

Croissance polynomiale ou exponentielle

La croissance d'une fonction $f(x)$ quand x tend vers l'infini peut être similaire (entre autres) à celle d'un polynôme x^n ou à celle d'une exponentielle a^x (a fixé). Peu importe le comportement de $f(x)$ dans un intervalle fini, la croissance exponentielle devient tôt ou tard plus rapide que la croissance polynomiale.

Cette distinction est essentielle pour les calculs numériques. Un problème où le temps de calcul nécessaire croît de façon polynomiale en fonction de la variable étudiée (ou problème P) est considéré comme « facile » : il peut être résolu en un temps raisonnable. Si, en revanche, le nombre d'opérations

croît exponentiellement avec la variable considérée (problème NP, pour *non polynomial*), le problème est considéré comme difficile et dépasse vite les capacités de calcul existantes. Une des sept « questions du millénaire » est de savoir si les problèmes NP peuvent se ramener à des problèmes P.

d'équation n'a aucune solution parmi les entiers naturels non nuls (par exemple, $x^3 + y^3 = z^3$ n'a pas de solutions, d'après le théorème de Fermat), parfois elles en ont une infinité.

Si les nombres x, y, z sont à peu près du même ordre de grandeur et sont très supérieurs aux coefficients a, b et c , alors on obtient, par une estimation analogue à la précédente, que $\kappa(A, B, C) \approx \delta(x)$ et que cette valeur est probablement inférieure à 1,06. Si, en revanche, x est beaucoup plus petit (de plusieurs ordres de grandeur) que y et z , on obtient $\kappa(A, B, C) \approx 3/2 \delta(x)$.

Le triplet $(51^3, 5 \cdot 49^3, 22 \cdot 32^3)$ donne par exemple $\kappa(A, B, C) = 1,27509\dots$, le triplet $(1, 17 \cdot 7^3, 18^3)$ donne $\kappa = 1,31962\dots$, et le triplet $(1, 5 \cdot 2^4, 3 \cdot 3^3)$ donne $\kappa = 1,29\dots$

Le dernier exemple est particulièrement intéressant, car $81 = 3^4 = 5 \cdot 2^4 + 1$ est une solution de l'équation $x^4 = 5y^4 + z^k$, où k est un entier aussi grand que l'on veut. Plus les exposants dans l'équation sont élevés (2 et 3 dans les exemples précédents), plus la valeur de $\kappa(A, B, C)$ que l'on peut obtenir est grande – si tant est que l'équation en question admette encore des solutions. Or il n'y en a pas beaucoup. Gerd Faltings, lauréat de la médaille Fields en 1986 pour sa démonstration de la conjecture de Mordell, a montré par celle-ci que l'équation $x^4 = 5y^4 + z^k$ n'a, pour chaque exposant $k \geq 4$, qu'un nombre fini de solutions dont les termes sont premiers entre eux. On pense même que l'ensemble des solutions pour tous k confondus est fini, c'est-à-dire que l'ensemble des triplets (x, y, z) premiers entre eux et pour lesquels il existe un entier $k \geq 4$ tel que $x^4 = 5y^4 + z^k$ est fini.

Résumons. Nos expériences numériques suggèrent qu'en moyenne, la puissance moyenne $\kappa(A, B, C)$ d'un triplet est d'environ 0,5 ; dans tous les cas étudiés, κ est inférieur à 2 ; pour de nombreux exemples,

κ est supérieur à 1, et ces valeurs élevées sont intimement liées à des solutions d'équations polynomiales à trois variables.

La version forte de la conjecture ABC

Tous ces résultats expérimentaux permettent enfin de proposer – avec toute la prudence requise vis-à-vis de résultats empiriques – la conjecture suivante : la puissance moyenne $\kappa(A, B, C)$ des triplets (A, B, C) , où A, B et C sont premiers entre eux et tels que $A + B = C$, est bornée, c'est-à-dire qu'il existe un nombre positif α tel que $\kappa(A, B, C) \leq \alpha$.

On peut exprimer la même chose sans faire référence aux quantités C et κ , qui dépendent de A et de B . Un peu de travail donne :

$$A + B \leq [\text{Rad}(A \cdot B \cdot (A + B))]^\alpha$$

Plutôt que d'affirmer l'existence d'une telle borne α , on aurait préféré qu'elle soit calculable. Des algorithmes qui peuvent en principe déterminer cette valeur ont

TAILLER LE COSTUME IDÉAL
pour les entiers signifie couvrir tous les cas, mais avec une approximation aussi proche du corps que possible.

été mis au point ; mais en pratique, le temps de calcul prendrait des siècles, voire plus. On cherche toujours un algorithme effectif, c'est-à-dire qui pourrait livrer un résultat en un temps raisonnable, par exemple une semaine de calcul sur un ordinateur personnel.

