Nombres premiers et chaos quantique

Andrew Granville

Cet article est la transcription d'une conférence donnée devant un public d'amis des mathématiques le 6 février 2002. Il a été publié initialement dans sa version originale en juin 2002, dans l'Emissary, le bulletin d'information du Mathematical Sciences Research Institute (`www.msri.org/publications/emissary`*). Nous remercions les Pr. Singer et Hoffman de leur autorisation.*

Les figures sont dues à Andrew Odlyzko (dernière figure) et Silvio Levy (autres figures).

Pour la traduction, merci à Marc Yor et Frédérique Petit, ainsi qu'à quelques collègues volontairement anonymes qui se reconnaîtront.

Andrew Granville est un spécialiste bien connu et enthousiaste des nombres premiers.

La répartition des nombres premiers est l'un des sujets les plus anciens des mathématiques. Depuis cent cinquante ans, il fait l'objet de recherches intensives au moyen des méthodes les plus modernes. Malgré cela et en dépit de la grande qualité des chercheurs qui s'y sont consacrés, il est désespérant de constater que nous savons encore très peu de choses sur les questions les plus fondamentales. Comme on peut s'y attendre dans un domaine aussi ancien et respectable, les progrès des dernières décennies ont été lents, et, comme le sujet a été si profondément étudié, les avancées apparemment les plus mineures nécessitent des idées profondes et difficiles, et bien souvent une grande virtuosité technique.

Mais récemment notre compréhension du phénomème a connu un progrès extraordinaire en provenance d'une direction inattendue. Les idées en question viennent d'un domaine qui semblait n'avoir rien à voir avec les nombres premiers, celui des mathématiques de la physique quantique.

Je suis un spécialiste de la théorie analytique des nombres, et je n'ai pas été formé à la physique : en fait, les cours de physique quantique que j'ai suivis comme étudiant, ne m'ont guère éclairé et m'ont laissé plutôt perplexe. À cause des progrès récents dans mon propre domaine, j'ai dû m'y replonger et essayer de me faire une idée des points clés de la physique quantique. Je vais essayer ici de vous faire partager le peu que j'en ai compris, de parler des conséquences troublantes de la mécanique quantique et des origines de la célèbre phrase d'Einstein :

Dieu ne joue pas aux dés avec l'univers.

Pour une bonne introduction à l'usage des profanes, voir *The Ghost in the Atom* [5].

Mais je vais commencer par un sujet avec lequel je me sens bien plus à l'aise :

Que sont les nombres premiers et pourquoi avons-nous besoin d'eux ?

Cette année, 2002, se décompose en produit de nombres premiers sous la forme $2 \times 7 \times 11 \times 13$. À l'année prochaine correspondra une autre factorisation, et en fait, chaque nombre entier se décompose à sa façon sous forme de produit de nombres premiers. « Et alors ? » me direz-vous ; eh bien chacun se sert sans arrêt du fait qu'il est difficile de factoriser les grands nombres... Avez-vous déjà acheté quelque chose sur la toile et été inondé de petites fenêtres qui s'étendent à longueur de pages sur « les systèmes de cryptage RSA » ?

C'est la théorie des nombres qui est derrière tout cela - c'est la difficulté qu'il y a à factoriser les grands nombres qui permet de conserver vos informations à l'abri des regards indiscrets !

Aussi, les nombres premiers valent-ils la peine d'être étudiés attentivement. De plus, tout comme les atomes sont les briques dont la nature est fabriquée, de même les nombres premiers sont les briques qui constituent les nombres ; ainsi, pour étudier la théorie des nombres, nous devons avoir une bonne connaissance des nombres premiers. Ensuite, je voudrais aborder l'une des questions fondamentales pour la compréhension des nombres premiers.

Combien y a-t-il de nombres premiers inférieurs à un million ? inférieurs à un milliard ? à n'importe quel nombre donné ?

En 1849, Carl Friedrich Gauss écrivait :

Lorsque j'étais adolescent, en 1792 ou 1793, j'ai réfléchi à ce problème et ai trouvé que la densité des nombres premiers autour de t est $\frac{1}{\log t}$, *si bien que le nombre de nombres premiers inférieurs à un x donné est approximativement* $\int_2^x \frac{dt}{logt}$.

Gauss, qui avait tout juste 15 ans à l'époque de cette découverte, fit cette conjecture en étudiant les tables de nombres premiers jusqu'à trois millions. Une estimation extraordinaire, qui s'est révélée d'une étonnante précision.

x	nombre de nombres premiers inférieurs à x	surestimation de Gauss
10^8	5761455	754
10^9	50847534	1701
10^{10}	455052511	3104
10^{11}	4118054813	11588
10^{12}	37607912018	38263
10^{13}	346065536839	108971
10^{14}	3204941750802	314890
10^{15}	29844570422669	1052619
10^{16}	279238341033925	3214632
10^{17}	2623557157654233	7956589
10^{18}	24739954287740860	21949555
10^{19}	234057667276344607	99877775
10^{20}	2220819602560918840	223744644

Peut-on estimer l'ordre de grandeur de l'erreur de Gauss ? Après un rapide coup d'œil à la table ci-dessus, nous voyons que le nombre de chiffres de l'erreur est environ la moitié de celui du nombre de nombres premiers, c'est-à-dire de l'ordre de sa racine carrée. En d'autres termes, on peut émettre la conjecture que

$$\int_2^x \frac{dt}{\log t} - \text{cardinal de l'ensemble des nombres premiers inférieurs à } x$$

est borné supérieurement par une fonction comme $\sqrt{x}$. Une autre caractéristique surprenante de ces données est que l'erreur est toujours positive, indiquant que, au moins dans les données calculées jusqu'à présent, l'estimation de Gauss est trop grande. Ceci peut nous amener à penser qu'en introduisant un terme supplémentaire, on pourrait obtenir une estimation plus précise. Or ce n'est pas le cas : l'erreur change de signe une infinité de fois, comme l'a montré Littlewood en 1914.

