Fonctions L et courses de nombres premiers

Alexandre Bailleul

Séminaire Lambda

12 mars 2020

Sommaire

Introduction

- Titre pompeux : **Harmonie et disparités dans la répartition des nombres premiers**.

Introduction

- Titre pompeux : **Harmonie et disparités dans la répartition des nombres premiers**.
- Harmonie : Équirépartition uniforme des nombres premiers dans certains ensembles naturels.

Introduction

- Titre pompeux : **Harmonie et disparités dans la répartition des nombres premiers**.
- Harmonie : Équirépartition uniforme des nombres premiers dans certains ensembles naturels.
- Disparités : Équirépartition à des vitesses différentes.

Le théorème de la progression arithmétique

Théorème (Dirichlet, 1837).

Soit $q \geq 1$ entier et $a \in \mathbb{Z}$ premier avec q. Alors il existe une infinité de nombres premiers de la forme $p = a + qn, n \in \mathbb{Z}$.

Le théorème de la progression arithmétique

Théorème (Dirichlet, 1837).

Soit $q \geq 1$ entier et $a \in \mathbb{Z}$ premier avec q. Alors il existe une infinité de nombres premiers de la forme $p = a + qn, n \in \mathbb{Z}$.

- À la main, on peut montrer l'existence d'une infinité de nombres premiers de la forme $4n + 1$ ou $4n + 3$ par exemple

Le théorème de la progression arithmétique

Théorème (Dirichlet, 1837).

Soit $q \geq 1$ entier et $a \in \mathbb{Z}$ premier avec q. Alors il existe une infinité de nombres premiers de la forme $p = a + qn, n \in \mathbb{Z}$.

- À la main, on peut montrer l'existence d'une infinité de nombres premiers de la forme $4n + 1$ ou $4n + 3$ par exemple, mais ce n'est pas clair pour $1000n + 379$!

Outils

Définition.

Soit $q \geq 1$ entier. Un caractère de Dirichlet modulo q est un morphisme de groupes

$$\chi : (\mathbb{Z}/q\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times.$$

On prolonge un tel caractère à $\mathbb{Z}/q\mathbb{Z}$ par 0, puis à $\mathbb{Z}$ par q-périodicité.

Outils

Définition.

Soit $q \geq 1$ entier. Un caractère de Dirichlet modulo q est un morphisme de groupes

$$\chi : (\mathbb{Z}/q\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times.$$

On prolonge un tel caractère à $\mathbb{Z}/q\mathbb{Z}$ par 0, puis à $\mathbb{Z}$ par q-périodicité.

Caractères de Dirichlet

Exemples :

i) Le caractère trivial χ_0 vérifie

$$\chi_0(n) = \begin{cases} 1 \text{ si } n \text{ est premier avec } q \\ 0 \text{ sinon} \end{cases}.$$

Caractères de Dirichlet

Exemples :

i) Le caractère trivial χ_0 vérifie

$$\chi_0(n) = \begin{cases} 1 \text{ si } n \text{ est premier avec } q \\ 0 \text{ sinon} \end{cases}.$$

ii) Le caractère χ modulo 5 défini par

$$\chi(n) = \begin{cases} 1 \text{ si } n \equiv 1 \bmod 5 \\ i \text{ si } n \equiv 3 \bmod 5 \\ -1 \text{ si } n \equiv 4 \bmod 5 \\ -i \text{ si } n \equiv 2 \bmod 5 \\ 0 \text{ sinon} \end{cases}.$$

Caractères de Dirichlet

Exemples :

i) Le caractère trivial χ_0 vérifie

$$\chi_0(n) = \begin{cases} 1 \text{ si } n \text{ est premier avec } q \\ 0 \text{ sinon} \end{cases}.$$

ii) Le caractère χ modulo 5 défini par

$$\chi(n) = \begin{cases} 1 \text{ si } n \equiv 1 \bmod 5 \\ i \text{ si } n \equiv 3 \bmod 5 \\ -1 \text{ si } n \equiv 4 \bmod 5 \\ -i \text{ si } n \equiv 2 \bmod 5 \\ 0 \text{ sinon} \end{cases}.$$

iii) Si p est un nombre premier impair, le symbole de Legendre $\left(\frac{\cdot}{p}\right)$ est un caractère de Dirichlet modulo p.

Caractères de Dirichlet

Proposition (Relations d'orthogonalité).

Soit $q \geq 1$ un entier et $a \in \mathbb{Z}$ premier avec q. Pour tout $k \in \mathbb{Z}$, on a

$$\frac{1}{\varphi(q)} \sum_{\chi \bmod q} \chi(k)\overline{\chi(a)} = \begin{cases} 1 \text{ si } k \equiv a \bmod q \\ 0 \text{ sinon} \end{cases}.$$

Caractères de Dirichlet

Proposition (Relations d'orthogonalité).

Soit $q \geq 1$ un entier et $a \in \mathbb{Z}$ premier avec q. Pour tout $k \in \mathbb{Z}$, on a

$$\frac{1}{\varphi(q)} \sum_{\chi \bmod q} \chi(k)\overline{\chi(a)} = \begin{cases} 1 \text{ si } k \equiv a \bmod q \\ 0 \text{ sinon} \end{cases}.$$

Caractères de Dirichlet

Proposition (Relations d'orthogonalité).

Soit $q \geq 1$ un entier et $a \in \mathbb{Z}$ premier avec q. Pour tout $k \in \mathbb{Z}$, on a

$$\frac{1}{\varphi(q)} \sum_{\chi \bmod q} \chi(k)\overline{\chi(a)} = \begin{cases} 1 \text{ si } k \equiv a \bmod q \\ 0 \text{ sinon} \end{cases}.$$

Les caractères de Dirichlet permettent de détecter analytiquement la condition $k \equiv a$ mod q.

Fonctions L de Dirichlet

Définition.

Soit $q \geq 1$ un entier et χ un caractère de Dirichlet modulo q. La fonction L de Dirichlet associée à χ est

$$L(s, \chi) = \sum_{n=1}^{+\infty} \frac{\chi(n)}{n^s}.$$

Fonctions L de Dirichlet

Définition.

Soit $q \geq 1$ un entier et χ un caractère de Dirichlet modulo q. La fonction L de Dirichlet associée à χ est

$$L(s,\chi) = \sum_{n=1}^{+\infty} \frac{\chi(n)}{n^s}.$$

Proposition (Produit eulérien).

Soit $q \geq 1$ un entier et χ un caractère de Dirichlet modulo q. Pour $\mathfrak{Re}(s) > 1$, on a

$$L(s,\chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

Idées de démonstration

- On peut montrer

$$\frac{1}{\varphi(q)} \sum_{\chi \bmod q} \overline{\chi(a)} \log(L(s,\chi)) = \sum_{p \equiv a \bmod q} \frac{1}{p^s} + O(1) \quad \text{pour } s > 1$$

Idées de démonstration

- On peut montrer

$$\frac{1}{\varphi(q)} \sum_{\chi \bmod q} \overline{\chi(a)} \log(L(s,\chi)) = \sum_{p \equiv a \bmod q} \frac{1}{p^s} + O(1) \quad \text{pour } s > 1$$

- On a facilement $\lim_{s \to 1^+} L(s, \chi_0) = +\infty$.

