Ça tombe juste(*)

Éliane Vandembroucq(**)

« x désignant un angle compris au sens large entre 0° et 90°, trouvez sin x sachant que cos x = … ». Quelles valeurs décimales peut-on donner à cos x pour que la réponse à cet exercice soit aussi un nombre décimal ?

La restriction des valeurs pour l'angle permet de nous limiter aux valeurs positives pour cos x. Aussi, dans un premier temps, nous pouvons proposer la formulation suivante du problème. Avec $\{\sin x ; \cos x\} = \{\alpha ; \beta\}$.

(I) : trouver toutes les paires $\{\alpha ; \beta\} \subset \mathbb{D}^+$ telles que $\alpha^2 + \beta^2 = 1$.

Chercher des paires plutôt que des couples ne supprime pas de solutions au problème initial puisque, α et β étant décimaux, il n'y a pas de solutions où $\alpha = \beta$.
Nous connaissons tous, la solution {0,6 ; 0,8} de ce problème.
Remarquons que dans une solution, les zéros inutiles étant supprimés, les nombres α et β ont exactement le même nombre de chiffres après la virgule. Nous appellerons solution « d'ordre n » une solution où α et β ont n chiffres après la virgule. La solution ci-dessus est la solution unique d'ordre 1 ; {0 ; 1} est la solution unique d'ordre 0.
Au passage, dans ce travail sera démontrée la propriété inattendue suivante :
« *Quel que soit le nombre entier n, il existe une seule paire de nombres décimaux positifs ayant n chiffres après la virgule, dont la somme des carrés est égale à* 1. »
Ces nombres seront aussi les uniques valeurs décimales d'ordre n de cos x satisfaisant à la condition imposée. De plus, nous découvrirons une méthode pour calculer ces nombres.
Pour l'instant, voici une deuxième formulation de notre problème, comme le permet la remarque précédente. En posant, $\alpha = \mathrm{A} \cdot 10^{-n}$ et $\beta = \mathrm{B} \cdot 10^{-n}$:

(II) : pour tout n, trouver toutes les paires $\{\mathrm{A} ; \mathrm{B}\} \subset \mathbb{N} \setminus 10\mathbb{N}$ telles que $\mathrm{A}^2 + \mathrm{B}^2 = 10^{2n}$.

Dans cette nouvelle formulation, ({A ; B} est une solution) si et seulement si ((A ; B ; 10^n) est un triplet pythagoricien).

Avant de poursuivre, rappelons à ce sujet, quelques définitions et propriétés.

D1. (A ; B ; C) est un triplet pythagoricien $\Longleftrightarrow$ ((A ; B ; C) $\in \mathbb{N} \times \mathbb{N} \times \mathrm{N}^*$ et $\mathrm{A}^2 + \mathrm{B}^2 = \mathrm{C}^2$).

D2. Le triplet pythagoricien (a ; b ; c) est premier $\Longleftrightarrow$ PGCD(a ; b ; c) = 1.

P1. $\forall k \in \mathbb{N}^*$ ((A ; B ; C) est un triplet pythagoricien) $\Longleftrightarrow$ ((kA ; kB ; kC) est un triplet pythagoricien).

(*) Atelier aux Journées Nationales de Paris 2010
(**) eliane.vandembroucq@gmx.fr

P2. ((A ; B ; C) est un triplet pythagoricien) $\Longrightarrow$ (PGCD(A ; B) = PGCD(A ; C) = PGCD(B ; C)).
P3. ((a ; b ; c) est un triplet pythagoricien premier) $\Longrightarrow$ (c est impair).
P4. On trouve tous les triplets pythagoriciens premiers, sans répétition, en choisissant de toutes les manières possibles deux nombres entiers p et q, premiers entre eux et p impair en posant : $c = p^2 + (2q)^2$ et $\{a\ ;\ b\} = \{|p^2 - (2q)^2|\ ;\ 4pq\}$.
Remarquons que la propriété P4 *affirme en particulier que, si un nombre c impair est décomposable en une somme de deux carrés de nombres premiers entre eux, alors il en est de même pour* c^2. *Nous utiliserons cette remarque un peu plus loin.*
Revenons pour l'instant à la formulation (II) de notre problème et remarquons que le triplet pythagoricien (A ; B ; 10^n) n'est pas premier car la propriété P3 permet de l'affirmer. Le PGCD des trois termes est forcément 2^n. En effet, le triplet pythagoricien (A ; B ; 10^n) doit être simplifié par 2^n pour rendre le troisième terme impair. A et B sont donc multiples de 2^n ; si ils étaient aussi multiples de 5, ils seraient multiples de 10, ce qui est exclu. Dans ces conditions, la propriété P1 permet de le simplifier et on peut en déduire une troisième formulation de notre problème.

