Autour du théorème des nombres premiers

Alexandre Bailleul

Séminaire des doctorants - Université de Bordeaux

5 octobre 2018

Sommaire

Introduction

Les nombres premiers :

i) Sujet très ancien (Antiquité)...

Introduction

Les nombres premiers :

i) Sujet très ancien (Antiquité)... mais toujours très actuel !

Introduction

Les nombres premiers :

i) Sujet très ancien (Antiquité)... mais toujours très actuel !

ii) De grands noms de mathématiciens associés à leur étude...

Introduction

Les nombres premiers :

i) Sujet très ancien (Antiquité)... mais toujours très actuel !
ii) De grands noms de mathématiciens associés à leur étude... et d'autres moins connus.

Introduction

Les nombres premiers :

i) Sujet très ancien (Antiquité)... mais toujours très actuel !

ii) De grands noms de mathématiciens associés à leur étude... et d'autres moins connus.

iii) Des résultats jolis et simples à concevoir...

Introduction

Les nombres premiers :

i) Sujet très ancien (Antiquité)... mais toujours très actuel !
ii) De grands noms de mathématiciens associés à leur étude... et d'autres moins connus.
iii) Des résultats jolis et simples à concevoir... mais très difficiles à démontrer !

Introduction

Les nombres premiers :

i) Sujet très ancien (Antiquité)... mais toujours très actuel !
ii) De grands noms de mathématiciens associés à leur étude... et d'autres moins connus.
iii) Des résultats jolis et simples à concevoir... mais très difficiles à démontrer !

Un sujet d'étude parfait !

Introduction

Fil rouge :

Le Théorème des Nombres Premiers

Introduction

Fil rouge :

Le Théorème des Nombres Premiers (ou TNP)

Introduction

Fil rouge :

Le Théorème des Nombres Premiers (ou TNP)

et quelques questions proches.

Plan

Les débuts : Euclide et Eratosthène

Dans le livre VII des *Éléments* d'**Euclide**(≈ -325 - ≈ -270) on trouve :
« Tout nombre non premier est mesuré par un nombre premier. »

Les débuts : Euclide et Eratosthène

Dans le livre VII des *Éléments* d'**Euclide**(≈ -325 - ≈ -270) on trouve :
« Tout nombre non premier est mesuré par un nombre premier. »

Théorème (fondamental de l'arithmétique).

Tout nombre entier $n \geq 1$ s'écrit de manière unique (à l'ordre des facteurs près) sous la forme

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r},$$

où les p_i sont premiers.

Euclide et Eratosthène

Dans le livre IX des *Éléments*, on trouve :
« Les nombres premiers sont plus nombreux que n'importe quelle multitude de nombres premiers proposée. »

Euclide et Eratosthène

Dans le livre IX des *Éléments*, on trouve :
« Les nombres premiers sont plus nombreux que n'importe quelle multitude de nombres premiers proposée. »

Instant notation : dans toute la suite, p désignera un nombre premier.

Euclide et Eratosthène

Dans le livre IX des *Éléments*, on trouve :
« Les nombres premiers sont plus nombreux que n'importe quelle multitude de nombres premiers proposée. »

Instant notation : dans toute la suite, p désignera un nombre premier.

Définition.

Pour $x \geq 2$, on note

$$\pi(x) = |\{p \leq x\}| .$$

Euclide et Eratosthène

Dans le livre IX des *Éléments*, on trouve :
« Les nombres premiers sont plus nombreux que n'importe quelle multitude de nombres premiers proposée. »

Instant notation : dans toute la suite, p désignera un nombre premier.

Définition.

Pour $x \geq 2$, on note

$$\pi(x) = |\{p \leq x\}|.$$

Théorème (d'Euclide).

On a

$$\pi(x) \underset{x \to +\infty}{\longrightarrow} +\infty.$$

Euclide et Eratosthène

Problème 1 : à quelle vitesse ?

Euclide et Eratosthène

Problème 1 : à quelle vitesse ?

Démonstration d'Euclide. Si $p_1, \ldots, p_n$ sont les n premiers nombres premiers, les facteurs premiers de

$$N = p_1 \ldots p_n + 1$$

ne sont pas des p_i. □

Euclide et Eratosthène

Problème 1 : à quelle vitesse ?

Démonstration d'Euclide. Si $p_1, \ldots, p_n$ sont les n premiers nombres premiers, les facteurs premiers de

$$N = p_1 \ldots p_n + 1$$

ne sont pas des p_i. $\square$

En particulier

$$p_{n+1} \leq p_1 \ldots p_n + 1,$$

Euclide et Eratosthène

Problème 1 : à quelle vitesse ?

Démonstration d'Euclide. Si $p_1, \ldots, p_n$ sont les n premiers nombres premiers, les facteurs premiers de

$$N = p_1 \ldots p_n + 1$$

ne sont pas des p_i. $\square$

En particulier

$$p_{n+1} \leq p_1 \ldots p_n + 1,$$

et par récurrence

$$p_n \leq 2^{2^{n-1}}$$

Euclide et Eratosthène

Problème 1 : à quelle vitesse ?

Démonstration d'Euclide. Si $p_1, \dots, p_n$ sont les n premiers nombres premiers, les facteurs premiers de

$$N = p_1 \dots p_n + 1$$

ne sont pas des p_i. □

En particulier

$$p_{n+1} \leq p_1 \dots p_n + 1,$$

et par récurrence

$$p_n \leq 2^{2^{n-1}}$$

d'où l'on tire

$$\pi(x) \gg \log\log x \qquad (i.e.\ \pi(x) \geq C \log\log x).$$

Euclide et Eratosthène

Problème 2 : comment trouver tous les nombres premiers ?

Euclide et Eratosthène

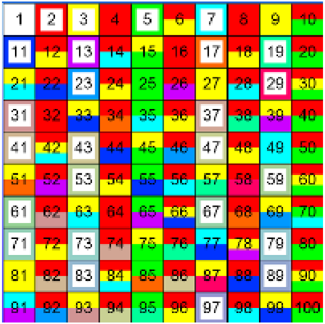
Problème 2 : comment trouver tous les nombres premiers ?

À la main, la méthode la plus naturelle est **le crible d'Ératosthène** (≈ -276 - ≈ -194).

Euclide et Eratosthène

Problème 2 : comment trouver tous les nombres premiers ?

À la main, la méthode la plus naturelle est **le crible d'Ératosthène** (≈ -276 - ≈ -194).



Euclide et Eratosthène

Trois grandes questions :

i) Peut-on donner une formule donnant le n-ième nombre premier ?

Euclide et Eratosthène

Trois grandes questions :

i) Peut-on donner une formule donnant le n-ième nombre premier ?
ii) Y a-t-il une manière efficace de trouver les nombres premiers ?

Euclide et Eratosthène

Trois grandes questions :

i) Peut-on donner une formule donnant le n-ième nombre premier ?
ii) Y a-t-il une manière efficace de trouver les nombres premiers ?
iii) Comment les nombres premiers se répartissent parmi les nombres entiers ?