Idées de démonstration

- On peut montrer

$$\frac{1}{\varphi(q)} \sum_{\chi \bmod q} \overline{\chi(a)} \log(L(s,\chi)) = \sum_{p \equiv a \bmod q} \frac{1}{p^s} + O(1) \quad \text{pour } s > 1$$

- On a facilement $\lim_{s \to 1^+} L(s, \chi_0) = +\infty$. Dirichlet montre ensuite que pour $\chi \neq \chi_0$, $L(1, \chi) \neq 0$ (difficile).

Idées de démonstration

- On peut montrer

$$\frac{1}{\varphi(q)} \sum_{\chi \bmod q} \overline{\chi(a)} \log(L(s,\chi)) = \sum_{p \equiv a \bmod q} \frac{1}{p^s} + O(1) \quad \text{pour } s > 1$$

- On a facilement $\lim_{s \to 1^+} L(s, \chi_0) = +\infty$. Dirichlet montre ensuite que pour $\chi \neq \chi_0$, $L(1, \chi) \neq 0$ (difficile). On obtient la divergence de la série

$$\sum_{p \equiv a \bmod q} \frac{1}{p}$$

et en particulier l'existence d'une infinité de $p \equiv a \bmod q$!

Théorème des nombres premiers en progression arithmétique

Théorème (De la Vallée-Poussin, 1899).

Soit $q \geq 1$ entier et $a \in \mathbb{Z}$ premier avec q. On note

$$\pi(x, q, a) := \#\{p \leq x \mid p \equiv a \bmod q\}.$$

Alors

$$\pi(x, q, a) \underset{x \to +\infty}{\sim} \frac{1}{\varphi(q)} \frac{x}{\log x}.$$

Théorème des nombres premiers en progression arithmétique

Théorème (De la Vallée-Poussin, 1899).

Soit $q \geq 1$ entier et $a \in \mathbb{Z}$ premier avec q. On note

$$\pi(x, q, a) := \#\{p \leq x \mid p \equiv a \bmod q\}.$$

Alors

$$\pi(x, q, a) \underset{x \to +\infty}{\sim} \frac{1}{\varphi(q)} \frac{x}{\log x}.$$

- Dirichlet n'obtenait que

$$\sum_{p \equiv a \bmod q} \frac{1}{p^s} \underset{s \to 1^+}{\sim} \frac{1}{\varphi(q)} \log\left(\frac{1}{s-1}\right).$$

Théorème des nombres premiers en progression arithmétique

- C'est un résultat **d'équirépartition** : les p mod q s'équirépartissent uniformément parmi les classes inversibles modulo q.

Théorème des nombres premiers en progression arithmétique

- C'est un résultat **d'équirépartition** : les p mod q s'équirépartissent uniformément parmi les classes inversibles modulo q.

- En vertu du théorème des nombres premiers

$$\pi(x) := \#\{p \leq x\} \underset{x \to +\infty}{\sim} \frac{x}{\log x}$$

et donc

$$\frac{\pi(x, q, a)}{\pi(x)} \underset{x \to +\infty}{\longrightarrow} \frac{1}{\varphi(q)}.$$

Théorème des nombres premiers en progression arithmétique

- C'est un résultat **d'équirépartition** : les p mod q s'équirépartissent uniformément parmi les classes inversibles modulo q.
- En vertu du théorème des nombres premiers

$$\pi(x) := \#\{p \leq x\} \underset{x \to +\infty}{\sim} \frac{x}{\log x}$$

et donc

$$\frac{\pi(x, q, a)}{\pi(x)} \underset{x \to +\infty}{\longrightarrow} \frac{1}{\varphi(q)}.$$

- Un nombre premier a une « probabilité » $\frac{1}{\varphi(q)}$ de valoir a mod q.

Théorème des nombres premiers en progression arithmétique

- La démonstration passe par l'étude des propriétés analytiques des fonctions L de Dirichlet (prolongement analytique et équation fonctionnelle) et l'étude de la disposition de leurs zéros dans le plan complexe.

Théorème des nombres premiers en progression arithmétique

- La démonstration passe par l'étude des propriétés analytiques des fonctions L de Dirichlet (prolongement analytique et équation fonctionnelle) et l'étude de la disposition de leurs zéros dans le plan complexe.

- Le point clé est que $L(1+it,\chi) \neq 0$ pour $t \neq 0$.

Théorème des nombres premiers en progression arithmétique

- La démonstration passe par l'étude des propriétés analytiques des fonctions L de Dirichlet (prolongement analytique et équation fonctionnelle) et l'étude de la disposition de leurs zéros dans le plan complexe.

- Le point clé est que $L(1+it,\chi) \neq 0$ pour $t \neq 0$. Estimation du reste $\longleftrightarrow$ région sans zéro à gauche de la droite $\{s \in \mathbb{C} \mid \mathfrak{Re}(s) = 1\}$. Le reste le plus petit possible correspond à l'**hypothèse de Riemann**$^{\mathbb{R}}$.

Biais de Tchebychev

- D'après le TNPPA, on a, pour a et b inversibles modulo q, $\pi(x,q,a) \underset{x\to+\infty}{\sim} \pi(x,q,b)$

Biais de Tchebychev

- D'après le TNPPA, on a, pour a et b inversibles modulo q, $\pi(x,q,a) \underset{x\to+\infty}{\sim} \pi(x,q,b)$, mais en pratique on peut observer une asymétrie.

Biais de Tchebychev

- D'après le TNPPA, on a, pour a et b inversibles modulo q, $\pi(x,q,a) \underset{x\to+\infty}{\sim} \pi(x,q,b)$, mais en pratique on peut observer une asymétrie.

- En 1853, Tchebychev écrit dans une lettre à Fuss qu'il semble que

$$\pi(x,4,3) > \pi(x,4,1).$$

Biais de Tchebychev

- D'après le TNPPA, on a, pour a et b inversibles modulo q, $\pi(x,q,a) \underset{x\to+\infty}{\sim} \pi(x,q,b)$, mais en pratique on peut observer une asymétrie.

- En 1853, Tchebychev écrit dans une lettre à Fuss qu'il semble que

$$\pi(x,4,3) > \pi(x,4,1).$$

- Il prétend même que

$$\sum_p (-1)^{\frac{p-1}{2}} \mathrm{e}^{-px} \underset{x\to 0}{\longrightarrow} -\infty.$$

Biais de Tchebychev

Problèmes :

i) Tchebychev n'a pas regardé assez loin : $\pi(26861, 4, 1) > \pi(26861, 4, 3)$.

Biais de Tchebychev

Problèmes :

i) Tchebychev n'a pas regardé assez loin : $\pi(26861, 4, 1) > \pi(26861, 4, 3)$.

ii) Pire, $\pi(x, 4, 3) - \pi(x, 4, 1)$ change de signe une infinité de fois (Littlewood, 1914).