Même si l'on parvenait à démontrer la conjecture pour une très grande valeur de α , cela ne servirait pas à grand-chose : une approximation trop grossière ne dit plus grand-chose sur le comportement des triplets. La borne α doit être aussi petite que possible. D'après nos résul-

tats empiriques, on serait tenté de choisir $\alpha = 1,4$. Malheureusement, dans certains cas, $\kappa(A, B, C)$ est supérieur à 1,4. Par ailleurs, dans la plupart des cas, $\kappa(A, B, C)$ est beaucoup plus petit. Cette borne est à la fois trop grande et trop petite.

Pour contourner ce problème, on introduit une deuxième constante. À la place de l'équation précédente, on pose :

$$A + B \leq d [\text{Rad}(A \cdot B \cdot (A + B))]^\alpha$$

où d est une constante qui devrait être effective. En exprimant cette inégalité en fonction de κ , on obtient l'inégalité suivante :

$$\kappa(A, B, C) \leq \alpha + \frac{\log d}{\log(\text{Rad}(A \cdot B \cdot C))}$$

À première vue, la conjecture initiale est si déformée qu'elle semble vidée de sa substance. Si un contre-exemple ne vérifie pas l'inégalité, on n'a qu'à choisir une valeur de d plus grande pour que l'inégalité soit satisfaite. Supposons que l'on ait cherché un contre-exemple parmi tous les nombres inférieurs à un milliard ; il suffit de prendre d supérieur au plus grand des nombres C testés, soit un milliard, pour que la conjecture soit vérifiée pour tout α , ce qui n'a aucun intérêt.

Mais cette première impression est trompeuse. On a montré que plus A, B et C sont grands, plus $\log(\text{Rad}(A \cdot B \cdot C))$ devient grand, bien que plus lentement. Ainsi, le degré de liberté que nous offre la constante d devient négligeable lorsque les nombres considérés deviennent grands. Pour les nombres « très grands », seule la borne α compte.

Cependant, cette formulation contient encore trop de choix. Pour faire rentrer un contre-exemple dans le rang, on a le choix d'augmenter α ou d . Le but est pourtant de tailler, par un choix approprié de α et d , un « costume idéal » pour tous les entiers naturels : il devrait tout couvrir (aucun contre-exemple) et en même temps être aussi proche du corps que possible (l'approximation ne doit pas être trop large). Cela signifie que pour au moins quelques triplets, l'inégalité ci-dessus devrait être une égalité. En prenant α et d légèrement plus petits que ces valeurs bien ajustées, on pourrait trouver un contre-exemple. Diminuer α demanderait d'agrandir d et inversement.

La conjecture ABC dans la version énoncée par J. Oesterlé et D. Masser est encore plus forte que notre dernière version. Elle dit qu'il suffit de prendre α supérieur à 1, mais aussi proche de 1

que l'on veut. Tous les cas particuliers peuvent alors être englobés en choisissant une valeur appropriée de d . Il faut juste accepter que d devienne arbitrairement grand si α s'approche de 1. En termes précis, la conjecture ABC s'énonce ainsi :

Pour tout nombre réel $\varepsilon > 0$, il existe un nombre réel $d_\varepsilon > 0$ tel que, pour tous entiers naturels A , B et C premiers entre eux et tels que $A + B = C$, on ait :

$$C \leq d_\varepsilon [\text{Rad}(A \cdot B \cdot C)]^{1+\varepsilon}$$

Autrement dit, en prenant le logarithme :

$$\kappa(A, B, C) \leq 1 + \varepsilon + \frac{\log(d_\varepsilon)}{\log(\text{Rad}(A \cdot B \cdot C))}$$

où le terme d'erreur $\log(d_\varepsilon)$ dépend de ε .

Pourquoi ne pas choisir α égal à 1, voire moins ? Parce que l'on connaît certains contre-exemples (notamment de la forme $(A, B, C) = (1, 2^{p(p-1)} - 1, 2^{p(p-1)})$, où p est un nombre impair tel que $2^{p(p-1)} - 1$ est divisible par p^2). Par ailleurs, peut-on trouver un ε pour lequel on peut prendre $d_\varepsilon = 1$, ce qui correspond à notre première version de la conjecture ? Bien sûr, on cherche $\alpha = 1 + \varepsilon$ qui soit le plus petit possible.

La plus grande valeur connue pour $\kappa(A, B, C)$ est 1,629 911 7. Elle correspond au triplet $(2, 3^{10} \cdot 109, 23^5)$, solution de l'équation $x^5 - 109y^{10} = 2$, trouvée par Éric Reyssat, aujourd'hui à l'Université de Caen. Ayant testé tous les nombres jusqu'à 10^{20} , nous savons qu'au moins dans cet intervalle immense, il n'existe pas de contre-exemple (pour $d_\varepsilon = 1$) à la conjecture ABC avec $\alpha = 2$ (qui correspond à $\varepsilon = 1$), c'est-à-dire $\kappa(A, B, C) \leq 2$.