Euclide et Eratosthène

Trois grandes questions :

i) Peut-on donner une formule donnant le n-ième nombre premier ?

ii) Y a-t-il une manière efficace de trouver les nombres premiers ?

iii) Comment les nombres premiers se répartissent parmi les nombres entiers ?

Pendant des siècles, aucune avancée sur le problème. (Wilson, Fermat, etc.)

Euclide et Eratosthène

Trois grandes questions :

i) Peut-on donner une formule donnant le n-ième nombre premier ?

ii) Y a-t-il une manière efficace de trouver les nombres premiers ?

iii) Comment les nombres premiers se répartissent parmi les nombres entiers ?

Pendant des siècles, aucune avancée sur le problème. (Wilson, Fermat, etc.)

$$\emptyset$$

Produits infinis et divergence : Euler

En 1735, **Euler** (1707-1783) résout le problème de Bâle :

Produits infinis et divergence : Euler

En 1735, **Euler** (1707-1783) résout le problème de Bâle :

$$\text{« Déterminer la valeur de } \sum_{n=1}^{+\infty} \frac{1}{n^2}. \text{ ».}$$

Produits infinis et divergence : Euler

En 1735, **Euler** (1707-1783) résout le problème de Bâle :

$$\text{« Déterminer la valeur de } \sum_{n=1}^{+\infty} \frac{1}{n^2}. \text{ ».}$$

Chemin faisant, il détermine les valeurs des sommes de la forme

$$\sum_{n=1}^{+\infty} \frac{1}{n^{2k}}, k \geq 1 \text{ entier.}$$

Euler

Euler est donc amené, sans penser aux nombres premiers, à étudier la fonction suivante :

Euler

Euler est donc amené, sans penser aux nombres premiers, à étudier la fonction suivante :

Définition.

La fonction ζ d'Euler est la fonction définie sur $]1, +\infty[$ par

$$x \mapsto \zeta(x) := \sum_{n=1}^{+\infty} \frac{1}{n^x}.$$

Euler

Euler est donc amené, sans penser aux nombres premiers, à étudier la fonction suivante :

Définition.

La fonction ζ d'Euler est la fonction définie sur $]1,+\infty[$ par

$$x \mapsto \zeta(x) := \sum_{n=1}^{+\infty} \frac{1}{n^x}.$$

Il obtient le résultat **fondamental** suivant :

Théorème (produit eulérien).

Pour tout $x > 1$, on a

$$\zeta(x) = \prod_p \left(1 - \frac{1}{p^x}\right)^{-1}.$$

Euler

Theorema 8.

Si ex ſerie numerorum primorum ſequens formetur expreſſio

$$\frac{2^n \cdot 3^n \cdot 5^n \cdot 7^n \cdot 11^n \cdot \text{ etc.}}{(2^n-1)(3^n-1)(5^n-1)(7^n-1)(11^n-1) \text{ etc.}}$$

erit

CIRCA SERIES INFINITAS. 175

erit eius valor aequalis ſummae huius ſeriei

$$1+\frac{1}{2^n}+\frac{1}{3^n}+\frac{1}{4^n}+\frac{1}{5^n}+\frac{1}{6^n}+\frac{1}{7^n}+ \text{etc.}$$

Euler

Démonstration. Le premier terme du produit est

$$\frac{1}{1-\frac{1}{2^x}} = \sum_{k=0}^{+\infty} \frac{1}{2^{kx}}.$$

Euler

Démonstration. Le premier terme du produit est

$$\frac{1}{1-\frac{1}{2^x}} = \sum_{k=0}^{+\infty} \frac{1}{2^{kx}}.$$

Le second est

$$\frac{1}{1-\frac{1}{3^x}} = \sum_{k=0}^{+\infty} \frac{1}{3^{kx}}$$

et leur produit vaut donc

$$\sum_{k_1,k_2\geq 0} \frac{1}{2^{k_1x}3^{k_2x}}.$$

Euler

Démonstration. Le premier terme du produit est

$$\frac{1}{1-\frac{1}{2^x}} = \sum_{k=0}^{+\infty} \frac{1}{2^{kx}}.$$

Le second est

$$\frac{1}{1-\frac{1}{3^x}} = \sum_{k=0}^{+\infty} \frac{1}{3^{kx}}$$

et leur produit vaut donc

$$\sum_{k_1,k_2\geq 0} \frac{1}{2^{k_1 x} 3^{k_2 x}}.$$

Avec le produit portant sur tous les nombres premiers, on obtient une et une seule fois chaque $\frac{1}{n^x}$ pour $n \geq 1$ entier. □

Euler

La relation

$$\zeta(x) = \prod_p \left(1 - \frac{1}{p^x}\right)^{-1}$$

est la **version analytique du théorème fondamental de l'arithmétique** !

Euler

La relation

$$\zeta(x) = \prod_p \left(1 - \frac{1}{p^x}\right)^{-1}$$

est la **version analytique du théorème fondamental de l'arithmétique** !

La fonction ζ doit donc certainement contenir de l'information à propos des nombres premiers.

Euler

Théorème (« Euler »).

Pour $x \geq 2$, on a
$$\sum_{p \leq x} \frac{1}{p} \geq \log \log x + C.$$

Euler

Théorème (« Euler »).

Pour $x \geq 2$, on a
$$\sum_{p \leq x} \frac{1}{p} \geq \log\log x + C.$$

Démonstration. On développe
$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} \approx \text{"}\zeta(1)\text{"} = +\infty.$$

Euler

Théorème (« Euler »).

Pour $x \geq 2$, on a
$$\sum_{p \leq x} \frac{1}{p} \geq \log\log x + C.$$

Démonstration. On développe
$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} \approx \text{"}\zeta(1)\text{"} = +\infty.$$

On a
$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} = \sum_{n \geq 1, P^+(n) \leq x} \frac{1}{n} \geq \sum_{n \leq x} \frac{1}{n} \geq \log x.$$

Euler

Théorème (« Euler »).

Pour $x \geq 2$, on a

$$\sum_{p \leq x} \frac{1}{p} \geq \log\log x + C.$$

Démonstration. On développe

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} \approx \text{"}\zeta(1)\text{"} = +\infty.$$

On a

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} = \sum_{n \geq 1, P^+(n) \leq x} \frac{1}{n} \geq \sum_{n \leq x} \frac{1}{n} \geq \log x.$$

Puis on utilise

$$-\log\left(1 - \frac{1}{p}\right) = \frac{1}{p} + O\left(\frac{1}{p^2}\right).$$

Euler

$A \quad \frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+$ etc.

$e \;= e \qquad\qquad = 1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+$ etc.

Atque conſequenter erit

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+ \text{etc.}$$

$$= l\left(1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{7}+ \text{etc.}\right)$$

illius ergo feriei ſumma erit infinities minor quam huius, atque cum huius ſumma ſit $= l\infty$ erit

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+ \text{etc.} = l.\, l\infty.$$

Q. E. D.

Euler

Moralité :

$\zeta(1) = +\infty \longleftrightarrow$ il existe une infinité de nombres premiers.

