

## Transcription par outils d'ia de la conférence de Peter Sarnak à l'occasion de la conférence célébrant les 100 ans de Jean-Pierre Serre

[...] <sup>1</sup>

Nous disposons de la machinerie de croissance qui permet de se passer de formes automorphes tout en comprenant tous les problèmes.

Dans le cas des corps de nombres, Riemann utilisait des fonctions thêta, et les formes automorphes sont précisément la manière dont on construit les objets dont je veux parler. Il s'agit donc d'une conjecture, d'une supposition, comme je l'ai dit, et je souhaite approfondir le sujet. Ainsi, toutes les fonctions  $L$  qui généralisent les fonctions zêta de Riemann sont supposées être les fonctions  $L$  principales pour  $GL(n)$ .

Les fonctions  $L$  principales constituent une représentation standard. Lorsque Hecke, et peut-être Riemann avant lui, définissaient les fonctions zêta, ils n'avaient pas de groupe dual et donc pas de  $Ls\pi p$ . Il existe une représentation du groupe dual.

Je vais me limiter à la fonction  $L$  standard, car, par conjecture, toute fonction  $L$  et toute fonction zêta sont censées être un produit de ces fonctions. Je cherche à comprendre l'aspect analytique de ce phénomène. Quels sont donc ces objets ? Je vais prendre le temps de les définir, mais j'aborderai d'abord quelques cas simples. Si vous n'êtes pas familier avec ce concept, soyez patients.

Nous allons donc examiner le groupe linéaire général d'un corps. On considère un espace de Hilbert, l'espace d'un groupe d'adèles, et on s'intéresse aux objets invariants par les points rationnels du groupe. On les décompose en éléments irréductibles ; c'est la définition. Ces éléments irréductibles apparaissent dans l'espace cuspidal, d'où le terme "forme cuspidale", qui est central dans ce cours. Je ne donne pas la définition car si vous ne l'avez jamais vue, elle ne vous sera d'aucune utilité, et si vous la connaissez déjà, elle est superflue. Sachez simplement que, parmi tous les sous-groupes paraboliques rationnels, les radicaux unipotents de tous les sous-groupes paraboliques ont des périodes nulles.

Donc, vous imposez cet ensemble infini de conditions linéaires et il se peut qu'il ne vous reste rien. C'est une question à un million de dollars, comme vous le verrez dans un instant. Quoi qu'il en soit, nous décomposons en éléments irréductibles. La théorie des nombres est née de cette périodicité sous  $GL(n, \mathbb{Q})$ . Ces éléments irréductibles sont alors des représentations irréductibles des groupes locaux  $GL(n_q, V)$ ,  $V$  un corps fini et  $GL(n, \mathbb{R})$ .

Ces concepts sont désormais bien compris. Concrètement, il s'agit ici de  $GL(n)$ , mais pour les groupes réels, Harish-Chandra a posé les bases, Langlands a introduit certains paramètres, et si l'on déramifie le groupe (le conducteur traitant de la ramification par rapport à la non-ramification),

---

Denise Vella-Chemla utilisant les outils d'ia Downsub et Turboscribe, 15 septembre 2026.

1. *J'ai oublié d'allumer audacity au tout début de la conférence de Peter Sarnak.*

on obtient les paramètres de Satake, ou classe de conjugaison semi-simple dans  $GL(n, \mathbb{C})$ , qui sont les paramètres de la représentation et apparaissent dans le facteur local des fonctions  $L$ . Lorsqu'on ramifie le groupe, des calculs beaucoup plus subtils sont nécessaires, et j'en parlerai brièvement, mais je vais supposer des bornes standard pour étayer mon point de vue analytique. La fonction  $L$  locale En tout lieu fini, est de la forme produit 1 moins ces racines au lieu non ramifié, ces paramètres de Satake, sinon vous devez être plus prudent avec les paramètres de Langlands et certains de ces alphas peuvent être 0 et là où vous avez ramifié, il y aura un nombre magique, dont je vais parler, et c'est le conducteur.

Il existe une situation similaire à l'infini. Si l'on dispose du facteur archimédien de la fonction  $L$ , il s'agit d'un produit de fonctions gamma réelles. Je travaille sur  $\mathbb{Q}$ , qui ne possède qu'une seule complétion réelle. Ces fonctions gamma sont  $\Gamma\left(\frac{s}{2}\right)$ , soit  $p/2$ , et  $\Gamma\left(\frac{1+s}{2}\right)$ . Riemann nous a fourni ce facteur, et les  $J$  sont maintenant positionnés dans la formulation suivante :  $\gamma s + \mu\pi i$ . Je reviendrai plus tard sur la position de ces paramètres ; il s'agit de la conjecture de Ramanujan, mais la formulation est similaire à celle de Riemann : on prend le produit des facteurs locaux, qui constitue la partie finie.

Mon point de vue est de toujours distinguer le fini de l'infini. Ainsi, concernant la fonction  $L$ , si vous consultez un ouvrage de référence sur Jacquet, par exemple (il est le maître incontesté de la fonction  $L$ ), vous constaterez que la fonction  $L$  inclut tous les points, la partie archimédienne n'étant pas isolé. Or, pour moi, il est absolument distinct, et vous comprendrez pourquoi. Quant à la partie finie de la fonction zêta de Riemann, Riemann ne l'a pas définie avec le facteur gamma ; il l'a définie comme  $n^{-s}$ . Il ne faut donc pas la modifier. D'ailleurs, nous utilisons  $S$ , et non  $Z$ . L'ia proposera probablement une démonstration plus concise, incluant alors  $Z$ .

Très bien, donc la fonction  $L$  complète que j'appelle  $\lambda$ , ce n'est peut-être pas la meilleure notation, mais le plus important est que cette fonction possède un prolongement analytique et une équation fonctionnelle, étant donné une représentation cuspidale, ou la représentation automorphe cuspidale, la représentation contragradiente est une représentation qui correspond à l'involution,  $G$  devient  $G$  transposée inverse sur  $GL(\mathbb{N})$ , et c'est la dualité, vous changez  $s$  en  $1 - s$  et  $p$  en  $\tilde{p}$ , et puis il y a des nombres magiques qui entrent en jeu ici, et c'est le conducteur, il y a un entier, un nombre naturel,  $q$ , qui à chaque endroit ramifié peut donner un facteur, il donne un facteur, mais aux endroits non ramifiés, il vaut 1, c'est comme ça, donc cela implique une factorisation de  $Q_p$ , et j'y reviendrai, car nous allons essayer de faire quelque chose d'étrange. Donc  $Q_p$  est le conducteur, il mesure la ramification, les calculs pour le calculer sont non triviaux, et il y a aussi ce  $\tau_p$ , qui est une somme de Gauss  $\tau_p$ , tout comme dans le travail de Riemann, le travail de Dirichlet,  $\tau_p \hat{\tau}_p$ , contragradient est ce conducteur  $Q_p$ , et si  $p$  est auto-contragradient, alors vous aurez les carrés  $Q_p$ , et dont la racine carrée est le nombre racine, un nombre très important et délicat, un nombre très difficile à calculer, aussi difficile que de factoriser  $Q_p$ . Ces fonctions possèdent donc des propriétés analytiques, ce qui est très important, généralisant celles de Riemann. Ceci est dû à Godement et Jacquet en premier lieu. Jacquet, Shahidi, Piatetski et Shapiro ont développé la théorie sous des formes très explicites, et surtout, la fonction  $L$  de Rankin-Selberg, qui est associée. Nous ne connaissons donc pas la fonctionnalité, mais la fonction que j'utiliserai à plusieurs reprises est la fonction  $L$  de Rankin-Selberg,  $RS(p \times p')$ , qui est une nouvelle fonction  $L$ , et qui est ensuite un produit de fonctions  $L$  standard, un produit isobare.

