# Une introduction aux courses de nombres premiers

**Alexandre Bailleul**

ENS Paris-Saclay

19 novembre 2025

# Sommaire

## Théorie analytique des nombres

- Qu'est-ce que la théorie analytique des nombres ?

# Théorie analytique des nombres

- Qu'est-ce que la théorie analytique des nombres ?

- La théorie des nombres s'intéresse à des questions concernant les nombres entiers

## Théorie analytique des nombres

- Qu'est-ce que la théorie analytique des nombres ?
- La théorie des nombres s'intéresse à des questions concernant les nombres entiers :
  - Est-ce que, pour $n \geq 3$, l'équation $x^n + y^n = z^n$ admet des solutions avec $x, y, z \in \mathbb{Z}$ et $xyz \neq 0$ ?

# Théorie analytique des nombres

- Qu'est-ce que la théorie analytique des nombres ?
- La théorie des nombres s'intéresse à des questions concernant les nombres entiers :
  - Est-ce que, pour $n \geq 3$, l'équation $x^n + y^n = z^n$ admet des solutions avec $x, y, z \in \mathbb{Z}$ et $xyz \neq 0$ ?
  - Est-ce que tout entier pair supérieur à 2 peut s'écrire comme la somme de deux nombres premiers ?

## Théorie analytique des nombres

- Qu'est-ce que la théorie analytique des nombres ?
- La théorie des nombres s'intéresse à des questions concernant les nombres entiers :
  - Est-ce que, pour $n \geq 3$, l'équation $x^n + y^n = z^n$ admet des solutions avec $x, y, z \in \mathbb{Z}$ et $xyz \neq 0$ ?
  - Est-ce que tout entier pair supérieur à 2 peut s'écrire comme la somme de deux nombres premiers ?
  - Soit $n \in \mathbb{N}^*$. Existe-t-il un triangle rectangle à côtés rationnels dont l'aire vaut $n$ ?

# Théorie analytique des nombres

- Qu'est-ce que la théorie analytique des nombres ?
- La théorie des nombres s'intéresse à des questions concernant les nombres entiers :
  - Est-ce que, pour $n \geq 3$, l'équation $x^n + y^n = z^n$ admet des solutions avec $x, y, z \in \mathbb{Z}$ et $xyz \neq 0$ ?
  - Est-ce que tout entier pair supérieur à 2 peut s'écrire comme la somme de deux nombres premiers ?
  - Soit $n \in \mathbb{N}^*$. Existe-t-il un triangle rectangle à côtés rationnels dont l'aire vaut $n$ ?
  - Soit $m \geq 2$. De combien de manières est-il possible d'avoir $m = \binom{n}{k}$ ?

# Théorie analytique des nombres

- Qu'est-ce que la théorie analytique des nombres ?
- La théorie des nombres s'intéresse à des questions concernant les nombres entiers :
  - Est-ce que, pour $n \geq 3$, l'équation $x^n + y^n = z^n$ admet des solutions avec $x, y, z \in \mathbb{Z}$ et $xyz \neq 0$ ?
  - Est-ce que tout entier pair supérieur à 2 peut s'écrire comme la somme de deux nombres premiers ?
  - Soit $n \in \mathbb{N}^*$. Existe-t-il un triangle rectangle à côtés rationnels dont l'aire vaut $n$ ?
  - Soit $m \geq 2$. De combien de manières est-il possible d'avoir $m = \binom{n}{k}$ ?
- Sa partie analytique utilise des outils d'analyse (limites, continuité, analyse complexe, intégration, *etc.*) pour répondre à ces questions.

# Théorie analytique des nombres

- Qu'est-ce que la théorie analytique des nombres ?
- La théorie des nombres s'intéresse à des questions concernant les nombres entiers :
  - Est-ce que, pour $n \geq 3$, l'équation $x^n + y^n = z^n$ admet des solutions avec $x, y, z \in \mathbb{Z}$ et $xyz \neq 0$ ?
  - Est-ce que tout entier pair supérieur à 2 peut s'écrire comme la somme de deux nombres premiers ?
  - Soit $n \in \mathbb{N}^*$. Existe-t-il un triangle rectangle à côtés rationnels dont l'aire vaut $n$ ?
  - Soit $m \geq 2$. De combien de manières est-il possible d'avoir $m = \binom{n}{k}$ ?
- Sa partie analytique utilise des outils d'analyse (limites, continuité, analyse complexe, intégration, *etc.*) pour répondre à ces questions.
- Elle est particulièrement adaptée pour étudier les **nombres premiers** (notés $p$ dans toute la suite).

# Sommaire

# Une preuve vieille comme le monde

**Théorème. (Euclide, -300 av. J.-C.)**

Il existe une infinité de nombres premiers.

# Une preuve vieille comme le monde

**Théorème. (Euclide, -300 av. J.-C.)**

Il existe une infinité de nombres premiers.

- Si $p_1, \ldots, p_r$ sont des nombres premiers, on pose $N = 1 + p_1 \times \cdots \times p_r$.

# Une preuve vieille comme le monde

**Théorème. (Euclide, -300 av. J.-C.)**

Il existe une infinité de nombres premiers.

- Si $p_1, \ldots, p_r$ sont des nombres premiers, on pose $N = 1 + p_1 \times \cdots \times p_r$.
- Alors $N \geq 2$ donc admet un facteur premier $p$.

# Une preuve vieille comme le monde

**Théorème. (Euclide, -300 av. J.-C.)**

Il existe une infinité de nombres premiers.

- Si $p_1, \ldots, p_r$ sont des nombres premiers, on pose $N = 1 + p_1 \times \cdots \times p_r$.
- Alors $N \geq 2$ donc admet un facteur premier $p$. Mais $p \neq p_i$ sinon $p$ diviserait $N - p_1 \times \cdots \times p_r = 1$ !

# Une preuve vieille comme le monde

**Théorème. (Euclide, -300 av. J.-C.)**

Il existe une infinité de nombres premiers.

- Si $p_1, \ldots, p_r$ sont des nombres premiers, on pose $N = 1 + p_1 \times \cdots \times p_r$.
- Alors $N \geq 2$ donc admet un facteur premier $p$. Mais $p \neq p_i$ sinon $p$ diviserait $N - p_1 \times \cdots \times p_r = 1$ !
- Donc la liste $p_1, \ldots, p_r$ est **incomplète**.