Trouver le moment où l'erreur devient négative pour la première fois n'est pas chose aisée. La première borne concernant un tel x (appelons-le x_0) fut donnée en 1933 par Skewes,

$$x_0 < 10^{10^{10^{34}}}.$$

Pendant longtemps, ce nombre était considéré, selon plusieurs sources, comme le plus grand nombre connu ayant une propriété distinctive. Cette borne a été réduite petit à petit à $x_0 < 1,39822 \times 10^{316}$, et on peut trouver dans [1] des arguments convaincants indiquant qu'il s'agit là à peu près de la bonne valeur de x_0 ! (Pour plus de détails, voir mon article à paraître [8]).

On peut facilement modifier l'énoncé de Gauss et obtenir un modèle probabiliste pour les nombres premiers, comme le fit Cramér en 1936 [4] : soit X_3, X_4, ... une suite de variables aléatoires indépendantes telles que

$$\mathbb{P}[X_n = 1] = \frac{1}{\log n} \quad \text{et} \quad \mathbb{P}[X_n = 0] = 1 - \frac{1}{\log n}.$$

On peut considérer comme élément « typique » de cet espace de probabilité la suite π_3, π_4, etc., où $\pi_n = 1$ si et seulement si n est premier, et s'il est possible de faire un énoncé dans cet espace dont la probabilité soit 1, alors on peut s'attendre à ce qu'il soit vrai pour les nombres premiers (c'est-à-dire pour la suite π_3, π_4, ...). Certainement,

$$\sum_{n \leqslant x} X_n \sim \int_2^x \frac{dt}{\ln t} \quad \text{quand } x \to +\infty \text{ avec une probabilité égale à } 1\,;$$

en d'autres termes, la valeur attendue pour le dénombrement des nombres premiers par le modèle de Gauss-Cramér est conforme à la réalité. De plus, dans de petits intervalles (ce qui correspond mieux à ce que Gauss regardait)

$$\sum_{x < n \leqslant x+y} X_n \sim \int_x^{x+y} \frac{dt}{\ln t} \qquad \text{quand } x \to +\infty, \text{ avec probabilité } 1,$$

où y est une petite puissance fixée de x.

La seconde statistique que les gens ont tendance en général à considérer est la variance :

$$\text{la moyenne de } \left| \sum_{x<n\leqslant x+y} X_n - \int_x^{x+y} \frac{dt}{\ln t} \right|^2 .$$

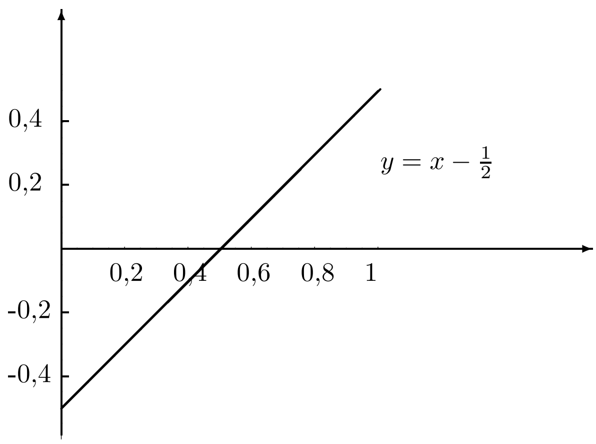
Et là, se produit une grosse surprise : on peut montrer que la valeur prédite par le modèle de Gauss-Cramér ne peut en aucun cas être la variance du dénombrement des nombres premiers ! Alors que le modèle de Gauss marchait si bien jusque-là, le fait qu'il s'effondre sur cette question est tout à fait inattendu, comme l'a remarqué Paul Erdös :

Dieu ne joue peut-être pas aux dés avec l'univers, mais il se passe quelque chose d'étrange avec les nombres premiers.

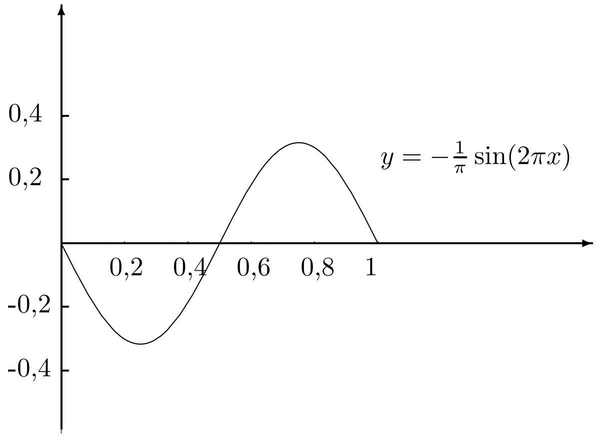
La prédiction de Gauss n'est qu'une prédiction, ce n'est pas une preuve du tout, et on aimerait bien en avoir une preuve, après tout. Trouver une méthode qui donne une estimation des nombres premiers que l'on puisse prouver s'est révélé très difficile. Quand une telle méthode est enfin apparue, elle est venue d'une direction complètement inattendue.

Les nombres premiers et la musique

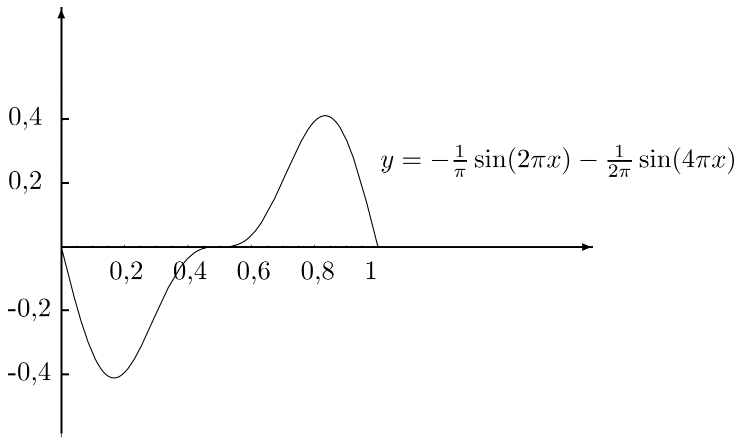
Nous commençons par un sujet qui apparemment n'a pas de rapport : comment transmet-on des signaux qui ne sont pas des « ondes » ? Nous avons tous entendu parler des « ondes radios » et des « ondes sonores », et en effet, le son se transmet sous la forme d'une onde, mais le son que nous produisons ne me semble pas très ondulatoire ; au contraire, il apparaît comme brisé, morcelé, entrecoupé d'arrêts et de soubresauts. Comment s'opère la conversion sous forme d'onde ? À titre d'exemple, considérons une ligne qui monte progressivement :



