Une Note Sur La Conjecture ABC

Abdelmajid Ben Hadj Salem
Résidence Bousten 8, Mosquée Raoudha,
1181 Soukra Raoudha,
Tunisia
E-mail: abenhadjsalem@gmail.com

Abstract: It is a paper of Gerhard Frey published in 2012. It is an introduction about the *abc* conjecture and its subtleties and consequences for the theory of numbers. It is a scientific version of the original paper.

Une Note Sur La Conjecture ABC

To the memory of Jean Bourgain (1954-2018) for his mathematical work notably in the field of Number Theory[1]

À première vue, la conjecture ABC semble être d'une trompeuse simplicité. Elle énonce une certaine propriété sur trois nombres entiers naturels A, B et C liés par la relation la plus simple possible : $A + B = C$. Ce qu'elle affirme exactement n'est pas évident. L'idée est que si les facteurs premiers de deux nombres A et B se répètent beaucoup, il y a peu de chance pour que ce soit aussi le cas pour leur somme.

La conjecture ABC a été énoncée en 1985 par Joseph Oesterlé, de l'Université Paris VI, et David Masser, de l'Université de Bâle, en Suisse. Malgré de solides indices en faveur de la validité de cette conjecture, aucune piste de démonstration ne semblait jusqu'ici très évidente, et la preuve paraissait encore éloignée. Cependant, cela pourrait avoir changé : un mathématicien reconnu de l'Université de Kyoto, Shinichi Mochizuki, affirme aujourd'hui avoir démontré la conjecture ABC. Ses pairs ont commencé à examiner sa démonstration, très longue et faisant appel à des outils nouveaux, mais il est trop tôt pour dire si son approche a été couronnée de succès.

La preuve de la conjecture ABC apporterait une solution à de nombreux problèmes importants de la théorie des nombres. En particulier, dans sa version forte, elle entraînerait la preuve du grand théorème de Fermat par une méthode différente de celle utilisée par Andrew Wiles et Richard Taylor en 1994.

La plupart des problèmes concernant les nombres entiers impliquent d'une façon ou d'une autre leurs facteurs premiers. Les nombres premiers sont les nombres qui ne sont divisibles que par eux-mêmes et par 1. La suite commence ainsi : $2, 3, 5, 7, 11, 13, 17\ldots$ À première vue, la répartition des nombres premiers semble aléatoire. Y chercher une structure occupe les mathématiciens depuis des siècles. Le « théorème des nombres premiers » fournit cependant une estimation : le nombre de nombres premiers inférieurs à n croît comme $\frac{n}{logn}$ lorsque n devient grand.

D'après le théorème fondamental de l'arithmétique, chaque entier naturel se décompose de façon unique en un produit de nombres premiers (à l'ordre des facteurs près). Par exemple, $6\,936 = 2^3.3.17^2$ n'est divisible par aucun autre nombre premier que 2, 3 et 17.

La conjecture ABC porte sur les facteurs premiers des nombres entiers, et plus précisément sur leur diversité et leur fréquence. Un entier pris au hasard a en général peu de facteurs premiers, bien que certains soient présents plusieurs fois. Tout multiple de 9 contient par exemple deux fois au moins le facteur premier 3 (car $9 = 3^2$). Mais il est rare

[1] The quote was not in the original paper.

que la majorité des facteurs premiers apparaissent de nombreuses fois dans la décomposition. Les puissances pures, comme $67\,108\,864 = 2^26$, sont peu fréquentes, de même que les nombres « puissants », où chaque facteur premier apparaît avec un exposant au moins égal à 2 (comme dans $614\,810\,677 = 13^3.23^4$). Si A et B sont deux nombres exceptionnels comportant des puissances élevées de leurs facteurs premiers, il faudrait que le diable s'en mêle pour que leur somme $A+B=C$ soit encore un entier exceptionnel. La conjecture ABC précise cet énoncé un peu flou.

Cette conjecture cache une particularité de la théorie des nombres. La structure additive des entiers naturels est particulièrement simple, et la structure multiplicative n'est guère plus compliquée. Mais les deux structures ne cohabitent pas bien : si on les combine, les choses se compliquent... et deviennent intéressantes. En d'autres termes, des propriétés de la somme $A+B$, du point de vue de la structure additive, dépendent de façon très régulière de celles de A et de B, mais du point de vue de la structure multiplicative, cette dépendance semble presque aléatoire. Le grand théorème de Fermat, selon lequel il n'existe pas d'entiers non nuls a,b et c vérifiant l'égalité $a^n+b^n=c^n$ pour $n>2$, mélange ainsi addition et multiplication (sous forme de puissances), pour un résultat d'une redoutable complexité.

