Hypothèse de Riemann

Peter Sarnak

Conférence du prix du millénaire du CMI
Harvard, 15 avril 2026.

ÉNONCÉ (RIEMANN 1859)

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

(FACTORISATION UNIQUE)

S'étend en une fonction holomorphe (sauf pour un pôle simple en $s = 1$) de la variable complexe s et satisfait

Équation fonctionnelle :

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

Hypothèse de Riemann (RH) : Tous les zéros de $\zeta(s)$ ont $\Re(\rho) = \frac{1}{2}$.

- Comme l'a découvert Siegel (1932), Riemann a calculé les premiers zéros et a vérifié qu'ils satisfaisaient son hypothèse. Comment ? Il avait besoin d'une bonne approximation de $\zeta(s)$ dans $0 < \Re(s) < 1$. Connue maintenant sous le nom de formule de Riemann–Siegel, qui reste la référence absolue dans ce type de calculs (conducteur jusqu'à 10^{12}).

$$\frac{1}{2\pi i} \int_{\gamma} \frac{f'(z)}{f(z)} dz = 1$$

- Le plus grand zéro qui semble avoir été calculé se situe autour du 10^{36}ième zéro (Böser–Hiary). Tous les zéros calculés satisfont RH et sont simples (sinon, nous ne pourrions pas le vérifier numériquement).

Pour Riemann, c'était une hypothèse de travail

Puisqu'avec elle, il pouvait accomplir son objectif à partir de sa formule explicite :

$$\psi(x) := \sum_{p \leq x} \log p = x - \sum_{\rho} \frac{x^{\rho}}{\rho}$$

(tous les zéros) que $\psi(x) \sim x$ quand $x \to \infty$. C'est le théorème des nombres premiers (PNT).

Bien que Riemann n'ait pas revisité son hypothèse à notre connaissance, son approche du PNT via $\zeta(s)$ a conduit à une preuve de ce dernier par Hadamard et de la Vallée Poussin (1896). Ils ont montré que

$$\Re(\rho) < 1 \quad \text{pour tout zéro } \rho.$$

RH possède les caractéristiques d'un bon problème :

(a) Élégant ; facile à énoncer ; attrayant.

(b) Falsifiable.

Mais pourquoi tout ce tapage ?

- Démontrer RH serait une réalisation monumentale. Gagner le prix Clay et bien plus encore.
- Nous nous attendons à ce que cela entraîne de nouvelles compréhensions sur les entiers et que cela s'applique à des fonctions zêta plus générales ci-dessous. Sinon, ce serait décevant, car $\zeta(s)$ elle-même concerne la distribution archimédienne des nombres premiers, qui est limitée.

Une conséquence nette typique est :

$$\text{Presque tous les intervalles } [x, x + (\log x)^2]$$

contiennent un nombre premier (Selberg, 1943).

- **Infirmer RH** en trouvant un ρ avec $\Re(\rho) > \frac{1}{2}$ et à une hauteur disons 10^5 devrait rapporter le prix (mais lisez attentivement les petits caractères juridiques de Clay !).
- **Quel serait l'impact ?** (Nick Treffen)

— Curieusement, en raison d'une caractéristique de "répulsion des zéros" et des zéros de Landau–Siegel, un tel ρ pourrait probablement être utilisé pour résoudre certaines questions d'effectivité.

- Mais le réel impact serait pour ceux comme Museuf qui croient que RH et bien plus sont vrais : un tel zéro ferait éclater notre bulle.
- Bien que les preuves numériques en faveur de RH semblent très convaincantes, il convient de tempérer cela par la "complexité" : la densité locale des zéros à la hauteur T n'est que $\log T$, ce qui n'est pas si grand.

Hypothèse de Riemann généralisée (GRH)

La fonction zêta de Riemann a des généralisations naturelles aux fonctions zêta de Dedekind et aux fonctions L de formes automorphes sur GL_n. L'analogue de RH pour celles-ci est une hypothèse de travail puissante et, si elle est vraie, une caractéristique profonde des nombres d'ondes.

