Que fait un mathématicien et pourquoi ? de Serge Lang

Alors, dans cette conférence, je pense que je vais parler de certaines choses en général pendant dix minutes, et après, on essaiera de faire des mathématiques ensemble. L'exposé sera comme le dit le titre : "Que fait un mathématicien (en mathématiques pures) et pourquoi ?"

C'est très difficile d'expliquer "pourquoi" de façon générale, et aussi ce que nous faisons, de façon générale. Par exemple, "mathématiques" est un mot qui est utilisé pour beaucoup d'activités qui n'ont pas grand-chose à voir les unes avec les autres. Je suis sûr que le mot signifie des choses très différentes pour différentes personnes. Par exemple, vous, Madame [*Serge Lang désigne une dame dans le public*], que signifient pour vous "les mathématiques" ?

La dame. L'abstraction des nombres, la manipulation des nombres.

Serge Lang. En fait, on peut faire des mathématiques sans utiliser de nombres du tout : comme en géométrie ou en mathématiques spatiales. C'est vrai que pour vous donner un exemple de mathématiques, comme je le ferai un peu plus tard, j'utiliserai des nombres, mais dans un contexte qui, je pense, sera différent de celui auquel vous pensez. Et pour vous, monsieur, qu'est-ce que ça veut dire "mathématiques" ?

Gentleman. La manipulation des structures.

Serge Lang. Oui, mais lesquelles ? Il y a beaucoup de structures qui ne sont pas mathématiques. Les mathématiques ne sont pas seulement une question de structures. Par exemple, quand on fait de la physique, on manipule aussi certaines structures. En fait, le mot "mathématiques" est utilisé dans de nombreux contextes différents. Vous avez les mathématiques telles qu'elles se font au primaire ou au secondaire. Vous avez les mathématiques informatiques, appliquées aux problèmes de communications. Si vous aimez la physique ou la chimie, vous utilisez les mathématiques pour décrire le monde empirique. Mais ce dont je veux parler aujourd'hui, c'est de ce que j'appellerai les "mathématiques pures", celles qui se font d'un point de vue purement esthétique. Faire des mathématiques comme ça est très différent d'étudier le monde empirique. C'est différent de décrire ou de classer le monde empirique au moyen de modèles mathématiques. Un scientifique expérimental fait un choix parmi de nombreux modèles possibles, pour trouver ceux qui correspondent au monde empirique, le monde des expériences, en essayant de trouver un système pour le monde. Il y a beaucoup de mathématiques pures qui ne sont pas utilisées dans l'étude du monde empirique, et qui sont considérées uniquement pour leur beauté. Et cela a toujours été le cas, depuis des siècles, depuis qu'il y a eu des civilisations - arabe, hindoue, peu importe. Les Grecs faisaient des mathématiques pour la beauté[1].

Traduction : Denise Vella-Chemla, assistée de Google translate, février 2023.

[1]Ce qui n'exclut pas qu'ils aient aussi fait des mathématiques ayant des applications pratiques. Tout le monde s'accorde à inclure la physique, la chimie, la biologie, sous la rubrique générale de "science". Décider si les "mathématiques pures" telles que je les ai décrites doivent également être placées sous cette rubrique est une question de terminologie dont je ne souhaite pas parler maintenant.

Il est vrai que certaines parties des mathématiques ont leur source dans le monde empirique, mais une grande partie des mathématiques se fait indépendamment de ces sources. Ce point de vue a été exprimé par d'autres mathématiciens, et je veux vous lire quelque chose écrit par d'autres mathématiciens, par exemple sur la relation entre le fait de faire des mathématiques et le fait qu'elles aient des applications.

Jacobi, qui était un mathématicien du XIX$^{\text{ième}}$ siècle, écrivait dans une lettre à Legendre[2] :

> J'ai lu avec plaisir le rapport de M. Poisson sur mon travail, et pense pouvoir en être très satisfait... mais M. Poisson n'aurait pas dû reproduire une phrase assez maladroite de M. Fourier, qui nous reprochait à Abel et à moi de ne pas avoir préféré travailler sur les flux de chaleur. Il est vrai que M. Fourier pensait que le but principal des mathématiques était leur utilité publique et leur utilisation dans l'explication des phénomènes naturels. Un philosophe comme lui aurait dû savoir que le seul but de la Science est l'honneur de l'esprit humain, et qu'à ce titre, une question de théorie des nombres vaut une question concernant le système du monde.

Dans un article paru dans la collection "Les grands Courants de la pensée mathématique", dirigée par F. Le Lionnais en 1948, André Weil (qui est l'un des grands mathématiciens de ce siècle), cite Jacobi dans le contexte suivant :

> Mais si, comme Panurge, nous posons à l'oracle des questions trop indiscrètes, l'Oracle nous répondra comme à Panurge : Tchin ! Conseil auquel le mathématicien obéit volontiers, satisfait qu'il est de croire étancher sa soif aux sources mêmes du savoir, satisfait qu'elles jaillissent toujours aussi pures et abondantes, alors que d'autres doivent recourir aux sentiers boueux d'une actualité sordide. Que si on lui fait reproche de la superbe de son attitude, si on le somme de s'engager, si on demande pourquoi il s'obstine en ces hauts glaciers ou nul de ses congénères ne peut le suivre, il répond avec Jacobi : "Pour l'honneur de l'esprit humain !"

Bon, c'est de la littérature. C'est aussi un style pompeux, qui ne reflète pas fidèlement la pensée de Jacobi. Se référer à d'autres, qui doivent recourir aux voies boueuses d'une actualité sordide , ce n'est pas exactement la même chose que de dire qu'"une question de théorie des nombres vaut une question concernant le système du monde". Weil, ailleurs, a décrit d'une autre manière ses propres raisons de faire des mathématiques. Dans une interview publiée dans "Pour la Science" (novembre 1979, la version française du "Scientific American") il dit[3] :

---

[2]Non datée, timbrée en date du 2 juillet 1830, *Collected Works of Jacobi*, Vol. 1. p. 454.

[3]Lors d'une conférence au Congrès international de mathématiques à Helsinki, 1976, reproduite dans son Collected Works Vol. III, Weil avait déjà effleuré ce thème : "Que l'humanité soit stimulée par la perspective d'une renommée éternelle vers des réalisations toujours plus élevées est bien sûr un thème classique, hérité de l'antiquité ; nous semblons y être devenus moins sensibles que nos ancêtres, bien qu'une telle sensibilité n'ait peut-être pas épuisé toute sa force."

> Selon Plutarque, c'est un noble idéal de travailler à rendre son nom immortel. Depuis mon plus jeune âge, j'espèrais que mon travail aurait une certaine place dans l'histoire des mathématiques. N'est-ce pas une motivation aussi noble que d'essayer d'obtenir un prix Nobel ?

Donc, ce n'est pas tant pour l'honneur de l'esprit humain que pour l'honneur de son propre esprit. Je pense plutôt qu'on fait des mathématiques parce qu'on aime faire ce genre de choses, et aussi, beaucoup plus naturellement, parce que quand on a du talent pour quelque chose, généralement, on n'a pas de talent pour faire autre chose, et on fait ce pour quoi on a du talent, si on a la chance d'en avoir. Je dois aussi ajouter que je fais des mathématiques parce que c'est difficile, et c'est un très beau défi pour l'esprit. Je fais des mathématiques pour me prouver que je suis capable de relever ce défi, et de le gagner.

Donc on fait des mathématiques, mais cela ne veut pas dire que les gens sont mécontents si les mathématiques qu'ils font sont suffisamment bonnes pour figurer dans les livres d'histoire. Bien sûr, tous les mathématiciens que je connais sont parfaitement heureux lorsqu'ils font des mathématiques à ce niveau. Ils sont heureux des honneurs qu'ils peuvent en tirer et ils sont heureux de laisser un nom en mathématiques. Mais je ne dirais pas qu'qu'ils se livrent aux mathématiques, qu'elles soient pures ou appliquées, spécifiquement dans ce but.