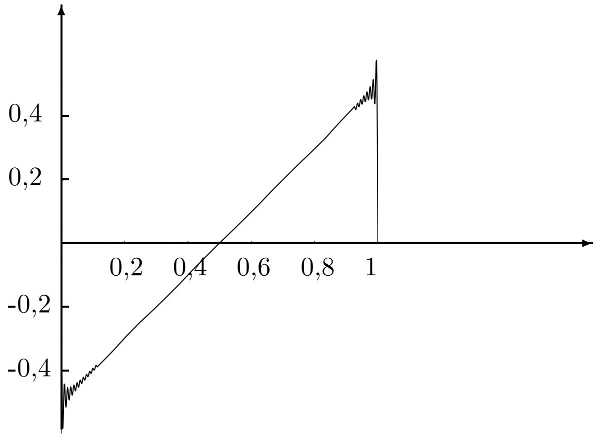
Si nous l'approchons à l'aide d'une sinusoïde, le mieux que nous puissions faire ressemble à ceci :



La partie centrale constitue une bonne approximation de la ligne droite, mais l'approximation est mauvaise pour $x < \frac{1}{4}$ et $x > \frac{3}{4}$. Comment faire pour améliorer les choses ? L'idée est « d'ajouter » à la première sinusoïde une seconde qui effectue deux cycles complets au lieu d'un à l'intérieur de notre intervalle. En ajoutant une telle sinusoïde à celle de la figure précédente, on obtient l'approximation améliorée suivante :



On peut continuer ainsi, en superposant de plus en plus de sinusoïdes afin d'améliorer sans cesse notre approximation de la ligne droite. Voici la superposition de 100 ondes sinusoïdales soigneusement choisies :



C'est une bonne approximation de la droite de départ, même si on voit qu'aux extrêmités, l'approximation n'est pas tout à fait aussi bonne (ce problème ennuyeux et incontournable est connu sous le nom de « phénomène de Gibbs »).

Comme on peut s'en douter à partir des figures ci-dessus, l'approximation obtenue sera d'autant meilleure que l'on utilisera un grand nombre de sinusoïdes. Pour le son, peut-être une centaine d'ondes fera l'affaire ; pour les transferts de données, il en faudra peut-être plus. De toute façon, pour obtenir une transmission « parfaite », il faudrait utiliser une infinité d'ondes sinusoïdales, ce que l'on obtient à l'aide de la formule

$$x - \frac{1}{2} = -2 \sum_{n \geqslant 1} \frac{\sin(2\pi n x)}{2\pi n} \quad \text{pour } 0 < x < 1.$$

Une magnifique formule, quoique sans utilité pratique (puisqu'en pratique, nous ne pouvons pas additionner une infinité de termes) !

La formule révolutionnaire de Riemann

Le grand géomètre Riemann n'a écrit qu'un seul article qui puisse être considéré comme relevant de la théorie des nombres, mais l'impact de ce court mémoire s'est exercé pendant 140 ans, et les idées qu'il contient sont le fondement de ce que nous appelons aujourd'hui la théorie analytique des nombres. Traduite dans notre langage, l'idée de Riemann est simple, quoique plutôt surprenante : *essayer de compter les nombres premiers comme une somme de* *sinusoïdes.* Sa formule précise est un peu trop technique pour cet exposé, mais on peut s'en faire une bonne idée à partir de l'approximation suivante :

$$(*)\qquad \frac{\text{cardinal de l'ensemble des nombres premiers inférieurs à } x - \displaystyle\int_2^x \frac{dt}{\ln t}}{\dfrac{\sqrt{x}}{\ln x}} \approx -1 - 2 \sum_{\substack{\gamma>0 \text{ et } \frac{1}{2}+i\gamma \\ \text{est un zéro de } \zeta}} \frac{\sin(\gamma \ln x)}{\gamma}$$

Remarquez que le membre de gauche de cette formule est suggéré par la conjecture de Gauss : c'est le terme d'erreur quand on compare la conjecture de Gauss au nombre effectif de nombres premiers inférieurs à x, divisé par ce qui, d'après nos données, ressemble à l'ordre de grandeur de l'erreur commise, à savoir $\frac{\sqrt{x}}{\ln x}$ (ce qui est proche de $\sqrt{x}$, notre première conjecture).

Le membre de droite de la formule ressemble beaucoup à notre formule pour $x - \frac{1}{2}$. Il fait intervenir une somme de fonctions sinusoïdales où $2\pi n$ est remplacé en deux endroits par γ : dans le sinus (l'inverse de la « longueur d'onde ») et au dénominateur (l'inverse de « l'amplitude »). Il y a aussi le facteur -2 dans les deux formules. Cependant, la définition des γ ici, est bien plus subtile que les simples $2\pi n$, et nécessite une explication.

La fonction zêta de Riemann est définie par :

$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + ...$$

où $s = \sigma + it$ est un nombre complexe. La série converge absolument quand $\sigma > 1$; et il n'est pas évident au premier abord de savoir s'il s'agit là d'une vraie borne pour le domaine de définition d'une fonction de ce type. En fait, la très belle théorie du « prolongement analytique » nous dit qu'il est souvent possible de définir de façon raisonnable une fonction pour tout $s \in \mathbb{C}$ à condition qu'elle soit déjà définie dans une partie de $\mathbb{C}$; et c'est ce qui se passe ici pour ζ. En d'autres termes, il est possible de définir ζ dans le plan complexe tout entier (voir [17] pour les détails).