En posant, $A = a \cdot 2^n$ et $B = b \cdot 2^n$,

(III) : pour tout n, trouver toutes les paires $\{a\ ;\ b\} \subset \mathbb{N} \setminus 5\mathbb{N}$ telles que $a^2 + b^2 = 5^{2n}$.

Utilisant enfin la propriété P4, on écrit une quatrième formulation du problème. Avec $\{a\ ;\ b\} = \{|p^2 - (2q)^2|\ ;\ 4pq\}$,

(IV) : pour tout n, trouver les couples $(p\ ;\ q) \in (\mathbb{N} \setminus 5\mathbb{N})^2$ tels que $p^2 + (2q)^2 = 5^n$ et p impair.

On est donc ramené à prouver, pour tout n, l'existence et l'unicité d'une solution de rang n à l'un des problèmes (I), (II), (III) ou (IV), existence et unicité qui se transmettront aux autres.
Les solutions au problème (I) citées précédemment permettent de trouver en résolvant des systèmes simples, les solutions respectives (et uniques) des problèmes (III) et (IV) :

à l'ordre 0 : $\{a_0\ ;\ b_0\} = \{1\ ;\ 0\}$ et $(p_0\ ;\ q_0) = (1; 0)$,
à l'ordre 1 : $\{a_1\ ;\ b_1\} = \{3\ ;\ 4\}$ et $(p_1\ ;\ q_1) = (1\ ;\ 1)$.

Comme annoncé, utilisons la remarque relative à la propriété P4 du triplet pythagoricien pour découvrir quelques nouvelles solutions. Partant, à l'ordre 1, de la solution $\{a_1\ ;\ b_1\} = \{3\ ;\ 4\}$ et en appliquant la dite remarque, on trouve une solution à l'ordre 2 du problème (IV) : $(p\ ;\ q) = (3\ ;\ 2)$ car $3^2 + (2 \times 2)^2 = 5^2$.
Plus généralement, une solution d'ordre n du problème (III) permet de calculer une solution d'ordre $2n$ du problème (IV). Cette remarque permet des « raccourcis », mais ne donne pas de solutions à tous les ordres, ni ne prouve l'unicité annoncée.

Pour commencer l'étude du cas général, nous établirons deux lemmes.
Lemme 1. *Quels que soient les nombres entiers p et q, ou les nombres $p + 4q$ et $p - q$ sont tous les deux multiples de 5, ou aucun d'entre eux ne l'est. Il en est de même pour $p - 4q$ et $p + q$.*

En effet, puisque $4 \equiv -1$ modulo 5, il s'ensuit que $p + 4q \equiv p - q$ modulo 5.
<u>Lemme 2</u>. *Quels que soient les entiers p et q premiers avec 5, et quel que soit $n \geq 1$, si $p^2 + (2q)^2 = 5^n$, alors un et un seul des deux nombres $p + q$ ou $p - q$ est multiple de 5.*
Partant de l'hypothèse $p^2 + (2q)^2 = 5^n$, avec $n \geq 1$, on peut en déduire $p^2 + 4q^2 \equiv 0$ modulo 5, ce qui peut s'écrire $p^2 - q^2 \equiv 0$ modulo 5, ou encore $(p + q)(p - q) \equiv 0$ modulo 5. Ceci équivaut à $p + q \equiv 0$ ou $p - q \equiv 0$ modulo 5, car 5 est premier.
D'autre part, on ne peut avoir $p + q \equiv 0$ et $p - q \equiv 0$ modulo 5, car on aurait alors $p + q \equiv p - q$, ce qui entraînerait $2q \equiv 0$ modulo 5 et finalement $q \equiv 0$ modulo 5, ce qui est contraire à l'hypothèse du lemme.