Si je vous demandais ce que signifie la musique pour vous, répondriez-vous : "c'est la manipulation des notes" ? Quand on fait des mathématiques pures, on fait tout autre chose que "manipuler". Pour clarifier les raisons pour lesquelles les gens font des mathématiques pures, d'un point de vue esthétique, je dois vous donner un exemple. Mais pour vous montrer ce que sont les mathématiques, si vous n'êtes pas vous-même mathématicien, j'ai des difficultés qui sont analogues à celles que j'aurais si j'essayais de dire à un Japonais, ou à un Hindou, qui n'a jamais eu de contact avec la civilisation occidentale, ce qu'est une symphonie de Beethoven ou une ballade de Chopin, c'est comme ça. Si vous prenez quelqu'un de totalement étranger à la culture occidentale, et sourd de surcroît, comment lui faire comprendre à quoi ressemble une symphonie de Beethoven ou une ballade de Chopin ? C'est impossible. Même si la personne n'est pas sourde, et est capable d'écouter, c'est quand-même presque impossible si la personne n'a aucun lien avec la culture occidentale, si la personne n'a pas entendu ces morceaux plusieurs fois. La musique occidentale est trop différente de la musique japonaise, ou de la musique hindoue ; c'est joué sur des instruments différents, avec des orchestrations différentes, avec des rythmes différents, etc. Il y a donc une grande difficulté à faire comprendre à quelqu'un de quoi il s'agit. Et à l'inverse, les concerts de Koto ou de Sitar ici à Paris ne se produisent pas si souvent, et ne touchent qu'un petit nombre de personnes.

Par ailleurs, il y a une difficulté qui se présente dans toutes les situations esthétiques : quelqu'un peut aimer une chose et pas une autre. Il y a des gens qui aiment Brahms et qui n'aiment pas Bach ; qui aiment Bach et n'aiment pas Chopin ; qui aiment Chopin et n'aiment pas Dowland (un compositeur anglais de pièces et de chansons pour luth à l'époque de Shakespeare).

Comment allez-vous faire comprendre à quelqu'un ce qu'est une chanson de Dowland, ou une ballade de Chopin, sans la lui faire écouter ? C'est impossible. Et c'est beaucoup plus facile de vous faire écouter de la musique que de vous faire faire des mathématiques, car pour écouter de la musique vous êtes dans un état passif. Vous êtes pris par l'esthétique musicale et vous laissez le compositeur et l'interprète jouer un rôle actif. Mais pour faire des mathématiques, vous avez besoin d'un degré de concentration beaucoup plus élevé et d'un effort personnel. De plus, pour vous faire faire des mathématiques, je dois trouver un sujet suffisamment approfondi, qui soit un vrai sujet de mathématiques, reconnu comme tel par les mathématiciens. Je ne peux pas tricher. Mais encore faut-il que je sois capable d'expliquer les choses avec des mots que tout le monde comprendra. Il n'y a que très peu de sujets de ce type ; et comme je dois faire un choix, peut-être que certains vont aimer et d'autres pas.

Le sujet doit être suffisamment approfondi pour vous faire comprendre pourquoi certaines personnes feront des mathématiques toute leur vie, et négligeront peut-être leurs femmes, ou maris, ou enfants, ou Dieu sait quoi. D'ailleurs, laissez-moi vous lire deux phrases extraites d'une lettre de Legendre à Jacobi[4] qui venait de se marier assez tard :

> Félicitations pour avoir rencontré une jeune femme dont, après une *assez longue* expérience, vous avez décidé qu'elle vous rendrait heureux pour toujours. Vous étiez en âge de vous marier. Un homme destiné à passer beaucoup de temps à travailler dans son bureau a besoin d'une compagne qui s'occupera de tous les détails du ménage et évitera à son mari d'avoir à se soucier de ces petits objets quotidiens qu'un homme n'est pas capable de gérer.

La phrase sonne drôlement, surtout à notre époque “libérée” .

Bon, cela fait une dizaine de minutes que je parle de généralités, ça suffit. Faisons maintenant des mathématiques. Dans le choix du sujet, je suis très restreint, et j'ai été presque obligé de choisir un sujet ayant à voir avec les nombres. Le sujet concerne les nombres premiers.

Qui a entendu parler des nombres premiers ? [*Réactions et réponses variées dans le public.*] Presque tout le monde, ou personne ? Levez la main. Qui n'a jamais entendu parler des nombres premiers ? [*Presque tout le monde dans le public a entendu parler des nombres premiers et sait approximativement ce que le mot signifie.*] Par exemple, vous, Madame, quels sont les nombres premiers ?

UNE DAME. 1, 3, 5, 7...

SERGE LANG. Non ! Ce sont les nombres impairs. Je veux dire les nombres premiers, c'est-à-dire 2, 3, 5, 7, 11, 13. Quel est le suivant ?

LA DAME. 17, 19...

SERGE LANG. Très bien, vous avez compris ce qu'est un nombre premier.

LA DAME. J'ai oublié 2.

SERGE LANG. Oui, vous avez raison. J'ai mal écouté. Mais c'est une convention générale que 1

[4]Écrite le 30 juin 1832, loc. cit p. 460.

n'est pas un nombre premier. Donc dire qu'un nombre est premier signifie qu'il est au moins égal à 2, et qu'il n'est divisible que par lui-même et par 1.

Le nombre 4 n'est pas premier parce que $4 = 2 \times 2$.
6 n'est pas premier parce que $6 = 2 \times 3$.
8 n'est pas premier parce que $8 = 2 \times 4$.
9 n'est pas premier parce que $9 = 3 \times 3$.

Et ainsi de suite. Quant aux nombres premiers, nous les avons déjà répertoriés jusqu'à 19. Après cela, nous trouvons 23, 29, 31, 37...

Maintenant, voici une question sur les nombres premiers. Y en a-t-il une infinité ou n'y en a-t-il qu'un nombre fini ?

La dame. Oui, une infinité.

Serge Lang. Très bien. Comment le prouver ?

Lady. Je ne sais pas.

Serge Lang. [*Désignant un jeune homme.*] Vous, savez-vous comment le démontrer ?

Le jeune homme. Les mathématiciens en ont trouvé des millions.

Serge Lang. Non, je ne veux pas dire en trouver des millions, je veux dire prouver que la suite des nombres premiers ne s'arrête pas.

[*Brouhaha dans le public, diverses preuves sont suggérées par certaines personnes.*]

Serge Lang. Êtes-vous un mathématicien ? Oui ? OK, je demande aux mathématiciens dans le public de ne rien dire. Je ne parle pas ici pour eux. [*Rires.*] Sinon, c'est de la triche.

Je dis qu'il existe une infinité de nombres premiers. Cela signifie que la suite des nombres premiers ne s'arrête pas. Et je vais le prouver, car il y a une preuve très simple, qui est aussi très ancienne, et qui est attribuée à Euclide. Voici comment les Grecs procédaient.

Commençons par une remarque. Prenez n'importe quel nombre entier, c'est-à-dire un nombre entier, par exemple 38, que je peux écrire sous la forme 2×19 où 2 et 19 sont des nombres premiers. Alors 38 est un produit de ces deux nombres premiers. Si je prends 144, alors je peux écrire

$$144 = 12 \times 12 = 3 \cdot 4 \cdot 3 \cdot 4 = 3 \cdot 2 \cdot 2 \cdot 3 \cdot 2 \cdot 2.$$

Encore une fois, c'est un produit de nombres premiers, et j'en ai écrit quelques-uns plusieurs fois. Dans tous les cas, je peux toujours exprimer un entier comme un produit de nombres premiers. Parce que si on me donne un entier N plus grand que 2, alors soit N est déjà premier, soit N peut être exprimé comme un produit de deux nombres plus petits Chacun de ces nombres plus petits est soit premier, soit peut être exprimé comme un produit de nombres encore plus petits. Si vous continuez ce processus, vous vous retrouvez avec des nombres premiers.

Donnons maintenant la preuve des Grecs qu'il existe une infinité de nombres premiers. Nous allons voir que si nous faisons la liste des nombres premiers

$$2, 3, 5, 7, 11, 13, 17, \ldots, P$$

allant de 2 à P, alors on peut toujours trouver un autre nombre premier qui n'est pas dans cette liste. Nous procédons comme suit. Je prends le produit de tous les nombres premiers de la liste. Cela me donne un certain nombre, auquel j'ajoute 1. Soit N ce nouveau nombre. Ainsi nous avons

$$N \;=\; (2 \cdot 3 \cdot 5 \cdot 7 \cdot \ldots \cdot P) + 1.$$

Alors soit N est premier, soit N n'est pas premier. Si N est premier, il n'est égal à aucun de ceux que nous avons listés de 2 à P. et nous venons donc de construire un nouveau nombre premier. Si N n'est pas premier, alors nous pouvons exprimer N comme un produit de nombres premiers. En particulier, on peut écrire $N = qN'$, où q est un nombre premier divisant N. q peut-il être égal à l'un des nombres premiers compris entre 2 et P ?

Les gens dans le public. C'en est un nouveau.

Serge Lang. Pourquoi ? Choisissons quelqu'un. Vous, le jeune homme là-bas.

Le jeune homme. Divisé par les autres, les divisions ne tombent pas juste.