J'utiliserai librement les propriétés analytiques de la fonction de Rankin-Selberg, développées par les mêmes auteurs, Jacquet, Piatetski, Shapiro et Shahidi. Cependant, les estimations que je ferai plus tard seront très importantes pour le conducteur  $p$ ,  $p$  premier. Ces estimations, loin d'être triviales, sont principalement dues à Bushnell et Yacht. Bon, vous avez... ah, ça a été coupé, mais ce n'est pas grave, je sais ce qui reste. La formule explicite de Guinand-Weil est au cœur de ce cours.

On peut donc prendre l'une de ces fonctions  $L$  et en écrire une formule explicite. Guinand était un mathématicien canadien qui s'intéressait aux structures arithmétiques et, pour cette raison, il a formulé cette formule avant Weil. Elle est quelque part dans les archives.

Weil l'a écrit car il s'agissait d'une approche visant à démontrer l'hypothèse de Riemann et à interpréter une formule explicite en fonction de l'influence de Frobenius ; il a d'ailleurs publié plusieurs articles dans ce sens. Je souhaite m'attarder sur cette formule explicite car elle va révéler le principe fondamental, et plus précisément ce qui m'importe le plus : le principe analytique. La formule explicite s'énonce donc comme suit.

J'ai cette fonction  $L$ ,  $L(s\mathbb{R})$ . J'écris ses zéros sous la forme  $0,5 + si$  car je souhaite que  $s$  soit réel. Ainsi, lorsque je dis que je suppose l'hypothèse de GRH, c'est parce que je suppose que ces nombres sont réels.

Cela facilitera la résolution de tout problème d'optimisation ou de tout argument de positivité que j'essaie de résoudre. La somme d'une fonction test aux ordonnées des zéros est donc égale à... Il ne s'agit pas d'une dualité de Fourier.  $g$  est à support compact.

C'est ce que représente  $s\mathbb{R}$ .  $H$  est maintenant entier, donc je peux évaluer  $H$  pour  $i/2$ , ce qui est logique. Cette formule est donc cohérente.

Pour toute fonction test  $g$ , vous autoriseriez à passer en revue tous les  $g$ , qui sont lisses ou à support compact. L'idée d'utiliser des fonctions non lisses est absurde. Ne le faites surtout pas. C'est complètement inutile. Tout ce qu'on peut faire, on peut le faire avec cette formule et prendre une limite à la fin. C'est ce que les gens essaient de faire.

Ce n'est pas... Oui, c'est mon avis. Bon, la somme des ordonnées est égale à un terme qui contient le logarithme du conducteur. Ensuite, il y a la somme de la partie archimédienne avec la dérivée logarithmique de la fonction gamma.

Puis vient le signe moins, qui correspond à une somme sur la dérivée logarithmique.  $L$  prime sur  $L$  s'écrit ici comme la somme de  $a_p(k)$ . Les  $a_p$  sont les coefficients. Le  $\lambda$  utilisé ici est différent.

L'autre a des petits gribouillis sur le côté. Celui-ci est le  $\lambda$  de von Mangoldt. C'est  $\log p$  pour  $n$  est une puissance première.

Et c'est... Dans les travaux de Riemann, on retrouve déjà cette fonction. Elle provient de la dérivée logarithmique. Il s'agit simplement d'un calcul de décalage de contour.

Et cela vaut pour toutes les fonctions de test. C'est parfaitement équivalent à toutes les informations. Toutes les informations se trouvent dans cette formule explicite.

Et des gens essaient d'utiliser cette formule, ou plutôt, l'une des premières personnes à avoir réellement utilisé cette formule. En quelque sorte, en termes de discriminants, c'est Serre, en fait. C'est donc une des raisons pour lesquelles nous reviendrons sur ce point. S'il y a un pôle, alors l'ordre du pôle est  $\Delta_p$ .

Et si vous voulez avancer un argument de positivité, vous devez connaître l'ordre du pôle. Voici donc la formule explicite. Et je souhaite définir le conducteur, le conducteur analytique.

Vous voyez donc déjà qu'à la ligne cinq, ou quelque chose comme ça, vous avez  $\log QT$ . Supposons que je choisisse librement  $H$  d'être localisé près du point zéro. On obtient alors  $\log q$  multiplié par l'intégrale de  $H$  sur  $R$ . La densité locale des zéros de cette fonction  $L$ , près du centre est donc égale au logarithme du conducteur issu de la ramification finie.

Il y a ensuite cette autre partie, la dérivée logarithmique. Si l'on veut comprendre la densité locale de zéros au voisinage du centre, le logarithme du conducteur sera égal à ce nombre. Cela me permettra de définir le conducteur analytique, qui est le concept intégrant la partie archimédienne.

Si vous travaillez dans un corps de fonctions, il n'existe pas de lieu archimédien. C'est une différence fondamentale, même pour formuler la conjecture de Langlands. Il existe ici un groupe important, appelé  $L_F$ , le groupe de Langlands, qui est censé être une extension du groupe de Galois.

Et je vais vous expliquer pourquoi c'est si difficile dans le cas archimédien. C'est là toute la différence. Iwaniec et moi travaillions sur différents problèmes.

Dans ce que j'appellerai le cas "dompté", je vais parler de cas "dompté" et "non dompté". Dans le cas "dompté", j'entends les modèles linéaires généralisés ( $GL(n)$ ), où  $M$  est borné. C'est comme les corps de degrés bornés.

Et puis, plus tard, nous laisserons  $M$  tendre vers l'infini. C'est une limite qui, à mon avis, n'a pas été suffisamment étudiée, et c'est là que je compte aller finalement. Nous avons donc donné la définition, qui découle de la compréhension du nombre de zéros proches de la moitié le logarithme du conducteur devrait être égal à ce nombre.

Nous avons donc défini le conducteur archimédien de cette manière précise. Depuis, cette définition a subi quelques modifications. Je crois même qu'elle a changé dans l'ouvrage de Kowalski et Ivanich, pour une raison qui m'échappe.

Vous n'auriez pas dû le modifier. Cela ne change rien dans le cas d'une configuration simple, mais c'est radicalement différent si l'on autorise  $M$  à tendre vers l'infini. Ils ont ajouté un 3 à cet endroit.

Je me trompe peut-être. Quelqu'un a ajouté un 3 quelque part. Bon, si  $p$  est non ramifié, je tiens



à souligner que ces formes automorphes, dont je parlerai plus tard, étaient partout non ramifiées.

Partout. Elles existent peut-être même. Donc, si nous sommes non ramifiés à l'infini, cela signifie que nous sommes une représentation qui possède des paramètres de Satake, et si les paramètres de Satake sont tous nuls, alors je tiens à souligner que le conducteur archimédien,  $C_\infty$ , est supérieur ou égal à 1. Bien sûr, le conducteur fini est un nombre naturel, donc un entier supérieur ou égal à 1. Ceci n'est pas un entier, mais une quantité supérieure ou égale à 1. Il s'agit d'une mesure de complexité.

Et si tous les  $\mu_j$  sont nuls, donc je ne place rien à l'emplacement archimédien, alors cette représentation a tous les  $\mu_j$  égaux à 0, et c'est une représentation qui apparaîtrait dans une représentation de Galois paire, totalement paire. J'ai commencé le cours par impair. La théorie est impaire. J'essaie d'être équilibré. Les personnes équilibrées sont ici. Certaines d'entre elles, dans ce cas précis, sont probablement algébriques.