Euler

Moralité :

$$\zeta(1) = +\infty \longleftrightarrow \text{ il existe une infinité de nombres premiers.}$$

Euler (1747) : « On n'a qu'à jeter les yeux sur les tables des nombres premiers, que quelques personnes se sont donné la peine de continuer au-delà de cent mille : et on s'apercevra d'abord qu'il n'y règne aucun ordre ni règle. »

Conjectures : Legendre et Gauss

En 1797-1798, **Legendre** (1752-1833) observe que

$$\pi(x) \approx \frac{x}{\log x - 1.08366},$$

et conjecture qu'il s'agit du bon ordre de grandeur.

Legendre et Gauss

Gauss (1777-1855) aurait conjecturé à l'âge de 15 ans (!) que la densité des nombres premiers inférieurs à x serait d'environ $\frac{1}{\log x}$, autrement dit que

$$\pi(x) \approx \int_2^x \frac{dt}{\log t}.$$

Legendre et Gauss

Conjecture (Legendre, Gauss).

On a

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

Legendre et Gauss

Conjecture (Legendre, Gauss).

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

Cela suggère que la probabilité qu'un entier $n \in [1, N]$ soit premier vaut environ
$$\frac{1}{\log N}$$

Legendre et Gauss

Conjecture (Legendre, Gauss).

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

Cela suggère que la probabilité qu'un entier $n \in [1, N]$ soit premier vaut environ
$$\frac{1}{\log N} \underset{N\to+\infty}{\longrightarrow} 0.$$

La "probabilité" d'être premier est nulle !*

Legendre et Gauss

En utilisant le crible d'Eratosthène, Legendre montre la

Proposition (Formule du crible de Legendre, 1808).

Pour $x \geq 2$, on a

$$\pi(x) - \pi(\sqrt{x}) + 1 = \sum_{d \leq x, P^+(d) \leq \sqrt{x}} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor .$$

Legendre et Gauss

En utilisant le crible d'Eratosthène, Legendre montre la

Proposition (Formule du crible de Legendre, 1808).

Pour $x \geq 2$, on a

$$\pi(x) - \pi(\sqrt{x}) + 1 = \sum_{d \leq x, P^+(d) \leq \sqrt{x}} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor.$$

On part des entiers $\leq x$, on enlève les multiples $\leq x$ de 2, de 3, de 5, on ajoute ceux de 6 (rayés deux fois), etc.

Legendre et Gauss

Théorème (de la raréfaction des nombres premiers).

On a

$$\pi(x) = o(x)$$

quand $x \to +\infty$.

Legendre et Gauss

Théorème (de la raréfaction des nombres premiers).

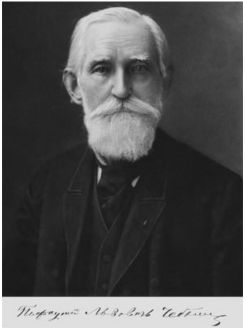
On a

$$\pi(x) = o(x)$$

quand $x \to +\infty$.

Les nombres premiers se font de plus en plus rare dans la liste ordonnée des entiers.

Premiers résultats : Chebychev



Dans les années 1840-50, **Chebychev** (1821-1894) s'attaque au problème.

Chebychev

Son apport est de réaliser que

$$\textbf{estimer } \pi(x) \longleftrightarrow \textbf{ estimer } \psi(x),$$

où

$$\psi(x) = \sum_{p^m \leq x} \log p.$$

Chebychev

Son apport est de réaliser que

$$\textbf{estimer } \pi(x) \longleftrightarrow \textbf{ estimer } \psi(x),$$

où

$$\psi(x) = \sum_{p^m \leq x} \log p.$$

En particulier

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

Chebychev

Théorème (Chebychev, 1848).

On a

$$\liminf_{x\to+\infty} \frac{\pi(x)\log x}{x} \leq 1 \leq \limsup_{x\to+\infty} \frac{\pi(x)\log x}{x}.$$

Chebychev

Théorème (Chebychev, 1848).

On a

$$\liminf_{x\to+\infty} \frac{\pi(x)\log x}{x} \leq 1 \leq \limsup_{x\to+\infty} \frac{\pi(x)\log x}{x}.$$

En particulier si $\frac{\pi(x)}{x/\log x}$ admet une limite quand $x \to +\infty$, elle ne peut valoir que 1.

Chebychev

Théorème (Chebychev, 1850).

Pour tout $x \geq 2$,

$$0.92 \frac{x}{\log x} \leq \pi(x) \leq 1.11 \frac{x}{\log x}.$$

Chebychev

Théorème (Chebychev, 1850).

Pour tout $x \geq 2$,

$$0.92 \frac{x}{\log x} \leq \pi(x) \leq 1.11 \frac{x}{\log x}.$$

Corollaire (Postulat de Bertrand, 1845).

Pour tout $x \geq 2$, il y a un nombre premier p tel que

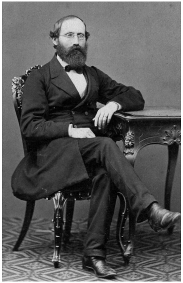
$$x < p < 2x.$$

Démonstration. Pour $x \geq 30$ on a

$$\pi(2x) \geq 0.92 \frac{2x}{\log(2x)} > 1.11 \frac{x}{\log x} \geq \pi(x),$$

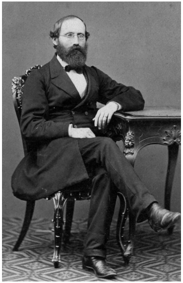
et on vérifie à la main que c'est vrai pour $x < 30$. □

Le mémoire qui changea tout : Riemann



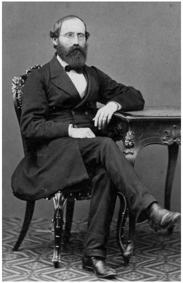
En 1859, **Riemann** (1826-1866) publie *Über die Anzahl der Primzahlen unter einer gegebenen Grösse* (Sur le nombre de nombres premiers inférieurs à une taille donnée)

Le mémoire qui changea tout : Riemann



En 1859, **Riemann** (1826-1866) publie *Über die Anzahl der Primzahlen unter einer gegebenen Grösse* (Sur le nombre de nombres premiers inférieurs à une taille donnée) « sur $\pi(x)$ » quoi...

Le mémoire qui changea tout : Riemann



En 1859, **Riemann** (1826-1866) publie *Über die Anzahl der Primzahlen unter einer gegebenen Grösse* (Sur le nombre de nombres premiers inférieurs à une taille donnée) « sur $\pi(x)$ » quoi...

Riemann ressort du placard la fonction ζ d'Euler, et l'étudie de manière poussée comme **fonction de la variable complexe** s.

Riemann

Bei dieser Untersuchung diente mir als Ausgangspunkt die von Euler gemachte Bemerkung, dass das Product

$$\prod \frac{1}{1-\frac{1}{p^s}} = \Sigma \frac{1}{n^s},$$

wenn für p alle Primzahlen, für n alle ganzen Zahlen gesetzt werden. Die Function der complexen Veränderlichen s, welche durch diese beiden Ausdrücke, so lange sie convergiren, dargestellt wird, bezeichne ich durch $\zeta(s)$. Beide convergiren nur, so lange der reelle Theil von s grösser als 1 ist; es lässt sich indess leicht ein immer gültig blei-

Riemann

Théorème (Riemann, 1859).

i) La fonction

$$\zeta : s \mapsto \sum_{n=1}^{+\infty} \frac{1}{n^s}$$

est holomorphe sur $\Omega_1 := \{s \in \mathbb{C} \mid \mathfrak{Re}(s) > 1\}$.