Pour $K/\mathbb{Q}$ une extension de degré n et de discriminant Δ_K, sa fonction zêta est

$$\zeta_K(s) = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s} = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1}.$$

Statistiques (disons que K a r_1 plongements réels) :

$$Z_K(s) := |\Delta_K|^{s/2} \left(\pi^{-s/2}\right)^{r_1} \zeta_K(s) = Z_K(1-s).$$

Ici $D = \Delta_K$ est le "conducteur" mesurant la complexité de la ramification, et $\log D$ est la complexité en termes de densité locale des zéros.

GRH affirme que les zéros de $Z_K(s)$ (et de toutes les fonctions L automorphes) ont leur partie réelle égale à $\frac{1}{2}$.

La base de données des fonctions L et des formes modulaires : www.lmfdb.org contient une richesse d'informations sur ces fonctions zêta de petit conducteur et de petit n, y compris des vérifications de GRH.

La théorie analytique moderne des fonctions L consiste en des approximations de GRH :

- Théorèmes de non-annulation.
- Théorèmes de densité.
- Sous-convexité.

Qui servent souvent de substituts à GRH dans les applications.

Un exemple :

PNT en supposant RH (Riemann)	Démontré de manière inconditionnelle (1896).
Il existe un algorithme en temps polynomial en $\log n$ pour déterminer si un grand n est premier ou non en supposant GRH (Miller, 1975)	De manière inconditionnelle Agrawal–Kayal–Saxena (2002).
La conjecture d'André–Oort concerne la fermeture de Zariski d'une suite de points spéciaux (points CM) dans les variétés de Shimura. Résolue par Edixhoven, Klingler–Yafaev en supposant GRH (2014).	De manière inconditionnelle Pila–Shahkar–Tsimerman (Esnault–Groechenig) (2022). Cependant, pour rendre la preuve inconditionnelle effective, on a besoin de GRH.

- Polynômes irréductibles sur $\mathbb{Q}$:

$$P(x) = x^d + a_1 x^{d-1} + \cdots + a_d x + 1$$

avec $a_j \in \{0, 1\}$ choisis avec probabilité $1/2$ (i.i.d.). Alors, en supposant GRH,

$$\text{Prob}(P \text{ est irréductible}) \to 1 \quad \text{quand } d \to \infty$$

(démontré par Breuillard–Varjú ; conjecturé par Odlyzko–Poonen).

- Équations diophantiennes cubiques : Un problème critique central est de donner des bornes fines pour le nombre d'entiers $(x_1, \ldots, x_6) \in \mathbb{Z}^6$, $|x_j| \leq T$, satisfaisant

$$x_1^3 + x_2^3 + x_3^3 = x_4^3 + x_5^3 + x_6^3.$$

Hua a montré $N(T) \ll T^{7/2}$. Hooley, en supposant GRH pour les fonctions zêta de Hasse–Weil des 3-variétés associées :

$$N(T) \ll T^{3+\varepsilon}, \quad \varepsilon > 0$$

ce qui est optimal en exposant.

Analogues

Le cadre dans lequel de grands progrès ont été réalisés est celui des **corps de fonctions**.
Les rationnels $\mathbb{Q}$ sont remplacés par $k = \mathbb{F}_q(t)$, corps fini. Les entiers par les polynômes $\mathbb{F}_q[t]$. Premiers : polynômes irréductibles.

$$\text{Norme}(f) = q^{\deg f}, \qquad T = q^{-s}.$$

$$\sum_{(f)} \text{Norme}(f)^{-s} = \sum_{(f)} T^{\deg f} = \frac{1}{(1-T)(1-qT)}.$$

Si K est une extension finie de k (ou une courbe sur $\mathbb{F}_q$), alors sa fonction zêta prend la forme :

$$Z_K(T) = \frac{P_K(T)}{(1-T)(1-qT)}.$$

P_K a pour degré $2g$, où g est le genre de K ; donc # de zéros est $2g$.

$$Z_K(T) \quad \text{a une équation fonctionnelle invariante sous } T \mapsto \frac{1}{qT}.$$

Artin a construit l'analogue de GRH : tous les zéros ont $|\rho| = \sqrt{q}$.

