L'univers creux des mathématiques

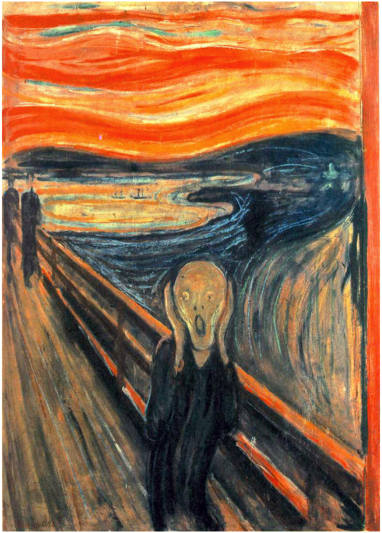
Université Laval

Jean-Marie De Koninck

23 mai 2024

L'univers creux des mathématiques

L'écart alarmant
entre le connu
et l'attendu



"Le cri" (Edvard Munch)

L'intrigante fonction zêta

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Des séries familières

Des séries familières

$$\zeta(1) = \sum_{n=1}^{\infty} \frac{1}{n} = +\infty$$

Des séries familières

$$\zeta(1) = \sum_{n=1}^{\infty} \frac{1}{n} = +\infty$$

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

Des séries familières

$$\zeta(1) = \sum_{n=1}^{\infty} \frac{1}{n} = +\infty$$

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

La probabilité que deux entiers positifs choisis au hasard n'aient aucun facteur premier en commun est égal à

Des séries familières

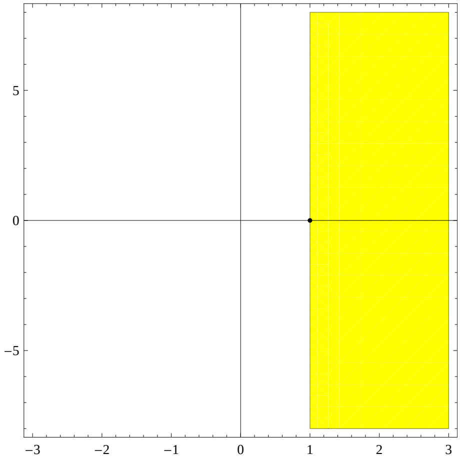
$$\zeta(1) = \sum_{n=1}^{\infty} \frac{1}{n} = +\infty$$

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

La probabilité que deux entiers positifs choisis au hasard n'aient aucun facteur premier en commun est égal à

$$\left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right)\left(1 - \frac{1}{5^2}\right)\cdots = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}$$

Une représentation dans le demi-plan $\Re(s) > 1$



Définition

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

valide pour tout $s \in \mathbb{C}$ avec $\Re(s) > 1$

Une définition valide pour tout $s \in \mathbb{C} \setminus \{1\}$

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) \qquad (\Re(s) > 1)$$

Une définition valide pour tout $s \in \mathbb{C} \setminus \{1\}$

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) \qquad (\Re(s) > 1)$$

- $\zeta(s)$ peut être prolongée analytiquement au demi-plan $\Re(s) > 0$ grâce à la représentation

$$\zeta(s) = \frac{s}{s-1} - s\int_1^{\infty} \frac{x - \lfloor x \rfloor}{x^{s+1}}\, dx \qquad (s \neq 1)$$

Une définition valide pour tout $s \in \mathbb{C} \setminus \{1\}$

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) \qquad (\Re(s) > 1)$$

- $\zeta(s)$ peut être prolongée analytiquement au demi-plan $\Re(s) > 0$ grâce à la représentation

$$\zeta(s) = \frac{s}{s-1} - s \int_1^{\infty} \frac{x - \lfloor x \rfloor}{x^{s+1}}\, dx \qquad (s \neq 1)$$

- En utilisant l'équation fonctionnelle

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

on peut prolonger $\zeta(s)$ pour tout $s \in \mathbb{C} \setminus \{1\}$

Un lien important avec la distribution des nombres premiers

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) \qquad (\Re(s) > 1)$$

Un lien important avec la distribution des nombres premiers

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) \qquad (\Re(s) > 1)$$

- $\pi(x) := \#\{p \leq x : p \text{ premier}\}$

Un lien important avec la distribution des nombres premiers

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) \qquad (\Re(s) > 1)$$

- $\pi(x) := \#\{p \leq x : p \text{ premier}\}$
- Pour $\Re(s) > 1$, on a

$$\log \zeta(s) = s \int_2^{\infty} \frac{\pi(x)}{x(x^s - 1)} dx$$

Un lien important avec la distribution des nombres premiers

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots \right) \qquad (\Re(s) > 1)$$

- $\pi(x) := \#\{p \leq x : p \text{ premier}\}$
- Pour $\Re(s) > 1$, on a

$$\log \zeta(s) = s \int_2^{\infty} \frac{\pi(x)}{x(x^s - 1)} dx$$

- ce qui permet d'établir que $\pi(x) \sim \dfrac{x}{\log x}$

La localisation des zéros

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) \qquad (\Re(s) > 1)$$

La localisation des zéros

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) \qquad (\Re(s) > 1)$$

- Il découle de

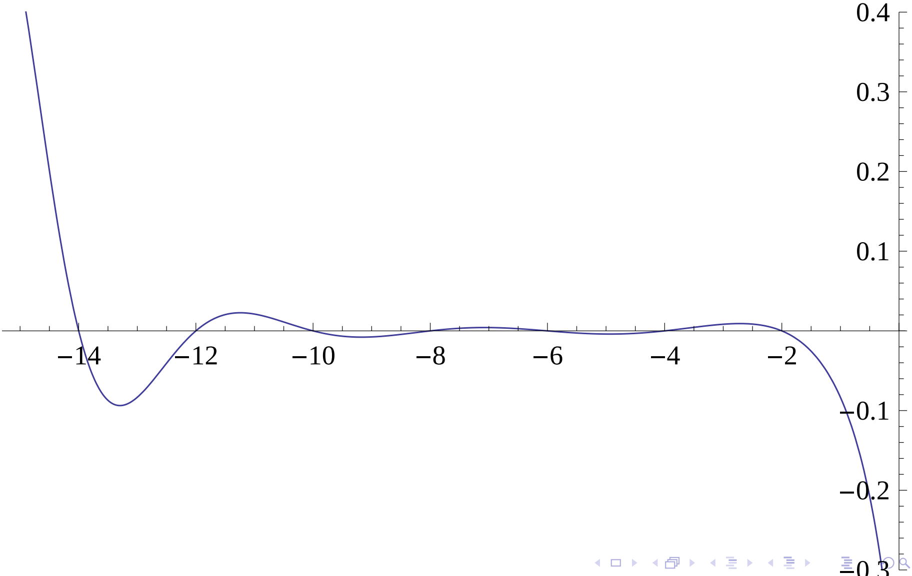
$$\zeta(s) = 2^s \pi^{s-1} \sin(\pi s/2)\Gamma(1-s)\zeta(1-s)$$

