

construction des premiers à partir des seconds). L'explication des contradictions obtenues tient en quelques mots :

– la formule $\sqrt{a} \times \sqrt{b} = \sqrt{a \cdot b}$ est vraie si a et b sont des nombres positifs, mais personne n'a jamais dit qu'elle était vraie pour tout nombre complexe a et b . L'erreur provient donc de l'utilisation d'une formule que personne ne démontre jamais.

Essayons d'approfondir un peu l'explication. Rappelons d'abord que :

– tout nombre réel positif possède deux racines carrées, de même que tout nombre complexe non nul.

– la notation $\sqrt{a}$, lorsque a est un nombre réel positif, désigne la racine carrée positive de a , l'autre racine étant $-\sqrt{a}$, et c'est seulement lorsque a est un nombre réel positif qu'on utilise la notation $\sqrt{a}$.

Lorsqu'on passe aux nombres complexes, la difficulté pour étendre la notation est qu'il n'est pas facile de choisir une fois pour toutes l'une des deux racines de a et de lui attribuer la notation $\sqrt{a}$. En fait, il n'existe aucune façon de choisir une convention qui permette de maintenir la formule $\sqrt{a} \times \sqrt{b} = \sqrt{ab}$. S'il existait une telle convention, on aurait justement : $-1 = \sqrt{-1} \times \sqrt{-1} = \sqrt{(-1) \times (-1)} = \sqrt{1} = 1$, ce qui est absurde.

Notre petit jeu a au moins une utilité : correctement interprété, il établit qu'il est impossible de définir $\sqrt{a}$ pour tout nombre complexe de manière à préserver la formule $\sqrt{a} \times \sqrt{b} = \sqrt{ab}$, ce qui n'est pas un résultat si évident que cela. La démonstration absurde une fois

remise sur ses pieds fournit une démonstration intéressante. Comme il est difficile de se discipliner pour ne pas utiliser $\sqrt{a} \times \sqrt{b} = \sqrt{ab}$ pour les nombres négatifs et les nombres complexes, il est préférable d'éviter totalement l'utilisation de la notation $\sqrt{a}$ en dehors des nombres réels positifs.

LE MONDE MATHÉMATIQUE EST IMMOBILE

Le principe de récurrence, l'un des outils les plus puissants du raisonnement arithmétique, consiste, pour établir une propriété générale du type «pour tout n , $P(n)$ », à montrer que :

(i) $P(0)$ est vrai

(ii) si $P(n)$ est vrai, pour $n = 0, 1, \dots, k$, alors $P(k+1)$.

Une variante consiste à remplacer (ii) par :

(ii') si $P(n)$ est vrai pour $n = k$, alors $P(k+1)$.

Malheureusement, l'intuition est un peu perdue dans la récurrence, aussi de nombreuses erreurs sont-elles possibles. Voici quelques exemples de faux raisonnements par récurrence, dont le premier est dû à Alex Kuperman.

Nous allons démontrer qu'en mathématiques rien ne bouge ; plus précisément, nous établirons que toutes les fonctions x^n sont des fonctions constantes.

(i) C'est vrai pour $n = 0$, car $x^0 = 1$.

(ii) Supposons que c'est vrai pour $n = 0, 1, \dots, k$, c'est-à-dire que la dérivée de x^n est nulle : $(x^n)' = 0$ pour $n = 0, 1, \dots, k$. Utilisons maintenant la formule de déri-

vation d'un produit $(uv)' = u'v + uv'$. On a : $(x^{k+1})' = (x \cdot x^k)' = x' \cdot x^k + x \cdot (x^k)'$.

On obtient 0, car $x' = (x^1)' = (x^k)' = 0$ d'après l'hypothèse de récurrence. Nous avons donc $(x^{k+1})' = 0$, ce que nous souhaitons.

Qu'est-ce qui cloche ?

Solution : Lorsque $k = 0$ on a l'hypothèse que $(x^0)' = 0$ et non pas, comme le raisonnement l'utilise, que $(x^0)' = (x^1)' = 0$. Le passage de k à $k+1$ ne marche donc pas pour aller de 0 à 1. La confusion provient de la notation $n = 0, 1, 2, \dots, k$, qui laisse croire qu'à chaque étape on a au moins $P(0)$ et $P(1)$ vrais, alors qu'en fait lorsque $k = 0$, on a seulement $P(0)$.

