La théorie analytique des nombres, ou comment le continu permet d’étudier le discret

Alexandre Bailleul

ENS Paris-Saclay

13 novembre 2024

Sommaire

- 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 $xyz \neq 0$?

- 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 $m = \binom{n}{k}$?

- 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**.

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.

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.
- On peut extraire de la preuve d'Euclide que $p_n = O\left(2^{2^n}\right)$

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.
- On peut extraire de la preuve d'Euclide que $p_n = O\left(2^{2^n}\right)$ (très mauvais...).

Euler

- En 1748, Euler pose
$$P(x) = \prod_{p \leq x} \frac{1}{1 - \frac{1}{p}}.$$

Euler

- En 1748, Euler pose
$$P(x) = \prod_{p \leq x} \frac{1}{1 - \frac{1}{p}}.$$

- Alors par produit de Cauchy on a
$$P(x) = \prod_{p \leq x} \sum_{k=0}^{+\infty} \frac{1}{p^k}$$

Euler

- En 1748, Euler pose

$$P(x) = \prod_{p \leq x} \frac{1}{1 - \frac{1}{p}}.$$

- Alors par produit de Cauchy on a

$$P(x) = \prod_{p \leq x} \sum_{k=0}^{+\infty} \frac{1}{p^k} = \sum_{\substack{n \geq 1 \\ p \mid n \Rightarrow p \leq x}} \frac{1}{n}$$

Euler

- En 1748, Euler pose
$$P(x) = \prod_{p \leq x} \frac{1}{1 - \frac{1}{p}}.$$

- Alors par produit de Cauchy on a
$$P(x) = \prod_{p \leq x} \sum_{k=0}^{+\infty} \frac{1}{p^k} = \sum_{\substack{n \geq 1 \\ p \mid n \Rightarrow p \leq x}} \frac{1}{n} \geq \sum_{1 \leq n \leq x} \frac{1}{n}$$

Euler

- En 1748, Euler pose

$$P(x) = \prod_{p \leq x} \frac{1}{1 - \frac{1}{p}}.$$

- Alors par produit de Cauchy on a

$$P(x) = \prod_{p \leq x} \sum_{k=0}^{+\infty} \frac{1}{p^k} = \sum_{\substack{n \geq 1 \\ p \mid n \Rightarrow p \leq x}} \frac{1}{n} \geq \sum_{1 \leq n \leq x} \frac{1}{n} \geq \ln(x).$$

Euler

- En 1748, Euler pose
$$P(x) = \prod_{p \leq x} \frac{1}{1 - \frac{1}{p}}.$$

- Alors par produit de Cauchy on a
$$P(x) = \prod_{p \leq x} \sum_{k=0}^{+\infty} \frac{1}{p^k} = \sum_{\substack{n \geq 1 \\ p \mid n \Rightarrow p \leq x}} \frac{1}{n} \geq \sum_{1 \leq n \leq x} \frac{1}{n} \geq \ln(x).$$

- Mais on a aussi
$$\ln(P(x)) = \sum_{p \leq x} - \ln\left(1 - \frac{1}{p}\right)$$

Euler

- En 1748, Euler pose
$$P(x) = \prod_{p \leq x} \frac{1}{1 - \frac{1}{p}}.$$

- Alors par produit de Cauchy on a
$$P(x) = \prod_{p \leq x} \sum_{k=0}^{+\infty} \frac{1}{p^k} = \sum_{\substack{n \geq 1 \\ p \mid n \Rightarrow p \leq x}} \frac{1}{n} \geq \sum_{1 \leq n \leq x} \frac{1}{n} \geq \ln(x).$$

- Mais on a aussi
$$\ln(P(x)) = \sum_{p \leq x} - \ln\left(1 - \frac{1}{p}\right) = \sum_{p \leq x} \frac{1}{p} + \sum_{\substack{p \leq x \\ k \geq 2}} \frac{1}{kp^k}$$

Euler

- En 1748, Euler pose
$$P(x) = \prod_{p \leq x} \frac{1}{1 - \frac{1}{p}}.$$

- Alors par produit de Cauchy on a
$$P(x) = \prod_{p \leq x} \sum_{k=0}^{+\infty} \frac{1}{p^k} = \sum_{\substack{n \geq 1 \\ p \mid n \Rightarrow p \leq x}} \frac{1}{n} \geq \sum_{1 \leq n \leq x} \frac{1}{n} \geq \ln(x).$$

- Mais on a aussi
$$\ln(P(x)) = \sum_{p \leq x} - \ln\left(1 - \frac{1}{p}\right) = \sum_{p \leq x} \frac{1}{p} + \sum_{\substack{p \leq x \\ k \geq 2}} \frac{1}{kp^k} = \sum_{p \leq x} \frac{1}{p} + O(1).$$