1. Richesse et pauvreté chez les nombres entiers

Mais revenons à la notion de nombre exceptionnel. On dit qu'un entier est « riche » si certains de ses facteurs premiers sont présents plusieurs fois dans la décomposition (c'est-à-dire avec une puissance supérieure ou égale à deux). On l'« appauvrit » en supprimant les facteurs premiers redondants pour ne conserver qu'un seul exemplaire de chaque. Cette version dépouillée d'un entier n est appelée son radical, noté $Rad(n)$. Par exemple :

$$Rad(324) = Rad(2^2.3^4) = 2.3 = 6$$
$$Rad(424) = Rad(2^3.53) = 2.53 = 106$$
$$Rad(437) = Rad(23.19) = 23.19 = 437$$

Le radical d'un nombre est toujours inférieur ou égal à ce nombre. Les nombres premiers et ceux qui contiennent une seule fois chacun de leurs facteurs premiers sont « au seuil de pauvreté » : ils sont égaux à leur radical. À l'inverse, si chaque facteur premier de n est muni d'un exposant élevé, alors $Rad(n)$ est beaucoup plus petit que n.

Pour quantifier la richesse d'un nombre, on lui associe sa « puissance moyenne » $d(n)$, définie par l'égalité :

$$n = Rad(n)^{d(n)} \tag{1.1}$$

En passant au logarithme, on obtient une définition explicite :

$$d(n) = \frac{log(n)}{logRad(n)} \tag{1.2}$$

Pour les exemples précédents, on a :

$$d(324) = log(324)/log(6) = 3,22629...$$
$$d(424) = log(424)/log(106) = 1,29726...$$
$$\text{et évidemment } \; d(437) = log(437)/log(437) = 1$$

Un petit programme suffit à calculer rapidement la valeur moyenne d^* de d pour un ensemble de nombres. En tirant plusieurs fois au hasard 10 000 entiers entre un et un milliard, nous avons obtenu successivement les moyennes $d^* = 1,047519...$, puis $d^* = 1,05267...$, et $d^* = 1,04793...$ Un tirage de 100 000 nombres au hasard sans limite de taille a donné $d^* = 1,049266...$. Cela suggère qu'un nombre « moyen » ne vit que légèrement au-dessus du seuil de pauvreté. En règle générale, on s'attend à ce que la puissance moyenne ne dépasse pas 1,06.

Cette valeur moyenne suffit-elle à capturer la diversité des nombres entiers ? Évidemment, non. Il existe des cas isolés qui sont loin de toute valeur moyenne. Par exemple, dans l'intervalle allant de un à un milliard, on trouve le nombre richissime $67\,108\,864 = 2^{26}$, qui a une puissance moyenne $d = 26$. Et la richesse n'est pas bornée, puisqu'il existe des puissances de 2 avec un exposant aussi grand que l'on veut.

Cherchons le nombre le plus riche parmi 10 000 choisis au hasard dans l'intervalle précédent. Un premier essai donne $n = 692\,599\,663$, avec $d(n) = 3,831201...$. Sa décomposition en facteurs premiers est $n = 7^7.29^2$. Une deuxième tentative donne $n = 614\,810\,677 = 13^3.23^4$, avec $d(n) = 3,55004...$ Les nombres riches sont en général des nombres puissants. Par définition, la puissance moyenne des nombres puissants vaut au moins deux, donc la valeur maximale de d pour un grand échantillon de nombres ne peut pas être inférieure à 2. En général, elle est nettement supérieure, comme le montrent les exemples.

Nos expériences numériques montrent en outre que les nombres puissants sont plus fréquents que les puissances pures (du type 2^{26}), ce que confirment des arguments – difficiles – de la théorie des nombres. Plus fréquents encore sont les nombres « presque puissants », c'est-à-dire puissants à un facteur près, petit par rapport à ce nombre (par exemple, 5 000 000 est presque puissant, car 5 est petit devant 1 000 000, très puissant). Eux aussi ont une puissance moyenne d qui est bien au-dessus de la moyenne des entiers.