Nous pouvons maintenant démontrer l'existence de solutions au problème (IV) pour tout entier $n \geq 1$. Nous allons bien sûr raisonner par récurrence.
À l'ordre 1, nous avons la solution du problème (IV) : $(p_1 ; q_1) = (1 ; 1)$.
Supposons que le problème (IV) a une solution $(p ; q)$ à l'ordre $n \geq 1$. On a alors en particulier $p^2 + (2q)^2 = 5^n$ ou encore $p^2 + 4q^2 = 5^n$. En multipliant à droite par 5 et à gauche par $4 + 1$, on obtient $4p^2 + 16q^2 + p^2 + 4q^2 = 5^{n+1}$.
Or cette égalité peut s'écrire $(p + 4q)^2 + (2|p - q|)^2 = 5^{n+1}$ ou encore $|p - 4q|^2 + (2(p + q))^2 = 5^{n+1}$. Ces égalités qui ont la forme exigée par l'une des conditions du problème (IV) suggèrent deux solutions possibles à ce problème à l'ordre $n + 1$: $(\mathrm{P} ; \mathrm{Q}) = (p + 4q ; |p - q|)$ ou $(\mathrm{P} ; \mathrm{Q}) = (|p - 4q| ; p + q)$. Ces solutions seront valables si les autres conditions sont satisfaites.
D'abord P doit être impair : c'est vérifié dans les deux cas car p étant lui-même impair, $p + 4q$ et $p - 4q$ le sont aussi.

On doit aussi avoir : $\mathrm{P} \notin 5\mathbb{N}$ et $\mathrm{Q} \notin 5\mathbb{N}$. Or, d'après le lemme 1, on sait que dans les deux cas, les deux coordonnées du couple (P ; Q) sont toutes deux multiples de 5 ou aucune ne l'est.
Or l'hypothèse $p^2 + (2q)^2 = 5^n$ étant satisfaite, on déduit du lemme 2 qu'une et une seule des deuxièmes coordonnées $p + q$ ou $p - q$ est multiple de 5. Le couple dont la deuxième coordonnée est multiple de 5 ne peut être solution du problème. Mais l'autre couple respecte la condition : sa deuxième coordonnée n'étant pas multiple de 5, sa première ne l'est pas non plus.
Donc, parmi les deux couples $(p + 4q ; |p - q|)$ et $(|p - 4q| ; p + q)$, un et un seul est solution du problème (IV) au rang $n + 1$.
Ainsi, quel que soit n, le problème (IV) a au moins une solution, mais notre procédé ne permet de n'en calculer qu'une seule.
On peut remarquer que ce procédé permet aussi de passer $(p_0 ; q_0)$ à $(p_1 ; q_1)$ et de $(p_1 ; q_1)$ à la solution déjà trouvée au rang 2.

Notons Φ l'application de $\mathbb{N} \times \mathbb{N}$ dans $\mathbb{N} \times \mathbb{N}$ qui permet de passer d'une solution d'ordre n à une solution d'ordre $n + 1$ pour le (IV) ainsi :

– si $p - q \notin 5\mathbb{N}$, alors $\Phi(p ; q) = (p + 4q ; |p - q|)$,

– si $p - q \in 5\mathbb{N}$, alors $\Phi(p ; q) = (|p - 4q| ; p + q)$.

Définissons une suite de solutions $(p_n ; q_n)_n$ du problème (IV) en posant

$(p_0 ; q_0) = (1 ; 0)$ et $(p_{n+1} ; q_{n+1}) = \Phi(p_n ; q_n)$.
Pour démontrer l'unicité annoncée, il suffira de démontrer qu'une solution quelconque d'ordre n du problème (IV) est égale à $(p_n ; q_n)$.