Nous allons maintenant nous intéresser aux « zéros » de ζ, c'est-à-dire aux valeurs de s pour lesquelles $\zeta(s) = 0$. On peut montrer que :

$$\zeta(-2) = \zeta(-4) = \zeta(-6) = ... = 0$$

(que l'on appelle les « zéros triviaux »), et que tous les autres $s = \sigma + it$ pour lesquels $\zeta(\sigma + it) = 0$ satisfont à la condition $0 \leqslant \sigma \leqslant 1$.

Dans son mémoire, Riemann a énoncé une conjecture remarquable (« l'hypothèse de Riemann ») :

$$\text{si } \ \zeta(\sigma + it) = 0 \text{ avec } 0 \leqslant \sigma \leqslant 1 \text{ alors } \ \sigma = \frac{1}{2} \ ;$$

c'est-à-dire que les zéros non triviaux de ζ se trouvent sur la droite $\mathrm{Re}\,(s) = \frac{1}{2}$. Cela conduit à la définition des γ dans notre formule ; ce sont les valeurs de γ

pour lesquelles $\zeta(\frac{1}{2}+i\gamma)=0$. On a démontré qu'il existe une infinité de tels γ, aussi, pourriez-vous vous demander de quelle façon on calcule cette somme infinie. C'est simple : additionnez selon les valeurs croissantes de $|\gamma|$ et cela marchera.

La formule (*) ci-dessus est valide si et seulement si l'hypothèse de Riemann l'est aussi. Sinon, il existe une formule analogue, mais elle est plutôt compliquée, et techniquement beaucoup moins sympathique, puisque les coefficients $\frac{1}{\gamma}$, qui sont des constantes, sont remplacés par des fonctions de x.

Aussi, nous voudrions que l'hypothèse de Riemann soit vraie, car elle donne la formule ci-dessus et que cette formule est une vraie merveille. Enrico Bombieri, l'un des grands spécialistes contemporains des nombres premiers remarque :

Que la distribution des nombres premiers puisse être [ainsi] représentée de façon aussi précise est absolument stupéfiant et d'une beauté incroyable. Voilà qui évoque une musique mystérieuse et une harmonie secrète qui composeraient les nombres premiers.

Si l'on veut, ce serait un peu comme la formule qui décompose le son en ondes sinusoïdales. Ainsi, on peut proposer une paraphrase de l'hypothèse de Riemann : *il y a de la musique dans les nombres premiers.*

L'hypothèse de Riemann : les pièces à conviction

L'hypothèse de Riemann. *Tous les zéros s de ζ tels que* $0 \leqslant \mathrm{Re}\,(s) \leqslant 1$ *satisfont à la condition* $\mathrm{Re}\ (s) = \frac{1}{2}$.

Le mémoire de Riemann (1859) ne comporte aucune indication sur la façon dont il est parvenu à cette remarquable conjecture. Il s'est contenté d'écrire : « il est très probable que tous vérifient [$\mathrm{Re}\,(s) = \frac{1}{2}$]. Il est certain qu'on pourrait souhaiter une démonstration plus rigoureuse : j'ai temporairement mis de côté mes recherches dans ce sens, après quelques brèves et vaines tentatives. » Pendant de nombreuses années, cette conjecture a servi d'illustration pour montrer quels sommets il est possible d'atteindre par la seule force de l'intelligence pure. C'était comme si Riemann était parvenu à cette prédiction, de nature très numérique, à partir d'une profonde intuition non révélée, plutôt qu'à l'aide d'un calcul terre à terre, ultime conclusion du pouvoir de la seule pensée pure.

En 1929, bien des années après la mort de Riemann, le grand théoricien des nombres Siegel apprit que la veuve de Riemann avait légué ses brouillons à la bibliothèque de l'université de Göttingen. Ce fut une vaste entreprise que de déchiffrer les vieilles notes de Riemann, mais Siegel y découvrit plusieurs perles rares. Tout d'abord, il trouva une formule d'une utilité fantastique, que Riemann n'avait pas encore complètement mise au point (et donc omise lors de la publication de son mémoire) qu'il fit alors éclore (bien qu'il lui fallût trois ans pour la démontrer, tout en ayant constamment la formule sous les yeux). En second lieu, Siegel découvrit des pages entières de calculs effectifs, dont plusieurs où il avait calculé les premiers zéros avec plusieurs décimales. Autant pour « la seule pensée pure ».

L'histoire du calcul des zéros de ζ est longue, et la question est intimement liée à plusieurs grands événements de l'histoire de la science. Lorsque les premiers ordinateurs sont devenus opérationnels, quelle est l'une des premières tâches qui leur fut confiée ? Calculer les zéros de la fonction zêta de Riemann. (Ce calcul, effectué sur l'ordinateur Mark 1 de l'université de Manchester, fut la dernière publication d'Alan Turing). Quand le Clay Math Institute a créé sept prix d'un million de dollars chacun pour la résolution de certains problèmes au cours du nouveau millénaire, c'est l'hypothèse de Riemann qui est arrivée en tête de liste (bien que, soyez-en sûrs, il existe bien des façons plus aisées de gagner un million de dollars). En novembre dernier, les premiers dix milliards de zéros avaient été calculés (par Stephan Wedeniwski de IBM, Allemagne) et chacun des derniers d'entre eux se trouve sur la droite $\mathrm{Re}\,(s) = \frac{1}{2}$. Cela semble être un assez bon gage en faveur de la véracité de l'hypothèse de Riemann, mais qui sait ? Peut-être le dix milliard et unième zéro n'est-il pas sur cette droite. Suis-je trop prudent ? Peut-être que oui, peut-être que non... Souvenez-vous que la prédiction de Gauss sur le dénombrement des nombres premiers ne devient une valeur par défaut qu'au delà de 10^{316}, qui est un nombre bien plus grand que 10^{10} (dix milliards).