Riemann

Théorème (Riemann, 1859).

i) La fonction
$$\zeta : s \mapsto \sum_{n=1}^{+\infty} \frac{1}{n^s}$$
est holomorphe sur $\Omega_1 := \{s \in \mathbb{C} \mid \mathfrak{Re}(s) > 1\}$.

ii) Cette fonction admet un prolongement méromorphe à $\mathbb{C}$ tout entier, avec un unique pôle, simple, en 1, de résidu 1.

Riemann

Théorème (Riemann, 1859).

i) La fonction
$$\zeta : s \mapsto \sum_{n=1}^{+\infty} \frac{1}{n^s}$$
est holomorphe sur $\Omega_1 := \{s \in \mathbb{C} \mid \mathfrak{Re}(s) > 1\}$.

ii) Cette fonction admet un prolongement méromorphe à $\mathbb{C}$ tout entier, avec un unique pôle, simple, en 1, de résidu 1.

iii) Elle satisfait l'équation fonctionnelle
$$\xi(s) = \xi(1-s)$$
où
$$\xi(s) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s).$$

Riemann

Riemann continue sur sa lancée, et obtient une formule **exacte** pour $\pi(x)$, faisant apparaître des harmoniques de cette fonction, dépendant des zéros de la fonction ζ.

Riemann

Riemann continue sur sa lancée, et obtient une formule **exacte** pour $\pi(x)$, faisant apparaître des harmoniques de cette fonction, dépendant des zéros de la fonction ζ.

Cependant :

i) Le style est expéditif (8 pages !), difficile à lire.

Riemann

Riemann continue sur sa lancée, et obtient une formule **exacte** pour $\pi(x)$, faisant apparaître des harmoniques de cette fonction, dépendant des zéros de la fonction ζ.

Cependant :

i) Le style est expéditif (8 pages !), difficile à lire.

ii) Tout n'est pas démontré (notamment une certaine hypothèse* ...) et certains passages contiennent des erreurs.

Riemann

Riemann continue sur sa lancée, et obtient une formule **exacte** pour $\pi(x)$, faisant apparaître des harmoniques de cette fonction, dépendant des zéros de la fonction ζ.

Cependant :

i) Le style est expéditif (8 pages !), difficile à lire.

ii) Tout n'est pas démontré (notamment une certaine hypothèse* ...) et certains passages contiennent des erreurs.

iii) Riemann ne parvient pas, malgré sa formule exacte, à obtenir le TNP.

Riemann

Riemann continue sur sa lancée, et obtient une formule **exacte** pour $\pi(x)$, faisant apparaître des harmoniques de cette fonction, dépendant des zéros de la fonction ζ.

Cependant :

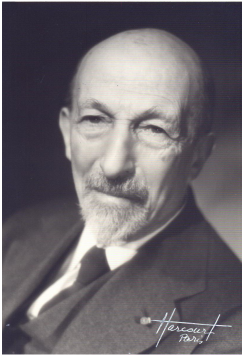
i) Le style est expéditif (8 pages !), difficile à lire.

ii) Tout n'est pas démontré (notamment une certaine hypothèse* ...) et certains passages contiennent des erreurs.

iii) Riemann ne parvient pas, malgré sa formule exacte, à obtenir le TNP.

* « [...] il est très probable que toutes les racines sont réelles. Il serait à désirer, sans doute, que l'on eût une démonstration rigoureuse de cette proposition ; néanmoins j'ai laissé cette recherche de côté pour le moment après quelques rapides essais infructueux, car elle paraît superflue pour le but immédiat de mon étude. »

La démonstration : Hadamard et de la Vallée-Poussin



Hadamard
(1865-1963)

de la Vallée-Poussin
(1866-1962)

Hadamard et de la Vallée-Poussin

Théorème (Hadamard, de la Vallée-Poussin, 1896).

Pour $t \in \mathbb{R}^*$ on a

$$\zeta(1 + it) \neq 0.$$

Hadamard et de la Vallée-Poussin

Théorème (Hadamard, de la Vallée-Poussin, 1896).

Pour $t \in \mathbb{R}^*$ on a
$$\zeta(1+it) \neq 0.$$

Corollaire (Théorème des nombres premiers, 1896).

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

Plan

La formule exacte de Riemann

Théorème (Riemann, 1859).

Pour $x \geq 2$, on a

$$f(x) = \mathrm{li}(x) - \sum_{\rho} \mathrm{li}(x^{\rho}) + \int_{x}^{+\infty} \frac{1}{u^2 - 1} \frac{du}{u \log u} - \log 2,$$

où la somme porte sur tous les zéros de ζ, où

$$\mathrm{li}(x) = \int_{0}^{x} \frac{dt}{\log t},$$

et où

$$f(x) = \sum_{n=1}^{+\infty} \frac{\pi(x^{1/n})}{n}.$$

Où sont mes zéros ?

i) On a $\zeta(s) \neq 0$ pour $\mathfrak{Re}(s) > 1$ (produit eulérien).

Où sont mes zéros ?

i) On a $\zeta(s) \neq 0$ pour $\mathfrak{Re}(s) > 1$ (produit eulérien).

ii) À l'aide de

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

tous les $-2n$ avec $n \in \mathbb{N}$ sont des zéros simples de ζ (zéros triviaux).

Où sont mes zéros ?

i) On a $\zeta(s) \neq 0$ pour $\mathfrak{Re}(s) > 1$ (produit eulérien).

ii) À l'aide de

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

tous les $-2n$ avec $n \in \mathbb{N}$ sont des zéros simples de ζ (zéros triviaux).

iii) Les autres zéros vérifient $0 \leq \mathfrak{Re}(s) \leq 1$ (zéros non triviaux).

iv) Si ρ est un zéro non trivial, alors $\overline{\rho}, 1-\rho$ et $1-\overline{\rho}$ aussi.

