Fonctions L et courses de nombres premiers

Alexandre Bailleul

Université de Bordeaux

15 octobre 2018

Sommaire

Plan

Une infinité de nombres premiers

Théorème (Euclide).

Il existe une infinité de nombres premiers.

Une infinité de nombres premiers

Théorème (Euclide).

Il existe une infinité de nombres premiers.

Démonstration. Si $p_1, \ldots, p_n$ sont des nombres premiers, les facteurs premiers de

$$p_1 \ldots p_n + 1$$

ne font pas partie des p_i. □

Complications

Proposition.

Il existe une infinité de nombres premiers de la forme $p = 4n + 3, n \in \mathbb{Z}$.

Complications

Proposition.

Il existe une infinité de nombres premiers de la forme $p = 4n + 3, n \in \mathbb{Z}$.

Démonstration. On considère

$$4(p_1 \dots p_n) - 1.$$

□

Complications

Proposition.

Il existe une infinité de nombres premiers de la forme $p = 4n + 3, n \in \mathbb{Z}$.

Démonstration. On considère

$$4(p_1 \dots p_n) - 1.$$

□

Proposition.

Il existe une infinité de nombres premiers de la forme $p = 4n + 1, n \in \mathbb{Z}$.

Complications

Proposition.

Il existe une infinité de nombres premiers de la forme $p = 4n+3, n \in \mathbb{Z}$.

Démonstration. On considère

$$4(p_1 \dots p_n) - 1.$$

□

Proposition.

Il existe une infinité de nombres premiers de la forme $p = 4n+1, n \in \mathbb{Z}$.

Démonstration. On considère

$$4(p_1 \dots p_n)^2 + 1,$$

et on utilise

$$-1 \text{ est un carré mod } p \Leftrightarrow p = 2 \text{ ou } p = 1 \bmod 4.$$

Complications

Question : Si a et q sont premiers entre eux (condition nécessaire), existe-t-il toujours une infinité de nombres premiers de la forme $a + qn, n \in \mathbb{Z}$?

Complications

Question : Si a et q sont premiers entre eux (condition nécessaire), existe-t-il toujours une infinité de nombres premiers de la forme $a + qn, n \in \mathbb{Z}$?

Théorème (Schur 1912, Ram Murty, 1988).

Soient $a, q \in \mathbb{Z}$ premiers entre eux. Il existe une « preuve euclidienne » de l'existence d'une infinité de nombres premiers de la forme $a + qn, n \in \mathbb{Z}$ si et seulement si $a^2 = 1 \bmod q$.

Caractères de Dirichlet

Définition.

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

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

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

Caractères de Dirichlet

Définition.

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

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

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

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

ii) Le caractère χ modulo 5 défini par

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

Caractères de Dirichlet

ii) Le caractère χ modulo 5 défini par

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

iii) Le caractère χ_4 modulo 4 défini par

$$\chi_4(n) = \begin{cases} 1 \text{ si } n = 1 \bmod 4 \\ -1 \text{ si } n = 3 \bmod 4 \\ 0 \text{ sinon} \end{cases} .$$

Caractères de Dirichlet

ii) Le caractère χ modulo 5 défini par

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

iii) Le caractère χ_4 modulo 4 défini par

$$\chi_4(n) = \begin{cases} 1 \text{ si } n = 1 \bmod 4 \\ -1 \text{ si } n = 3 \bmod 4 \\ 0 \text{ sinon} \end{cases}.$$

iv) 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

Quelque propriétés :

Proposition.

Soit $q \geq 1$ un entier.

a) Pour tout caractère de Dirichlet modulo q et $a \in \mathbb{Z}$ premier avec q, $\chi(a)$ est une racine $\varphi(q)$-ième de l'unité dans $\mathbb{C}$. En particulier $\overline{\chi(a)} = \chi(a)^{-1}$.

Caractères de Dirichlet

Quelque propriétés :

Proposition.

Soit $q \geq 1$ un entier.

a) Pour tout caractère de Dirichlet modulo q et $a \in \mathbb{Z}$ premier avec q, $\chi(a)$ est une racine $\varphi(q)$-ième de l'unité dans $\mathbb{C}$. En particulier $\overline{\chi(a)} = \chi(a)^{-1}$.

b) *Relations d'orthogonalité :* Pour $a \in \mathbb{Z}$ premier avec q et $k \in \mathbb{Z}$, on a

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

Caractères de Dirichlet

Quelque propriétés :

Proposition.