À la recherche des bons triplets

Depuis que la conjecture ABC a été énoncée, elle a suscité une recherche intense de triplets nécessitant de grandes constantes α et d , c'est-à-dire pour lesquels $\kappa(A, B, C)$ est grand. Ces exemples resserrent l'intervalle pour le choix de ε et d_ε , mais il y a aussi une part de compétition dans cette recherche des triplets les plus riches. C'est à qui mettra au point l'algorithme le plus rapide et le plus performant. On peut en outre espérer découvrir des équations intéressantes.

On dit que (A, B, C) est un « bon triplet » si $\kappa(A, B, C) > 1,4$. Ces triplets sont extrêmement rares. Dans la tranche des entiers allant jusqu'à 10^{20} , presque entièrement explorée, il n'y en a qu'environ 200.

Sur le modèle des projets participatifs de recherche de signaux extraterrestres

ou d'étude du repliement des protéines, le projet ABC@home invite tous les internautes à participer à la recherche d'autres bons triplets en donnant un peu de temps de calcul de leur ordinateur, ou même en développant leur propre algorithme.

Outre son intérêt intrinsèque, la démonstration de la conjecture ABC entraînerait celle de nombreux problèmes de la théorie des nombres. C'est le cas notamment du redoutable théorème de Fermat, dont la conjecture ABC apporte une preuve – du moins pour n assez grand – d'une simplicité dérisoire.

Dans l'équation $x^n + y^n = z^n$, posons $A = x^n$, $B = y^n$, $C = z^n$. On donne d'abord une borne supérieure grossière pour $\text{Rad}(ABC)$:

$$\begin{aligned} \text{Rad}(ABC) &= \text{Rad}(x^n y^n z^n) \\ &= \text{Rad}(xyz) \leq xyz < z^3. \end{aligned}$$

Cela donne une borne inférieure pour $\kappa(A, B, C)$: $\kappa(A, B, C) = \log(C) / \log(\text{Rad}(ABC)) \geq \log(z^n) / \log(z^3) = n/3$.

Cette dernière quantité tend vers l'infini pour des exposants n élevés. Si par exemple $\kappa(A, B, C)$ était borné par 2, on aurait ainsi démontré que l'équation de Fermat n'a pas de solutions pour $n \geq 6$. Le théorème de Fermat étant prouvé depuis longtemps pour des petits exposants, cela suffirait pour boucler sa démonstration.

La validité de la conjecture ABC apporterait des démonstrations faciles et élégantes à d'autres poids lourds de la théorie des

L'AUTEUR



Gerhard FREY est professeur à l'Institut de mathématiques expérimentales de l'Université

Duisburg-Essen, en Allemagne.

Le logarithme

Le logarithme (décimal) d'un nombre strictement positif X est le nombre $\log X$ tel que $X = 10^{\log X}$. La fonction logarithme transforme un produit en somme : $\log(ab) = \log(a) + \log(b)$, et $\log(a^n) = n \log(a)$. Par ailleurs, $\log 1 = 0$.

On peut choisir une autre base que la base 10. Pour la base $e = 2,718...$, le logarithme est dit népérien et est noté $\ln$.

	$\kappa > 1$	$\kappa > 1,05$	$\kappa > 1,1$	$\kappa > 1,2$	$\kappa > 1,3$	$\kappa > 1,4$
$C < 10^2$	6	4	4	2	0	0
$C < 10^3$	31	17	14	8	3	1
$C < 10^4$	120	74	50	22	8	3
$C < 10^5$	418	240	152	51	13	6
$C < 10^6$	1 268	667	379	102	29	11
$C < 10^7$	3 499	669	856	210	60	17
$C < 10^8$	8 987	3 869	1 801	384	98	25
$C < 10^9$	22 316	8 742	3 693	706	144	34
$C < 10^{10}$	51 677	18 233	7 035	1 159	218	51
$C < 10^{11}$	116 978	37 612	13 266	1 947	327	64
$C < 10^{12}$	252 856	73 714	23 773	3 028	455	74
$C < 10^{13}$	528 275	139 762	41 438	4 519	599	84
$C < 10^{14}$	1 075 319	258 168	70 047	6 665	769	98
$C < 10^{15}$	2 131 671	463 446	115 041	9 497	998	112
$C < 10^{16}$	4 119 410	812 499	184 727	13 118	1 232	126
$C < 10^{17}$	7 801 334	1 396 909	290 965	17 890	1 530	143
$C < 10^{18}$	14 482 065	2 352 105	449 194	24 013	1 843	160

4. LA LISTE DES « BONS » TRIPLETS. Ce tableau présente le nombre de valeurs de C dans certains intervalles (lignes) pour lesquelles il existe A et B premiers entre eux, avec $A + B = C$, tels que la richesse $\kappa(A, B, C)$ soit supérieure à une borne donnée (colonnes).