Solution

Cet énoncé, que Charles Notari m’a soumis en octobre 1998, figurait dans le livre de Denis Gerll et Georges Girard : *Les Olympiades internationales de mathématiques*

(Hachette 1976, réimprimé par Jacques Gabay en 1994). Mais il a fallu attendre l'ouvrage *Supermath* de Pierre Bornsztein (paru en novembre 1999 chez Vuibert, quelques semaines avant le bulletin 425 de l'APMEP contenant cet énoncé) pour en trouver une solution rédigée (p. 174, énoncé : al 34).

Tout d'abord, ma rédaction de l'énoncé pouvait induire en erreur : j'aurais dû dire « … prend consécutivement deux valeurs entières », car on ne suppose évidemment pas que u_k et u_{k+1} sont deux entiers consécutifs. Toutes mes excuses à Marie-Laure Chaillout. Charles Notari écrivait seulement : « montrer que si u_k et u_{k+1} sont entiers tous les u_n sont entiers », et l'énoncé publié dans l'ouvrage d'Olympiades : « démontrer que, si pour un entier k, u_k et u_{k+1} sont des entiers, alors pour tout entier n, u_n est un entier ». Par ailleurs, quitte à échanger a et $1/a$, on peut supposer $a > 1$. En outre, la fonction $a^x + \dfrac{1}{a^x}$, qui rappelle la fonction cosinus hyperbolique, vérifie pour tout couple (n, m) :

$$u_{n+m} + u_{n-m} = u_n u_m.$$

En particulier, pour tout $n \geq 1$,

$$u_{n+1} = u_n u_1 - u_{n-1}.$$

Dans la mesure où, quel que soit a, $u_0 = 2$ est entier, il suffit que u_1 soit entier pour en déduire par récurrence que tous les u_n sont entiers. Alain Pichereau signale que la relation

$$u_{n+1} = u_n u_1 - u_{n-1}$$

peut s'obtenir en remarquant que a et $1/a$ sont tous deux racines de $x^2 - u_1 x + 1$, donc de $x^{n+1} - u_1 x^n + x^{n-1}$.

Un peu rerédigée, la solution de Charles Notari est assez astucieuse. Si

$$u_k = a^k + \frac{1}{a^k} = p \text{ entier,}$$

et

$$u_{k+1} = a^{k+1} + \frac{1}{a^{k+1}} = q \text{ entier,}$$

alors

$$a^k - \frac{1}{a^k} = \sqrt{p^2 - 4}$$

et

$$a^{k+1} - \frac{1}{a^{k+1}} = \sqrt{q^2 - 4}\,.$$

On a donc :

$$u_{2k+1} + u_1 = u_{k+1} u_k = pq$$

ainsi que :

$$u_{2k+1} - u_1 = \sqrt{(p^2 - 4)(q^2 - 4)}.$$

Or

$$a^k = \frac{p + \sqrt{p^2 - 4}}{2}$$

et

$$a^{k+1} = \frac{q + \sqrt{q^2 - 4}}{2},$$

donc

$$a^{k(k+1)} = \left[\frac{p + \sqrt{p^2 - 4}}{2}\right]^{k+1} = \left[\frac{q + \sqrt{q^2 - 4}}{2}\right]^{k}.$$

En développant par la formule du binôme, on trouve des entiers A > 0, B > 0 et C tels que :

$$\mathrm{A}\sqrt{p^2 - 4} - \mathrm{B}\sqrt{q^2 - 4} = \mathrm{C},$$

soit, en élevant au carré :

$$2\mathrm{AB}\sqrt{(p^2 - 4)(q^2 - 4)} = \mathrm{D} \text{ entier}.$$

$\sqrt{(p^2 - 4)(q^2 - 4)}$ est rationnel, donc entier, et il est manifestement de même parité que pq. D'où

$$u_1 = \frac{pq - \sqrt{(p^2 - 4)(q^2 - 4)}}{2}$$

est entier, ce qui achève la démonstration.

Mais j'ai reçu d'autres solutions, de Pierre BORNSZTEIN (95-Pontoise), Jean-Marc BRESLAW (97-St Denis de la Réunion), Alain CORRE (03-Moulins), Christian DUFIS (87-Limoges), Bernard MALFON (28-Marboue), René MANZONI (76-Le Havre), Moubinool OMARJEE (75-Paris), Alain PICHEREAU (16-St Yrieix), G. PRIGENT (93-Dugny), Pierre SAMUEL (92-Bourg la Reine), sans compter trois réponses erronées.