# Compliquons la question

- Il existe une infinité de nombres premiers de la forme $4n+3$

# Compliquons la question

- Il existe une infinité de nombres premiers de la forme $4n + 3$ :
  $N = 4p_1 \times \cdots \times p_r - 1$ est congru à $-1 = 3$ modulo 4 donc a au moins un facteur premier congru à $3$ modulo 4 !

## Compliquons la question

- Il existe une infinité de nombres premiers de la forme $4n + 3$ :
  $N = 4p_1 \times \cdots \times p_r - 1$ est congru à $-1 = 3$ modulo 4 donc a au moins un facteur premier congru à $3$ modulo 4 !

- Il existe une infinité de nombres premiers de la forme $4n + 1$

# Compliquons la question

- Il existe une infinité de nombres premiers de la forme $4n+3$ :
  $N = 4p_1 \times \cdots \times p_r - 1$ est congru à $-1 = 3$ modulo 4 donc a au moins un facteur premier congru à 3 modulo 4 !

- Il existe une infinité de nombres premiers de la forme $4n+1$ :
  $N = 4(p_1 \times \cdots \times p_r)^2 + 1$ a un facteur premier $p$ tel que
  $(2p_1 \times \cdots \times p_r)^2 \equiv -1 \bmod p$

# Compliquons la question

- Il existe une infinité de nombres premiers de la forme $4n+3$ :
  $N = 4p_1 \times \cdots \times p_r - 1$ est congru à $-1 = 3$ modulo 4 donc a au moins un facteur premier congru à $3$ modulo 4 !

- Il existe une infinité de nombres premiers de la forme $4n+1$ :
  $N = 4(p_1 \times \cdots \times p_r)^2 + 1$ a un facteur premier $p$ tel que
  $(2p_1 \times \cdots \times p_r)^2 \equiv -1 \bmod p$ d'où $p \equiv 1 \bmod 4$

## Compliquons la question

- Il existe une infinité de nombres premiers de la forme $4n+3$ :
  $N = 4p_1 \times \cdots \times p_r - 1$ est congru à $-1 = 3$ modulo $4$ donc a au moins un facteur premier congru à $3$ modulo $4$ !

- Il existe une infinité de nombres premiers de la forme $4n+1$ :
  $N = 4(p_1 \times \cdots \times p_r)^2 + 1$ a un facteur premier $p$ tel que
  $(2p_1 \times \cdots \times p_r)^2 \equiv -1 \bmod p$ d'où $p \equiv 1 \bmod 4$ (une racine carrée de $-1$ est un élément d'ordre $4$ dans le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$).

# Compliquons la question

- Il existe une infinité de nombres premiers de la forme $4n+3$ :
  $N = 4p_1 \times \cdots \times p_r - 1$ est congru à $-1 = 3$ modulo 4 donc a au moins un facteur premier congru à $3$ modulo 4 !

- Il existe une infinité de nombres premiers de la forme $4n+1$ :
  $N = 4(p_1 \times \cdots \times p_r)^2 + 1$ a un facteur premier $p$ tel que $(2p_1 \times \cdots \times p_r)^2 \equiv -1 \bmod p$ d'où $p \equiv 1 \bmod 4$ (une racine carrée de $-1$ est un élément d'ordre $4$ dans le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$).

- Schur (1912), Murty (1988) : Il existe d'autres cas $qn+a$ traitables de manière élémentaire, mais **on ne sait pas se passer d'analyse pour les progressions arithmétiques** $qn+a$ **générales**.

# Démonstration alternative

- Montrons l'existence d'une infinité de nombres premiers de la forme $4n + 1$ de manière **analytique**, en suivant Dirichlet (inspiré d'Euler).

## Démonstration alternative

- Montrons l'existence d'une infinité de nombres premiers de la forme $4n+1$ de manière **analytique**, en suivant Dirichlet (inspiré d'Euler). On considère les produits (dits **eulériens**)

$$L_1(s) = \prod_{p \neq 2} \frac{1}{1 - \frac{1}{p^s}}$$

et

$$L_2(s) = \prod_{p \neq 2} \frac{1}{1 - \frac{(-1)^{\frac{p-1}{2}}}{p^s}}$$

pour $s > 1$.

## Démonstration alternative

- Montrons l'existence d'une infinité de nombres premiers de la forme $4n+1$ de manière **analytique**, en suivant Dirichlet (inspiré d'Euler). On considère les produits (dits **eulériens**)

$$L_1(s) = \prod_{p\neq 2} \frac{1}{1-\frac{1}{p^s}}$$

et

$$L_2(s) = \prod_{p\neq 2} \frac{1}{1-\frac{(-1)^{\frac{p-1}{2}}}{p^s}}$$

pour $s > 1$.

- Alors

$$\ln L_1(s) = \sum_{p\neq 2} -\ln\left(1-\frac{1}{p^s}\right) = \sum_{k\geq 1}\sum_{p\neq 2} \frac{1}{kp^{ks}} = \sum_{p\neq 2} \frac{1}{p^s} + O(1)$$

et de même

$$\ln L_2(s) = \sum_{p\neq 2} \frac{(-1)^{\frac{p-1}{2}}}{p^s} + O(1).$$

## Démonstration alternative

- On en déduit que

$$\frac{1}{2}(\ln L_1(s) + \ln L_2(s)) = \sum_{p \equiv 1 \bmod 4} \frac{1}{p^s} + O(1).$$

# Démonstration alternative

- On en déduit que

$$\frac{1}{2}(\ln L_1(s) + \ln L_2(s)) = \sum_{p \equiv 1 \bmod 4} \frac{1}{p^s} + O(1).$$

- Or, en développant,

$$L_1(s) = \prod_{p \neq 2} \sum_{k=0}^{+\infty} \frac{1}{p^{ks}} = \sum_{n \text{ impair}} \frac{1}{n^s}$$

et

$$L_2(s) = \prod_{p \neq 2} \sum_{k=0}^{+\infty} \frac{(-1)^{\frac{p-1}{2}}}{p^{ks}} = \sum_{n \geq 1} \frac{(-1)^n}{(2n+1)^s}.$$

# Démonstration alternative

- On en déduit que

$$\frac{1}{2}(\ln L_1(s) + \ln L_2(s)) = \sum_{p \equiv 1 \bmod 4} \frac{1}{p^s} + O(1).$$

- Or, en développant,

$$L_1(s) = \prod_{p \neq 2} \sum_{k=0}^{+\infty} \frac{1}{p^{ks}} = \sum_{n \text{ impair}} \frac{1}{n^s}$$

et

$$L_2(s) = \prod_{p \neq 2} \sum_{k=0}^{+\infty} \frac{(-1)^{\frac{p-1}{2}}}{p^{ks}} = \sum_{n \geq 1} \frac{(-1)^n}{(2n+1)^s}.$$

- Donc $\ln L_1(s) \underset{s \to 1^+}{\to} +\infty$ et $\ln L_2(s) \underset{s \to 1^+}{\to} \ln\left(\frac{\pi}{4}\right) \neq -\infty$.