Biais de Tchebychev

Problèmes :

i) Tchebychev n'a pas regardé assez loin : $\pi(26861, 4, 1) > \pi(26861, 4, 3)$.

ii) Pire, $\pi(x, 4, 3) - \pi(x, 4, 1)$ change de signe une infinité de fois (Littlewood, 1914).

iii) L'assertion sur la somme est équivalente à l'hypothèse de Riemann pour $L(s, \chi_4)$... (Hardy-Littlewood/Landau, 1914)

Biais de Tchebychev

- Ce phénomène (appelé **biais de Tchebychev**) semble tout de même présent

Biais de Tchebychev

- Ce phénomène (appelé **biais de Tchebychev**) semble tout de même présent : juste après 26861, la « course » entre l'équipe 1 mod 4 vs 3 mod 4 rebascule en la faveur des $p \equiv 3 \bmod 4$ pendant longtemps.

Biais de Tchebychev

- Ce phénomène (appelé **biais de Tchebychev**) semble tout de même présent : juste après 26861, la « course » entre l'équipe 1 mod 4 vs 3 mod 4 rebascule en la faveur des $p \equiv 3 \bmod 4$ pendant longtemps.

Comment quantifier ce biais ?

Quantifier le biais

- On est amené à « mesurer » l'ensemble

$$\mathcal{P}_{q;a,b} := \{x \geq 2 \mid \pi(x,q,a) > \pi(x,q,b)\}.$$

Quantifier le biais

- On est amené à « mesurer » l'ensemble

$$\mathcal{P}_{q;a,b} := \{x \geq 2 \mid \pi(x,q,a) > \pi(x,q,b)\}.$$

- Comme cet ensemble n'est pas borné (Littlewood), une notion naturelle de taille de cet ensemble serait sa **densité naturelle**

$$\lim_{x \to +\infty} \frac{|\mathcal{P}_{q;a,b} \cap [0,x]|}{x}.$$

Quantifier le biais

- On est amené à « mesurer » l'ensemble

$$\mathcal{P}_{q;a,b} := \{x \geq 2 \mid \pi(x,q,a) > \pi(x,q,b)\}.$$

- Comme cet ensemble n'est pas borné (Littlewood), une notion naturelle de taille de cet ensemble serait sa **densité naturelle**

$$\lim_{x \to +\infty} \frac{|\mathcal{P}_{q;a,b} \cap [0,x]|}{x}.$$

- Malheureusement, cette limite n'existe pas en général (Kaczorowski, 1995).

Quantifier le biais

Définition.

La densité logarithmique d'un borélien A de $\mathbb{R}^+$ est, quand elle existe,

$$\delta(A) = \lim_{x \to +\infty} \frac{1}{\log x} \int_2^x \mathbb{1}_A(t) \frac{dt}{t} = \lim_{Y \to +\infty} \frac{1}{Y} \int_2^Y \mathbb{1}_A(\mathrm{e}^t)\, dt.$$

Quantifier le biais

Définition.

La densité logarithmique d'un borélien A de $\mathbb{R}^+$ est, quand elle existe,

$$\delta(A) = \lim_{x \to +\infty} \frac{1}{\log x} \int_2^x \mathbb{1}_A(t) \frac{dt}{t} = \lim_{Y \to +\infty} \frac{1}{Y} \int_2^Y \mathbb{1}_A(e^t)\, dt.$$

- C'est la bonne notion de taille dans ce contexte.

Quelques résultats

Théorème (Rubinstein, Sarnak, 1994).

Supposons l'hypothèse de Riemann pour toutes les fonctions L de Dirichlet modulo q, et que les parties imaginaires des zéros non triviaux de ces fonctions sont linéairement indépendants sur $\mathbb{Q}$. Alors $\delta(\mathcal{P}_{q;a,b})$ existe et satisfait $0 < \delta(\mathcal{P}_{q;a,b}) < 1$.

Quelques résultats

Théorème (Rubinstein, Sarnak, 1994).

Supposons l'hypothèse de Riemann pour toutes les fonctions L de Dirichlet modulo q, et que les parties imaginaires des zéros non triviaux de ces fonctions sont linéairement indépendants sur $\mathbb{Q}$. Alors $\delta(\mathcal{P}_{q;a,b})$ existe et satisfait $0 < \delta(\mathcal{P}_{q;a,b}) < 1$.

- Dans toute « course de nombres premiers », il y a une infinité de changements de « leader » et les deux positions se produisent une proportion strictement positive du temps !

Idées de preuve

- On commence par exprimer $\pi(x, q, a)$ et $\pi(x, q, b)$ en fonction des zéros des fonctions L de Dirichlet modulo q (**formules explicites**).

Idées de preuve

- On commence par exprimer $\pi(x, q, a)$ et $\pi(x, q, b)$ en fonction des zéros des fonctions L de Dirichlet modulo q (**formules explicites**).

- Sous l'hypothèse de Riemann, on a

$$\pi(x, q, c) = \text{terme principal ne dépendant pas de } c + \text{ erreur en } \sqrt{x},$$

il est donc naturel de regarder le signe de

$$\frac{\pi(x, q, a) - \pi(x, q, b)}{\sqrt{x}}.$$

Idées de preuve

- On trouve

$$\frac{\pi(x,q,a)-\pi(x,q,b)}{\sqrt{x}/\log x} = \overbrace{|\sqrt{\{b\}}|-|\sqrt{\{a\}}|}^{:=c(q,a,b)} + \sum_{\chi}\overline{\chi(b)-\chi(a)}\sum_{\gamma_\chi}\frac{x^{i\gamma_\chi}}{\frac{1}{2}+i\gamma_\chi}+O\left(\frac{1}{\log x}\right),$$

où la somme porte sur les parties imaginaires des zéros non triviaux des $L(s,\chi)$ (rappel : sous GRH les zéros sont de la forme $\frac{1}{2}+i\gamma_\chi$).

Idées de preuve

- Cela se réécrit

$$\frac{\pi(e^t,q,a)-\pi(e^t,q,b)}{e^{t/2}}t = c(q,a,b) + \sum_{\chi}\overline{\chi(b)-\chi(a)}\sum_{\gamma_\chi}\frac{e^{i\gamma_\chi t}}{\frac{1}{2}+i\gamma_\chi}+O\left(\frac{1}{t}\right),$$

Idées de preuve

- Cela se réécrit

$$\frac{\pi(e^t,q,a)-\pi(e^t,q,b)}{e^{t/2}}t = c(q,a,b) + \sum_{\chi}\overline{\chi(b)-\chi(a)}\sum_{\gamma_\chi}\frac{e^{i\gamma_\chi t}}{\frac{1}{2}+i\gamma_\chi}+O\left(\frac{1}{t}\right),$$

- On applique alors le théorème d'équirépartition de Kronecker-Weyl : l'hypothèse d'indépendance linéaire permet de traiter les $e^{i\gamma_\chi t}$ comme des variables aléatoires uniformes **indépendantes** sur le cercle unité.