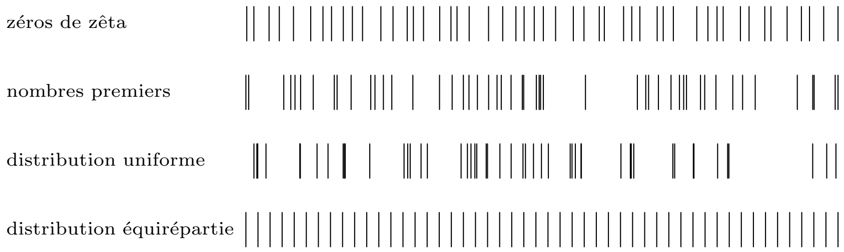
De mon point de vue personnel, la formule de Riemann évoquée plus haut est bien trop belle pour ne pas être vraie : oui, je crois qu'il y a bien une musique dans les nombres premiers.

La variance associée au dénombrement des nombres premiers : un nouveau commencement

Dans sa thèse soutenue en 1976, Julia Mueller, suivant par là un conseil de son directeur, Pat Gallagher, a repris la vieille question de la variance pour le dénombrement des nombres premiers (comparée à la prédiction de Gauss). Se souvenant que le modèle de Gauss-Cramér donne une prédiction qui ne peut être correcte, Mueller a développé l'approche de Riemann pour obtenir une meilleure idée, en considérant la question un peu plus fine de la distribution des nombres premiers dans de petits intervalles autour de x (par exemple entre x et $x+x^{\delta}$ pour des valeurs de δ comprises entre 0 et 1, ce qui est en fait plus proche de l'énoncé original de Gauss), et a établi une relation importante. À partir de son travail, Golston et Montgomery, ont fait la découverte remarquable selon laquelle une bonne compréhension de la variance *équivaut* à une compréhension préalable de l'espacement entre les couples de zéros de ζ.

Riemann a montré qu'il était équivalent de comprendre le dénombrement des nombres premiers ou de connaître les zéros de ζ, et que ce dénombrement est prévisible à partir d'une belle formule naturelle à condition que tous les zéros non triviaux soient sur la droite $\mathrm{Re}\,(s) = \frac{1}{2}$. Ces idées nouvelles permettent de penser un peu plus que l'hypothèse de Riemann est vraie. C'est en étudiant les couples de zéros et la distance qui les sépare que l'on peut comprendre en gros l'amplitude des variations dans le dénombrement des nombres premiers.

Si l'on admet l'hypothèse de Riemann, les zéros sont de la forme $\frac{1}{2} \mp i\gamma_1$, $\frac{1}{2} \mp i\gamma_2$, ... avec $0 \leqslant \gamma_1 \leqslant \gamma_2 \leqslant \gamma_3 \leqslant ...$ jusqu'à la hauteur T (c'est-à-dire, les γ_n tels que $0 \leqslant \gamma_n \leqslant T$). On pourrait se demander comment ces γ_j sont répartis sur le segment $[0, T]$. Ressemblent-ils à des nombres choisis au hasard sur cet intervalle ? Ou semblent-ils suivre un autre modèle ? Dans le diagramme ci-dessous, nous comparons les données correspondant aux zéros de ζ avec des ensembles de points dont la répartition correspond à d'autres phénomènes mathématiques.



Cinquante zéros consécutifs de la fonction zêta ; cinquante nombres premiers consécutifs à partir du millionième ; cinquante nombres distribués aléatoirement selon une loi uniforme ; cinquante nombres espacés régulièrement. D'après « Chaotic motion and random matrix theories », par O. Bohigas et M. J. Giannoni, dans Mathematical and Computational Methods in Nuclear Physics, Springer-Verlag, 1984.

Il n'est pas difficile de constater que les données correspondant aux γ_j ne ressemblent guère à une distribution aléatoire (schéma de Poisson). En fait, dans la distribution uniforme, on voit que les points s'agglomèrent de temps en temps (les rendant alors plus ou moins impossibles à distinguer), alors que les γ_j n'ont pas l'air de s'agglomérer du tout, et apparaissent mieux répartis que dans le cas uniforme. On a même plutôt l'impression que les γ_j se repoussent les uns les autres.

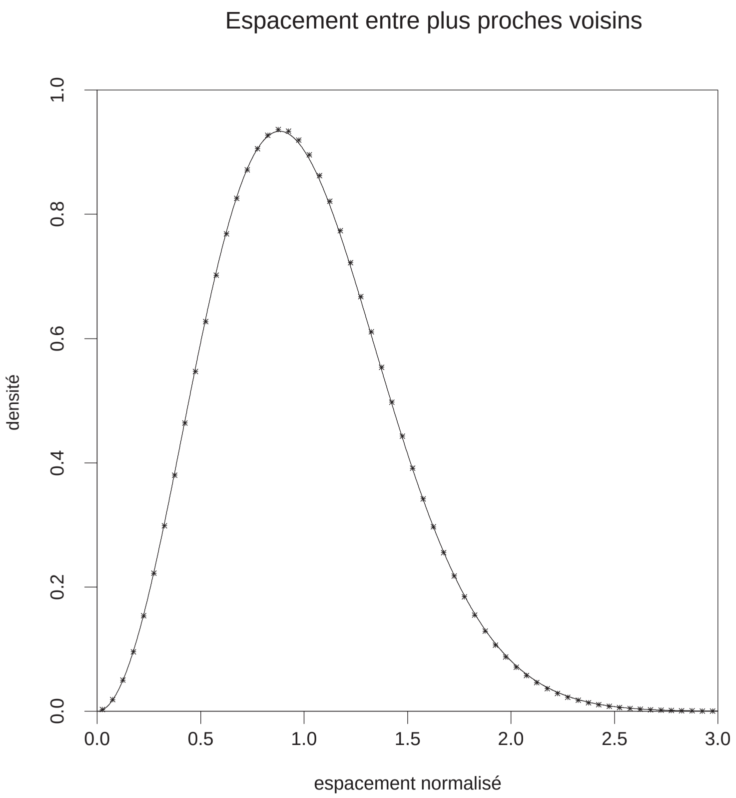
À peine deux ans plus tôt, motivé par un tout autre problème de théorie des nombres, Montgomery avait tenté de comprendre cette répartition, et énoncé pour cela une conjecture précise sur les sauts entre les zéros.