Serge Lang. C'est vrai, si on divise N par q alors il n'y a pas de reste ; mais si on divise N par l'un des nombres premiers entre 2 et P, il reste 1. On découvre alors un nouveau nombre premier qui n'était pas dans la liste. Cela signifie que vous ne pouvez pas constituer une liste finie de tous les nombres premiers, et cela conclut la preuve.

Maintenant, comment les nombres premiers sont-ils répartis entre tous les nombres ? Y a-t-il une règle qui vous dit combien il y en a ? Comment sont-ils répartis entre tous les entiers ?

Un homme. Il y en a des millions.

Serge Lang. Bien sûr, il y en a aussi des milliards, mais ce n'est pas la question que je pose. Par exemple, combien y a-t-il de nombres premiers inférieurs à 10 000, environ ? Pouvez-vous répondre à cela ?

Quelqu'un. Vous pouvez les compter.

Serge Lang. C'est vrai, mais si je disais jusqu'à 1 000 000, ou jusqu'à un nombre arbitraire x ? Posons la question autrement. Existe-t-il une formule qui donne le nombre de nombres premiers inférieur à x ? Qui dit oui ? Une formule approximative. [*Hésitations dans le public, les gens commentent simultanément.*] D'accord, c'est compliqué. Il faudrait que je décrive plus précisément les nombres premiers. N'abordons pas cela tout de suite. Permettez-moi de soulever d'autres types de questions sur les nombres premiers. En particulier, ce qu'on appelle les nombres premiers jumeaux.

Par exemple :

3 et 5 diffèrent de 2 ;
5 et 7 diffèrent de 2 ;
11 et 13 diffèrent de 2 ;
17 et 19 diffèrent de 2 ;
29 et 31 également.

On dit "nombres premiers jumeaux" pour des raisons évidentes.

Maintenant, y a-t-il une infinité de nombres premiers comme ça, une infinité de nombres premiers jumeaux ?

Qui dit oui ? Levez la main. [*Quelques mains se lèvent.*]

Qui dit non ? [*D'autres mains se lèvent.*]

Qui garde un silence prudent ? [*De nombreuses mains se lèvent. Sourires.*]

Qui pense que c'est une question intéressante ?

Le public. Oui, c'est intéressant. [*Plusieurs personnes parlent en même temps.*]

Serge Lang. Bien sûr, vous pouvez aimer ou ne pas aimer cela. En fait, les mathématiciens pensent en général que c'est un problème intéressant. Bon, vous voyez, c'est un problème. Personne ne sait la réponse. Si vous trouvez la réponse, vous serez une sorte de Plutarque, vous entrerez dans l'Histoire des mathématiques. En fait, on pense qu'il y en a un nombre infini, et on peut même faire mieux que ça. On peut essayer de comprendre pourquoi il pourrait exister une infinité de nombres premiers jumeaux.

Quelqu'un. Y a t-il un nombre infini de triplets ?

Serge Lang. La question est intéressante. Pouvez-vous y répondre directement ?

Plusieurs voix dans le public. Oui, je pense qu'il y en a une infinité.

Serge Lang. Voyons ! Essayons d'ajouter un nombre aux couples de nombres premiers que nous avons déjà.

3	5	7
5	7	9
11	13	15
17	19	21
29	31	33
etc.		

Quelqu'un. 21 n'est pas premier.

Serge Lang. Oui. Que remarquez-vous avec vos triplets ? Il y en a un qui contient trois nombres premiers, 3, 5, 7. Mais après ça, que se passe-t-il ? Vous ne savez pas ? Regardez attentivement : 9, 15, 21, 33...

La public. Ce sont des multiples de...

Serge Lang. Chut ! Monsieur, là-bas. [*Hésitations. Pas de réponse du Monsieur.*] Ils ont une propriété, ces nombres : ils sont tous divisibles par 3. C'est un exercice très facile, que de montrer que dans tout triplet de nombres impairs, il y a toujours un multiple de 3. Par conséquent, il ne peut pas y avoir de triplet de nombres premiers.

Le public. Excepté le premier, 3, 5, 7.

Serge Lang. Excepté le premier, bien sûr, qui contient aussi un multiple de 3, mais 3 est premier, et il n'y en a pas d'autres[5].

Revenons aux nombres premiers jumeaux, aux couples de nombres premiers si vous voulez. Essayons de comprendre pourquoi il devrait y en avoir un nombre infini. Mais avant, revenons à la question : combien y a-t-il de nombres premiers inférieurs ou égaux à x ? Une formule approximative.

OK, prenons tous les entiers jusqu'à x :

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ ...,\ x.$$

Parmi ces nombres, vous avez les nombres pairs et les nombres impairs. Que signifie qu'un nombre est premier ? Cela signifie qu'il n'est divisible que par lui-même et 1. Par conséquent, si un nombre est premier, il n'est certainement pas pair.

Le public. Sauf 2.

Serge Lang. Bien sûr, sauf 2. Maintenant, si je monte jusqu'à x, combien y a-t-il de nombres impairs ?

Plusieurs voix dans le public. La moitié d'entre eux.

[5] de multiples de 3 autres que 3 et qui soient premiers.

Serge Lang. Environ la moitié. C'est vrai, $x/2$. C'est une certaine fraction de x. Le nombre de nombres premiers inférieur ou égal à x sera une certaine fraction fois x. Et cette fraction dépendra de x. C'est cette fraction que nous cherchons à déterminer.

D'accord, donc parmi tous les entiers 1, 2, 3 jusqu'à x, il y en aura environ la moitié qui seront impairs, donc non divisibles par 2. Parmi les nombres impairs, combien ne seront pas divisibles par 3 ?

Le public. Un tiers.

Serge Lang. Non, un tiers est divisible par 3 et deux tiers ne seront pas divisibles par 3. OK ? Écrivons $2/3$ sous la forme $(1 - 1/3)$. Maintenant parmi ceux qui restent, combien ne seront pas divisibles par 5 ?

Une voix dans le public. $1 - \frac{1}{5}$.

Serge Lang. Êtes-vous mathématicien ? Oui ? Alors taisez-vous ! C'est de la triche. Ce n'est pas bien.

Parmi ceux qui restent, combien y en a-t-il qui ne soient pas divisibles par le nombre premier suivant ?

Le public. $1 - \frac{1}{7}$.

Serge Lang. Bon, et puis enfin pour trouver les nombres premiers, de quoi a-t-on besoin ? Nous avons besoin qu'ils ne soient divisibles par aucun nombre premier, de 2 à quelque part. On est donc amené à prendre le produit

$$\frac{1}{2}\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)\ldots$$

qui doit monter jusqu'où ?

Le public. Jusqu'au dernier nombre premier avant x.

Serge Lang. Oui, mais on peut faire mieux que ça. De toute façon, au pire, ce sera le produit

$$\text{produit de tous les facteurs } \left(1-\frac{1}{p}\right)$$

où p monte jusqu'à x. Ce sera approximativement la fraction de x qui donne la fraction de tous les nombres premiers.

Maintenant, en fait, je n'ai pas besoin d'aller jusqu'à x. J'ai seulement besoin d'aller jusqu'à la racine carrée de x, qu'on note $\sqrt{x}$. Parce que supposons qu'un nombre qui est plus petit que x et qui n'est pas un nombre premier, soit divisible par un nombre premier supérieur à $\sqrt{x}$. Alors il est nécessairement divisible par un nombre premier qui est plus petit que $\sqrt{x}$[6]. Par conséquent,

[6] Je donne les détails de cette affirmation. Soit N inférieur ou égal à x. Supposons que N est un produit, $N = pN'$

on peut éliminer un tel nombre quand on a rencontré le plus petit de ses facteurs premiers. Mais quand x est grand, et quand p est compris entre $\sqrt{x}$ et x, le terme $(1 - 1/p)$ est très proche de 1. On peut montrer que le produit pris sur tous les p tels que $\sqrt{x} \leq p \leq x$ est proche de $1/2$. Pour simplifier les formules, je continuerai d'écrire le produit sous la forme produit des $(1 - 1/p)$ pour tous les $p \leq x$. Pour avoir une meilleure approximation, ou l'approximation la meilleure possible, je devrais cependant multiplier le produit par une constante qui est difficile à déterminer, et qui reflète des relations qui sont plus cachées que la relation que l'on vient de décrire.