Weil a formulé et conjecturé des généralisations aux variétés de $\sqrt{q}$. Les preuves de celles-ci sont l'un des points forts des mathématiques du 20e siècle.

- Weil pour les courbes.
- Grothendieck, Deligne pour les variétés.

Crucial pour ces développements est la **linéarisation** qui réalise les zéros comme valeurs propres du morphisme de Frobenius $x \mapsto x^q$ agissant sur les groupes de cohomologie.

Il est à noter que le passage de la linéarisation à la démonstration que les zéros se trouvent sur une droite (ou un cercle) est une étape majeure (pas de "miracle" de type Hilbert–Pólya avec auto-adjoint). En général (Deligne), cela implique de déformer la variété dans une famille et d'utiliser la colle de la symétrie de monodromie pour passer de l'un à tous.

Vérification des critères d'un bon problème : GRH

(a) Élégante et falsifiable.
(b) Si elle est vraie, c'est une vérité puissante sur les nombres.
(c) Elle a des analogues et des généralisations profonds dans des domaines connexes.

RH et GRH : Où en sommes-nous aujourd'hui ?

Je passe en revue quelques éléments et j'ajoute à ma conférence de Bristol 2018 "Commentaire et comparaisons de quelques approches de GRH".

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_p (1-p^{-s})^{-1}.$$

(i) Le membre de gauche permet d'étudier $\zeta(s)$ en utilisant la structure additive de $\mathbb{R}$ et de $\mathbb{Z}$ en tant que sous-groupe discret à quotient compact. En particulier, la formule de sommation de Poisson conduit aux propriétés analytiques.

(ii) Le membre de droite capture la structure multiplicative de $\mathbb{Z}$.

Le fait que l'on doive utiliser à la fois (i) et (ii) est rendu clair par

Davenport–Heilbronn (1936) (pas de produit eulérien) : Soit $Q(x,y)$ une forme quadratique binaire entière de discriminant $d<0$ pour laquelle $R(d)$ est impair et différent de 1. Alors

$$Q_0(s)=\sum_{(x,y)\neq(0,0)} Q(x,y)^{-s}$$

a une infinité de zéros dans $\Re(s)>1$.

Deligne (1980) a montré que $Q_0(s)$ a une proportion positive de ses zéros sur $\Re(s)=\frac{1}{2}$ (en accord avec son résultat sur $\zeta(s)$), montrant que de tels résultats sont de nature statistique.

Mélanger efficacement les structures additive et multiplicative reste un défi.

- Dans les 30 ou 50 premières années après l'article de Riemann, on ne savait pas s'il s'agissait d'un problème difficile ou non (comme Riemann lui-même l'a exprimé). Cependant, il est désormais clair que s'il existe une solution élémentaire, elle est bien cachée.
- Il existe de nombreuses équivalences de RH dans la littérature. Il est difficile de prédire si l'une d'entre elles apporte des éclaircissements ou non. Tant qu'elles ne produisent pas de nouveaux résultats ayant des applications dans la lignée de RH en tant qu'hypothèse de travail, leur pertinence reste floue.

Par exemple, si $\lambda(n)=(-1)^{\Omega(n)}$ est la parité du nombre total de facteurs premiers de n, alors

(i') $\sum_{n\leq x}\lambda(n)=o(x)$ quand $x\to\infty$ est équivalent au PNT.

(ii') $\sum_{n\leq x}\lambda(n)=O\left(x^{\frac{1}{2}+\varepsilon}\right)$ pour tout $\varepsilon>0$ est équivalent à RH.