Où sont mes zéros ?

i) On a $\zeta(s) \neq 0$ pour $\mathfrak{Re}(s) > 1$ (produit eulérien).

ii) À l'aide de

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

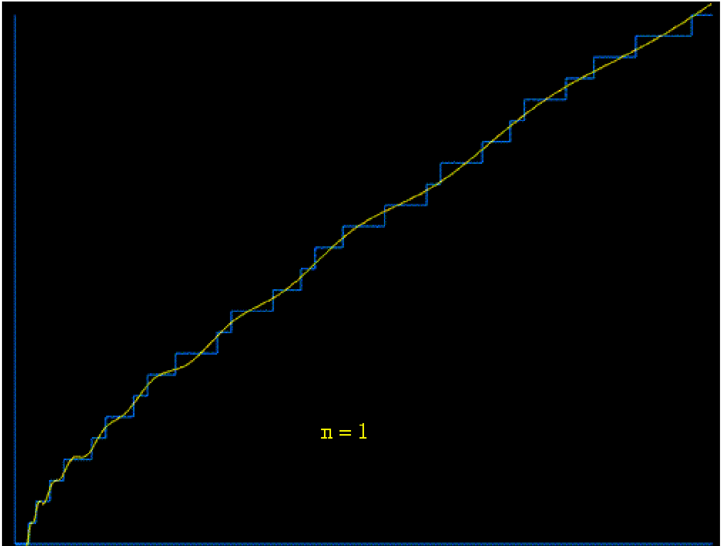
tous les $-2n$ avec $n \in \mathbb{N}$ sont des zéros simples de ζ (zéros triviaux).

iii) Les autres zéros vérifient $0 \leq \mathfrak{Re}(s) \leq 1$ (zéros non triviaux).

iv) Si ρ est un zéro non trivial, alors $\overline{\rho}, 1-\rho$ et $1-\overline{\rho}$ aussi.

Riemann avait calculé les quelques premiers zéros :
$\frac{1}{2} + i14,03\ldots$, $\frac{1}{2} + i21,02\ldots$ et $\frac{1}{2} + i25,01\ldots$

La mélodie des nombres premiers...



Pour y voir plus clair

Pour $x \geq 2$, on a

$$\psi_0(x) = \frac{1}{2i\pi} \int_{2-i\infty}^{2+i\infty} -\frac{\zeta'(s)}{\zeta(s)} \frac{x^s}{s} \, ds.$$

Pour y voir plus clair

Pour $x \geq 2$, on a

$$\psi_0(x) = \frac{1}{2i\pi} \int_{2-i\infty}^{2+i\infty} -\frac{\zeta'(s)}{\zeta(s)} \frac{x^s}{s} \, ds.$$

Par la magie des intégrales curvilignes et le théorème des résidus ($\frac{\zeta'}{\zeta}$ a des pôles en chaque zéro et pôle de ζ), on obtient

$$\psi_0(x) = x - \sum_{\rho \text{ non trivial}} \frac{x^\rho}{\rho} - \log(2\pi) - \frac{1}{2} \log\left(1 - \frac{1}{x^2}\right) \text{ (Von Mangoldt, 1895).}$$

Pour y voir plus clair

Pour $x \geq 2$, on a

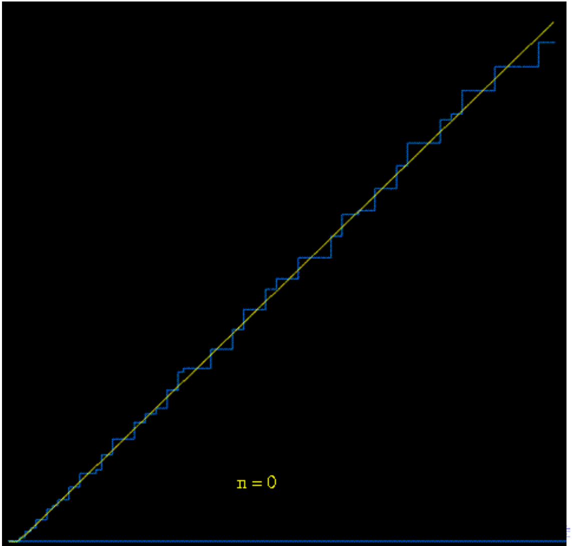
$$\psi_0(x) = \frac{1}{2i\pi} \int_{2-i\infty}^{2+i\infty} -\frac{\zeta'(s)}{\zeta(s)} \frac{x^s}{s} \, ds.$$

Par la magie des intégrales curvilignes et le théorème des résidus ($\frac{\zeta'}{\zeta}$ a des pôles en chaque zéro et pôle de ζ), on obtient

$$\psi_0(x) = x - \sum_{\rho \text{ non trivial}} \frac{x^\rho}{\rho} - \log(2\pi) - \frac{1}{2}\log\left(1 - \frac{1}{x^2}\right) \text{ (Von Mangoldt, 1895).}$$

Comme $|x^\rho| = x^{\mathfrak{Re}(\rho)}$, **les parties réelles des zéros non triviaux régissent l'amplitude des harmoniques de la fonction ψ_0 !**

Mélodie : le retour



Régions sans zéros

Notons $\sigma = \Re\mathfrak{e}(s)$ et $t = \Im\mathfrak{m}(s)$.

i) Hadamard, de la Vallée-Poussin (1896) : $\zeta(s) \neq 0$ pour $\sigma = 1$ et $t \neq 0$

Régions sans zéros

Notons $\sigma = \mathfrak{Re}(s)$ et $t = \mathfrak{Im}(s)$.

i) Hadamard, de la Vallée-Poussin (1896) : $\zeta(s) \neq 0$ pour $\sigma = 1$ et $t \neq 0$

$$\Rightarrow \pi(x) \underset{x\to+\infty}{\sim} \mathrm{li}(x).$$

Régions sans zéros

Notons $\sigma = \mathfrak{Re}(s)$ et $t = \mathfrak{Im}(s)$.

i) Hadamard, de la Vallée-Poussin (1896) : $\zeta(s) \neq 0$ pour $\sigma = 1$ et $t \neq 0$

$$\Rightarrow \pi(x) \underset{x\to+\infty}{\sim} \mathrm{li}(x).$$

ii) de la Vallée-Poussin (1899) : $\zeta(s) \neq 0$ pour $\sigma \geq 1 - \frac{c}{\log(|t|+2)}$

Régions sans zéros

Notons $\sigma = \mathfrak{Re}(s)$ et $t = \mathfrak{Im}(s)$.

i) Hadamard, de la Vallée-Poussin (1896) : $\zeta(s) \neq 0$ pour $\sigma = 1$ et $t \neq 0$

$$\Rightarrow \pi(x) \underset{x \to +\infty}{\sim} \operatorname{li}(x).$$

ii) de la Vallée-Poussin (1899) : $\zeta(s) \neq 0$ pour $\sigma \geq 1 - \frac{c}{\log(|t|+2)}$

$$\Rightarrow \pi(x) = \operatorname{li}(x) + O(x \exp(-c\sqrt{\log x})).$$

Régions sans zéros

Notons $\sigma = \mathfrak{Re}(s)$ et $t = \mathfrak{Im}(s)$.

i) Hadamard, de la Vallée-Poussin (1896) : $\zeta(s) \neq 0$ pour $\sigma = 1$ et $t \neq 0$

$$\Rightarrow \pi(x) \underset{x \to +\infty}{\sim} \mathrm{li}(x).$$

ii) de la Vallée-Poussin (1899) : $\zeta(s) \neq 0$ pour $\sigma \geq 1 - \frac{c}{\log(|t|+2)}$

$$\Rightarrow \pi(x) = \mathrm{li}(x) + O(x \exp(-c\sqrt{\log x})).$$

iii) Korobov, Vinogradov (1958) : $\zeta(s) \neq 0$ pour $\sigma \geq 1 - \frac{c}{(\log(|t|+2))^{2/3}(\log\log(|t|+2))^{1/3}}$