EN MATHÉMATIQUES, TOUT S'ANNULE

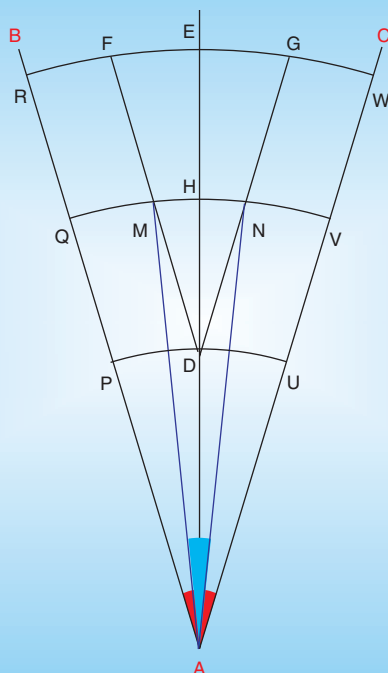
Voici un autre raisonnement faux (mais intéressant!) dû à Richard Johnsonbaugh. Nous allons établir que tous les entiers sont nuls. Démontrons d'abord par récurrence, que si deux entiers positifs ou nuls, a et b , ont un maximum inférieur ou égal à n , alors ils sont égaux. C'est vrai pour les deux entiers a et b si leur maximum est inférieur ou égal à 0, car alors nécessairement $a = 0$ et $b = 0$. Supposons que la propriété soit vraie pour tout couple d'entiers a et b dont le maximum est inférieur ou égal à k et montrons que c'est vrai pour $k+1$. Soit a et b deux entiers positifs ou nuls dont le maximum est inférieur ou égal à $k+1$. Le maximum de $a-1$ et $b-1$ est inférieur ou égal à k , donc l'hypothèse de récurrence s'applique, donnant $a-1 =$

4. LA TRISECTION DE L'ANGLE

En 1837, Pierre-Laurent Wantzel, répétiteur à l'École polytechnique publiait un mémoire où il démontrait que la trisection de l'angle était impossible en général. Il réglait en même temps le problème de la duplication du cube (tracer à la règle et au compas un segment de longueur $\sqrt[3]{2}$ [racine cubique de 2]), mais laissait non résolu le problème de la quadrature du cercle (construire à la règle et au compas un segment de longueur $\sqrt{\pi}$), construction dont on ne démontra l'impossibilité que 45 années plus tard.

Le problème de la trisection de l'angle, vieux de plus de deux mille ans, consiste à se donner un angle quelconque et à dessiner un angle trois fois plus petit, en n'utilisant que des constructions faites avec une règle et un compas. Une solution de Tom Cunniffham semble contredire le résultat de Wantzel.

Soit l'angle BAC à triséquer. En prenant pour centre A, on construit des arcs



de cercle de rayons 2, 3 et 4 unités qui donnent les points P, U, Q, V, R, W. Traçons D, E, F et G, les milieux des arcs PU, RW, RE et EW (c'est faisable à la règle et au compas). Soit M et N les intersections respectives des segments FD et GD avec l'arc QV. L'angle MAN triseque l'angle BAC.

En effet, puisque par construction $\text{arc}(RW) = 2 \text{ arc}(PU)$, on déduit que $\text{arc}(PD) = \text{arc}(RF)$, et donc que FD est parallèle à RP, d'où il suit que $\text{arc}(QM) = \text{arc}(RF)$. De même $\text{arc}(NV) = \text{arc}(GW) = \text{arc}(RF)$. Puisque par construction $3 \text{ arc}(RW) = 4 \text{ arc}(QV)$ et que $4 \text{ arc}(RF) = \text{arc}(RW)$, on a $\text{arc}(QV) = 3 \text{ arc}(RF)$. QV est triséqué par M et N. Wantzel s'est-il trompé ?

Solution. Non. La longueur des deux arcs $\text{arc}(PD)$ et $\text{arc}(RF)$ est bien la même, mais cela ne signifie pas que FD est parallèle à RP, car les cercles supports n'ont pas le même rayon.

$b - 1$, d'où l'on déduit que $a = b$, ce que nous souhaitons.

Maintenant, soit un entier positif ou nul quelconque b . Soit n le maximum de 0 et b (bien sûr $n = b$). Le raisonnement précédent a montré que 0 et b étaient égaux, donc $b = 0$. En conclusion, tous les entiers positifs ou nuls sont nuls.

Si tel était le cas, là aussi les entiers seraient majorés par 0! Où est l'erreur? **Solution :** Simplement dans le fait que, même si a et b sont des entiers positifs ou nuls, $a - 1$ et $b - 1$ ne le sont pas nécessairement (car $0 - 1 = -1$). On ne peut donc pas appliquer l'hypothèse de récurrence au couple $a - 1, b - 1$.