Commençons par définir, pour tout $i \in \{1; 2; 3; 4\}$, les isomorphismes φ_i de $\mathbb{R}^2$ par le tableau suivant.

i	1	2	3	4
$\varphi_i(p;q)$	$(p+4q;p-q)$	$(p+4q;-p+q)$	$(p-4q;p+q)$	$(-p+4q;p+q)$
$\varphi_i^{-1}(\mathrm{P};\mathrm{Q})$	$\left(\frac{\mathrm{P}+4\mathrm{Q}}{5};\frac{\mathrm{P}-\mathrm{Q}}{5}\right)$	$\left(\frac{\mathrm{P}-4\mathrm{Q}}{5};\frac{\mathrm{P}+\mathrm{Q}}{5}\right)$	$\left(\frac{\mathrm{P}+4\mathrm{Q}}{5};\frac{-\mathrm{P}+\mathrm{Q}}{5}\right)$	$\left(\frac{-\mathrm{P}+4\mathrm{Q}}{5};\frac{\mathrm{P}+\mathrm{Q}}{5}\right)$

En quelque sorte, les applications φ_i sont « derrière » Φ : plus précisément, pour tout $(p ; q)$ solution de rang n du problème (IV), il existe un seul $i \in \{1; 2; 3; 4\}$ tel que $\Phi(p ; q) = \varphi_i(p ; q)$.

Raisonnons par récurrence.
On a démontré que, quel que soit n, le problème (IV) a au moins une solution de rang n, à savoir $(p_n ; q_n)$.
On sait que pour $n = 0$ et $n = 1$, cette solution est unique.
Supposons cette unicité vraie jusqu'à un rang $n \geq 1$; il s'agit alors de la solution $(p_n ; q_n)$, et considérons (P ; Q) une solution de rang $n + 1$.
Démontrons d'abord que (P ; Q) est l'image par l'un des φ_i de $(p_n ; q_n)$.

Quel que soit $i \in \{1;2; 3;4\}$, (P ; Q) a pour antécédent $\varphi_i^{-1}(\mathrm{P} ; \mathrm{Q})$ par φ_i. Pour l'un de ces i, $\varphi_i^{-1}(\mathrm{P} ; \mathrm{Q})$ est-il solution du problème (IV), c'est-à-dire vérifie-t-il les critères correspondants ?

– Tout d'abord, existe-t-il i pour lequel les coordonnées de $\varphi_i^{-1}(\mathrm{P} ; \mathrm{Q})$ sont positives ? On observe que $\varphi_1^{-1}(\mathrm{P} ; \mathrm{Q})$ et $\varphi_3^{-1}(\mathrm{P} ; \mathrm{Q})$ ont la même première coordonnée positive et que leurs deuxièmes coordonnées sont opposées. Donc, un seul de ces deux couples a ses deux coordonnées positives. Ce couple s'écrit : $\left(\frac{\mathrm{P}+4\mathrm{Q}}{5};\frac{|\mathrm{P}-\mathrm{Q}|}{5}\right)$.

De même, un seul des deux couples $\varphi_2^{-1}(\mathrm{P} ; \mathrm{Q})$ et $\varphi_4^{-1}(\mathrm{P} ; \mathrm{Q})$ a ses deux coordonnées positives et s'écrit : $\left(\frac{|\mathrm{P}-4\mathrm{Q}|}{5};\frac{\mathrm{P}+\mathrm{Q}}{5}\right)$.

– Les coordonnées de ces couples sont-elles des nombres entiers ? Elles se présentent comme des fractions de dénominateur 5. Il s'agit donc de savoir si les numérateurs sont multiples de 5. Or, l'hypothèse de récurrence : $\mathrm{P}^2 + (2\mathrm{Q})^2 = 5^{n+1}$ et le lemme 2 permettent de conclure qu'un seul des deux nombres P + Q et P – Q est multiple de 5, donc, un seul des deux couples jusqu'ici retenus a sa deuxième coordonnée entière. Et pour ce couple-là, la première coordonnée est aussi entière d'après le lemme 1. Appelons $(p ; q)$ ce couple.