Euler

- Conclusion :

$$\sum_{p \leq x} \frac{1}{p} \geq \ln \ln(x) + O(1).$$

Euler

- Conclusion :
$$\sum_{p \leq x} \frac{1}{p} \geq \ln \ln(x) + O(1).$$

- La série des inverses des nombres premiers diverge (très lentement)

Euler

- Conclusion :
$$\sum_{p \leq x} \frac{1}{p} \geq \ln \ln(x) + O(1).$$

- La série des inverses des nombres premiers diverge (très lentement), il y a donc une infinité de nombres premiers !

Euler

- Conclusion :
$$\sum_{p \leq x} \frac{1}{p} \geq \ln \ln(x) + O(1).$$

- La série des inverses des nombres premiers diverge (très lentement), il y a donc une infinité de nombres premiers !

- **On peut l'expliquer par le fait que** $\sum_{n} \frac{1}{n}$ **diverge.**

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 $4n+3$:
  $N = 4p_1 \times \cdots \times p_r + 3$ est congru à 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 $4n+3$:
  $N = 4p_1 \times \cdots \times p_r + 3$ est congru à 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 $4n + 3$:
  $N = 4p_1 \times \cdots \times p_r + 3$ est congru à 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 $4n+3$:
  $N = 4p_1 \times \cdots \times p_r + 3$ est congru à 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 $4n+3$:
  $N = 4p_1 \times \cdots \times p_r + 3$ est congru à 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 $4n + 3$:
  $N = 4p_1 \times \cdots \times p_r + 3$ est congru à 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 $(\mathbb{Z}/p\mathbb{Z})^\times$).

- Est-ce qu'il existe une infinité de nombres premiers de la forme $10n + 3$ (*i.e.* avec pour chiffre des unités 3) ?

Compliquons la question

- Il existe une infinité de nombres premiers de la forme $4n+3$:
$N = 4p_1 \times \cdots \times p_r + 3$ est congru à 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 $(\mathbb{Z}/p\mathbb{Z})^\times$).
- Est-ce qu'il existe une infinité de nombres premiers de la forme $10n+3$ (*i.e.* avec pour chiffre des unités 3) ? Il semble compliqué d'en trouver une démonstration élémentaire...

Dirichlet

Théorème. (Dirichlet, 1837)

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

Dirichlet

Théorème. (Dirichlet, 1837)

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

- Conséquences :

Dirichlet

Théorème. (Dirichlet, 1837)

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

- Conséquences :
  - Une infinité de nombres premiers avec pour chiffre des unités 1, ou encore 3, ou 7, ou 9.

Dirichlet

Théorème. (Dirichlet, 1837)

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

- Conséquences :
  - Une infinité de nombres premiers avec pour chiffre des unités 1, ou encore 3, ou 7, ou 9.
  - Si n n'est pas de la forme $4^a(8k + 7)$ alors il existe $x, y, z \in \mathbb{N}$ tels que $n = x^2 + y^2 + z^2$ (théorème des trois carrés).

Dirichlet

Théorème. (Dirichlet, 1837)

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

- Conséquences :
  - Une infinité de nombres premiers avec pour chiffre des unités 1, ou encore 3, ou 7, ou 9.
  - Si n n'est pas de la forme $4^a(8k + 7)$ alors il existe $x, y, z \in \mathbb{N}$ tels que $n = x^2 + y^2 + z^2$ (théorème des trois carrés).
  - Si n est un carré modulo tout nombre premier alors n est un carré d'entier ("principe local-global").

Démonstration dans un cas simple

- Montrons le résultat à la manière de Dirichlet (inspiré d'Euler) pour $q = 4$ et $a = 1$.

Démonstration dans un cas simple

- Montrons le résultat à la manière de Dirichlet (inspiré d'Euler) pour $q = 4$ et $a = 1$. On considère les produits

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

et

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

pour $s > 1$.

Démonstration dans un cas simple

- Montrons le résultat à la manière de Dirichlet (inspiré d'Euler) pour $q = 4$ et $a = 1$. On considère les produits
$$L_1(s) = \prod_{p \neq 2} \frac{1}{1 - \frac{1}{p^s}}$$
et
$$L_2(s) = \prod_{p \neq 2} \frac{1}{1 - \frac{(-1)^{\frac{p-1}{2}}}{p^s}}$$
pour $s > 1$.

