Les écarts entre les nombres premiers

Dimitris Koukoulopoulos

Université de Montréal

Club mathématique, Université de Montréal
11 février 2015

Les nombres premiers

- Un nombre $n > 1$ est appelé *composé* si $n = ab$ pour quelques $a, b < n$.
- Un nombre $p > 1$ est appelé *premier* s'il n'est pas composé.

Les nombres premiers

- Un nombre $n > 1$ est appelé *composé* si $n = ab$ pour quelques $a, b < n$.
- Un nombre $p > 1$ est appelé *premier* s'il n'est pas composé.

Théorème (Euclid)

1. *Chaque nombre naturel n peut s'écrire comme le produit de quelques nombres premiers de façon unique (modulo permutation des facteurs).*
2. *Il y a une infinité de nombres premiers.*

Les nombres premiers

- Un nombre $n > 1$ est appelé *composé* si $n = ab$ pour quelques $a, b < n$.
- Un nombre $p > 1$ est appelé *premier* s'il n'est pas composé.

Théorème (Euclid)

1. *Chaque nombre naturel n peut s'écrire comme le produit de quelques nombres premiers de façon unique (modulo permutation des facteurs).*
2. *Il y a une infinité de nombres premiers.*

Question

Comment est-ce que les nombres premiers sont distribués parmi les nombres naturels ? Comportement déterministe ou aléatoire ?

Les nombres premiers

- Un nombre $n > 1$ est appelé *composé* si $n = ab$ pour quelques $a, b < n$.
- Un nombre $p > 1$ est appelé *premier* s'il n'est pas composé.

Théorème (Euclid)

1. *Chaque nombre naturel n peut s'écrire comme le produit de quelques nombres premiers de façon unique (modulo permutation des facteurs).*
2. *Il y a une infinité de nombres premiers.*

Question

Comment est-ce que les nombres premiers sont distribués parmi les nombres naturels ? Comportement déterministe ou aléatoire ?

Remarque

La définition des nombres premiers « par exclusion » fait leur détection très difficile.

Le théorème des nombres premiers

$\pi(x) := \{p \text{ premier} : p \leq x\},\ p_n$ est le n-ième nombre premier.

Le théorème des nombres premiers

$$\pi(x) := \{p \text{ premier} : p \leq x\},\ p_n \text{ est le } n\text{-ième nombre premier.}$$

En étudiant des tables de premiers, Gauss a observé (quand il avait 15 ou 16 ans) que la densité des nombres premiers autour de x est à peu prés $1/\log x$.

Le théorème des nombres premiers

$$\pi(x) := \{p \text{ premier} : p \leq x\},\ p_n \text{ est le } n\text{-ième nombre premier.}$$

En étudiant des tables de premiers, Gauss a observé (quand il avait 15 ou 16 ans) que la densité des nombres premiers autour de x est à peu prés $1/\log x$.

$$\Longrightarrow \qquad \frac{d}{dx}\pi(x) \sim \frac{1}{\log x}$$

Le théorème des nombres premiers

$$\pi(x) := \{p \text{ premier} : p \leq x\},\ p_n \text{ est le } n\text{-ième nombre premier.}$$

En étudiant des tables de premiers, Gauss a observé (quand il avait 15 ou 16 ans) que la densité des nombres premiers autour de x est à peu prés $1/\log x$.

$$\Longrightarrow \quad \frac{d}{dx}\pi(x) \sim \frac{1}{\log x} \quad \Longrightarrow \pi(x) \sim \mathrm{Li}(x) := \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x}.$$

Le théorème des nombres premiers

$$\pi(x) := \{p \text{ premier} : p \leq x\},\ p_n \text{ est le } n\text{-ième nombre premier.}$$

En étudiant des tables de premiers, Gauss a observé (quand il avait 15 ou 16 ans) que la densité des nombres premiers autour de x est à peu prés $1/\log x$.

$$\Longrightarrow \quad \frac{d}{dx}\pi(x) \sim \frac{1}{\log x} \quad \Longrightarrow \pi(x) \sim \mathrm{Li}(x) := \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x}.$$

Théorème des nombres premiers (de la Vallée Poussin - Hadamard (1896), de la Vallée Poussin (1899))

$$\lim_{x\to\infty} \frac{\pi(x)}{\mathrm{Li}(x)} = 1. \quad \textit{En particulier, } p_n \sim n\log n.$$

Comparaison numérique de $\pi(x)$ et $\mathrm{Li}(x)$

x	$\pi(x)$	$\mathrm{Li}(x) - \pi(x)$
10^{13}	346065536839	108970
10^{14}	3204941750802	314889
10^{15}	29844570422669	1052618
10^{16}	279238341033925	3214631
10^{17}	2623557157654233	7956588
10^{18}	24739954287740860	21949554
10^{19}	234057667276344607	99877774
10^{20}	2220819602560918840	222744643
10^{21}	21127269486018731928	597394253
10^{22}	201467286689315906290	1932355207
10^{23}	1925320391606803968923	7250186214

Comparaison numérique de $\pi(x)$ et $\mathrm{Li}(x)$

x	$\pi(x)$	$\mathrm{Li}(x) - \pi(x)$
10^{13}	346065536839	108970
10^{14}	3204941750802	314889
10^{15}	29844570422669	1052618
10^{16}	279238341033925	3214631
10^{17}	2623557157654233	7956588
10^{18}	24739954287740860	21949554
10^{19}	234057667276344607	99877774
10^{20}	2220819602560918840	222744643
10^{21}	21127269486018731928	597394253
10^{22}	201467286689315906290	1932355207
10^{23}	1925320391606803968923	7250186214

Hypothèse de Riemann : $\pi(x) = \mathrm{Li}(x) + O_\epsilon(x^{1/2+\epsilon})$

Comparaison numérique de $\pi(x)$ et $\mathrm{Li}(x)$

x	$\pi(x)$	$\mathrm{Li}(x) - \pi(x)$
10^{13}	346065536839	108970
10^{14}	3204941750802	314889
10^{15}	29844570422669	1052618
10^{16}	279238341033925	3214631
10^{17}	2623557157654233	7956588
10^{18}	24739954287740860	21949554
10^{19}	234057667276344607	99877774
10^{20}	2220819602560918840	222744643
10^{21}	21127269486018731928	597394253
10^{22}	201467286689315906290	1932355207
10^{23}	1925320391606803968923	7250186214

Hypothèse de Riemann : $\pi(x) = \mathrm{Li}(x) + O_\epsilon(x^{1/2+\epsilon})$

Question

Qu'est-ce qu'on peut dire pour les plus fines propriétés statistiques des nombres premiers ? e.g. Répartition de leurs différences $d_n := p_{n+1} - p_n$?

Structure vs Hasard

On a que $\pi(x) \sim \mathrm{Li}(x)$ et que $p_n \sim n \log n$.

Structure vs Hasard

On a que $\pi(x) \sim \mathrm{Li}(x)$ et que $p_n \sim n \log n$.

Deux autres suites avec la même propriété :

Structure vs Hasard

On a que $\pi(x) \sim \mathrm{Li}(x)$ et que $p_n \sim n \log n$.

Deux autres suites avec la même propriété :

- $p'_n = \lfloor n \log n \rfloor$ (bien structurée)

Structure vs Hasard

On a que $\pi(x) \sim \mathrm{Li}(x)$ et que $p_n \sim n \log n$.

Deux autres suites avec la même propriété :

- $p'_n = \lfloor n \log n \rfloor$ (bien structurée)
- Soient $\{Y_k\}_{k \geq 3}$ de variables aléatoires de Bernoulli indépendantes avec

$$\begin{cases} \mathbb{P}(Y_k = 1) = \dfrac{1}{\log k} \\ \mathbb{P}(Y_k = 0) = 1 - \dfrac{1}{\log k} \end{cases}$$

Structure vs Hasard

On a que $\pi(x) \sim \mathrm{Li}(x)$ et que $p_n \sim n \log n$.