que

$$\zeta(-2) = \zeta(-4) = \zeta(-6) = \cdots = 0$$

Ces valeurs sont appelées les *zéros triviaux* de $\zeta(s)$

Graphique de $\zeta(\sigma)$ pour $-15 < \sigma < -1/5$



La localisation des zéros

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) \qquad (\Re(s) > 1)$$

La localisation des zéros

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) \qquad (\Re(s) > 1)$$

- Les *zéros triviaux*: $\zeta(-2) = \zeta(-4) = \cdots = 0$

La localisation des zéros

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) \qquad (\Re(s) > 1)$$

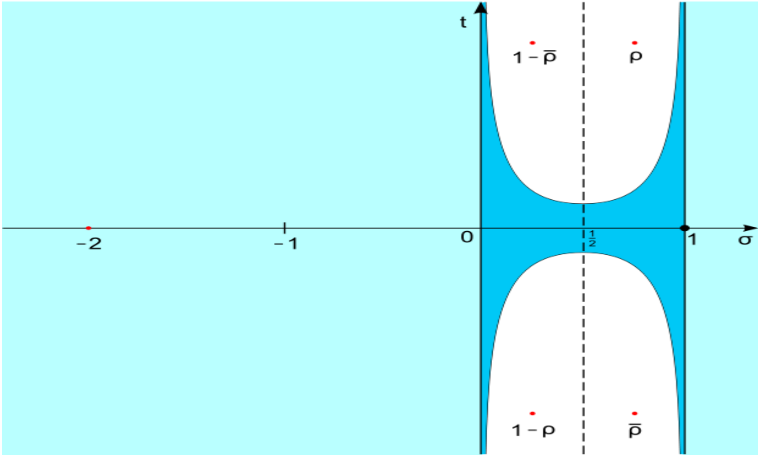
- Les *zéros triviaux*: $\zeta(-2) = \zeta(-4) = \cdots = 0$
- Autrement, $\zeta(s) \neq 0$ pour $\Re(s) \leq 0$ et $\Re(s) \geq 1$

La localisation des zéros

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) \qquad (\Re(s) > 1)$$

- Les *zéros triviaux*: $\zeta(-2) = \zeta(-4) = \cdots = 0$
- Autrement, $\zeta(s) \neq 0$ pour $\Re(s) \leq 0$ et $\Re(s) \geq 1$
- Les seuls zéros non réels de $\zeta(s)$ sont donc situés dans la bande critique $0 < \Re(s) < 1$

Région sans zéros dans la bande critique



$$\zeta(\rho) = 0 \iff \zeta(\overline{\rho}) = 0 \iff \zeta(1-\rho) = 0 \iff \zeta(1-\overline{\rho}) = 0$$

La localisation des zéros

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) \qquad (\Re(s) > 1)$$

- Les *zéros triviaux*: $\zeta(-2) = \zeta(-4) = \cdots = 0$
- Autrement, $\zeta(s) \neq 0$ pour $\Re(s) \leq 0$ et $\Re(s) \geq 1$
- Les seuls zéros non réels de $\zeta(s)$ sont situés dans la bande critique $0 < \Re(s) < 1$

La localisation des zéros

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) \qquad (\Re(s) > 1)$$

- Les *zéros triviaux*: $\zeta(-2) = \zeta(-4) = \cdots = 0$
- Autrement, $\zeta(s) \neq 0$ pour $\Re(s) \leq 0$ et $\Re(s) \geq 1$
- Les seuls zéros non réels de $\zeta(s)$ sont situés dans la bande critique $0 < \Re(s) < 1$
- Hardy (1914): $\zeta(s)$ admet une infinité de zéros sur la droite critique $\Re(s) = \frac{1}{2}$

La localisation des zéros

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) \qquad (\Re(s) > 1)$$

- Les *zéros triviaux*: $\zeta(-2) = \zeta(-4) = \cdots = 0$
- Autrement, $\zeta(s) \neq 0$ pour $\Re(s) \leq 0$ et $\Re(s) \geq 1$
- Les seuls zéros non réels de $\zeta(s)$ sont situés dans la bande critique $0 < \Re(s) < 1$
- Hardy (1914): $\zeta(s)$ admet une infinité de zéros sur la droite critique $\Re(s) = \frac{1}{2}$
- Conrey (1989): Au moins 40% des zéros non réels sont sur la droite critique

La localisation des zéros

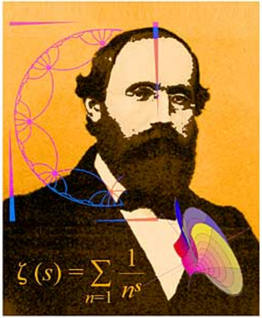
$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) \qquad (\Re(s) > 1)$$

- Les *zéros triviaux*: $\zeta(-2) = \zeta(-4) = \cdots = 0$
- Autrement, $\zeta(s) \neq 0$ pour $\Re(s) \leq 0$ et $\Re(s) \geq 1$
- Les seuls zéros non réels de $\zeta(s)$ sont situés dans la bande critique $0 < \Re(s) < 1$
- Hardy (1914): $\zeta(s)$ admet une infinité de zéros sur la droite critique $\Re(s) = \frac{1}{2}$
- Conrey (1989): Au moins 40% des zéros non réels sont sur la droite critique
- Gourdon (2004): Les 10^{13} premiers zéros sont tous sur la droite critique

L'hypothèse de Riemann (1859)