- Alors comme avant
$$\ln L_1(s) = \sum_{p \neq 2} \frac{1}{p^s} + O(1)$$
et
$$\ln L_2(s) = \sum_{p \neq 2} \frac{(-1)^{\frac{p-1}{2}}}{p^s} + O(1).$$

Démonstration dans un cas simple

- 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 dans un cas simple

- 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

$$L_1(s) = \sum_{n \text{ impair}} \frac{1}{n^s}$$

et

$$L_2(s) = \sum_{n \geq 1} \frac{(-1)^n}{(2n+1)^s}.$$

Démonstration dans un cas simple

- 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

$$L_1(s) = \sum_{n \text{ impair}} \frac{1}{n^s}$$

et

$$L_2(s) = \sum_{n \geq 1} \frac{(-1)^n}{(2n+1)^s}.$$

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

Démonstration dans un cas simple

- Conclusion : $\displaystyle\sum_{p\equiv 1 \bmod 4} \frac{1}{p^s} \underset{s\to 1^+}{\longrightarrow} +\infty$ et il existe une infinité de nombres premiers de la forme $4n+1$.

Démonstration dans un cas simple

- Conclusion : $\displaystyle\sum_{p\equiv 1 \bmod 4} \frac{1}{p^s} \underset{s\to 1^+}{\longrightarrow} +\infty$ 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 dans un cas simple

- Conclusion : $\displaystyle\sum_{p\equiv 1 \bmod 4} \frac{1}{p^s} \underset{s\to 1^+}{\longrightarrow} +\infty$ 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 $L_2(1) = \frac{\pi}{4} \neq 0$!**
- Plus généralement, chaque cas traité par Dirichlet repose sur le fait que $L(1) \neq 0$ pour certaines fonctions L, et c'est la partie la plus difficile de la démonstration.

Démonstration dans un cas simple

- Conclusion : $\displaystyle\sum_{p\equiv 1 \bmod 4} \frac{1}{p^s} \underset{s\to 1^+}{\longrightarrow} +\infty$ 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 $L_2(1) = \frac{\pi}{4} \neq 0$!**

- Plus généralement, chaque cas traité par Dirichlet repose sur le fait que $L(1) \neq 0$ pour certaines fonctions L, et c'est la partie la plus difficile de la démonstration.

- **On ne sait pas se passer d'analyse pour démontrer ce résultat !**

Sommaire

Une nouvelle question

- Il y a une infinité de nombres premiers (y compris dans des progressions arithmétiques).

Une nouvelle question

- Il y a une infinité de nombres premiers (y compris dans des progressions arithmétiques).
- Question : Peut-on dire combien il y en a en-dessous d'une borne x grande ?

Une nouvelle question

- Il y a une infinité de nombres premiers (y compris dans des progressions arithmétiques).
- Question : Peut-on dire combien il y en a en-dessous d'une borne x grande ?

Conjecture (Gauss, 1793).

Si $\pi(x) = \#\{p \leq x\}$, alors

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

Quelques observations

- Cela donne $p_n \underset{n\to+\infty}{\sim} n \ln n$.

Quelques observations

- Cela donne $p_n \underset{n\to+\infty}{\sim} n\ln n$.
- Cela implique que $\frac{\pi(x)}{x} \underset{x\to+\infty}{\longrightarrow} 0$: les nombres premiers se raréfient quand x devient grand (théorème de Legendre, 1808).

Quelques observations

- Cela donne $p_n \underset{n\to+\infty}{\sim} n \ln n$.
- Cela implique que $\frac{\pi(x)}{x} \underset{x\to+\infty}{\longrightarrow} 0$: les nombres premiers se raréfient quand x devient grand (théorème de Legendre, 1808). Autrement dit, ils ont une densité nulle dans les entiers.

Quelques observations

- Cela donne $p_n \underset{n \to +\infty}{\sim} n \ln n$.
- Cela implique que $\frac{\pi(x)}{x} \underset{x \to +\infty}{\longrightarrow} 0$: les nombres premiers se raréfient quand x devient grand (théorème de Legendre, 1808). Autrement dit, ils ont une densité nulle dans les entiers.
- C'est cohérent avec le $\displaystyle\sum_{p \leq x} \frac{1}{p} \geq \ln \ln(x) + O(1)$ d'Euler (on a même un équivalent).