Idées de preuve

- Cela permet de montrer l'existence d'une variable aléatoire X, d'espérance $c(q, a, b)$, telle que

$$\delta(\mathcal{P}_{q;a,b}) = \mathbb{P}(X > 0).$$

Idées de preuve

- Cela permet de montrer l'existence d'une variable aléatoire X, d'espérance $c(q,a,b)$, telle que

$$\delta(\mathcal{P}_{q;a,b}) = \mathbb{P}(X > 0).$$

- Il reste à étudier cette variable aléatoire à l'aide de sa fonction caractéristique :

$$\varphi : \xi \mapsto \mathrm{e}^{ic(q,a,b)\xi} \prod_{\chi \neq \chi_0} \prod_{\gamma_\chi > 0} J_0\left(\frac{2|\chi(a) - \chi(b)|}{\sqrt{\frac{1}{4} + \gamma_\chi^2}} \xi \right),$$

où

$$J_0 : z \mapsto \sum_{n=0}^{+\infty} \frac{(-1)^n (z/2)^{2n}}{(n!)^2}$$

est la fonction de Bessel de première espèce d'indice 0. □

Calculs numériques

- Rubinstein et Sarnak calculent

$$\delta(\mathcal{P}_{4;3,1}) \approx 0.9959\ldots$$

Calculs numériques

- Rubinstein et Sarnak calculent

$$\delta(\mathcal{P}_{4;3,1}) \approx 0.9959\ldots$$

- Le biais de Tchebychev est quantifié : « 99,59% du temps », les premiers $p \equiv 3 \bmod 4$ sont plus nombreux que les premiers $p \equiv 1 \bmod 4$.

Calculs numériques

- Rubinstein et Sarnak calculent

$$\delta(\mathcal{P}_{4;3,1}) \approx 0.9959\ldots$$

- Le biais de Tchebychev est quantifié : « 99,59% du temps », les premiers $p \equiv 3 \bmod 4$ sont plus nombreux que les premiers $p \equiv 1 \bmod 4$.

- Ils calculent également

$$\delta(\mathcal{P}_{3;2,1}) \approx 0.9990\ldots$$

Calculs numériques

- Rubinstein et Sarnak calculent

$$\delta(\mathcal{P}_{4;3,1}) \approx 0.9959\ldots$$

- Le biais de Tchebychev est quantifié : « 99,59% du temps », les premiers $p \equiv 3 \bmod 4$ sont plus nombreux que les premiers $p \equiv 1 \bmod 4$.

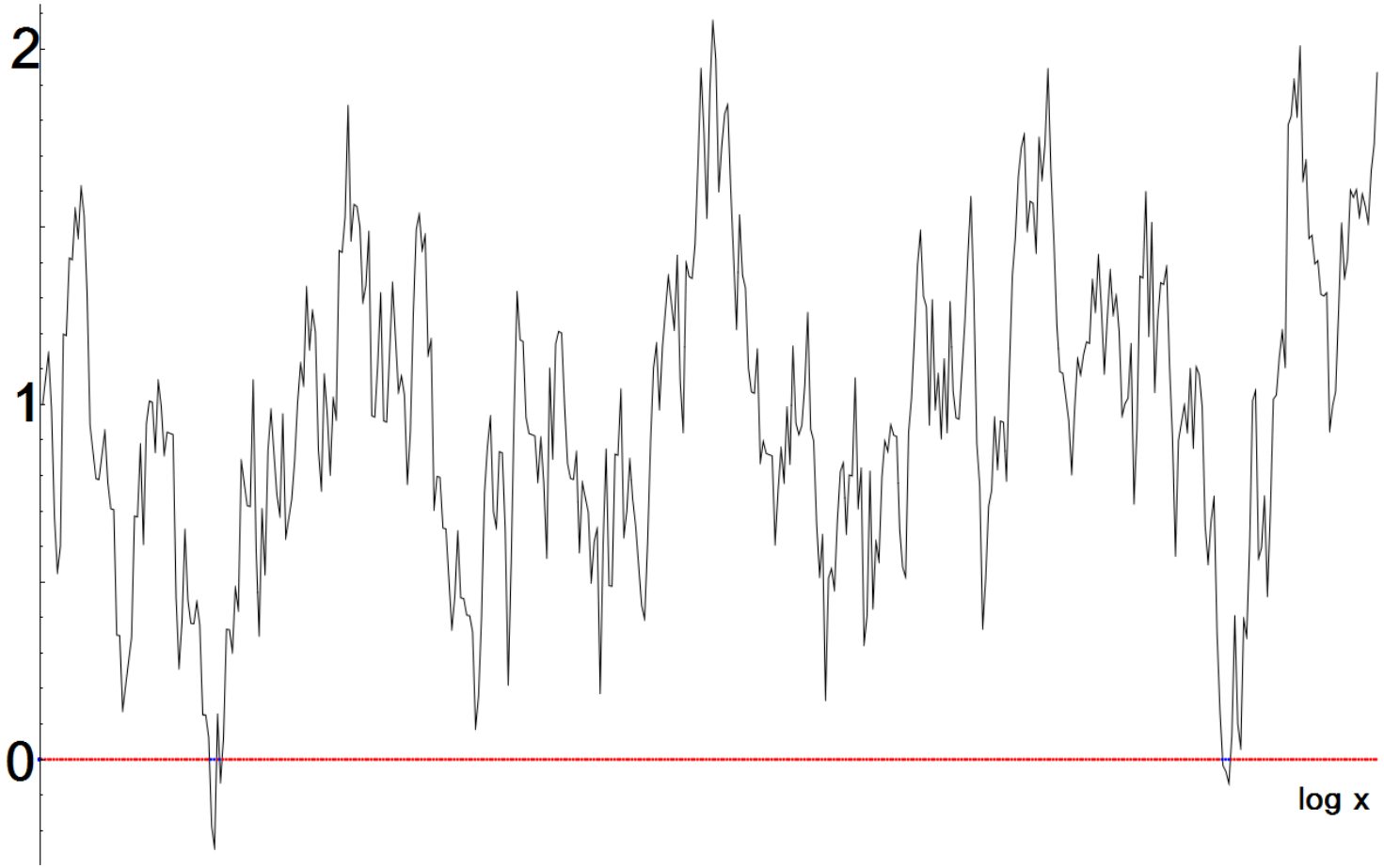
- Ils calculent également

$$\delta(\mathcal{P}_{3;2,1}) \approx 0.9990\ldots$$

ce qui était à prévoir car le plus petit élément de $\mathcal{P}_{3;1,2}$ est

$$608981813029(!)$$

Calculs numériques



$$\frac{\pi(x,4,3)-\pi(x,4,1)}{\sqrt{x}/\log x},\ 10^4 \leq x \leq 10^8$$

Source : Daniel Fiorilli

Théorème (Rubinstein, Sarnak, 1994).

Sous les mêmes hypothèses que précédemment, et si a et b sont simultanément des carrés ou non mod q, alors

$$\delta(\mathcal{P}_{q;a,b}) = \frac{1}{2}.$$

Si a est un carré mod q et b n'est pas un carré mod q alors

$$\delta(\mathcal{P}_{q;a,b}) < \frac{1}{2}.$$

Théorème (Rubinstein, Sarnak, 1994).