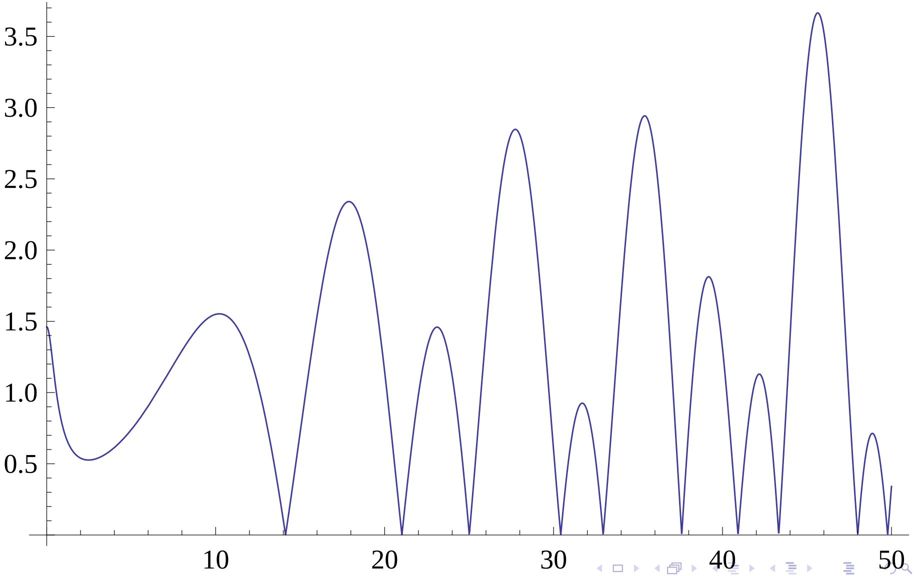
$$\boxed{\textit{Si } \zeta(s) = 0 \textit{ with } 0 < \Re(s) < 1, \textit{ alors } \Re(s) = \frac{1}{2}}$$

Dans les mots de Riemann: *Il est fort probable que ces zéros vérifient tous $\Re(s) = 1/2$. On peut certainement espérer une preuve plus rigoureuse. J'ai temporairement mis de côté cette question après quelques vaines tentatives car elle m'apparait inutile pour le prochain objectif de mes recherches.*



Georg Friedrich Bernhard Riemann 1826 - 1866

Graphique de $|\zeta(\frac{1}{2}+it)|$ pour $0 < t < 50$



Énoncés équivalents à l'hypothèse de Riemann (HR)

Soit $\pi(x) := \#\{p \leq x : p \text{ premier}\}$ et $\mathrm{Li}(x) := \displaystyle\int_2^x \frac{dt}{\log t}$

Énoncés équivalents à l'hypothèse de Riemann (HR)

Soit $\pi(x) := \#\{p \leq x : p \text{ premier}\}$ et $\mathrm{Li}(x) := \displaystyle\int_2^x \frac{dt}{\log t}$

- On peut démontrer que

$$\pi(x) = \mathrm{Li}(x) + O\left(\frac{x}{e^{\sqrt{\log x}}}\right)$$

Énoncés équivalents à l'hypothèse de Riemann (HR)

Soit $\pi(x) := \#\{p \leq x : p \text{ premier}\}$ et $\mathrm{Li}(x) := \displaystyle\int_2^x \frac{dt}{\log t}$

- On peut démontrer que

$$\pi(x) = \mathrm{Li}(x) + O\left(\frac{x}{e^{\sqrt{\log x}}}\right)$$

- HR $\iff \pi(x) = \mathrm{Li}(x) + O(\sqrt{x} \log x)$

Énoncés équivalents à l'hypothèse de Riemann (HR)

Soit $\pi(x) := \#\{p \leq x : p \text{ premier}\}$ et $\mathrm{Li}(x) := \displaystyle\int_2^x \frac{dt}{\log t}$

- On peut démontrer que

$$\pi(x) = \mathrm{Li}(x) + O\left(\frac{x}{e^{\sqrt{\log x}}}\right)$$

- HR $\iff \pi(x) = \mathrm{Li}(x) + O(\sqrt{x}\log x)$
- $\pi(x) = \mathrm{Li}(x) + O(x^{1-\varepsilon}) \quad ??$

La localisation des zéros et le terme d'erreur

Soit $$\Theta = \sup\{\sigma : \zeta(\sigma + it) = 0\}$$

Then,

- $\dfrac{1}{2} \leq \Theta \leq 1$
- $\mathrm{HR} \iff \Theta = \dfrac{1}{2}$

La localisation des zéros et le terme d'erreur

Soit $\quad \Theta = \sup\{\sigma : \zeta(\sigma + it) = 0\}$

Then,

- $\dfrac{1}{2} \leq \Theta \leq 1$
- HR $\iff \Theta = \dfrac{1}{2}$

On peut démontrer que

$$\pi(x) - \mathrm{Li}(x) = O\left(x^{\Theta} \log x\right)$$

Énoncés équivalents à HR

Soit

$$\sigma(n) := \sum_{d|n} d$$

Énoncés équivalents à HR

Soit

$$\sigma(n) := \sum_{d|n} d$$

- On sait démontrer que

$$\limsup_{n\to\infty} \frac{\sigma(n)}{e^\gamma n \log\log n} = 1,$$

où $\gamma = \lim_{N\to\infty} \left(\sum_{n=1}^{N} \frac{1}{n} - \log N \right) = 0.57721\ldots$

Énoncés équivalents à HR

Soit

$$\sigma(n) := \sum_{d|n} d$$

- On sait démontrer que

$$\limsup_{n\to\infty} \frac{\sigma(n)}{e^\gamma n \log\log n} = 1,$$

où $\gamma = \lim_{N\to\infty} \left(\sum_{n=1}^{N} \frac{1}{n} - \log N \right) = 0.57721\ldots$

- Pour $n = 5040$, on a $\frac{\sigma(n)}{e^\gamma n \log\log n} = 1.00556\ldots$

Énoncés équivalents à HR

Soit

$$\sigma(n) := \sum_{d|n} d$$

- On sait démontrer que

$$\limsup_{n\to\infty} \frac{\sigma(n)}{e^\gamma n \log\log n} = 1,$$

où $\gamma = \lim_{N\to\infty} \left(\sum_{n=1}^{N} \frac{1}{n} - \log N \right) = 0.57721\ldots$