Quelques observations

- Cela donne $p_n \underset{n\to+\infty}{\sim} n\ln n$.
- Cela implique que $\frac{\pi(x)}{x} \underset{x\to+\infty}{\longrightarrow} 0$: les nombres premiers se raréfient quand x devient grand (théorème de Legendre, 1808). Autrement dit, ils ont une densité nulle dans les entiers.
- C'est cohérent avec le $\displaystyle\sum_{p\leq x}\frac{1}{p} \geq \ln\ln(x) + O(1)$ d'Euler (on a même un équivalent).
- Beaucoup de conséquences de statistique arithmétique

Quelques observations

- Cela donne $p_n \underset{n\to+\infty}{\sim} n\ln n$.
- Cela implique que $\frac{\pi(x)}{x} \underset{x\to+\infty}{\longrightarrow} 0$: les nombres premiers se raréfient quand x devient grand (théorème de Legendre, 1808). Autrement dit, ils ont une densité nulle dans les entiers.
- C'est cohérent avec le $\displaystyle\sum_{p\leq x}\frac{1}{p} \geq \ln\ln(x) + O(1)$ d'Euler (on a même un équivalent).
- Beaucoup de conséquences de statistique arithmétique, par exemple si $\omega(n)$ désigne le nombre de facteurs premiers de n, alors

$$\frac{1}{x}\sum_{n\leq x}\omega(n)$$

Quelques observations

- Cela donne $p_n \underset{n\to+\infty}{\sim} n\ln n$.
- Cela implique que $\frac{\pi(x)}{x} \underset{x\to+\infty}{\longrightarrow} 0$: les nombres premiers se raréfient quand x devient grand (théorème de Legendre, 1808). Autrement dit, ils ont une densité nulle dans les entiers.
- C'est cohérent avec le $\displaystyle\sum_{p\leq x}\frac{1}{p} \geq \ln\ln(x) + O(1)$ d'Euler (on a même un équivalent).
- Beaucoup de conséquences de statistique arithmétique, par exemple si $\omega(n)$ désigne le nombre de facteurs premiers de n, alors

$$\frac{1}{x}\sum_{n\leq x}\omega(n) = \frac{1}{x}\sum_{n\leq x}\sum_{p|n} 1$$

Quelques observations

- Cela donne $p_n \underset{n\to+\infty}{\sim} n\ln n$.
- Cela implique que $\frac{\pi(x)}{x} \underset{x\to+\infty}{\longrightarrow} 0$: les nombres premiers se raréfient quand x devient grand (théorème de Legendre, 1808). Autrement dit, ils ont une densité nulle dans les entiers.
- C'est cohérent avec le $\displaystyle\sum_{p\leq x}\frac{1}{p} \geq \ln\ln(x) + O(1)$ d'Euler (on a même un équivalent).
- Beaucoup de conséquences de statistique arithmétique, par exemple si $\omega(n)$ désigne le nombre de facteurs premiers de n, alors

$$\frac{1}{x}\sum_{n\leq x}\omega(n) = \frac{1}{x}\sum_{n\leq x}\sum_{p\mid n} 1 = \frac{1}{x}\sum_{p\leq x}\sum_{\substack{n\leq x\\ p\mid n}} 1$$

Quelques observations

- Cela donne $p_n \underset{n \to +\infty}{\sim} n \ln n$.
- Cela implique que $\frac{\pi(x)}{x} \underset{x \to +\infty}{\longrightarrow} 0$: les nombres premiers se raréfient quand x devient grand (théorème de Legendre, 1808). Autrement dit, ils ont une densité nulle dans les entiers.
- C'est cohérent avec le $\displaystyle\sum_{p \leq x} \frac{1}{p} \geq \ln \ln(x) + O(1)$ d'Euler (on a même un équivalent).
- Beaucoup de conséquences de statistique arithmétique, par exemple si $\omega(n)$ désigne le nombre de facteurs premiers de n, alors

$$\frac{1}{x} \sum_{n \leq x} \omega(n) = \frac{1}{x} \sum_{n \leq x} \sum_{p \mid n} 1 = \frac{1}{x} \sum_{p \leq x} \sum_{\substack{n \leq x \\ p \mid n}} 1 = \frac{1}{x} \sum_{p \leq x} \left\lfloor \frac{x}{p} \right\rfloor$$

Quelques observations

- Cela donne $p_n \underset{n\to+\infty}{\sim} n\ln n$.

- Cela implique que $\frac{\pi(x)}{x} \underset{x\to+\infty}{\longrightarrow} 0$: les nombres premiers se raréfient quand x devient grand (théorème de Legendre, 1808). Autrement dit, ils ont une densité nulle dans les entiers.

- C'est cohérent avec le $\displaystyle\sum_{p\leq x}\frac{1}{p} \geq \ln\ln(x) + O(1)$ d'Euler (on a même un équivalent).