Deux autres suites avec la même propriété :

- $p'_n = \lfloor n \log n \rfloor$ (bien structurée)
- Soient $\{Y_k\}_{k \geq 3}$ de variables aléatoires de Bernoulli indépendantes avec

$$\begin{cases} \mathbb{P}(Y_k = 1) = \dfrac{1}{\log k} \\ \mathbb{P}(Y_k = 0) = 1 - \dfrac{1}{\log k} \end{cases}$$

$\mathcal{P}'' := \{k \geq 3 : Y_k = 1\} = \{p''_n\}_{n \geq 1}$ (nombres premiers « aléatoires »)

Structure vs Hasard

On a que $\pi(x) \sim \mathrm{Li}(x)$ et que $p_n \sim n \log n$.

Deux autres suites avec la même propriété :

- $p'_n = \lfloor n \log n \rfloor$ (bien structurée)
- Soient $\{Y_k\}_{k \geq 3}$ de variables aléatoires de Bernoulli indépendantes avec

$$\begin{cases} \mathbb{P}(Y_k = 1) = \dfrac{1}{\log k} \\ \mathbb{P}(Y_k = 0) = 1 - \dfrac{1}{\log k} \end{cases}$$

$\mathcal{P}'' := \{k \geq 3 : Y_k = 1\} = \{p''_n\}_{n \geq 1}$ (nombres premiers « aléatoires »)

$$\pi''(x) := \#\mathcal{P}'' \cap [1, x]; \quad \mathbb{E}[\pi''(x)] = \sum_{3 \leq k \leq x} \frac{1}{\log k} = \mathrm{Li}(x) + O(1),$$

$$\mathrm{Var}[\pi''(x)] = \mathrm{Li}(x) + O(1) \sim \frac{x}{\log x}$$

Structure vs Hasard

On a que $\pi(x) \sim \mathrm{Li}(x)$ et que $p_n \sim n \log n$.

Deux autres suites avec la même propriété :

- $p'_n = \lfloor n \log n \rfloor$ (bien structurée)
- Soient $\{Y_k\}_{k \geq 3}$ de variables aléatoires de Bernoulli indépendantes avec

$$\begin{cases} \mathbb{P}(Y_k = 1) = \dfrac{1}{\log k} \\ \mathbb{P}(Y_k = 0) = 1 - \dfrac{1}{\log k} \end{cases}$$

$\mathcal{P}'' := \{k \geq 3 : Y_k = 1\} = \{p''_n\}_{n \geq 1}$ (nombres premiers « aléatoires »)

$$\pi''(x) := \#\mathcal{P}'' \cap [1, x]; \quad \mathbb{E}[\pi''(x)] = \sum_{3 \leq k \leq x} \frac{1}{\log k} = \mathrm{Li}(x) + O(1),$$

$$\mathrm{Var}[\pi''(x)] = \mathrm{Li}(x) + O(1) \sim \frac{x}{\log x}$$

$$\text{TCL} \implies \pi''(x) = \mathrm{Li}(x) + O(x^{1/2+\epsilon}) \text{ p.s.} \implies p''_n \sim n \log n \text{ p.s.}$$

Dieu joue aux dés

Si p, q sont deux nombres premiers, alors on les appelle

- *jumeaux* si $q = p + 2$,
- *cousins* si $q = p + 4$,
- *sexy* si $q = p + 6$.

Dieu joue aux dés

Si p, q sont deux nombres premiers, alors on les appelle

- *jumeaux* si $q = p + 2$,
- *cousins* si $q = p + 4$,
- *sexy* si $q = p + 6$.

Modèle déterministe : $p'_n = \lfloor n \log n \rfloor$**.** On a $p'_{n+1} - p'_n \sim \log n$. Ceci prédit qu'il y a qu'un nombre fini de nombres premiers jumeaux, cousins et sexy.

Dieu joue aux dés

Si p, q sont deux nombres premiers, alors on les appelle

- *jumeaux* si $q = p + 2$,
- *cousins* si $q = p + 4$,
- *sexy* si $q = p + 6$.

Modèle déterministe : $p'_n = \lfloor n \log n \rfloor$**.** On a $p'_{n+1} - p'_n \sim \log n$. Ceci prédit qu'il y a qu'un nombre fini de nombres premiers jumeaux, cousins et sexy.

Les évidences numériques sont contre cette prediction.

Dieu joue aux dés

Si p, q sont deux nombres premiers, alors on les appelle

- *jumeaux* si $q = p + 2$,
- *cousins* si $q = p + 4$,
- *sexy* si $q = p + 6$.

Modèle déterministe : $p'_n = \lfloor n \log n \rfloor$**.** On a $p'_{n+1} - p'_n \sim \log n$. Ceci prédit qu'il y a qu'un nombre fini de nombres premiers jumeaux, cousins et sexy.

Les évidences numériques sont contre cette prediction.

Modèle aléatoire : $\mathcal{P}'' = \{k \geq 3 : Y_k = 1\}$**.** Soit $\pi''_2(x) = \{k \leq x : k, k+2 \in \mathcal{P}''\}$.

$$\mathbb{E}\left[\pi''_2(x)\right] \overset{\text{indep.}}{=} \sum_{3 \leq k \leq x} \mathbb{P}(Y_k = 1)\mathbb{P}(Y_{k+2} = 1) \sim \frac{x}{(\log x)^2} \to \infty.$$

Dieu joue aux dés

Si p, q sont deux nombres premiers, alors on les appelle

- *jumeaux* si $q = p + 2$,
- *cousins* si $q = p + 4$,
- *sexy* si $q = p + 6$.

Modèle déterministe : $p'_n = \lfloor n \log n \rfloor$**.** On a $p'_{n+1} - p'_n \sim \log n$. Ceci prédit qu'il y a qu'un nombre fini de nombres premiers jumeaux, cousins et sexy.

Les évidences numériques sont contre cette prediction.

Modèle aléatoire : $\mathcal{P}'' = \{k \geq 3 : Y_k = 1\}$**.** Soit $\pi''_2(x) = \{k \leq x : k, k+2 \in \mathcal{P}''\}$.

$$\mathbb{E}\left[\pi''_2(x)\right] \overset{\text{indep.}}{=} \sum_{3 \leq k \leq x} \mathbb{P}(Y_k = 1)\mathbb{P}(Y_{k+2} = 1) \sim \frac{x}{(\log x)^2} \to \infty.$$

Ce modèle aléatoire est appelé le *modèle de Cramér* après Harald Cramér qui l'a introduit en 1936.

Dieu joue aux dés

Si p, q sont deux nombres premiers, alors on les appelle

- *jumeaux* si $q = p + 2$,
- *cousins* si $q = p + 4$,
- *sexy* si $q = p + 6$.

Modèle déterministe : $p'_n = \lfloor n \log n \rfloor$**.** On a $p'_{n+1} - p'_n \sim \log n$. Ceci prédit qu'il y a qu'un nombre fini de nombres premiers jumeaux, cousins et sexy.

Les évidences numériques sont contre cette prediction.

Modèle aléatoire : $\mathcal{P}'' = \{k \geq 3 : Y_k = 1\}$**.** Soit $\pi''_2(x) = \{k \leq x : k, k+2 \in \mathcal{P}''\}$.

$$\mathbb{E}\left[\pi''_2(x)\right] \overset{\text{indep.}}{=} \sum_{3 \leq k \leq x} \mathbb{P}(Y_k = 1)\mathbb{P}(Y_{k+2} = 1) \sim \frac{x}{(\log x)^2} \to \infty.$$

Ce modèle aléatoire est appelé le *modèle de Cramér* après Harald Cramér qui l'a introduit en 1936.

Problème : on a aussi que $\mathbb{E}\left[\#\{k \leq x : k, k+1 \in \mathcal{P}''\}\right] \sim K/\log^2 K \to \infty$, qui est absurd car si $p \geq 3$ est premier, alors $p + 1$ est pair...