Sous les mêmes hypothèses que précédemment, et si a et b sont simultanément des carrés ou non mod q, alors

$$\delta(\mathcal{P}_{q;a,b}) = \frac{1}{2}.$$

Si a est un carré mod q et b n'est pas un carré mod q alors

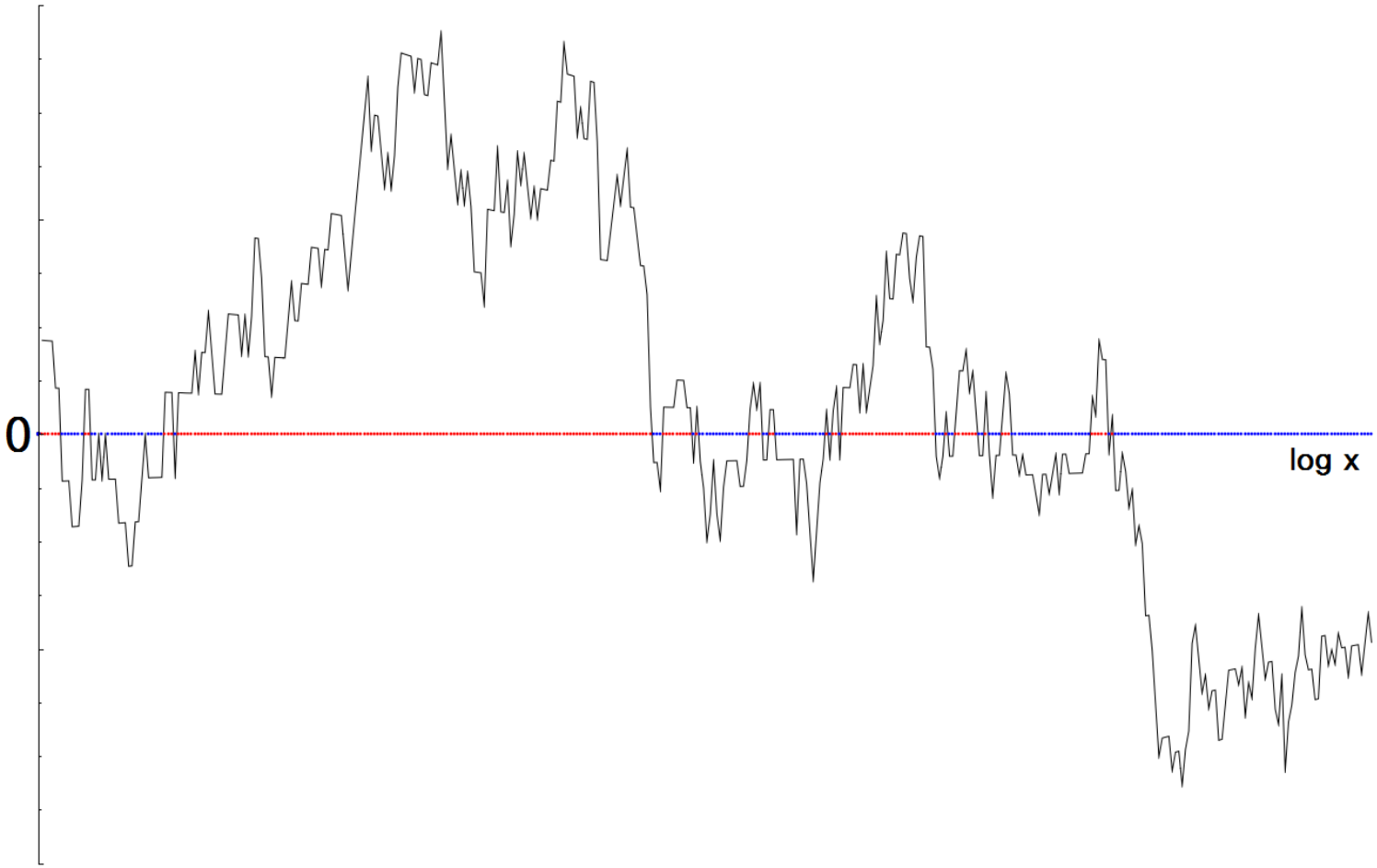
$$\delta(\mathcal{P}_{q;a,b}) < \frac{1}{2}.$$

Théorème (« central limite » pour les courses).

On a

$$\max_{\substack{a,b \\ (q,ab)=1}} \left| \delta(\mathcal{P}_{q;a,b}) - \frac{1}{2} \right| \underset{q \to +\infty}{\longrightarrow} 0.$$

Atténuation du biais



$$\frac{\pi(x,101,3)-\pi(x,101,1)}{\sqrt{x}/\log x},\ 10^4 \leq x \leq 10^8$$

Source : Daniel Fiorilli

Corps de nombres

Définition.

Un corps de nombres est un corps K de degré fini sur $\mathbb{Q}$. L'anneau des entiers de K est l'ensemble $\mathcal{O}_K$ des entiers algébriques dans K.

Corps de nombres

Définition.

Un corps de nombres est un corps K de degré fini sur $\mathbb{Q}$. L'anneau des entiers de K est l'ensemble $\mathcal{O}_K$ des entiers algébriques dans K.

- Un nombre algébrique est racine d'un polynôme à coefficients entiers.

Corps de nombres

Définition.

Un corps de nombres est un corps K de degré fini sur $\mathbb{Q}$. L'anneau des entiers de K est l'ensemble $\mathcal{O}_K$ des entiers algébriques dans K.

- Un nombre algébrique est racine d'un polynôme à coefficients entiers. Un entier algébrique est racine d'un polynôme **unitaire** à coefficients entiers.

Corps de nombres

Définition.

Un corps de nombres est un corps K de degré fini sur $\mathbb{Q}$. L'anneau des entiers de K est l'ensemble $\mathcal{O}_K$ des entiers algébriques dans K.

- Un nombre algébrique est racine d'un polynôme à coefficients entiers. Un entier algébrique est racine d'un polynôme **unitaire** à coefficients entiers.

$$K \longleftrightarrow \mathbb{Q}$$

$$\mathcal{O}_K \longleftrightarrow \mathbb{Z}$$

Arithmétique dans les corps de nombres

- L'anneau $\mathcal{O}_K$ n'est pas factoriel en général, par exemple dans

$$\mathcal{O}_{\mathbb{Q}(i\sqrt{5})} = \mathbb{Z}[i\sqrt{5}]$$

on a

$$6 = 2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$$

avec $2, 3, 1 + i\sqrt{5}$ et $1 - i\sqrt{5}$ irréductibles non associés.

Arithmétique dans les corps de nombres

Théorème (Dedekind, 1876).

Tout idéal $\mathcal{I}$ de $\mathcal{O}_K$ admet une factorisation (unique à l'ordre près des facteurs) sous la forme

$$\mathcal{I} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$$

où les $\mathfrak{p}_i$ sont des idéaux premiers de $\mathcal{O}_K$.

Arithmétique dans les corps de nombres

Théorème (Dedekind, 1876).

Tout idéal $\mathcal{I}$ de $\mathcal{O}_K$ admet une factorisation (unique à l'ordre près des facteurs) sous la forme

$$\mathcal{I} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$$

où les $\mathfrak{p}_i$ sont des idéaux premiers de $\mathcal{O}_K$.

- Par exemple, dans $\mathbb{Z}[i\sqrt{5}]$, on a $(6) = (2, 1+i\sqrt{5})^2(3, 1+i\sqrt{5})(3, 1-i\sqrt{5})$.