- Beaucoup de conséquences de statistique arithmétique, par exemple si $\omega(n)$ désigne le nombre de facteurs premiers de n, alors

$$\frac{1}{x}\sum_{n\leq x}\omega(n) = \frac{1}{x}\sum_{n\leq x}\sum_{p|n}1 = \frac{1}{x}\sum_{p\leq x}\sum_{\substack{n\leq x\\ p|n}}1 = \frac{1}{x}\sum_{p\leq x}\left\lfloor\frac{x}{p}\right\rfloor$$

$$= \sum_{p\leq x}\frac{1}{p} + O(1)$$

Quelques observations

- Cela donne $p_n \underset{n \to +\infty}{\sim} n \ln n$.
- Cela implique que $\frac{\pi(x)}{x} \underset{x \to +\infty}{\longrightarrow} 0$: les nombres premiers se raréfient quand x devient grand (théorème de Legendre, 1808). Autrement dit, ils ont une densité nulle dans les entiers.
- C'est cohérent avec le $\displaystyle\sum_{p \leq x} \frac{1}{p} \geq \ln\ln(x) + O(1)$ d'Euler (on a même un équivalent).
- Beaucoup de conséquences de statistique arithmétique, par exemple si $\omega(n)$ désigne le nombre de facteurs premiers de n, alors

$$\frac{1}{x} \sum_{n \leq x} \omega(n) = \frac{1}{x} \sum_{n \leq x} \sum_{p \mid n} 1 = \frac{1}{x} \sum_{p \leq x} \sum_{\substack{n \leq x \\ p \mid n}} 1 = \frac{1}{x} \sum_{p \leq x} \left\lfloor \frac{x}{p} \right\rfloor$$

$$= \sum_{p \leq x} \frac{1}{p} + O(1) = \ln\ln(x) + O(1).$$

Quelques observations

- Cela donne $p_n \underset{n\to+\infty}{\sim} n\ln n$.

- Cela implique que $\frac{\pi(x)}{x} \underset{x\to+\infty}{\to} 0$: les nombres premiers se raréfient quand x devient grand (théorème de Legendre, 1808). Autrement dit, ils ont une densité nulle dans les entiers.

- C'est cohérent avec le $\displaystyle\sum_{p\leq x}\frac{1}{p} \geq \ln\ln(x) + O(1)$ d'Euler (on a même un équivalent).

- Beaucoup de conséquences de statistique arithmétique, par exemple si $\omega(n)$ désigne le nombre de facteurs premiers de n, alors

$$\frac{1}{x}\sum_{n\leq x}\omega(n) = \frac{1}{x}\sum_{n\leq x}\sum_{p\mid n} 1 = \frac{1}{x}\sum_{p\leq x}\sum_{\substack{n\leq x\\ p\mid n}} 1 = \frac{1}{x}\sum_{p\leq x}\left\lfloor\frac{x}{p}\right\rfloor$$

$$= \sum_{p\leq x}\frac{1}{p} + O(1) = \ln\ln(x) + O(1).$$

("Un entier inférieur à x a en moyenne $\ln\ln(x)$ facteurs premiers")

Idées de démonstration

- L'équivalent $\pi(x) \underset{x\to+\infty}{\sim} \frac{x}{\ln x}$ est appelé le **théorème des nombres premiers** (ou TNP), démontré par Hadamard et de la Vallée-Poussin en 1896).

Idées de démonstration

- L'équivalent $\pi(x) \underset{x \to +\infty}{\sim} \frac{x}{\ln x}$ est appelé le **théorème des nombres premiers** (ou TNP), démontré par Hadamard et de la Vallée-Poussin en 1896).

- La démonstration repose sur l'étude de la fonction

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

Idées de démonstration

- L'équivalent $\pi(x) \underset{x \to +\infty}{\sim} \frac{x}{\ln x}$ est appelé le **théorème des nombres premiers** (ou TNP), démontré par Hadamard et de la Vallée-Poussin en 1896).

- La démonstration repose sur l'étude de la fonction

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

- L'apport de Riemann par rapport à Euler est de considérer s comme variable **complexe** et d'utiliser l'**analyse complexe**.

Idées de démonstration

- On a vu que

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

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

Idées de démonstration

- On a vu que
$$\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}}$$
pour $\mathfrak{Re}(s) > 1$.

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

Idées de démonstration

- On a vu que
$$\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}}$$
pour $\mathfrak{Re}(s) > 1$.

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

- La clé pour démontrer le TNP est de localiser les **zéros de** ζ.

Quel rapport avec les zéros ?

- Pour des raisons techniques, posons

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

Quel rapport avec les zéros ?

- Pour des raisons techniques, posons

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

- On montre que

$$\pi(x) = \sum_{p \leq x} 1$$

Quel rapport avec les zéros ?

- Pour des raisons techniques, posons

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

- On montre que

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

Quel rapport avec les zéros ?