Ajustement du modèle de Cramér

Idée : on ignore les entiers divisibles par un petit nombre premier. Si w est un parametre, on travail dans

$$\mathcal{K} := \{k \in \mathbb{N} : k \text{ n'a pas de facteurs premiers } \leq w\}.$$

Ajustement du modèle de Cramér

Idée : on ignore les entiers divisibles par un petit nombre premier. Si w est un parametre, on travail dans

$$\mathcal{K} := \{k \in \mathbb{N} : k \text{ n'a pas de facteurs premiers } \leq w\}.$$

On a que $\#\mathcal{K} \cap [1,x] \approx x \cdot \prod_{p \leq w}(1 - 1/p)$.

Ajustement du modèle de Cramér

Idée : on ignore les entiers divisibles par un petit nombre premier. Si w est un parametre, on travail dans

$$\mathcal{K} := \{k \in \mathbb{N} : k \text{ n'a pas de facteurs premiers } \leq w\}.$$

On a que $\#\mathcal{K} \cap [1,x] \approx x \cdot \prod_{p \leq w}(1-1/p)$. Donc

$$\mathbb{P}\Big(k \text{ premier} \Big| k \in \mathcal{K}\Big) = \frac{1}{\log k} \prod_{p \leq w} \left(1 - \frac{1}{p}\right)^{-1} =: \rho_k$$

Ajustement du modèle de Cramér

Idée : on ignore les entiers divisibles par un petit nombre premier. Si w est un parametre, on travail dans

$$\mathcal{K} := \{k \in \mathbb{N} : k \text{ n'a pas de facteurs premiers } \leq w\}.$$

On a que $\#\mathcal{K} \cap [1,x] \approx x \cdot \prod_{p \leq w}(1-1/p)$. Donc

$$\mathbb{P}\Big(k \text{ premier} \Big| k \in \mathcal{K}\Big) = \frac{1}{\log k} \prod_{p \leq w} \left(1 - \frac{1}{p}\right)^{-1} =: \rho_k$$

$$\rightsquigarrow \quad (Z_k)_{k \geq 3} \text{ var. aleat. indep. avec } \begin{cases} Z_k = 0 & \text{si } k \notin \mathcal{K} \\ \mathbb{P}(Z_k = 1) = \rho_k & \text{si } k \in \mathcal{K} \\ \mathbb{P}(Z_k = 0) = 1 - \rho_k & \text{si } k \in \mathcal{K} \end{cases}$$

Ajustement du modèle de Cramér

Idée : on ignore les entiers divisibles par un petit nombre premier. Si w est un parametre, on travail dans

$$\mathcal{K} := \{k \in \mathbb{N} : k \text{ n'a pas de facteurs premiers } \leq w\}.$$

On a que $\#\mathcal{K} \cap [1,x] \approx x \cdot \prod_{p \leq w}(1-1/p)$. Donc

$$\mathbb{P}\Big(k \text{ premier} \Big| k \in \mathcal{K}\Big) = \frac{1}{\log k} \prod_{p \leq w} \left(1 - \frac{1}{p}\right)^{-1} =: \rho_k$$

$$\rightsquigarrow \quad (Z_k)_{k \geq 3} \text{ var. aleat. indep. avec } \begin{cases} Z_k = 0 & \text{si } k \notin \mathcal{K} \\ \mathbb{P}(Z_k = 1) = \rho_k & \text{si } k \in \mathcal{K} \\ \mathbb{P}(Z_k = 0) = 1 - \rho_k & \text{si } k \in \mathcal{K} \end{cases}$$

$$\mathbb{E}\left[\sum_{k \leq x} Z_k Z_{k+2}\right] = \sum_{\substack{k \leq x \\ k, k+2 \in \mathcal{K}}} \mathbb{P}(Z_k = Z_{k+2} = 1) \sim 2 \prod_{3 \leq p \leq w} \frac{1-2/p}{(1-1/p)^2} \frac{x}{\log^2 x}$$

Test numérique de la prédiction

$$\pi_2(x) := \#\{p \leq x : p+2 \text{ premier}\}, \quad F(x) = c_2 \cdot \int_2^x \frac{dt}{(\log t)^2},$$

$$c_2 = 2 \prod_{p>2} \left(1 - \frac{2}{p}\right) \left(1 - \frac{1}{p}\right)^{-2} \quad \text{(constante des nombres premiers jumeaux)}$$

x	$\pi_2(x)$	$F(x)$	$\pi_2(x) - F(x)$
10^{10}	27412679	27411417	1262
10^{11}	224376048	224368865	7183
10^{12}	1870585220	1870559867	25353
10^{13}	15834664872	15834598305	66567
10^{14}	135780321665	135780264894	56771
10^{15}	1177209242304	1177208491861	750443
10^{16}	10304195697298	10304192554495	3142803

Source : Wolfram MathWorld

Test numérique de la prédiction

$$\pi_2(x) := \#\{p \le x : p+2 \text{ premier}\}, \quad F(x) = c_2 \cdot \int_2^x \frac{dt}{(\log t)^2},$$

$$c_2 = 2\prod_{p>2}\left(1-\frac{2}{p}\right)\left(1-\frac{1}{p}\right)^{-2} \quad \text{(constante des nombres premiers jumeaux)}$$

x	$\pi_2(x)$	$F(x)$	$\pi_2(x) - F(x)$
10^{10}	27412679	27411417	1262
10^{11}	224376048	224368865	7183
10^{12}	1870585220	1870559867	25353
10^{13}	15834664872	15834598305	66567
10^{14}	135780321665	135780264894	56771
10^{15}	1177209242304	1177208491861	750443
10^{16}	10304195697298	10304192554495	3142803

Source : Wolfram MathWorld

Conjecture : $\pi_2(x) = F(x) + O_\epsilon(x^{1/2+\epsilon})$

Tamisage pour trouver des premiers jumeaux

Question : Comment est-ce qu'on peut detecter un pair $(p, p+2)$ des nombres premiers jumeaux ?

Tamisage pour trouver des premiers jumeaux

Question : Comment est-ce qu'on peut detecter un pair $(p, p+2)$ des nombres premiers jumeaux ?

Problème : la définition de la primalité « par exclusion » : $n > 1$ est premier si

n n'est pas divisible par $2, 3, \ldots, n-1$

Tamisage pour trouver des premiers jumeaux

Question : Comment est-ce qu'on peut detecter un pair $(p, p+2)$ des nombres premiers jumeaux ?

Problème : la définition de la primalité « par exclusion » : $n > 1$ est premier si

n n'est pas divisible par $2, 3, \ldots, n-1$

$\Leftrightarrow$ n n'est pas divisible par un premier $q < n$

Tamisage pour trouver des premiers jumeaux

Question : Comment est-ce qu'on peut detecter un pair $(p, p+2)$ des nombres premiers jumeaux ?

Problème : la définition de la primalité « par exclusion » : $n > 1$ est premier si

n n'est pas divisible par $2, 3, \ldots, n-1$

$\Leftrightarrow$ n n'est pas divisible par un premier $q < n$

$\Leftrightarrow$ n n'est pas divisible par un premier $q \leq \sqrt{n}$ (crible d'Eratosthenes)

Tamisage pour trouver des premiers jumeaux

Question : Comment est-ce qu'on peut detecter un pair $(p, p+2)$ des nombres premiers jumeaux ?