En fait, Weil donne une définition de ce qu'il entend par paramètres algébriques des représentations, dont ceci serait un exemple. Ils sont censés être algébriques. Mais je tiens à souligner que cela se pose dans ce cas précis, et dans le cas où tous les  $\mu_j$  seraient nuls, ce qui correspondrait à une représentation de Galois impaire, totalement paire et irréductible, alors ce facteur, le conducteur archimédien, serait égal à 1. J'essaie donc de le normaliser correctement.

Le logarithme de ce mesure donc la densité des zéros proches de  $\frac{1}{2}$ . Précisons que, dans le cas dompté, cette notion de conducteur archimédien a été éprouvée et, à mon avis, a résisté à de nombreuses évolutions, que je souhaite souligner. La première concerne les familles domptées : je fixe un produit eulérien de degré  $m$ , de forme parabolique, et je peux faire varier une famille, un sous-ensemble, l'ensemble entier, la famille universelle, en les ordonnant selon le conducteur analytique. C'est là le but recherché.

Dans le cadre de l'hypothèse de Riemann généralisée (HRG), un phénomène remarquable se produit. C'est l'une des applications les plus courantes et les plus puissantes de cette hypothèse, qui permet d'obtenir des résultats considérables : le conducteur est censé représenter la complexité de la fonction  $L$ , et c'est très important... En fait, le conducteur est le conducteur analytique, mais le nombre de zéros, qui correspond au degré, est une fonction à part entière.

Il y a bien une notion de genre dans la théorie de Hadamard, mais je cherche simplement à calculer le nombre de zéros proches du centre. On verra, lorsque j'aborderai le corps des fonctions, que cela correspond au degré du polynôme. Le degré est donc le conducteur, et le logarithme du conducteur représente ici le degré de cette fonction. C'est sa complexité.

Voici une démonstration élémentaire remarquable, bien connue dans la littérature sous diverses formes, qui utilise la théorie de Rankin-Selberg (que j'ai dit utiliser librement ici). La question est donc : les  $pa_p$  déterminent-ils le complet ? J'examine donc les  $a_2$ ,  $a_3$  et  $a_5$ . Combien de ces valeurs dois-je connaître pour avoir la réponse complète ? Il me suffit de connaître le logarithme du carré des coefficients du conducteur analytique. Log.

Je suis passé d'une progression exponentielle à une progression logarithmique. D'accord, pour cela, j'ai besoin de l'hypothèse de Riemann. Nous n'allons donc pas la supposer maintenant, mais seulement pour cet exemple.

Il s'agit donc d'une question fondamentale que vous essayez de comprendre. Eh bien, je vais peut-être calculer quelques-uns de ces  $pa_p$ , et à partir de là, je pourrai peut-être vous donner la valeur de la racine. Rapidement.

En temps polynomial, car je n'ai que le logarithme. C'était un rêve que tu vas voir.

Voilà ce qui lui est arrivé. Bon, j'expliquais pourquoi on a testé et approuvé cette notion de conducteur analytique.

Donc, si vous vous demandez quelle est la valeur de la fonction  $L$  au centre, il existe une borne toujours identique en fonction de ce conducteur analytique. Il s'agit d'un conducteur à  $1/4$ , et il existe des millions de problèmes où, si l'on améliore cet exposant (on se retrouve face à un problème de sous-convexité), on résout une multitude de problèmes complètement, et non approximativement. C'est précisément pour cette raison qu'Ivanich et moi avons introduit ce conducteur analytique : afin de formuler le problème de sous-convexité de manière totalement générale.

Très bien, si ce conducteur est une mesure de complexité, de hauteur, nous appliquons en quelque sorte la théorie des hauteurs, non pas aux points, mais aux formes automorphes. Il devrait exister un nombre fini de formes automorphes dont le conducteur est inférieur à  $x$ . On pourrait donc essayer de compter le nombre de formes automorphes dont le conducteur analytique est inférieur à  $x$ , et c'est possible. Si l'on ne considérait que les caractères de Dirichlet, on se demanderait combien de caractères ont un conducteur inférieur à  $x$ .

Le conducteur est un entier sans facteur carré, et vous cherchez à déterminer combien d'entiers sans facteur carré inférieurs à  $x$  existent. C'est facile à calculer : il suffit de compter le nombre de formes automorphes sur  $GL(m)$ ,  $m \geq 2$ , et d'utiliser la formule de la trace. J'y reviendrai souvent. Il y a aussi ce remarquable travail de Brumley et Milicevic, datant de quelques années, qui démontre ce qu'ils appellent une formule de Weyl-Schanuel : le nombre de formes automorphes ordonnées par conducteur analytique présente un comportement asymptotique.

C'est tout à fait naturel, ce qui correspond au nombre de caractères de Dirichlet.

Il existe un  $\phi$  de  $q$  caractères de Dirichlet, des caractères de Dirichlet primitifs pour chaque  $q$ . Le nombre total de caractères dont le conducteur est inférieur à  $x$  est donc égal à  $\pm 1$ . Il n'existe pas de conducteur analytique pour les nombres rationnels, car le cas archimédien ne contient que des éléments triviaux. Ainsi, le nombre de caractères dont le conducteur est inférieur à  $x$  est simplement une constante multipliée par  $x^2$ , ce qui est cohérent avec ce résultat. Je tiens à souligner un point, car il s'agit d'un thème récurrent dans le domaine des fonctions  $L$ , et Serre l'a certainement exploré sous tous ses aspects.

Supposons que j'examine ces fonctions  $L$  dont la conductance tend vers l'infini, et que localement

la densité soit logarithmique de la conductance au voisinage de la moitié. Je procède alors à une renormalisation, j'attribue des mesures de probabilité aux zéros, et je cherche à déterminer la mesure limite obtenue. Dans une famille de fonctions  $L$  bien ordonnée, la distribution limite sera toujours uniforme par rapport à  $dt$  si l'on suppose l'hypothèse de Riemann. En revanche, si je mets les zéros à l'échelle par le logarithme du conducteur de sorte qu'ils soient espacés approximativement avec une moyenne de un, alors il existe une toute nouvelle théorie liée à la théorie des matrices aléatoires, et ce conducteur analytique la capture parfaitement.

C'est ce que Katz et moi avons fait il y a de nombreuses années. Nous avons compris cela dans le domaine des fonctions, puis, avec une astuce (je ne la dévoilerai pas), nous avons d'abord laissé  $q$  tendre vers l'infini. Mais j'y reviendrai plus tard ; peut-être est-il possible de procéder sans laisser  $q$  tendre vers l'infini. Quoi qu'il en soit, nous avons utilisé cette astuce, mais nous avons obtenu des résultats intéressants. Ensuite, de nombreuses personnes ont examiné ces conjectures dans le domaine des nombres, et tout semble cohérent en termes de distribution locale et de distribution d'échelle suivant quatre modèles de matrices aléatoires. Nous avons quatre limites d'échelle aléatoires, quatre types de limites d'échelle de groupes de monodromie.

Donc, je réaffirme que le conducteur analytique semble particulièrement pertinent dans le cas simple, et celui que je souhaite mettre en avant aujourd'hui est la référence absolue de Riemann. Riemann a calculé les trois premiers zéros de la fonction zêta de Riemann. Ce calcul est loin d'être trivial, car la formule de la fonction zêta, telle qu'on la connaît généralement, contient une fonction gamma.