Ici je compte approximativement, et je suis amené à considérer ce produit. Il donne approximativement la fraction de x donnant le nombre de nombres premiers inférieurs ou égaux à x. Cette fraction de x est plutôt mystérieuse, mais elle donne tout de même une idée de ce qui se passe. Par exemple, cette fraction est-elle constante ? Clairement pas. Plus on avance, plus elle devient petite. Si je prends x très grand, la fraction sera petite. La vitesse à laquelle le produit devient petit n'est pas claire. Le comportement de ce produit n'est pas du tout clair. Et maintenant, je suis coincé. Je vous donnerai une réponse plus tard, mais je ne pourrai pas la prouver car cela deviendrait trop technique.

C'est compliqué d'analyser ce produit, mais quand même, nous avons fait un pas en avant en trouvant ce produit, qui nous donne une certaine fraction de x, décroissant à mesure que x augmente.

Les mathématiciens utilisent le signe

$$\prod$$

pour désigner un produit. On note donc le produit de tous les facteurs $(1 - 1/p)$, pris pour tout nombre premier p inférieur ou égal à x par le symbole

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right).$$

Le nombre de nombres premiers $\leq x$ devrait alors être approximativement égal à

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) \cdot x.$$

Comme c'est un peu lourd d'écrire le produit, on va l'exprimer par une seule lettre, $F(x)$ (F pour "fraction", dépendant de x). Alors on laisse

$$F(x) = \prod_{p \leq x} \left(1 - \frac{1}{p}\right).$$

Avec cette abréviation, on peut alors écrire que le nombre de nombres premiers inférieurs à x est approximativement égal à

$$F(x)x,$$

avec p premier supérieur à $\sqrt{x}$. Alors $N' = N/p$, et N' est plus petit que $\sqrt{x}$. Si q est un facteur premier de N' alors q est plus petit que $\sqrt{x}$ et est également un facteur de N.

qui a l'air plus simple.

Essayons maintenant d'appliquer la même analyse aux nombres premiers jumeaux. Que se passe-t-il pour les nombres premiers jumeaux qui ne se produisait pas dans le cas de tous les nombres premiers ? Il y a une restriction supplémentaire : si p est premier, alors $p+2$ doit aussi être premier. Prenons tous les nombres

$$1, 2, 3, 4, 5, 6, 7, 8, 9, \text{ jusqu'à } x.$$

Environ la moitié d'entre eux sont impairs. Donc, encore une fois, nous obtenons un facteur de 1/2. Regardons maintenant ceux qui ne sont pas divisibles par 3, et écrivons sous chaque nombre le reste après l'avoir divisé par 3 :

$$\begin{array}{ccccccccccc} 1 & 2 & 3 & & 4 & 5 & 6 & & 7 & 8 & 9 & \ldots \\ 1 & 2 & 0 & & 1 & 2 & 0 & & 1 & 2 & 0 & \ldots \end{array}$$

Puisque p ne peut pas être divisible par 3, après l'avoir divisé par 3, nous obtenons un reste de 1 ou 2. Nous avons deux choix possibles.

Pour les nombres premiers jumeaux, à la fois p et $p+2$ doivent être premiers. Donc non seulement p n'est pas divisible par 3 mais aussi $p+2$ n'est pas divisible par 3. Cela signifie que lorsque l'on divise p par 3, le reste doit être...

Le public. Différent de 1.

Serge Lang. Oui, car si le reste est égal à 1, et si j'ajoute 2, alors $p+2$ est divisible par 3. Nous avons donc trouvé une nouvelle condition sur p, qu'après avoir divisé par 3, le reste doit être 2.

Au lieu d'exclure une seule possibilité, comme nous le faisions auparavant, nous excluons maintenant deux possibilités. Notre produit commence donc par

$$\frac{1}{2}\left(1-\frac{2}{3}\right).$$

Faisons maintenant la même chose avec 5. Si on divise un entier par 5, et que l'entier n'est pas exactement divisible par 5, alors il y a quatre restes possibles, à savoir 1, 2, 3, 4. Parmi ceux-ci, si j'ajoute 2, je veux que le nombre $p+2$ ne soit pas non plus divisible par 5. Alors combien y a-t-il de restes possibles ? Autrement dit, pour que $p+2$ ne soit pas divisible par 5, le reste ne doit pas être égal à quoi ?

Le public. 3.

Serge Lang. Oui en effet, si on divise l'entier par 5, le reste devrait être différent de 0 ou 3. Cela me donne un facteur

$$\frac{3}{5} \quad \text{ou} \quad \left(1-\frac{2}{5}\right).$$

Ensuite pour 7, je veux caractériser les entiers p qui ne sont pas divisibles par 7, et tels que, si ajoute 2, alors $p+2$ n'est pas divisible par 7. Alors je dois omettre les multiples de 7, et de plus ceux dont le reste après division par 7 est égal à 5. Le facteur suivant sera donc...

Le public. $1 - \frac{2}{7}$.

Serge Lang. Excellent. Par conséquent, la fraction que nous recherchons sera le produit

$$\frac{1}{2}\prod\left(1-\frac{2}{p}\right),$$

pris sur tous les nombres premiers ≥ 3 et inférieurs ou égaux à x. Lorsque nous avons considéré tous les nombres premiers, sans autre restriction, nous avons été amenés à prendre le produit de tous les termes $(1-1/p)$. Maintenant, avec la condition supplémentaire que $p+2$ est premier, nous sommes conduits au produit des termes $(1-2/p)$ Tout cela est approximatif, mais cela donne une bonne idée du nombre de nombres premiers jumeaux. C'est la conjecture :

Conjecture. Le nombre de nombres premiers jumeaux inférieur ou égal à x est approximativement égal à

$$\frac{1}{2}\prod_{3\leq p\leq x}\left(1-\frac{2}{p}\right)x.$$

Là encore, le produit change avec x, c'est une fonction de x. Ce n'est pas une fonction constante comme 4/5, ou 1/12. Comme précédemment, on abrège le produit, et on pose

$$F_2(x)=\frac{1}{2}\prod_{3\leq p\leq x}\left(1-\frac{2}{p}\right),$$

de sorte que le nombre de nombres premiers jumeaux $\leq x$ est approximativement égal à $F_2(x)x$. Nous sommes maintenant dans une situation similaire à celle où nous comptions tous les nombres premiers, et il reste à analyser ce produit, qui est calculé sur les nombres premiers alors même que nous essayons de compter des nombres premiers. Il y a quelque chose d'un peu circulaire ici, mais pas complètement.

Nous obtenons des informations de ce produit. On peut calculer ce produit. Même si la fraction

$$\frac{1}{2}\prod_{3\leq p\leq x}\left(1-\frac{2}{p}\right)$$

diminue avec x, cette fraction est encore assez grande, mais il faudrait que j'explique ce que j'entends par "plutôt grand". Maintenant je suis coincé, on ne peut le dire qu'avec un vocabulaire plus avancé, avec un peu plus de connaissances en mathématiques. Jusqu'à présent, je ne pouvais me débrouiller qu'avec les règles de base de l'arithmétique qu'on utilise en classe de 7ème. Mais essayons quand même.

Qui a entendu parler du logarithme ? [*Quelques mains se lèvent.*] Qui n'a jamais entendu parler du logarithme ? [*Quelques mains se lèvent.*] Qui garde un silence prudent ? [*Plusieurs mains se* *lèvent.*] OK, il y a quelque chose qui s'appelle le logarithme. On le note $\log x$. Vous le trouverez sur toutes les petites calculatrices à main dans les magasins. Je n'ai pas le temps de l'expliquer plus en détail. [*Quelques explications supplémentaires sont données plus loin.*].

Alors il est vrai que

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) \text{ est approximativement égal à } \frac{1}{\log x}.$$

Mais ce n'est pas trivial à prouver, et il n'y a aucun moyen que je puisse vous donner une idée de la façon dont cela est prouvé. C'est assez technique, et c'est même difficile à faire. C'est élémentaire si on part du calcul différentiel et intégral, mais même en étant élémentaire, c'est dur. Vous pourriez vous débrouiller en disons... trente pages.

[*Diverses réactions dans le public.*]

Serge Lang. Oh, vous savez, trente pages, ce n'est rien. Il y a six mois, de nouveaux théorèmes ont été prouvés et nécessitaient 10 000 pages. Alors trente pages, ce n'est pas grave. En partant de zéro, bien sûr.

Quoi qu'il en soit, il existe une fonction qui s'appelle $\log x$, et le premier produit

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right)$$

est approximativement égal à $1/\log x$.