Problème : la définition de la primalité « par exclusion » : $n > 1$ est premier si

n n'est pas divisible par $2, 3, \ldots, n-1$

$\Leftrightarrow$ n n'est pas divisible par un premier $q < n$

$\Leftrightarrow$ n n'est pas divisible par un premier $q \leq \sqrt{n}$ (crible d'Eratosthenes)

$$\begin{aligned}\pi_2(x) &= \#\{p \leq x : p+2 \text{ premier}\} = \#\{p \leq x : q|p+2 \ \Rightarrow \ q > \sqrt{p+2}\} \\ &= \#\{p \leq x : q|p+2 \ \Rightarrow \ q > \sqrt{x}\} + O(\sqrt{x}) \\ &= \#\{p \leq x : p \not\equiv -2 \pmod{q} \ \forall q \leq \sqrt{x}\} + O(\sqrt{x})\end{aligned}$$

Tamisage pour trouver des premiers jumeaux

Question : Comment est-ce qu'on peut detecter un pair $(p, p+2)$ des nombres premiers jumeaux ?

Problème : la définition de la primalité « par exclusion » : $n > 1$ est premier si

n n'est pas divisible par $2, 3, \ldots, n-1$

$\Leftrightarrow$ n n'est pas divisible par un premier $q < n$

$\Leftrightarrow$ n n'est pas divisible par un premier $q \leq \sqrt{n}$ (crible d'Eratosthenes)

$$\begin{aligned}\pi_2(x) &= \#\{p \leq x : p+2 \text{ premier}\} = \#\{p \leq x : q|p+2 \ \Rightarrow \ q > \sqrt{p+2}\} \\ &= \#\{p \leq x : q|p+2 \ \Rightarrow \ q > \sqrt{x}\} + O(\sqrt{x}) \\ &= \#\{p \leq x : p \not\equiv -2 \pmod q \ \forall q \leq \sqrt{x}\} + O(\sqrt{x})\end{aligned}$$

$$\Longrightarrow \ \pi_2(x) \approx \frac{x}{\log x} \prod_{3 \leq q \leq \sqrt{x}} \frac{q-2}{q-1} \sim (2e^{-\gamma})^2 \frac{c_2 x}{\log^2 x}$$

Tamisage pour trouver des premiers jumeaux

Question : Comment est-ce qu'on peut detecter un pair $(p, p+2)$ des nombres premiers jumeaux ?

Problème : la définition de la primalité « par exclusion » : $n > 1$ est premier si

n n'est pas divisible par $2, 3, \ldots, n-1$

$\Leftrightarrow$ n n'est pas divisible par un premier $q < n$

$\Leftrightarrow$ n n'est pas divisible par un premier $q \leq \sqrt{n}$ (crible d'Eratosthenes)

$$\begin{aligned}\pi_2(x) &= \#\{p \leq x : p+2 \text{ premier}\} = \#\{p \leq x : q|p+2 \ \Rightarrow \ q > \sqrt{p+2}\} \\ &= \#\{p \leq x : q|p+2 \ \Rightarrow \ q > \sqrt{x}\} + O(\sqrt{x}) \\ &= \#\{p \leq x : p \not\equiv -2 \pmod q \ \forall q \leq \sqrt{x}\} + O(\sqrt{x})\end{aligned}$$

$$\Longrightarrow \ \pi_2(x) \approx \frac{x}{\log x} \prod_{3 \leq q \leq \sqrt{x}} \frac{q-2}{q-1} \sim (2e^{-\gamma})^2 \frac{c_2 x}{\log^2 x}$$

$$\frac{\#\{n \leq x : n \equiv a \pmod{q_1 q_2}\}}{x} = \frac{1}{q_1 q_2} + O\left(\frac{1}{x}\right) : \text{problème quand } q_1 q_2 \approx x$$

Résultats partiels

Théorème (Viggo Brun (1919))

$$\#\{p \leq x : p+2 \text{ premier}\} \leq \frac{cx}{\log^2 x}$$

$$\Longrightarrow \qquad \sum_{p,p+2 \text{ premier}} \frac{1}{p} < \infty$$

Résultats partiels

Théorème (Viggo Brun (1919))

$$\#\{p \leq x : p+2 \text{ premier}\} \leq \frac{cx}{\log^2 x}$$

$$\Longrightarrow \qquad \sum_{p,p+2 \text{ premier}} \frac{1}{p} < \infty$$

Un effort de calculer cette somme (appelée *la constante de Brun*) par Thomas Nicely a relevé le Pentium FDIV bug du processor Intel P5 Pentium.

Résultats partiels

Théorème (Viggo Brun (1919))

$$\#\{p \leq x : p+2 \text{ premier}\} \leq \frac{cx}{\log^2 x}$$

$$\Longrightarrow \qquad \sum_{p,p+2 \text{ premier}} \frac{1}{p} < \infty$$

Un effort de calculer cette somme (appelée *la constante de Brun*) par Thomas Nicely a relevé le Pentium FDIV bug du processor Intel P5 Pentium.

Théorème (Chen, 1966)

Il y un nombre infini de nombres premiers p pour lesquels $p+2$ a un ou deux facteurs premiers.

Résultats partiels

Théorème (Viggo Brun (1919))

$$\#\{p \leq x : p+2 \text{ premier}\} \leq \frac{cx}{\log^2 x}$$

$$\Longrightarrow \quad \sum_{p,p+2 \text{ premier}} \frac{1}{p} < \infty$$

Un effort de calculer cette somme (appelée *la constante de Brun*) par Thomas Nicely a relevé le Pentium FDIV bug du processor Intel P5 Pentium.

Théorème (Chen, 1966)

Il y un nombre infini de nombres premiers p pour lesquels $p+2$ a un ou deux facteurs premiers.

Remarque

Un entier avec un nombre borné de facteurs premiers est appelé quasi-premier.

Petits écarts entre des nombres premiers

Si $h \in \mathbb{N}$ est donné, on ne peut pas montrer que $\#\{p : p + 2h \text{ premier}\} = \infty$.

Est-ce qu'on peut montrer qu'il existe $H \in \mathbb{N}$ tel que
$\#\{p : p^+ \leq p + H\} = \infty$, où p^+ est le prochain nombre premier ?

Petits écarts entre des nombres premiers

Si $h \in \mathbb{N}$ est donné, on ne peut pas montrer que $\#\{p : p + 2h \text{ premier}\} = \infty$.

Est-ce qu'on peut montrer qu'il existe $H \in \mathbb{N}$ tel que
$\#\{p : p^+ \leq p + H\} = \infty$, où p^+ est le prochain nombre premier ?

L'idée de GPY (Goldston, Pintz, Yildirim) : considèrons

$$S := \sum_{x<n\leq 2x} \left(\sum_{h=0}^{H} \mathbf{1}_{\text{premier}}(n+h) - 1 \right) w_n,$$

où w_n est un poids **positif**. Si $S > 0$, alors $\liminf_{p\to\infty}(p^+ - p) \leq H$.

Petits écarts entre des nombres premiers

Si $h \in \mathbb{N}$ est donné, on ne peut pas montrer que $\#\{p : p + 2h \text{ premier}\} = \infty$.

Est-ce qu'on peut montrer qu'il existe $H \in \mathbb{N}$ tel que
$\#\{p : p^+ \leq p + H\} = \infty$, où p^+ est le prochain nombre premier ?

L'idée de GPY (Goldston, Pintz, Yildirim) : considèrons

$$S := \sum_{x<n\leq 2x} \left(\sum_{h=0}^{H} \mathbf{1}_{\text{premier}}(n+h) - 1 \right) w_n,$$

où w_n est un poids **positif**. Si $S > 0$, alors $\liminf_{p\to\infty}(p^+ - p) \leq H$.

Exigence : calculer $\sum_{x<n\leq 2x} \mathbf{1}_{\text{premier}}(n+h)w_n$ et $\sum_{x<n\leq 2x} w_n$.

Petits écarts entre des nombres premiers

Si $h \in \mathbb{N}$ est donné, on ne peut pas montrer que $\#\{p : p + 2h \text{ premier}\} = \infty$.

Est-ce qu'on peut montrer qu'il existe $H \in \mathbb{N}$ tel que
$\#\{p : p^+ \leq p + H\} = \infty$, où p^+ est le prochain nombre premier ?

