Transcription en LaTeX et traduction de la conférence de Peter Sarnak au sujet de l'hypothèse de Riemann

Dan Freed : Bonjour. Je suis Dan Freed et c'est un plaisir de vous accueillir à cette septième et dernière conférence de notre série consacrée aux problèmes du Prix du Millénaire. Cette série de conférences, organisée tout au long de l'année, est parrainée conjointement par le Département de mathématiques de Harvard, le Centre CMSA de sciences mathématiques et applications de Harvard et l'Institut de mathématiques Clay. Sans plus tarder, nous avons le grand plaisir d'accueillir aujourd'hui Peter Sarnak de l'Institute for Advanced Study, qui nous parlera de l'hypothèse de Riemann.

Peter Sarnak : Merci, et merci pour l'invitation à faire cela.

Lorsque vous m'avez invité, je suis certain que vous ne vous attendiez pas à ce que j'annonce une démonstration de l'hypothèse de Riemann aujourd'hui. Si j'en avais une, je l'aurais même annoncée ici. Mais je peux vous dire que depuis que j'ai accepté de donner cette conférence, et surtout ces dernières semaines, le nombre de démonstrations dans ma boîte mail a considérablement augmenté. Auparavant, j'en recevais une toutes les deux ou trois semaines, et je les lisais attentivement, voire j'y répondais.

Mais depuis l'avènement de l'ia, ce nombre a considérablement augmenté, et ces dernières semaines, il a encore explosé avec les demandes pour que j'annonce les démonstrations d'autres personnes à la présente occasion. Je n'ai vérifié aucune démonstration. Je n'ai rien vu qui y ressemble. Mais c'est parce que je n'ai pas examiné la plupart de ces documents qui me sont parvenus. Je souhaite donc vous expliquer pourquoi il s'agit d'un bon problème. C'est un problème que l'on appelle une hypothèse. Je vais donc commencer par là.

Je ne vais pas m'attarder sur les détails mathématiques, mais plutôt vous expliquer pourquoi Riemann a formulé cette conjecture, quelles applications possibles il pourrait y avoir de cette hypothèse, pourquoi je considère ce problème comme pertinent, et quel est, selon moi, le véritable problème ici. Alors, passons à la suite.

(*aparté technique : Je peux m'en servir ? Je peux pointer du doigt si je veux, mais j'aime bien bouger un peu. D'accord.*)

L'affirmation de Riemann peut donc être énoncée très rapidement.

Voici l'énoncé : on considère la somme de n à la puissance moins s, qui, avant Riemann, était principalement vue par des théoriciens comme Euler comme une fonction de la variable réelle s lorsque s est supérieur à un. Il s'agit d'un produit sur les nombres premiers de 1 moins p la puissance moins s à la puissance moins 1.

$$\zeta(s) = \sum_n n^{-s} = \prod_n \left(1 - p^{-s}\right)^{-1}$$

Denise Vella-Chemla, assistée d'outils ia, septembre 2026.

Vidéo consultable à cette adresse https://www.youtube.com/watch?v=DtaFyE9BcXw .

On peut développer cette expression, la regrouper, et on obtient ainsi le théorème de la factorisation unique des entiers, qui est équivalent à cette identité. Nous avons donc deux représentations de cette fonction lorsque s est supérieur à un, et Riemann autorise d'abord s à être complexe.

En fait, une grande partie de la théorie des fonctions entières a été développée après ses travaux afin de mieux comprendre ce problème. Riemann a notamment publié un article important à ce sujet, dont je vais parler longuement. Il étend cette fonction à une fonction holomorphe dans tout le plan complexe, en tant que fonction d'une variable complexe. Cette fonction possède un pôle simple en 1, et il établit une relation remarquable, appelée équation fonctionnelle, qui consiste à ajouter à zêta la fonction gamma. La fonction gamma (Γ) est une fonction que nous connaissons très bien ; Riemann la comprenait parfaitement. Je vais vous montrer où elle intervient.

Il faisait ça en une minute. On prend $\Gamma\left(\frac{s}{2}\right)$. On a π à la puissance moins s sur 2. Vous multipliez par ce facteur, la nouvelle fonction est dans son article, il multiplie en fait par $\zeta(s)$ et $\zeta(1-s)$ afin de se débarrasser du pôle pour que la fonction soit entière.

Bref, admettons le pôle. Cette fonction présente une symétrie sa valeur en s est égale à sa valeur en $1-s$. Dans cet article, il formule non pas une conjecture, et je tiens à le souligner, mais une hypothèse. C'est un point crucial de sa réflexion. Il émet l'hypothèse de Riemann, selon laquelle tous les de zéros de la fonction complète se situent sur l'axe de symétrie. Il existe donc une infinité de zéros. Il le sait. Ce n'est peut-être pas évident, mais il le sait assurément. Voilà. Tout problème énoncé aussi rapidement présente un avantage certain. Je vais maintenant énumérer tous les points forts de ce problème.

Facile à énoncer si vous savez ce qu'est une fonction complexe.

Élégant dans sa réponse. Tous les zéros se trouvent sur la droite de partie réelle 0.5. Mais en quoi est-ce intéressant ? Bon. Alors, Riemann ne fait pas d'hypothèse. Il n'émet pas une conjecture. Et il ne formule pas d'hypothèse sans preuves. Personne ne le savait, mais Riemann a vérifié lui-même les premiers zéros. Une tâche loin d'être triviale, effectuée avec un crayon et du papier. Nombreux furent ceux qui consultèrent les écrits de Riemann dans ses archives, mais il fallut le génie de Siegel, bien des années plus tard, pour comprendre sa démarche, notamment lorsque, dans certains calculs, nous avions nous-mêmes calculé les premiers zéros. Je souhaite vous démontrer qu'il a calculé ces premiers zéros afin de formuler son hypothèse.

Il n'allait pas formuler cette hypothèse sans la moindre preuve. Alors, comment a-t-il procédé ? Comment calculer cela avec un crayon et du papier et affirmer que la partie réelle de zéro est exactement un demi ? Les premiers zéros qu'il a calculés sont environ 14, puis 21, 25, et ainsi de suite. Ils se situent sur la droite. Ils sont symétriques car la fonction est identique en s et en $-s$ Ce sont donc les premiers zéros. Comment peut-il être sûr, en calculant ici, que la partie réelle est exactement égale à $1/2$? Pour cela, il lui fallait une approximation de la fonction zêta de Riemann dans la bande critique. Je ne vous l'ai pas encore expliqué. J'en reparlerai plus tard, mais il est naturel de dire que cette fonction se décrit très facilement comme une série à convergence rapide. Mais il y a un fait concernant $\Gamma\left(\frac{s}{2}\right)$. Et si vous connaissez la formule de Stirling, si le premier zéro est à la

hauteur $14 \cdot i$, $\Gamma(s)$ sur la demi-droite sera égal à $e(-14 \cdot 2\pi)$, ce qui est un nombre extrêmement petit si vous effectuez le calcul manuellement. Vous avez donc considérablement réduit ce nombre, car tous vos calculs sont arrondis à zéro avec une très grande précision. Il a donc dû surmonter cet obstacle.

Et il l'a fait. Ce qui est remarquable, c'est qu'il a obtenu une expression pour la dérivée logarithmique, ou pour la fonction zêta et sa dérivée logarithmique dans la bande critique, une expression si précise qu'elle reste la meilleure connue à ce jour. C'est la référence absolue. Riemann a développé une méthode désormais appelée formule de Riemann-Siegel, car Siegel a compris la démarche de Riemann et l'a formalisée. La question est : combien d'étapes faut-il pour calculer la fonction zêta de Riemann à la hauteur t ? Il connaissait la hauteur à la hauteur t, et il y a environ $\log t$ zéros, ce nombre correspondant à la complexité. Cela nous permettra de comprendre pourquoi cette hypothèse, au moins généralisée, est l'une des plus importantes.

De belles conjectures. Son idée est d'intégrer f' sur f le long d'un petit contour contenant le premier zéro, qu'il parcourt en devinant sa position. Il effectue cette intégrale. Le résultat obtenu est un entier. Il calcule avec suffisamment de précision que cet entier vaut un. L'entier est donc un.