Le premier zéro correspond à une hauteur d'environ 14,1347..., et  $\gamma = \frac{1}{2} + 14,1347 i$ , d'après la formule de Stirling, est un nombre minuscule. Cet homme ne disposait pas de beaucoup d'outils d'ia ; il a donc dû se débrouiller avec un crayon et du papier, et la méthode de référence est ce qu'on appelle une équation fonctionnelle approchée. Il n'y a rien d'approximatif là-dedans.

Cela se traduit par une terminologie complexe, mais il existe une formule permettant de calculer la valeur d'une fonction  $L$ , ou son logarithme, ou encore  $L$  prime sur  $L$ . C'est ce qu'il faisait systématiquement pour calculer les zéros de la racine carrée des intervalles du conducteur<sup>2</sup>. C'est la méthode de référence de Riemann.

Vous pouvez calculer, et cela n'a jamais été surpassé, mais vous pouvez toujours calculer la valeur, quelle qu'elle soit, avec la précision que vous souhaitez, en racine carrée du conducteur plus un demi, car il possède une formule qui implique une équation fonctionnelle, comme je l'ai dit, appelée l'équation fonctionnelle approximative, qui a une certaine longueur, et cette longueur, lorsqu'elle est équilibrée pour être aussi courte que possible, vous donne la racine carrée.

Mais il y a un hic. Cela n'est valable que si l'on peut calculer rapidement les coefficients. Or, pour Riemann, les coefficients étaient égaux à un.

Et là, Riemann est un peu différent, mais si l'on prend une fonction  $L$  de Dirichlet, personne ne sait faire mieux, ou si l'on prend une fonction  $L$  de courbe elliptique, ce que je vais faire dans un instant, alors on peut calculer rapidement les coefficients, ce qui est très pratique. Il existe donc

---

2.  $\sqrt{Q}$  ?

une méthode de référence pour Riemann, calculable au voisinage du point  $1/2$  en racine carrée des pas du conducteur. Mais nous savons déjà qu'un nombre logarithmique de coefficients détermine tout.

Vous vous demandez peut-être : “Ne puis-je pas faire mieux ? Ne puis-je pas réaliser une opération en temps polynomial ?” C’était un rêve que Rubinstein et moi partagions, et il nous a fallu quinze ans pour le concrétiser et enfin le mettre en œuvre. Et c’est ce que je veux vous montrer. Non, pas exactement.

Si vous voulez une précision de 100 décimales, il suffit de l’ajouter à l’epsilon. Riemann est doué. Il sait ce qu’il fait.

D’ailleurs, il y a toute une histoire à propos de Riemann : ce document se trouve dans ses archives. Il ne l’avait pas publié dans son journal. Et beaucoup de gens ont vu ces archives sans savoir ce qu’elles contenaient.

Il a fallu que Siegel comprenne qu’il effectuait une opération de phase stationnaire et calculait le nombre avec la précision décimale souhaitée. Ceci ne concerne que zêta et ses trois premiers zéros. Or, Rubinstein et moi-même rêvions depuis de nombreuses années du fait que la densité locale de zéros est égale au logarithme du conducteur et que, pour calculer la racine carrée, il suffit de calculer le logarithme.

On dirait un polynôme de degré logarithmique du conducteur. On peut certainement partir de la formule explicite, la décomposer en un système d’équations et calculer ainsi une propriété des zéros, comme la racine. Et la réponse est oui, on a réussi et on le savait déjà depuis un moment.

J’ai même donné des cours sur ce sujet, mais nous n’avons jamais réussi à l’implémenter. Un théorème qui repose sur des conjectures est acceptable lorsqu’on cherche à réaliser quelque chose, à condition de démontrer son fonctionnement. On sait donc qu’il est possible de factoriser en un temps sous-exponentiel, mais cela n’est pas démontrable.

La factorisation ne peut s’effectuer qu’en temps sous-exponentiel. Concrètement, si vous fournissez un grand nombre, l’algorithme le factorisera correctement lors du calcul du résultat.

Ceci aussi. Je suppose qu’il s’agit de la méthode de Riemann, mais à part ça, elle donnera la bonne réponse. Et pour cette réponse, le seul élément aléatoire est la rapidité d’exécution.

Je ne suis pas au courant de tout ce qui se passe, mais à l’époque, on appelait ça Las Vegas euh... non ! Monte Carlo ! Donc, ça donne la bonne réponse.

Le seul hic, c’est que si ça ne marche pas, on peut toujours relancer une pièce et ça finira par marcher.

Et c’est précisément ce que nous aurons ici. Nous avons donc un algorithme qui... mais que calcule-t-il ? J’aimerais pouvoir dire que c’est ce que calcule Riemann. Eh bien non.

Vous m'avez donc demandé ce que ce programme calcule ? Il calcule quelque chose concernant les zéros. Il trouve les régions interdites. où il n'y a pas de zéros. Plus précisément, il me permet de calculer le nombre exact de zéros, un entier et non une approximation, pour une certaine valeur de  $T$ . Je suppose qu'il s'agit de la fonction de Riemann, donc je considère les ordonnées jusqu'à  $T$ . Et il me donne le nombre exact pour certaines valeurs de  $T$ .

Je vais avancer en marchant et un événement va se produire. Quand il donnera la réponse, la réponse sera correcte. Il s'agit donc d'une sous-exponentielle, ce qui signifie qu'elle surpasse largement la fonction de Riemann.

Elle est conduite à epsilon pour chaque epsilon. C'est ce que signifie sous-exponentiel. Nous avons déjà rencontré ce phénomène dans un problème modèle, au sein d'une théorie que nous avons dû développer pour le comprendre, mais nous n'avions pu l'implémenter que récemment.

Et voici ce que nous faisons... J'ai déjà brièvement expliqué les hypothèses. Je suppose que l'algorithme repose sur la factorisation de Riemann, et par conséquent sur la conjecture de Katz et moi-même. Cela fait partie des données d'entrée, mais c'est uniquement pour démontrer la rapidité d'exécution de l'algorithme la preuve de sa performance réside donc dans son exécution, comme pour tout algorithme de factorisation.

Personne ne prouve l'équirépartition dont vous avez besoin. Vous disposez d'une heuristique. Si vous l'appliquez, tout le monde se tait.

La preuve est là. Si quelque chose fonctionne, c'est indiscutable. Et nous ne l'avons jamais vérifié jusqu'à présent, donc toute la théorie, sur laquelle j'ai parfois donné des cours, est remise en question.

D'accord. Il nous a fallu beaucoup de temps pour comprendre pourquoi on ne peut pas simplement utiliser la formule explicite et, enfin, quel est ce système d'équations ? Comment obtenir les zéros ? Et que peut-on déduire des zéros en calculant les  $a_p$  ? C'est un problème de moments où le nombre de moments est indéterminé. On pourrait croire qu'on n'y apprend rien, mais en fait, si.

Le modèle sur lequel nous avons travaillé et que nous comprenons parfaitement sur le plan théorique et que nous allons publier prochainement, puisqu'il est enfin implémenté consiste à prendre un groupe orthogonal, un grand groupe orthogonal ordinaire de taille impaire, dont l'une des valeurs propres est égale à 1. Je cherche à déterminer laquelle, c'est-à-dire la racine carrée. Je ne dispose que d'un nombre limité de moments.

J'ai donc cette trace des puissances de la matrice. J'ai donc  $p$  à la puissance  $k$  plus les autres.

Ils vont par paires conjuguées.

J'ai ces valeurs pour  $k$  jusqu'à une valeur maximale. Donc  $k/n \leq a$ . Si  $a = n$ , je serai dans la position de Riemann.