Arithmétique dans les corps de nombres

Théorème (Dedekind, 1876).

Tout idéal $\mathcal{I}$ de $\mathcal{O}_K$ admet une factorisation (unique à l'ordre près des facteurs) sous la forme

$$\mathcal{I} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$$

où les $\mathfrak{p}_i$ sont des idéaux premiers de $\mathcal{O}_K$.

- Par exemple, dans $\mathbb{Z}[i\sqrt{5}]$, on a $(6) = (2, 1+i\sqrt{5})^2(3, 1+i\sqrt{5})(3, 1-i\sqrt{5})$.
- Si p est un nombre premier, l'idéal $p\mathcal{O}_K$ admet donc une factorisation

$$(p) = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}.$$

Automorphismes de Frobenius

- Soit p un nombre premier et $\mathfrak{p}$ un idéal premier de K au-dessus de p. Alors on dispose d'une extension de corps finis

$$(\mathcal{O}_K/\mathfrak{p})/(\mathbb{Z}/p\mathbb{Z}).$$

Automorphismes de Frobenius

- Soit p un nombre premier et $\mathfrak{p}$ un idéal premier de K au-dessus de p. Alors on dispose d'une extension de corps finis

$$(\mathcal{O}_K/\mathfrak{p})/(\mathbb{Z}/p\mathbb{Z}).$$

- Cette extension est galoisienne, et un générateur du groupe de Galois est l'automorphisme de Frobenius

$$\begin{aligned} \mathcal{O}_K/\mathfrak{p} &\longrightarrow \mathcal{O}_K/\mathfrak{p} \\ x &\longmapsto x^p. \end{aligned}$$

Si $K/\mathbb{Q}$ est galoisienne, le Frobenius se remonte dans $\mathrm{Gal}(K/\mathbb{Q})$.

Automorphismes de Frobenius

- Pour les algébristes : on a une suite exacte

$$0 \longrightarrow I_{\mathfrak{p}} \longrightarrow D_{\mathfrak{p}} \longrightarrow \mathrm{Gal}\left((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p\right) \longrightarrow 0$$

où $D_{\mathfrak{p}} = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}$ et
$I_{\mathfrak{p}} = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mid \forall x \in \mathcal{O}_K, \sigma(x) \equiv x \bmod \mathfrak{p}\}$.

Automorphismes de Frobenius

- Pour les algébristes : on a une suite exacte

$$0 \longrightarrow I_{\mathfrak{p}} \longrightarrow D_{\mathfrak{p}} \longrightarrow \mathrm{Gal}\left((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p\right) \longrightarrow 0$$

où $D_{\mathfrak{p}} = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}$ et
$I_{\mathfrak{p}} = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mid \forall x \in \mathcal{O}_K, \sigma(x) \equiv x \bmod \mathfrak{p}\}$.

- Autrement dit, quand $I_{\mathfrak{p}}$ est trivial (ce qui arrive pour tous les p sauf un nombre fini), on a un $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(K/\mathbb{Q})$ déterminé par

$$\forall x \in \mathcal{O}_K, \mathrm{Frob}_{\mathfrak{p}}(x) \equiv x^p \bmod \mathfrak{p}.$$

Automorphismes de Frobenius

- Par contre, $\mathrm{Frob}_{\mathfrak{p}}$ dépend de $\mathfrak{p}$, mais seulement à conjugaison près. On a donc une classe de conjugaison dans $\mathrm{Gal}(K/\mathbb{Q})$, notée Frob_p, appelée (classe d') automorphisme de Frobenius de p dans $\mathrm{Gal}(K/\mathbb{Q})$.

Automorphismes de Frobenius

- Par contre, $\mathrm{Frob}_{\mathfrak{p}}$ dépend de $\mathfrak{p}$, mais seulement à conjugaison près. On a donc une classe de conjugaison dans $\mathrm{Gal}(K/\mathbb{Q})$, notée Frob_p, appelée (classe d') automorphisme de Frobenius de p dans $\mathrm{Gal}(K/\mathbb{Q})$.

Théorème (Chebotarev, 1928).

Soit C une classe de conjugaison de $G := \mathrm{Gal}(K/\mathbb{Q})$. Alors

$$\pi(x, K/\mathbb{Q}, C) := \#\{p \leq x \mid \mathrm{Frob}_p = C\} \underset{x \to +\infty}{\sim} \frac{|C|}{|G|} \frac{x}{\log x}.$$

Retour aux sources

- Soit $q \geq 1$. On considère $K = \mathbb{Q}(\zeta_q)$, où ζ_q est une racine primitive q-ième de l'unité. On a alors un isomorphisme

$$\begin{aligned} (\mathbb{Z}/q\mathbb{Z})^\times &\longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \\ a &\longmapsto \left(\zeta_q \mapsto \zeta_q^a\right). \end{aligned}$$

Retour aux sources

- Soit $q \geq 1$. On considère $K = \mathbb{Q}(\zeta_q)$, où ζ_q est une racine primitive q-ième de l'unité. On a alors un isomorphisme

$$\begin{aligned} (\mathbb{Z}/q\mathbb{Z})^\times &\longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \\ a &\longmapsto \left(\zeta_q \mapsto \zeta_q^a\right). \end{aligned}$$

- Pour $a \in \mathbb{Z}$ premier avec q et $p \equiv a \bmod q$, on vérifie facilement que

$$\mathrm{Frob}_p : \zeta_q \mapsto \zeta_q^p = \zeta_q^a.$$

Retour aux sources

- Soit $q \geq 1$. On considère $K = \mathbb{Q}(\zeta_q)$, où ζ_q est une racine primitive q-ième de l'unité. On a alors un isomorphisme

$$\begin{aligned} (\mathbb{Z}/q\mathbb{Z})^\times &\longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \\ a &\longmapsto \left(\zeta_q \mapsto \zeta_q^a\right). \end{aligned}$$

- Pour $a \in \mathbb{Z}$ premier avec q et $p \equiv a \bmod q$, on vérifie facilement que

$$\mathrm{Frob}_p : \zeta_q \mapsto \zeta_q^p = \zeta_q^a.$$

Le théorème de Chebotarev donne alors que

$$\#\{p \leq x \mid p \equiv a \bmod q\} \underset{x \to +\infty}{\sim} \frac{1}{\varphi(q)} \frac{x}{\log x}.$$

Une autre application arithmétique

- Soit $d \in \mathbb{Z} \setminus \{0, 1\}$ sans facteur carré. On considère $K = \mathbb{Q}(\sqrt{d})$. Alors $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$ est d'ordre 2, et on note σ son élément non trivial, $\sigma : \sqrt{d} \mapsto -\sqrt{d}$.

Une autre application arithmétique

- Soit $d \in \mathbb{Z} \setminus \{0, 1\}$ sans facteur carré. On considère $K = \mathbb{Q}(\sqrt{d})$. Alors $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$ est d'ordre 2, et on note σ son élément non trivial, $\sigma : \sqrt{d} \mapsto -\sqrt{d}$.