Résumons: les conclusions de ces expériences numériques. Le nombre moyen est pauvre : $d(n) < 1,06$. Les nombres riches, avec $d > 2$, sont rares, bien plus encore que les nombres premiers, mais ils sont plus fréquents que les puissances pures et leur richesse est en principe illimitée.

On ne peut pas dire grand-chose d'intéressant de plus sur la richesse d'un seul nombre. Il est peu probable que deux nombres choisis au hasard soient tous les deux riches. Mais, en reprenant l'idée évoquée précédemment de combiner les structures multiplicative et

additive, posons-nous la question suivante: la somme de deux nombres assez riches est-elle riche elle aussi ?

2. Mesurer la puissance moyenne d'un triplet

Choisissons deux entiers A et B avec la seule restriction qu'ils soient premiers entre eux (sans facteurs premiers en commun). En posant $C = A + B$, on s'attend en fait à ce qu'au moins un des nombres A, B ou C se comporte comme un nombre moyen.

Si A est un nombre moyen, on s'attend à ce que $A < Rad(A)^{1,06}$ ou, de façon équivalente, $logRad(A) > \dfrac{logA}{1.06}$. Si c'est vrai pour A, B et C, alors $logRad(ABC) = (logRad(A) + logRad(B) + logRad(C)) > \dfrac{log(A) + log(B) + log(C)}{1,06}$ (comme A, B et donc C sont premiers entre eux, on a :

$$Rad(ABC) = Rad(A).Rad(B).Rad(C)$$

Or pour des nombres entiers positifs, on a $A + B < A.B + 1$, ce qui entraîne que $log(C) < log(A) + log(B)$. En substituant cette inégalité dans la précédente, on obtient $logRad(ABC) > \dfrac{2logC}{1.06}$. Autrement dit, on s'attend à ce que, en moyenne, $C < Rad(ABC)^{0,53}$, ce qui peut être approximé par $\sqrt{Rad(ABC)}$.

Par analogie avec la puissance moyenne, qui quantifie la richesse d'un nombre, on introduit une mesure de la « richesse » d'un triplet : pour des entiers naturels A, B, C premiers entre eux qui vérifient $A + B = C$, on pose :

$$q(A, B, C) = \frac{log(c)}{logRad(ABC)} \Longrightarrow C = Rad(ABC)^q \tag{2.1}$$

$q(A, B, C)$ est la puissance à laquelle il faut élever le radical de ABC pour retrouver C.

Nous avons évalué cette mesure par des expériences numériques. En choisissant au hasard 10 000 triplets $(A, B, A + B = C)$ entre 1 et 10 milliards, nous avons obtenu une valeur moyenne $q^*(A, B, C) = 0,3848\ldots$ C'est largement en dessous de la valeur 0,53 conjecturée précédemment. En fait, l'approximation de $A + B$ par AB est très grossière.

La valeur moyenne de $q(A, B, C)$ ne livre cependant pas beaucoup d'informations. Déterminer une borne supérieure serait plus intéressant. Mais existe-t-elle ?

Commençons par essayer de construire des triplets A, B, C pour lesquels $q(A, B, C)$ est assez grand. Pour cela, il est utile de prendre un nombre C riche, par exemple l'entier $614\,810\,677 = 13^3.23^4$ utilisé précédemment, et de l'écrire comme une somme de deux entiers A et B premiers entre eux. En choisissant 10 000 couples (A, B) au hasard qui vérifient ces conditions, nous avons obtenu $q*(A, B, C) = 0,70195$. C'est déjà bien plus que la valeur conjecturée 0,53, et ce pour un choix aléatoire.

En outre, il existe des triplets particuliers pour lesquels q est encore plus grand. Par exemple, $q(13\,365, 614\,797\,312, 614\,810\,677)$ est égal à $0,864135...$ Comment expliquer cela ? Les nombres $A = 13\,365 = 3^5.5.11$ et $B = 614\,797\,312 = 150\,097.2^{12}$ sont assez riches, et $C = 13^3.23^4$ l'est davantage. De plus, A est petit par rapport à C, ce qui en général signifie qu'il a peu de chances de contribuer au radical. Il est remarquable que notre exploration aléatoire ait trouvé cette solution.

À partir d'un tel triplet de nombres presque puissants, on peut construire une équation pour laquelle des facteurs du triplet sont une solution. Pour l'exemple précédent, on peut construire l'équation $55x^5 + 150\,097y^{12} = 23z^3$, qui a pour solution $x = 3, y = 2$ et $z = 299 = 13.23$.

