \mathbb{N}$, 5 divise U_n et 25 ne divise pas U_n.*

Preuve — Comme $U_0 = 5 = U_1$, le résultat est établi pour $n = 0$ et $n = 1$.

Pour $n > 2$, on écrit $\varphi^2 = \dfrac{3+\sqrt{5}}{2}$, $\varphi^4 = \dfrac{7+3\sqrt{5}}{2}$ et les relations conjuguées, puis

$$\begin{aligned}
\mathrm{U}_n &= \left(\varphi^4\right)^n + \left(\psi^4\right)^n + (-1)^n\left(\left(\varphi^2\right)^n + \left(\psi^2\right)^n\right) + 1 \\
&= \frac{1}{2^n}\left(\left(7+3\sqrt{5}\right)^n + \left(7-3\sqrt{5}\right)^n + (-1)^n\left(\left(3+\sqrt{5}\right)^n + \left(3-\sqrt{5}\right)^n\right) + 2^n\right) \\
&= \frac{1}{2^n}\left(2\sum_{p=0}^{\left[\frac{n}{2}\right]}\binom{n}{2p}7^{n-2p}3^{2p}5^p + 2(-1)^n\,2\sum_{p=0}^{\left[\frac{n}{2}\right]}\binom{n}{2p}3^{n-2p}5^p + 2^n\right).
\end{aligned}$$

En isolant dans les sommes les termes obtenus pour $p = 0$, cela prouve que 5 divise U_n si et seulement si 5 divise $2\,(7^n + (-3)^n) + 2^n$. Or

$$\begin{aligned}
2\left(7^n + (-3)^n + 2^n\right) &\equiv 2\left(2^n + 2^n\right) + 2^n \mod 5 \\
&\equiv 5 \times 2^n \mod 5 \\
&\equiv 0 \mod 5.
\end{aligned}$$

d'où le premier point.

Si $n = 0$ ou 1, $\mathrm{U}_0 = \mathrm{U}_1 = 5$ n'est pas divisible par 25. Pour $n \geq 2$, on va prouver que $2^n\mathrm{U}_n$ n'est pas divisible par 25. Pour cela, dans l'expression de U_n obtenue dans le point précédent, on isole les ternies obtenus pour $p = 0$ et $p = 1$:

$$\begin{aligned}
2^n\mathrm{U}_n = {} & 2\sum_{p=2}^{\left[\frac{n}{2}\right]}\binom{n}{2p}7^{n-2p}3^{2p}5^p + 2(-1)^n\,2\sum_{p=2}^{\left[\frac{n}{2}\right]}\binom{n}{2p}3^{n-2p}5^p \\
& + 2\left(7^n + (-3)^n\right) + 2^n + 5n(n-1)\left(9\cdot 7^{n-2} + (-3)^{n-2}\right).
\end{aligned}$$

Ainsi, U_n est divisible par 25 si et seulement si l'expression

$$2\left(7^n + (-3)^n\right) + 2^n + 5n(n-1)\left(9\cdot 7^{n-2} + (-3)^{n-2}\right)$$

l'est. En écrivant $7 = 2 + 5$ et $-3 = 2 - 5$ et en utilisant la formule du binôme de Newton, on prouve que

$$2\left(7^n + (-3)^n\right) + 2^n + 5n(n-1)\left(9\cdot 7^{n-2} + (-3)^{n-2}\right) \equiv 5\cdot 2^n \mod 25.$$

Ainsi U_n n'est pas divisible par 25.

Pour tout $n \in \mathbb{N}$, on pose $\mathrm{U}_n = 5\mathrm{V}_n$ où V_n est un entier premier avec 5. Pour finir, le lemme suivant permet de répondre positivement à la question posée.

Lemme 4. *La valuation 5-adique de* F_n *est la même que celle de* n.

Preuve — Soit $n \in \mathbb{N}$, que l'on écrit $n = 5^k q$ avec $k \in \mathbb{N}$ et q premier avec 5. On va prouver que $\mathrm{F}_n = 5^k\mathrm{H}_n$ où H_n est un entier naturel premier avec 5. Pour $k = 0$ le résultat est fourni par le lemme 1. Pour $k \geq 1$, grâce au lemme 2, on montre par récurrence sur k que

$$F_{5^k q} = F_q \prod_{p=0}^{k-1} U_{5^p q},$$

soit encore, puisque $U_j = 5V_j$, pour tout $j \in \mathbb{N}$

$$F_{5^k q} = 5^k F_q \prod_{p=0}^{k-1} V_{5^p q},$$

Comme F_q et $V_{5^p q}$ sont premiers avec 5 pour $p \in [[0, k-1]]$, on en déduit que l'entier $H_n = F_q \prod_{p=0}^{k-1} V_{5^p q},$ est aussi premier avec 5.