Bien que des preuves élémentaires de (i') aient été trouvées, plus récemment une jolie preuve ergodique par Richter et McNamara (2021), celles-ci apportent peu à la version quantifiée (ii').

(ii') dit que les $\lambda(n)$ ont des valeurs ±1 imitant des valeurs aléatoires, mais montrer des caractéristiques aléatoires dans quelque chose d'explicite est difficile.

- Avec le succès de la linéarisation par les méthodes cohomologiques dans le corps de fonctions, on pourrait espérer quelque chose de similaire sur $\mathbb{Q}$.
- Une indication prometteuse de la nature spectrale des zéros des fonctions zêta est le **Dyson–Montgomer (1973)**. Les statistiques d'espacement local

$$\text{(c'est-à-dire si } \rho=\frac{1}{2}+i\gamma,\quad \log T\,(\gamma-\gamma') \text{ correspondant à } \rho,\rho' \text{ avec } \gamma\sim T)$$

des zéros élevés de (toutes les) fonctions zêta suivent les lois statistiques des matrices hermitiennes aléatoires : **GUE**.

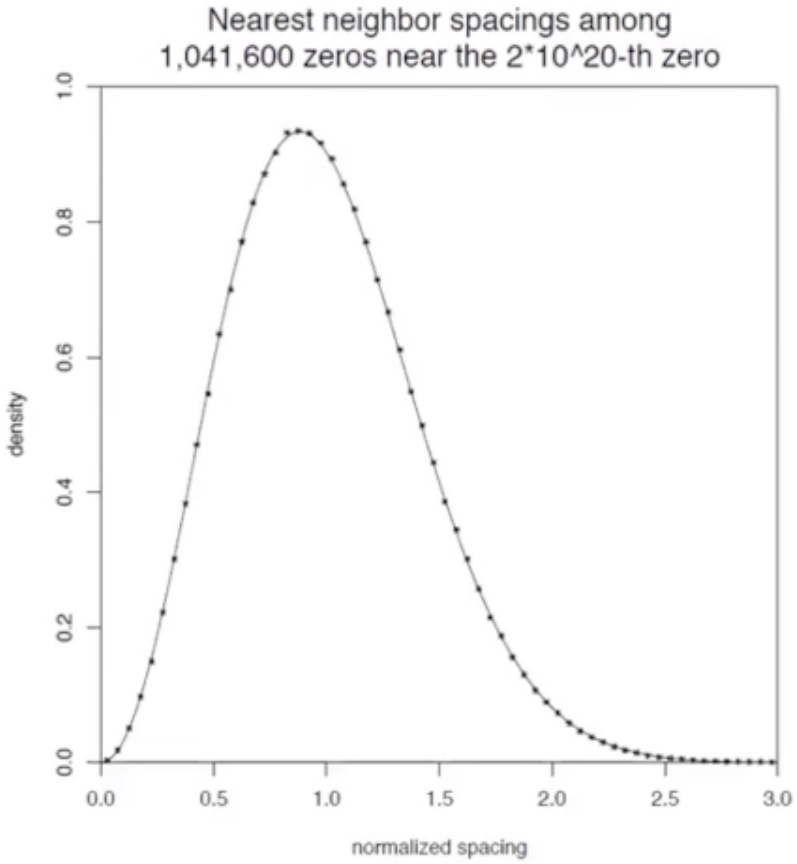

Figure : Espacements entre plus proches voisins parmi 1 041 600 zéros près du $2 \cdot 10^{20}$*-ième zéro.* (densité vs espacement normalisé)

- Cela a été vérifié numériquement et théoriquement dans des plages restreintes (en supposant GRH). C'est très convaincant et a conduit à une étude active de ces statistiques des fonctions zêta ainsi que de familles de celles-ci.
- La source dans le corps de fonctions d'une telle connexion est comprise (Katz–Sarnak, 1998) et provient des limites d'échelle des groupes de monodromie de familles de fonctions zêta.
- Une linéarisation qui a été suggérée par Paul Cohen en 1977 et qui a été avancée par Connes (1999) et Meyer (2005) est une action de la multiplication sur l'addition sur certains espaces d'adèles/idèles.