## Démonstration alternative

- Conclusion : $\displaystyle\sum_{p\equiv 1 \bmod 4} \frac{1}{p^s} = \frac{1}{2}(\ln L_1(s) + L_2(s)) + O(1) \underset{s\to 1^+}{\to} +\infty$ et il existe une infinité de nombres premiers de la forme $4n+1$.

## Démonstration alternative

- Conclusion : $\displaystyle\sum_{p\equiv 1 \bmod 4} \frac{1}{p^s} = \frac{1}{2}(\ln L_1(s) + L_2(s)) + O(1) \underset{s\to 1^+}{\to} +\infty$ et il existe une infinité de nombres premiers de la forme $4n+1$.
- **On peut l'expliquer par le fait que $\displaystyle\sum_n \frac{1}{n}$ diverge et $L_2(1) = \frac{\pi}{4} \neq 0$ !**

# Démonstration alternative

- Conclusion : $\displaystyle\sum_{p\equiv 1 \bmod 4} \frac{1}{p^s} = \frac{1}{2}(\ln L_1(s) + L_2(s)) + O(1) \underset{s\to 1^+}{\to} +\infty$ et il existe une infinité de nombres premiers de la forme $4n+1$.
- **On peut l'expliquer par le fait que $\displaystyle\sum_n \frac{1}{n}$ diverge et $L_2(1) = \frac{\pi}{4} \neq 0$ !**
- En prenant la différence, on obtient l'existence d'une infinité de nombres premiers de la forme $4n+3$.

# Le théorème de la progression arithmétique

**Théorème. (Dirichlet, 1837)**

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

# Le théorème de la progression arithmétique

**Théorème. (Dirichlet, 1837)**

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

- Pour détecter la condition $p \equiv a \bmod q$, Dirichlet introduit les **caractères de Dirichlet** : morphismes $\chi : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$.

# Le théorème de la progression arithmétique

**Théorème. (Dirichlet, 1837)**

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

- Pour détecter la condition $p \equiv a \bmod q$, Dirichlet introduit les **caractères de Dirichlet** : morphismes $\chi : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$. Ils vérifient la formule d'orthogonalité suivante :

$$\frac{1}{\varphi(q)} \sum_{\chi \text{ caractère de Dirichlet mod } q} \chi(p)\overline{\chi(a)} = \begin{cases} 1 \text{ si } p \equiv a \bmod q, \\ 0 \text{ sinon.} \end{cases}$$

# Le théorème de la progression arithmétique

**Théorème. (Dirichlet, 1837)**

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

- Pour détecter la condition $p \equiv a \bmod q$, Dirichlet introduit les **caractères de Dirichlet** : morphismes $\chi : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$. Ils vérifient la formule d'orthogonalité suivante :

$$\frac{1}{\varphi(q)} \sum_{\chi \text{ caractère de Dirichlet mod } q} \chi(p)\overline{\chi(a)} = \begin{cases} 1 \text{ si } p \equiv a \bmod q, \\ 0 \text{ sinon.} \end{cases}$$

- A chaque caractère de Dirichlet, on associe une **fonction $L$ de Dirichlet**

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

# Le théorème de la progression arithmétique

**Théorème. (Dirichlet, 1837)**

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

- Pour détecter la condition $p \equiv a \bmod q$, Dirichlet introduit les **caractères de Dirichlet** : morphismes $\chi : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$. Ils vérifient la formule d'orthogonalité suivante :

$$\frac{1}{\varphi(q)} \sum_{\chi \text{ caractère de Dirichlet mod } q} \chi(p)\overline{\chi(a)} = \begin{cases} 1 \text{ si } p \equiv a \bmod q, \\ 0 \text{ sinon.} \end{cases}$$

- A chaque caractère de Dirichlet, on associe une **fonction $L$ de Dirichlet**

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

Le point-clé (et le plus difficile) de la démonstration de Dirichlet est que $L(1, \chi) \neq 0$ pour tout caractère non trivial, tandis que $L(s, 1) \underset{s \to 1^+}{\to} +\infty$.

# Une application

**Théorème. ("Principe local-global")**

Soit $n \in \mathbb{Z}$ tel que $n$ est un carré modulo tous les nombres premiers sauf au plus un nombre fini. Alors $n$ est un carré.

# Une application

**Théorème. ("Principe local-global")**

Soit $n \in \mathbb{Z}$ tel que $n$ est un carré modulo tous les nombres premiers sauf au plus un nombre fini. Alors $n$ est un carré.

- Soit $n \in \mathbb{Z}$ qui n'est pas un carré (ni une puissance de 2, cas plus simple). Alors $4n$ n'est pas un carré non plus et on a $4n = p^r m$ avec $p$ un nombre premier impair, $r \in \mathbb{N}$ impair et $m$ premiers avec $p$. Fixons un entier $a$ tel que $a$ n'est pas un carré modulo $p$ et notons $p_1, \ldots, p_t$ les facteurs premiers de $m$.

# Une application

**Théorème. ("Principe local-global")**

Soit $n \in \mathbb{Z}$ tel que $n$ est un carré modulo tous les nombres premiers sauf au plus un nombre fini. Alors $n$ est un carré.

- Soit $n \in \mathbb{Z}$ qui n'est pas un carré (ni une puissance de 2, cas plus simple). Alors $4n$ n'est pas un carré non plus et on a $4n = p^r m$ avec $p$ un nombre premier impair, $r \in \mathbb{N}$ impair et $m$ premiers avec $p$. Fixons un entier $a$ tel que $a$ n'est pas un carré modulo $p$ et notons $p_1, \ldots, p_t$ les facteurs premiers de $m$.