Quant à l'autre produit, associé aux nombres premiers jumeaux, on peut prouver que

$$F_2(x) \text{ est approximativement égal à } \frac{1}{(\log x)^2}.$$

Le carré vient du fait que l'on remplace $1/p$ par $2/p$. Par exemple, nous avons

$$\prod \left(1 - \frac{1}{p}\right)^2 = 1 - \frac{2}{p} + \frac{1}{p^2},$$

et si p est grand, alors $1/p^2$ est très petit par rapport à $2/p$. Donc, approximativement, nous pouvons le laisser de côté. et on trouve que

$$\prod \left(1 - \frac{1}{p}\right)^2 \text{ est approximativement égal à } \prod \left(1 - \frac{2}{p}\right).$$

La conjecture est donc :

> **Le nombre de nombres premiers jumeaux inférieurs ou égaux à x est approximativement égal à**
>
> $$F_2(x)x, \quad \textbf{ou encore à} \quad \frac{x}{(\log x)^2}$$

Naturellement, il me faudrait encore expliquer plus précisément ce que j'entends par "approximativement", et je n'ai pas le temps maintenant de le faire. C'est un peu plus technique. Peut-être aurons-nous le temps plus tard, après la discussion.

La fonction $\log x$ est une fonction qui croît lentement avec x. Par conséquent, notre fraction est relativement importante. Mais malgré ces arguments heuristiques, personne ne sait prouver qu'il existe un nombre infini de nombres premiers jumeaux.

Qu'est-ce que je viens de faire ? Il ne fait aucun doute que nous avons fait des mathématiques ! Mais rien n'a été prouvé, sauf le premier théorème d'Euclide. Nous avons donné des arguments qui n'étaient qu'heuristiques, mais cela ne veut pas dire que l'esprit ne fonctionnait pas. Au contraire. Nous avons formulé une conjecture, ce qui signifie que nous avons essayé de deviner quelle était la réponse, et nous sommes maintenant confrontés à un problème. Eh bien, c'est ce que signifie faire des mathématiques : trouver des problèmes intéressants et essayer de les résoudre. Finalement, résolvez-les.

Maintenant, posons une autre question. On observe que :

$2^2+1 = 4+1 = 5$ est un nombre premier
$4^2+1 = 16+1 = 17$ est un nombre premier
$6^2+1 = 36+1 = 37$ est un nombre premier
$8^2+1 = 64+1 = 65$ n'est pas un nombre premier
$10^2+1 = 101$ semble être un nombre premier ; en fait, c'en est un.

Question : Dans cette liste de nombres qui s'écrivent comme le carré d'un nombre plus un, y a-t-il une infinité de nombres premiers ? Pensez-y, je demande votre intuition. Je ne vous demande pas encore de prouver quoi que ce soit. Existe-t-il une infinité de nombres premiers de la forme n^2+1 ?

Quelqu'un. Non.

Serge Lang. Qui dit oui...? Qui dit non... ? Qui garde un silence prudent ? [*Réactions variées dans le public. Les suppositions vont dans les deux sens.*] C'est moins clair, n'est-ce pas ?

Le public. Il y a plus d'espace entre eux. Ils surviennent moins fréquemment.

Serge Lang. C'est vrai, madame, il y a plus d'espace entre eux. Et il y a plus d'espace qu'il n'y en avait entre les nombres premiers jumeaux, qui à leur tour avaient plus d'espace entre eux que tous les nombres premiers. Pouvons-nous deviner combien d'espace il devrait y avoir, environ ? Un peu ? Beaucoup ? Pouvez-vous donner une mesure quantitative ?

Laissez-moi d'abord vous donner la réponse : personne ne sait s'il en existe un nombre infini. C'est un problème non résolu. C'est un des grands problèmes des mathématiques. On pense que la réponse est oui. Je le répète, si vous trouvez la réponse, vous entrerez dans les livres d'Histoire des mathématiques (mais vous ne l'aurez pas nécessairement fait dans ce but)

La conjecture est qu'il existe une infinité de nombres premiers de la forme n^2+1, mais comme pour le jumeaux, on peut faire mieux que cela. On peut donner une idée de la fraction correspondante qu'ils représentent.

Pour tous les nombres premiers, la fraction est

$$F(x)x \quad \text{ou} \quad \frac{1}{\log x}x = \frac{x}{\log x}.$$

Pour les nombres premiers jumeaux, la fraction est

$$F_2(x)x \quad \text{ou} \quad \frac{1}{(\log x)^2} = \frac{x}{(\log x)^2}.$$

Quelle fraction allons-nous trouver pour les nombres premiers de la forme n^2+1 ?

Quelqu'un. Vous devez nécessairement avoir n plus petit que $\sqrt{x}$.

Serge Lang. Exact ! Si n^2+1 est plus petit que x alors n est borné par $\sqrt{x}$. Essayons de deviner quelle fraction de tous les nombres est représentée par les nombres premiers de la forme n^2+1. Si les nombres premiers sont distribués au hasard, c'est probablement la même fraction de $\sqrt{x}$ que la fraction de tous les nombres premiers par rapport à x. C'est plutôt plausible. Quoi qu'il en soit, c'est une hypothèse de travail. Quelle est donc la conjecture ? Le monsieur là-bas.

Un homme dans le public. [*Tout le monde hésite.*]

Serge Lang. La fraction de ces nombres premiers inférieurs ou égaux à x est

$$\frac{1}{\log x}x.$$

Si vous appliquez cela à $\sqrt{x}$, vous obtenez approximativement

$$\frac{1}{\log x}\sqrt{x}.$$

C'est la conjecture, grosso modo, à un facteur constant près.

Quelqu'un. Pourquoi n'est-ce pas $\frac{1}{\log\sqrt{x}}\sqrt{x}$?

Serge Lang. OK, ce n'est pas si clair si ça doit être x ou $\sqrt{x}$. Mais d'abord, on a la relation

$$\log\sqrt{x} = \frac{1}{2}\log x,$$

donc les deux expressions ne diffèrent que d'un facteur 2 ; et deuxièmement, je ne prétends pas donner autre chose qu'une approximation, à un certain facteur constant près. En tout cas, ces idées heuristiques, qui sont purement intuitives, vous donnent l'idée qu'il devrait y avoir un nombre infini de tels nombres premiers, puisqu'on peut en donner une mesure quantitative.

Bien sûr, je devrais expliquer ce que j'entends par "approximativement", non seulement pour les nombres premiers de la forme $n^2 + 1$, mais aussi pour tous les nombres premiers, ou les nombres premiers jumeaux. Ce serait le sujet d'un autre exposé, que je ne peux donner aujourd'hui et qui durerait peut-être une heure. C'est précisément le terme d'erreur dans cette approximation qui fait l'objet d'un problème généralement reconnu comme étant le plus grand problème des mathématiques. C'est le terme d'erreur qui apparaît dans la formule $x/(\log x)$ pour tous les nombres premiers. Il existe une conjecture précise, due à Riemann, et appelée l'hypothèse de Riemann, faite il y a environ 130 ans, et qui donne le meilleur terme d'erreur possible. Elle n'est toujours pas prouvée aujourd'hui, malgré le fait que de nombreux mathématiciens aient travaillé dessus.

Mais je parle depuis une heure, Arrêtons-nous ici.

Les questions

QUESTION. Vous avez cité d'autres mathématiciens purs, mais vous, pourquoi faites-vous ce genre de travail ?

SERGE LANG. Pourquoi ? Pourquoi composez-vous une symphonie ou une ballade ? Je voua ai déjà dit pourquoi. Parce que ça me donne des frissons dans le dos. Voilà pourquoi. Mais je n'ai pas dit que cela devrait provoquer la même chose pour vous. Vous êtes libres.

QUESTION. Pouvez-vous dire où se situe la limite entre les mathématiques pures et appliquées ?

SERGE LANG. Il n'y a pas de limites. Les deux se mélangent sans que je puisse définir une limite. Si vous essayez de définir plus précisément une limite, en général, je ne dis pas que vous n'y arriverez pas, mais personnellement, je n'ai jamais vu quelqu'un y parvenir.

QUESTION. Ce que vous avez fait tout à l'heure, vous pensez que ça pourrait être utile quelque part ?

SERGE LANG. Vous avez dit "pourrait". C'est un conditionnel, je suis donc obligé de répondre logiquement : oui.

QUESTION. Lorsque vous faites de la recherche mathématique, avez-vous un objectif en tête ?

SERGE LANG. Le but est de prouver la conjecture.

QUESTION. Mais au début ?

SERGE LANG. Au départ, il s'agit d'abord de trouver la conjecture que l'on veut prouver, puis d'essayer de la prouver. L'une des principales difficultés en mathématiques est de trouver le sujet sur lequel on veut se concentrer, et le problème que l'on va essayer de résoudre.

QUESTION. Mais est-ce fait par déduction logique ou par intuition ?

