Article extrait de la REE 2013-5

Le 13 novembre 2013

Les nombres premiers en première ligne

Jean-Pierre Hauet

Membre émérite de la SEE

Depuis des siècles, le mystère des nombres premiers fascine. De grands noms des mathématiques ont fait faire des progrès considérables à leur compréhension : Euclide, Eratosthène, Euler, Gauss, Riemann, Legendre, Tchébychev, Hadamard, La Vallée Poussin, Hilbert… sans oublier les mathématiciens contemporains : André Weil, Hughes Montgomery, Jean-Pierre Serre, Alain Connes, Grigori Perelman et bien d'autres.

Les nombres premiers restent au centre de grands défis et en particulier des trois conjectures qui constituaient le 8e problème de Hilbert :

- l'hypothèse de Riemann ;
- la conjecture de Goldbach ;
- la conjecture des nombres premiers jumeaux.

Aucune de ces trois conjectures n'est formellement démontrée aujourd'hui. Toutefois, Il y a de bonnes raisons de s'y intéresser à nouveau et en particulier à celle de Riemann qui fait partie des sept défis du Millénaire lancés en 2000 par le Clay Mathematical Institute et dont six restent non résolus à ce jour[1].

On notera tout d'abord que des progrès importants ont été réalisés en 2013 sur les deux dernières conjectures.

La conjecture de Goldbach (1742), selon laquelle « *Tout nombre entier pair supérieur à 3 peut s'écrire comme la somme de deux nombres premiers* », semble avoir été démontrée en mai 2013 dans sa version faible « *Tout nombre impair supérieur ou égal à 9 est somme de trois nombres premiers impairs* » par le mathématicien péruvien Harald Helfgott, chargé de recherches à l'Ecole normale supérieure de Paris. La démonstration est en cours de validation.

La conjecture des nombres premiers jumeaux selon laquelle *il existerait une infinité de nombres premiers p et p' tels que p'=p+2*, n'est toujours pas démontrée mais le mathématicien chinois Yitang Zhang a démontré une version faible de cette conjecture en établissant en mai 2013 qu'il existait une infinité de paires de nombres premiers qui diffèrent l'un de l'autre de 70 000 000 au plus.

Evidemment, on voudrait que ces 70 000 000 soient ramenés à 2, mais l'existence même de cette preuve jointe aux travaux d'Helfgott montre que quelque chose « bouge » autour des nombres premiers et que l'on n'est pas à l'abri de découvertes plus importantes. On pense donc à nouveau à la fameuse conjecture de Riemann.

Pures spéculations intellectuelles, dira-t-on. Pas vraiment, car la conjecture de Riemann débouche sur des considérations qui peuvent être d'un intérêt primordial dans d'autres domaines que les mathématiques, la cryptographie et la physique quantique notamment. De quoi s'agit-il ?

La conjecture de Riemann

La conjecture de Riemann (1859) a trait à la fonction Zêta (s) de Riemann qui étend au domaine des nombres complexes (notés s = x + i y) la classique série d'Euler :

$$\zeta(s)=1+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4^s}+\ldots=\sum_{n=1}^{\infty}\frac{1}{n^s} \qquad (1)$$

[1] La conjecture de Poincaré a été résolue en 2003.

Il n'est pas possible de calculer directement la fonction $\zeta(s)$ pour toutes les valeurs de s. En particulier, on sait que la série est divergente si l'on prend s égal à 1 sur l'axe des réels. Le point 1 est une singularité de la fonction. Mais il est possible de contourner cette singularité en remplaçant la formulation analytique de la fonction (1) par une équation fonctionnelle dont l'expression fait sens pour toute valeur de s prise en dehors du pôle s=1 et dont la solution s'identifie à l'expression (1) lorsque cette dernière peut être calculée. On parle alors de *prolongement analytique.*

Riemann a montré que l'équation fonctionnelle constituant le prolongement analytique de $\zeta(s)$ pouvait s'écrire :

$$\pi^{-\frac{s}{2}}\,\Gamma\left(\frac{s}{2}\right)\zeta(s)=\pi^{-\frac{1-s}{2}}\,\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s) \quad (2)$$

formule dans laquelle la fonction Γ d'Euler prolonge la fonction factorielle ! à l'ensemble des nombres complexes. Elle a du sens partout dans le plan complexe en dehors de s=1.