- Par le théorème chinois et le théorème de Dirichlet, on montre l'existence d'une infinité de nombres premiers $q$ tel que :

$$\begin{cases} q \equiv 1 \bmod 4, \\ q \equiv a \bmod p, \\ \forall i \in \{1, \ldots, t\}, q \equiv 1 \bmod p_i. \end{cases}$$

# Une application

**Théorème. ("Principe local-global")**

Soit $n \in \mathbb{Z}$ tel que $n$ est un carré modulo tous les nombres premiers sauf au plus un nombre fini. Alors $n$ est un carré.

- Soit $n \in \mathbb{Z}$ qui n'est pas un carré (ni une puissance de 2, cas plus simple). Alors $4n$ n'est pas un carré non plus et on a $4n = p^r m$ avec $p$ un nombre premier impair, $r \in \mathbb{N}$ impair et $m$ premiers avec $p$. Fixons un entier $a$ tel que $a$ n'est pas un carré modulo $p$ et notons $p_1, \ldots, p_t$ les facteurs premiers de $m$.

- Par le théorème chinois et le théorème de Dirichlet, on montre l'existence d'une infinité de nombres premiers $q$ tel que :

$$\begin{cases} q \equiv 1 \bmod 4, \\ q \equiv a \bmod p, \\ \forall i \in \{1, \ldots, t\}, q \equiv 1 \bmod p_i. \end{cases}$$

- Alors $n$ n'est pas un carré modulo $q$ :

$$\left(\frac{n}{q}\right) = \left(\frac{p}{q}\right)^r \left(\frac{m}{q}\right) \overset{\text{(réciprocité quadratique)}}{=} \left(\frac{q}{p}\right)^r = -1.$$

# Sommaire

# Répartition des nombres premiers dans les progressions arithmétiques

- On a établi l'existence d'une infinité de nombres premiers congrus à $a$ modulo $q$. Peut-on les compter jusqu'à une borne $x$ donnée ?

# Répartition des nombres premiers dans les progressions arithmétiques

- On a établi l'existence d'une infinité de nombres premiers congrus à $a$ modulo $q$. Peut-on les compter jusqu'à une borne $x$ donnée ?

**Théorème. (des nombres premiers en progressions arithmétiques, de la Vallée-Poussin, 1896)**

Soit $q \geq 2$ et $a \in \mathbb{Z}$ premier avec $q$. Notons $\pi(x; q, a) = \#\{p \leq x \mid p \equiv a \bmod q\}$. Alors

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

# Répartition des nombres premiers dans les progressions arithmétiques

- On a établi l'existence d'une infinité de nombres premiers congrus à $a$ modulo $q$. Peut-on les compter jusqu'à une borne $x$ donnée ?

**Théorème. (des nombres premiers en progressions arithmétiques, de la Vallée-Poussin, 1896)**

Soit $q \geq 2$ et $a \in \mathbb{Z}$ premier avec $q$. Notons $\pi(x; q, a) = \#\{p \leq x \mid p \equiv a \bmod q\}$. Alors

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

- Avec $q = 2$, on retrouve le **théorème des nombres premiers**, $\pi(x) = \#\{p \leq x\} \underset{x \to +\infty}{\sim} \frac{x}{\ln x}$.

# Répartition des nombres premiers dans les progressions arithmétiques

- On a établi l'existence d'une infinité de nombres premiers congrus à $a$ modulo $q$. Peut-on les compter jusqu'à une borne $x$ donnée ?

**Théorème. (des nombres premiers en progressions arithmétiques, de la Vallée-Poussin, 1896)**

Soit $q \geq 2$ et $a \in \mathbb{Z}$ premier avec $q$. Notons $\pi(x; q, a) = \#\{p \leq x \mid p \equiv a \bmod q\}$. Alors

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

- Avec $q = 2$, on retrouve le **théorème des nombres premiers**, $\pi(x) = \#\{p \leq x\} \underset{x \to +\infty}{\sim} \frac{x}{\ln x}$. L'équivalent dans le TNPPA montre donc que **les nombres premiers sont bien répartis dans les** $\varphi(q)$ **classes inversibles modulo** $q$.

# Idées de démonstration

- Nous allons esquisser la preuve dans le cas $q = 2$, le cas général utilisant les mêmes idées appliquées aux fonctions $L(s, \chi)$ de Dirichlet.

# Idées de démonstration

- Nous allons esquisser la preuve dans le cas $q = 2$, le cas général utilisant les mêmes idées appliquées aux fonctions $L(s, \chi)$ de Dirichlet.

- Dans ce contexte, on retombe sur la fonction zêta de Riemann

$$\zeta : s \mapsto \sum_{n=1}^{+\infty} \frac{1}{n^s}, \quad \mathrm{Re}(s) > 1.$$

# Idées de démonstration

- Nous allons esquisser la preuve dans le cas $q = 2$, le cas général utilisant les mêmes idées appliquées aux fonctions $L(s, \chi)$ de Dirichlet.

- Dans ce contexte, on retombe sur la fonction zêta de Riemann

$$\zeta : s \mapsto \sum_{n=1}^{+\infty} \frac{1}{n^s}, \quad \mathrm{Re}(s) > 1.$$

- Comme précédemment on a un produit eulérien

$$\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}}$$

pour $\mathfrak{Re}(s) > 1$.

# Idées de démonstration

- L'**analyse complexe** permet de prolonger de manière unique $\zeta$ en une fonction "raisonnable" (holomorphe) sur $\mathbb{C} \setminus \{1\}$.

# Idées de démonstration

- L'**analyse complexe** permet de prolonger de manière unique $\zeta$ en une fonction "raisonnable" (holomorphe) sur $\mathbb{C} \setminus \{1\}$.

- Pour des raisons techniques, posons

$$\psi(x) = \sum_{\substack{p,k \in \mathbb{N}^* \\ p^k \leq x}} \ln p.$$

# Idées de démonstration

- L'**analyse complexe** permet de prolonger de manière unique $\zeta$ en une fonction "raisonnable" (holomorphe) sur $\mathbb{C} \setminus \{1\}$.
- Pour des raisons techniques, posons

$$\psi(x) = \sum_{\substack{p,k \in \mathbb{N}^* \\ p^k \leq x}} \ln p.$$

- On montre que

$$\pi(x) = \sum_{p \leq x} 1 = \frac{\psi(x)}{\ln(x)} + o\left(\frac{x}{\ln(x)}\right),$$

# Idées de démonstration

- L'**analyse complexe** permet de prolonger de manière unique $\zeta$ en une fonction "raisonnable" (holomorphe) sur $\mathbb{C} \setminus \{1\}$.