On peut généraliser cet exemple trouvé par hasard : on se donne une équation de trois variables, on cherche autant de solutions que possible et l'on construit à partir de celles-ci des triplets de nombres riches. Voici deux types d'équations intéressantes.

D'après un résultat élémentaire de la théorie des nombres, l'équation$x^2 = 3y^2 + 1$ admet un nombre infini de solutions. Le couple $(3\,650\,401, 2\,107\,560)$ en est une. Si on pose $A = 1, B = 3y^2$ et $C = x^2$, on obtient :

$$q(A,B,C) = \frac{logc}{logRad(ABC)} = \frac{2logx}{logRad(x.3.y)} \tag{2.2}$$

Comme x et $3y$ sont premiers entre eux (sinon, un diviseur diviserait $x^2 - 3y^2 = 1$), on a $Rad(x.3y) = Rad(x)Rad(3y)$. En outre, $log(3y)$ et $log(x)$ sont presque égaux pour x et y assez grands; par conséquent, si l'on suppose que ceux-ci sont des nombres « moyens » dont la puissance moyenne d vaut 1,06, on déduit que $q(A,B,C) \approx 1,06$, soit $q(A,B,C) > 1$. Pour les nombres cités en exemple, on trouve $q(1, 13\,325\,427\,460\,800, 13\,325\,427\,460\,801) = 1,06843$. C'est en effet supérieur à 1, mais pas de beaucoup.

Le deuxième type d'équations donne des puissances q encore plus grandes : il s'agit de $ax^3 + by^3 = cz^3$, où les coefficients a, b et c sont des entiers relatifs. Si une solution (x, y, z) comporte des termes négatifs, on peut toujours modifier l'équation pour n'avoir que des termes positifs. Si tous les monômes de l'équation sont positifs, on pose $A = ax^3, B = by^3$ et $C = cz^3$.

On connaît assez bien l'ensemble des solutions de ce type d'équations : elles appartiennent aux courbes elliptiques, des objets très étudiés en théorie des nombres et en géométrie algébrique. Parfois, ce type 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 $q(A,B,C) \approx d(x)$ 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 $q(A,B,C) \approx \frac{3}{2}d(x)$.

Le triplet $(1, 5.2^4, 3^4)$ donne $q = 1,29\ldots$

Le dernier exemple est particulièrement intéressant, car $81 = 3^4 = 5.2^4 + 1$ 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 $q(A,B,C)$ 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 $k > 4$, 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 $k > 4$ tel que $x^4 = 5y^4 + z^k$ est fini.

Résumons. Nos expériences numériques suggèrent qu'en moyenne, la puissance moyenne $q(A,B,C)$ d'un triplet est d'environ 0,5 ; dans tous les cas étudiés, q est inférieur à 2 ; pour de nombreux exemples, q est supérieur à 1, et ces valeurs élevées sont intimement liées à des solutions d'équations polynomiales à trois variables.

3. 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 $q(A,B,C)$ 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 a tel que $q(A,B,C) < a$.

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

$$A + B < Rad(A.B.(A+B))^a \tag{3.1}$$

Plutôt que d'affirmer l'existence d'une telle borne a, on aurait préféré qu'elle soit calculable. Des algorithmes qui peuvent en principe déterminer cette valeur ont 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 a, cela ne servirait pas à grand-chose : une approximation trop grossière ne dit plus grand-chose sur le comportement des triplets. La borne a doit être aussi petite que possible. D'après

nos résultats empiriques, on serait tenté de choisir $a = 1,4$. Malheureusement, dans certains cas, $q(A,B,C)$ est supérieur à 1,4. Par ailleurs, dans la plupart des cas, $q(A,B,C)$ 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 :

$$A+B < K.Rad(AB.(A+B))^a \tag{3.2}$$

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

$$q(A,B,C) < a + \frac{logK}{logRad(ABC)} \tag{3.3}$$

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 K 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 K supérieur au plus grand des nombres C testés, soit un milliard, pour que la conjecture soit vérifiée pour tout a, ce qui n'a aucun intérêt.