Soit $q \geq 1$ un entier.

a) Pour tout caractère de Dirichlet modulo q et $a \in \mathbb{Z}$ premier avec q, $\chi(a)$ est une racine $\varphi(q)$-ième de l'unité dans $\mathbb{C}$. En particulier $\overline{\chi(a)} = \chi(a)^{-1}$.

b) *Relations d'orthogonalité :* Pour $a \in \mathbb{Z}$ premier avec q et $k \in \mathbb{Z}$, on a

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

Les caractères de Dirichlet permette de détecter analytiquement la condition $k = a$ 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.

Soit $q \geq 1$ un entier et χ un caractère de Dirichlet modulo q.

a) La fonction $s \mapsto L(s, \chi)$ est définie (et holomorphe) pour $\mathfrak{Re}(s) > 1$, et même pour $\mathfrak{Re}(s) > 0$ si $\chi \neq \chi_0$.

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.

Soit $q \geq 1$ un entier et χ un caractère de Dirichlet modulo q.

a) La fonction $s \mapsto L(s,\chi)$ est définie (et holomorphe) pour $\mathfrak{Re}(s) > 1$, et même pour $\mathfrak{Re}(s) > 0$ si $\chi \neq \chi_0$.

b) Pour $\mathfrak{Re}(s) > 1$, on a

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

Fonctions L de Dirichlet

En particulier pour $s > 1$ réel on a

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

Fonctions L de Dirichlet

En particulier pour $s > 1$ réel on a

$$\log(L(s,\chi)) = -\sum_p \log\left(1-\frac{\chi(p)}{p^s}\right) = \sum_p \frac{\chi(p)}{p^s} + O(1).$$

Fonctions L de Dirichlet

En particulier pour $s > 1$ réel on a

$$\log(L(s,\chi)) = -\sum_p \log\left(1-\frac{\chi(p)}{p^s}\right) = \sum_p \frac{\chi(p)}{p^s} + O(1).$$

D'après les relations d'orthogonalités on trouve, pour $a \in \mathbb{Z}$ premier avec q,

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

Retour aux nombres premiers

Prenons le cas $q = 4, a = 1$. La formule précédente donne, pour $s > 1$,

$$\frac{1}{2}(\log(L(s,\chi_0)) + \log(L(s,\chi_4))) = \sum_{p=1 \bmod 4} \frac{1}{p^s} + O(1).$$

Retour aux nombres premiers

Prenons le cas $q = 4, a = 1$. La formule précédente donne, pour $s > 1$,

$$\frac{1}{2}(\log(L(s,\chi_0)) + \log(L(s,\chi_4))) = \sum_{p=1 \bmod 4} \frac{1}{p^s} + O(1).$$

Or

$$L(1,\chi_4) = \sum_{n=0}^{+\infty} \frac{(-1)^n}{2n+1} = \frac{\pi}{4} \neq 0,$$

Retour aux nombres premiers

Prenons le cas $q = 4, a = 1$. La formule précédente donne, pour $s > 1$,

$$\frac{1}{2}(\log(L(s,\chi_0)) + \log(L(s,\chi_4))) = \sum_{p=1 \bmod 4} \frac{1}{p^s} + O(1).$$

Or

$$L(1,\chi_4) = \sum_{n=0}^{+\infty} \frac{(-1)^n}{2n+1} = \frac{\pi}{4} \neq 0,$$

tandis que

$$L(s,\chi_0) \underset{s\to 1}{\longrightarrow} +\infty,$$

Retour aux nombres premiers

Prenons le cas $q = 4, a = 1$. La formule précédente donne, pour $s > 1$,

$$\frac{1}{2}(\log(L(s,\chi_0)) + \log(L(s,\chi_4))) = \sum_{p=1 \bmod 4} \frac{1}{p^s} + O(1).$$

Or

$$L(1,\chi_4) = \sum_{n=0}^{+\infty} \frac{(-1)^n}{2n+1} = \frac{\pi}{4} \neq 0,$$

tandis que

$$L(s,\chi_0) \underset{s\to 1}{\longrightarrow} +\infty,$$

donc en faisant tendre s vers 1, on trouve que la série des $\frac{1}{p}$, $p = 1 \bmod 4$, diverge.

Théorème de la progression arithmétique

Théorème (Dirichlet, 1837).