- Pour des raisons techniques, posons

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

- On montre que

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

- 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 ζ.

- 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 ζ.

- 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 ζ.

- 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 ζ.

- 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**).

Sommaire

Un dernier exemple

- Est-ce que tout entier peut s'écrire comme une **somme** de carrés ?

Un dernier exemple

- Est-ce que tout entier peut s'écrire comme une **somme** de carrés ?
  - $n = a^2 + b^2$ si et seulement si pour tout $p \equiv 3 \bmod 4$ divisant n, $v_p(n)$ est pair (Fermat, 1640).

Un dernier exemple

- Est-ce que tout entier peut s'écrire comme une **somme** de carrés ?
  - $n = a^2 + b^2$ si et seulement si pour tout $p \equiv 3 \bmod 4$ divisant n, $v_p(n)$ est pair (Fermat, 1640).
  - $n = a^2 + b^2 + c^2$ si et seulement si n n'est pas de la forme $4^k(8n + 7)$ (Legendre, 1801).

Un dernier exemple

- Est-ce que tout entier peut s'écrire comme une **somme** de carrés ?
  - $n = a^2 + b^2$ si et seulement si pour tout $p \equiv 3 \bmod 4$ divisant n, $v_p(n)$ est pair (Fermat, 1640).
  - $n = a^2 + b^2 + c^2$ si et seulement si n n'est pas de la forme $4^k(8n+7)$ (Legendre, 1801).
  - Tout n est somme de quatre carrés (Lagrange, 1770).

Un dernier exemple

- Est-ce que tout entier peut s'écrire comme une **somme** de carrés ?
  - $n = a^2 + b^2$ si et seulement si pour tout $p \equiv 3 \bmod 4$ divisant n, $v_p(n)$ est pair (Fermat, 1640).
  - $n = a^2 + b^2 + c^2$ si et seulement si n n'est pas de la forme $4^k(8n+7)$ (Legendre, 1801).
  - Tout n est somme de quatre carrés (Lagrange, 1770).
- Conclusion : le nombre minimal de carrés qui permet d'écrire tout nombre entier est 4.

Un dernier exemple

- Est-ce que tout entier peut s'écrire comme une **somme** de carrés ?
  - $n = a^2 + b^2$ si et seulement si pour tout $p \equiv 3 \bmod 4$ divisant n, $v_p(n)$ est pair (Fermat, 1640).
  - $n = a^2 + b^2 + c^2$ si et seulement si n n'est pas de la forme $4^k(8n+7)$ (Legendre, 1801).
  - Tout n est somme de quatre carrés (Lagrange, 1770).
- Conclusion : le nombre minimal de carrés qui permet d'écrire tout nombre entier est 4.
- Waring pose la question pour toute puissance plus grande que 2.

- Hilbert montre en 1909, algébriquement et de manière non effective, que pour tout $k \geq 2$, il existe $G(k) \in \mathbb{N}^*$ tel que tout entier suffisamment grand est somme de $G(k)$ puissances k-ièmes (sans donner de borne sur $G(k)$).

- Hilbert montre en 1909, algébriquement et de manière non effective, que pour tout $k \geq 2$, il existe $G(k) \in \mathbb{N}^*$ tel que tout entier suffisamment grand est somme de $G(k)$ puissances k-ièmes (sans donner de borne sur $G(k)$).

- On sait que $G(2) = 4$, et $G(4) = 16$ (Davenport) mais aucune autre valeur n'est connue. Comment estimer $G(k)$ en général ?

La méthode du cercle de Hardy-Littlewood

- Pour tout $n \in \mathbb{N}^*$, notons $r_{k,\ell}(n) = \#\{(a_1, \ldots, a_\ell) \in \mathbb{N}^\ell \mid a_1^k + \cdots + a_l^k = n\}$. On veut montrer que pour ℓ assez grand et n suffisamment grand en fonction de ℓ et k, $r_{k,\ell}(n) > 0$.

La méthode du cercle de Hardy-Littlewood

- Pour tout $n \in \mathbb{N}^*$, notons $r_{k,\ell}(n) = \#\{(a_1, \dots, a_\ell) \in \mathbb{N}^\ell \mid a_1^k + \cdots + a_l^k = n\}$. On veut montrer que pour ℓ assez grand et n suffisamment grand en fonction de ℓ et k, $r_{k,\ell}(n) > 0$.