- Pour $n = 5040$, on a $\frac{\sigma(n)}{e^\gamma n \log\log n} = 1.00556\ldots$
- HR $\iff \sigma(n) < e^\gamma n \log\log n$ pour tout $n \geq 5041$

Comparer $\pi(x)$ avec $\mathrm{Li}(x)$

Comparer $\pi(x)$ avec $\mathrm{Li}(x)$

x	$\pi(x)$	$\mathrm{Li}(x)$	$\Delta(x) = \mathrm{Li}(x) - \pi(x)$
10	4	6	2
10^2	25	30	5
10^3	168	178	10
10^4	1229	1246	17
10^5	9592	9630	38
10^6	78498	78628	130
10^7	664579	664918	339
10^8	5761455	5762209	754
10^9	50847534	50849235	1701
10^{10}	455052511	455055615	3104

Comparer $\pi(x)$ avec $\mathrm{Li}(x)$

x	$\pi(x)$	$\mathrm{Li}(x)$	$\Delta(x) = \mathrm{Li}(x) - \pi(x)$
10	4	6	2
10^2	25	30	5
10^3	168	178	10
10^4	1229	1246	17
10^5	9592	9630	38
10^6	78498	78628	130
10^7	664579	664918	339
10^8	5761455	5762209	754
10^9	50847534	50849235	1701
10^{10}	455052511	455055615	3104

Pour $x = 10^{27}$, on a $\Delta(x) = 465\,365\,954\,297$

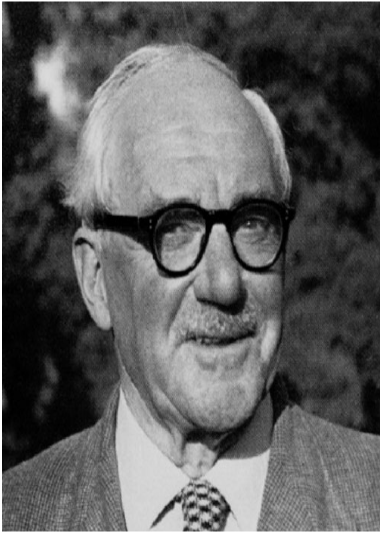
Comparer $\pi(x)$ avec $\mathrm{Li}(x)$

x	$\pi(x)$	$\mathrm{Li}(x)$	$\Delta(x) = \mathrm{Li}(x) - \pi(x)$
10	4	6	2
10^2	25	30	5
10^3	168	178	10
10^4	1229	1246	17
10^5	9592	9630	38
10^6	78498	78628	130
10^7	664579	664918	339
10^8	5761455	5762209	754
10^9	50847534	50849235	1701
10^{10}	455052511	455055615	3104

Pour $x = 10^{27}$, on a $\Delta(x) = 465\,365\,954\,297$

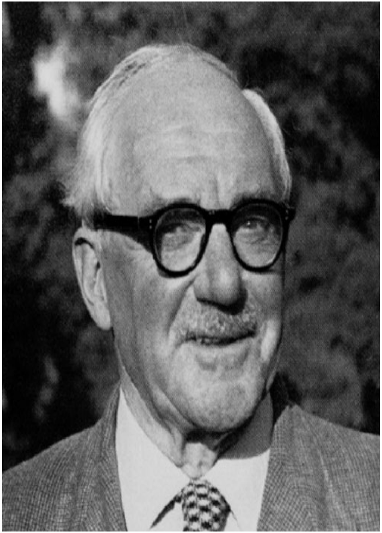
Gauss et Riemann croyaient que $\pi(x) < \mathrm{Li}(x)$ pour tout $x \geq 2$

La réalité défie l'intuition



J.E. Littlewood (1885-1977)

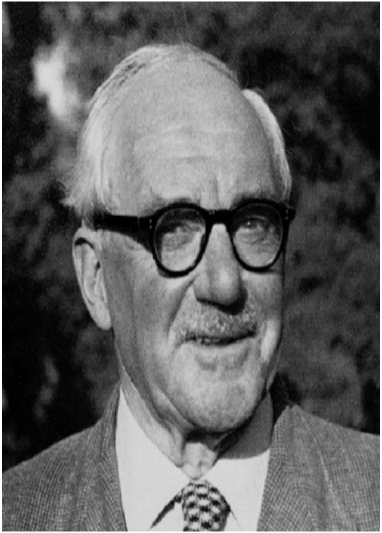
La réalité défie l'intuition



J.E. Littlewood (1885-1977)

1914: La différence $\pi(x) - \mathrm{Li}(x)$ change de signe une infinité de fois

La réalité défie l'intuition



J.E. Littlewood (1885-1977)

1914: La différence $\pi(x) - \mathrm{Li}(x)$ change de signe une infinité de fois

Il existe une suite croissante de nombres réels $x_0, x_1, x_2, \ldots$ telle que pour $n = 0, 1, 2, \ldots,$ on a

$$\pi(x_{2n+1}) - \mathrm{Li}(x_{2n+1}) > \sqrt{x_{2n+1}} \frac{\log\log\log x_{2n+1}}{\log\log x_{2n+1}}$$

et

$$\pi(x_{2n}) - \mathrm{Li}(x_{2n}) < -\sqrt{x_{2n}} \frac{\log\log\log x_{2n}}{\log\log x_{2n}}$$

Les nombres premiers de Wieferich

Les nombres premiers de Wieferich

Rappel de l'énoncé du petit théorème de Fermat :

$$2^{p-1} \equiv 1 \pmod{p} \qquad \forall p > 2.$$

Les nombres premiers de Wieferich

Rappel de l'énoncé du petit théorème de Fermat :

$$2^{p-1} \equiv 1 \pmod{p} \qquad \forall p > 2.$$

En 1909, Arthur Wieferich prouve:

$$\begin{aligned} x^p + y^p = z^p \quad \text{avec} \quad & p > 2, \quad (p, xyz) = 1 \\ \Longrightarrow \quad & 2^{p-1} \equiv 1 \pmod{p^2} \end{aligned}$$