SERGE LANG. Ai-je utilisé la logique ici ? Moitié moitié. Il y avait beaucoup de trucs intuitifs, et la logique, vous savez, quand je vous dis que quelque chose ou autre est un tiers ou un cinquième de quelque chose d'autre, j'ai supposé beaucoup de choses sans les prouver. C'est plus par intuition que par logique que j'ai fait des mathématiques ici. Quoi qu'il en soit, en général, les nouveaux résultats sont découverts par intuition, les preuves sont découvertes par intuition, et finalement elles sont écrites selon un schéma logique. Mais ne confondez pas les deux. C'est comme en littérature : la grammaire et la syntaxe ne sont pas de la littérature. Lorsque vous écrivez une pièce musicale, vous utilisez des notes, mais les notes ne sont pas la musique. Lire un morceau de musique à partir du texte écrit ne remplace pas l'écoute du morceau au Carnegie Hall ou ailleurs. La logique est l'hygiène des mathématiques, tout comme la grammaire et la syntaxe sont l'hygiène du langage et même alors ! "Sous le bam, sous le boo, sous le bambou...", il n'y a pas de grammaire. L'essentiel chez Shakespeare, ou chez Goethe, ce n'est pas la grammaire ou la syntaxe. C'est la poésie, l'effet musical des mots, les allusions poétiques, l'impressionnisme esthétique, et bien d'autres choses. Mais tandis que la beauté de la poésie pâlit sous la traduction, la beauté des mathématiques est invariante selon les transformations linguistiques.

QUESTION. Vous avez utilisé des arguments heuristiques et des approximations pour décrire ce que fait un mathématicien pur. Mais un mathématicien fait autre chose que cela.

SERGE LANG. Attention, je n'ai pas dit qu'un mathématicien ne fait que ça. On essaie de prouver quelque chose, on découvre une conjecture un peu comme je l'ai décrit ici. Mais une fois la conjecture faite, on essaie de la prouver. Parfois on réussit, parfois non. Nous procédons par approximations successives, à la fois en faisant des suppositions et en essayant de les prouver. La négation d'un absolu n'est pas l'absolu de type opposé.

Selon la fréquence à laquelle vous réussissez ou la profondeur de vos résultats, vous serez un grand mathématicien, ou un mathématicien moyen, ou...

QUESTION. Par exemple, vous n'avez pas parlé d'axiomatisation.

SERGE LANG. L'axiomatisation, c'est ce qu'on fait en dernier, ce sont des déchets. C'est l'hygiène des mathématiques, l'axiomatisation. C'est la discipline de l'esprit. Comme la grammaire et la syntaxe. Mais faites ce que vous voulez. Chacun doit déterminer ce qu'il aime faire. Le mot "déchets" est trop fort. J'axiomatise aussi, quand je trouve que c'est approprié de le faire, et il y a beaucoup d'autres choses dont je n'ai pas parlé. J'ai fait un choix. Je voulais montrer un aspect essentiel des mathématiques dont la plupart des gens n'ont aucune idée qu'il existe.

QUELQU'UN. Il y a un problème qui me donne des frissons, le problème de la dénombrabilité des nombres réels. Cantor a essayé de résoudre ce problème, et je pense qu'il est devenu un peu fou à cause de cela. J'ai entendu dire que Cantor l'avait prouvé. J'aimerais savoir si c'est vrai.

SERGE LANG. Prouvé quoi ? Que les nombres réels ne sont pas dénombrables ? Oui, il l'a sûrement fait.

LA MÊME PERSONNE. Pouvez-vous nous donner une idée de la preuve ?

SERGE LANG. [*Hésite.*]

LA MÊME PERSONNE. Sans aller trop loin.

SERGE LANG. Bon, le monsieur voudrait... [*Brouhaha dans le public.*]

Oui ! Je peux le faire en quelques minutes.

UN HOMME. J'étais juste curieux.

SERGE LANG. Mais c'est exactement ce que c'est, la curiosité ! [*Rires.*] Au contraire, tout le but de l'opération était d'aiguiser votre curiosité en vous montrant ce qui m'intéressait. Alors je donne la preuve. Qu'est-ce qu'un nombre réel ? C'est un nombre avec une infinité de décimales, par exemple 27.9130523... Comme je ne peux pas écrire un nombre infini de chiffres comme ça, je dois utiliser une notation avec des indices. Et pour simplifier, je ne considérerai que les nombres compris entre 0 et 1. Supposons que l'on puisse écrire tous ces nombres dans une séquence, avec un premier, un second, un troisième, etc., sans en manquer aucun, comme suit :

$$\begin{array}{l} 0.\ a_{11}\ a_{12}\ a_{13;}a_{14}... \\ 0.\ a_{21}\ a_{22}\ a_{23}\ a_{24}... \\ 0.\ a_{31}\ a_{32}\ a_{33}\ a_{34}... \end{array}$$

avec des entiers a_{ij} tous compris entre 0 et 9. Je vais montrer qu'il existe un nombre avec une infinité de décimales qui n'est pas dans cette liste Je choisis un entier b_1 qui n'est pas égal à a_{11}. Alors un entier b_2 qui n'est pas égal à a_{22}. Alors un entier b_3 qui n'est pas égal à a_{33}. En général, je choisis un entier b_n qui n'est pas égal à a_{nn}, et je choisis b_n entre 1 et 8 (pour éviter les ambiguités liées à une suite de 0 ou de 9). Alors le nombre avec une infinité de décimales

$$0.\ b_1\ b_2\ b_3\ b_4...$$

n'est égal à aucun des nombres de la liste à cause de la façon dont je l'ai construit, c'est donc un nouveau nombre.

Notez que ce que nous venons de faire est similaire à la méthode d'Euclide au début. On a fait une liste, puis on a montré qu'il y a un nombre décimal qui n'est pas dans la liste.

QUESTION. J'aimerais savoir ce que vous pensez des grandes écoles de pensée mathématique concernant l'infini.

SERGE LANG. Je n'y pense pas. Tout cela a été réglé pour moi il y a longtemps. Il avait une certaine importance historique, mais aujourd'hui, c'est réglé. Quelque chose est infini ou ne l'est pas.

QUESTION. Mais ce n'est pas si simple que ça !

Serge Lang. Ok, vous avez raison.

Question. L'infini existe-t-il ?

Serge Lang. Quand j'évoquais les nombres premiers, saviez-vous s'il y en avait un nombre infini ou non ?

Question. Oui.

Serge Lang. Alors ça y est, vous avez compris. Cela règle la question.

Question. Mais la preuve de Cantor a été plus ou moins rejetée par les intuitionnistes. Je pense qu'il y a eu beaucoup de disputes à ce sujet.

Serge Lang. Si les gens veulent se battre, ils sont libres de le faire. Je fais juste des mathématiques.

Question. Avez-vous travaillé vous-même sur les problèmes que vous soulevez aujourd'hui ?

Serge Lang. Oui, sur le problème des nombres premiers de la forme $n^2 + 1$. Puisque cela vous intéresse, et que vous êtes toujours assis ici, permettez-moi de donner quelques précisions sur ce problème. Quand j'ai commencé à réfléchir à ce que j'allais vous dire aujourd'hui, j'ai pensé aux nombres premiers jumeaux mais je ne savais pas moi-même s'il y avait une conjecture à leur sujet, ni comment la motiver. J'ai recherché le livre de Hardy et Wright, et je l'ai trouvé. Cette conjecture, ainsi que celle sur les nombres premiers de la forme n^2+1, sont dues à Hardy et Littlewood, datant de 1923. Je vais énoncer leur conjecture un peu plus précisément que je ne l'ai fait jusqu'ici.

J'ai dit plusieurs fois que certaines expressions étaient approximatives, à un facteur constant près. Qu'est-ce que cela signifie ? Supposons que j'ai deux expressions $A(x)$ et $B(x)$. On dit que $A(x)$ est asymptotique à $B(x)$ si le quotient

$$\frac{A(x)}{B(x)}$$

tend vers 1 lorsque x devient de plus en plus grand. Cela signifie que lorsque x est très grand, alors le quotient est très proche de 1. Les relations selon lesquelles $A(x)$ est asymptotique à $B(x)$ sont notées par le symbole

$$A(x) \sim B(x).$$

On peut alors énoncer le théorème des nombres premiers comme suit.