Le zéro doit avoir une partie réelle égale à un demi, sinon l'entier serait égal à deux ou plus. C'est pourquoi tous les zéros calculés de la fonction zêta de Riemann sont simples ; sinon, nous ne saurions pas qu'ils se situent sur la droite des nombres complexes de partie réelle un demi. Donc, quand on dit que nous avons vérifié, c'est que nous avons eu de la chance qu'il soit simple. Il a eu de la chance qu'il soit simple. De nombreux zéros ont été calculés, et j'en reparlerai dans un instant. Mais c'était son idée, et sa méthode montre que pour obtenir le zéro à la hauteur t, il faut environ vt étapes de calcul. C'est la méthode de référence.

En fait, elle a été améliorée par Odlyzko et Schönhage, puis par Hiary, qui, pour la seule fonction zêta, peut la réduire à $t^{1/3}$. Grâce à cela, je crois que les plus grands zéros jamais calculés se situent à 10 puissance 36. On ne va pas jusqu'à cette valeur ; on s'en approche directement.

Trouvez un calcul qui vous permette de déterminer précisément de quel zéro il s'agit. C'est ce qu'a fait Bob Hiary, et c'est la limite de ce que l'on peut atteindre. Comme je le disais, si nous savons que les zéros se trouvent sur la droite, c'est uniquement parce qu'ils sont simples. S'ils n'étaient pas simples, nous ne pourrions pas déterminer, par un calcul fini, s'il s'agit d'un double zéro ou d'un zéro presque parfait. Voilà.

C'est précisément ce qu'a fait Riemann, et il a qualifié cela d'hypothèse. Mais pourquoi l'a-t-il appelé une hypothèse ? Parce qu'il cherchait à faire autre chose. Il s'agissait d'une hypothèse de travail pour atteindre l'objectif de ce court article : démontrer le théorème des nombres premiers, le grand problème non résolu concernant les nombres premiers à l'époque. C'est Gauss qui avait conjecturé le théorème des nombres premiers, Gauss qui occupait la chaire avant lui, il y a eu Gauss, puis Dirichlet, puis Riemann.

Il fut le premier à formaliser cela correctement. Riemann découvrit qu'en utilisant l'analyse complexe et certaines intégrales de contour, et en comprenant les zéros de la fonction, on pouvait écrire

la fonction suivante, déjà bien documentée dans la littérature par Tchebychev.

La somme de $p^k(x)$ est une somme de puissances de nombres premiers, et non pas seulement de nombres premiers. Donc, $p^k \leq x$. Par conséquent, le théorème des nombres premiers n'est pas pertinent. Il s'agit d'une identité. La somme de $\log\, p_k(x)$ pour $p^k \leq x, x \geq 1$ (un nombre réel), est égale à x moins la somme de tous les zéros de la fonction C, et non seulement les zéros de la fonction C, mais de la fonction zêta. C'est une série conditionnellement convergente. Cet homme nous a montré la convergence, les sommes de Riemann et les séries de Fourier. Il savait de quoi il parlait. Cette somme est conditionnellement convergente, et son membre de droite donne une formule exacte pour le nombre de nombres premiers inférieurs ou égaux à x.

Il voulait ensuite démontrer le théorème des nombres premiers, c'est-à-dire le comportement asymptotique de $\pi(x)$, c'est-à-dire que la partie réelle de $\dfrac{\pi(x)}{\dfrac{x}{\log\, x}}$ tend vers 1 lorsque x tend vers l'infini. Comme il voyait x, il était très pratique que toutes les parties réelles soient inférieures à 1.

Et où sont-ils ? Eh bien, c'est à mi-chemin, d'après les trois premiers zéros qu'il avait calculés. Il a donc émis cette hypothèse. Et il disait qu'il y reviendrait. Oui, il est mort très jeune, comme nous le savons tous, mais je ne pense pas qu'il soit revenu à son hypothèse.

Il a exposé comment aborder le problème. Son hypothèse de travail lui a permis de parvenir à la conclusion qu'il jugeait la plus intéressante. Je ne sais pas s'il y est revenu, mais ses idées, et je vais vous donner de nombreux exemples de ce genre, ont abouti à une démonstration inconditionnelle de la conséquence. C'est le théorème des nombres premiers. Il s'agit du célèbre théorème de Hadamard et de la Vallée Poussin, établi quelques années plus tard, en 1896. Ils ont démontré juste assez pour prouver le théorème des nombres premiers, à savoir que la partie réelle de tout zéro est strictement inférieure à 1.

Je ne parle pas de records du monde ou quoi que ce soit de ce genre. C'est l'équivalent du théorème des nombres premiers, et c'était une étape très complexe. C'est ce que j'appellerais une solution de contournement.

Il y a une hypothèse, une hypothèse de travail, qui mène au résultat souhaité, mais on arrive quand même à sa conclusion. Voilà l'exemple. C'est un excellent problème. D'abord, il est élégant, facile à énoncer et falsifiable. Mais pourquoi tout ce tapage ? Franchement, qui s'intéresse aux zéros sur la droite $\dfrac{1}{2}$? Bon, on a le théorème des nombres premiers. Pourquoi s'intéresser aux zéros sur la droite $\dfrac{1}{2}$?

En fait, permettez-moi de préciser. Si l'hypothèse de Riemann est prouvée, ce serait une avancée mathématique majeure. L'Institut Clay, je crois, verserait la somme due si la preuve s'avérait exacte.

Je n'en ai aucun doute. Personnellement, je suis certain que cela impliquerait de nouvelles idées sur les entiers et les structures, certains produits, etc. Je vais en discuter en détail. Cependant, je serais extrêmement déçu si vous vous contentiez de démontrer l'hypothèse de Riemann pour

la fonction zêta de Riemann et aucune autre, car je ne connais aucune application intéressante ou particulièrement marquante de cette hypothèse. C'est donc dans le contexte d'hypothèses plus générales, toutes identiques, que le problème prend toute sa dimension. Cela dit, cela ne signifie pas que vous ne devriez pas travailler sur l'hypothèse de Riemann, car je suis sûr que si vous la démontrez, quelqu'un dira : "Je démontrerai les autres demain".

Mais on ne sait jamais. Quelqu'un pourrait y découvrir une fonctionnalité très spéciale. Mais je n'en sais rien. Je dis ça comme ça, au hasard : "Quelle est la meilleure conséquence que je connaisse de l'hypothèse de Riemann elle-même ?" Eh bien, il s'agira des nombres premiers. Plus tard, je vous montrerai que l'hypothèse de Riemann a des implications dans de très nombreux domaines différents.

C'est ce qui rend la chose intéressante. Mais, une des conséquences est que nous aimerions savoir que tout cela se résume à la place archimédienne des nombres premiers. Ainsi, Selberg a démontré en 1943 que, sous l'hypothèse de Riemann, il existe toujours un nombre premier dans un intervalle $[x, (x + \log(x))^{2+\varepsilon}]$, qui est un petit intervalle. C'est extrêmement difficile à démontrer, mais c'est vrai pour presque tout x.

Et cela se produit à une échelle déjà très petite, puisqu'il s'agit d'un logarithme élevé à une puissance. C'est une conséquence de la fonction zêta de Riemann, et c'est sans doute la plus intéressante à mes yeux. Si vous voulez voir les conséquences liées à la fonction zêta de Riemann, jetez un œil au livre de Titchmarsh, un ouvrage remarquable intitulé "*La fonction zêta de Riemann*". Il est entièrement consacré à cette fonction, et à aucune autre.

Et puis il y a une section sur les conséquences de l'hypothèse de Riemann, et vous dites : "Ah, est-ce un problème sur lequel nous travaillons, que nous mettons en lumière ?". Eh bien, c'est un problème majeur, car je suis sûr qu'il fait partie du tableau d'ensemble, et c'est là mon argument. Très bien.

Maintenant, si vous réfutez l'hypothèse de Riemann, c'est-à-dire si vous trouvez un zéro hors de la droite et Nick Trefethen m'a demandé : "Que serait-ce catastrophique ?" -, imaginez nous avons atteint une certaine hauteur, et il y a un zéro hors de la droite. Il y a plusieurs points intéressants à considérer. Premièrement, Clay pourrait ne pas vous payer. Le saviez-vous ? J'ai lu les petites lignes, non pas parce que j'avais un contre-exemple.

Mais ils sont fous. Ils prétendent ne pas avoir à vous payer si vous réfutez une hypothèse. Moi, je vous paierai.

[Rires]

Je ferai appel à la communauté si vous trouvez un zéro manquant. C'est pour ça que j'ai parlé de contribution collective.