Je dispose de tous les moments. Il me suffit ensuite de trouver les racines. Tout ceci se déroule dans le cadre d'un polynôme en  $n$ .

Ce n'est pas un problème.

Mais la question est : supposons que j'en aie beaucoup moins. Supposons que j'en aie la moitié, ou seulement le quart.

Alors vous me dites : "Eh bien, on ne peut pas calculer avec  $\zeta$ ."

En fait, on exploite la géométrie et certaines formes pour identifier des régions et obtenir des résultats significatifs, même pour de petites valeurs d' $\alpha$ . C'est pourquoi la fonction est sous-exponentielle. On peut calculer, avec une probabilité proche de 1 lorsque  $n$  est grand, le nombre de zéros entre  $-t$  et  $t$ . Si ce nombre est pair, il n'y a pas de zéro en 1. S'il est impair, il y a un zéro en 1. On peut donc déterminer gratuitement la racine à la fin grâce à cet algorithme.

C'est ce que nous avons compris et nous avons toute une théorie des problèmes de moments sous-déterminés. Nous l'appliquons maintenant aux courbes elliptiques, car ce sont les objets les plus riches pour lesquels on peut calculer les suites arithmétiques. On sait qu'il existe une forme automorphe associée à chaque courbe elliptique.

I FOCUS ON THE AUTOMORPHIC AND FURTHER ANALYTIC SIDE OF THE CONDUCTOR THEME.

- CONJECTURALLY ALL ZETA FUNCTIONS GENERALIZING THE RIEMANN ZETA FUNCTION ARE PRODUCTS OF PRINCIPAL L-FUNCTIONS ASSOCIATED TO CUSP FORMS  $\pi$  FOR  $GL_m/\mathbb{Q}$ ,  $m \geq 1$
- $\pi \cong \bigotimes_v \pi_v$ ,  $v = \infty$  OR  $v = p < \infty$
- $\pi_v$  IS A REPRESENTATION OF  $GL_m(\mathbb{Q}_v)$  AND FOR THE ALMOST ALL UNRAMIFIED  $v$ 'S IT IS DETERMINED BY ITS SATAKE PARAMETERS  $\alpha_{\pi}(j, v)$ ;  $j = 1, 2, \dots, m$  AND BY ITS LANGLANDS PARAMETERS IN THE RAMIFIED CASES.
- IN ALL FINITE  $v$  CASES THE LOCAL FACTORS OF THE L-FUNCTION ARE OF THE FORM

$$L(s, \pi_p) = \prod_{j=1}^m (1 - \alpha_{\pi}(j, p) p^{-s})^{-1}$$

• En direct

Serre 100 Institut Henri Poincaré

AND FOR  $V = \mathbb{R}^m$

$$L(s, \pi_\infty) = \prod_{j=1}^m \Gamma_{\mathbb{R}}(s + \mu_\pi(j)), \quad \Gamma_{\mathbb{R}}(s) = \pi^{-s/2} \Gamma(s/2)$$

THE  $\mu_\pi(j)$  PARAMETERS ASSOCIATED WITH THE REPRESENTATION  $\pi_\infty$  OF  $GL_m(\mathbb{R})$ .

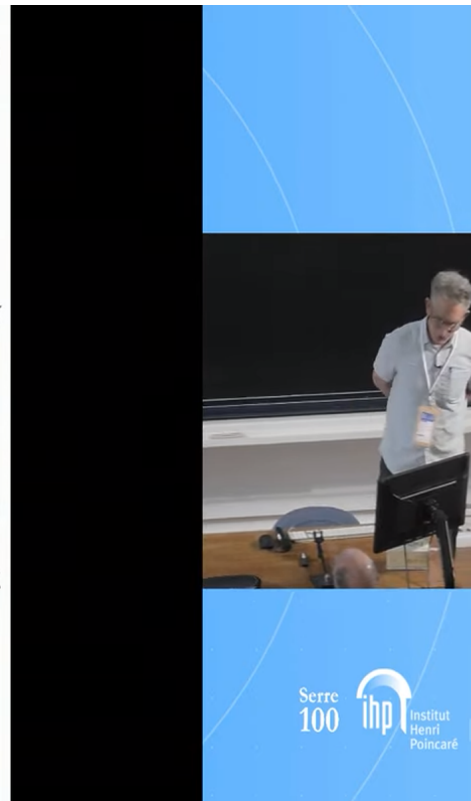
THE GLOBAL (PRINCIPAL) L-FUNCTIONS ARE

$$L(s, \pi) = \prod_{p < \infty} L(s, \pi_p) \quad \text{AND} \quad \Lambda(s, \pi) = L(s, \pi_\infty) L(s, \pi)$$

THEY HAVE ANALYTIC CONTINUATIONS AND FUNCTIONAL EQUATION

$$\Lambda(s, \pi) = \tau(\pi) Q_\pi^{-s} \Lambda(1-s, \tilde{\pi})$$

- $\tilde{\pi}$  IS THE CONTRAGREDIENT REPRESENTATION
- $Q_\pi$  IS A NATURAL NUMBER THE CONDUCTOR WHICH HAS ITS PRIME FACTORS AT THE RAMIFIED FINITE PRIMES  
 $\tau(\pi) \tau(\tilde{\pi}) = Q_\pi$ ; IF  $\pi \neq \tilde{\pi}$ ,  $\tau(\pi)^2 = Q_\pi$ .
- THIS IS DUE TO GODEMENT-JACQUET, JACQUET-PIATETSKI SHAPIRO-SHALIK AND ESPECIALLY FOR THE SAME RESULTS FOR THE RANKIN-SELBERG L-FUNCTIONS  $L(s, \pi \times \pi')$ . WE USE THESE FREELY AS WELL AS IMPORTANT CONDUCTOR COMPUTATIONS OF BUSHNELL AND HENRIART.



THE CONDUCTOR

FOR  $g \in C_c^\infty(\mathbb{R})$ ,  $h(r) = \int_{-\infty}^{\infty} g(u) e^{i r u} du$

$\rho_\pi = \frac{1}{2} + i \gamma_\pi$  THE ZEROS OF  $\Lambda(s, \pi)$

$$\sum_i h(\gamma_\pi) - \delta(\pi) \left\{ h\left(\frac{1}{2}\right) + h\left(\frac{i}{2}\right) \right\}$$

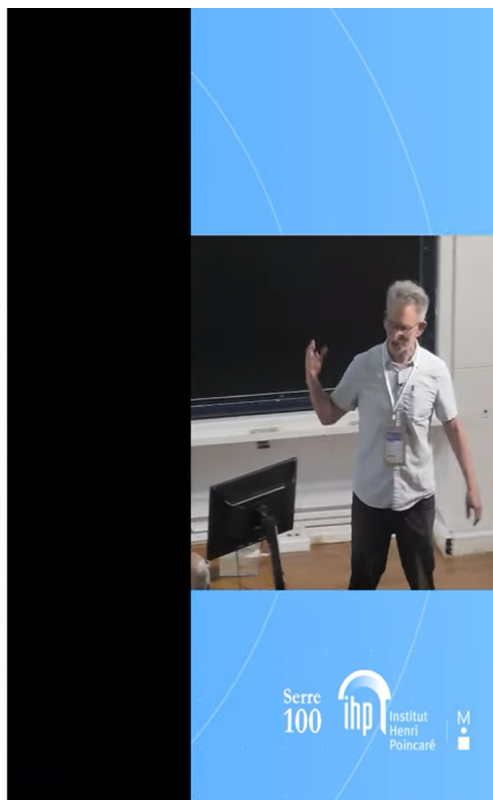
$$= \frac{1}{2\pi i} \int_{-\infty}^{\infty} \left[ \log Q_\pi + \sum_{j=1}^m \left( \frac{\Gamma'_{\mathbb{R}}(\frac{1}{2} + \mu_\pi(j) + i r)}{\Gamma_{\mathbb{R}}(\frac{1}{2} + \mu_\pi(j) + i r)} + \frac{\Gamma'_{\mathbb{R}}(\frac{1}{2} + \mu_\pi(j) - i r)}{\Gamma_{\mathbb{R}}(\frac{1}{2} + \mu_\pi(j) - i r)} \right) h(r) \right] dr$$

$$- \sum_{n=1}^{\infty} \left[ \frac{\Lambda(n) Q_\pi(n)}{\sqrt{n}} g(\log n) + \frac{\Lambda(n) \overline{Q_\pi(n)}}{\sqrt{n}} g(-\log n) \right]$$