- Pour des raisons techniques, posons

$$\psi(x) = \sum_{\substack{p,k \in \mathbb{N}^* \\ p^k \leq x}} \ln p.$$

- On montre que

$$\pi(x) = \sum_{p \leq x} 1 = \frac{\psi(x)}{\ln(x)} + o\left(\frac{x}{\ln(x)}\right),$$

donc il suffit de montrer que $\psi(x) \underset{x \to +\infty}{\sim} x$.

# Quel rapport avec les zéros ?

- La clé pour démontrer le TNP est de localiser les **zéros de** $\zeta$.

## Quel rapport avec les zéros ?

- La clé pour démontrer le TNP est de localiser les **zéros de** $\zeta$.
- Avec encore plus d'**analyse complexe**, on montre la **formule explicite** suivante :

$$\psi(x) = x - \sum_{\substack{\rho \\ \zeta(\rho)=0}} \frac{x^\rho}{\rho} - \ln(2\pi).$$

# Illustration

- Comme
$$\left|\frac{x^\rho}{\rho}\right| = \frac{x^{\mathfrak{Re}(\rho)}}{|\rho|},$$
comprendre la taille de $\psi(x)$ (et donc de $\pi(x)$), c'est comprendre la **localisation des zéros** de $\zeta$.

- Comme
$$\left|\frac{x^\rho}{\rho}\right| = \frac{x^{\mathfrak{Re}(\rho)}}{|\rho|},$$
comprendre la taille de $\psi(x)$ (et donc de $\pi(x)$), c'est comprendre la **localisation des zéros** de $\zeta$.

- En particulier, **on montre que le TNP est équivalent au fait que** $\zeta(1+it) \neq 0$ **pour tout** $t \in \mathbb{R}^*$ **!**

- Comme
$$\left|\frac{x^\rho}{\rho}\right| = \frac{x^{\mathfrak{Re}(\rho)}}{|\rho|},$$
comprendre la taille de $\psi(x)$ (et donc de $\pi(x)$), c'est comprendre la **localisation des zéros** de $\zeta$.

- En particulier, **on montre que le TNP est équivalent au fait que** $\zeta(1+it) \neq 0$ **pour tout** $t \in \mathbb{R}^*$ **!**

- Toute amélioration de cette information améliore le terme d'erreur dans le TNP.

- Comme
$$\left|\frac{x^\rho}{\rho}\right| = \frac{x^{\mathfrak{Re}(\rho)}}{|\rho|},$$
comprendre la taille de $\psi(x)$ (et donc de $\pi(x)$), c'est comprendre la **localisation des zéros** de $\zeta$.

- En particulier, **on montre que le TNP est équivalent au fait que** $\zeta(1+it) \neq 0$ **pour tout** $t \in \mathbb{R}^*$ **!**

- Toute amélioration de cette information améliore le terme d'erreur dans le TNP. La meilleure estimation possible correspond au fait que $\zeta(\rho) = 0$ (et $\mathfrak{Re}(\rho) > 0$) implique que $\mathfrak{Re}(\rho) = \frac{1}{2}$ (**hypothèse de Riemann**).

# Le biais de Tchebychev

- On a vu que $\pi(x;4,1) \underset{x\to+\infty}{\sim} \pi(x;4,3) \underset{x\to+\infty}{\sim} \frac{x}{2\ln(x)}$. Dans une lettre de 1853, Tchebychev affirme que $\pi(x;4,3) > \pi(x;4,1)$ à partir d'un certain rang.

# Le biais de Tchebychev

- On a vu que $\pi(x;4,1) \underset{x\to+\infty}{\sim} \pi(x;4,3) \underset{x\to+\infty}{\sim} \frac{x}{2\ln(x)}$. Dans une lettre de 1853, Tchebychev affirme que $\pi(x;4,3) > \pi(x;4,1)$ à partir d'un certain rang.

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

# Le biais de Tchebychev

- On a vu que $\pi(x;4,1) \underset{x\to+\infty}{\sim} \pi(x;4,3) \underset{x\to+\infty}{\sim} \frac{x}{2\ln(x)}$. Dans une lettre de 1853, Tchebychev affirme que $\pi(x;4,3) > \pi(x;4,1)$ à partir d'un certain rang.
- Notons
$$\mathcal{P}_{4;3,1} = \{x \geq 2 \mid \pi(x;4,3) > \pi(x;4,1)\}$$
et
$$\mathcal{P}_{4;1,3} = \{x \geq 2 \mid \pi(x;4,1) > \pi(x;4,3)\}.$$

**Théorème. (Littlewood, 1914)**

Les ensembles $\mathcal{P}_{4;3,1}$ et $\mathcal{P}_{4;1,3}$ sont non bornés.

# Le biais de Tchebychev

- On a vu que $\pi(x;4,1) \underset{x\to+\infty}{\sim} \pi(x;4,3) \underset{x\to+\infty}{\sim} \frac{x}{2\ln(x)}$. Dans une lettre de 1853, Tchebychev affirme que $\pi(x;4,3) > \pi(x;4,1)$ à partir d'un certain rang.

- Notons

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

et

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

**Théorème. (Littlewood, 1914)**

Les ensembles $\mathcal{P}_{4;3,1}$ et $\mathcal{P}_{4;1,3}$ sont non bornés.

- Autrement dit, il y a une infinité de changement de signe entre les quantités $\pi(x;4,3)$ et $\pi(x;4,1)$ : Tchebychev s'est trompé !