DÉSOLANTES DÉRIVÉES

Calculons la dérivée de x^3 de deux façons différentes :

(a) Par la formule habituelle $(x^n)' = nx^{n-1}$. Pour tout x , on a donc $(x^3)' = 3x^2$

(b) Par le raisonnement suivant. Pour x entier, on écrit :

$x^3 = x^2 + x^2 + x^2 + \dots + x^2$ (la somme comporte x fois le terme x^2)

On dérive de chaque côté :

$(x^3)' = (x^2)' + (x^2)' + (x^2)' + \dots + (x^2)'$ (la dérivée d'une somme est la somme des dérivées).

$(x^3)' = 2x + 2x + 2x + \dots + 2x$ (application de la formule générale rappelée plus haut).

$(x^3)' = 2x^2$ (car, sur la ligne précédente il y a x fois le terme $2x$, ce qui permet de remplacer le second membre par $2x^2$).

Pour tout x entier, on a donc :

$(x^3)' = 3x^2 = 2x^2$.

En prenant pour x un entier non nul et en simplifiant par x^2 , on a : $2 = 3$.

Où est l'erreur?

Solution : Le raisonnement (b) suppose que x est entier (sinon, on ne pourrait pas écrire : $x^3 = x^2 + x^2 + x^2 + \dots + x^2$). Appelons n l'entier auquel on s'intéresse.

Les fonctions $x \rightarrow x^3$ et $x \rightarrow x^2 + x^2 + x^2 + \dots + x^2$ (n fois le terme x^2) ont effectivement la même valeur au point $x = n$, et cette valeur est n^3 . Mais, autour de la valeur n , ces deux fonctions n'ont plus les mêmes valeurs, car : $(n+\epsilon)^3 \neq (n+\epsilon)^2 + (n+\epsilon)^2 + \dots + (n+\epsilon)^2 = n(n+\epsilon)^2$. Puisque les deux fonctions sont différentes, il est sans surprise que leur dérivée le soit.

L'endroit où se produit l'erreur est lorsqu'on écrit «on dérive de chaque côté» car, l'égalité $x^3 = x^2 + x^2 + x^2 + \dots + x^2$ désigne une égalité valable entre deux fonctions différentes en un point précis, et non pas une égalité entre deux fonctions sur tout leur ensemble de définition. L'erreur est en fait la même que celle qu'on commettrait en disant :

$\sin 45^\circ = \cos 45^\circ = \sqrt{2}/2$, et donc que $(\sin 45^\circ)' = (\cos 45^\circ)'$, ce qui est absurde car en utilisant que $\sin x' = \cos x$ et que $\cos x' = -\sin x$, on en déduirait que $\cos 45^\circ = -\sin 45^\circ$, soit $\sqrt{2}/2 = -\sqrt{2}/2$.

5. LA PLUS BELLE PROPRIÉTÉ DE π

L'importance mathématique du nombre π n'est plus à démontrer. Pourtant la propriété suivante de π ne manquera pas de vous étonner : toute série converge vers π .

En effet, soit une série quelconque (par prudence, vous pouvez considérer une série absolument convergente) :

$a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + \dots$

Les égalités (finies) suivantes sont immédiates :

$a_1 = \pi + (a_1 - \pi)$

$a_2 = -(a_1 - \pi) + (a_1 + a_2 - \pi)$

$a_3 = -(a_1 + a_2 - \pi) + (a_1 + a_2 + a_3 - \pi)$

$a_4 = -(a_1 + a_2 + a_3 - \pi) + (a_1 + a_2 + a_3 + a_4 - \pi)$. Etc.

En ajoutant toutes ces égalités, nous obtenons :

$a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + \dots = \pi + (a_1 - \pi) - (a_1 - \pi) + (a_1 + a_2 - \pi) - (a_1 + a_2 - \pi) + (a_1 + a_2 + a_3 - \pi) - (a_1 + a_2 + a_3 - \pi) + (a_1 + a_2 + a_3 + a_4 - \pi) - \dots$

Toutes les parenthèses se simplifient deux à deux et disparaissent. Donc :

$a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + \dots = \pi$.

Pensez-vous vraiment que cela soit normal?