WHERE  $-\frac{L'}{L}(s, \pi) = \sum_{n=1}^{\infty} \frac{\Lambda(n) Q_\pi(n)}{n^s}$

$\delta(\pi)$  IS THE MULTIPLICITY OF THE POLE OF  $\Lambda(\pi, s)$  AT  $s=1$ .

FOR OUR PRINCIPAL  $\pi$ 'S  $\delta(\pi)=0$  UNLESS  $L(s, \pi) = \zeta(s)$  THE RIEMANN ZETA FUNCTION.





## ANALYTIC CONDUCTOR (IWANIEC-5)

$$C(\pi) := C(\pi_\infty) Q_\pi$$

WHERE  $C(\pi_\infty) = \prod_{j=1}^m (1 + |A_j|)$

IN PARTICULAR  $C(\pi_\infty) \geq 1$  AND EQUALS 1  
 IFF  $\pi_\infty$  IS UNRAMIFIED AND  $A_j = 0$ ,  $j=1, \dots, m$ .  
 THAT IS  $\pi_\infty$  IS OF THE TYPE OF AN EVEN  
 ARTIN GALOIS REPRESENTATION (CLOZEL  
 CALLS THESE 'ALGEBRAIC' PARAMETERS).

$C(\pi) \geq 1$  AND WE WILL SEE  
 THAT  $C(\pi) = 1$  IFF  $L(s, \pi) = \zeta(s)$ .

- $\log C(\pi)$  MEASURES THE LOCAL  
 DENSITY OF ZEROS OF  $\Lambda(s, \pi)$   
 NEAR THE CENTRAL POINT  $s = \frac{1}{2}$ .



## (b) CONVEXITY AND SUBCONVEXITY

$$L(\tfrac{1}{2}, \pi) \ll C(\pi)^{\frac{1}{4}}$$

SUBCONVEX PROBLEM:  $L(\tfrac{1}{2}, \pi) \ll C(\pi)^{\frac{1}{4}-\delta}$   
 SOME FIXED  $\delta > 0$

$$(c) \quad N(X) = |\{\pi \text{ ON } GL_m : C(\pi) \leq X\}|$$

IS FINITE AND SATISFIES A "WEYL-  
 SCHAUNUEL" ASYMPTOTICS

$$N(X) \sim \beta_m X^{m+1} \text{ AS } X \rightarrow \infty \quad (\text{BRUMLEY-MILICEVIC, USES TRACE FORMULA})$$

(d) THE LOCAL DENSITY OF ZEROS ON  $s = \frac{1}{2} + it$   
 (ASSUMING GRH) NEAR  $s = \frac{1}{2}$  IS UNIFORM  $dt$ ,  
 ON THE OTHER THE SCALED SPACING  
 DISTRIBUTIONS  $k$ -LEVEL DENSITIES ( $k \geq 1$ ).  
 FOLLOW THE RANDOM MATRIX STATISTICS CONJECTURED  
 IN KATZ-S.

(e) RIEMANN'S GOLD STANDARD ("APPROXIMATE  
 FUNCTIONAL EQUATION")

IF THE  $Q_\pi(p)$ 'S CAN BE COMPUTED IN  
 POLYNOMIAL (IN  $\log p$ ) STEPS THEN  $L(s, \pi)$   
 FOR  $s$  NEAR  $\frac{1}{2}$  CAN BE COMPUTED IN  
 $C(\pi)^{\frac{1}{4}+\epsilon}$  STEPS.





• THE DENSITY OF ZEROS OF  $L(s, \pi)$  NEAR  $s = \frac{1}{2}$  IS  $\log C(\pi)$  SO ONE MIGHT HOPE THAT WITH FAR FEWER  $Q_\pi(p)$ 'S ONE CAN SAY SOMETHING ABOUT THESE ZEROS

WHY NOT  $\text{POLY}(\log C(\pi))$  COEFF?

RUBINSTEIN ~ 5 2013, ... , 2026.

THE IDEA IS TO USE THE EXPLICIT FORMULA WITH BAND LIMITED TEST FUNCTIONS  $g$

THEOREM: ASSUMING GRH + LOCAL DISTRIBUTION (SCALED) OF ZEROS CONJECTURES OF KATZ-S WE GIVE A SUBEXPONENTIAL TIME ALGORITHM TO COMPUTE

$$N_\pi(t) := \# \{ \gamma_\pi : |\gamma_\pi| \leq t \}$$

FOR SOME  $t$ 'S, THAT IS IT RUNS IN  $O(C(\pi)^{o(1)})$  STEPS

(WE ASSUME OF COURSE THAT THE  $Q_\pi(p)$ 'S CAN BE COMPUTED IN  $\text{POLY}(\log p)$  STEPS.

WHAT ABOUT ALL OF THESE ASSUMPTIONS?

FIRSTLY THE COUNT IS CORRECT WHEN AN ANSWER IS GIVEN (SO FAR AT LEAST ASSUMING GRH); WHAT THE KATZ-S ~~SALMA~~ CONJECTURES ARE USED FOR IS TO ENSURE THAT THE RUNNING TIME IS AS SHORT AS CLAIMED.

• SO THE PROOF OF THE PUDDING IS IN THE IMPLEMENTATION.

AT THE HEART OF THE ANALYSIS IS A STUDY OF AN UNDERDETERMINED MOMENT PROBLEM:

LET  $A \in O(2n+1)$  BE CHOSEN RANDOM HAAK WITH EIGENVALUES

$$s_0 = \pm 1, s_1, \bar{s}_1, s_2, \bar{s}_2, \dots, s_n, \bar{s}_n$$

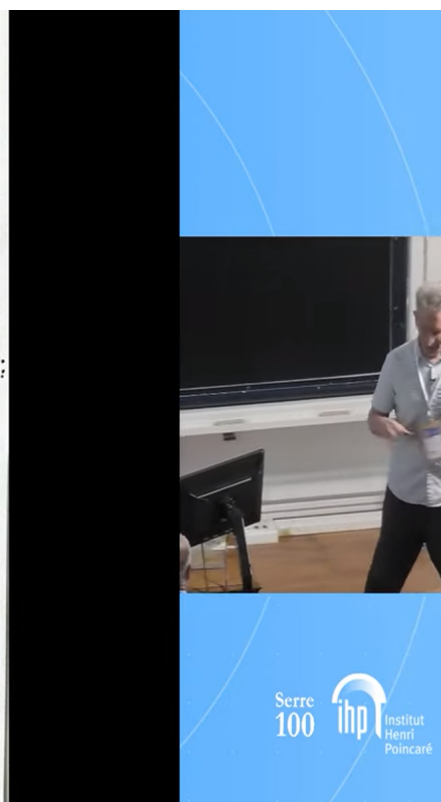
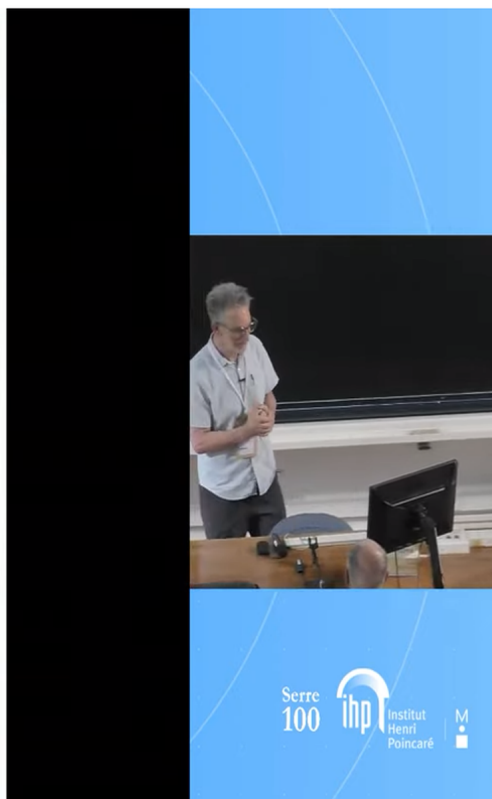
FOR  $0 < \alpha \leq 1$  (CORRESPONDS TO THE COMPLEXITY EXPONENT  $\alpha \log C(\pi)$ )

GIVEN THE MOMENTS FOR  $k \leq \alpha n$

$$p_0^k + \sum_{j=1}^n s_j^k + \bar{s}_j^k$$

WHAT CAN WE SAY ABOUT INTERVALS CONTAINING  $s_j$ 'S?

FOR EXAMPLE COMPUTE THE NO' OF ZEROS IN THE INTERVAL  FOR SOME  $t$ ?



WE APPLY THIS TO ELLIPTIC CURVES

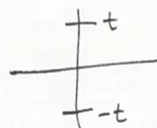
$E/\mathbb{Q}$ ,  $N(E)$  CONDUCTOR

$$E: Y^2 = X^3 + aX + b \quad a, b \in \mathbb{Z}$$

ONE CAN COMPUTE  $Q_E(p)$  IN POLYNOMIAL TIME  
(SCHOOF ; AND IS IMPLEMENTED)

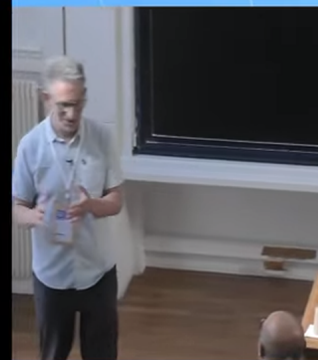
WE DO SO FOR  ~~$Q_E(p)$~~   $p \leq N^{1/2}$

USE OUR METHOD OF DETERMINING INFORMATION  
IN THE UNDERDETERMINED MOMENTUM PROBLEM



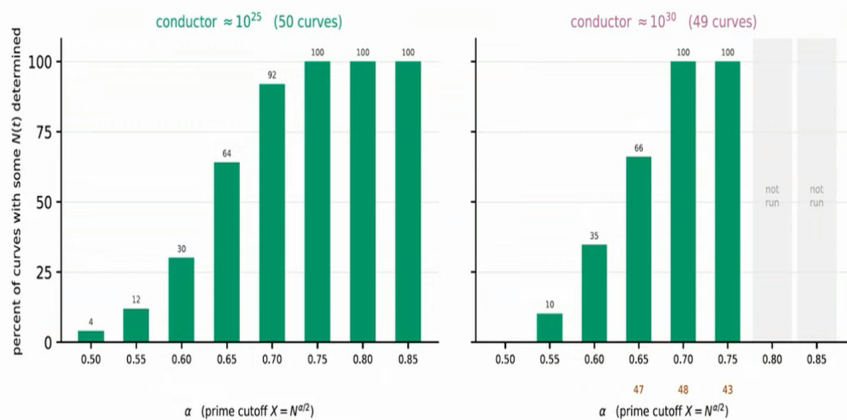
$N_E(t) = \#$  OF ZEROS  
OF  $L(s, E)$

NOTE THAT THE PARITY OF  $N_E(t)$   
IS THE ROOT NUMBER  $W(E) \in \{1, -1\}$   
THAT IS WE COMPUTE  $W(E)$  IN  
SUBEXponential TIME WITHOUT  
FACTORING  ~~$N(E)$~~  !



Curves with some  $N(t)$  determined, cumulative in  $\alpha$ , sweep  $0 < t \leq 10$  on the 0.01 grid

ROOT NUMBER ASSUMED



### CLAUDE'S $\frac{2}{3}$ :

AFTER REPEATED PROMPTS TO USE SWARMS OF AGENTS TO ATTACK THE RIEMANN HYPOTHESIS, IT SETTLED WITH A PROOF THAT AT LEAST  $\frac{2}{3}$  OF THE ZEROS ARE ON THE LINE AND ARE SIMPLE, IMPROVING ON WHAT WAS KNOWN (SELBERG, LEVINSON, CONREY, ...)

- USING THE EXPLICIT FORMULA FOR  $\zeta(s)$  AT HEIGHT  $t$  (FOR ZEROS) THE ANALYTIC CONDUCTOR IS  $C(t) = t$ ; ONE CAN COMPUTE THE SCALED PAIR CORRELATION OF ZEROS WITH BAND LIMITED WIDTH, UNCONDITIONALLY (MONTGOMERY).
- TO USE THIS BAND LIMITED INFORMATION, IF ONE ASSUMES RH ONE CAN SOLVE THE RESULTING LINEAR PROGRAM TO OPTIMIZE BY HAND AND SHOW THAT AT LEAST  $\frac{2}{3}$  OF THE ZEROS OF  $\zeta(s)$  ARE SIMPLE.

Serre  
100



Institut  
Henri  
Poincaré

WHAT CLAUDE <sup>(13)</sup> DOES IS TO CARRY OUT THIS OPTIMIZATION ALLOWING FOR THE ZEROS TO BE OFF THE LINE.

• THIS IS DONE BY A STANDARD DISCRETIZATION OF THE SPACE OF BAND LIMITED TEST FUNCTIONS AND ESTIMATING THE SIGNATURES OF THE RESULTING HERMITIAN FORMS ASSOCIATED WITH PAIR CORRELATION SUMS (WEIL POSITIVITY). SPECIFICALLY EXPLOITING THE DIFFERENT CONTRIBUTIONS OF MULTIPLE AND OFF-LINE ZEROS TO THESE.

• WHILE AS FAR AS RH THIS IS NOT PARTICULARLY SIGNIFICANT IT HAS A NEW FEATURE. THAT IT PRODUCES MANY ZEROS ON THE LINE WITHOUT SELBERG'S "MOLLIFIERS".

• LUCKILY FOR MATHEMATICS SELBERG'S MUCH MORE ROBUST AND FLEXIBLE MOLLIFIERS LED HIM TO THE SELBERG SIEVE WITH ITS FAR REACHING IMPACT AND APPLICATIONS.