## Le biais de Tchebychev

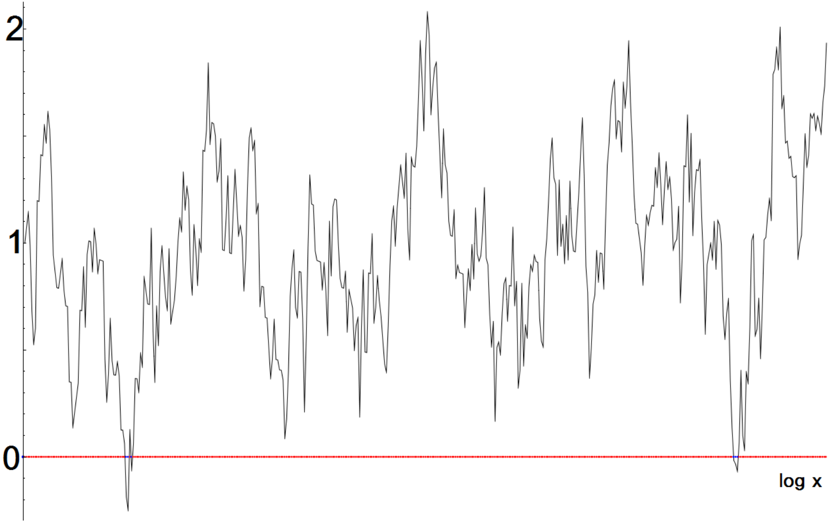
- On a vu que $\pi(x;4,1) \underset{x\to+\infty}{\sim} \pi(x;4,3) \underset{x\to+\infty}{\sim} \frac{x}{2\ln(x)}$. Dans une lettre de 1853, Tchebychev affirme que $\pi(x;4,3) > \pi(x;4,1)$ à partir d'un certain rang.

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

**Théorème. (Littlewood, 1914)**

Les ensembles $\mathcal{P}_{4;3,1}$ et $\mathcal{P}_{4;1,3}$ sont non bornés.

- Autrement dit, il y a une infinité de changement de signe entre les quantités $\pi(x;4,3)$ et $\pi(x;4,1)$ : Tchebychev s'est trompé ! (Mais pas tant que ça...)




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

Source : Daniel Fiorilli

# Rubinstein-Sarnak

- On peut essayer d'aller plus loin et mesurer la "taille" de $\mathcal{P}_{4;3,1}$.

**Théorème. (Rubinstein-Sarnak, 1994)**

Supposons GRH et LI pour la fonction $L(s, \chi_4)$. Alors la **densité logarithmique**

$$\delta(\mathcal{P}_{4;3,1}) = \lim_{X \to +\infty} \frac{1}{\ln X} \int_2^X \mathbf{1}_{\mathcal{P}_{4;3,1}}(t) \frac{\mathrm{d}t}{t}$$

existe et $\delta(\mathcal{P}_{4;3,1}) \approx 0,9959\ldots$

# Rubinstein-Sarnak

- On peut essayer d'aller plus loin et mesurer la "taille" de $\mathcal{P}_{4;3,1}$.

**Théorème. (Rubinstein-Sarnak, 1994)**

Supposons GRH et LI pour la fonction $L(s,\chi_4)$. Alors la **densité logarithmique**

$$\delta(\mathcal{P}_{4;3,1}) = \lim_{X\to+\infty} \frac{1}{\ln X}\int_2^X \mathbf{1}_{\mathcal{P}_{4;3,1}}(t)\frac{\mathrm{d}t}{t}$$

existe et $\delta(\mathcal{P}_{4;3,1}) \approx 0,9959\dots$

- Autrement dit, "$99,59\%$ du temps" il y a plus de nombres premiers congrus à 3 mod 4 que congrus à 1 mod 4.

# Rubinstein-Sarnak

- On peut essayer d'aller plus loin et mesurer la "taille" de $\mathcal{P}_{4;3,1}$.

**Théorème. (Rubinstein-Sarnak, 1994)**

Supposons GRH et LI pour la fonction $L(s, \chi_4)$. Alors la **densité logarithmique**

$$\delta(\mathcal{P}_{4;3,1}) = \lim_{X \to +\infty} \frac{1}{\ln X} \int_2^X \mathbf{1}_{\mathcal{P}_{4;3,1}}(t) \frac{\mathrm{d}t}{t}$$

existe et $\delta(\mathcal{P}_{4;3,1}) \approx 0,9959\ldots$

- Autrement dit, "$99,59\%$ du temps" il y a plus de nombres premiers congrus à 3 mod 4 que congrus à 1 mod 4.

- LI est une hypothèse d'indépendance linéaire sur $\mathbb{Q}$ plausible pour les zéros de $L(s, \chi_4) = \sum_{n=1, n \text{ impair}}^{+\infty} \frac{(-1)^{\frac{n-1}{2}}}{n^s}$.

# Idées de preuve

- Des méthodes standards montrent que

$$\frac{\pi(\mathrm{e}^t;4,3)-\pi(\mathrm{e}^t;4,1)}{\mathrm{e}^{t/2}/t} = 2 + 2\sum_{j=1}^{+\infty} \frac{\mathrm{e}^{i\gamma_j t}}{\frac{1}{2}+i\gamma_j} + O\left(\frac{1}{t}\right),$$

où l'on a listé les zéros $\frac{1}{2}+i\gamma_1, \frac{1}{2}+i\gamma_2, \ldots$ de $L(s,\chi_4)$.

# Idées de preuve

- Des méthodes standards montrent que

$$\frac{\pi(\mathrm{e}^t;4,3)-\pi(\mathrm{e}^t;4,1)}{\mathrm{e}^{t/2}/t} = 2 + 2\sum_{j=1}^{+\infty} \frac{\mathrm{e}^{i\gamma_j t}}{\frac{1}{2}+i\gamma_j} + O\left(\frac{1}{t}\right),$$

où l'on a listé les zéros $\frac{1}{2}+i\gamma_1, \frac{1}{2}+i\gamma_2, \dots$ de $L(s,\chi_4)$.

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

# Idées de preuve

- Des méthodes standards montrent que

$$\frac{\pi(\mathrm{e}^t;4,3)-\pi(\mathrm{e}^t;4,1)}{\mathrm{e}^{t/2}/t} = 2 + 2\sum_{j=1}^{+\infty} \frac{\mathrm{e}^{i\gamma_j t}}{\frac{1}{2}+i\gamma_j} + O\left(\frac{1}{t}\right),$$

  où l'on a listé les zéros $\frac{1}{2}+i\gamma_1, \frac{1}{2}+i\gamma_2, \ldots$ de $L(s,\chi_4)$.