Solution

Non, bien sûr, et d'ailleurs le même raisonnement, s'il était juste, s'appliquerait à n'importe quelle constante. Le raisonnement est faux, car l'expression obtenue au second membre après l'addition infinie est une série qui n'est pas même convergente (ni les parenthèses, ni leurs composants ne tendent vers zéro en général). Or avec une série de nombres réels qui n'est pas convergente, toute manipulation, même les simplifications les plus simples, est dangereuse et susceptible de nous entraîner dans l'absurde. Si vous en doutez, considérez l'exemple classique suivant :

$1 - 1 + 1 - 1 + 1 - 1 + 1 - 1 + \dots = (1 - 1) + (1 - 1) + (1 - 1) + (1 - 1) + (1 - 1) + \dots = 0$
 $1 - 1 + 1 - 1 + 1 - 1 + 1 - 1 + \dots = 1 + (-1 + 1) + (-1 + 1) + (-1 + 1) + \dots = 1$

SOMMES INFINIES

En analyse, on démontre que la série : $\ln(2) = 1 - 1/2 + 1/3 - 1/4 + 1/5 - 1/6 + \dots$ est une série convergente, c'est-à-dire qu'en prenant 1, puis 2, puis 3, ... termes de la série, on obtient des nombres qui s'approchent de plus en plus d'une constante, qui est ici le logarithme népérien de 2 : $\ln 2 = 0,6931\dots$

Groupons les termes positifs d'une part et les termes négatifs de l'autre :

$\ln 2 = (1 + 1/3 + 1/5 + \dots) - (1/2 + 1/4 + 1/6 + \dots)$.

Par ailleurs nous avons certainement :

$0 = (1/2 + 1/4 + 1/6 + \dots) - (1/2 + 1/4 + 1/6 + \dots)$.

ce qui, en ajoutant membre à membre avec l'égalité au-dessus, donne :

$\ln 2 = (1 + 1/2 + 1/3 + 1/4 + 1/5 + 1/6 + \dots) - 2(1/2 + 1/4 + 1/6 + \dots)$,

c'est-à-dire :

$\ln 2 = (1 + 1/2 + 1/3 + 1/4 + 1/5 + 1/6 + \dots) - (1 + 1/2 + 1/3 + 1/4 + 1/5 + 1/6 + \dots) = 0$,

Donc, $\ln 2 = 0$.

D'où vient cette absurdité?

Solution : L'absurdité provient du fait général qu'on ne peut manipuler les séries sans précaution et qu'en particulier on ne peut changer l'ordre des termes sans risque. Il existe deux sortes de séries convergentes :
 - celles (dénommées «absolument convergentes») dont la série des valeurs absolues est convergente,
 - celles (dénommées «semi-convergentes») dont la série des valeurs absolues est infinie. C'est le cas de :

$\ln(2) = 1 - 1/2 + 1/3 - 1/4 + 1/5 - 1/6 + \dots$

Pour les premières, on peut changer l'ordre des termes, additionner termes à termes, etc, comme nous l'avons fait ici. Pour les autres, Riemann a démontré au contraire que changer l'ordre des termes pouvait conduire à n'importe quelle valeur entre $-\infty$ et $+\infty$, et en fait toutes sortes d'absurdités peuvent être déduites de la manipulation sans précaution de séries semi-convergentes. L'exemple proposé est l'un des plus brefs qui le montre.

ARISTOTE, Organon VI, Réfutation des arguments sophistiques. Traduction J. Tricot. Librairie philosophique J. Vrin, Paris, 1987.

Edward BARREAU, Mathematical Fallacies, Flaws, and Flimflam, édité par The Mathematical Association of America, 2000, (ISBN 0-88385-529-1).

E.P. NORTHROP, Fantaisies et paradoxes mathématiques, Dunod, Paris, 1956, (tra-

duction de : **Riddles in Mathematics**, D. Van Nostrand Company Inc., New York, 1944).

Sylviane GASQUET-MORE, Plus vite que son nombre. Déchiffrer l'information. Éditions du Seuil, Paris 1999.

Massimo PIATELLI-PALMARINI, Inevitable Illusions : How Mistake of Reason Rule our Minds, John Wiley and Sons, New York, 1994 (ISBN 0-471-58126-7).



Un démineur millionnaire

IAN STEWART

Ou comment un jeu informatique peut faire de vous un homme riche.

En manque d'argent? L'Institut mathématique Clay, une fondation éducative à but non lucratif de Cambridge, dans le Massachusetts, offre des prix de un million de dollars pour la résolution de sept problèmes. L'un d'eux est le célèbre problème de l'égalité de la classe P et de la classe NP , dont nous éclaircirons plus loin l'énoncé hermétique. Bien qu'il s'agisse d'une question très difficile, un amateur astucieux peut y répondre grâce au démineur, un jeu populaire accessible à la plupart des ordinateurs personnels.