Soit $q \geq 1$ un entier et $\chi \neq \chi_0$ un caractère de Dirichlet. Alors

$$L(1, \chi) \neq 0.$$

Théorème de la progression arithmétique

Théorème (Dirichlet, 1837).

Soit $q \geq 1$ un entier et $\chi \neq \chi_0$ un caractère de Dirichlet. Alors

$$L(1, \chi) \neq 0.$$

Corollaire (Théorème de la progression arithmétique).

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

Théorème des nombres premiers en progression arithmétique

Théorème (De la Vallée-Poussin, 1899).

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

$$\pi(x, q, a) = |\{p \leq x \,|\, p = a \bmod q\}|.$$

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 $q \in Z$ et $a \in \mathbb{Z}$ premier avec q. On note

$$\pi(x, q, a) = |\{p \leq x \,|\, p = a \bmod q\}|.$$

Alors

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

Moralement, les nombres premiers sont **bien répartis asymptotiquement** dans les classes inversibles modulo q.

Théorème des nombres premiers en progression arithmétique

Théorème (De la Vallée-Poussin, 1899).

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

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

Alors

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

Moralement, les nombres premiers sont **bien répartis asymptotiquement** dans les classes inversibles modulo q.
Un nombre premier a une « probabilité » $\frac{1}{\varphi(q)}$ de valoir a mod q, en vertu du théorème des nombres premiers

$$\pi(x) \underset{x \to +\infty}{\sim} \frac{x}{\log x}.$$

Plan

Biais de Chebychev

Bien que, pour a et b inversibles modulo q, $\pi(x, q, a)$ et $\pi(x, q, b)$ soient asymptotiquement équivalents, on peut observer une asymétrie.

Biais de Chebychev

Bien que, pour a et b inversibles modulo q, $\pi(x, q, a)$ et $\pi(x, q, b)$ soient asymptotiquement équivalents, on peut observer une asymétrie.

En 1853, Chebychev écrit dans une lettre à Fuss qu'il semble qu'on ait toujours

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

Biais de Chebychev

Bien que, pour a et b inversibles modulo q, $\pi(x, q, a)$ et $\pi(x, q, b)$ soient asymptotiquement équivalents, on peut observer une asymétrie.

En 1853, Chebychev écrit dans une lettre à Fuss qu'il semble qu'on ait toujours

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

Il prétend même que

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

Biais de Chebychev

Problèmes :

i) Chebychev n'a pas regardé assez loin : en dessous de 26861, on a plus de $p = 1 \bmod 4$ que de $p = 3 \bmod 4$.

Biais de Chebychev

Problèmes :

i) Chebychev n'a pas regardé assez loin : en dessous de 26861, on a plus de $p = 1 \bmod 4$ que de $p = 3 \bmod 4$.

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

Biais de Chebychev

Problèmes :

i) Chebychev n'a pas regardé assez loin : en dessous de 26861, on a plus de $p = 1 \bmod 4$ que de $p = 3 \bmod 4$.

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 $L(s, \chi_4)$...

Biais de Chebychev

Cependant, ce phénomène (appelé **biais de Chebychev**) semble quand même présent

Biais de Chebychev

Cependant, ce phénomène (appelé **biais de Chebychev**) semble quand même présent : juste après 26861, la « course » entre l'équipe 1 mod 4 vs 3 mod 4 rebascule en la faveur des premiers $p = 3 \bmod 4$ pendant longtemps.

Biais de Chebychev

Cependant, ce phénomène (appelé **biais de Chebychev**) semble quand même présent : juste après 26861, la « course » entre l'équipe 1 mod 4 vs 3 mod 4 rebascule en la faveur des premiers $p = 3 \bmod 4$ 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), un candidat naturel pour la 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), un candidat naturel pour la 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 jamais (Wintner, 1941).

Quantifier le biais

La solution est de parcourir l'ensemble $\mathcal{P}_{q;a,b}$ à une vitesse logarithmique (changement d'échelle naturel quand on parle de nombres premiers).

Quantifier le biais

La solution est de parcourir l'ensemble $\mathcal{P}_{q;a,b}$ à une vitesse logarithmique (changement d'échelle naturel quand on parle de nombres premiers).

Définition.

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

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

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 » !

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 exactes**).

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 exactes**).