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

- Ce sont des variables aléatoires centrées et on contrôle la variance de la somme, d'où des estimations sur

$$"\mathbb{P}(\pi(x;4,3)-\pi(x;4,1)>0)".$$

# Courses de nombres premiers

- Plus généralement, Rubinstein et Sarnak montrent (sous les bonnes hypothèses) l'existence de la densité logarithmique de

$$\mathcal{P}_{q;a_1,\ldots,a_r} = \{x \geq 2 \mid \pi(x;q,a_1) > \cdots > \pi(x;q,a_r)\}$$

pour $q \geq 2, a_1, \ldots, a_r \in \mathbb{Z}$ deux à deux distincts, premiers avec $q$. On parle de **course de nombres premiers**.

# Courses de nombres premiers

- Plus généralement, Rubinstein et Sarnak montrent (sous les bonnes hypothèses) l'existence de la densité logarithmique de

$$\mathcal{P}_{q;a_1,\ldots,a_r} = \{x \geq 2 \mid \pi(x;q,a_1) > \cdots > \pi(x;q,a_r)\}$$

  pour $q \geq 2, a_1, \ldots, a_r \in \mathbb{Z}$ deux à deux distincts, premiers avec $q$. On parle de **course de nombres premiers**.

- Dans une course à deux participants $a$ et $b$ mod $q$, il y a un biais en faveur de $a$ lorsque ce n'est pas un carré mod $q$ et $b$ en est un.

# Courses de nombres premiers

- Plus généralement, Rubinstein et Sarnak montrent (sous les bonnes hypothèses) l'existence de la densité logarithmique de

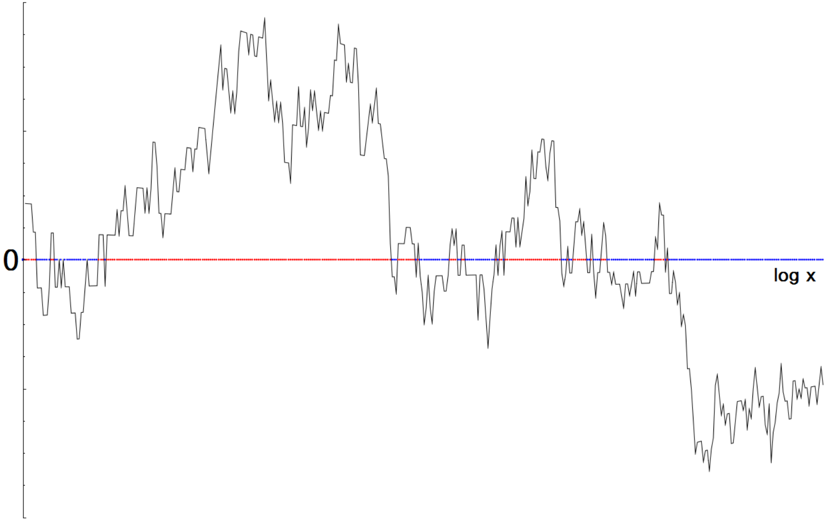
$$\mathcal{P}_{q;a_1,\ldots,a_r} = \{x \geq 2 \mid \pi(x;q,a_1) > \cdots > \pi(x;q,a_r)\}$$

  pour $q \geq 2, a_1, \ldots, a_r \in \mathbb{Z}$ deux à deux distincts, premiers avec $q$. On parle de **course de nombres premiers**.

- Dans une course à deux participants $a$ et $b$ mod $q$, il y a un biais en faveur de $a$ lorsque ce n'est pas un carré mod $q$ et $b$ en est un.

- Il y a aussi atténuation du biais lorsque $q \to +\infty$ :

$$\delta(\mathcal{P}_{q;a_1,\ldots,a_r}) \underset{q\to+\infty}{\to} \frac{1}{r!}.$$




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

Source : Daniel Fiorilli

# Quelques résultats récents

- On peut généraliser les questions de biais de Tchebychev dans beaucoup de directions, par exemple :

# Quelques résultats récents

- On peut généraliser les questions de biais de Tchebychev dans beaucoup de directions, par exemple :
  - Courses de nombres premiers avec $r(q) \underset{q \to +\infty}{\to} +\infty$ compétiteurs [Lamzouri, Lamzouri-Harper].

# Quelques résultats récents

- On peut généraliser les questions de biais de Tchebychev dans beaucoup de directions, par exemple :
  - Courses de nombres premiers avec $r(q) \underset{q\to+\infty}{\longrightarrow} +\infty$ compétiteurs [Lamzouri, Lamzouri-Harper]. Dépend de manière cruciale de la taille de $r(q)$ par rapport à $q$, seuil critique autour de $\ln q$.

# Quelques résultats récents

- On peut généraliser les questions de biais de Tchebychev dans beaucoup de directions, par exemple :
  - Courses de nombres premiers avec $r(q) \underset{q \to +\infty}{\to} +\infty$ compétiteurs [Lamzouri, Lamzouri-Harper]. Dépend de manière cruciale de la taille de $r(q)$ par rapport à $q$, seuil critique autour de $\ln q$.
  - Nombres premiers $\to$ polynômes irréductibles dans $\mathbb{F}_q[X]$ [Cha, Devin-Meng, B.-Devin-Keliher-Li].

# Quelques résultats récents

- On peut généraliser les questions de biais de Tchebychev dans beaucoup de directions, par exemple :
  - Courses de nombres premiers avec $r(q) \underset{q\to+\infty}{\to} +\infty$ compétiteurs [Lamzouri, Lamzouri-Harper]. Dépend de manière cruciale de la taille de $r(q)$ par rapport à $q$, seuil critique autour de $\ln q$.
  - Nombres premiers $\to$ polynômes irréductibles dans $\mathbb{F}_q[X]$ [Cha, Devin-Meng, B.-Devin-Keliher-Li]. L'hypothèse LI n'est pas toujours vérifiée, mais elle l'est "génériquement". Quand elle ne l'est pas, il peut y avoir des biais inattendus.