$(p\ ;q)$ est donc le seul couple parmi les $\varphi_i^{-1}(\mathrm{P}\ ;\mathrm{Q})$ pour i de 1 à 4, dont les coordonnées sont à la fois entières et positives ; nous démontrerons plus loin que ni l'une ni l'autre n'est multiple de 5.

– Pour l'instant, vérifions que la première coordonnée p est impaire. On a $p=\dfrac{\mathrm{P}+4\mathrm{Q}}{5}$ ou $p=\dfrac{|\mathrm{P}-4\mathrm{Q}|}{5}$. Puisque P est impair, chacun de ces quotients a son numérateur impair ; celui des deux qui est entier est aussi impair. Donc, ce critère est bien vérifié par le couple $(p\ ;q)$.

– L'égalité $p^2 + (2q)^2 = 5^n$ est-elle vérifiée ? On a $(p,q)=\left(\dfrac{\mathrm{P}+4\mathrm{Q}}{5};\dfrac{|\mathrm{P}-\mathrm{Q}|}{5}\right)$ ou $(p,q)=\left(\dfrac{|\mathrm{P}-4\mathrm{Q}|}{5};\dfrac{\mathrm{P}+\mathrm{Q}}{5}\right)$. Dans les deux cas : $p^2 + (2q)^2 = \dfrac{5\mathrm{P}^2+20\mathrm{Q}^2}{25}$, ce qui donne après simplification $p^2+(2q)^2=\dfrac{\mathrm{P}^2+4\mathrm{Q}^2}{5}$. Or, par hypothèse de récurrence, $\mathrm{P}^2 + 4\mathrm{Q}^2 = 5^{\nu+1}$. On obtient donc bien $p^2 + (2q)^2 = 5^n$.

–Vérifions enfin que ni p ni q n'est multiple de 5. Si l'un de ces deux nombres était multiple de 5, compte tenu de l'égalité $p^2 + (2q)^2 = 5^n$, l'autre le serait aussi. Dans ces conditions, ce serait le cas de P et Q car le couple $(\mathrm{P}\ ;\mathrm{Q})$ étant l'image par l'un des φ_i de $(p\ ;q)$, ces nombres sont des combinaisons linéaires à coefficients entiers de p et q. Mais cette conclusion est contraire à l'hypothèse de récurrence, donc le dernier critère est bien vérifié. $(p\ ;q)$ est donc la solution d'ordre n du problème (IV) soit $(p\ ;q) = (p_n\ ;q_n)$.

Il existe donc un unique i pour lequel $\varphi_i^{-1}(\mathrm{P}\ ;\mathrm{Q}) = (p_n\ ;q_n)$, c'est-à-dire pour lequel $(\mathrm{P}\ ;\mathrm{Q}) = \varphi_i(p_n\ ;q_n)$, autrement dit : $(\mathrm{P}\ ;\mathrm{Q}) = \Phi(p_n\ ;q_n) = (p_{n+1}\ ;q_{n+1})$, et la solution d'ordre $n + 1$ au problème (IV) est unique. Le problème (IV) a donc, quel que soit n une solution unique d'ordre n, ainsi donc que les problèmes (III), (II) et (I), et les valeurs correspondantes pour cos x sont exactement au nombre de deux. Le tableau récapitulatif suivant pourra être continué aussi loin que nous le voulons, en rappelant les notations :

$$\{a;b\}=\left\{\left|p^2-(2q)^2\right|;4pq\right\};\{\alpha_n;\beta_n\}=\left\{\frac{a_n}{5^n}:\frac{b_n}{5^n}\right\};$$
$$p_{2n}=\text{ l'impair de }\{a_n;b_n\};q_{2n}=\text{ la moitié du pair de }\{a_n;b_n\};$$
$$\text{si } p_n-q_n\notin 5\mathbb{N},\text{ alors }(p_{n+1};q_{n+1})=(p_n+4q_n;|p_n-q_n|)$$
$$\text{et si } p_n-q_n\in 5\mathbb{N},\text{ alors }(p_{n+1};q_{n+1})=(|p_n-4q_n|;p_n+q_n).$$