Serre  
100



Institut  
Henri  
Poincaré

## (14)

# NON-TAME FAMILIES

THIS REFERS TO ALLOWING  $m$  TO VARY AND GIVING ABSOLUTE UNIFORM BOUNDS IN TERMS OF CONDUCTORS.

- FOR DISCRIMINANTS OF NUMBER FIELDS  $K$  (WHICH ARE THEIR CONDUCTORS IN TERMS OF THEIR ZETA FUNCTIONS  $\zeta_K(s)$ ) THESE RESULTS GO BACK TO

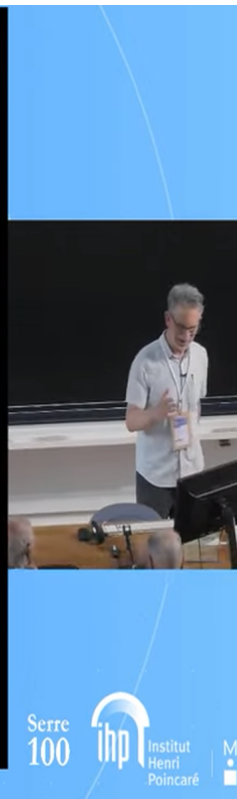
HERMITE, MINKOWSKI (GEOMETRY OF NUMBERS)

STARK, ODLYZKO, SERRE (USING  $\zeta_K(s)$ )

- FOR ZETA FUNCTIONS OF CURVES AND ABELIAN VARIETIES OVER FINITE FIELDS

TSFASMAN, VLADUT, SERRE.

WE REVIEW THESE BRIEFLY.



(15)

$D = D(K)$   $\text{discr}(K)$ ,  $K/\mathbb{Q}$  TOTALLY REAL

GEOMETRY OF NUMBERS:

• HERMITE  $\# \{K: D(K) \leq X\}$  IS FINITE FOR ANY  $X$ .

- MINKOWSKI; IF  $m = \text{deg}(K)$  THE ROOT DISCRIMINANT:

$$\lim_{m \rightarrow \infty} D(K)^{1/m} \geq e^2 \quad \left( \text{IMPROVED BY BLICHFELD, ROGERS, SIEGEL, \dots} \right)$$

USING VARIANTS OF THE EXPLICIT FORMULA AND POSITIVITY OPTIMIZATION

STARK, ODLYZKO, SERRE (WHO ALSO INTRODUCED RAMAN-SERBERG INTO THE ANALYSIS)

$$\Rightarrow \text{UNDER GRH} \quad \lim_{m \rightarrow \infty} D(K)^{1/m} \geq 8\pi e^{1/2}$$

• ON THE OTHER HAND THERE ARE EXOTIC NON-TAME TOWERS WITH LIMITED RAMIFICATION COMING FROM CLASS FIELD THEORY BY GOLD-SHAFAREVICH

$$\lim_{m \rightarrow \infty} D(K)^{1/m} < 1059 \quad (\text{VOIGHT})$$





IN THE FUNCTION FIELD SETTING OF ZETA FUNCTIONS OF CURVES  $C$  OF GENUS  $g$  OVER A FIXED  $\mathbb{F}_q$ :

- THE DENSITY OF ZEROS ON  $|Z|=\sqrt{q}$  IS  $2g$  AND CORRESPONDS TO  $\log(\chi)$ . (WEIL)
- A SEQUENCE OF CURVES  $C$  WITH  $gonality(C) = o(g)$  AS  $g \rightarrow \infty$  IS TAME (TSFASMAN-VLADUT, SHPARLINSKI)
- THERE ARE EXTREMAL NON-TAME SEQUENCES, SPECIFICALLY MODULAR CURVES WITH THE DENSITY OF THEIR ZEROS NOT UNIFORM AND FOR WHICH THE POSITIVITY INEQUALITIES ARE SATURATED! TSFASMAN-VLADUT - DRINFELD.
- WHETHER THE RANDOM  $C$  ON  $M_g/\mathbb{F}_q$  THE MODULI SPACE OF GENUS  $g$  CURVES HAS ITS ZEROS EQUIDISTRIBUTED UNIFORMLY, IS A CHALLENGING QUESTION. RECENT ADVANCES IN HOMOLOGICAL STABILITY FOR  $M_g$  SUGGEST THAT YES. (SEE RECENT ARXIV PAPER J. SHAH).



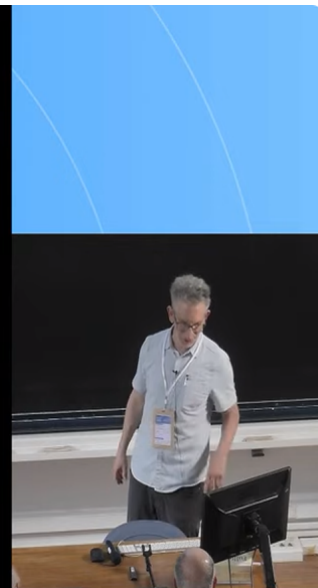
$\pi_1^i$  WITH  $Q_{\pi} = 1$ , IE UNRAMIFIED AT FINITE PLACES AND WITH  $\pi_{\infty}$  HAVING MOTIVIC WEIGHTS HAVE BEEN STUDIED WIDELY:

- GROSS GROUPS OVER  $\mathbb{Z}$ , MESTRE, CHENEVIER EXPLICIT FORMULA ...
- A HIGHLIGHT IS FONTAINE AN ABELIAN VARIETY OR CURVE OF POSITIVE GENUS DEFINED OVER  $\mathbb{Q}$  CANNOT HAVE GOOD REDUCTION AT ALL PLACES.

A FEATURE OF THE ARCHIMEDIAN PLACE OF  $\mathbb{Q}$  IS THAT THERE ARE CUSP FORMS  $\pi$  WHICH ARE EVERYWHERE UNRAMIFIED.

$\pi_{\infty}$  IS UNRAMIFIED AND WRITE ITS SATAKE PARAMETERS  $\mu_j = i t_j$  ;  $t_j \in \mathbb{R} \iff$  RAMANUSJAN CONJECTURE.

- THESE UNRAMIFIED  $\pi$ 'S ARE ELUSIVE. IT WAS IN RESPONSE TO A QUESTION OF SIEGEL THAT SELBERG DEVELOPED HIS TRACE FORMULA TO PRODUCE SUCH CUSP FORMS FOR  $m=2$ .



PHILLIPS-S SHOW THAT FOR  $m=2$  THE  
CONDITION OF BEING CUSPIDAL FOR UNRAMIFIED  
AT  $\mathbb{R}$  IS VERY RESTRICTIVE AT LEAST IF  
ONE ALLOWS NON-ARITHMETIC QUOTIENTS.

HENCE THE EXISTENCE OF THESE BASIC  
BUILDING BLOCKS OF THE THEORY IS TIED  
TO NUMBER THEORY EVEN IF THEY ARE  
HIGHLY TRANSCENDENTAL.

THE CASE  $t_1=t_2=\dots=t_m=0$  FOR WHICH  
 $\Pi_\infty$  HAS PARAMETERS OF AN EVEN ARTIN  
GALOIS REPRESENTATION CANNOT OCCUR WITH  
 $Q_\pi=1$ .

THIS FOLLOWS FROM MILLER'S LOWER  
BOUND FOR THE FIRST CUSPIDAL EIGENVALUE  
OF THE LAPLACIAN FOR SUCH FORMS AT FULL  
LEVEL FOR  $GL_m(\mathbb{Z})$

$$\lambda - \frac{m^2 m}{24} = t_1^2 + \dots + t_m^2 \geq \beta m, \quad \text{FOR } \beta > 0, m \geq 1.$$