# Quelques résultats récents

- On peut généraliser les questions de biais de Tchebychev dans beaucoup de directions, par exemple :
    - Courses de nombres premiers avec $r(q) \underset{q \to +\infty}{\to} +\infty$ compétiteurs [Lamzouri, Lamzouri-Harper]. Dépend de manière cruciale de la taille de $r(q)$ par rapport à $q$, seuil critique autour de $\ln q$.
    - Nombres premiers $\to$ polynômes irréductibles dans $\mathbb{F}_q[X]$ [Cha, Devin-Meng, B.-Devin-Keliher-Li]. L'hypothèse LI n'est pas toujours vérifiée, mais elle l'est "génériquement". Quand elle ne l'est pas, il peut y avoir des biais inattendus.
    - Nombres premiers en progressions arithmétiques $\to$ nombres premiers vérifiant des "congruences supérieures" (par exemple, 2 est un cube mod $p$) [Ng, Fiorilli-Jouve, B., B.-Hayani].

# Quelques résultats récents

- On peut généraliser les questions de biais de Tchebychev dans beaucoup de directions, par exemple :
  - Courses de nombres premiers avec $r(q) \underset{q \to +\infty}{\to} +\infty$ compétiteurs [Lamzouri, Lamzouri-Harper]. Dépend de manière cruciale de la taille de $r(q)$ par rapport à $q$, seuil critique autour de $\ln q$.
  - Nombres premiers $\to$ polynômes irréductibles dans $\mathbb{F}_q[X]$ [Cha, Devin-Meng, B.-Devin-Keliher-Li]. L'hypothèse LI n'est pas toujours vérifiée, mais elle l'est "génériquement". Quand elle ne l'est pas, il peut y avoir des biais inattendus.
  - Nombres premiers en progressions arithmétiques $\to$ nombres premiers vérifiant des "congruences supérieures" (par exemple, 2 est un cube mod $p$) [Ng, Fiorilli-Jouve, B., B.-Hayani]. Le biais ne s'atténue pas forcément quand (l'analogue de) $q \to +\infty$, et la présence de zéro en $1/2$ peut apporter des biais inattendus.

# Un résultat très récent

- Le **nombre de Skewes** est la borne inférieure $x_S$ des $x \geq 2$ tels que $\pi(x) > \mathrm{li}(x) = \int_2^x \frac{\mathrm{d}t}{\ln t}$ (le "bon" équivalent dans le TNP).

# Un résultat très récent

- Le **nombre de Skewes** est la borne inférieure $x_S$ des $x \geq 2$ tels que $\pi(x) > \mathrm{li}(x) = \int_2^x \frac{\mathrm{d}t}{\ln t}$ (le "bon" équivalent dans le TNP). Son existence suit des travaux de Littlewood, et son étudiant Skewes fut le premier à en déterminer une borne :

$$x_S \leq 10^{10^{10^{963}}}.$$

# Un résultat très récent

- Le **nombre de Skewes** est la borne inférieure $x_S$ des $x \geq 2$ tels que $\pi(x) > \mathrm{li}(x) = \int_2^x \frac{\mathrm{d}t}{\ln t}$ (le "bon" équivalent dans le TNP). Son existence suit des travaux de Littlewood, et son étudiant Skewes fut le premier à en déterminer une borne :
$$x_S \leq 10^{10^{10^{963}}}.$$
Aujourd'hui on sait que $x_S$ est proche de $10^{316}$.

# Un résultat très récent

- Le **nombre de Skewes** est la borne inférieure $x_S$ des $x \geq 2$ tels que $\pi(x) > \mathrm{li}(x) = \int_2^x \frac{\mathrm{d}t}{\ln t}$ (le "bon" équivalent dans le TNP). Son existence suit des travaux de Littlewood, et son étudiant Skewes fut le premier à en déterminer une borne :
$$x_S \leq 10^{10^{10^{963}}}.$$
Aujourd'hui on sait que $x_S$ est proche de $10^{316}$.

- Si $q \geq 2$ on peut considérer un nombre de Skewes $x_q$ pour la course entre les nombres premiers qui sont des carrés modulo $q$ et ceux qui n'en sont pas, *i.e.* le premier changement de signe $x_q$ entre $\pi(x; q, \square) - \pi(x; q, \boxtimes)$.

# Un résultat très récent

- Le **nombre de Skewes** est la borne inférieure $x_S$ des $x \geq 2$ tels que $\pi(x) > \mathrm{li}(x) = \int_2^x \frac{\mathrm{d}t}{\ln t}$ (le "bon" équivalent dans le TNP). Son existence suit des travaux de Littlewood, et son étudiant Skewes fut le premier à en déterminer une borne :
$$x_S \leq 10^{10^{10^{963}}}.$$
Aujourd'hui on sait que $x_S$ est proche de $10^{316}$.

- Si $q \geq 2$ on peut considérer un nombre de Skewes $x_q$ pour la course entre les nombres premiers qui sont des carrés modulo $q$ et ceux qui n'en sont pas, *i.e.* le premier changement de signe $x_q$ entre $\pi(x; q, \square) - \pi(x; q, \boxtimes)$.

**Théorème. (B.-Hayani-Untrau, 2025)**

En supposant GRH et une hypothèse convenable d'indépendance linéaire, il existe une constante $C > 0$ telle que $x_q \leq e^{e^{e^{Cq}}}$.

# Un résultat très récent

- Le **nombre de Skewes** est la borne inférieure $x_S$ des $x \geq 2$ tels que $\pi(x) > \mathrm{li}(x) = \int_2^x \frac{\mathrm{d}t}{\ln t}$ (le "bon" équivalent dans le TNP). Son existence suit des travaux de Littlewood, et son étudiant Skewes fut le premier à en déterminer une borne :
$$x_S \leq 10^{10^{10^{963}}}.$$
Aujourd'hui on sait que $x_S$ est proche de $10^{316}$.

- Si $q \geq 2$ on peut considérer un nombre de Skewes $x_q$ pour la course entre les nombres premiers qui sont des carrés modulo $q$ et ceux qui n'en sont pas, *i.e.* le premier changement de signe $x_q$ entre $\pi(x; q, \square) - \pi(x; q, \boxtimes)$.

**Théorème. (B.-Hayani-Untrau, 2025)**

En supposant GRH et une hypothèse convenable d'indépendance linéaire, il existe une constante $C > 0$ telle que $x_q \leq e^{e^{e^{Cq}}}$.

- Utilise les techniques précédentes et des outils provenant des probabilités transport optimal (distances de Wasserstein, inégalité de Bobkov-Ledoux, inégalités de grandes déviations, *etc.*).

Merci de votre attention !