L'idée de GPY (Goldston, Pintz, Yildirim) : considèrons

$$S := \sum_{x<n\leq 2x} \left(\sum_{h=0}^{H} \mathbf{1}_{\text{premier}}(n+h) - 1 \right) w_n,$$

où w_n est un poids **positif**. Si $S > 0$, alors $\liminf_{p\to\infty}(p^+ - p) \leq H$.

Exigence : calculer $\sum_{x<n\leq 2x} \mathbf{1}_{\text{premier}}(n+h)w_n$ et $\sum_{x<n\leq 2x} w_n$.

Le choix de GPY : si $\mathcal{H} \subset [0, H] \cap \mathbb{Z}$ est 'admissible' et fixé, on pose
$w_n \approx \prod_{h\in\mathcal{H}} \mathbf{1}_{\text{quasi-premier}}(n+h)$.

Petits écarts entre des nombres premiers

Si $h \in \mathbb{N}$ est donné, on ne peut pas montrer que $\#\{p : p + 2h \text{ premier}\} = \infty$.

Est-ce qu'on peut montrer qu'il existe $H \in \mathbb{N}$ tel que
$\#\{p : p^+ \leq p + H\} = \infty$, où p^+ est le prochain nombre premier ?

L'idée de GPY (Goldston, Pintz, Yildirim) : considèrons

$$S := \sum_{x<n\leq 2x} \left(\sum_{h=0}^{H} \mathbf{1}_{\text{premier}}(n+h) - 1 \right) w_n,$$

où w_n est un poids **positif**. Si $S > 0$, alors $\liminf_{p\to\infty}(p^+ - p) \leq H$.

Exigence : calculer $\sum_{x<n\leq 2x} \mathbf{1}_{\text{premier}}(n+h)w_n$ et $\sum_{x<n\leq 2x} w_n$.

Le choix de GPY : si $\mathcal{H} \subset [0, H] \cap \mathbb{Z}$ est 'admissible' et fixé, on pose
$w_n \approx \prod_{h\in\mathcal{H}} \mathbf{1}_{\text{quasi-premier}}(n+h)$.

Défi : afin de calculer S, on a besoin d'information sur la repartition des premiers en progressions arithmétiques.

Le travail de GPY est ses limitations

Hypothèse $BV(\theta)$: pour 'presque tous' $q \leq x^{\theta}$, on a que

$$\#\{p \leq x : p \equiv a \,(\mathrm{mod}\, q)\} \sim \frac{\pi(x)}{\phi(q)} \quad \text{pour tout } (a,q) = 1.$$

Le travail de GPY est ses limitations

Hypothèse $BV(\theta)$: pour 'presque tous' $q \leq x^{\theta}$, on a que

$$\#\{p \leq x : p \equiv a \,(\mathrm{mod}\, q)\} \sim \frac{\pi(x)}{\phi(q)} \quad \text{pour tout } (a,q) = 1.$$

GPY ont montré que si $BV(1/2+\epsilon)$ est vrai, alors $\liminf_{p\to\infty}(p^{+} - p) < \infty$.

Le travail de GPY est ses limitations

Hypothèse $BV(\theta)$: pour 'presque tous' $q \leq x^{\theta}$, on a que

$$\#\{p \leq x : p \equiv a \,(\mathrm{mod}\, q)\} \sim \frac{\pi(x)}{\phi(q)} \quad \text{pour tout } (a,q) = 1.$$

GPY ont montré que si $BV(1/2+\epsilon)$ est vrai, alors $\liminf_{p\to\infty}(p^{+}-p) < \infty$.

Théorème de Bombieri-Vinogradov : l'hypothèse $BV(1/2-\epsilon)$ est vraie ; on échoue pour ϵ !

Le travail de GPY est ses limitations

Hypothèse $BV(\theta)$: pour 'presque tous' $q \leq x^{\theta}$, on a que

$$\#\{p \leq x : p \equiv a \,(\mathrm{mod}\, q)\} \sim \frac{\pi(x)}{\phi(q)} \quad \text{pour tout } (a,q) = 1.$$

GPY ont montré que si $BV(1/2+\epsilon)$ est vrai, alors $\liminf_{p\to\infty}(p^{+}-p) < \infty$.

Théorème de Bombieri-Vinogradov : l'hypothèse $BV(1/2-\epsilon)$ est vraie ; on échoue pour ϵ !

Problème : l'hypothèse $BV(1/2+\epsilon)$ est même plus forte que l'Hypothèse de Riemann Généralisée…

Le travail de GPY est ses limitations

Hypothèse $BV(\theta)$: pour 'presque tous' $q \leq x^{\theta}$, on a que

$$\#\{p \leq x : p \equiv a \,(\mathrm{mod}\, q)\} \sim \frac{\pi(x)}{\phi(q)} \quad \text{pour tout } (a,q) = 1.$$

GPY ont montré que si $BV(1/2+\epsilon)$ est vrai, alors $\liminf_{p\to\infty}(p^+ - p) < \infty$.

Théorème de Bombieri-Vinogradov : l'hypothèse $BV(1/2-\epsilon)$ est vraie ; on échoue pour ϵ !

Problème : l'hypothèse $BV(1/2+\epsilon)$ est même plus forte que l'Hypothèse de Riemann Généralisée...

Théorème (Goldston, Pintz, Yildirim (2005))

$$\liminf_{p\to\infty} \frac{p^+ - p}{\log p} = 0.$$

(En moyenne, $p^+ - p \sim \log p$.)

(a) Dan Goldston

(b) János Pintz

(c) Cem Yil-di-rim

Le grand shock : écarts bornés entre les premiers

En mai 2013, un mathématicien appelé Yitang Zhang, inconnu à cette époque-là, a prouve que

$$\liminf_{p\to\infty}(p^+ - p) < 70\,000\,000.$$

Afin de faire ceci, il a montré quelque chose même plus stupéfiant : $\widetilde{BV}(1/2+\epsilon)$ est vraie un certain $\epsilon > 0$. (Travaux reliés de Bombieri-Friedlander-Iwaniec et de Fouvry.)

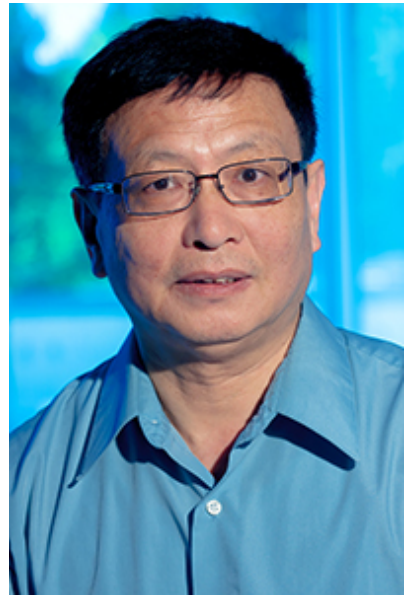


FIGURE : Yitang Zhang

AMERICAN MATHEMATICAL SOCIETY
MathSciNet 75 years 1940-2015
Mathematical Reviews
ISSN 2167-5163

Matches: 3

Batch Download: Reviews (HTML) Retrieve Marked | Retrieve First 50 | Unmark All

Publications results for "Items authored by Zhang, Yi Tang "

MR3171761 Reviewed Zhang, Yitang Bounded gaps between primes. *Ann. of Math. (2)* 179 (2014), no. 3, 1121–1174. (Reviewer: S. W. Graham) 11N05 (11N36)
PDF | Clipboard | Journal | Article
Obtenir

MR1869116 Reviewed Zhang, Yitang On the zeros of $\zeta'(s)$ near the critical line. *Duke Math. J.* 110 (2001), no. 3, 555–572. (Reviewer: Daniel A. Goldston) 11M26 (11M06)
PDF | Clipboard | Journal | Article
Obtenir

MR0867509 Reviewed Zhang, Yi Tang Two theorems on the zero density of the Riemann zeta function. *Acta Math. Sinica (N.S.)* 1 (1985), no. 3, 274–285. (Reviewer: Aleksandar Ivić) 11M06
PDF | Clipboard | Journal | Article
Obtenir

Matches: 3

AMS American Mathematical Society

Mirror Sites Providence, RI USA

Une approche alternative : les poids de Maynard-Tao

En novembre 2013, James Maynard, un postdoc à l'Université de Montréal à cette époque-là, a annoncé le résultat

$$\liminf_{p\to\infty}(p^+ - p) \leq 600.$$

Une approche alternative : les poids de Maynard-Tao

En novembre 2013, James Maynard, un postdoc à l'Université de Montréal à cette époque-là, a annoncé le résultat

$$\liminf_{p\to\infty}(p^+ - p) \leq 600.$$

Il a annoncé un autre résultat, même plus étonnant : pour tout $m \in \mathbb{N}$, on a que

$$\liminf_{n\to\infty}(p_{n+m} - p_n) < \infty,$$

c'est-à-dire, on peut detecter $m+1$ nombres premiers dans un intervalle de longuer bornée !