Pour des raisons explicitées plus loin, Riemann s'est intéressé aux **zéros de la fonction** $\zeta(s)$.

L'équation fonctionnelle (2) est invariante par rapport à la transformation $s\rightarrow(1-s)$. La fonction $\zeta(s)$ présente donc une symétrie par rapport à la droite $x=\frac{1}{2}$. Il est facile de démontrer que la fonction ne peut pas s'annuler si la partie réelle x est > 1. Il en ira donc de même si x < 0. Cela élimine donc deux demi-plans dans la recherche des zéros de $\zeta(s)$ (figure 1).

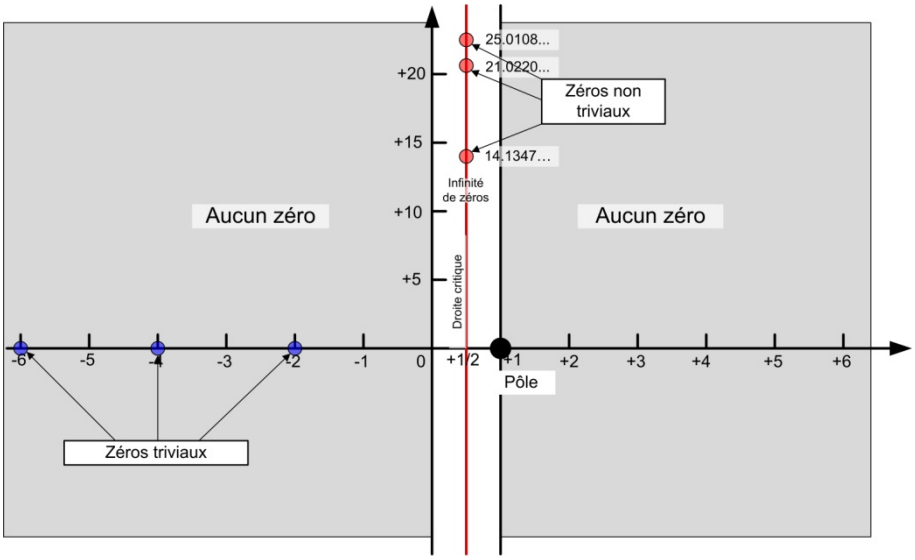

Figure 1 : Les zones clés de la recherche des zéros de la fonction Zêta.

Une exception importante cependant : si $s=-2,-4,-6\ldots$ le facteur $\Gamma\left(\frac{s}{2}\right)$ dans le membre de gauche de l'équation (2) devient infini alors que le membre de droite reste borné. Il faut donc que pour ces points la fonction $\zeta(s)$ soit nulle : c'est qu'on appelle les ***zéros triviaux*** de $\zeta(s)$.

Mais il existe des ***zéros non triviaux*** qui, pour les raisons exprimées ci-dessus, ne peuvent se trouver que dans la bande [0,1]. La conjecture de Riemann consiste à affirmer que tous ces zéros sont situés sur la médiane $x=\frac{1}{2}$. On a de fait calculé un nombre considérable de zéros le long de cette droite : des centaines de milliards, en commençant par 14.1347…, 21.0220…, 25.0108… etc. Mais on n'a jamais pu trouver de zéros en dehors de la droite $x=\frac{1}{2}$ sans jamais parvenir cependant à prouver qu'il n'en existait pas. De plus, la statistique de la répartition de ces zéros sur la fameuse droite a quelque chose de bizarre : le 4 088 664 936 217^{e} zéro n'est distant de son

suivant que $\delta = 0.00001709$ sur l'axe des y. Voilà qui rappelle étrangement le phénomène des nombres premiers jumeaux…