Solution de Marie-Laure Chaillout (Épinay sur Orge) — Par récurrence ou par division euclidienne du polynôme X^n par $X^2 - X - 1$, on établit, pour tout $n \geq 1$,

$$\varphi^n = F_n \varphi + F_{n-1}.$$

Les premières puissances de φ sont $\varphi^2 = \varphi + 1$, $\varphi^3 = 2\varphi + 1$, $\varphi^4 = 3\varphi + 2$, $\varphi^5 = 5\varphi + 3$. Par ailleurs, pour $n \geq 1$,

$$F_{5n}\varphi + F_{5n-1} = \varphi^{5n} = \left(F_n \varphi + F_{n-1}\right)^5.$$

On développe par la formule du binôme, on utilise les calculs des puissances de φ ci-dessus pour obtenir

$$F_{5n}\varphi + F_{5n-1} = A_n \varphi + B_n$$

avec A_n, B_n entiers, l'expression de B_n important peu et

$$A_n = 5F_n\left(F_n^4 + 3F_n^3 F_{n-1} + 4F_n^2 F_{n-1}^2 + 2F_n F_{n-1}^3 + F_{n-1}^4\right).$$

L'irrationalité de φ rendant possible l'identification du coefficient devant φ, on en déduit que $F_{5n} = A_n$, i. e.

$$F_{5n} = 5F_n P_n \text{ avec } P_n = F_n^4 + 3F_n^3 F_{n-1} + 4F_n^2 F_{n-1}^2 + 2F_n F_{n-1}^3 + F_{n-1}^4. \qquad (1)$$

Par ailleurs, la formule de Binet donne

$$2^{n-1} F_n = n + 5 \sum_{j=1}^{\left[\frac{n-1}{2}\right]} \binom{n}{2j+1} 5^{j-1}.$$

Donc 5 divise F_n si et seulement si 5 divise n. De plus,

$$2^{n-1} F_n \equiv n \bmod 5.$$

$$2^{n-1} F_{n-1} \equiv 2(n-1) \bmod 5.$$

Comme $16 \equiv 1 \bmod 5$, on déduit de ces congruences que, module 5,

$$\begin{aligned}
P_n &\equiv 2^{4(n-1)} P_n \\
&\equiv \left(2^{n-1}F_n\right)^4 + 3\left(2^{n-1}F_n\right)^3\left(2^{n-1}F_{n-1}\right) + 4\left(2^{n-1}F_n\right)^2\left(2^{n-1}F_{n-1}\right)^2 \\
&\qquad + 2\left(2^{n-1}F_n\right)\left(2^{n-1}F_{n-1}\right)^3 + \left(2^{n-1}F_{n-1}\right)^4 \\
&\equiv n^4 + 6n^3(n-1) + 16n^2(n-1)^2 + 16n(n-1)^3 + 16(n-1)^4 \\
&\equiv 1.
\end{aligned}$$

Ainsi,

$$v_5(F_{5n}) = 1 + v_5(F_n) \qquad (n \in \mathbb{N}^*).$$

Soit maintenant $n \in \mathbb{N}^*$ que l'on décompose en $n = 5^k q$ avec $q \in \mathbb{N}^*$ non divisible par 5. Alors

$$v_5(F_n) = k + v_5(F_q),$$

et puisque 5 ne divise pas $_\theta$, il ne divise pas non plus F_q. Finalement,

$$v_5(F_n) = k = v_5(n),$$

ce qui permet de conclure.

Solution de Pierre Renfer (Ostwald) — On démontre par récurrence sur $k \in \mathbb{N}^*$ que pour tout $n \in \mathbb{N}$, F_n est divisible par 5^k si et seulement si n l'est et que de plus F_{5^k} n'est pas divisible par 5^{k+1}. Pour initialiser au rang $k = 1$, on établit pour tout $n \in \mathbb{N}$,