Une approche alternative : les poids de Maynard-Tao

En novembre 2013, James Maynard, un postdoc à l'Université de Montréal à cette époque-là, a annoncé le résultat

$$\liminf_{p\to\infty}(p^+ - p) \leq 600.$$

Il a annoncé un autre résultat, même plus étonnant : pour tout $m \in \mathbb{N}$, on a que

$$\liminf_{n\to\infty}(p_{n+m} - p_n) < \infty,$$

c'est-à-dire, on peut detecter $m+1$ nombres premiers dans un intervalle de longuer bornée !

Nouvelle idée : changer les poids de GPY (idée indépendamment découverte par Terence Tao presque simultanément).

Une approche alternative : les poids de Maynard-Tao

En novembre 2013, James Maynard, un postdoc à l'Université de Montréal à cette époque-là, a annoncé le résultat

$$\liminf_{p\to\infty}(p^+ - p) \leq 600.$$

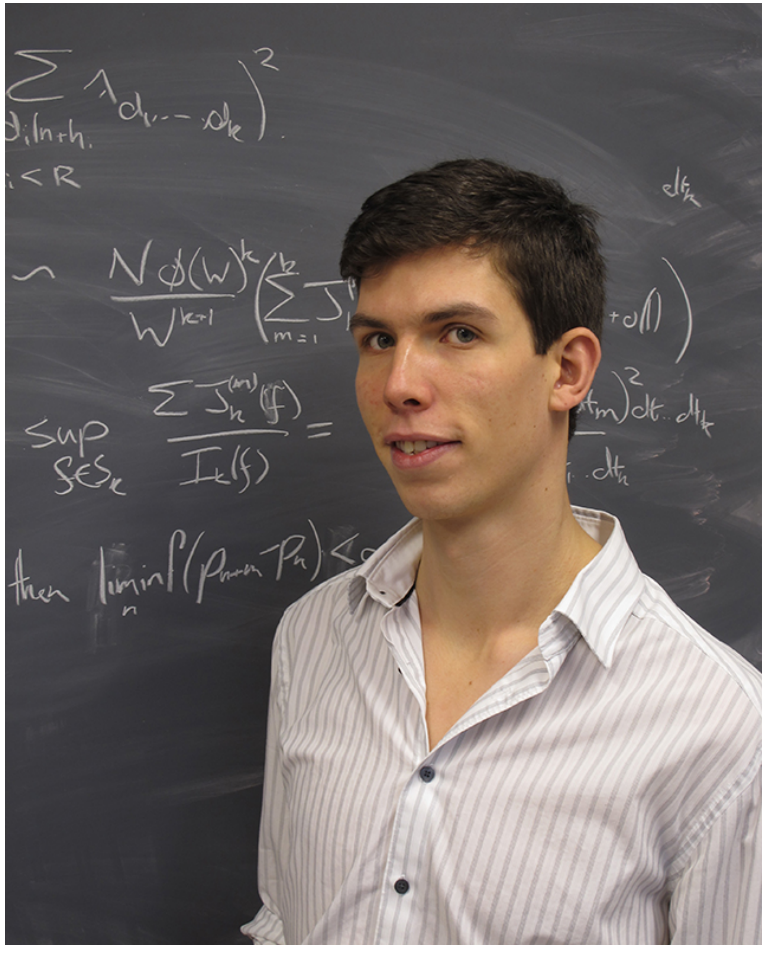
Il a annoncé un autre résultat, même plus étonnant : pour tout $m \in \mathbb{N}$, on a que

$$\liminf_{n\to\infty}(p_{n+m} - p_n) < \infty,$$

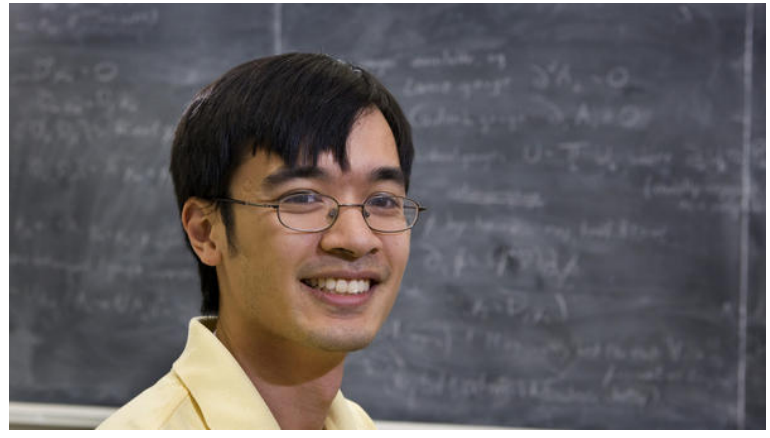
c'est-à-dire, on peut detecter $m+1$ nombres premiers dans un intervalle de longuer bornée !

Nouvelle idée : changer les poids de GPY (idée indépendamment découverte par Terence Tao presque simultanément).

Record courant : $\liminf_{p\to\infty}(p^+ - p) \leq 246$, un résultat de D. H. J. Polymath (une collaboration de plusieurs mathématiciens accueilli par le blog de Terence Tao).



(a) James Maynard



(b) Terence Tao

Et les nombres premiers jumeaux ?

Sur une conjecture (une grande généralisation de l'hypothèse $BV(\theta)$), Polymath a montré que

$$\liminf_{p\to\infty}(p^+ - p) \leq 6.$$

Et les nombres premiers jumeaux ?

Sur une conjecture (une grande généralisation de l'hypothèse $BV(\theta)$), Polymath a montré que

$$\liminf_{p\to\infty}(p^+ - p) \leq 6.$$

En fait, il a montré qu'il y a une infinité des premiers p tels que $p+2$ ou $p+6$ sont également premiers.

Et les nombres premiers jumeaux ?

Sur une conjecture (une grande généralisation de l'hypothèse $BV(\theta)$), Polymath a montré que

$$\liminf_{p\to\infty}(p^+ - p) \leq 6.$$

En fait, il a montré qu'il y a une infinité des premiers p tels que $p+2$ ou $p+6$ sont également premiers.

$$\#\{p : p+2 \text{ a un ou deux facteurs premiers}\} = \infty$$
$$\#\{p : p+2 \text{ ou } p+6 \text{ est premier}\} = \infty$$

Et les nombres premiers jumeaux ?

Sur une conjecture (une grande généralisation de l'hypothèse $BV(\theta)$), Polymath a montré que

$$\liminf_{p\to\infty}(p^+ - p) \leq 6.$$

En fait, il a montré qu'il y a une infinité des premiers p tels que $p+2$ ou $p+6$ sont également premiers.

$$\#\{p : p+2 \text{ a un ou deux facteurs premiers}\} = \infty$$
$$\#\{p : p+2 \text{ ou } p+6 \text{ est premier}\} = \infty$$

Il y a un obstacle très subtile que ne nous permet pas de montrer la conjecture des premiers jumeaux. Il s'appelle *la barrière de parité* (ici, 'parité' se réfère à la parité du nombre de facteurs premiers d'un entier, e.g. de $p+2$).