[Rires]

Ainsi, si vous trouvez un zéro, curieusement, vous pourriez résoudre des problèmes qui restent insolubles en trouvant un zéro hors de la droite. En effet, il existe une propriété de répulsion de Landau-Siegel selon laquelle, dès qu'un zéro est hors de la droite, pour n'importe quelle fonction L, il empêche les autres zéros de se comporter d'une certaine manière.

Et vous pourriez même prendre ce zéro et résoudre un problème, et je pourrais même vous indiquer de quel problème il s'agit au fur et à mesure. Donc, vous pourriez résoudre un problème, mais si vous trouviez un zéro hors de la droite, la vérité est que ce serait une catastrophe. Et la raison pour laquelle ce serait une catastrophe n'est pas qu'un seul zéro hors de la droite nous perturberait. Mais comment pouvons-nous croire qu'il n'y a qu'un seul zéro hors de la droite ? Nous devons alors croire que c'est faux, et donc que c'est faux de manière plus générale. Et ensuite, je vais essayer de vous convaincre que si c'est vrai, c'est l'une des grandes preuves de la théorie des nombres en mathématiques. Donc, cela ferait éclater nos illusions. Je suis sûr que quiconque le souhaite serait très heureux de voir ces illusions éclater. Mais, de toute façon, beaucoup d'entre nous seraient très contrariés si c'était faux. Mais, vous pourriez demander : "Eh bien, qu'en est-il de cette preuve que je viens de mentionner, 10 puissance... quoi déjà ?". C'est assez élevé. Comme je l'ai dit, vous savez, lorsqu'on vérifie les zéros, nous connaissons probablement les 10^{12} premiers d'entre eux.

Turing cherchait aussi à ce que sa machine trouve immédiatement un zéro hors de la droite. Et c'est ce que certains essaient de vous faire croire pour vous convaincre de la puissance d'autres technologies. Est-ce convaincant ? Eh bien, il faut être prudent, car le plus important, c'est la complexité, sur laquelle je reviendrai constamment, où le fil conducteur, c'est le nombre de zéros. Et si vous êtes à une hauteur de 10^{26}, ou à une hauteur T, le nombre de zéros est seulement $\log T$. Et donc, ils n'ont pas encore commencé à s'en approcher beaucoup, car vous avez considéré que le nombre de zéros n'est que $\log 10^{26}$. Il y a pas mal de zéros, mais s'il existe une caractéristique où ils vont s'en approcher beaucoup et peut-être sortir de la droite, il faut aller beaucoup plus haut. Donc, il faut aborder ces choses avec prudence, et tout le monde a calculé jusque-là, et les zéros étaient toujours sur la droite critique. Mais, je pense que l'hypothèse est réfutable, et il existe de nombreux cas où elle a été prouvée. Donc, c'est très bien de ce point de vue. Très bien.

Je vais donc maintenant présenter ce qu'on appelle l'hypothèse de Riemann généralisée. C'est ici qu'elle prend forme après l'hypothèse de Riemann, à travers d'autres fonctions L, et qu'elle devient une hypothèse de travail extrêmement puissante permettant de résoudre des problèmes par des approches alternatives. Si elle s'avérait vraie, de nombreuses conjectures seraient résolues. De nombreux théorèmes s'appuient sur l'hypothèse de Riemann. Non, il n'existe pas beaucoup de théorèmes qui disent : "Supposons l'hypothèse de Riemann." Il existe de nombreux théorèmes qui disent : "Supposons l'hypothèse de Riemann généralisée." Je ne vais donc pas vous donner la définition la plus générale, mais au moins celle qui vous donnera une idée de ce dont je parle. La fonction zêta de Riemann admet de nombreuses généralisations. Je parlerai des fonctions zêta de Dedekind. Enfin, j'aborderai les fonctions L que nous connaissons. C'est très important. Nous connaissons le terreau dans lequel ces fonctions se développent. Elles proviennent toutes de formes automorphes. Ce qui rend les formes automorphes si intéressantes à mes yeux, c'est qu'elles sont les seules source des fonctions L.

Nous savons donc où faire croître ces objets, et c'est dans ce contexte que nous pensons que toutes

ces conjectures sont vraies. Par conséquent, je ne parlerai plus beaucoup des formes automorphes, sauf à la fin.

Considérons la fonction zêta de Dedekind. Considérons une extension finie des rationnels, et nous pouvons procéder de la même manière. Le nombre de classes peut différer de 1, mais il existe une factorisation unique en idéaux premiers, et l'identité énoncée par Euler reste vraie. Ceci est dû à Dedekind.

$$\sum_a N(a)^{-s} = \prod_P (1 - N(P)^{-s})^{-1}$$

La somme des normes des idéaux puissance $-s$ est égale au produit de 1 moins la norme de l'idéal P puissance $-s$, la différence étant élevée à la puissance -1 (on prend son inverse). De plus, cette fonction admet une équation de prolongement analytique. Ce n'est pas chose aisée. Dedekind n'a pas réussi à le démontrer. Il a fallu le génie de Hecke pour y parvenir, car, à mon avis, la structure additive, combinée aux unités du corps des nombres, était trop complexe pour les premiers chercheurs.

Mais Hecke l'a expliqué. Et la fonction possède la même caractéristique. C'est très important. Il y a quelque chose de nouveau. Si le degré de l'extension est n, il y aura, je suppose, tous les plongements d'extension du corps des nombres réels, alors c'est ce fameux sur 2π que Riemann a introduit. Et puis il y a le discriminant, et tout cela concerne le conducteur de ramification. C'est ce que contrôle l'hypothèse de Riemann. Elle contrôle la ramification de manière très profonde. C'est de là que vient la puissance des applications de l'hypothèse de Riemann. Donc, le discriminant représente les nombres premiers auxquels le corps de nombres est ramifié, et la ramification est intégrée au discriminant par un entier, et cela apparaît dans l'équation fonctionnelle. Ainsi, l'équation fonctionnelle possède maintenant ce conducteur, ou complexité.

Et le plus important, c'est que le nombre de zéros localement... Donc, si vous augmentez le degré, vous aurez de plus en plus de zéros, mais localement, le nombre de zéros d'une fonction zêta de Dedekind sera de $\frac{\log D}{2\pi}$. Je vous encourage à bien noter le logarithme. Cela va me permettre de dépasser les classes de complexité. Le logarithme du conducteur est le nombre de zéros. Et le nombre de zéros, si vous avez un polynôme, sera lié au degré, donc clairement à la complexité.

Donc, le logarithme du conducteur est comme le degré. Très bien. Donc, nous avons la même chose. Et qu'est-ce que l'hypothèse de Riemann généralisée (GRH) ? Eh bien, une belle conjecture. Ce sont des conjectures, on dit "si", il y a certaines conditions, mais rien ne change : tous les zéros sont sur la droite un demi.

Aucun changement. L'hypothèse de Riemann généralisée affirme que tous les zéros de toutes ces fonctions L sur la droite sont égaux à un demi, point final. D'accord. Donc, il s'agit de la conjecture appelée GRH, celle que nous considérons tous, ou du moins moi, comme l'hypothèse de Riemann. Bien sûr, ces conjectures ont été vérifiées, mais seulement à des degrés très faibles. Car, comme je l'ai dit, on peut toutes les développer, mais c'est difficile. Il existe une base de données incroyable que vous pouvez explorer vous-même. C'est la base de données des fonctions L et des formes modulaires, et Drew en est l'un des principaux contributeurs. Elle contient une mine d'informations sur le "zoo". Et pour chaque élément du "zoo", on obtient une fonction zêta. Et chaque fonction zêta possède son hypothèse de Riemann.

Et chacun d'eux, je crois, a été plus ou moins vérifié pour ses premiers zéros. Et cette espèce est assez complexe, et donc on pourrait penser : "Eh bien, ces types de fonctions-là ne vont probablement pas la satisfaire." J'y reviendrai. L'hypothèse de Riemann généralisée (GRH) est qu'ils la satisfont tous. Point final. Je ne vais pas essayer de convaincre. Une fois, quelqu'un est venu me voir et m'a dit : "Vous n'avez pas prouvé l'hypothèse de Riemann, qu'avez-vous fait ?"

[Rires]

Bon, j'ai trouvé un emploi, d'accord. Tout comme Riemann, il existe une solution de contournement, une hypothèse. Précisons d'emblée que l'hypothèse de Riemann reste une hypothèse. Je ne l'ai jamais entendue qualifiée de conjecture. C'est une hypothèse, une hypothèse de travail.