Les nombres premiers de Wieferich

Rappel de l'énoncé du petit théorème de Fermat :

$$2^{p-1} \equiv 1 \pmod{p} \qquad \forall p > 2.$$

En 1909, Arthur Wieferich prouve:

$$\begin{aligned} x^p + y^p = z^p \quad \text{avec} \quad & p > 2, \quad (p, xyz) = 1 \\ \Longrightarrow \quad & 2^{p-1} \equiv 1 \pmod{p^2} \end{aligned}$$

Voilà qui motive la définition suivante:

p est un *nombre premier de Wieferich* si $2^{p-1} \equiv 1 \pmod{p^2}$

Les nombres premiers de Wieferich

Les nombres premiers de Wieferich

Un premier p est un *nombre premier de Wieferich* si $2^{p-1} \equiv 1 \pmod{p^2}$

Les nombres premiers de Wieferich

Un premier p est un *nombre premier de Wieferich* si $2^{p-1} \equiv 1 \pmod{p^2}$

$$\begin{aligned} W &= \text{l'ensemble des nombres premiers de Wieferich} \\ W^c &= \text{le complément de } W \text{ (dans l'ensemble des premiers)} \end{aligned}$$

Les nombres premiers de Wieferich

Un premier p est un *nombre premier de Wieferich* si $2^{p-1} \equiv 1 \pmod{p^2}$

$$\begin{aligned} W &= \text{l'ensemble des nombres premiers de Wieferich} \\ W^c &= \text{le complément de } W \text{ (dans l'ensemble des premiers)} \end{aligned}$$

On sait que $1093, 3511 \in W$
et que autre élément de W est $> 10^{15}$.

Les nombres premiers de Wieferich

Un premier p est un *nombre premier de Wieferich* si $2^{p-1} \equiv 1 \pmod{p^2}$

$$\begin{aligned} W &= \text{l'ensemble des nombres premiers de Wieferich} \\ W^c &= \text{le complément de } W \text{ (dans l'ensemble des premiers)} \end{aligned}$$

On sait que $1093, 3511 \in W$
et que autre élément de W est $> 10^{15}$.

$$|W| = +\infty \quad ?? \qquad\qquad |W^c| = +\infty \quad ??$$

Les nombres premiers de Wieferich

Les nombres premiers de Wieferich

Soit $W(x) := |\{p \le x : p \in W\}|$ et $W^c(x) := |\{p \le x : p \in W^c\}|$.

Les nombres premiers de Wieferich

Soit $W(x) := |\{p \leq x : p \in W\}|$ et $W^c(x) := |\{p \leq x : p \in W^c\}|$.

Heuristiquement, $W(x) \sim \log\log x$.

Les nombres premiers de Wieferich

Soit $W(x) := |\{p \le x : p \in W\}|$ et $W^c(x) := |\{p \le x : p \in W^c\}|$.

Heuristiquement, $W(x) \sim \log\log x$.

En effet, comme p divide $\dfrac{2^{p-1}-1}{p}$ avec une probabilité $1/p$,

$$\text{alors} \qquad W(x) \sim \sum_{p \le x} \frac{1}{p} \sim \log\log x,$$

Les nombres premiers de Wieferich

Soit $W(x) := |\{p \leq x : p \in W\}|$ et $W^c(x) := |\{p \leq x : p \in W^c\}|$.

Heuristiquement, $W(x) \sim \log\log x$.

En effet, comme p divide $\dfrac{2^{p-1}-1}{p}$ avec une probabilité $1/p$,

$$\text{alors} \qquad W(x) \sim \sum_{p \leq x} \frac{1}{p} \sim \log\log x,$$

ce qui implique en particulier que l'on devrait avoir

$$W^c(x) \sim \frac{x}{\log x}$$

La conjecture *abc*

La conjecture *abc*

La conjecture *abc*

Énoncé: Pour tout $\varepsilon > 0$, il existe une constante $M = M(\varepsilon) > 0$ telle que, quels que soient les entiers co-premiers $a, b, c \in \mathbb{N}$ avec $a + b = c$, on a

$$c < M \cdot \left(\prod_{p|abc} p \right)^{1+\varepsilon} .$$

La conjecture *abc*

Énoncé: Pour tout $\varepsilon > 0$, il existe une constante $M = M(\varepsilon) > 0$ telle que, quels que soient les entiers co-premiers $a, b, c \in \mathbb{N}$ avec $a + b = c$, on a

$$c < M \cdot \left(\prod_{p \mid abc} p \right)^{1+\varepsilon}.$$

La conjecture *abc* implique que l'équation $x^{10} + y^{10} = z^{10}$ n'a pas de solution en entiers positifs x, y, z.

La conjecture *abc*

Énoncé: Pour tout $\varepsilon > 0$, il existe une constante $M = M(\varepsilon) > 0$ telle que, quels que soient les entiers co-premiers $a, b, c \in \mathbb{N}$ avec $a + b = c$, on a

$$c < M \cdot \left(\prod_{p \mid abc} p \right)^{1+\varepsilon}.$$

La conjecture *abc* implique que l'équation $x^{10} + y^{10} = z^{10}$ n'a pas de solution en entiers positifs x, y, z. En effet, si la conjecture *abc* est vraie, en choisissant $\varepsilon = 1/2$, on aurait

$$z^{10} < M \left(\prod_{p \mid xyz} p \right)^{3/2} \leq M(xyz)^{3/2} < M(z^3)^{3/2} < Mz^5,$$

un non sens si z est assez grand.