Et les nombres premiers jumeaux ?

Sur une conjecture (une grande généralisation de l'hypothèse $BV(\theta)$), Polymath a montré que

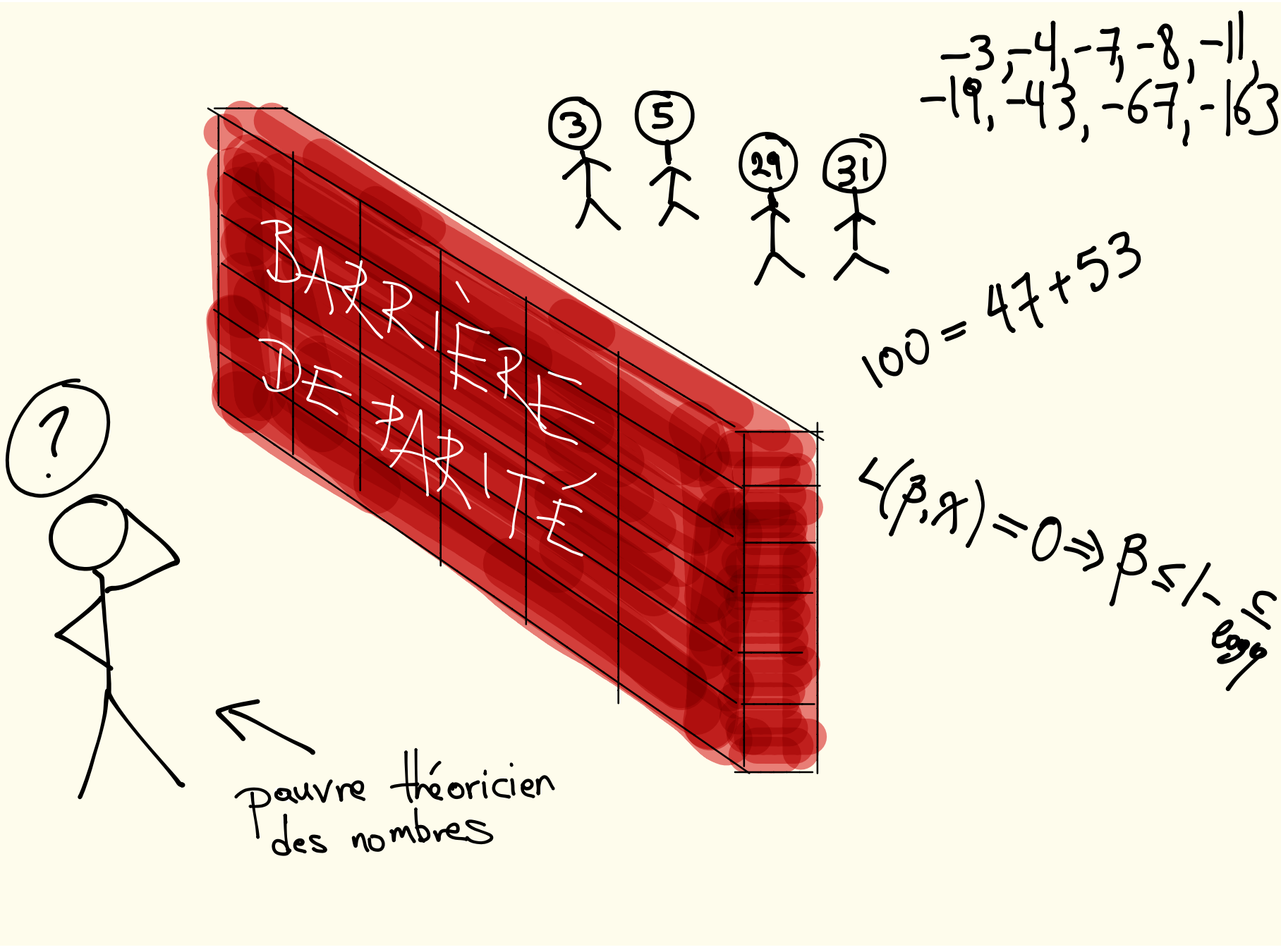
$$\liminf_{p\to\infty}(p^+ - p) \leq 6.$$

En fait, il a montré qu'il y a une infinité des premiers p tels que $p+2$ ou $p+6$ sont également premiers.

$$\#\{p : p+2 \text{ a un ou deux facteurs premiers}\} = \infty$$
$$\#\{p : p+2 \text{ ou } p+6 \text{ est premier}\} = \infty$$

Il y a un obstacle très subtile que ne nous permet pas de montrer la conjecture des premiers jumeaux. Il s'appelle *la barrière de parité* (ici, 'parité' se réfère à la parité du nombre de facteurs premiers d'un entier, e.g. de $p+2$).

Enlèvement de la barrière de parité ' $\Longrightarrow$ ' conjecture de Goldbach $(p+q=2N)$, conjecture des premiers jumeaux, nombres premiers de Germain ($p, 2p+1$ premiers), faible version de l'HRG, calcul des nombres de classe des corps de nombres,...


-3, -4, -7, -8, -11,
-19, -43, -67, -163
3
5
29
31
BARRIÈRE DE PARITÉ
100 = 47 + 53
L(β,π) = 0 ⇒ β ≤ 1 - log n
?
pauvre théoricien des nombres

Grands écarts entre les nombres premiers

En moyenne, $p^+ - p \sim \log p$. Est-ce qu'on peut montrer que

$$\limsup_{p\to\infty} \frac{p^+ - p}{\log p} = +\infty ?$$

Grands écarts entre les nombres premiers

En moyenne, $p^+ - p \sim \log p$. Est-ce qu'on peut montrer que

$$\limsup_{p\to\infty} \frac{p^+ - p}{\log p} = +\infty ?$$

Si $m = n!$, alors les nombres $m, m+1, \ldots, m+n$ sont composés.

Grands écarts entre les nombres premiers

En moyenne, $p^+ - p \sim \log p$. Est-ce qu'on peut montrer que

$$\limsup_{p\to\infty} \frac{p^+ - p}{\log p} = +\infty?$$

Si $m = n!$, alors les nombres $m, m+1, \ldots, m+n$ sont composés.

Ici $\log m = \log n! \sim n \log n$ et, donc, $n \sim \frac{\log m}{\log\log m}$.

Grands écarts entre les nombres premiers

En moyenne, $p^+ - p \sim \log p$. Est-ce qu'on peut montrer que

$$\limsup_{p\to\infty} \frac{p^+ - p}{\log p} = +\infty?$$

Si $m = n!$, alors les nombres $m, m+1, \ldots, m+n$ sont composés.

Ici $\log m = \log n! \sim n \log n$ et, donc, $n \sim \frac{\log m}{\log\log m}$.

On généralise : étant donné $z \geq 1$, on cherche H aussi grand que possible et classes de résidus $a_p \pmod p$, $p \leq z$, tels que $[1, H] \cap \mathbb{Z} \subset \bigcup_{p\leq z} \{a_p \pmod p\}$.

Grands écarts entre les nombres premiers

En moyenne, $p^+ - p \sim \log p$. Est-ce qu'on peut montrer que

$$\limsup_{p\to\infty} \frac{p^+ - p}{\log p} = +\infty?$$

Si $m = n!$, alors les nombres $m, m+1, \ldots, m+n$ sont composés.

Ici $\log m = \log n! \sim n \log n$ et, donc, $n \sim \frac{\log m}{\log\log m}$.

On généralise : étant donné $z \geq 1$, on cherche H aussi grand que possible et classes de résidus $a_p \pmod p$, $p \leq z$, tels que $[1, H] \cap \mathbb{Z} \subset \bigcup_{p\leq z}\{a_p \pmod p\}$.