- On remarque que $r_{k,\ell}(n)$ est le coefficient devant z^n de

$$F_{k,\ell}(z) = \left(\sum_{a \leq n^{1/k}} z^{a^k} \right)^\ell = \sum_{j=0}^{n} r_{k,\ell}(j) z^j + z^{n+1} P(z).$$

La méthode du cercle de Hardy-Littlewood

- Pour tout $n \in \mathbb{N}^*$, notons $r_{k,\ell}(n) = \#\{(a_1, \ldots, a_\ell) \in \mathbb{N}^\ell \mid a_1^k + \cdots + a_l^k = n\}$. On veut montrer que pour ℓ assez grand et n suffisamment grand en fonction de ℓ et k, $r_{k,\ell}(n) > 0$.

- On remarque que $r_{k,\ell}(n)$ est le coefficient devant z^n de

$$F_{k,\ell}(z) = \left(\sum_{a \leq n^{1/k}} z^{a^k} \right)^\ell = \sum_{j=0}^{n} r_{k,\ell}(j) z^j + z^{n+1} P(z).$$

- On pourrait extraire ce coefficient par la formule

$$r_{k,\ell}(n) = \frac{F_{k,\ell}^{(n)}(0)}{n!},$$

mais il semble difficile de contrôler les dérivées de $F_{k,\ell}$.

La méthode du cercle de Hardy-Littlewood

- À la place, on utilise l'égalité

$$r_{k,\ell}(n) = \int_0^1 F_{k,\ell}(e^{2i\pi x})e^{-2i\pi nx}\,\mathrm{d}x,$$

en vertu de la relation d'orthogonalité

$$\int_0^1 e^{2i\pi kx}\,\mathrm{d}x = \begin{cases} 1 \text{ si } k = 0 \\ 0 \text{ sinon.} \end{cases}$$

La méthode du cercle de Hardy-Littlewood

- À la place, on utilise l'égalité

$$r_{k,\ell}(n) = \int_0^1 F_{k,\ell}(e^{2i\pi x})e^{-2i\pi nx}\,\mathrm{d}x,$$

en vertu de la relation d'orthogonalité

$$\int_0^1 e^{2i\pi kx}\,\mathrm{d}x = \begin{cases} 1 \text{ si } k = 0 \\ 0 \text{ sinon.} \end{cases}$$

- Pour montrer que

$$\int_0^1 F_{k,l}(e^{2i\pi x})e^{-2i\pi nx}\,\mathrm{d}x > 0,$$

on découpe $[0, 1]$ en des "arcs majeurs", où $F_{k,l}(x)$ est grand en module, et en des "arcs mineurs" où l'intégrale sur ces arcs est négligeable par rapport à la contribution des arcs majeurs.

- Imaginons que $k = 1$. Alors (pour $x \notin \mathbb{Z}$),

$$|F_{k,\ell}(e^{2i\pi x})| = \left| \sum_{a \leq n^{1/k}} e^{2i\pi a x} \right|^{\ell} = \left| \frac{e^{2i\pi(n^{1/k}+1)x} - 1}{e^{2i\pi x} - 1} \right|^{\ell} = \frac{\left|\sin\left((n^{1/k}+1)\pi x\right)\right|^{\ell}}{\left|\sin(\pi x)\right|^{\ell}}.$$

- Imaginons que $k = 1$. Alors (pour $x \notin \mathbb{Z}$),

$$|F_{k,\ell}(e^{2i\pi x})| = \left| \sum_{a \leq n^{1/k}} e^{2i\pi a x} \right|^{\ell} = \left| \frac{e^{2i\pi(n^{1/k}+1)x} - 1}{e^{2i\pi x} - 1} \right|^{\ell} = \frac{\left|\sin\left((n^{1/k}+1)\pi x\right)\right|^{\ell}}{\left|\sin(\pi x)\right|^{\ell}}.$$

- Des estimations (beaucoup plus difficiles) de sommes d'exponentielles permettent de généraliser à tout $k \geq 1$. De manière générale, la taille de $|F_{k,\ell}(e^{2i\pi x})|$ est contrôlée par la proximité de x aux rationnels.

- Imaginons que $k = 1$. Alors (pour $x \notin \mathbb{Z}$),

$$|F_{k,\ell}(e^{2i\pi x})| = \left| \sum_{a \leq n^{1/k}} e^{2i\pi a x} \right|^{\ell} = \left| \frac{e^{2i\pi (n^{1/k}+1)x} - 1}{e^{2i\pi x} - 1} \right|^{\ell} = \frac{\left| \sin\left((n^{1/k}+1)\pi x \right) \right|^{\ell}}{|\sin(\pi x)|^{\ell}}.$$

- Des estimations (beaucoup plus difficiles) de sommes d'exponentielles permettent de généraliser à tout $k \geq 1$. De manière générale, la taille de $|F_{k,\ell}(e^{2i\pi x})|$ est contrôlée par la proximité de x aux rationnels.