Sous l'hypothèse de Riemann, on a

$$\pi(x, q, c) = \frac{1}{\varphi(q)} \frac{x}{\log x} + \text{ erreur en } \sqrt{x},$$

il est donc naturel de regarder le signe de

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

Idées de preuve

La théorie donne

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

où la somme porte sur les parties imaginaires des zéros non triviaux des $L(s,\chi)$ avec $\chi \neq \chi_0$ (rappel : sous GRH les zéros sont de la forme $\frac{1}{2}+i\gamma$).

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

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

L'hypothèse d'indépendance linéaire sur $\mathbb{Q}$ de ces γ_χ permet d'appliquer le théorème d'équirépartition de Kronecker-Weyl : les termes oscillants $e^{i\gamma_\chi t}$ se répartissent bien dans le "tore infini" $(\mathbb{S}^1)^\infty$.

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

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

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

Calculs numériques

Rubinstein et Sarnak calculent

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

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

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 Chebychev est quantifié : « 99% du temps », les premiers $p = 3 \bmod 4$ sont plus nombreux que les premiers $p = 1 \bmod 4$.

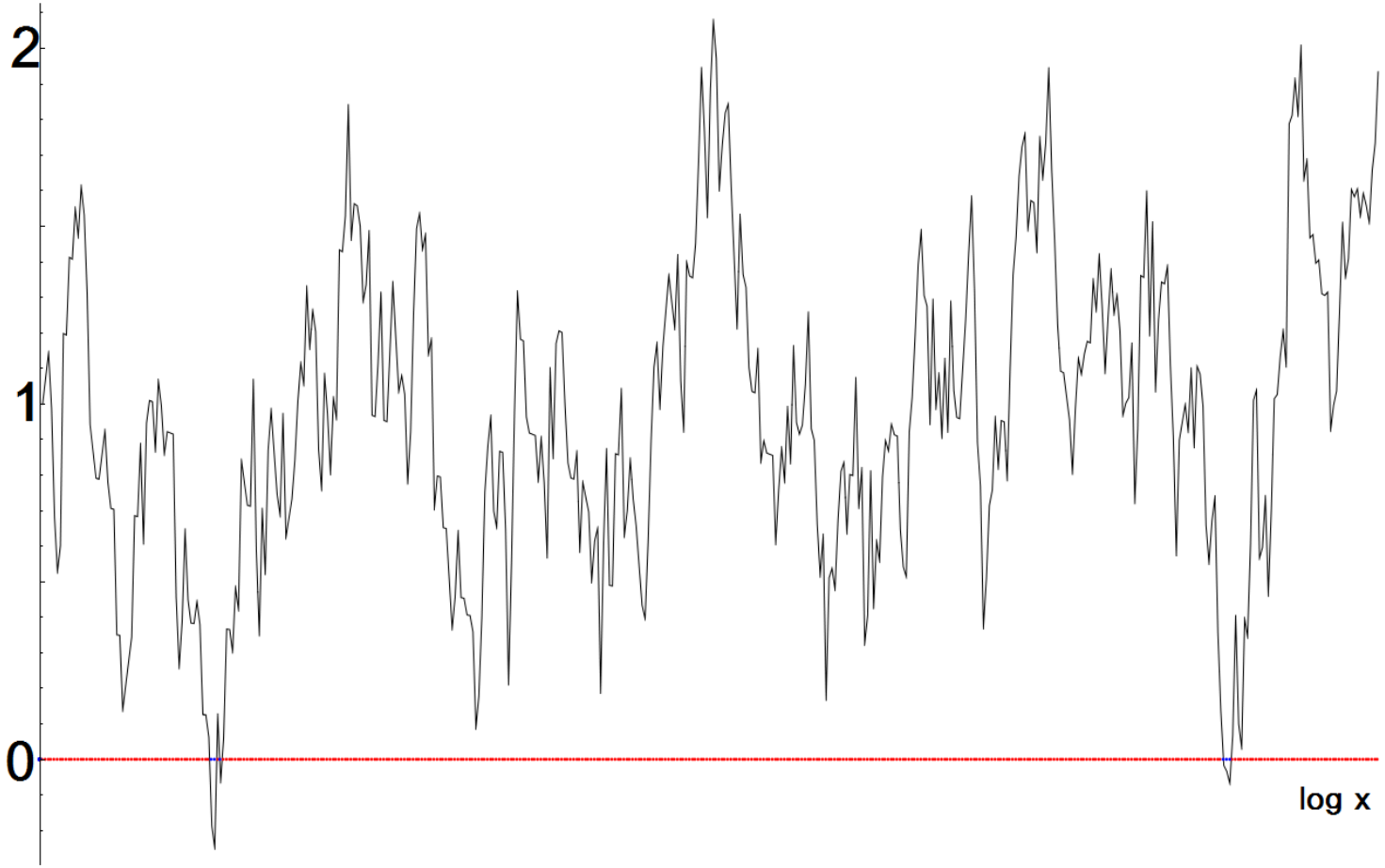
Ils calculent également

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

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

$$608981813029(!)$$

Quelques graphes



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

Source : Daniel Fiorilli

Quelques résultats

Théorème (Rubinstein, Sarnak, 1994).