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

Cependant, cette formulation contient encore trop de choix. Pour faire rentrer un contre-exemple dans le rang, on a le choix d'augmenter a ou K. Le but est pourtant de tailler, par un choix approprié de a et K, 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 a et K légèrement plus petits que ces valeurs bien ajustées, on pourrait trouver un contre-exemple. Diminuer a demanderait d'agrandir K 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 a 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 a s'approche de 1. En termes précis, la conjecture ABC s'énonce ainsi :

Conjecture 3.4. *Pour tout nombre réel $\epsilon > 0$, il existe un nombre réel $K(\epsilon) > 0$ tel que, pour tous entiers naturels A, B et C premiers entre eux et tels que $A+B=C$, on ait :*

$$C < K(\epsilon).Rad(ABC)^{1+\epsilon} \tag{3.5}$$

Autrement dit, en prenant le logarithme :

$$q(A,B,C) < 1+\epsilon+\frac{logK(\epsilon)}{logRad(ABC)}$$

où le terme d'erreur $logK(\epsilon)$ dépend de ϵ.

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

La plus grande valeur connue pour $q(A,B,C)$ est $1,6299117$. Elle correspond au triplet $(2, 3^{10}.109, 23^5)$, 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 1020, nous savons qu'au moins dans cet intervalle immense, il n'existe pas de contre-exemple (pour $K(\epsilon) = 1$) à la conjecture ABC avec $a = 2$ (qui correspond à $\epsilon = 1$), c'est-à-dire $q(A,B,C) < 2$.

4. 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 a et K, c'est-à-dire pour lesquels $q(A,B,C)$ est grand. Ces exemples resserrent l'intervalle pour le choix de ϵ et $K(\epsilon)$, 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 $q(A,B,C) > 1,4$. Ces triplets sont extrêmement rares. Dans la tranche des entiers allant jusqu'à 1020, 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 $Rad(ABC)$:

$$Rad(ABC) = Rad(x^n y^n z^n) = Rad(xyz) < xyz < z^3$$

Cela donne une borne inférieure pour $q(A,B,C)$:

$$q(A,B,C) = log(C)/log(Rad(ABC) > log(z^n)/log(z^3) = n/3$$

Cette dernière quantité tend vers l'infini pour des exposants n élevés. Si par exemple $q(A,B,C)$ était borné par 2, on aurait ainsi démontré que l'équation de Fermat n'a pas de solutions pour $n > 6$. 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 nombres. Il s'agit en général de problèmes diophantiens, du nom du mathématicien du IIIe siècle Diophante d'Alexandrie. Ces problèmes font intervenir des équations polynomiales à coefficients entiers, dont on cherche les solutions parmi les nombres entiers (on parle d'équations diophantiennes). Une démonstration de la conjecture ABC fournirait en particulier une solution simple aux problèmes suivants :

– La conjecture de Catalan, selon laquelle l'équation $x^m - y^n = 1$ n'a qu'une seule solution parmi les entiers naturels : $3^2 - 2^3 = 1$. Elle a été démontrée en 2002 par le mathématicien roumain Preda $Mihăilescu$.

- La conjecture de Mordell, démontrée en 1983 par Gerd Faltings, affirme que chaque courbe dont le « genre » est plus grand que 1, définie par une équation polynomiale à coefficients rationnels, ne peut contenir qu'un nombre fini de points dont les coordonnées sont rationnelles (le genre peut être vu comme le nombre de fois où il est possible de couper la courbe sans obtenir deux morceaux séparés). Noam Elkies, de l'Université Harvard, a démontré en 1991 que la conjecture de Mordell est une conséquence de la conjecture ABC. Si la conjecture ABC était valable dans sa version la plus forte, cela prouverait non seulement l'existence de ces points rationnels, mais donnerait aussi un procédé effectif pour les déterminer.

- Un grand nombre de généralisations de ces problèmes. La preuve de la conjecture ABC entraînerait par exemple celle que chaque égalité (dite de Fermat) $ax^n + by^n = cz^n$ pour $n > 4$ (et a, b, c entiers relatifs) n'a qu'un nombre fini de solutions. Il en est de même pour l'équation de Catalan-Fermat $x^n + y^m = z^k$, si les exposants sont « grands », c'est-à-dire si $1/n + 1/m + 1/k < 1$.

Il reste qu'à ce jour, la conjecture ABC n'est pas démontrée – du moins tant que les affirmations de S. Mochizuki n'ont pas été vérifiées. Pourquoi serait-elle vraie ? Et quels sont les résultats intermédiaires atteints à ce stade ?