Si elle est prouvée, bien sûr, on n'a plus besoin de la conjecturer. Mais elle implique des choses étonnantes, et ce qui est remarquable, c'est que dans de très nombreux problèmes, on peut encore prouver ces choses de manière inconditionnelle. C'est pourquoi le sujet est si dynamique. Il existe toute une théorie de l'analogue du théorème des nombres premiers, à savoir le théorème de non-annulation des fonctions L. C'est un problème très général. Il existe des substituts à l'hypothèse de Riemann qui disent, eh bien, peut-être... Alors, voici comment déterminer si cela pourrait être utile. Si j'ai un problème et que je peux dire : "en supposant l'hypothèse de Riemann généralisée, j'obtiens ma conclusion", je suis très content. Puis-je m'en débarrasser ? Eh bien, la première question à se poser est : s'il y a un zéro, est-ce que ce zéro hors sujet va tout gâcher ? Si oui, alors vous êtes dans le pétrin. Mais si un zéro ne vous pose pas de problème, alors probablement que plusieurs zéros ne vous en poseront pas non plus. Il existe des théorèmes de densité qui stipulent qu'il y a très peu de zéros hors de la droite, et que les conditions deviennent alors inconditionnelles. Ce sont des théorèmes classiques de ce type, très répandus dans le domaine.

Il existe des estimations uniformes obtenues en considérant les zéros sur la droite. Si vous êtes analyste, vous prenez le logarithme de zêta, vous appliquez le théorème des trois droites et vous utilisez le fait que le logarithme est analytique jusqu'à la droite 1/2. Là où tout le monde calcule des puissances, vous obtenez le logarithme à une puissance, ce qui constitue une borne beaucoup plus précise. Vous obtenez ainsi des bornes uniformes en fonction des paramètres et vous savez exactement comment les choses se comportent si vous supposez l'hypothèse de Riemann généralisée (GRH). Parfois, dans de nombreux problèmes intéressants, il n'est pas nécessaire d'obtenir les bornes optimales complètes, il suffit d'être en dessous de certaines bornes ; c'est ce qu'on appelle la sous-convexité. Je ne vais donc pas vous faire un exposé sur ce que nous pouvons faire, mais je tiens simplement à souligner que le sujet est en plein essor et que c'est précisément l'objectif de la théorie des fonctions L. Et si cette grande vérité était enfin connue, cela aurait un impact tel qu'on pourrait prendre de très nombreux théorèmes et dire : "Je n'ai plus besoin de travailler, vous savez, bien souvent nous sommes comme sur un fil au-dessus d'un pont pour utiliser telle estimation ici et telle autre là, puis atteindre l'autre côté", et ensuite on aurait simplement cette autoroute, qu'il suffirait de traverser Et de nombreux théorèmes contenus dans les livres ne seraient plus nécessaires. Désormais, les techniques sont souvent plus intéressantes. Très bien. Je vais donc vous donner quelques exemples d'application où l'hypothèse de Riemann généralisée (GRH) sert d'hypothèse de travail, et pour lesquels les résultats ont été démontrés, comme il se doit si l'hypo-

thèse de Riemann généralisée est vérifiée. Le théorème des nombres premiers est le premier exemple que j'ai donné, à titre d'exemple principal.

Voici un autre exemple. Les nombres premiers appartiennent à l'ensemble $\mathcal{P}$. Peut-on déterminer si un grand nombre (dont je vous donnerai la complexité, le nombre de chiffres) est premier ou non ? Existe-t-il un algorithme qui me permette de le savoir en un temps fini ? Cela a été démontré pour la première fois sous l'hypothèse de Riemann par Gary Miller en 1975. Il a utilisé l'hypothèse de Riemann généralisée (GRH) de manière rigoureuse. Il a exploité la propriété de conducteur dont je vous parle : si deux fonctions L sont identiques à un logarithme près, alors elles le sont indéfiniment. C'est ce qu'on appelle le contrôle par conducteur. Exactement de cette manière. La démonstration inconditionnelle de ce résultat par Agrawal, Kayal et Saxena en 2002, en utilisant certaines des mêmes idées, mais non pas avec les fonctions L elles-mêmes, mais dans un autre contexte, a été assez inattendue, mais très appréciée. Ainsi, souvent, le substitut peut être directement obtenu. Souvent, il s'agit de la même idée ou d'une variante, et c'est ce qui a été utilisé. Parfois, c'est assez différent. Je vais donc passer à quelque chose de très récent.

Il s'agit de la conjecture d'André Oort, démontrée par Bruno Klingler, Emmanuel Ullmo et Andrei Yafaev en 2014 sous l'hypothèse de Riemann généralisée (GRH). Cette conjecture porte sur des points spéciaux sur des variétés particulières appelées variétés de Shimura. L'affirmation de la conjecture est la suivante : si l'on considère une sous-variété ne contenant pas de sous-variété de Shimura (donc non spéciale), alors il n'existe qu'un nombre fini de ces points sur cette sous-variété. C'est donc un théorème de finitude. Ce théorème a été démontré sous l'hypothèse de Riemann généralisée, mais il a récemment été démontré de manière totalement inconditionnelle par Pila, Shankar et Zimmermann, avec un appendice de H. Esnault and M. Groechenig. C'est une avancée remarquable, mais il faut savoir que démontrer des théorèmes aussi profonds et complexes, comme celui de la finitude, est souvent inefficace. Autrement dit, le fait qu'il n'existe qu'un nombre fini de points sur la sous-variété fait partie du théorème ; ils le démontrent, mais ils ne peuvent pas affirmer avoir trouvé tous les points. Or, si l'on connaissait l'hypothèse de Riemann, on pourrait rendre leur démonstration valide.

Et si vous trouviez un zéro sur la droite, c'est le genre de chose qui pourrait rendre le système, vous savez, inefficace. Donc, pour moi, le problème d'André Oort est résolu, sauf pour la question de l'efficacité, qui, compte tenu des informations dont nous disposons, deviendrait inefficace, voire efficace.

Actuellement, cette méthode est inefficace. Une élégante conjecture de Odlyzko-Poonen a récemment été résolue grâce à l'hypothèse de Riemann généralisée (GRH). Nous ne savons pas encore comment la lever. Je suis certain qu'elle le sera un jour, mais pour l'instant, elle est conditionnelle sous l'hypothèse de Riemann généralisée (GRH). Autrement dit, si l'on considère un polynôme à coefficients nuls ou égaux à un, est-il valide avec une probabilité de un lorsque d tend vers l'infini ? Il existe de nombreux théorèmes où les coefficients a varient parmi les entiers jusqu'à t, et le théorème devient alors très simple. De même, si l'on fixe les coefficients a à des ensembles finis de taille finie, ce théorème a également été démontré. Il existe de nombreuses variantes, mais avec des coefficients nuls ou égaux à un, la situation est très complexe. C'est précisément le cas de la conjecture de Odlyzko-Poonen, récemment démontrée par Varjú et Breuillard. La démonstration repose sur le théorème de Riemann, qui consiste à prouver qu'une grandeur est un expandeur, et nécessite de

démontrer qu'une opération et un produit sont également des expandeurs. C'est peut-être mon exemple préféré.

Je vous ai donc montré un exemple de complexité. D'ailleurs, il y en a un autre.

Peut-on reconnaître si un nœud est noué ou non ? Le problème de savoir si le fait de reconnaître qu'un nœud est noué ou non est dans NP a obtenu sa première démonstration, par Kuperberg, et sa démonstration supposait l'hypothèse de Riemann généralisée (GRH), puis Lackenby et Eagle, je crois, ont fourni une démonstration inconditionnelle. Ces problèmes impliquent souvent l'utilisation d'entiers, généralement premiers, de manière approfondie. Je souhaite vous présenter un cas où l'hypothèse de Riemann généralisée (GRH) est étroitement liée à la théorie des nombres. C'est d'ailleurs celui que je préfère. Depuis l'invention de la méthode du cercle de Hardy-Littlewood, ce problème a toujours constitué un goulot d'étranglement. Je cherche à dénombrer les solutions de l'équation "somme de trois cubes égale somme de trois cubes" ($x_1^3 + x_2^3 + x_3^3 = x_4^3 + x_5^3 + x_6^3$). Il existe de nombreuses solutions, mais je souhaite fournir une borne supérieure précise pour d'autres applications. Je ne vais donc pas expliquer pourquoi il s'agit d'une question centrale, souvent soulevée dans ce domaine. Hua, expert en la méthode du cercle de Hardy-Littlewood dans les années 1940, a donné une limite.