Conjecture de Montgomery (1973). Le nombre attendu de zéros dans un intervalle de longueur T multiplié par la longueur moyenne du saut qui suit un zéro, vaut

$$\int_0^T \left(1 - \left(\frac{\sin \pi u}{u}\right)^2\right) du.$$

Si les zéros étaient répartis selon une distribution uniforme, alors cette valeur vaudrait simplement T ; en fait, un examen attentif de cette conjecture montre qu'elle affirme la répulsion des zéros observée dans les quelques données de la figure précédente. Par exemple, pour des zéros obéissant à une distribution uniforme, on s'attendrait à trouver une fois sur 100 un zéro à une distance $\frac{1}{100}$ d'un zéro donné, alors que cette fréquence est d'une fois sur 911963 si la conjecture de Montgomery est vraie.

Voyons comment se comporte la conjecture de Montgomery face aux données rassemblées par Andrew Odlyzko au cours des quinze dernières années. Le graphe ci-dessous, tiré de [14], mesure en fait les « espacements entre plus proches voisins », c'est-à-dire la distribution de $(\gamma_{n+1} - \gamma_n)$ divisé par l'espacement moyen. La ligne continue suit la prédiction de Montgomery ; les points représentent les données rassemblées par Odlyzko (un graphe éparpillé). Les données reposent sur un milliard de zéros à proximité du $1,3.10^{16}$-ième zéro.



Comme cela colle bien ! On croit sûrement que la conjecture de Montgomery est vraie. Montgomery a même prouvé en partie que sa conjecture est vraie (techniquement, il a montré que la transformée de Fourier de sa fonction de répartition est la bonne dans un petit domaine, si l'hypothèse de Riemann est vraie).

La mécanique quantique entre en scène

Les progrès scientifiques se produisent parfois d'étrange manière. Quelquefois, on dirait que la même idée révolutionnaire jaillit en même temps chez deux personnes, bien qu'elles ne se soient jamais rencontrées, et sans qu'aucun changement visible ne soit apparu récemment dans le domaine ou des domaines voisins. Alors pourquoi cette simultanéité ? Les grandes idées nouvelles résultent parfois de rencontres fortuites, et c'est ce qui s'est produit dans notre domaine. Peu après avoir développé son nouveau point de vue sur le dénombrement des zéros, Montgomery est passé à Princeton, désireux en particulier de débattre de son idée avec deux grands experts de la théorie analytique des nombres, Selberg et Bombieri, tous les deux à l'Institute for Advanced Study. Pendant la semaine a lieu chaque jour à l'Institut, un thé où des gens de disciplines différentes peuvent se rencontrer et discuter d'intérêts communs. Freeman Dyson, le grand théoricien de la physique mathématique (bien qu'à l'origine théoricien des nombres), était venu au thé, et Montgomery lui expliqua ce qu'il faisait. Montgomery fut surpris de découvrir que Dyson connaissait très bien la fonction compliquée qui apparaît dans la conjecture de Montgomery, et même qu'il la connaissait dans un contexte de comparaison de sauts entre points avec le saut moyen. Cependant, et c'est ce qui est étonnant, ce n'est pas par la théorie des nombres que Dyson connaissait cette fonction, mais par la mécanique quantique. C'était précisément la fonction que Dyson avait découverte lui-même dix ans plus tôt en modélisant, du point de vue de la physique quantique, les niveaux d'énergie d'un système dynamique complexe. On pense maintenant que la même statistique décrit les niveaux d'énergie d'un système chaotique : en d'autres termes, le chaos quantique !

Pouvait-il s'agir d'une coïncidence ? Sûrement pas. Est-ce le signe de quelque chose de plus profond ? Ces questions demandent des réponses et fournissent le point de départ d'une bonne part des progrès récents.

D'un point de vue mathématique, les équations du chaos quantique sont relativement simples à développer si on les compare à celles de la théorie des nombres premiers, et par conséquent, on en savait (et on en sait toujours) beaucoup plus à leur sujet. Les observations de Montgomery et Dyson réclamaient des mathématiciens qu'ils développent de nouvelles formules pour les zéros de la fonction zêta de Riemann et qu'ils les comparent à celles du chaos quantique. Les premières choses à étudier étaient les modèles mis au point par les physiciens pour comparer les zéros proches, pas seulement deux à la fois, mais aussi trois, quatre, ou même n à la fois (ce que l'on appelle les « corrélations à n niveaux »).

Bien qu'on ait été ainsi conduit à formuler des conjectures précises sur les zéros de ζ, prouver ces conjectures, au moins en partie, constituait un obstacle sérieux que beaucoup ont tenté de franchir malgré la difficulté et les déceptions... Il a fallu plus de vingt ans pour que Rudnick et Sarnack réalisent leur percée en 1996, et démontrent que le résultat de Montgomery n'était pas une simple analogie (si l'on admet l'hypothèse de Riemann, la transformée de Fourier de la fonction des corrélations à n niveaux prévue est la bonne fonction, dans un petit domaine : en fait, ce domaine est l'analogue exact de celui de Montgomery). Désormais, les théoriciens des nombres étaient bien obligés de croire qu'au moins certaines des prédictions issues d'analogies avec le chaos quantique devaient être correctes, et tout un flot de recherches s'en est suivi.

Toujours en 1996, deux mathématiciens physiciens, Bogolmony et Keating, ont redécouvert la prédiction de Montgomery et Dyson (pour les corrélations à n niveaux sans aucune restriction sur le domaine), à partir d'un nouveau point de vue (qui avait été envisagé par [12] dans le cas $n = 2$). Ils sont partis d'une conjecture classique de théorie analytique des nombres, la version de Hardy-Littlewood de la conjecture sur les k-uplets de nombres premiers, pour montrer qu'elle conduisait à la même conclusion. Maintenant, le doute n'était plus permis, il fallait que ces conjectures soient correctes !

Les mathématiciens au travail : l'école de Sarnak

Les conjectures de Montgomery et Dyson nous disent que les zéros de la fonction ζ de Riemann se « comportent » plutôt comme des nombres qui apparaissent dans certaines questions sur le chaos quantique. Bien que les niveaux d'énergie quantique varient selon les systèmes chaotiques, il est remarquable d'observer que ces niveaux d'énergie sont distribués selon seulement une poignée de possibilités.