Régions sans zéros

Notons $\sigma = \mathfrak{Re}(s)$ et $t = \mathfrak{Im}(s)$.

i) Hadamard, de la Vallée-Poussin (1896) : $\zeta(s) \neq 0$ pour $\sigma = 1$ et $t \neq 0$

$$\Rightarrow \pi(x) \underset{x\to+\infty}{\sim} \mathrm{li}(x).$$

ii) de la Vallée-Poussin (1899) : $\zeta(s) \neq 0$ pour $\sigma \geq 1 - \frac{c}{\log(|t|+2)}$

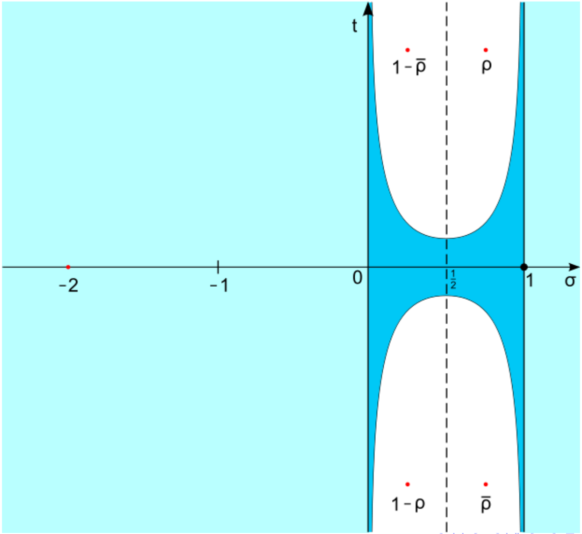
$$\Rightarrow \pi(x) = \mathrm{li}(x) + O(x\exp(-c\sqrt{\log x})).$$

iii) Korobov, Vinogradov (1958) : $\zeta(s) \neq 0$ pour $\sigma \geq 1 - \frac{c}{(\log(|t|+2))^{2/3}(\log\log(|t|+2))^{1/3}}$

$$\Rightarrow \pi(x) = \mathrm{li}(x) + O\left(x\exp\left(-c\frac{(\log x)^{3/5}}{(\log\log x)^{1/5}}\right)\right).$$

iv) On ne connaît aucune région sans zéro de la forme $\sigma \geq 1 - \delta$ avec $\delta > 0$.

Régions sans zéros



L'hypothèse de Riemann

À cause de la symétrie par rapport à la droite critique ($\zeta(\rho) = 0 \Leftrightarrow \zeta(1-\rho) = 0$ pour ρ dans la bande critique), le mieux que l'on puisse espérer est que les amplitudes des "harmoniques" soient $x^{1/2}$.

L'hypothèse de Riemann

À cause de la symétrie par rapport à la droite critique ($\zeta(\rho) = 0 \Leftrightarrow \zeta(1-\rho) = 0$ pour ρ dans la bande critique), le mieux que l'on puisse espérer est que les amplitudes des "harmoniques" soient $x^{1/2}$.

Hypothèse de Riemann

Pour tout zéro non trivial ρ de ζ, on a

$$\mathfrak{Re}(\rho) = \frac{1}{2}.$$

L'hypothèse de Riemann

Théorème (Schoenflies, 1976).

L'hypothèse de Riemann est équivalente à l'estimation

$$|\pi(x) - \mathrm{li}(x)| < \frac{1}{8\sqrt{\pi}} x^{1/2} \log(x).$$

L'hypothèse de Riemann

Théorème (Schoenflies, 1976).

L'hypothèse de Riemann est équivalente à l'estimation

$$|\pi(x) - \mathrm{li}(x)| < \frac{1}{8\sqrt{\pi}} x^{1/2} \log(x).$$

On sait que $\pi(x) - \mathrm{li}(x)$ n'est pas $O(x^{1/2} \log\log\log x)$ (Littlewood, 1914) donc on ne peut guère espérer mieux.

Ce que l'on sait

i) Riemann (1859) : Les 3 premiers zéros de ζ ont pour partie réelle $\frac{1}{2}$.

Ce que l'on sait

i) Riemann (1859) : Les 3 premiers zéros de ζ ont pour partie réelle $\frac{1}{2}$.

ii) Hardy (1912) : ζ admet une infinité de zéros de partie réelle $\frac{1}{2}$.

Ce que l'on sait

i) Riemann (1859) : Les 3 premiers zéros de ζ ont pour partie réelle $\frac{1}{2}$.

ii) Hardy (1912) : ζ admet une infinité de zéros de partie réelle $\frac{1}{2}$.

iii) Conrey (1989) : Au moins 40% des zéros de ζ ont pour partie réelle $\frac{1}{2}$.

Ce que l'on sait

i) Riemann (1859) : Les 3 premiers zéros de ζ ont pour partie réelle $\frac{1}{2}$.

ii) Hardy (1912) : ζ admet une infinité de zéros de partie réelle $\frac{1}{2}$.

iii) Conrey (1989) : Au moins 40% des zéros de ζ ont pour partie réelle $\frac{1}{2}$.

iv) Gourdon, Demichel (2004) : Les 10^{13} premiers zéros de ζ ont pour partie réelle $\frac{1}{2}$.

Ce que l'on sait

i) Riemann (1859) : Les 3 premiers zéros de ζ ont pour partie réelle $\frac{1}{2}$.

ii) Hardy (1912) : ζ admet une infinité de zéros de partie réelle $\frac{1}{2}$.

iii) Conrey (1989) : Au moins 40% des zéros de ζ ont pour partie réelle $\frac{1}{2}$.

iv) Gourdon, Demichel (2004) : Les 10^{13} premiers zéros de ζ ont pour partie réelle $\frac{1}{2}$.

v) Atiyah (2018)

Ce que l'on sait

i) Riemann (1859) : Les 3 premiers zéros de ζ ont pour partie réelle $\frac{1}{2}$.

ii) Hardy (1912) : ζ admet une infinité de zéros de partie réelle $\frac{1}{2}$.

iii) Conrey (1989) : Au moins 40% des zéros de ζ ont pour partie réelle $\frac{1}{2}$.

iv) Gourdon, Demichel (2004) : Les 10^{13} premiers zéros de ζ ont pour partie réelle $\frac{1}{2}$.

v) Atiyah (2018) : rien !

Plan

Nombres premiers en progressions arithmétiques

Autre question : la répartition des nombres premiers en progressions arithmétiques.

Nombres premiers en progressions arithmétiques

Autre question : la répartition des nombres premiers en progressions arithmétiques.

La stratégie d'Euclide permet de montrer qu'il y a une infinité de nombres premiers de la forme $4n+3$, $n \in \mathbb{Z}$:

$$4p_1 \dots p_k - 1.$$

Nombres premiers en progressions arithmétiques

Autre question : la répartition des nombres premiers en progressions arithmétiques.