- On montre que pour p premier ne divisant pas $2d$,

$$\mathrm{Frob}_p = \sigma \Leftrightarrow d \text{ n'est pas un carré modulo } p.$$

Une autre application arithmétique

- Soit $d \in \mathbb{Z} \setminus \{0, 1\}$ sans facteur carré. On considère $K = \mathbb{Q}(\sqrt{d})$. Alors $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$ est d'ordre 2, et on note σ son élément non trivial, $\sigma : \sqrt{d} \mapsto -\sqrt{d}$.

- On montre que pour p premier ne divisant pas $2d$,

$$\mathrm{Frob}_p = \sigma \Leftrightarrow d \text{ n'est pas un carré modulo } p.$$

- Le théorème de Chebotarev donne donc

$$\#\{p \leq x \mid d \text{ n'est pas carré mod } p\} \underset{x \to +\infty}{\sim} \#\{p \leq x \mid d \text{ est carré mod } p\}$$
$$\underset{x \to +\infty}{\sim} \frac{1}{2} \frac{x}{\log x}.$$

Fonctions L d'Artin

- À un caractère d'une représentation linéaire ρ de $\mathrm{Gal}(K/\mathbb{Q})$, on associe une fonction L (d'Artin), donnée par un produit eulérien, dont un facteur typique est

$$\left(\det\left(id - \frac{\rho(\mathrm{Frob}_p)}{p^s}\right)\right)^{-1},$$

qui va jouer un rôle analogues aux fonctions L de Dirichlet dans le cadre des progressions arithmétiques.

Fonctions L d'Artin

- À un caractère d'une représentation linéaire ρ de $\mathrm{Gal}(K/\mathbb{Q})$, on associe une fonction L (d'Artin), donnée par un produit eulérien, dont un facteur typique est

$$\left(\det\left(id - \frac{\rho(\mathrm{Frob}_p)}{p^s}\right)\right)^{-1},$$

  qui va jouer un rôle analogues aux fonctions L de Dirichlet dans le cadre des progressions arithmétiques.

- Le théorème de Chebotarev provient de l'étude des propriétés analytiques de ces fonctions, et de la répartition de leurs zéros.

Courses dans les corps de nombres

- On fixe deux classes de conjugaison C_1 et C_2 de $\mathrm{Gal}(K/\mathbb{Q})$, et on veut étudier la course entre les nombres premiers p tels que $\mathrm{Frob}_p = C_1$ et ceux tels que $\mathrm{Frob}_p = C_2$.

Courses dans les corps de nombres

- On fixe deux classes de conjugaison C_1 et C_2 de $\mathrm{Gal}(K/\mathbb{Q})$, et on veut étudier la course entre les nombres premiers p tels que $\mathrm{Frob}_p = C_1$ et ceux tels que $\mathrm{Frob}_p = C_2$.

- Pour équilibrer la course, on regarde le signe de

$$\frac{\pi(x, K/\mathbb{Q}, C_1)}{|C_1|} - \frac{\pi(x, K/\mathbb{Q}, C_2)}{|C_2|}.$$

Courses dans les corps de nombres

- On fixe deux classes de conjugaison C_1 et C_2 de $\mathrm{Gal}(K/\mathbb{Q})$, et on veut étudier la course entre les nombres premiers p tels que $\mathrm{Frob}_p = C_1$ et ceux tels que $\mathrm{Frob}_p = C_2$.

- Pour équilibrer la course, on regarde le signe de

$$\frac{\pi(x, K/\mathbb{Q}, C_1)}{|C_1|} - \frac{\pi(x, K/\mathbb{Q}, C_2)}{|C_2|}.$$

On pose

$$\mathcal{P}_{K/\mathbb{Q};C_1,C_2} = \left\{ x \geq 2 \mid \frac{\pi(x, K/\mathbb{Q}, C_1)}{|C_1|} > \frac{\pi(x, K/\mathbb{Q}, C_2)}{|C_2|} \right\}.$$

Courses dans les corps de nombres

Théorème (Ng, 2000).

« Tout se passe comme pour les courses de nombres premiers, en remplaçant les fonctions L de Dirichlet par les fonctions L d'Artin. »

En supposant l'hypothèse de Riemann, la conjecture d'Artin et l'indépendance linéaire des parties imaginaires des zéros non triviaux des fonctions L d'Artin associées aux caractères irréductibles de $K/\mathbb{Q}$, $\delta(\mathcal{P}_{K/\mathbb{Q};C_1,C_2})$ existe et satisfait $0 < \delta(\mathcal{P}_{K/\mathbb{Q};C_1,C_2}) < 1$.

Courses dans les corps de nombres

Théorème (Ng, 2000).

« Tout se passe comme pour les courses de nombres premiers, en remplaçant les fonctions L de Dirichlet par les fonctions L d'Artin. »

En supposant l'hypothèse de Riemann, la conjecture d'Artin et l'indépendance linéaire des parties imaginaires des zéros non triviaux des fonctions L d'Artin associées aux caractères irréductibles de $K/\mathbb{Q}$, $\delta(\mathcal{P}_{K/\mathbb{Q};C_1,C_2})$ existe et satisfait $0 < \delta(\mathcal{P}_{K/\mathbb{Q};C_1,C_2}) < 1$.

- Une différence par rapport aux progressions arithmétiques : les fonctions L d'Artin peuvent admettre un zéro en $\frac{1}{2}$, ce qui peut avoir une influence sur la répartition des

$$\frac{\pi(x, K/\mathbb{Q}, C_1)}{|C_1|} - \frac{\pi(x, K/\mathbb{Q}, C_2)}{|C_2|}.$$

Root numbers

- Comment produire des zéros en 1/2 ?

Root numbers

- Comment produire des zéros en 1/2 ? Les fonctions L d'Artin vérifient une équation fonctionnelle de la forme $\Lambda(s,\chi) = W(\chi)\Lambda(1-s,\overline{\chi})$ avec $|W(\chi)| = 1$.

Root numbers

- Comment produire des zéros en 1/2 ? Les fonctions L d'Artin vérifient une équation fonctionnelle de la forme $\Lambda(s,\chi) = W(\chi)\Lambda(1-s,\overline{\chi})$ avec $|W(\chi)| = 1$.

- Si χ prend des valeurs réelles, $W(\chi) = \pm 1$. En particulier, si $W(\chi) = -1$ alors $\Lambda(1/2,\chi) = 0$ (et donc $L(1/2,\chi) = 0$).

Root numbers

- Comment produire des zéros en 1/2 ? Les fonctions L d'Artin vérifient une équation fonctionnelle de la forme $\Lambda(s,\chi) = W(\chi)\Lambda(1-s,\overline{\chi})$ avec $|W(\chi)| = 1$.
- Si χ prend des valeurs réelles, $W(\chi) = \pm 1$. En particulier, si $W(\chi) = -1$ alors $\Lambda(1/2,\chi) = 0$ (et donc $L(1/2,\chi) = 0$).
- Parmi les caractères réels, seuls les **symplectiques** peuvent fournir un root number $W(\chi) = -1$.