Les conséquences de la conjecture *abc*

Les conséquences de la conjecture *abc*

- Le grand théorème de Fermat

Les conséquences de la conjecture *abc*

- Le grand théorème de Fermat
- Il existe une infinité de nombres premiers qui ne sont pas des nombres premiers de Wieferich, i.e. qu'il existe une infinité de nombres premiers p tels que

$$2^{p-1} \not\equiv 1 \pmod{p^2}$$

Les conséquences de la conjecture *abc*

- Le grand théorème de Fermat
- Il existe une infinité de nombres premiers qui ne sont pas des nombres premiers de Wieferich, i.e. qu'il existe une infinité de nombres premiers p tels que

$$2^{p-1} \not\equiv 1 \pmod{p^2}$$

- Étant donné $k \in \mathbb{N}$, l'équation $x^m - y^n = k$ a tout au plus une nombre fini de solutions en entiers $x, y, m, n \geq 2$

Les conséquences de la conjecture *abc*

- Le grand théorème de Fermat
- Il existe une infinité de nombres premiers qui ne sont pas des nombres premiers de Wieferich, i.e. qu'il existe une infinité de nombres premiers p tels que

$$2^{p-1} \not\equiv 1 \pmod{p^2}$$

- Étant donné $k \in \mathbb{N}$, l'équation $x^m - y^n = k$ a tout au plus une nombre fini de solutions en entiers $x, y, m, n \geq 2$
- Il existe tout au plus un nombre fini de triplets $n, n+1, n+2$ tous puissants $\quad$ (n est puissant si $p \mid n$ implique que $p^2 \mid n$)

L'énorme fossé entre la conjecture *abc* et ce que l'on a prouvé jusqu'ici

L'énorme fossé entre la conjecture *abc* et ce que l'on a prouvé jusqu'ici

Soit $\gamma(n) := \prod_{p|n} p$

L'énorme fossé entre la conjecture *abc* et ce que l'on a prouvé jusqu'ici

Soit $\gamma(n) := \prod_{p|n} p$

- **La conjecture** *abc*: Pour tout $\varepsilon > 0$, il existe une constante $M = M(\varepsilon) > 0$ telle que, pour tous les entiers co-prmiers $a, b, c \in \mathbb{N}$ avec $a + b = c$, on a
$$c < M \cdot \gamma(abc)^{1+\varepsilon}.$$

L'énorme fossé entre la conjecture *abc* et ce que l'on a prouvé jusqu'ici

Soit $\gamma(n) := \prod_{p|n} p$

- **La conjecture** *abc*: Pour tout $\varepsilon > 0$, il existe une constante $M = M(\varepsilon) > 0$ telle que, pour tous les entiers co-prmiers $a, b, c \in \mathbb{N}$ avec $a + b = c$, on a
$$c < M \cdot \gamma(abc)^{1+\varepsilon}.$$
- C.L. Stewart et K.Yu (1996): Pour tout $\varepsilon > 0$, il existe une constante $C = C(\varepsilon) > 0$ telle que, pour tous les entiers co-premiers $a, b, c \in \mathbb{N}$ avec $a + b = c$, on a
$$c < \exp\{C \cdot \gamma(abc)^{\frac{1}{3}+\varepsilon}\}.$$

Les nombres normaux

Les nombres normaux

Les nombres normaux

0.1

Les nombres normaux

0.11

Les nombres normaux

0.110

Les nombres normaux

0.1101

Les nombres normaux

0.11011

Les nombres normaux

0.110110

Les nombres normaux

0.1101100

Les nombres normaux

$0.1101100\ldots$

Le monde fascinant des nombres normaux

Ces constantes bien connues

$$
\begin{aligned}
\pi &= 3.14159265358979323846264338327950288419 7\ldots \\
e &= 2.71828182845904523536028747135266249775 7\ldots \\
\gamma &= 0.57721566490153286060651209008240243104 22\ldots \\
\sqrt{2} &= 1.41421356237309504880168872420969807857 0\ldots \\
\log 2 &= 0.69314718055994530941723212145817656807 55\ldots
\end{aligned}
$$

sont telles des nombres normaux ?

La définition d'un nombre normal

Étant donné un entier $q \geq 2$, un nombre normal en base q est un nombre irrationnel dont le développement des chiffres en base q est tel que toute séquence arbitraire de k chiffres apparait dans son développement à la même fréquence, soit $1/q^k$.

La définition d'un nombre normal

Étant donné un entier $q \geq 2$, un nombre normal en base q est un nombre irrationnel dont le développement des chiffres en base q est tel que toute séquence arbitraire de k chiffres apparait dans son développement à la même fréquence, soit $1/q^k$.

- En 1933, Champernowne démontre que le nombre

$$0.123456789101112131415161718192021\ldots$$

est normal en base 10

La définition d'un nombre normal

Étant donné un entier $q \geq 2$, un nombre normal en base q est un nombre irrationnel dont le développement des chiffres en base q est tel que toute séquence arbitraire de k chiffres apparait dans son développement à la même fréquence, soit $1/q^k$.

- En 1933, Champernowne démontre que le nombre

$$0.123456789101112131415161718192021\ldots$$

  est normal en base 10
- En 1971, Stoneham prouve que le nombre

$$\sum_{n=3^k>1}^{\infty} \frac{1}{n2^n} = \sum_{k=1}^{\infty} \frac{1}{3^k 2^{3^k}} = 0.0418837\ldots$$

  est normal en base 2.

Les nombres normaux

Il est connu que

Les nombres normaux

Il est connu que

- personne n'a réussi à prouver que π, e, $\sqrt{2}$, $\log 2$ et $\zeta(3)$ sont des nombres normaux,

Les nombres normaux

Il est connu que

- personne n'a réussi à prouver que π, e, $\sqrt{2}$, $\log 2$ et $\zeta(3)$ sont des nombres normaux,
- l'on croit que tout nombre algébrique irrationnel est normal,

Les nombres normaux

Il est connu que

- personne n'a réussi à prouver que π, e, $\sqrt{2}$, $\log 2$ et $\zeta(3)$ sont des nombres normaux,
- l'on croit que tout nombre algébrique irrationnel est normal,
- aucun nombre algébrique irrationnel n'a été démontré "normal",

Les nombres normaux

Il est connu que

- personne n'a réussi à prouver que π, e, $\sqrt{2}$, $\log 2$ et $\zeta(3)$ sont des nombres normaux,
- l'on croit que tout nombre algébrique irrationnel est normal,
- aucun nombre algébrique irrationnel n'a été démontré "normal",
- Émile Borel (1909) a prouvé que presque tous les nombres réels (avec la mesure de Lebesgue) sont absolument normaux.