Soit $\pi(x)$ le nombre de nombres premiers $\leq x$. Alors on a la relation

$$\pi(x) \sim e^{\gamma} F(x) x,$$

où e et γ sont des constantes utilisées tout le temps en mathématiques et F est comme avant. La constante e est appelée la base naturelle des logarithmes ; et γ est appelée constante d'Euler. Le produit $F(x)$ lui-même paraissant plutôt mystérieux, on préfère le remplacer par une autre expression. C'est un théorème dû à Mertens qui énonce que l'on a la relation asymptotique

$$e^{\gamma}F(x) \sim \frac{1}{\log x},$$

et donc on trouve que

$$\pi(x) \sim \frac{x}{\log x},$$

qui est la formulation habituelle du théorème des nombres premiers. Il est utile de l'écrire de cette façon, car la fonction log est très connue. Nous savons comment le logarithme grandit quand x devient grand. Par exemple, nous avons les valeurs suivantes :

$$\begin{array}{ll} \log\ 10 = \ 2.3... & \log\ 10\,000 = \ 9.2... \\ \log\ 100 = \ 4.6... & \log\ 100\,000 = \ 11.5... \\ \log\ 1\,000 = \ 6.9... & \log\ 1\,000\,000 = \ 13.8... \end{array}$$

et ainsi de suite. Observez que les nombres 10, 100, 1 000, 10 000, 100 000, 1 000 000 croissent par puissances de 10, mais le logarithme ne croît qu'en ajoutant environ 2.3 à chaque fois. Cela signifie que la fonction logarithme croît beaucoup plus lentement que la fonction identité.

De même, notons $\pi_2(x)$ le nombre de nombres premiers jumeaux $\leq x$. Alors la conjecture de Hardy-Littlewood est que

$$\pi_2(x) \sim (e^{\gamma})^2 F_2(x)x.$$

Cette formule peut aussi s'écrire asymptotiquement avec le logarithme, sous la forme

$$\pi_2(x) \sim 2C_2 \frac{x}{(\log x)^2},$$

où C_2 est une constante, donnée par un produit infini pris sur tous les nombres premiers ≥ 3, notamment

$$C_2 = \prod_{3 \leq p} \left(1 - \frac{1}{(p-1)^2}\right).$$

Hardy et Littlewood donnent des arguments probabilistes plus précis que ceux que je pourrais donner ici en une heure. En particulier, lorsque j'écrivais les produits, je supposais implicitement que les conditions de divisibilité par 2, 3, 5, etc. étaient indépendantes. Mais je n'ai pas prouvé cette hypothèse, qui en fait est fausse, Ces conditions ne sont pas indépendantes et la constante e^{γ} reflète les dépendances entre ces conditions de divisibilités[7].

[7]La preuve de la formule conjecturée du nombre de nombres premiers n'est pas du tout triviale. En effet, le problème de Goldbach, qui est tout à fait analogue au problème des nombres premiers jumeaux, stipule que tout nombre pair suffisamment grand est la somme de deux nombres premiers impairs. Hardy et Littlewood ont même conjecturé qu'il existe une formule asymptotique pour le nombre de telles représentations, donnée par

$$N_2(n) \sim 2C_2 \frac{n}{(\log n)^2} \prod \frac{p-1}{p-2},$$

où le produit (fini) est pris sur tous les nombres premiers $\neq 2$ divisant n. Remarquons à nouveau la même constante C_2 que nous avons trouvée dans le problème des nombres premiers jumeaux, ainsi que le dénominateur avec le carré du logarithme. Les arguments heuristiques sont similaires. Mais Hardy et Littlewood remarque que Sylvester en 1871 et Brun en 1915 avaient conjecturé une formule fausse, qui ne tenait pas compte des relations donnant lieu au facteur e^{γ}.

Mais cela devient maintenant beaucoup plus technique, et je ne peux entrer dans les détails nécessaires pour trouver la constante e^γ. Je dois vous renvoyerà l'article original d'Hardy et Littlewood, ou au livre de Hardy et Wright.

Pour en revenir à la question de mon propre travail, un ami Hale Trotter et moi nous sommes intéressés à des problèmes analogues, concernant la distribution des nombres premiers dans des contextes beaucoup plus compliqués. Je ne peux pas les détailler ici. Mais on retrouve la même relation asymptotique que Hardy et Littlewood pour les nombres premiers de la forme $n^2 + 1$, avec la même constante C_2 (heureusement !). L'article avec Trotter donne un modèle probabiliste qui est complètement différent de celui de Hardy et Littlewood. Naturellement, seules les personnes spécialisées en théorie des nombres peuvent le comprendre.

Question. Entre les mathématiques pures et appliquées, je ne vois pas très bien la différence.

Serge Lang. À première vue, le fait que le calcul du nombre de nombres premiers de la forme $n^2 + 1$ n'ait pas d'application ne signifie pas que cela n'aura jamais d'applications. Dans l'histoire des mathématiques, les résultats de recherches effectuées d'un point de vue purement esthétique ont été appliqués, parfois après un siècle, à des problèmes très concrets. Par exemple, aujourd'hui, on utilise des parties de la théorie des nombres premiers dans la théorie du codage. Autant que je sache, ce ne sont pas des théorèmes en question dont nous avons discuté aujourd'hui, mais cela aurait tout aussi bien pu être le cas. J'ai également apporté une citation de von Neumann[8], que je n'ai pas eu le temps de lire jusque-là. Il est peut-être temps de la lire maintenant. [*Approbation du public.*] Ah, la voilà.

> Je pense que c'est une assez bonne approximation de la vérité - qui est beaucoup trop compliquée pour permettre autre chose que des approximations - que les idées mathématiques trouvent leur origine dans la réalité empirique, bien que la généalogie soit parfois longue et obscure. Mais, une fois que les idées ont ainsi été conçues, elles commencent à vivre leur vie propre et le domaine mathématique se compare mieux à un domaine créatif, dirigé presque entièrement par des motivations esthétiques, qu'à toute autre chose, et en particulier qu'à une science empirique. Il y a cependant un autre point qui, je crois, mérite d'être souligné. Au fur et à mesure qu'un domaine des mathématiques s'éloigne de sa source empirique, ou plus encore, s'il n'est qu'indirectement inspiré par des idées venues de la "réalité", il est en proie à de très graves dangers. Il devient de plus en plus purement esthétisant, de plus en plus purement de l'art pour l'art. Cela n'a pas besoin d'être mauvais, si le domaine est entouré de sujets corrélés, qui ont encore des liens empiriques plus étroits ou si la discipline est sous l'influence d'hommes avec un goût exceptionnellement bien développé. Mais il y a un grave danger que le sujet se développe selon la ligne de moindre résistance, que le courant, si loin de sa source, se sépare en une multitude de branches insignifiantes, et que la discipline devienne une masse désorganisée de détails et de complexités.

[8]J. von Neumann, *The Mathematician*, Collected Works I, pp. 1-9.

> En d'autres termes, à grande distance de sa source empirique, ou après bien des consanguinités "abstraites", un sujet mathématique est en danger de dégénérescence. Au début, le style est généralement classique ; quand il montre des signes de devenir baroque, alors le signal de danger est élevé. Il serait facile de donner des exemples, de retracer des évolutions précises dans le baroque et le très haut baroque, mais là encore, ce serait trop technique.

J'ai quelques objections sur la façon dont von Neumann s'exprime. S'il n'exprime que ses goûts personnels, tant mieux. Il a le droit à ses propres goûts. Contrairement à lui, je ne ressens aucun danger à faire des mathématiques pour lesquelles je ne vois aucun rapport avec le monde empirique. Plusieurs fois au cours de ma vie, j'ai vu des situations où certains mathématiciens se sont plaints que certains domaines de recherche étaient trop "abstraits" - von Neumann pourrait dire "baroques". Mais quinze ans plus tard, ces recherches combinées à d'autres ont conduit à la solution de problèmes très classiques, qui s'étaient déjà posés au XIX$^{\text{ième}}$ siècle.

Il y a autant de possibilités de faire des mathématiques sans intérêt ou triviales en théorie des nombres qu'il y a de faire des mathématiques avec des conceptions empiriques. Quant à la "consanguinité", je ne comprends pas ce que veut dire von Neumann. Beaucoup des plus belles découvertes en mathématiques viennent du mariage de branches qui semblent a priori très éloignées les unes des autres. L'une des caractéristiques du génie mathématique est la capacité de réunir différentes branches, par ce qu'on pourrait appeler la "consanguinité", ou de réunir des fils partant dans plusieurs directions ; trouver des idées fondamentales dans la masse de détails et de complexités que d'autres ont accumulées. Cela ne signifie pas que le travail des autres a été sans valeur.