Groupes de quaternions

- Le groupe $\mathbb{H}_8$ est $\{\pm 1, \pm i, \pm j, \pm k\}$ avec -1 central et

$$i^2 = j^2 = k^2 = ijk = -1.$$

Groupes de quaternions

- Le groupe $\mathbb{H}_8$ est $\{\pm 1, \pm i, \pm j, \pm k\}$ avec -1 central et

$$i^2 = j^2 = k^2 = ijk = -1.$$

- Plus généralement, le groupe de quaternions généralisés d'ordre $2^n, n \geq 3$ est

$$\mathbb{H}_{2^n} = \langle x, y \mid x^{2^{n-2}} = y^2, x^{2^{n-1}} = 1, yxy^{-1} = x^{-1} \rangle.$$

Groupes de quaternions

- Le groupe $\mathbb{H}_8$ est $\{\pm 1, \pm i, \pm j, \pm k\}$ avec -1 central et

$$i^2 = j^2 = k^2 = ijk = -1.$$

- Plus généralement, le groupe de quaternions généralisés d'ordre $2^n, n \geq 3$ est

$$\mathbb{H}_{2^n} = \langle x, y \mid x^{2^{n-2}} = y^2, x^{2^{n-1}} = 1, yxy^{-1} = x^{-1} \rangle.$$

- Pourquoi s'intéresser à ces groupes ? Leurs tables de caractères sont les mêmes que celles des groupes diédraux $D_{2^{n-1}}$ (d'ordre 2^n),

Groupes de quaternions

- Le groupe $\mathbb{H}_8$ est $\{\pm 1, \pm i, \pm j, \pm k\}$ avec -1 central et
$$i^2 = j^2 = k^2 = ijk = -1.$$
- Plus généralement, le groupe de quaternions généralisés d'ordre $2^n, n \geq 3$ est
$$\mathbb{H}_{2^n} = \langle x, y \mid x^{2^{n-2}} = y^2, x^{2^{n-1}} = 1, yxy^{-1} = x^{-1} \rangle.$$
- Pourquoi s'intéresser à ces groupes ? Leurs tables de caractères sont les mêmes que celles des groupes diédraux $D_{2^{n-1}}$ (d'ordre 2^n), mais surtout ils ont beaucoup de caractères irréductibles symplectiques : 2^{n-3}.

Théorème

Théorème (B., aspect horizontal).

Sous les hypothèses précédentes, il existe deux familles $(K_d)_d$ et $(L_d)_d$ d'extensions galoisiennes de $\mathbb{Q}$ contenant $\mathbb{Q}(\sqrt{d})$ et telles que :

i) Pour tout $d \equiv 1 \bmod 4$ sans facteur carré,

$$\mathrm{Gal}(K_d/\mathbb{Q}) \simeq \mathrm{Gal}(L_d/\mathbb{Q}) \simeq \mathbb{H}_8.$$

ii)
$$0 < \frac{1}{2} - \delta(\mathcal{P}_{K_d/\mathbb{Q};1,-1}) \ll \frac{1}{(\log d)^{1/3}}.$$

iii)
$$0 < \delta(\mathcal{P}_{L_d/\mathbb{Q};1,-1}) - \frac{1}{2} \ll \frac{1}{(\log d)^{1/3}}.$$

Idées de démonstration

- Trouver deux familles d'extensions de $\mathbb{Q}$ de groupe de Galois $\mathbb{H}_8$ telles que $L\left(\frac{1}{2}, \psi, K/\mathbb{Q}\right) = 0$ et $L\left(\frac{1}{2}, \psi, L\right) = 0$. (Fröhlich, 70's)

Idées de démonstration

- Trouver deux familles d'extensions de $\mathbb{Q}$ de groupe de Galois $\mathbb{H}_8$ telles que $L\left(\frac{1}{2}, \psi, K/\mathbb{Q}\right) = 0$ et $L\left(\frac{1}{2}, \psi, L\right) = 0$. (Fröhlich, 70's)

- Pour estimer le biais, on utilise qu'il peut s'écrire sous la forme $\mathbb{P}(X > 0)$, où X est "connue".

Idées de démonstration

- Trouver deux familles d'extensions de $\mathbb{Q}$ de groupe de Galois $\mathbb{H}_8$ telles que $L\left(\frac{1}{2}, \psi, K/\mathbb{Q}\right) = 0$ et $L\left(\frac{1}{2}, \psi, L\right) = 0$. (Fröhlich, 70's)

- Pour estimer le biais, on utilise qu'il peut s'écrire sous la forme $\mathbb{P}(X > 0)$, où X est "connue".

- On met en évidence un comportement de type "théorème central limite" grâce au comportement de la quantité

$$\frac{\mathbb{E}(X)}{\mathrm{Var}(X)^{1/2}}.$$

Théorème

Théorème (B., aspect vertical).

Sous les hypothèses précédentes, il existe deux familles $(Q_n^+)_{n\geq 3}$ et $(Q_n^-)_{n\geq 3}$ d'extensions galoisiennes de $\mathbb{Q}$ telles que :

i) Pour tout $n \geq 3$,

$$\mathrm{Gal}(Q_n^{\pm}/\mathbb{Q}) \simeq \mathbb{H}_{2^n}.$$

ii)

$$c_1 \exp\left(-c_2 \frac{2^n}{n}\right) < 1 - \delta(\mathcal{P}_{Q_n^+/\mathbb{Q};1,-1}) < \exp\left(-c_3 \frac{2^n}{n}\right).$$

iii)

$$c_1 \exp\left(-c_2 \frac{2^n}{n}\right) < \delta(\mathcal{P}_{Q_n^-/\mathbb{Q};1,-1}) < \exp\left(-c_3 \frac{2^n}{n}\right).$$

Théorème

Théorème (B., aspect vertical).

Sous les hypothèses précédentes, il existe deux familles $(Q_n^+)_{n\geq 3}$ et $(Q_n^-)_{n\geq 3}$ d'extensions galoisiennes de $\mathbb{Q}$ telles que :

i) Pour tout $n \geq 3$,

$$\mathrm{Gal}(Q_n^{\pm}/\mathbb{Q}) \simeq \mathbb{H}_{2^n}.$$

ii)

$$c_1 \exp\left(-c_2 \frac{2^n}{n}\right) < 1 - \delta(\mathcal{P}_{Q_n^+/\mathbb{Q};1,-1}) < \exp\left(-c_3 \frac{2^n}{n}\right).$$

iii)

$$c_1 \exp\left(-c_2 \frac{2^n}{n}\right) < \delta(\mathcal{P}_{Q_n^-/\mathbb{Q};1,-1}) < \exp\left(-c_3 \frac{2^n}{n}\right).$$

- Démonstration : Proche du théorème précédent, mais la construction est beaucoup plus compliquée (théorie de Fröhlich de "Galois-module", contrôle du discriminant avec GRH). On exhibe un comportement de type « grandes déviations ».

Pour conclure : quelques pistes

i) Affaiblir les hypothèses d'indépendance linéaire sur les parties imaginaires des zéros.

Pour conclure : quelques pistes

i) Affaiblir les hypothèses d'indépendance linéaire sur les parties imaginaires des zéros.

ii) Étudier l'évolution du biais de Tchebychev dans des extensions de corps de fonctions de courbes sur des corps finis.

Merci de votre attention !