Donc, la borne triviale, évidemment, si les x sont au plus égaux à t, est t à la puissance six, mais il a donné une borne bien meilleure, qui est $t^{\frac{7}{2}}$. Et ils conjecturent qu'elle est de t à la puissance trois, plus un petit epsilon ($t^{3+\varepsilon}$).

On ne peut pas obtenir une valeur plus précise que t à la puissance trois, car on peut avoir $xxx = yyy$ et donc on obtient des solutions de l'ordre de t^3. Hooley a démontré un théorème remarquable : on obtient bien t^{3+e} si l'on suppose l'hypothèse de Riemann généralisée pour les fonctions de Hasse-Weil de variétés à trois dimensions, issues d'un outil analytique qu'il a inventé. Il s'agit d'une analyse diophantienne complète, et à un certain moment, l'opérateur 1 sur ces fonctions de Hasse-Weil intervient dans son analyse. L'opérateur 1 sur L ne recherche pas des nombres premiers, et il doit contrôler cela. Et si l'on y parvient, et il affirme que c'est en supposant l'hypothèse de Riemann, alors... Je ne pense pas que quiconque puisse actuellement espérer remplacer cette hypothèse et obtenir ce résultat de manière inconditionnelle. Les deux derniers exemples que je mentionne sont des cas pour lesquels nous n'avons pas encore trouvé de solution. Quant au dernier... Bon, j'ai plusieurs articles qui restent conditionnés par l'hypothèse de Riemann généralisée. J'étais aujourd'hui au séminaire de Katie Wu. Elle expliquait un théorème pour la démonstration duquel elle a supposé que l'hypothèse de Riemann généralisée était vérifiée. Elle va le retirer.

[Rires]

Voilà donc une hypothèse de travail. Bien. Une autre raison d'être de cette hypothèse et je la soulève car je souhaite expliquer son importance est son impact potentiel sur d'autres domaines et les enseignements que nous pourrions en tirer. Il existe d'autres analogues, comme le célèbre corps de fonctions qui nous permet de comprendre de nombreuses choses. On remplace les nombres rationnels par des fonctions rationnelles sur un corps fini, et les entiers par des polynômes. On retrouve alors la même propriété de factorisation des polynômes en polynômes premiers et la construction

d'une fonction zêta.

Ici, il est d'usage de ne pas utiliser la variable complexe s, mais le paramètre t, car toutes les fonctions sont désormais des polynômes ou des rationnels. On évite ainsi d'écrire une fonction analytique de P^{-s}, ce qui serait très confus. On effectue donc ce changement de variable. On obtient alors la fonction zêta de l'espace projectif, qui est simplement $\mathbb{F}_q[t]$, et elle possède un pôle en 1. Cette fonction zêta est complète : elle n'a pas de numérateur, ni de zéros.

Si c'était l'hypothèse de Riemann dans le domaine des fonctions, ce serait un peu ennuyeux. C'est ennuyeux. Mais Emil Artin, dans un article fondamental et novateur, a dit : "Considérons une extension finie de la courbe définie sur un corps fini, et l'on obtient alors un numérateur. Ce n'est pas si difficile à démontrer." Et c'est ce qu'il a démontré. Il s'agit d'un polynôme de degré $2g$, où g est le genre du corps de fonctions.

On pourrait se demander si l'hypothèse de Riemann est vraie dans ce cas. Et Artin l'a fait. Il existe une équation fonctionnelle qui transforme t en $1/qt$. Ainsi, pour cette variable t, les zéros de cette transformation se trouveront tous sur un cercle si l'hypothèse de Riemann est vérifiée, cercle qui est de rayon $1/\sqrt{q}$. André Weil a proposé une généralisation remarquable de cette conjecture, où l'on considère non plus des courbes sur un corps fini, mais des variétés projectives lisses d'un corps fini. Il a su formuler l'analogue de l'hypothèse de Riemann, on appelles ces analogues les conjectures de Weil. Weil lui-même a démontré cette hypothèse de Riemann posée par Emil Artin. Pendant la Seconde Guerre mondiale, il en a donné deux démonstrations. L'une d'elles, absolument brillante, utilise les surfaces et la propriété de croisement de courbes. C'est celle dont beaucoup espèrent encore qu'elle sera pertinente dans le cas réel, mais je ne m'y attarderai pas. Grothendieck a développé une théorie de la cohomologie qui s'est avérée essentielle, et Deligne a pu démontrer l'analogue de l'hypothèse de Riemann dans ce contexte. Croyez-moi, cela a des millions et des millions d'applications.

Je ne vais même pas commencer à énumérer toutes ces applications. La fonction ζ est utilisée dans les sommes exponentielles et dans de très nombreux domaines de l'ingénierie. Mais l'avancée cruciale qui a ouvert la voie ici, c'est la possibilité de linéariser le problème. Autrement dit, les zéros des fonctions zêta dans les corps de fonctions peuvent être réalisés à l'aide du morphisme de Frobenius, qui est une application qui à x associe x^q, agissant sur cette cohomologie. C'est ainsi que le problème est linéarisé, et nous obtenons une interprétation linéaire, ou spectrale, des zéros. Mais il est très important de comprendre que cette linéarisation ne place pas les zéros sur la droite, ni sur le cercle, dans ce cas précis. Ce n'est pas comme si tout cela relevait de la magie et qu'il y avait un problème de Hilbert-Pólya auto-adjoint.

J'y reviendrai. Il n'y a pas de formule magique. C'est une étape supplémentaire très importante. Weil a fourni deux démonstrations. Il existe une preuve utilisant la combinatoire, une méthode polynomiale de Stepanov, toutes deux pour les courbes, mais lorsqu'on atteint des dimensions supérieures, la seule preuve connue consiste à ne pas considérer une seule variété à la fois. Et c'est extrêmement important. On ne sait pas comment démontrer l'hypothèse de Riemann pour plusieurs variétés à la fois. Il faut les déformer au sein d'une famille. En mathématiques, on sait que lorsqu'on prend un élément en soi, on ne sait pas trop quoi en faire, mais si on peut le déplacer, on

peut faire quelque chose. Dans ce raisonnement, il y a un élément qui relie les différents éléments. On appelle cela la monodromie. C'est ce qu'a utilisé Deligne. Et en déformant les éléments, il a pu établir l'hypothèse de Riemann pour toutes les variétés, pour celle qu'il souhaitait et pour toutes en même temps. Le lien qui permet de passer d'une variété à toutes les autres, c'est la nouvelle fonction zêta. Et le plus important, c'est qu'on utilise aussi l'outil de Grothendieck.

C'est fantastique, c'est, comme je l'ai dit, l'une des plus grandes réussites du XXe siècle. Et tout ça grâce à ce problème analogique. Disons que je ne devrais peut-être pas le dire ici, mais ce fameux problème analogique. D'accord. J'espère donc qu'en expliquant l'hypothèse de Riemann généralisée (GRH), vous comprendrez qu'il s'agit d'un problème majeur. Pour moi, l'hypothèse de Riemann généralisée remplit tous les critères : elle est élégante et réfutable. Chacun de ses cas est élégamment réfutable. Si l'hypothèse de Riemann généralisée est vraie, je ne vous ai pas donné beaucoup d'exemples, mais c'est une vérité extrêmement puissante sur le monde. Cette hypothèse est donc un problème majeur. L'hypothèse de Riemann généralisée révèle quelque chose de profondément enfoui, dont nous ignorons la raison d'être, mais qui, si elle est vraie, est extrêmement puissant.

Ça, on le sait. Et bien sûr, un grand problème inspire aussi des généralisations dans des domaines connexes. Donc, en ce sens, l'hypothèse de Riemann généralisée (GRH), et je considère de manière indiscernable l'hypothèse de Riemann et l'hypothèse de Riemann généralisée (RH-GRH) est un problème qui devrait figurer sur la liste de tous, y compris celle du Clay Institute. Si quelqu'un réfute l'hypothèse de Riemann, il faudra le payer. Je n'aime pas ça. En bref, c'est même tout ce qui me déplaît. L'avantage, c'est que l'hypothèse de Riemann a remplacé le dernier théorème de Fermat. Le dernier théorème de Fermat, c'était ce que, vous savez, quand on arrive en mathématiques, on a envie de tester immédiatement. Maintenant, avec l'hypothèse de Riemann, on peut le faire, tout simplement parce que Perelman a démontré le dernier théorème de Fermat. Du coup, il n'y a plus grand-chose à en tirer pour eux.