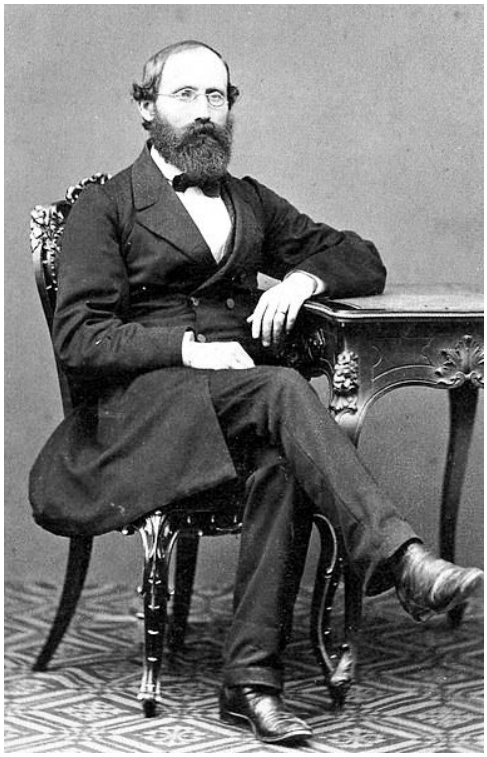

Figure 2 : Georg Friedrich Bernhard Riemann (1826 – 1866).

Fonction de Riemann et nombres premiers

Depuis fort longtemps, on sait que la fonction de Riemann (et son ancêtre la fonction d'Euler) constitue un pont entre l'analyse et l'arithmétique, c'est-à-dire entre le continu et le discret. Grâce au théorème fondamental de l'arithmétique[2], on peut démontrer assez facilement l'identité d'Euler permettant de transformer la somme de Riemann en un *produit infini étendu aux seuls nombres premiers* (3) :

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1 - \frac{1}{p^s}} \qquad (3)$$

[2] Tout entier strictement positif peut être écrit comme un produit de nombres premiers d'une unique façon, à l'ordre près des facteurs. Par conséquent, toute fraction $\frac{1}{n^s}$ peut s'écrire $\frac{1}{p^s q^s}$ dans laquelle p et q sont premiers.

où les nombres p sont premiers.

On comprend que la fonction d'Euler et celle de Riemann aient été perçues comme des moyens de pénétrer le mystère des nombres premiers et en particulier celui de leur répartition.

Cette répartition est usuellement caractérisée par la fonction $\pi(x)$ qui compte le nombre de nombres premiers inférieurs ou égaux à un nombre x donné. Depuis toujours, on sait que les nombres premiers se raréfient au fur et à mesure que x croit.

En 1808, Legendre avait proposé la relation :

$$\pi(x) \sim \frac{x}{\ln x} \qquad (4)$$

Gauss, pratiquement simultanément, proposa l'approximation, qui devait se révéler plus précise :

$$\pi(x) \sim \mathrm{Li}(x) \qquad (5)$$

formule dans laquelle $\mathrm{Li}(x)$ est le logarithme intégrale de x défini par :

$$\mathrm{Li}(x) = \int_0^x \frac{dt}{\ln t} \qquad (6)$$

x	$\pi(x)$	$\mathrm{Li}(x)$
10	4	6
100	25	30
1 000	168	178
10 000	1 226	1 246
100 000	9 592	9 630
1 000 000	78 498	78 628
10 000 000	664 579	664 918
100 000 000	5 761 455	5 762 209
1 000 000 000	50 847 534	50 849 235
10 000 000 000	455 052 511	455 055 615
100 000 000 000	4 118 054 813	4 118 066 401
1 000 000 000 000	37 607 912 018	37 607 950281

Tableau 1 : Comparaison entre la fonction $\boldsymbol{\pi(x)}$ et le logarithme intégral. Dans cette table, le logarithme intégral est toujours supérieur à $\boldsymbol{\pi(x)}$ mais on sait qu'il n'en va pas ainsi pour des valeurs de x extrêmement élevées. Source : Gilles Lachaud.

Ces formules (4) et (5) ne seront démontrées que beaucoup plus tard et pratiquement simultanément, par Jacques Hadamard et

Charles de la Vallée Poussin (1896), après qu'ils auront établi que $\zeta(s)$ ne possédait pas de zéro sur $x=1$.