Comme on l'a vu, de nombreuses données numériques soutiennent la validité de la conjecture, mais elles n'aident en rien à la prouver. En mathématiques, on cherche à obtenir des énoncés qui ne concernent pas seulement un comportement moyen, mais qui sont valables dans tous les cas. Or la difficulté de la conjecture ABC vient des nombres exceptionnels qui échappent à la statistique.

5. Des pistes ténues vers une démonstration

En utilisant des méthodes de ce qu'on appelle la théorie des nombres transcendants, Cameron Stewart, Robert Tijdeman et Kunrui Yu ont pu montrer que le taux de croissance de C en fonction de $Rad(ABC)$ est au plus exponentiel. D'après la conjecture ABC, cette croissance est polynomiale, avec un exposant égal au plus à 2 ou $1+\epsilon$, suivant la version de la conjecture. On sait donc au moins que la croissance de C n'est pas illimitée, mais cela est insuffisant pour des grandes valeurs de C. Et il semble hors de portée de gravir, avec les méthodes utilisées, la marche séparant la croissance exponentielle de la croissance polynomiale.

Une autre approche emprunte un chemin a priori paradoxal. En généralisant la conjecture ABC, donc en la rendant en quelque sorte plus difficile, on a l'espoir de faciliter la démonstration. La généralisation consiste à remplacer les nombres naturels usuels par des structures abstraites plus compliquées. Les propriétés des entiers naturels utilisées dans la conjecture sont la structure additive, la structure multiplicative et l'ordre total : deux entiers peuvent toujours être comparés, au sens que l'un est forcément plus petit ou égal à l'autre. Ces trois propriétés se retrouvent dans beaucoup d'autres structures mathématiques, par exemple :

– Les nombres rationnels, c'est-à-dire les fractions de la forme r/s, où r et s sont des entiers relatifs. On utilise l'addition et la multiplication usuelles, mais au lieu de l'ordre habituel, on ordonne ici les rationnels par leur « hauteur », c'est-à-dire le maximum entre le numérateur et le dénominateur de la fraction sous forme réduite (sans tenir compte du signe). La hauteur est en quelque sorte une mesure de la complexité d'un nombre rationnel.

– Les polynômes, c'est-à-dire des sommes de produits de puissances des variables et de constantes. L'ordre est donné par le degré du polynôme, la plus élevée des sommes des exposants d'un terme du polynôme.

– Les fonctions rationnelles, c'est-à-dire les fractions dont le numérateur et le dénominateur sont des polynômes.

– Les extensions algébriques des nombres rationnels (corps de nombres algébriques) et des fonctions rationnelles (corps de fonctions algébriques).

Il est possible de transposer la conjecture ABC pour ces structures ; le contexte devient ainsi plus clair. R. Mason et W. Stothers ont prouvé l'équivalent de la conjecture ABC pour les polynômes par des méthodes élémentaires en 1981, avant que la conjecture sur les entiers n'ait été énoncée. Et dans le cadre général des corps de fonctions, la relation avec les courbes elliptiques, qui avaient déjà joué un grand rôle dans la preuve du théorème de Fermat, devient évidente.

Considérons une courbe elliptique E. On peut définir trois nombres qui la caractérisent : son invariant modulaire, noté $j(E)$, son discriminant, noté ΔE, et sa hauteur, notée $h(E)$. Le comportement de la courbe E est décrit par le radical du discriminant, aussi appelé conducteur de la courbe.

Lucien Szpiro, de l'Université de New York, a conjecturé qu'il existe un nombre k tel que pour toute courbe elliptique E, $K(|\Delta E|) < k$ (la puissance moyenne du discriminant est bornée). Il est remarquable que L. Szpiro ait observé ce comportement dans le cas des corps de fonctions, et ait formulé un analogue pour le cas des corps de nombres.

L. Szpiro a prouvé cette conjecture dans le cas des corps de fonctions (pour $k = 6$), si bien que la version forte de la conjecture ABC est vraie pour ces corps (ce qui généralise le résultat de R. Mason et W. Stothers). Cela justifie l'espoir que la conjecture soit valable pour les nombres rationnels qui, du point de vue arithmétique, sont assez semblables aux fonctions rationnelles.

J'ai généralisé la conjecture de L. Szpiro en affirmant que la hauteur $h(E)$ est bornée par un multiple de $logRad(|\Delta E|)$. J'ai ensuite prouvé que cette « conjecture sur la hauteur des courbes elliptiques » entraîne la conjecture ABC. Ces deux dernières sont même équivalentes dans le cadre des fonctions rationnelles.