- Les arcs majeurs $\mathfrak{M}$ sont alors choisis comment étant les x proches de rationnels $\frac{p}{q}$ avec q "petit" (en fonction de k et ℓ), et les arcs mineurs sont $[0, 1] \setminus \mathfrak{M}$. (Il faut optimiser beaucoup de paramètres pour obtenir le résultat final...)

- Imaginons que $k = 1$. Alors (pour $x \notin \mathbb{Z}$),

$$|F_{k,\ell}(e^{2i\pi x})| = \left| \sum_{a \leq n^{1/k}} e^{2i\pi a x} \right|^{\ell} = \left| \frac{e^{2i\pi (n^{1/k}+1)x} - 1}{e^{2i\pi x} - 1} \right|^{\ell} = \frac{\left|\sin\left((n^{1/k}+1)\pi x\right)\right|^{\ell}}{|\sin(\pi x)|^{\ell}}.$$

- Des estimations (beaucoup plus difficiles) de sommes d'exponentielles permettent de généraliser à tout $k \geq 1$. De manière générale, la taille de $|F_{k,\ell}(e^{2i\pi x})|$ est contrôlée par la proximité de x aux rationnels.

- Les arcs majeurs $\mathfrak{M}$ sont alors choisis comment étant les x proches de rationnels $\frac{p}{q}$ avec q "petit" (en fonction de k et ℓ), et les arcs mineurs sont $[0,1] \setminus \mathfrak{M}$. (Il faut optimiser beaucoup de paramètres pour obtenir le résultat final...)

- Hardy et Littlewood parviennent alors à $G(k) = O(k2^k)$.

- Imaginons que $k = 1$. Alors (pour $x \notin \mathbb{Z}$),

$$|F_{k,\ell}(e^{2i\pi x})| = \left| \sum_{a \leq n^{1/k}} e^{2i\pi a x} \right|^{\ell} = \left| \frac{e^{2i\pi(n^{1/k}+1)x} - 1}{e^{2i\pi x} - 1} \right|^{\ell} = \frac{\left|\sin\left((n^{1/k}+1)\pi x\right)\right|^{\ell}}{\left|\sin\left(\pi x\right)\right|^{\ell}}.$$

- Des estimations (beaucoup plus difficiles) de sommes d'exponentielles permettent de généraliser à tout $k \geq 1$. De manière générale, la taille de $|F_{k,\ell}(e^{2i\pi x})|$ est contrôlée par la proximité de x aux rationnels.

- Les arcs majeurs $\mathfrak{M}$ sont alors choisis comment étant les x proches de rationnels $\frac{p}{q}$ avec q "petit" (en fonction de k et ℓ), et les arcs mineurs sont $[0, 1] \setminus \mathfrak{M}$. (Il faut optimiser beaucoup de paramètres pour obtenir le résultat final...)

- Hardy et Littlewood parviennent alors à $G(k) = O(k2^k)$.

- La méthode du cercle a initialement été imaginée par Hardy et Ramanujan pour établir que

$$p(n) \underset{n \to +\infty}{\sim} \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{\frac{2n}{3}}},$$

  où $p(n)$ est le nombre de manière d'écrire $n = \lambda_1 + \cdots + \lambda_r$ avec $\lambda_1 \geq \cdots \geq \lambda_r \geq 1$.

Quelques résultats récents

- La théorie analytique des nombres a une longue histoire et est toujours très active.

Quelques résultats récents

- La théorie analytique des nombres a une longue histoire et est toujours très active.

Théorème. (Helfgott, 2013)

Tout nombre impair plus grand que 5 est somme de trois nombres premiers.
(Conjecture de Goldbach faible)

Quelques résultats récents

- La théorie analytique des nombres a une longue histoire et est toujours très active.

Théorème. (Helfgott, 2013)

Tout nombre impair plus grand que 5 est somme de trois nombres premiers. (Conjecture de Goldbach faible)

Théorème. (Zhang, 2013)

Il existe $C > 0$ tel qu'il existe une infinité de nombres premiers consécutifs $p < q$ avec $q - p \leq C$.

Quelques résultats récents

- La théorie analytique des nombres a une longue histoire et est toujours très active.

Théorème. (Helfgott, 2013)

Tout nombre impair plus grand que 5 est somme de trois nombres premiers. (Conjecture de Goldbach faible)

Théorème. (Zhang, 2013)

Il existe $C > 0$ tel qu'il existe une infinité de nombres premiers consécutifs $p < q$ avec $q - p \leq C$.

Théorème. (Maynard, 2019)

Il existe une infinité de nombres premiers ne contenant pas le chiffre 7.

Merci de votre attention !