Il y a beaucoup de types de fonctions zêta qui apparaissent en théorie des nombres : non seulement pour compter les nombres premiers, mais aussi, au cœur de certains problèmes algébriques, arithmétiques et analytiques. Par exemple, la preuve de Wiles du théorème de Fermat repose entièrement sur un certain type de fonction zêta. Toutes ces fonctions zêta ont des propriétés communes avec l'originale : elles ont des zéros « triviaux » faciles à identifier, et tous les autres zéros sont situés dans une « bande critique » (comme $0 \leqslant \mathrm{Re}\,(s) \leqslant 1$). Pour citer une propriété supplémentaire, la plus importante, nous pensons que tous leurs zéros non triviaux se trouvent sur une droite critique (comme $\mathrm{Re}\,(s) = \frac{1}{2}$), c'est-à-dire une « Hypothèse de Riemann ». Sarnak a été intrigué par la question de savoir si les sauts entre les zéros des autres fonctions zêta sont également prévisibles à l'aide de cette même poignée de distributions issues du chaos quantique.

Avec Rubinstein, ils ont effectué des calculs à grande échelle et ont découvert une excellente corrélation entre la répartition des zéros de plusieurs fonctions zêta et les niveaux d'énergie de divers systèmes chaotiques. Ensuite, Katz et Sarnak ont imaginé se livrer à des expériences sur d'autres données, plutôt différentes, mais intéressantes pour des théoriciens des nombres : par exemple, que dire du plus petit zéro de chacune des fonctions zêta ? Pourraient-ils être distribués selon l'une de ces distributions magiques ? Les données expérimentales imposaient un modèle chaotique quantique pour cette question et plusieurs autres (voir [9]). Enfin, ils ont étudié les analogies des fonctions zêta qui apparaissent en géométrie algébrique, domaine bien éloigné du chaos quantique. Ces fonctions ont un nombre fini de zéros, et elles vérifient l'analogue approprié de l'Hypothèse de Riemann (certains optimistes pensent que les preuves de ces résultats pourraient indiquer la direction à suivre pour l'Hypothèse de Riemann : beaucoup d'entre nous ont des doutes). Katz et Sarnak se sont dits que, puisque l'Hypothèse de Riemann est vraie pour ces fonctions zêta (résultat dû à Deligne), ils pourraient peut-être aller un peu plus loin en démontrant l'analogue de la conjecture de Montgomery sur la corrélation entre couples (de zéros), ou même la conjecture de Montgomery et Dyson.

Dans l'un des travaux récents de théorie des nombres les plus remarquables, Katz et Sarnak ont accompli leur programme ([10]), en utilisant les résultats de Deligne de façon peut-être inattendue mais extrêmement ingénieuse. Les quatre cents pages de leur livre feront date : motivés par des prévisions incertaines à partir du chaos quantique, ils ont démontré un résultat profond sur les fonctions zêta dans un domaine complètement indépendant. C'est merveilleux !

Les physiciens au travail : l'école de Berry

Au même moment où une nouvelle génération de théoriciens des nombres, conduite par Peter Sarnak, apprenait à exploiter ces connexions de façon nouvelle et passionnante, la nouvelle génération de physiciens-mathématiciens, avec à sa tête Sir Michael Berry et ses collaborateurs de l'université de Bristol, a adopté une approche nouvelle et plus agressive pour développer les analogies entre les deux domaines. Leur philosophie est de prendre des risques et de pousser les analogies bien au-delà de ce que les mathématiciens oseraient faire. C'est une attitude complètement différente, que je trouve très séduisante et un peu provoquante. Ils regardent des équations dont ils savent qu'elles ne peuvent être justifiées rigoureusement, mais dont ils tirent néanmoins beaucoup d'informations utiles.

Les principaux développements sont parus dans une séries d'articles de Michael Berry et Jon Keating, et peut-être contiennent-ils la carte des progrès futurs sur les nombres premiers. Ce qu'ils affirment n'est pas toujours d'une grande exactitude, mais je suis sûr qu'ils sont près de la vérité, et, sur plusieurs questions, ils formulent des conjectures là où nous-autres, théoriciens des nombres, n'avions aucune idée.

Le flot des idées ne coule pas non plus dans une direction unique. Plus prudemment, la théorie des nombres premiers permet d'énoncer plusieurs formules assez précises (comme la formule de Riemann-Siegel citée plus haut), qui ont permis de corriger et de modifier les formules analogues du chaos quantique obtenues de façon plus informelle.

La dernière génération de physiciens-mathématiciens, conduite par Jon Keating et Nina Snaith va encore un peu plus loin, et cela peut-être très utilement. Ils visent l'un des plus grands mystères de la fonction zêta de Riemann : quelle est sa borne supérieure sur un grand intervalle de la droite $\mathrm{Re}\,(s) = \frac{1}{2}$? En procédant avec grand soin, ils formulent des conjectures concernant des questions importantes sur lesquelles les spécialistes de théorie des nombres étaient restés impuissants.

En résumé, le côté plus intuitif du chaos quantique permet de faire des prédictions plus fructueuses sur la répartition des nombres premiers (et au-delà). D'autre part, le développement plus prudent de la théorie des nombres premiers conduit à des conjectures plus précises dans le domaine du chaos quantique. Cette intéraction mutuellement bénéfique entre deux domaines jusqu'ici indépendants, est une nouvelle tendance passionnante, et de nombreux chercheurs se tournent désormais vers ces questions dans chacun des deux domaines. C'est là exactement la raison d'être d'une institution comme le Mathematical Sciences Research Institute : le moment venu, nous avons l'occasion de rassembler les deux communautés en personne, ce qui autrement serait impossible, et d'accélérer ainsi les progrès.

Beaucoup de bruit pour rien ?