En exploitant la très riche théorie des courbes elliptiques, développée depuis plus de 200 ans, notamment en utilisant des résultats qui ont conduit G. Faltings à la preuve de la conjecture de Mordell, j'ai ainsi trouvé une borne – malheureusement toujours exponentielle – de C en fonction de $Rad(ABC)$.

Mais on a fait encore mieux. Par sa relation avec l'arithmétique des courbes elliptiques, la conjecture ABC s'intègre à la géométrie algébrique. Cette branche des mathématiques, qui donne une interprétation géométrique à des problèmes de la théorie des nombres et apporte ainsi des éclaircissements surprenants, a été révolutionnée dans les années 1960 par le mathématicien Alexandre Grothendieck.

D'après moi, la conjecture sur la hauteur des courbes elliptiques n'est pas seulement un énoncé profond sur ces objets en question, mais aussi l'arrière-plan structurel recherché pour la conjecture ABC. Et pour J. Oesterlé, la motivation essentielle de la conjecture

ABC était son rapport avec l'arithmétique des courbes elliptiques.

La conjecture sur la hauteur des courbes elliptiques étant vraie pour le corps des fonctions rationnelles, la conjecture ABC l'est aussi pour ce corps. Ma démonstration en est simple et courte, mais on ne peut malheureusement pas la transposer du monde géométrique vers celui des nombres. En revanche, la démonstration initiale de L. Szpiro, bien plus compliquée, fournit une ébauche d'une telle transposition.

Cette preuve tire parti de l'arithmétique des surfaces algébriques, bien étudiées en géométrie algébrique. Il existe un analogue à ces surfaces dans le monde des nombres, appelé « surfaces arithmétiques ». Ces objets jouent un rôle clef dans la démonstration de la conjecture de Mordell, et les propriétés des surfaces arithmétiques qui permettraient de prouver la conjecture sur la hauteur des courbes elliptiques sont bien identifiées. Nous sommes cependant loin d'avoir trouvé ces propriétés...

Les travaux de S. Mochizuki ont-ils changé la donne ? Expert reconnu dans le domaine des surfaces arithmétiques, S. Mochizuki a prouvé des résultats difficiles sur la relation entre les « groupes fondamentaux au sens de Grothendieck » et les surfaces. Derrière ces termes et ces résultats se cachent encore des idées profondes de A. Grothendieck reliant la théorie de Galois à l'arithmétique. De nombreux spécialistes de la théorie des nombres se sont attelés à la vérification des travaux de S. Mochizuki, qui occupent des centaines de pages et qui utilisent des objets et méthodes mathématiques peu classiques. En attendant leur verdict, la conjecture ABC reste non démontrée.

On est au moins sûr d'une chose. La conjecture ABC n'est pas une bizarrerie gratuite de la théorie des nombres. Elle a de vastes conséquences et découle elle-même d'autres conjectures, dont il y a de bonnes raisons de penser qu'elles sont vraies. La relation entre théorie des nombres et géométrie qui sert de fondation depuis 50 ans à la géométrie algébrique serait mise à rude épreuve si la conjecture ABC était fausse. Il est difficile de l'imaginer.

References

[1] S. Mochizuki, Inter-universal Teichmuller theory I : Construction of Hodge theatres, 2012. Prépublication : www.kurims.kyoto-u.ac.jp/ffmotizuki/Inter-universal/Teichmuller/Theory/I.pdf

[2] G. Frey, Der Beweis des Fermatschen Theorems, Moderne Mathematik, pp. 166-175, Spektrum Akademischer Verlag, 1996.

[3] G. Frey, Links between solutions of $A - B = C$ and elliptic curves, Number Theory - Lecture Notes in Mathematics, vol. 1380, pp. 31-62, Springer, 1989.

[4] J. Oesterlé, Nouvelles approches du théorème de Fermat, Séminaire Bourbaki, exposé 694, 1987-88.

[5] F. Beukers, Introduction to the ABC conjecture, conférence donnée le 9 septembre 2005 : *www.math.leidenuniv.nl/ desmit/ic/abc/fritsABCpresentation.pdf*

[6] La liste des bons triplets : www.rekenmeemetabc.nl.

[7] Projet de calcul collaboratif des bons triplets : www.abcathome.com