Riemann avait l'idée que la répartition des zéros non triviaux de la fonction Zêta commandait celle des nombres premiers. Il cherchait donc à réduire l'écart subsistant entre la fonction $\pi(x)$ telle qu'elle était observée et la fonction $\mathrm{Li}(x)$ telle qu'elle pouvait être calculée. Riemann est alors parvenu à un résultat remarquable.

Ce résultat consiste en la démonstration d'une formule *explicite* qui est une relation complexe établissant une identité formelle entre une fonction $f(x)$ dérivée de la fonction $\pi(x)$ et une expression dans laquelle l'écart à $\mathrm{Li}(x)$ s'exprime comme la sommation d'un terme complexe faite sur l'ensemble des zéros non triviaux de la fonction $\zeta(s)$. Cette formule n'a pas d'intérêt direct pour le calcul puisqu'elle suppose une sommation sur un ensemble qu'on ne connait pas de façon précise. Mais elle établit de façon irréfragable un lien entre deux mondes : la statistique des zéros de la fonction Zêta et la répartition des nombres premiers.

Partant de là, il a été démontré plus tard (Von Kock - 1901) que l'écart entre $\pi(x)$ et $\mathrm{Li}(x)$ pouvait être majoré par un multiple constant, aussi petit que l'on veut, de $(\ln x\sqrt{x})$ quand $x\to\infty$ et que cette estimation était la meilleure possible.

Mais… tous ces résultats demeurent subordonnés à la validation de la conjecture de Riemann ! Cette validation viendrait conforter bon nombre d'hypothèses faites jusqu'à présent et permettrait de relancer les investigations sur les nombres premiers dans de nouvelles directions.

Quel intérêt pour les technologies qui nous intéressent ?

La confirmation de l'hypothèse de Riemann ouvrira de nouvelles voies au moins dans deux domaines.

La cryptographie

On connait l'importance des nombres premiers dans les méthodes de chiffrement modernes, en particulier dans l'algorithme de chiffrement à clés asymétriques dénommé RSA qui repose sur l'extrême difficulté, supposée, de factoriser en nombres premiers des très grands nombres.

Il n'y a pas de raisons de supposer, comme cela a été fait dans certaines publications, que la démonstration de l'hypothèse de Riemann puisse du jour au lendemain rendre facile cette factorisation et donc caducs bon nombre de systèmes de protection. Aujourd'hui, l'algorithme RSA serait davantage menacé par la mise au point d'ordinateurs quantiques disposant d'une quantité de qubits intriqués suffisante (peut-être de l'ordre de 80) pour supporter des algorithmes quantiques, tels que l'algorithme de Peter Shor, capables de factoriser les grands nombres en un temps beaucoup plus court que les algorithmes classiques. Nous n'en sommes pas là, même si le sujet est considéré dans beaucoup de pays comme un très grand thème de recherches.

Par contre, il est probable que la validation de l'hypothèse de Riemann s'accompagnera de progrès importants des connaissances sur les nombres, sur la distribution des nombres premiers, sur les méthodes de factorisation, etc. Il est vraisemblable que de tels progrès auront des retombées considérables sur la conception des techniques de chiffrement, éventuellement sur les méthodes de craquage, surtout, bien entendu, si l'ordinateur quantique venait à devenir simultanément opérationnel.

La théorie des nombres premiers et la physique

Plusieurs approches ont tendu ces dernières années à établir un parallèle entre la théorie des nombres premiers et un certain nombre de phénomènes physiques. La fonction Zêta de Riemann fournit un modèle de relations entre le discret et le continu. N'en va-t-il pas de même de la mécanique quantique ? La répartition des nombres premiers ne serait-elle dès lors que l'une des manifestations d'une loi plus générale gouvernant notre

univers ? Les travaux d'André Weil et de Pierre Deligne les ont d'ailleurs conduit à étudier la transposition de la fonction Zêta sur d'autres corps que celui des complexes et à conjecturer puis à montrer que sur ces corps particuliers la transposée de l'hypothèse de Riemann était vraie.