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

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

Quelques résultats

Théorème (Rubinstein, Sarnak, 1994).

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

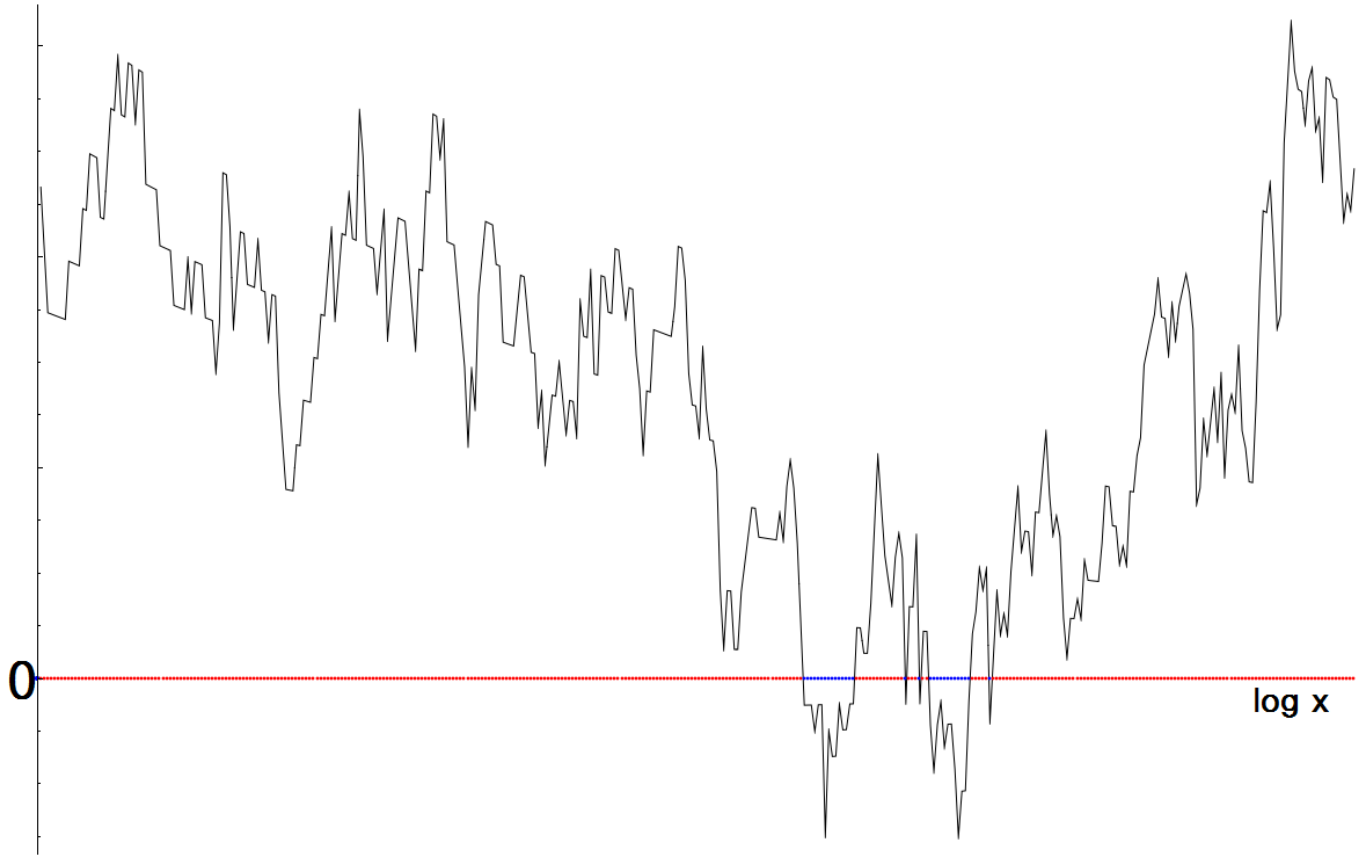
$$\delta(\mathcal{P}_{q;a,b}) = \frac{1}{2}.$$

Théorème (« central limite » pour les courses).