[Rires]

Mais c'est tellement facile à énoncer... et je voudrais maintenant commenter. Le reste de cette conférence sera donc un commentaire sur l'état actuel des choses et une exploration plus approfondie.

Nous avons donc des substituts, mais je n'en parlerai pas. J'ai donné une conférence il y a sept ans, je crois pour le 150e anniversaire de l'article de Riemann, lors d'un grand colloque à Bristol[1]. J'y ai comparé différentes approches et idées, et je ne les détaillerai pas ici, si ce n'est pour rappeler quelques points essentiels. Commençons par les plus fondamentaux. La fonction zêta de Riemann relie cette somme et ce produit. Or, nous ne savons pas comment combiner ces deux structures de manière décisive. Le prolongement analytique s'obtient par l'analyse harmonique.

Oui, c'est toujours la même analyse harmonique. On place les entiers à l'intérieur de la droite réelle. Ils s'y insèrent parfaitement, et $\mathbb{R}$ mod $\mathbb{Z}$ est un cercle muni de sa mesure. C'est un sous-groupe discret. Il préserve les mouvements.

Le quotient est compact, et nous effectuons une analyse harmonique sur le cercle. On obtient alors

1. Voir https://vimeo.com/539529535/0b096a810b .

une somme de Poisson, équivalente à l'équation de la fonction zêta de Riemann, et purement additive. C'est le premier aspect. Le second est multiplicatif. Et c'est précisément cette interaction entre les deux aspects qui rend le problème intéressant et profond. Mais d'un autre côté, nous raisonnons de manière multiplicative. Il est donc nécessaire de combiner les deux pour mieux comprendre ce problème. Ainsi, 99,9 % des tentatives d'application de l'hypothèse de Riemann par le grand public, par exemple, peuvent être démontrées comme erronées, car elles n'utilisent que l'équation fonctionnelle et non le produit eulérien. Ce point est crucial, et je tiens à le souligner particulièrement car il est fondamental. Si vous prenez une forme quadratique binaire définie $Q(x, y)$ à coefficients entiers, et que vous la sommez $\sum_{(x,y)\neq(0,0)} Q(x, y)^{-s}$, cela commencera à ressembler à une fonction zêta de Dedekind d'un corps quadratique imaginaire. Supposons que le nombre de classes de ce corps quadratique imaginaire soit supérieur à un et différent de un, alors cette série que vous avez écrite n'aura pas de produit eulérien.

Si j'additionne toutes les classes non équivalentes ayant le même discriminant, j'obtiens un produit eulérien. J'ai donc un nombre fini de séries de Dirichlet de la forme n^{-s}.

Chacune d'elles possède une équation fonctionnelle.

Chaque fonction semble, si on considère l'équation fonctionnelle, avoir le comportement attendu. Pourtant, aucune ne satisfait l'hypothèse de Riemann. Toutes possèdent des zéros lorsque la partie réelle s est supérieure à un, si le nombre de classes est supérieur à un. Si le nombre de classes est égal à un, il n'y a qu'un seul zéro, et il s'agit alors d'une fonction zêta de Dedekind. Celle-ci satisfait donc l'hypothèse de Riemann. Le produit eulérien est donc absolument crucial. Par conséquent, toute démonstration se basant uniquement sur l'équation fonctionnelle est vouée à l'échec. Même l'approche de Selberg, en 1980, qui était devenu célèbre 30 ou 40 ans auparavant pour avoir démontré que la fonction zêta de Riemann possède une proportion positive de ses zéros sur la droite des nombres complexes de partie réelle un demi.

Et puis les gens disaient : "D'accord, maintenant on sait qu'il a ce pourcentage. On va peut-être aller jusqu'au bout. Je ne sais pas. Même à 100 %, tout est en jeu. C'est juste une question de pourcentage."

Mais il s'en est rendu compte, et il a écrit un article très intéressant, ou peut-être a-t-il donné des conférences à ce sujet. Seul l'Institut archive ces conférences, si elles n'ont pas été publiées : chacune de ces fonctions zêta qui ne vérifient pas l'hypothèse de Riemann possède toujours une proportion positive de ses zéros sur la droite des nombres complexes de partie réelle un demi. Ainsi, ces théorèmes statistiques ne remettent pas en cause l'hypothèse de Riemann. Ils ne la remettent absolument pas en cause, et cela a dû être un peu difficile pour lui de venir dire : "Très bien, maintenant, laissez-moi vous montrer que je n'ai pas besoin du produit eulérien. Je peux quand même le prouver". En fait, 100 % de ces zéros se trouvent probablement sur la droite des nombres complexes de partie réelle un demi, et ce pour de bonnes raisons.

Ainsi, combiner les structures additive et multiplicative reste un défi. Des avancées remarquables ont été réalisées dans le domaine du produit de sommes et de produits, ainsi que dans l'algorithme de Kakeya et l'expansion. Ces méthodes reposent sur des propriétés combinatoires des produits,

mais concernant l'hypothèse de Riemann généralisée, il s'agit d'un problème très structuré pour lequel nous ne savons pas comment combiner directement les deux.

Très bien. Je continue d'expliquer pourquoi l'hypothèse de Riemann, ou le théorème des nombres premiers, est considérée comme difficile. Il me semble juste de dire, et je l'ai étudié, que pendant les trente premières années précédant la découverte du théorème des nombres premiers, on ne pensait pas vraiment que c'était un problème difficile. Il est clair que Riemann lui-même a déclaré : "Je vais y revenir pour vérifier sa véracité." Il a vérifié les premières hypothèses, a fait ce qu'il fallait, puis est passé à autre chose.

D'autres personnes ont commencé à y réfléchir, et je crois que certains ont même fait rédiger des thèses par leurs étudiants. Je crois que Littlewood a donné comme sujet de thèse : "Démontrer l'hypothèse de Riemann". Du coup, je ne pense pas que les gens aient compris si c'était difficile ou non.

Et nous ne savons pas. Comment savoir si quelque chose est difficile ? Je ne peux pas prouver qu'il n'existe pas de preuve simple. Mais je pense qu'il est juste de dire que rien n'est facile à dissimuler. S'il existe une preuve simple, elle est très bien cachée, et aucune manipulation simple ne permettra de la découvrir. Il est donc important d'en prendre conscience.

Il existe de nombreuses équivalences à l'hypothèse de Riemann. Elles pullulent. Et chacun s'y intéresse d'une manière ou d'une autre. Pour moi, ce sont des curiosités, car toute équivalence est intéressante, mais si on utilise ces équivalences pour affirmer quelque chose que j'ignore, alors c'est passionnant. Cependant, aucune de ces équivalences n'a abouti à des applications que la théorie standard n'offre pas déjà. Je ne les trouve donc pas particulièrement intéressantes. Mais permettez-moi de vous en présenter une, car je me demandais, en préparant ce texte, comment expliquer l'hypothèse de Riemann le plus rapidement possible au grand public.

J'ai donc dû supposer que la personne savait ce qu'est une fonction analytique complexe. Bon, passons. Elle doit simplement savoir ce qu'est un nombre premier. Une des équivalences classiques est la suivante : si l'on prend $\lambda(n) = (-1)^{\Omega(n)}$, avec $\Omega(n)$ le nombre total de facteurs premiers de n, alors $\lambda(n) = \pm 1$. On se demande alors : "Est-ce que la valeur $\sum_{n \leq x} \lambda(n) = \mathrm{o}(x)$ lorsque x tend vers l'infini."

Il est donc très facile de voir que la somme des valeurs de $\lambda(n)$ pour n jusqu'à x, si l'on fait la moyenne de ces nombres (les ± 1) et qu'on la divise par x, tend vers 1, ce qui est parfaitement équivalent au théorème des nombres premiers (TNP). C'est tautologiquement presque équivalent au théorème des nombres premiers. L'hypothèse de Riemann quantifie ce résultat : cette somme s'annule jusqu'à $\sqrt{x}$ si l'on introduit systématiquement le coefficient de sécurité ε. $\sum_{n \leq x} \lambda(n) = \mathrm{O}_\varepsilon\left(x^{1/2+\varepsilon}\right)$, $\varepsilon > 0$, c'est équivalent à l'hypothèse de Riemann.

[Il rit au sujet du ε filet de sécurité.]

Bien que des démonstrations élémentaires du premier théorème aient été trouvées et soient bien documentées, une démonstration que j'ai toujours rêvé de voir a récemment été découverte par Richter et McNamara en 2021. Le théorème des nombres premiers semble donc pouvoir être démontré de

manière élémentaire, mais ces méthodes ne permettent aucune quantification. En revanche, c'est probablement la manière la plus simple d'énoncer l'hypothèse de Riemann pour que n'importe qui puisse la comprendre maintenant, sans connaître l'analyse complexe.