Une fois établi que $u_1 u_{2k+1} = p^2 + q^2 - 4$, donc que u_1 est solution d'un trinôme :

$$\mathrm{T}(x) = x^2 - pqx + (p^2 + q^2 - 4),$$

plusieurs stratégies sont utilisées. Par exemple, Christian Dufis et G. Prigent montrent par récurrence que si $u_1 = r_1 - s_1\sqrt{b}$ avec b entier, r_1 et s_1 rationnels strictement positifs ($r_1 > 2$), alors $u_n = r_n - s_n\sqrt{b}$, les suites de rationnels r_n et s_n étant strictement croissantes. Il n'est donc pas possible que u_k soit rationnel si b n'est pas un carré parfait. Bernard Malfon explicite les racines complexes de

$$Q_n(x) = x^{2n} - u_n x^n + 1,$$

montrant ainsi que si k et ℓ sont premiers entre eux, Q_k et Q_ℓ ont pour PGCD : $x - u_1$. Or l'algorithme d'Euclide prouve que si u_k et u_ℓ sont entiers, le PGCD de Q_k et Q_ℓ est à coefficients entiers. Pierre Bornsztein écrit que si u_k est entier, u_{nk} est entier pour tout n, d'où il déduit que non seulement $u_1 + u_{2k+1}$ et $u_1 \times u_{2k+1}$ sont entiers, mais $u_1 + u_{2k^2-1}$ et $u_1 \times u_{2k^2-1}$ sont eux aussi entiers : racine de deux trinômes unitaires $x^2 - Sx + P$ et $x^2 - S'x + P'$ distincts, u_1 ne peut être qu'entier. Jean-Marc Breslaw utilise le polynôme T_n, unitaire à coefficients entiers, tel que si $u_1 = x$, $u_n = T_n(x)$. Si u_n est entier, le reste de la division euclidienne de $T_n(x) - u_n$ par $T(x) = x^2 - pqx + (p^2 + q^2 - 4)$ étant du premier degré à coefficients entiers, x ne peut être que rationnel, donc entier car racine du trinôme unitaire $T(x)$.

Le passage de « rationnel » à « entier » jouait d'ailleurs un rôle important dans ce problème. On appelle entier algébrique toute racine d'un polynôme unitaire à coefficients entiers, « unitaire » signifiant : dont le terme de plus haut degré a pour coefficient 1. La somme et le produit de deux entiers algébriques est un entier algébrique, les racines carrées, cubiques, … d'entiers algébriques sont des entiers algébriques, et tout entier algébrique appartenant à $\mathbf{Q}$ appartient à $\mathbf{Z}$: Pierre Bornsztein le démontre comme lemme, et G. Prigent démontre que si $\sqrt{n}$ est rationnel, $\sqrt{n}$ est entier. Très généralement, si $P(x)$ est un polynôme dont le terme de plus haut degré est x^n, pour tout rationnel irréductible $\frac{p}{q}$, $q^{n-1}P\left(\frac{p}{q}\right)$ est non entier, car p^n n'est pas divisible par q et tous les autres termes sont entiers, donc $P\left(\frac{p}{q}\right)$ est non nul. Tous les nombres intervenant dans le présent problème sont en fait des entiers algébriques, malgré le dénominateur 2 qui encombre de temps en temps : le nombre d'or $\frac{\sqrt{5}+1}{2}$ est entier puisqu'il est racine de $x^2 - x - 1$.

Une bonne connaissance des corps quadratiques donnait à ce problème un aspect différent. Par une méthode voisine de celle de Charles Notari, René Manzoni obtient une égalité :

$$A\sqrt{p^2-4} + C = B\sqrt{q^2-4} + D.$$

« Sachant que les réels $\sqrt{p^2-4}$ et $\sqrt{q^2-4}$ ne peuvent être qu'irrationnels, il apparaît que : $C = D$ et $A\sqrt{p^2-4} = B\sqrt{q^2-4}$ », écrit-il. En fait, observent Alain

Corre et Pierre Samuel, $a^k = \dfrac{p + \sqrt{p^2 - 4}}{2}$ et $a^{k+1} = \dfrac{q + \sqrt{q^2 - 4}}{2}$ appartiennent chacun à un corps quadratique $\mathbf{Q}\left(\sqrt{p^2 - 4}\right)$ et $\mathbf{Q}\left(\sqrt{q^2 - 4}\right)$, et $a^{k(k+1)}$ appartient à l'intersection de ces deux corps quadratiques, qui sont chacun un **Q**-espace vectoriel de dimension 2. Si ces corps sont distincts, leur intersection se limite à **Q**. Mais $a^{k(k+1)}$ ne peut pas être rationnel, donc ces deux corps quadratiques sont confondus : il existe b, u et v entiers tels que $\sqrt{p^2 - 4} = u\sqrt{b}$ et $\sqrt{q^2 - 4} = v\sqrt{b}$, d'où $\sqrt{(p^2 - 4)(q^2 - 4)} = uvb$ est un entier naturel. Pierre Samuel fait même appel au théorème des unités : $a^k = \dfrac{p + \sqrt{p^2 - 4}}{2}$ a pour inverse son conjugué : $\dfrac{1}{a^k} = \dfrac{p - \sqrt{p^2 - 4}}{2}$. C'est donc une unité du corps quadratique, et les unités d'un corps quadratique sont (au signe près) les puissances de la plus petite d'entre elles, U. Qui plus est, pour toute unité U^k, $\mathrm{U}^k + \mathrm{U}^{-k}$ est un entier naturel. Si a^n et $a^{n'}$ sont des unités d'un même corps quadratique $\mathbf{Q}\left(\sqrt{b}\right)$, alors $a^n = \mathrm{U}^j$ et $a^{n'} = \mathrm{U}^{j'}$: n et n' étant premiers entre eux, $nj' = n'j$ entraîne : $j = kn$ et $j' = kn'$, $a = \mathrm{U}^k$ est une unité, et $a + \dfrac{1}{a}$ est donc un entier naturel.