Revenant à la physique, Riemann lui-même, en travaillant sur sa formulation explicite, avait montré que le fameux écart entre $\pi(x)$ et $\mathrm{Li}(x)$ pouvait être approximé par une série de signaux sinusoïdaux du type $\sum_n \cos(\gamma_n x)$, expression dans laquelle γ_n désignent l'ensemble des coordonnées des zéros de $\zeta(s)$ sur l'axe imaginaire, ces zéros étant supposés être de la forme

$$\rho_n = \frac{1}{2} + i\gamma_n \qquad (7)$$

On voit ainsi apparaître l'idée que les zéros de la fonction de Riemann résulteraient de la combinaison de phénomènes vibratoires autour de l'axe $x = \frac{1}{2}$ dont les γ_n seraient les pulsations propres.

Cette idée fut reprise par David Hilbert puis George Polyà vers 1930 qui émirent l'hypothèse selon laquelle les γ_n pouvaient correspondre aux valeurs propres d'un opérateur hermitien[3] appliqué à l'espace de Hilbert constitué par l'ensemble des « vibrations » associées aux zéros de $\zeta(s)$. Publiée par Hugh Montgomery en 1973, cette hypothèse est connue sous le nom de « conjecture de Hilbert-Polyà ».

Toujours en 1973, après une conversation avec Freeman Dyson, Hugh Montgomery réalisa que la distribution supputée des écarts successifs entre zéros non triviaux de $\zeta(s)$ était asymptotiquement identique à celle de l'espacement entre les valeurs propres des matrices hermitiennes aléatoires qui sont utilisées en mécanique quantique pour caractériser les niveaux d'énergie des systèmes atomiques complexes.

On sait en effet que *« D'après la théorie quantique, les niveaux d'énergie d'un système atomique sont les valeurs propres d'un opérateur hermitien dans l'espace de Hilbert : le Hamiltonien du système. Lorsque le système atomique contient beaucoup de particules élémentaires, il y a une profusion de niveaux d'énergie et le Hamiltonien est trop complexe pour être diagonalisé numériquement. C'est dans ce contexte que le physicien E. Wigner a eu l'idée de modéliser les niveaux d'énergie d'un tel Hamiltonien par les valeurs propres d'une matrice hermitienne aléatoire de grande taille[4]. L'espoir de Wigner était que les propriétés statistiques des niveaux d'énergie, par exemple la distribution de leurs écartements, coïncideraient avec celles des matrices aléatoires.*

Après de nombreux travaux théoriques et expérimentaux l'intuition de Wigner s'est révélée fondée.» (Source : Philippe Biane).

Cette proposition qui lie les valeurs propres de $\zeta(s)$ aux niveaux quantiques des systèmes atomiques est désormais connue sous le nom de loi de Montgomery-Odlyzko. Elle a fait l'objet de vérifications par le calcul jusqu'à un ordre élevé mais elle reste empirique.

Depuis lors, des travaux très importants sont menés pour essayer de conforter cette relation étrange entre le monde des nombres et celui des particules. On ne sait pas si c'est la conjecture de Riemann qui permettra de démontrer la conjecture d'Hibert-Polyà, ou l'inverse. Mais on pressent qu'il y a là une relation forte et d'autres investigations, vers les bruits roses notamment, laisse penser qu'il existe une forme supérieure d'ordre qui nous échappe encore.

[3] Dans une base orthonormale, la matrice d'un opérateur hermitien est égale à la transposée de sa conjuguée. Les opérateurs hermitiens jouent un rôle important en mécanique quantique, car ils représentent les grandeurs physiques.

[4] Une matrice aléatoire est une matrice dont les coefficients sont aléatoires. Si ceux-ci obéissent à des distributions normales indépendantes, les matrices correspondantes constituent l'ensemble GUE (Gauss Unitary Ensemble).

Ce trop bref article, pour un sujet aussi difficile, ne clôt pas le débat et n'a pas la prétention de la rigueur scientifique. Il vise simplement à appeler l'attention de nos lecteurs sur une question essentielle où les progrès sont attendus dans les prochaines années viendront éclairer notre compréhension du monde, à moins qu'ils ne nous plongent dans un abime encore plus grand de perplexité.

Jean-Pierre Hauet