Anneau des Adèles de $\mathbb{Q}$ (additif) :

$$\mathbb{A} = \{(a_\infty, a_2, a_3, \dots) \mid a_p \in \mathbb{Z}_p \text{ pour } p \neq 0\}.$$

Anneau des Idèles :

$$\mathbb{A}^* = \left\{ (a_\infty^*, a_2^*, a_3^*, \dots) \mid a_p^* \in \mathbb{Q}_p^* \text{ pour } p \neq 0 \right\}.$$

Les espaces standards sont (les "vecteurs de valuation")

$$\mathbb{A}/\mathbb{Q}, \quad \mathbb{A}^*/\mathbb{Q}^*.$$

Considérons $\mathbb{A}^*/\mathbb{Q}^*$, un quotient très singulier. L'action

$$x \mapsto xy, \quad y \in \mathbb{A}^*/\mathbb{Q}^*, \quad x \in \mathbb{A}^*/\mathbb{Q}^*$$

mélange les structures.

On peut introduire des espaces vectoriels topologiques appropriés de fonctions sur $\mathbb{A}^*/\mathbb{Q}^*$ tels que la trace de l'action ci-dessus donne la formule explicite de Riemann–Guinand–Weil (Meyer). En particulier, on a les zéros des fonctions L interprétés comme valeurs propres de cette action.

Connes, arXiv :2602.04022 donne une mise à jour sur la façon d'utiliser une telle interprétation spectrale. Y est également incluse une lettre divertissante adressée au professeur Bernhard Riemann. Aucune contradiction autre que des erreurs de calcul n'est ressortie de ces travaux.

Il existe une autre espèce de fonctions zêta (ou L) qui proviennent de **formes automorphes transcendantes** (cuspidales) sur $\mathrm{GL}_n/\mathbb{Q}$ qui sont partout non ramifiées (formes de Maass). Ces formes insaisissables sont les blocs de construction de la théorie et n'existent qu'à cause de la "place archimédienne". Ce sont des fonctions propres d'opérateurs différentiels sur les espaces localement symétriques

$$X_n = \mathrm{SL}_n(\mathbb{Z}) \backslash \mathrm{SL}_n(\mathbb{R}) / \mathrm{SO}_n(\mathbb{R}).$$

Les "conducteurs analytiques" de leurs fonctions zêta, c'est-à-dire les densités locales de leurs zéros, impliquent leurs valeurs propres.

GRH $\Rightarrow$ des bornes très fortes pour leurs valeurs propres ainsi qu'une rareté de telles formes. En particulier, dans la limite $n \to \infty$, cela implique des propriétés de concentration très fortes pour les fonctions sur le cœur de X_n quand $n \to \infty$.

Grand n : cette limite n'a pas été sondée. Ce sera un véritable test de résistance, et je crois que c'est un test pour GRH.

Compte tenu de ses implications très fortes, GRH devrait être mise à l'épreuve dans des limites extrêmes et pour les différentes espèces de fonctions zêta.

Ramification dans la limite $n \to \infty$: Le décompte local du nombre de zéros de $\zeta_K(s)$ est contrôlé par

$$\log N_K = \text{"log du conducteur"}.$$

Ainsi, conjointement avec GRH, cela donne des bornes inférieures très fortes pour le conducteur de ramification en fonction du degré n de K (Stark, Odlyzko, ...). Ces bornes sont bien plus précises que celles issues de la géométrie des nombres (Minkowski). Au point qu'elles frôlent la violation de constructions explicites de tours à faible ramification (Golod–Shafarevich).