Et il semble que ce soit probablement vrai, car ces nombres sont aléatoires, si je comprends bien. Mais démontrer qu'une grandeur explicite est aléatoire est l'une des choses les plus difficiles en mathématiques. Si je vous disais : "Prouvez que π est normal", vous me prendriez pour un fou. Personne ne va essayer de prouver que π est normal. C'est tout simplement trop difficile pour l'être humain. Donc, lorsqu'on a une grandeur parfaitement explicite et qu'on veut montrer qu'elle se comporte comme une grandeur aléatoire, c'est un défi, et c'est l'une des raisons pour lesquelles ce problème est si difficile. Bien. J'ai mentionné la linéarisation qui s'est produite de manière remarquable dans le cas du corps de fonctions, et je mentionnerai également le théorème de Hilbert-Pólya, que vous voyez. Donc, je pense que Hilbert, d'après Odlyzko, a reçu une lettre de Pólya qui confirmait cela. Il suggérait qu'il existe peut-être une interprétation des zéros où l'on a un opérateur auto-adjoint, et ce sont ces zéros qui se trouvent sur la droite. Je trouve ça absurde. Enfin, c'est bien beau si vous le pensez, mais ça n'a jamais été prouvé comme ça, et je trouve que c'est chercher la petite bête.

D'un autre côté, je ne rejetterais pas la linéarisation car il existe des preuves convaincantes que les zéros se comportent comme des valeurs propres, si tant est que cela existe. Il y a eu cette rencontre remarquable entre Dyson et Montgomery en 1972 à l'Institut, qui a abouti à l'affirmation suivante, désormais vérifiée et comprise numériquement et phénoménologiquement, et qui trouve de nombreuses analogies. Cette affirmation est la suivante : si l'on observe l'espacement entre les zéros de la fonction zêta de Riemann... Donc, bien sûr, si une linéarisation était possible, une forme d'algèbre linéaire ou une linéarisation du problème constituerait une première étape. La seconde étape consisterait peut-être à comprendre pourquoi les zéros se trouvent sur la droite. Mais il y a ici quelque chose qui montre qu'il y a une auto-adjonction, au moins statistiquement. Et c'est ce qui suit. Si j'observe les zéros et que nous les calculons (Odlyzko les calcule aux alentours de 10 puissance 20 et il a calculé également 70 millions de relation de voisinage entre zéros), et sachant que la densité est donnée en $O(\log t)$, alors, si je veux que l'espacement soit approximativement égal à l'espacement moyen de un, et que j'observe ces nombres, et par exemple les espacements consécutifs, les statistiques d'espacement local, suivent les lois de la théorie des matrices aléatoires, ce qu'on appelle l'ensemble unitaire gaussien (GUE), en la variable t. Permettez-moi de vous montrer une image. Il s'agit de l'espacement consécutif des zéros. Ce sont les zéros tels que calculés par Odlyzko et la courbe ici représente ce que donnerait la théorie des matrices aléatoires, ce que donnerait une matrice d'émission aléatoire.

Cette courbe n'est pas élémentaire. C'est une courbe de Painlevé IV. D'accord. Elle est donnée. En fait, Wigner n'a pas pu la calculer, il a été aidé par Gaudin. Cette courbe correspond à un certain déterminant de Fredholm, puis une équation différentielle ordinaire non linéaire. Bref, on connaît théoriquement la courbe, et les prédictions de matrices aléatoires n'ont jamais aussi bien correspondu à quoi que ce soit. Les zéros se repoussent. C'est ce qui explique que cette équation soit du second ordre et ait ce profil. Donc, les zéros se comportent comme les valeurs propres de la matrice d'émission aléatoire, et on ne peut pas ignorer ça, n'est-ce pas ? C'est une observation statistique. Cela me donne une piste pour une interprétation linéaire. Et c'est ce qui motive de nombreuses personnes à réfléchir à ce problème.

Ce phénomène a également été vérifié pour les familles dans les corps de fonctions, où tout est clair. Katz et moi avons pu expliquer l'origine de cette théorie des matrices aléatoires, à savoir les limites d'échelle des groupes. Ainsi, dans les corps de fonctions, nous comprenons très bien cela, mais dans les corps de nombres, il y a certains indices laissent penser que quelque chose comme ça pourrait être vrai. Je voudrais maintenant parler de mon point de vue. Il existe de très nombreuses approches de l'hypothèse de Riemann. Je n'en ai jamais vu une qui soit vraiment convaincante. J'y reviendrai plus tard, lorsque j'aborderai l'intelligence artificielle. Mais, d'après mon expérience, je ne dirais pas que l'hypothèse de Riemann soit pertinente. Je ne veux pas limiter les connaissances et les travaux d'autrui, mais je n'ai jamais rien vu qui soit vraiment convaincant à ce jour. Il y a une idée qui me tient particulièrement à cœur, c'est celle de Paul Cohen. Je suis venu d'Afrique du Sud pour étudier la théorie des ensembles avec Paul Cohen. J'avais étudié le forçage (forcing) et je suis arrivé, je lui ai dit que je souhaitais étudier le forçage (forcing) avec lui et il a répondu : "Eh bien, cela ne m'intéresse pas pour le moment."

Il s'intéressait alors à l'hypothèse de Riemann. Il se trouve que je savais de quoi il s'agissait. J'ai dit : "Très bien, j'ai fait du chemin pour venir jusqu'à lui. Je vais simplement changer de centre d'intérêt."

[Rires]

Et puis, il a immédiatement dit : "Prenez cette formule au sujet des classes d'adèle", je ne savais pas de quoi il parlait. Prenez ce truc et mélangez-le avec tout et n'importe quoi." Il avait cette idée qu'Alain Connes a reprise plus tard dans les années 90, sur laquelle il a beaucoup écrit depuis, et qui a été formalisée par Meyer.

Il s'agit d'une interprétation spectrale des zéros. Je tiens donc à préciser qu'il s'agit bien d'une interprétation spectrale. Est-elle utile ? C'est une autre question. Mais, comme je l'ai déjà mentionné, dans le domaine des fonctions, on ne trouve pas de zéros sur la droite des nombres complexes de partie réelle un demi.

C'est donc une idée très intéressante. Elle combine les structures additive et multiplicative. Bien que, à ma connaissance, elle n'ait pas encore fonctionné, elle est séduisante. Considérons l'espace suivant, appelé espace des classes d'adèles. Il s'agit d'un produit infini a_1, a_2, a_3, où a_i est un nombre réel, a_2 un nombre 2-adique, a_3 un nombre 3-adique, et ainsi de suite. a_p est un entier p-adique à partir d'un certain point. On applique à ce produit la topologie dite du produit restreint. On forme ainsi un espace topologique. On procède de même avec les éléments inversibles, c'est-à-dire les éléments non nuls qui, à partir d'un certain point, valent un. On applique également la topologie du produit restreint. Ces espaces sont appelés vecteurs de valuation par Tate. Ils offrent une nouvelle interprétation des travaux de Hecke que j'ai mentionnés, qui est loin d'être triviale. Hecke et Tate l'ont magnifiquement conceptualisée. Ils utilisent une sommation de Poisson sur ces groupes d'adèles pour effectuer la partie additive. On considère $\mathbb{A}$ sur $\mathbb{Q}$, qui est un espace compact. $\mathbb{Q}$ est un sous-groupe discret plongé diagonalement dans ces adèles. Et les adèles, le quotient, ne sont pas tout à fait compactes, mais elles forment un sous-groupe discret bien compris. On peut procéder soit de manière additive, soit de manière multiplicative. En procédant de manière additive, on obtient l'équation fonctionnelle. En procédant de manière multiplicative, on obtient le produit eulérien

grâce au théorème de Fubini. C'est très élégant. Et on retrouve alors l'équation fonctionnelle de prolongement analytique.

L'idée de Connes est donc de prendre un objet étrange, l'adèle, dont la topologie est très différente de celle des idéaux, et de le diviser par $\mathbb{Q}^*$. On obtient ainsi un quotient très particulier. Ensuite, on considère l'action de la multiplication sur l'addition : $X \to X \times Y$, où Y est un idéal. On examine cette action. Et formellement, il répétait : "Si vous prenez la trace de ceci, vous obtiendrez la formule explicite, ce qu'on appelle la formule explicite vague".