Richard Kaye, de l'Université de Birmingham, a récemment mis en évidence les relations entre ce jeu et la question « $P = NP?$ » dans un article intitulé «le démineur est-il NP -complet?». Rappelons d'abord les règles du démineur. L'ordinateur commence la partie en présentant une grille de carrés dont certains dissimulent des mines explosives. Il s'agit de les localiser sans en faire exploser une seule. Au premier coup, vous

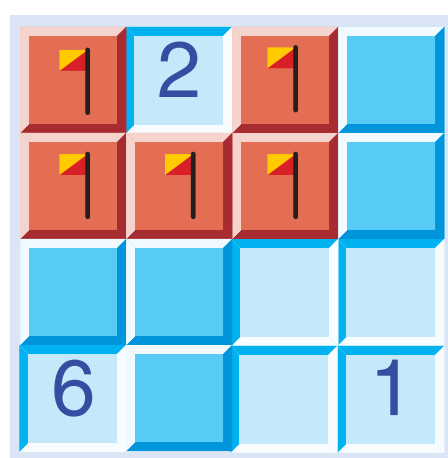
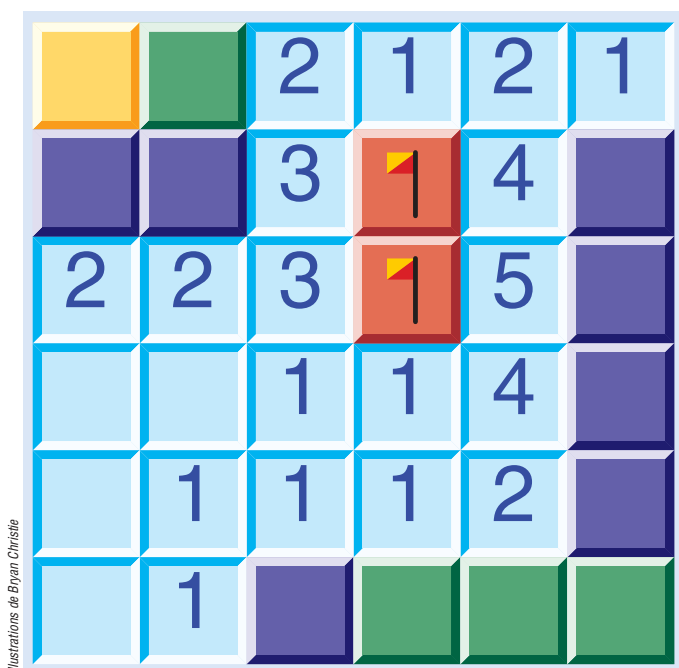
découvrez l'un des carrés : s'il cachait une mine, vous n'avez pas de chance et vous perdez, sinon l'ordinateur affiche dans le carré que vous avez choisi le nombre de mines dans les trois, cinq ou huit carrés adjacents.

Vous utilisez alors cette information pour choisir un autre carré, et de nouveau une mine explose ou un nombre est affiché. Lorsque vous pouvez déduire de ces informations la présence d'une mine dans un carré, vous marquez ce dernier d'un petit drapeau (voir la figure 1). Vous gagnez quand toutes les mines de la grille sont localisées.

Revenons à la question « $P = NP?$ ». Un algorithme est une procédure pas à pas qu'utilise un ordinateur pour résoudre un problème. Pour les informaticiens, il est crucial de savoir avec quelle efficacité un algorithme résout un problème donné, ou, en d'autres termes, comment le temps de traitement, c'est-à-dire le nombre de calculs exigés pour la réponse, varie suivant la taille des don-

nées initiales. On distingue principalement les problèmes de classe P (P comme polynôme) et les autres. Un problème est de classe P quand on peut le résoudre avec un algorithme dont le temps de traitement est majoré par un polynôme de la taille des données, c'est-à-dire par une somme de différentes puissances de la taille des données. Lorsqu'une telle solution n'existe pas, le problème est de classe non- P .

À l'inverse des problèmes de classe P , les problèmes de classe non- P ne sont pas efficacement traités par les ordinateurs : tout algorithme mis au point pour les résoudre requiert un temps trop long. On peut prouver qu'un problème est de classe P en trouvant un algorithme qui le résolve en un temps polynomial, par exemple, ordonner par ordre croissant un ensemble d'entiers est un problème de classe P que des programmes peuvent traiter sur des banques de données commerciales, même très importantes. En revanche, trouver les facteurs premiers



1. Une position typique du démineur (à gauche). Après les premiers coups, le joueur a localisé deux mines (sous les drapeaux). L'examen des chiffres montre que les carrés violets dissimulent d'autres mines tandis que les verts sont sans danger. L'état du carré jaune est encore inconnu, mais peut être déterminé après un coup judicieux. En revanche, la position à droite n'est pas consistante : aucune disposition de mines dans la grille ne peut respecter les chiffres indiqués.