Si $P = \prod_{p\leq z}$, il existe $m \in [P, 2P]$ tel que $m \equiv -a_p \pmod p$ pour tout $p \leq z$. Les nombres $m+1, \ldots, m+H$ sont composés.

Grands écarts entre les nombres premiers

En moyenne, $p^+ - p \sim \log p$. Est-ce qu'on peut montrer que

$$\limsup_{p\to\infty} \frac{p^+ - p}{\log p} = +\infty?$$

Si $m = n!$, alors les nombres $m, m+1, \ldots, m+n$ sont composés.

Ici $\log m = \log n! \sim n \log n$ et, donc, $n \sim \frac{\log m}{\log\log m}$.

On généralise : étant donné $z \geq 1$, on cherche H aussi grand que possible et classes de résidus $a_p \pmod p$, $p \leq z$, tels que $[1, H] \cap \mathbb{Z} \subset \bigcup_{p\leq z}\{a_p \pmod p\}$.

Si $P = \prod_{p\leq z}$, il existe $m \in [P, 2P]$ tel que $m \equiv -a_p \pmod p$ pour tout $p \leq z$. Les nombres $m+1, \ldots, m+H$ sont composés.

Rankin : $\exists c > 0$ t.q. $\max_{p\leq x} \frac{p^+ - p}{\log p} \geq c \frac{(\log\log x)(\log\log\log\log x)}{(\log\log\log x)^2}$.

Grands écarts entre les nombres premiers

En moyenne, $p^+ - p \sim \log p$. Est-ce qu'on peut montrer que

$$\limsup_{p\to\infty} \frac{p^+ - p}{\log p} = +\infty?$$

Si $m = n!$, alors les nombres $m, m+1, \ldots, m+n$ sont composés.

Ici $\log m = \log n! \sim n \log n$ et, donc, $n \sim \frac{\log m}{\log\log m}$.

On généralise : étant donné $z \geq 1$, on cherche H aussi grand que possible et classes de résidus $a_p \pmod p$, $p \leq z$, tels que $[1, H] \cap \mathbb{Z} \subset \bigcup_{p\leq z}\{a_p \pmod p\}$.

Si $P = \prod_{p\leq z}$, il existe $m \in [P, 2P]$ tel que $m \equiv -a_p \pmod p$ pour tout $p \leq z$.
Les nombres $m+1, \ldots, m+H$ sont composés.

Rankin : $\exists c > 0$ t.q. $\max_{p\leq x} \frac{p^+ - p}{\log p} \geq c \frac{(\log\log x)(\log\log\log\log x)}{(\log\log\log x)^2}$.

Erdős a offert \$10,000 pour remplacer c par une fonction $f(x) \to \infty$.

Grands écarts entre les nombres premiers

En moyenne, $p^+ - p \sim \log p$. Est-ce qu'on peut montrer que

$$\limsup_{p\to\infty} \frac{p^+ - p}{\log p} = +\infty?$$

Si $m = n!$, alors les nombres $m, m+1, \ldots, m+n$ sont composés.

Ici $\log m = \log n! \sim n \log n$ et, donc, $n \sim \frac{\log m}{\log\log m}$.

On généralise : étant donné $z \geq 1$, on cherche H aussi grand que possible et classes de résidus $a_p \pmod p$, $p \leq z$, tels que $[1,H] \cap \mathbb{Z} \subset \bigcup_{p\leq z}\{a_p \pmod p\}$.

Si $P = \prod_{p\leq z}$, il existe $m \in [P, 2P]$ tel que $m \equiv -a_p \pmod p$ pour tout $p \leq z$. Les nombres $m+1, \ldots, m+H$ sont composés.

Rankin : $\exists c > 0$ t.q. $\max_{p\leq x} \frac{p^+ - p}{\log p} \geq c \frac{(\log\log x)(\log\log\log\log x)}{(\log\log\log x)^2}$.

Erdős a offert \$10,000 pour remplacer c par une fonction $f(x) \to \infty$.

Maynard et Ford-Green-Konyagin-Tao ont résolu le défi d'Erdős à l'été 2014.

Grands écarts entre les premiers : conjectures

Rappelez le modèle (simple) de Cramér : $\{Y_k\}_{k\geq 3}$ var. aleat. ind. avec

$$\begin{cases} \mathbb{P}(Y_k = 1) = \dfrac{1}{\log k} \\ \mathbb{P}(Y_k = 0) = 1 - \dfrac{1}{\log k} \end{cases}$$

Grands écarts entre les premiers : conjectures

Rappelez le modèle (simple) de Cramér : $\{Y_k\}_{k\geq 3}$ var. aleat. ind. avec

$$\begin{cases} \mathbb{P}(Y_k = 1) = \dfrac{1}{\log k} \\ \mathbb{P}(Y_k = 0) = 1 - \dfrac{1}{\log k} \end{cases}$$

$$A_k = \{Y_k = 1,\ Y_{k+j} = 0\ (1 \leq j \leq c\log^2 k)\} \quad (k \geq 3).$$

$$\mathbb{P}(A_n) = \frac{1}{\log k} \prod_{j \leq c\log^2 k} \left(1 - \frac{1}{\log(k+j)}\right) \approx \frac{e^{-\frac{c\log^2 k}{\log k}}}{\log k} \approx \frac{1}{k^c \log k}$$

$$c > 1 \quad \Longrightarrow \quad \sum_{k\geq 1} \mathbb{P}(A_k) < \infty$$

Grands écarts entre les premiers : conjectures

Rappelez le modèle (simple) de Cramér : $\{Y_k\}_{k\geq 3}$ var. aleat. ind. avec

$$\begin{cases} \mathbb{P}(Y_k = 1) = \dfrac{1}{\log k} \\ \mathbb{P}(Y_k = 0) = 1 - \dfrac{1}{\log k} \end{cases}$$

$$A_k = \{Y_k = 1,\ Y_{k+j} = 0\ (1 \leq j \leq c\log^2 k)\} \quad (k \geq 3).$$

$$\mathbb{P}(A_n) = \frac{1}{\log k} \prod_{j \leq c\log^2 k} \left(1 - \frac{1}{\log(k+j)}\right) \approx \frac{e^{-\frac{c\log^2 k}{\log k}}}{\log k} \approx \frac{1}{k^c \log k}$$

$$c > 1 \quad \Longrightarrow \quad \sum_{k\geq 1} \mathbb{P}(A_k) < \infty$$

Borel-Cantelli $\Longrightarrow$ $\mathbb{P}(\limsup_{k\to\infty} A_k) = \mathbb{P}(A_k \text{ arrive pour une infinité de } k) = 0$

Grands écarts entre les premiers : conjectures

Rappelez le modèle (simple) de Cramér : $\{Y_k\}_{k\geq 3}$ var. aleat. ind. avec

$$\begin{cases} \mathbb{P}(Y_k = 1) = \dfrac{1}{\log k} \\ \mathbb{P}(Y_k = 0) = 1 - \dfrac{1}{\log k} \end{cases}$$

$$A_k = \{Y_k = 1,\ Y_{k+j} = 0\ (1 \leq j \leq c\log^2 k)\} \quad (k \geq 3).$$

$$\mathbb{P}(A_n) = \frac{1}{\log k} \prod_{j \leq c\log^2 k} \left(1 - \frac{1}{\log(k+j)}\right) \approx \frac{e^{-\frac{c\log^2 k}{\log k}}}{\log k} \approx \frac{1}{k^c \log k}$$

$$c > 1 \quad \Longrightarrow \quad \sum_{k\geq 1} \mathbb{P}(A_k) < \infty$$

Borel-Cantelli $\Longrightarrow$ $\mathbb{P}(\limsup_{k\to\infty} A_k) = \mathbb{P}(A_k \text{ arrive pour une infinité de } k) = 0$

Conjecture : $\max_{p\leq x}(p^+ - p) \sim c\log^2 x$, où $c = 1?, c = 2e^{-\gamma}?, c = ?$

Merci !