La stratégie d'Euclide permet de montrer qu'il y a une infinité de nombres premiers de la forme $4n+3$, $n \in \mathbb{Z}$:

$$4p_1 \dots p_k - 1.$$

En cherchant un peu, on peut faire la même chose avec $4n+1$:

$$4(p_1 \dots p_k)^2 + 1.$$

Nombres premiers en progressions arithmétiques

Autre question : la répartition des nombres premiers en progressions arithmétiques.

La stratégie d'Euclide permet de montrer qu'il y a une infinité de nombres premiers de la forme $4n+3$, $n \in \mathbb{Z}$:

$$4p_1 \dots p_k - 1.$$

En cherchant un peu, on peut faire la même chose avec $4n+1$:

$$4(p_1 \dots p_k)^2 + 1.$$

Question : quand peut-on avoir une infinité de nombres premiers de la forme $a + qn, n \in \mathbb{Z}$?

Nombres premiers en progressions arithmétiques

Condition nécessaire : a et q premiers entre eux.

Nombres premiers en progressions arithmétiques

Condition nécessaire : a et q premiers entre eux.

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 $a^2 = 1 \bmod q$.

Nombres premiers en progressions arithmétiques

Condition nécessaire : a et q premiers entre eux.

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 $a^2 = 1 \mod q$.

Nombres premiers en progressions arithmétiques

Théorème (Dirichlet, 1837).

Soient $a, q \in \mathbb{Z}$ premiers entre eux. Alors pour $x > 1$,

$$\sum_{p=a \bmod q} \frac{1}{p^x} = \frac{1}{\varphi(q)} \log\left(\frac{1}{x-1}\right) + O(1).$$

Nombres premiers en progressions arithmétiques

Théorème (Dirichlet, 1837).

Soient $a, q \in \mathbb{Z}$ premiers entre eux. Alors pour $x > 1$,

$$\sum_{p = a \bmod q} \frac{1}{p^x} = \frac{1}{\varphi(q)} \log\left(\frac{1}{x-1}\right) + O(1).$$

Corollaire (théorème de la progression arithmétique).

Soient $a, q \in \mathbb{Z}$ premiers entre eux. Alors il existe une infinité de nombres premiers de la forme $a + qn, n \in \mathbb{Z}$.

Nombres premiers en progressions arithmétiques

Ingrédients :

i) Les **caractères de Dirichlet**, morphismes $\chi : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^*$.

Nombres premiers en progressions arithmétiques

Ingrédients :

i) Les **caractères de Dirichlet**, morphismes $\chi : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^*$.
ii) Les **relations d'orthogonalité** qui donnent

$$\mathbb{1}_{\{a \bmod q\}}(k) = \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \chi(a)\overline{\chi(k)}.$$

Nombres premiers en progressions arithmétiques

Ingrédients :

i) Les **caractères de Dirichlet**, morphismes $\chi : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^*$.

ii) Les **relations d'orthogonalité** qui donnent

$$\mathbb{1}_{\{a \bmod q\}}(k) = \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \chi(a)\overline{\chi(k)}.$$

iii) Les **fonctions L de Dirichlet**,

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

Nombres premiers en progressions arithmétiques

Ingrédients :

i) Les **caractères de Dirichlet**, morphismes $\chi : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^*$.

ii) Les **relations d'orthogonalité** qui donnent

$$\mathbb{1}_{\{a \bmod q\}}(k) = \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \chi(a)\overline{\chi(k)}.$$

iii) Les **fonctions L de Dirichlet**,

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

iv) La clé : $L(1,\chi_0) = +\infty$ et $L(1,\chi) \neq 0$ pour $\chi \neq \chi_0$ (χ_0 étant le caractère trivial).

Nombres premiers en progressions arithmétiques

Théorème (de la Vallée-Poussin, 1899).

Pour $a, q \in \mathbb{Z}$ premiers entre eux on a

$$\pi(x, q, a) = \frac{\mathrm{li}(x)}{\varphi(q)} + O_q(x \exp(-c\sqrt{\log x})).$$

Nombres premiers en progressions arithmétiques

Théorème (de la Vallée-Poussin, 1899).

Pour $a, q \in \mathbb{Z}$ premiers entre eux on a

$$\pi(x, q, a) = \frac{\mathrm{li}(x)}{\varphi(q)} + O_q(x \exp(-c\sqrt{\log x})).$$

Théorème (Siegel, Walfisz, 1936).

Pour $a, q \in \mathbb{Z}$ premiers entre eux et $q \leq (\log x)^N$, on a

$$\pi(x, q, a) = \frac{\mathrm{li}(x)}{\varphi(q)} + O(x \exp(-c_N\sqrt{\log x})).$$

Nombres premiers en progressions arithmétiques

Théorème (Green, Tao, 2004).

Pour tout entier $k \geq 1$, il existe une progression arithmétique de longueur k dans l'ensemble des nombres premiers.

Nombres premiers en progressions arithmétiques

Théorème (Green, Tao, 2004).

Pour tout entier $k \geq 1$, il existe une progression arithmétique de longueur k dans l'ensemble des nombres premiers.

En pratique, la progression connue la plus longue est de 26 termes :

$$43142746595714191 + n(2\times3\times5\times7\times11\times13\times17\times19\times23\times23681770),$$

$$0 \leq n \leq 25.$$

Courses de nombres premiers

Une conséquence du théorème des nombres premiers en progressions arithmétiques : les nombres premiers sont bien répartis asymptotiquement dans les classes inversibles modulo q.

Courses de nombres premiers

Une conséquence du théorème des nombres premiers en progressions arithmétiques : les nombres premiers sont bien répartis asymptotiquement dans les classes inversibles modulo q.

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

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

Courses de nombres premiers

Une conséquence du théorème des nombres premiers en progressions arithmétiques : les nombres premiers sont bien répartis asymptotiquement dans les classes inversibles modulo q.

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

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

Courses de nombres premiers

Problèmes :

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

Courses de nombres premiers

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).

Courses de nombres premiers

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

Courses de nombres premiers

Cependant, les nombres premiers ont quand même une tendance à être plus souvent 3 mod 4 que 1 mod 4.

Courses de nombres premiers

Cependant, les nombres premiers ont quand même une tendance à être plus souvent 3 mod 4 que 1 mod 4.

Pour quantifier cette tendance (**biais de Chebychev**), on voudrait « mesurer »

$$\mathcal{P}_{4;3,1} := \{x \geq 2 \mid \pi(x,4,3) > \pi(x,4,1)\}.$$

Courses de nombres premiers

Cependant, les nombres premiers ont quand même une tendance à être plus souvent 3 mod 4 que 1 mod 4.

Pour quantifier cette tendance (**biais de Chebychev**), on voudrait « mesurer »

$$\mathcal{P}_{4;3,1} := \{x \geq 2 \mid \pi(x,4,3) > \pi(x,4,1)\}.$$

Une notion naturelle de taille serait la densité naturelle

$$\lim_{x \to +\infty} \frac{|\mathcal{P}_{4;3,1} \cap [0,x]|}{x},$$

mais elle n'existe pas (Wintner, 1941).

Courses de nombres premiers

Définition.

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

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

Courses de nombres premiers

Définition.

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

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

Théorème (Rubinstein, Sarnak, 1994).