Historiquement, dans les années 50, il est vrai que plusieurs branches des mathématiques pures se sont développées parallèlement les unes aux autres. Von Neumann n'était pas le seul à se plaindre que ces flux, qui pour beaucoup à l'époque semblaient sans lien les uns avec les autres, étaient trop abstraits. Mais dans les années 60, nous avons vu ces flux se rejoindre de manière très profonde et essentielle. Et non seulement cela, mais nous les avons vus rejoindre des sujets qui n'étaient plus à la mode depuis quarante ans, et nous les avons vus rejoindre des sujets presque oubliés depuis le XIX$^{\text{ième}}$ siècle. On a aussi vu de vieilles conjectures se prouver justement parce que depuis une quinzaine d'années, on a trouvé comment faire des synthèses qui se classent parmi les plus abouties de l'histoire des mathématiques. A posteriori, on voit aujourd'hui que les développements parallèles des années 50 ont été une étape essentielle pour les synthèses qui ont suivi.

Un homme. Pour revenir aux nombres premiers, on admet qu'il y en a une infinité, et par conséquent il y a une infinité d'inverses de ces nombres premiers. Est-il vrai que la somme de ces inverses est finie ?

Serge Lang. C'est une très belle question Vous voulez prendre la somme

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\dots$$

Un homme. Oui.

Serge Lang. C'est donc la somme

$$\sum_{p \leq x} \frac{1}{p}.$$

Eh bien, si je voulais pointer quelqu'un dans le public pour poser une question qui correspondait exactement à ce que j'ai dit auparavant, je n'aurais pas pu faire mieux que de pointer le monsieur là-bas [*Rire.*]

Rappelons-nous que notre produit était

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right).$$

Nous venons d'écrire une somme avec $1/p$. Les deux se ressemblent. L'un d'eux semble multiplicatif et l'autre additif. mais le fait qu'ils se ressemblent n'est nullement accidentel, et tient justement au logarithme dont je n'ai pas eu le temps de beaucoup discuter. Mais si vous me donnez deux minutes... Le logarithme a deux propriétés simples. La première est que

$$\log(ab) = \log a + \log b.$$

Autrement dit, le logarithme d'un produit est égal à la somme des logs. Si vous connaissez le logarithme, vous connaissez cette propriété.

La deuxième propriété est que lorsque t est très petit, $\log(1+t)$ est approximativement égal à t. Donc $\log(1-t)$ est approximativement égal à $-t$.

Supposons maintenant que je prenne le logarithme du produit. Comme le log d'un produit est égal à la somme des logs, on a

$$\log \prod_{p \leq x} \left(1 - \frac{1}{p}\right) = \sum_{p \leq x} \log \left(1 - \frac{1}{p}\right).$$

Mais $\log(1 - 1/p)$ est approximativement égal à $-1/p$. Donc notre somme est approximativement égale à

$$\sum_{p \leq x} \log \left(1 - \frac{1}{p}\right) \sim -\sum_{p \leq x} \frac{1}{p},$$

qui est précisément la somme que Monsieur veut considérer. C'est un théorème, qui se prouve quand on analyse la somme, que l'on a la relation asymptotique

$$\sum_{p \leq x} \frac{1}{p} \sim \log \log x.$$

Comme le logarithme croît très lentement, le logarithme itéré $\log \log x$ croît encore plus lentement. Mais il croît, et la somme est très intéressante. Il n'est donc pas vrai que la somme des inverses $1/p$ prise pour tous les nombres premiers p soit finie.

Vous voyez, si vous étudiez cette somme, vous trouvez log log x. Pour étudier le produit, vous effectuez l'opération inverse, vous exponentiez, et vous trouvez log x, toujours avec un signe moins. Alors vous trouvez que

$$\sum_{p \leq x} \log\left(1 - \frac{1}{p}\right) \text{ is approximately equal to } \frac{1}{\log x},$$

qui est précisément ce que nous avions avant. Tout cela appartient au même cercle d'idées. Le monsieur obtient un A+.

Question. Voyez-vous des applications de la théorie des nombres premiers dans les sciences ?

Serge Lang. Les sciences ? Vous voulez dire la physique, la chimie, la biologie ? Je n'en connais pas, mais l'histoire des mathématiques montre que des matières considérées comme pures peuvent, à tout moment, avoir les applications concrètes les plus inattendues. Je ne peux pas prédire à l'avance ce qui va se passer. Je n'en connais pas, mais ça ne veut pas dire qu'il n'y en a pas, car je ne connais pratiquement rien à la physique et à la chimie. Il peut y avoir des applications que je ne connais pas. Par contre, je ne peux pas prédire qu'il n'y en aura pas, et en fait, je fais exactement le contraire : je dis qu'il peut y en avoir, à tout moment. Par exemple, ces dernières années, des théories mathématiques pures de géométrie différentielle ou de topologie découvertes il y a dix ou vingt ans ont soudainement trouvé des applications à la théorie des particules élémentaires en physique !

J'essaie d'éviter les absolus, d'un côté ou de l'autre. Je vous ai dit ce que j'aime, je vous ai montré ce que j'aime. Et j'espère que ça vous plaît. Et si ça marche comme ça, c'est tout ce que je voulais faire.

Addenda

Question. Et l'hypothèse de Riemann, que vous avez mentionnée précédemment. Pouvez-vous nous dire ce que c'est ?

Serge Lang. Oui. Nous voulons donner une description plus précise du terme d'erreur dans la formule du nombre de nombres premiers. Le terme $x/\log x$ n'est qu'une approximation très grossière, voire asymptotique. Il existe une autre expression qui donne une bien meilleure approximation.

Rappelez-vous que nous avions trouvé une certaine fraction

$$e^{\gamma} F(x), \quad \text{ou également} \quad \frac{1}{\log x}$$

que nous appellerons maintenant la densité de nombres premiers, ou encore la probabilité que x soit premier, asymptotiquement. Après cela, nous avons dit que $\pi(x)$ est asymptotique au produit de cette densité par x, c'est-à-dire

$$\pi(x) \sim \frac{1}{\log x}\, x.$$

Mais on peut mieux faire que de prendre ce produit, car log x varie avec x. On obtient une bien meilleure formule en faisant la somme des densités, de 2 à x, que l'on note $L(x)$ Cela signifie qu'on pose

$$\begin{aligned} L(x) &= \frac{1}{\log 2} + \frac{1}{\log 3} + \frac{1}{\log 4} + \frac{1}{\log 5} + \ldots + \frac{1}{\log x} \\ &= \sum_{n=2}^{x} \frac{1}{\log n}. \end{aligned}$$

Alors on a aussi la relation asymptotique

$$\pi(x) \sim L(x) \sim \frac{x}{\log x},$$

mais $L(x)$ donne une bien meilleure approximation de $\pi(x)$ que $x/\log x$. L'hypothèse de Riemann stipule que

$$\pi(x) = L(x) + O(\sqrt{x} \log x),$$

où $O(\sqrt{x} \log x)$ est un terme d'erreur, borné par $C\sqrt{x} \log x$, où C est une constante. Puisque $\sqrt{x}$ et $\log x$ sont très petits comparés à x, on voit que $L(x)$ donne une très bonne approximation de $\pi(x)$.

L'hypothèse de Riemann permet également de mieux comprendre la relation entre le produit $F(x)$ et $1/\log x$. En effet, H. Montgomery me dit qu'elle implique la relation

$$e^{\gamma} F(x) x = \frac{x}{\log x} + O(\sqrt{x}),$$

où à nouveau $O(\sqrt{x})$ est un terme d'erreur borné par $C\sqrt{x}$, avec une certaine constante adéquate C. Par conséquent les expressions $e^{\gamma} F(x) x$ et $x/\log x$ donnent à peu près la même approximation de $\pi(x)$, et les deux sont pires que $L(x)$.

Références

[1] V. Brun, "Über das Goldbachsche Gesetz und die Anzahl der Primzahlpaare," *Archiv for Mathematik* (Christiania) 34 Part 2 (1915). p. 1-15.

[2] G.H. Hardy, *A Mathematician's Apology*, Cambridge University Press, 1969.

[3] G.H. Hardy, J.E. Littlewood, "Some problems of Partitio Numerorum," *Acta Math.* 44 (1923), pp. 1–70.

[4] G.H. Hardy, E.M. Wright, *An Introduction to the Theory of Numbers*, Fourth Edition, Oxford University Press, 1980.

[5] A.E. Ingham, *The Distribution of Prime Numbers*, Hafner Publishing Company, New York, 1971 (Reprinted from Cambridge University Press).

[6] S. Lang, H. Trotter, *Frobenius Distributions in GL_2-extensions*, Springer Lecture Notes 504, Springer-Verlag, New York, 1976.

[7] J.J. Sylvester, "On the partition of an even number into two prime numbers," *Nature*, 55 (1896-1897), pp. 196-197 (= *Math Papers* 4. pp. 734-737).

[8] D. Zagier, "The first 50 million prime numbers," *Mathematical Intelligencer*, 1978.