Oublions un instant tous ces progrès, ces généralisations, ces nouvelles formules passionnantes. Et le problème à un million de dollars ? Parmi ces nouvelles idées, y en a-t-il une qui nous permette de mieux attaquer l'Hypothèse de Riemann ? Avons-nous amélioré nos chances de voir enfin ce problème succomber ? Il y a seulement quelques années, en 1995, le grand Atle Selberg, en théorie analytique des nombres, déclarait :

Il y a eu très peu de tentatives pour prouver l'Hypothèse de Riemann parce que personne n'a jamais eu réellement une bonne idée à son sujet.

Il y a une vieille idée de Hilbert et Pólya pour prouver l'Hypothèse de Riemann, qui consiste à trouver un système de chaos quantique dans lequel tout zéro de la fonction zêta de Riemann correspondrait à un niveau d'énergie (ils l'ont énoncé dans un langage assez différent). Si un tel système de chaos quantique existe, il doit posséder plusieurs propriétés très particulières. Récemment, Berry et Keating ont même donné des conditions plus restrictives pour un tel système (en associant les nombres premiers aux orbites périodiques du système chaotique), ce qui pourrait bien indiquer la voie pour le trouver. C'est ce qui a peut-être poussé Berry, un preu chevalier s'il en est, à affirmer en 2000 :

j'ai le sentiment que l'Hypothèse de Riemann tombera dans les prochaines années. Je vois les fils s'assembler.

Il se peut qu'il ait raison bien que je soupçonne la preuve d'être encore loin. Néanmoins, ces nouvelles découvertes sont les plus passionnantes qui soient apparues depuis longtemps et promettent, à tout le moins, une bien meilleure compréhension de la fonction zêta de Riemann.

Remerciements

Merci à Malcolm Adams, Bob Anderson, Steve Donnelly, Cari Gervin, Dan Goldston, Will Kazez, Jon Keating, Gene and Rebecca McCarthy and K. Soundararajan pour leur aide dans la préparation de cet exposé et de cet article.

Références

[1] C. Bays and R. H. Hudson, *A new bound for the smallest x with $\pi(x) > li(x)$*, Math. Comp. **69**, (2000), 1285–1296.

[2] M.V. Berry and J.P. Keating, *The Riemann zeros and eigenvalue asymptotics*, SIAM Rev. **41**, (1999), 236–266.

[3] E.B. Bogomolny and J.P. Keating, *Random matrix theory and the Riemann zeros, II : n-point correlations*, Nonlinearity **9**, (1996), 911–935.

[4] H. Cramér, *On the order of magnitude of the difference between consecutive prime numbers*, Acta Arith. **2**, (1936), 23–46.

[5] P.C.W. Davies and J.R. Brown, *The ghost in the atom.* Cambridge University Press, 1986.

[6] C.F. Gauss, *Letter to Encke.* Reproduced in L.J. Goldstein's "*A history of the prime number theorem*" Amer. Math. Monthly **80**, (1973), 599–615.

[7] D.A. Goldston and H.L. Montgomery, *Pair correlation of zeros and primes in short intervals*, in *Analytic number theory and Diophantine problems*, (Stillwater. OK. 1984), Prog. Math. **70**, 183–203, Birkhäuser, 1987.
[8] A. Granville, *Prime races*, to appear.
[9] N.M. Katz and P. Sarnak, *Zeroes of zeta functions and symmetry*, Bull. Amer. Math. Soc. (N. S.) **36**, (1999), 1–26.
[10] N.M. Katz and P. Sarnak, *Random matrices. Frobenius eighenvalues and monodromy*, AMS Colloquium Publications **45**, Amer. Math. Soc., 1999.
[11] J.P. Keating and N.C. Snaith, *Random matrix theory and* $\zeta(\frac{1}{2}+it)$, Comm. Math. Phys. **214**, (2000), 57–89.
[12] H.L. Montgomery, *The pair correlation of zeros of the zeta function*, Proc. Symp. Pure Math. **24**, Amer. Math. Soc., (1973), 181–193.
[13] J.H. Mueller, *Primes and zeros in short intervals.* Thesis, Columbia University, (1976).
[14] A.M. Odlyzko, *The* 10^{20}*−th zero of the Riemann zeta function and* 70 *million of its neighbors*, (1989), to appear.
[15] B. Riemann, *Über die Anzahl der Primzahlen unter einer gegebenen Grösse*, Monatsberichte der berliner Akademie, November 1859.
[16] Z. Rudnick and P. Sarnak, *The n-level correlations of L-functions*, C. R. Acad. Sci. Paris Sér. I Math. **319**, (1994), 1027–1032.
[17] E.C. Titchmarsh. *Theory of functions.* Oxford University Press, 1938.

Pour en savoir plus, voici une petite liste non exhaustive de références sur le sujet.

P. Biane, *La fonction zêta de Riemann et les probabilités.* In *La fonction zêta.* Édité par Nicole Berline et Claude Sabbah. Éditions de l'École Polytechnique, 2003. (Voir la liste de références qui figure à la fin de cet article).

J. Brian Conrey, *The Riemann hypothesis*, Notices Amer. Math. Soc. **50** (2003), no. 3, p. 341–353.

M. Demazure, *Cours d'algèbre*, Nouvelle bibliothèque mathématique. Éd. Cassini, 1997.

W. Ellison, M. Mendès France, *Les nombres premiers.* Actualités scientifiques et industrielles. Éd. Hermann, 1975.

J. P. Kahane, *Une formule de Fourier sur les nombres premiers.* Gazette des mathématiciens **67**, janvier 1996.

M. Mendès France, G. Tenenbaum, *Les nombres premiers.* Que sais-je ? vol. **571**. Presses Universitaires de France, 1997.

W. Neudecker, D. Williams, *The 'Riemann hypothesis' for the Hawkins random sieve*, Compositio Math. **29**, p. 197–200, 1974.

S. J. Patterson, *An introduction to the theory of the Riemann zeta-function*, Cambridge Studies in Advanced Mathematics **14**. Cambridge University Press, Cambridge, 1988.

W. Sierpinski, 250 *problèmes de théorie élémentaire des nombres*, Éd. Jacques Gabay, 1970.