L'univers creux des nombres normaux

L'univers creux des nombres normaux

En base 2,

$$\sqrt{2} = 0.1011010100000100111100110011001111111100111\ldots$$

L'univers creux des nombres normaux

En base 2,

$$\sqrt{2} = 0.101101010000010011110011001100111111100111\ldots$$

Le nombre attendu de 1 dans le développement binaire de $\sqrt{2}$ jusqu'au rang N est $N/2$

L'univers creux des nombres normaux

En base 2,

$$\sqrt{2} = 0.1011010100000100111100110011001111111100111\ldots$$

Le nombre attendu de 1 dans le développement binaire de $\sqrt{2}$ jusqu'au rang N est $N/2$

Un petit pas

L'univers creux des nombres normaux

En base 2,

$$\sqrt{2} = 0.101101010000010011110011001100111111001 11\ldots$$

Le nombre attendu de 1 dans le développement binaire de $\sqrt{2}$ jusqu'au rang N est $N/2$

Un petit pas

Bailey, Borwein, Crandall, Pomerance (2003):
Il existe une constante positive c telle que le nombre de 1 dans le développement binaire de $\sqrt{2}$ jusqu'au rang N est au moins $c\sqrt{N}$.

Des percées inattendues

Le dernier théorème de Fermat

$$\boxed{\text{Pour tout entier } n \geq 3, \text{ l'équation } x^n + y^n = z^n \text{ admet aucune solution en entiers positifs } x, y, z}$$

Le dernier théorème de Fermat

$$\boxed{\text{Pour tout entier } n \geq 3, \text{ l'équation } x^n + y^n = z^n \text{ admet aucune solution en entiers positifs } x, y, z}$$

- D'abord énoncé par Pierre de Fermat autour de 1640

Le dernier théorème de Fermat

Pour tout entier $n \geq 3$, l'équation $x^n + y^n = z^n$ admet aucune solution en entiers positifs x, y, z

- D'abord énoncé par Pierre de Fermat autour de 1640
- Prouvé en 1994 par Andrew Wiles

La conjecture de Catalan

$$\boxed{\text{Les seules puissances d'entiers consécutifs sont } 2^3 \text{ et } 3^2}$$

La conjecture de Catalan

$$\boxed{\text{Les seules puissances d'entiers consécutifs sont } 2^3 \text{ et } 3^2}$$

- D'abord énoncé par Eugène Catalan en 1844

La conjecture de Catalan

$$\boxed{\text{Les seules puissances d'entiers consécutifs sont } 2^3 \text{ et } 3^2}$$

- D'abord énoncé par Eugène Catalan en 1844
- La conjecture *abc* implique qu'il existe tout au plus un nombre fini de telles puissances consécutives

La conjecture de Catalan

$$\boxed{\text{Les seules puissances d'entiers consécutifs sont } 2^3 \text{ et } 3^2}$$

- D'abord énoncé par Eugène Catalan en 1844
- La conjecture *abc* implique qu'il existe tout au plus un nombre fini de telles puissances consécutives
- Prouvé en 2002 par Preda Mihailescu

$\mathrm{P} = \mathrm{NP}$? ?

P = NP ? ?

$$
\begin{aligned}
\mathsf{P} &= \text{l'ensemble des problèmes dont la solution peut être obtenue} \\
&\ \text{en temps polynomial} \\
\mathsf{NP} &= \text{l'ensemble des problèmes qui n'appartiennent pas à } \mathsf{P}, \\
&\ \text{mais dont la solution peut être vérifiée en temps polynomial}
\end{aligned}
$$

P = NP ? ?

$$
\begin{array}{rcl}
\mathbf{P} & = & \text{l'ensemble des problèmes dont la solution peut être obtenue} \\
 & & \text{en temps polynomial} \\
\mathbf{NP} & = & \text{l'ensemble des problèmes qui n'appartiennent pas à } \mathbf{P}, \\
 & & \text{mais dont la solution peut être vérifiée en temps polynomial}
\end{array}
$$

- Addition, multiplication $\in \mathbf{P}$

$\mathbf{P} = \mathbf{NP}$? ?

$\mathbf{P}$ = l'ensemble des problèmes dont la solution peut être obtenue en temps polynomial

$\mathbf{NP}$ = l'ensemble des problèmes qui n'appartiennent pas à $\mathbf{P}$, mais dont la solution peut être vérifiée en temps polynomial

- Addition, multiplication $\in \mathbf{P}$
- Le problème du commis voyageur $\in \mathbf{NP}$? ?

$\mathbf{P} = \mathbf{NP}$? ?

$$
\begin{aligned}
\mathbf{P} &= \text{l'ensemble des problèmes dont la solution peut être obtenue} \\
&\quad\ \text{en temps polynomial} \\
\mathbf{NP} &= \text{l'ensemble des problèmes qui n'appartiennent pas à } \mathbf{P}, \\
&\quad\ \text{mais dont la solution peut être vérifiée en temps polynomial}
\end{aligned}
$$

- Addition, multiplication $\in$ **P**
- Le problème du commis voyageur $\in$ **NP** ? ?
- La factorisation $\in$ **NP** ? ?

$\mathbf{P} = \mathbf{NP}$? ?

$$
\begin{aligned}
\mathbf{P} &= \text{l'ensemble des problèmes dont la solution peut être obtenue} \\
&\quad \text{en temps polynomial} \\
\mathbf{NP} &= \text{l'ensemble des problèmes qui n'appartiennent pas à } \mathbf{P}, \\
&\quad \text{mais dont la solution peut être vérifiée en temps polynomial}
\end{aligned}
$$

- Addition, multiplication $\in$ **P**
- Le problème du commis voyageur $\in$ **NP** ? ?
- La factorisation $\in$ **NP** ? ?
- La primalité $\in$ **NP** ? ?

P = NP ? ?

$$\begin{aligned} \mathbf{P} &= \text{l'ensemble des problèmes dont la solution peut être obtenue} \\ &\ \text{en temps polynomial} \\ \mathbf{NP} &= \text{l'ensemble des problèmes qui n'appartiennent pas à } \mathbf{P}, \\ &\ \text{mais dont la solution peut être vérifiée en temps polynomial} \end{aligned}$$

- Addition, multiplication $\in$ **P**
- Le problème du commis voyageur $\in$ **NP** ? ?
- La factorisation $\in$ **NP** ? ?
- La primalité $\in$ **NP** ? ?

Le problème du millénaire: **P** = **NP** ? ?

Le problème de la somme des sous-ensembles

Le problème de la somme des sous-ensembles

Énoncé: Étant donné un ensemble A fait de n entiers, existe-t-il un sous-ensemble non vide de A dont la somme est 0 ?