$$F_{n+5} = 5F_{n+1} + 3F_n,$$

puis

$$F_{n+5} \equiv 3F_n \mod 5,$$

et donc pour $p \in \mathbb{N}$,

$$F_{n+5p} \equiv 3^p F_n \mod 5,$$

Les premières valeurs de F_n mod 5 étant

n	0	1	2	3	4
F_n mod 5	0	1	1	2	3

on en déduit que $F_n \equiv 0$ mod 5 si et seulement $n \equiv 0$ mod 5. Comme de plus $F_5 = 5$ n'est pas divisible par 25, l'initialisation est achevée.
On suppose la propriété établie à un certain rang k et on va la montrer au rang $k+1$.
On traitera séparément les cas $k = 1$ et $k \geq 2$. Pour $n \in \mathbb{N}$, on note

$$G_n^k = \frac{1}{5^k} F_{n5^k}.$$

Par hypothèse de récurrence, la suite G^k est à valeurs entières. D'après la formule de Binet,

$$G_n^k = \frac{1}{5^k\sqrt{5}}\left(\Phi^n - \Psi^n\right)$$

où

$$\Phi = \varphi^{5^k} = \left(\frac{1+\sqrt{5}}{2}\right)^{5^k} \quad \text{et} \quad \Psi = \psi^{5^k} = \left(\frac{1-\sqrt{5}}{2}\right)^{5^k}.$$

La suite G^k est donc récurrente linéaire d'ordre 2 et vérifie une relation du type

$$G_{n+2}^k = a_k G_{n+1}^k + b_k G_n^k \quad (n \in \mathbb{N})$$

avec

$$a_k = \Phi + \Psi = \varphi^{5^k} + \psi^{5^k}$$

qui est en réalité le terme L_{5^k} de la suite de Lucas et

$$b_k = -\Phi\Psi = -(\varphi\psi)^{5^k} = 1.$$

Pour $k = 1$, puisque $a_1 = 11 \equiv 1 \bmod 5$ et que $G_0^1 = F_0$, $G_1^1 = \frac{F_5}{5} = 1 = F_1$, la suite G^1 a les mêmes classes modulo 5 que la suite de Fibonacci. Ainsi, $G_n^1 = \frac{F_{5n}}{5}$ est divisible par 5 si et seulement si n l'est. Compte tenu de l'initialisation, F_n est divisible par 25 si et seulement si n l'est. On calcule ensuite modulo 25 les cinq premiers termes de la suite G^1. On trouve $G_5^1 \equiv 5 \bmod 25$ donc F_{25} n'est pas divisible par 5^2. Ainsi, la propriété est établie au rang $k = 2$.
Pour $k \geq 2$, l'hypothèse au rang k implique que $F_{5^k} \equiv 0 \bmod 25$ et que $F_{5^k-1} \bmod 25$ est un élément inversible α_k de $\mathbb{Z}/25\mathbb{Z}$. Une récurrence facile montre que

$$L_n = F_n + 2F_{n-1} \quad (n \geq 1)$$

et que

$$F_n^2 - F_{n-1}^2 - F_n F_{n-1} = F_n^2 - F_{n+1}F_{n-1} = (-1)^{n-1},$$

donc

$$\left(F_{5^k-1}\right)^2 \equiv -1 \mod 25$$

et ainsi,

$$a_k^2 = \left(L_{5^k}\right)^2 = \left(F_{5^k} + 2F_{2^k-1}\right)^2 \equiv -4 \mod 25.$$

Suite page 837

On note β_k la classe de $G_1^k = \dfrac{F_{5^k}}{5^k} \mod 25$. C'est un élément inversible de $\mathbb{Z}/25\mathbb{Z}$.

On calcule alors les classes modulo 25 des premiers termes de la suite G^k :

$$0, \beta_k, 2\alpha_k\beta_k, 3\alpha_k^2\beta_k, 4\alpha_k^3\beta_k, 5\alpha_k^4\beta_k, \ldots$$

Ainsi, $G_5^k = \dfrac{F_{5^{k+1}}}{5^k}$ est divisible par 5 mais pas par 25, c'est-à-dire que $F_{5^{k+1}}$ est divisible par 5^{k+1} mais pas par 5^{k+2}. Ensuite, on calcule les classes modulo 5 des premiers termes de la suite G^k :

$$0, \beta'_k, 2\alpha'_k\beta'_k, 3\alpha'^2_k\beta'_k, 4\alpha'^3_k\beta'_k, 0, \ldots$$

ce qui prouve que

$$G_{n+5}^k \equiv 4F_{5^k-1}G_n^k \mod 5.$$

Ainsi, $G_n^k = \dfrac{F_{n5^k}}{5^k}$ est divisible par 5 si et seulement si n l'est. Finalement, F_n est divisible par 5^{k+1} si et seulement si n l'est.