Si a et b sont fixés et q parcourt l'ensemble des entiers premiers avec a et b, alors

$$\delta(\mathcal{P}_{q;a,b}) \underset{q\to+\infty}{\longrightarrow} \frac{1}{2}.$$

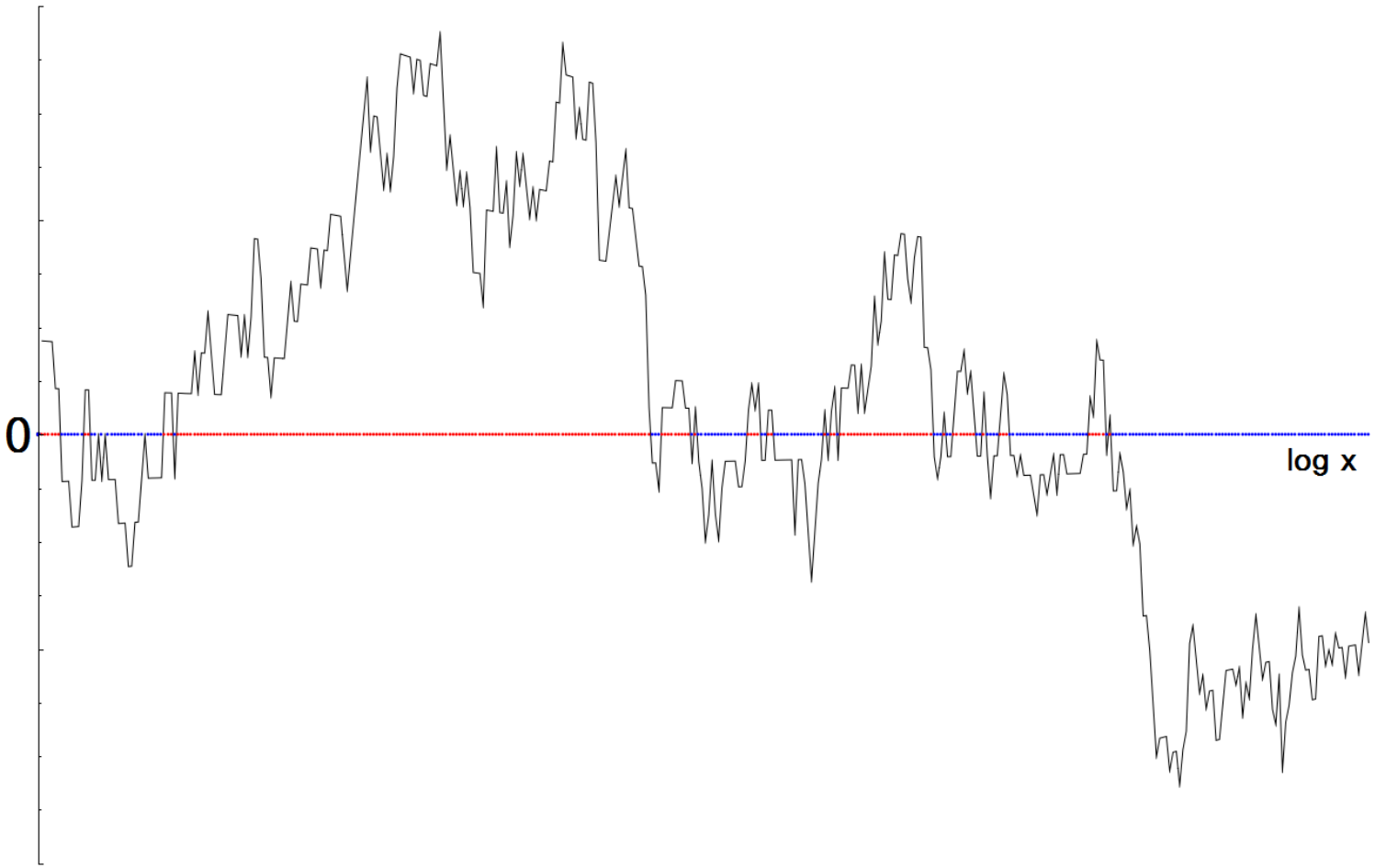
Quelques graphes



$\frac{\pi(x,53,3)-\pi(x,53,1)}{\sqrt{x}/\log x}$, $10^4 \leq x \leq 10^8$

Source : Daniel Fiorilli

Quelques graphes



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

Source : Daniel Fiorilli

Quelques autres courses

• Rubinstein et Sarnak montrent que la course « carrés vs non carrés mod q » est toujours biaisée en faveur des non carrés :