Le problème de la somme des sous-ensembles

Énoncé: Étant donné un ensemble A fait de n entiers, existe-t-il un sous-ensemble non vide de A dont la somme est 0 ?

Exemple: Considérons l'ensemble $A = \{-6, -3, -2, 5, 12\}$. On identifie rapidement le sous-ensemble $\{-3, -2, 5\}$ comme candidat dont la somme des éléments est 0.

Le problème de la somme des sous-ensembles

Énoncé: Étant donné un ensemble A fait de n entiers, existe-t-il un sous-ensemble non vide de A dont la somme est 0 ?

Exemple: Considérons l'ensemble $A = \{-6, -3, -2, 5, 12\}$. On identifie rapidement le sous-ensemble $\{-3, -2, 5\}$ comme candidat dont la somme des éléments est 0.

Ce problème appartient à **NP**, car le nombre d'étapes requis pour résoudre le problème peut être aussi élevé que 2^n, alors que toute solution peut être vérifiée en temps polynomial.

Primalité $\in$ P ? ?

Primalité $\in$ P ? ?

Agrawal, Kayal, Saxena (2002): Primalité $\in$ P

Nombres premiers en progressions arithmétique

1923: Hardy et Littlewood conjecturent que la suite des nombres premiers contient des progressions arithmétiques arbitrairement longues.

Nombres premiers en progressions arithmétique

1923: Hardy et Littlewood conjecturent que la suite des nombres premiers contient des progressions arithmétiques arbitrairement longues.

- En 2004, Markus Frind, Paul Underwood, et Paul Jobling prouvent que

$$56\,211\,383\,760\,397 + 44\,546\,738\,095\,860\,k \text{ pour } k = 0, 1, \ldots, 22$$

sont tous des nombres premiers.

Nombres premiers en progressions arithmétique

1923: Hardy et Littlewood conjecturent que la suite des nombres premiers contient des progressions arithmétiques arbitrairement longues.

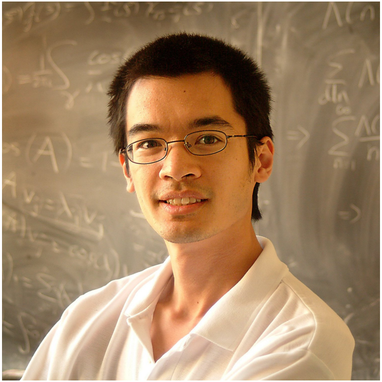
- En 2004, Markus Frind, Paul Underwood, et Paul Jobling prouvent que

$$56\,211\,383\,760\,397 + 44\,546\,738\,095\,860\,k \text{ pour } k = 0, 1, \ldots, 22$$

sont tous des nombres premiers.

- En 2008, Green et Tao prouvent la conjecture de Hardy et Littlewood

Ben Green et Terence Tao



Étant donné $k \geq 3$, le nombre de progressions arithmétiques de nombres premiers de longueur k (tous inférieurs à N) est au moins

$$C_k \frac{N^2}{\log^k N}$$

Un pas important vers la preuve de la conjecture des nombres premiers jumeaux

Un pas important vers la preuve de la conjecture des nombres premiers jumeaux

La conjecture des nombres premiers jumeaux:

$$\liminf_{n\to\infty}(p_{n+1} - p_n) = 2$$

Un pas important vers la preuve de la conjecture des nombres premiers jumeaux

La conjecture des nombres premiers jumeaux:

$$\liminf_{n\to\infty}(p_{n+1} - p_n) = 2$$

Jusqu'à avril 2013, personne ne pouvait démontrer que

$$\liminf_{n\to\infty}(p_{n+1} - p_n) \qquad \text{existe !}$$

Un pas important vers la preuve de la conjecture des nombres premiers jumeaux

La conjecture des nombres premiers jumeaux:

$$\liminf_{n\to\infty}(p_{n+1}-p_n)=2$$

Jusqu'à avril 2013, personne ne pouvait démontrer que

$$\liminf_{n\to\infty}(p_{n+1}-p_n) \qquad \text{existe !}$$

En mai 2013, Yitang Zhang prouve que

$$\liminf_{n\to\infty}(p_{n+1}-p_n)\leq 70\,000\,000$$

Un pas important vers la preuve de la conjecture des nombres premiers jumeaux

La conjecture des nombres premiers jumeaux:

$$\liminf_{n\to\infty}(p_{n+1} - p_n) = 2$$

Jusqu'à avril 2013, personne ne pouvait démontrer que

$$\liminf_{n\to\infty}(p_{n+1} - p_n) \qquad \text{existe !}$$

En mai 2013, Yitang Zhang prouve que

$$\liminf_{n\to\infty}(p_{n+1} - p_n) \leq 70\,000\,000$$

En 2014, James Maynard prouve que

$$\liminf_{n\to\infty}(p_{n+1} - p_n) \leq 600$$

Un pas important vers la preuve de la conjecture des nombres premiers jumeaux

Un pas important vers la preuve de la conjecture des nombres premiers jumeaux

En mai 2013, Yitang Zhang prouve que

$$\liminf_{n\to\infty}(p_{n+1}-p_n) \leq 70\,000\,000$$

Un pas important vers la preuve de la conjecture des nombres premiers jumeaux

En mai 2013, Yitang Zhang prouve que

$$\liminf_{n\to\infty}(p_{n+1}-p_n)\leq 70\,000\,000$$

En 2014, James Maynard prouve que

$$\liminf_{n\to\infty}(p_{n+1}-p_n)\leq 600$$

Un pas important vers la preuve de la conjecture des nombres premiers jumeaux

En mai 2013, Yitang Zhang prouve que

$$\liminf_{n\to\infty}(p_{n+1}-p_n) \leq 70\,000\,000$$

En 2014, James Maynard prouve que

$$\liminf_{n\to\infty}(p_{n+1}-p_n) \leq 600$$

Aujourd'hui, on sait remplacer le nombre 600 par le nombre 246.

Un pas important vers la preuve de la conjecture des nombres premiers jumeaux

Yitang Zhang (New Hampshire)

James Maynard (Montreal)

De quoi réfléchir ...

Merci !

www.jeanmariedekoninck.mat.ulaval.ca