Supposons l'hypothèse de Riemann pour toutes les fonctions L de Dirichlet modulo 4, et que les parties imaginaires des zéros non triviaux de ces fonctions sont linéairement indépendants sur $\mathbb{Q}$. Alors $\delta(\mathcal{P}_{4;3,1})$ existe et vaut

$$\approx 0,9959\ldots$$

Courses de nombres premiers

Ingrédients :

i) Formules exactes

$$\frac{\pi(x,4,3)-\pi(x,4,1)}{\sqrt{x}/\log x} = \overbrace{|\sqrt{\{1\}}|-|\sqrt{\{3\}}|}^{>0} + \sum_{\chi} \overline{\chi(1)-\chi(3)} \sum_{\gamma_\chi} \frac{x^{i\gamma_\chi}}{\frac{1}{2}+i\gamma_\chi} + O\left(\frac{1}{\log x}\right).$$

Courses de nombres premiers

Ingrédients :

i) Formules exactes

$$\frac{\pi(x,4,3)-\pi(x,4,1)}{\sqrt{x}/\log x} = \overbrace{|\sqrt{\{1\}}| - |\sqrt{\{3\}}|}^{>0} + \sum_{\chi} \overline{\chi(1)-\chi(3)} \sum_{\gamma_\chi} \frac{x^{i\gamma_\chi}}{\frac{1}{2}+i\gamma_\chi} + O\left(\frac{1}{\log x}\right).$$

ii) Un résultat d'équirépartition (Kronecker-Weyl) pour les $x^{i\gamma_\chi}$ grâce à l'indépendance linéaire des γ_χ.

Courses de nombres premiers

Ingrédients :

i) Formules exactes

$$\frac{\pi(x,4,3)-\pi(x,4,1)}{\sqrt{x}/\log x} = \overbrace{|\sqrt{\{1\}}|-|\sqrt{\{3\}}|}^{>0} + \sum_{\chi} \overline{\chi(1)-\chi(3)} \sum_{\gamma_\chi} \frac{x^{i\gamma_\chi}}{\frac{1}{2}+i\gamma_\chi} + O\left(\frac{1}{\log x}\right).$$

ii) Un résultat d'équirépartition (Kronecker-Weyl) pour les $x^{i\gamma_\chi}$ grâce à l'indépendance linéaire des γ_χ.

iii) Existence d'une mesure de probabilité $\mu_{4;3,1}$ telle que $\delta(\mathcal{P}_{4;3,1}) = \mu_{4;3,1}([0,+\infty[)$.

Courses de nombres premiers

Ingrédients :

i) Formules exactes

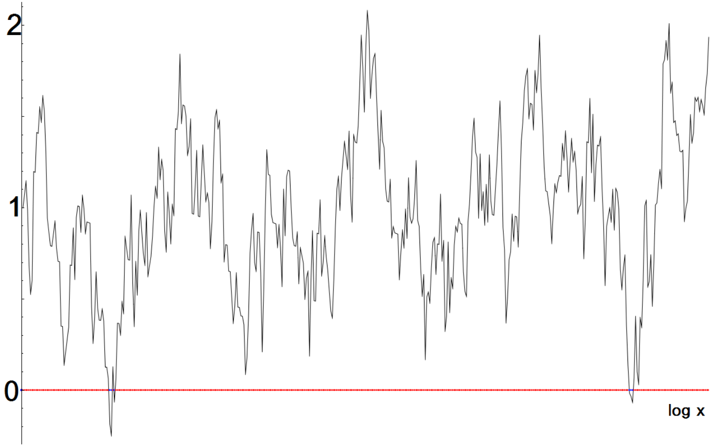
$$\frac{\pi(x,4,3)-\pi(x,4,1)}{\sqrt{x}/\log x} = \overbrace{|\sqrt{\{1\}}| - |\sqrt{\{3\}}|}^{>0} + \sum_{\chi} \overline{\chi(1)-\chi(3)} \sum_{\gamma_\chi} \frac{x^{i\gamma_\chi}}{\frac{1}{2}+i\gamma_\chi} + O\left(\frac{1}{\log x}\right).$$

ii) Un résultat d'équirépartition (Kronecker-Weyl) pour les $x^{i\gamma_\chi}$ grâce à l'indépendance linéaire des γ_χ.

iii) Existence d'une mesure de probabilité $\mu_{4;3,1}$ telle que $\delta(\mathcal{P}_{4;3,1}) = \mu_{4;3,1}([0,+\infty[)$.

iv) Étude de la transformée de Fourier de $\mu_{4;3,1}$.

Courses de nombres premiers



Source : Daniel Fiorilli, Graphe de $\frac{\pi(e^y,4,3)-\pi(e^y,4,1)}{e^{y/2}/y}$, $10^4 \leq y \leq 10^8$

Courses de nombres premiers

Le biais de Chebychev est quantifié : « 99% du temps », les nombres premiers valant 3 mod 4 sont en tête dans la course contre les nombres premiers valant 1 mod 4.

Courses de nombres premiers

Le biais de Chebychev est quantifié : « 99% du temps », les nombres premiers valant 3 mod 4 sont en tête dans la course contre les nombres premiers valant 1 mod 4.

4, 3 et 1 n'ont rien de particulier, et ils démontrent que pour $q, a, b \in \mathbb{Z}$ avec q premier avec a, b, $\delta(\mathcal{P}_{q;a,b})$ existe toujours et que

$$0 < \delta(\mathcal{P}_{q;a,b}) < 1.$$

Courses de nombres premiers

Le biais de Chebychev est quantifié : « 99% du temps », les nombres premiers valant 3 mod 4 sont en tête dans la course contre les nombres premiers valant 1 mod 4.

$4, 3$ et 1 n'ont rien de particulier, et ils démontrent que pour $q, a, b \in \mathbb{Z}$ avec q premier avec a, b, $\delta(\mathcal{P}_{q;a,b})$ existe toujours et que

$$0 < \delta(\mathcal{P}_{q;a,b}) < 1.$$

Si a et b sont simultanément des carrés ou non mod q alors $\delta(\mathcal{P}_{q;a,b}) = \frac{1}{2}$ (pas de biais de Chebychev).

Courses de nombres premiers

Le biais de Chebychev est quantifié : « 99% du temps », les nombres premiers valant 3 mod 4 sont en tête dans la course contre les nombres premiers valant 1 mod 4.

4, 3 et 1 n'ont rien de particulier, et ils démontrent que pour $q, a, b \in \mathbb{Z}$ avec q premier avec a, b, $\delta(\mathcal{P}_{q;a,b})$ existe toujours et que

$$0 < \delta(\mathcal{P}_{q;a,b}) < 1.$$

Si a et b sont simultanément des carrés ou non mod q alors $\delta(\mathcal{P}_{q;a,b}) = \frac{1}{2}$ (pas de biais de Chebychev).

$$\delta(\mathcal{P}_{3;2,1}) \approx 0.9990\ldots, \delta(\mathcal{P}_{\pi(x) \text{ vs } \mathrm{li}(x)}) \approx 0.00000026\ldots$$

Merci de votre attention

et vive les nombres premiers !