$$\delta\left(\{x \geq 2 \mid |\{p \leq x \mid p \neq \square \bmod q\}| > |\{p \leq x \mid p = \square \bmod q\}|\right) > \frac{1}{2}.$$

Quelques autres courses

• Rubinstein et Sarnak montrent que la course « carrés vs non carrés mod q » est toujours biaisée en faveur des non carrés :

$$\delta(\{x \geq 2 \mid |\{p \leq x \mid p \neq \square \bmod q\}| > |\{p \leq x \mid p = \square \bmod q\}|) > \frac{1}{2}.$$

• Ils considèrent également la « course dans le théorème des nombres premiers » et calculent que

$$\delta(\{x \geq 2 \mid \pi(x) > \mathrm{Li}(x)\}) \approx 0,00000026\ldots$$

Quelques autres courses

• Rubinstein et Sarnak montrent que la course « carrés vs non carrés mod q » est toujours biaisée en faveur des non carrés :

$$\delta(\{x \geq 2 \mid |\{p \leq x \mid p \neq \square \bmod q\}| > |\{p \leq x \mid p = \square \bmod q\}|) > \frac{1}{2}.$$

• Ils considèrent également la « course dans le théorème des nombres premiers » et calculent que

$$\delta(\{x \geq 2 \mid \pi(x) > \mathrm{Li}(x)\}) \approx 0,00000026\ldots$$

Le plus petit contre-exemple à $\mathrm{Li}(x) > \pi(x)$ est encore inconnu (nombre de Skewes). On sait qu'il est $\leq 7 \times 10^{370}$.

Quelques autres courses

• Généralisation des courses de nombres premiers en des « courses d'automorphismes de Frobenius » (Ng, 2000).

Quelques autres courses

• Généralisation des courses de nombres premiers en des « courses d'automorphismes de Frobenius » (Ng, 2000).

Soit L/K une extension galoisienne de corps de nombres. À chaque idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ non ramifié dans L (tous sauf un nombre fini), on peut associer une classe de conjugaison particulière $\sigma_{\mathfrak{p}}$ de $\mathrm{Gal}(L/K)$ appelée automorphisme de Frobenius ou symbole d'Artin de $\mathfrak{p}$.

Quelques autres courses

• Généralisation des courses de nombres premiers en des « courses d'automorphismes de Frobenius » (Ng, 2000).

Soit L/K une extension galoisienne de corps de nombres. À chaque idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ non ramifié dans L (tous sauf un nombre fini), on peut associer une classe de conjugaison particulière $\sigma_{\mathfrak{p}}$ de $\mathrm{Gal}(L/K)$ appelée automorphisme de Frobenius ou symbole d'Artin de $\mathfrak{p}$.

On peut alors faire la course

$$\frac{\pi(x, C_1, L/K)}{|C_1|} \; vs \; \frac{\pi(x, C_2, L/K)}{|C_2|}.$$

Quelques autres courses

On obtient des résultats similaires, mais un phénomène nouveau de biais apparaît : l'existence d'un zéro en $\frac{1}{2}$ pour une fonction L d'Artin peut influencer le biais.

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) En jouant avec des groupes de Galois ayant des représentations linéaires particulières ($\mathfrak{S}_n$, $\mathbf{PSL}_2(\mathbb{F}_p)$, $\mathbb{H}_8$), obtenir des biais extrêmes ou très modérés dans des familles d'extensions de corps de nombres.

Pour conclure : quelques pistes

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

ii) En jouant avec des groupes de Galois ayant des représentations linéaires particulières ($\mathfrak{S}_n$, $\mathbf{PSL}_2(\mathbb{F}_p)$, $\mathbb{H}_8$), obtenir des biais extrêmes ou très modérés dans des familles d'extensions de corps de nombres.

iii) Étudier des situations explicites où un zéro en $\frac{1}{2}$ existe (Artin root number $W = -1$).

Merci de votre attention !