Et c'est vrai. On peut en tirer une explication logique. C'est ce qu'a fait Connes. C'est ce que fait parfaitement Meyer.

Il faut construire des espaces vectoriels topologiques complexes pour obtenir des espaces de fonctions sur lesquels calculer cette trace. Rien d'auto-adjoint ici. Les espaces de fonctions sont des espaces vectoriels topologiques analogues à ceux utilisés précédemment. En décomposant cette action, on obtient la formule explicite de Riemann, ou de Riemann-Weil. De plus, la décomposition de cette action a pour valeurs propres les zéros de toutes les fonctions.

Personne ne prétend qu'ils se situent à mi-chemin, mais il s'agit d'une interprétation spectrale, et elle est assurément intéressante. Connes a beaucoup écrit à ce sujet depuis. Même récemment, un article d'arxiv présente ses idées, et fait le point sur ses réflexions. Et le plus fascinant, ce qui m'a vraiment marqué, c'est cette lettre remarquable qu'Alain Connes adresse au professeur Bernhard Riemann pour lui exposer ses idées.

[Rires]

Et je vous encourage vivement à le lire. Cet article est tout simplement magnifiquement écrit.

Je n'aurais jamais eu cette idée, mais maintenant qu'Alain Connes a écrit une lettre à Bernhard Riemann, je me sens obligé de lui en écrire une aussi.

[Rires]

Ce n'est pas tous les jours qu'on écrit une lettre au Professeur Riemann, et d'autres vont vouloir le faire aussi ! Bien.

Je voudrais terminer en expliquant ce qui, à mon avis, constitue une piste de recherche. La question est donc de savoir dans quelle mesure nous avons exploré cette hypothèse de Riemann. Nous avons examiné les zéros de degré élevé pour zêta. Nous avons examiné les zéros d'espèces de degré inférieur. Où devrions-nous chercher pour vraiment la tester ? Et le véritable test se situe, à mon avis, à la limite ultime, où nous ne l'avons pas vraiment testée. Certains l'ont un peu fait, mais pas dans le sens que je vais donner. Alors, nous laissons le degré du corps des nombres varier, et, et c'est la première fois, je vais également autoriser les fonctions L des formes automorphes qui sont définies sur des groupes de plus en plus grands. Et je vous rappelle que la complexité est toujours une fonction logarithmique du conducteur.

Et l'hypothèse de Riemann, telle qu'elle est utilisée dans nombre des applications étonnantes que je vous ai présentées, est que sa ramification est très fortement contrôlée si l'on connaît les zéros sur la droite critique (les zéros complexes de la fonction ζ de Riemann et qui sont de partie réelle $\frac{1}{2}$).

À tel point que si l'on a une suite de corps de nombres algébriques dont le discriminant est N_K, on obtient de meilleures bornes inférieures pour le discriminant en fonction de l'extension du degré que celles obtenues par la géométrie des nombres de Minkowski. En fait, ces bornes sont si précises qu'elles semblent violer l'hypothèse de Riemann dans certains cas. Et chaque fois qu'une violation est constatée, on vérifie et on constate : "Bien sûr, il y a eu une erreur". Riemann n'avait pas tort, mais il existe ces tours étonnantes composées de très peu d'extensions non ramifiées, appelées tours de Golod-Shafarevich. Et elles sont très proches de violer les inégalités que l'hypothèse de Riemann implique. C'est donc un excellent test. J'ai vu une interview de Serre où il disait : "Oui, il a fait quelques essais et cela contredit le théorème de Riemann." Et il a réalisé : "Bon, je ne vais pas remettre en question l'hypothèse de Riemann. Mais peut-être devriez-vous le faire". C'est une limite que nous n'avons, à ma connaissance, jamais testée numériquement.

Les exemples d'Elkies n'ont pas de contre-exemple. Je voudrais vous indiquer où ils pourraient se trouver, mais je ne crois pas qu'ils existeront. On appelle cela une ramification contrôlée, et je veux dire, à la limite, que la ramification est contrôlée par Riemann. Très fortement contrôlée par lui. Or, il existe des formes automorphes transcendantes. Mais, à mon avis, elles sont tout aussi valables que n'importe quelle autre forme de notre espèce. D'autres pourraient dire le contraire, mais je maintiens qu'elles le sont. On les appelle formes de Maass. Ce sont des formes automorphes non ramifiées. Leurs fonctions L sont donc non ramifiées partout. Vous pourriez dire : "Mon Dieu, c'est déjà une contradiction, car il est impossible d'avoir quelque chose qui n'est ramifié nulle part."

Ces éléments sont omniprésents, sans ramifications. Leur existence est déjà très subtile. Ils existent simplement, ils sont les briques élémentaires. Ils existent. On peut démontrer leur existence en basse dimension. En haute dimension, nous n'avons jamais vraiment exploré cette question. C'est précisément ce que je souhaite explorer. Et ils sont liés à la place archimédienne. Ainsi, tout ce qui se trouve dans ce corps de fonctions où nous appréhendons les choses, ce corps de fonctions ne possède pas de place archimédienne. C'est pourquoi il s'agit d'algèbre. C'est la fonction, la place archimédienne, qui est à l'origine de toutes nos difficultés.

Et ici, on a la simple existence de ces formes, qui sont partout non ramifiées. Donc, bien sûr, si l'on utilise la théorie de Riemann, je ne cesse de répéter qu'il n'existe qu'une seule définition de la complexité d'une fonction L.

Il s'agit du nombre de zéros localement. En effet, cela correspond au degré de la fonction entière. Combien de zéros possède-t-elle localement ? Si l'on considère la fonction zêta de Dedekind complète, et si N est fixé, tout provient du conducteur, comme je l'expliquais. Ici, il n'y a pas de conducteur.

Il est partout non ramifié. Il provient donc nécessairement de la place archimédienne, et c'est bien le cas. Ces places archimédiennes, c'est-à-dire les valeurs propres des opérateurs différentiels et

elliptiques, sont transcendantes sur ce bel espace localement symétrique des matrices $n \times n$ divisé par $\mathrm{SL}(n, \mathbb{Z})$, lui-même divisé par le compact maximal. Ce sont là des objets partout non ramifiés, et ils possèdent des fonctions L.

Et ces fonctions L sont censées satisfaire aux hypothèses de Riemann. Et ces hypothèses n'ont jamais été testées. C'est ce que j'aimerais vraiment voir testé, et j'y pense depuis un certain temps. Cela laisse supposer que ces choses sont très rares.

Ces objets ont une faible énergie. Cela signifie aussi que, selon Riemann, la concentration de Lévy, en haute dimension, implique que les fonctions présentant une certaine régularité se concentrent très nettement autour de la moyenne. Or, selon Riemann, cette concentration est si forte qu'on ne verrait que très peu d'objets de faible complexité si ses propriétés sont exactes. S'il y avait trop de formes de Maass, les propriétés de Riemann seraient invalidées. Pour ma part, concernant l'hypothèse de Riemann généralisée (GRH), j'ai été très prudent dans l'étude des fonctions zêta de Dedekind, et quelqu'un va me poser une question sur les fonctions L motiviques dans un instant.

Ces choses transcendantes ne sont pas motivées par des raisons intrinsèques. Pourtant, elles sont là, elles font partie de notre monde, elles ne diffèrent en rien de ce que nous savons des autres. Donc, pour moi, l'hypothèse de Riemann généralisée doit également s'appliquer à elles, si elle est vraie.

Et si ce n'était pas vrai pour certaines d'entre elles... Alors, c'est une enquête que j'ai vraiment hâte de voir. Et si ces affirmations étaient fausses pour les fonctions zêta de Dedekind, ou pour les fonctions motiviques, mais vraies pour celles-ci, cela expliquerait peut-être la complexité du problème. En effet, les formes automorphes sont incontournables dans les corps des nombres. Elles apparaissent dès l'écriture de la formule de la trace ; ce sont leurs éléments constitutifs. J'aimerais donc approfondir cette question. Et il y a un élément essentiel à prendre en compte : l'intelligence artificielle. Quel sera son rôle ?

Pour ma part, elle m'apporte déjà de nombreuses solutions à ce problème.

[Rires]

Mais il serait intéressant que l'ia explore certaines de ces limites pour lesquelles nous avons moins confiance en la démonstration. Quoi qu'il en soit, j'espère vous avoir convaincus que lorsqu'on ajoute G à RH, on est confronté à un problème vraiment intéressant.

Merci.