n	$\{p;q\}, p^2+4q^2=5^n$	$\{a;b\}, a^2+b^2=5^{2n}$	$\{\alpha;\beta\}, \alpha^2+\beta^2=1$	$\cos x$
0	$\{1;0\}$	$\{1;0\}$	$\{1;0\}$	$0;1$
1	$\{1;1\}$	$\{3;4\}$	$\{0,6;0,8\}$	$0,6;0,8$
2	$\{3;2\}$	$\{7;24\}$	$\{0,28;0,96\}$	$0,28;0,96$
3	$\{11;1\}$	$\{117;44\}$	$\{0,936;0,352\}$	$0,936;0,352$
4	$\{7;12\}$	$\{527;336\}$	$\{0,843\,2;0,537\,6\}$	$0,843\,2;0,537\,6$
5	$\{41;19\}$	$\{237;3\,116\}$	$\cdots$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
10	$\{237;1\,558\}$	$\cdots$	$\cdots$	$\cdots$
11	$\{6\,469;1\,321\}$	$\cdots$	$\cdots$	$\cdots$

Complément par Richard Choulet(*)

J'utilise les entiers de Gauss (les nombres $a + bi$, a et b dans $\mathbb{Z}$) dont parle l'article de Jacques Faisant qui paraît dans ce BV 494.
Un des problèmes rencontrés était de résoudre $a^2 + b^2 = 5^{2n}$ avec a et b étrangers.
Avec $5 = (2 + i)(2 - i)$ et $(2 + i)^2 = 3 + 4i$, ceci s'écrit :

$$(a + bi)(a - bi) = (3 + 4i)^n(3 - 4i)^n.$$

On démontre que si a et b sont étrangers dans $\mathbb{Z}$, ils le sont dans $\mathbb{Z}[i]$. Par ailleurs a et b sont étrangers dans $\mathbb{Z}$ si et seulement si $a + bi$ et $a - bi$ le sont dans $\mathbb{Z}[i]$.
Sachant que les inversibles de $\mathbb{Z}[i]$ sont $1, -1$, i et $-i$, on doit avoir :
$a + bi = (3 + 4i)^n$ ou $-(3 + 4i)^n$ ou $i(3 + 4i)^n$ ou $-i(3 + 4i)^n$ ou $(3 - 4i)^n$ ou $-(3 - 4i)^n$ ou $i(3 - 4i)^n$ ou $-i(3 - 4i)^n$.
On observe donc qu'un couple solution étant connu, il y en a, pour n supposé non nul, sept autres obtenus par des symétries simples du plan complexe (axe des coordonnées et les deux bissectrices). Ceci a pour conséquence qu'il suffit de connaître un représentant de cette classe de huit éléments pour avoir la classe. L'idée est de suivre la filiation d'un représentant et on aura tout. Je pars de $(a_0 ; b_0) = (1 ; 0)$ qui correspond à $(3 + 4i)^0$. Le suivant est alors le couple $(a_1 ; b_1) = (3 ; 4)$, puis ensuite $(-7 ; 24)$, etc. Comment s'obtiennent donc facilement ces divers couples ? a_n et b_n s'obtiennent comme combinaison linéaire de $(3 + 4i)^n$ et de son conjugué. Ce qui a pour conséquence que les suites a et b vérifient la même relation de récurrence linéaire : $u_{n+2} = 6u_{n+1} - 25u_n$.
Moralité : en travaillant dans $\mathbb{Z}$, on a tout de suite les suites $(1 ; 3 ; -7 ; \ldots)$ et $(0 ; 4 ; 24 ; \ldots)$ qui fournissent après changement de signe et multiplication par 2^n les nombres tels que $1^2 + 0^2 = 1$; $0,6^2 + 0,8^2 = 1$; $0,28^2 + 0,96^2 = 1$; etc.

(*) richardchoulet@wanadoo.fr