Le monde fascinant des nombres premiers

Un regard sur les travaux de James Maynard

Cédric Pilatte

Journées CGPE-ENS – Samedi 13 mai 2023

University of Oxford – Mathematical Institute

Plan de l'exposé

1. Introduction

2. Distribution des nombres premiers : échelle macroscopique

3. Distribution des nombres premiers : échelle microscopique

   Petits écarts entre les nombres premiers

   Grands écarts entre les nombres premiers

4. Approximations rationnelles de nombres réels

5. D'autres résultats de James Maynard

Introduction

Notations

Soient $f, g : \mathbb{R}^{>0} \to \mathbb{R}^{>0}$.

Notation	Signification
$f(x) \ll g(x)$ ou $f(x) = O(g(x))$	$f(x) \leqslant Cg(x)$ “$f(x) \leqslant 10^{100} g(x)$”
$f(x) \asymp g(x)$	$cg(x) \leqslant f(x) \leqslant Cg(x)$ “$10^{-100} g(x) \leqslant f(x) \leqslant 10^{100} g(x)$”
$f(x) \sim g(x)$	$\frac{f(x)}{g(x)} \to 1$ quand $x \to \infty$

- $\mathbb{N} = \{1, 2, \ldots\}$,
- “log” est le logarithme naturel,
- $|S|$ = nombre d’éléments de l’ensemble S,
- p est toujours un nombre premier,
- $\varphi(q)$ est le nombre d’entiers $1 \leqslant a < q$ premiers avec q.

À propos de James Maynard

- Doctorat obtenu en 2013 à Oxford (directeur : Roger Heath-Brown)
- Professeur à Oxford, 2017 (à 30 ans)
- Médaille Fields, 2022

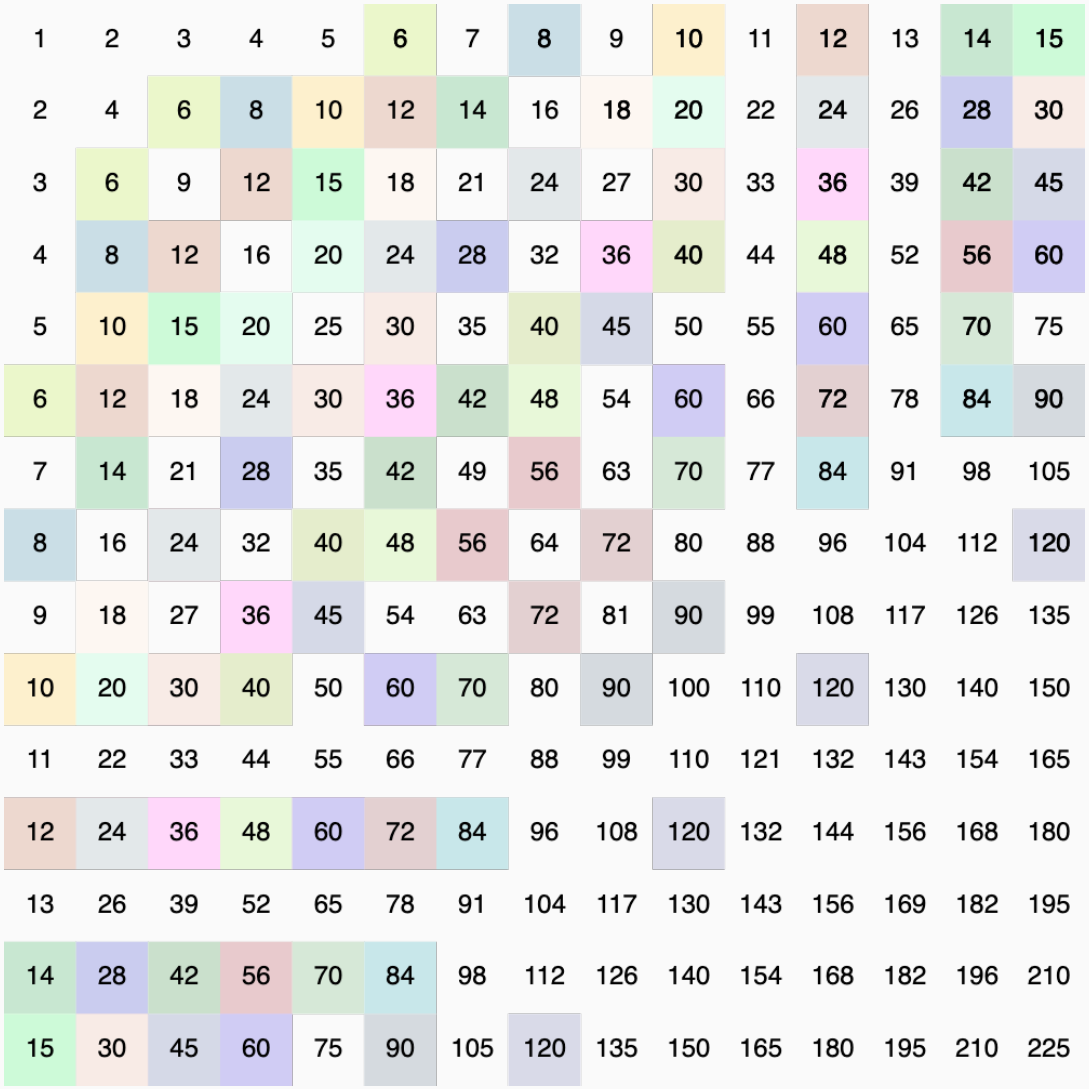
Pourquoi étudier les nombres premiers ?

- Applications (cryptographie, ...).
- Parmi les objets les plus naturels des mathématiques :

  "les constituants fondamentaux des nombres entiers".

- Pourtant, à bien des égards, il restent complètement mystérieux.

Combien de nombres dans la table de multiplication $N \times N$?



1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
3	6	9	12	15	18	21	24	27	30	33	36	39	42	45
4	8	12	16	20	24	28	32	36	40	44	48	52	56	60
5	10	15	20	25	30	35	40	45	50	55	60	65	70	75
6	12	18	24	30	36	42	48	54	60	66	72	78	84	90
7	14	21	28	35	42	49	56	63	70	77	84	91	98	105
8	16	24	32	40	48	56	64	72	80	88	96	104	112	120
9	18	27	36	45	54	63	72	81	90	99	108	117	126	135
10	20	30	40	50	60	70	80	90	100	110	120	130	140	150
11	22	33	44	55	66	77	88	99	110	121	132	143	154	165
12	24	36	48	60	72	84	96	108	120	132	144	156	168	180
13	26	39	52	65	78	91	104	117	130	143	156	169	182	195
14	28	42	56	70	84	98	112	126	140	154	168	182	196	210
15	30	45	60	75	90	105	120	135	150	165	180	195	210	225

Réponse (Ford, 2005) : $\asymp \dfrac{N^2}{(\log N)^{\delta}(\log\log N)^{3/2}}, \quad \delta = 1 - \dfrac{1+\log\log 2}{\log 2}.$

Les problèmes de Laudau (Congrès International Math. 1912)

1. Conjecture de Goldbach

Tout entier $n > 2$ *pair* est somme de deux nombres premiers.

2. Nombres premiers jumeaux

Il y a une infinité de p tels que $p + 2$ est aussi premier.

3. Conjecture de Legendre

Pour tout $n \geqslant 1$, il existe un nombre premier entre n^2 et $(n + 1)^2$.

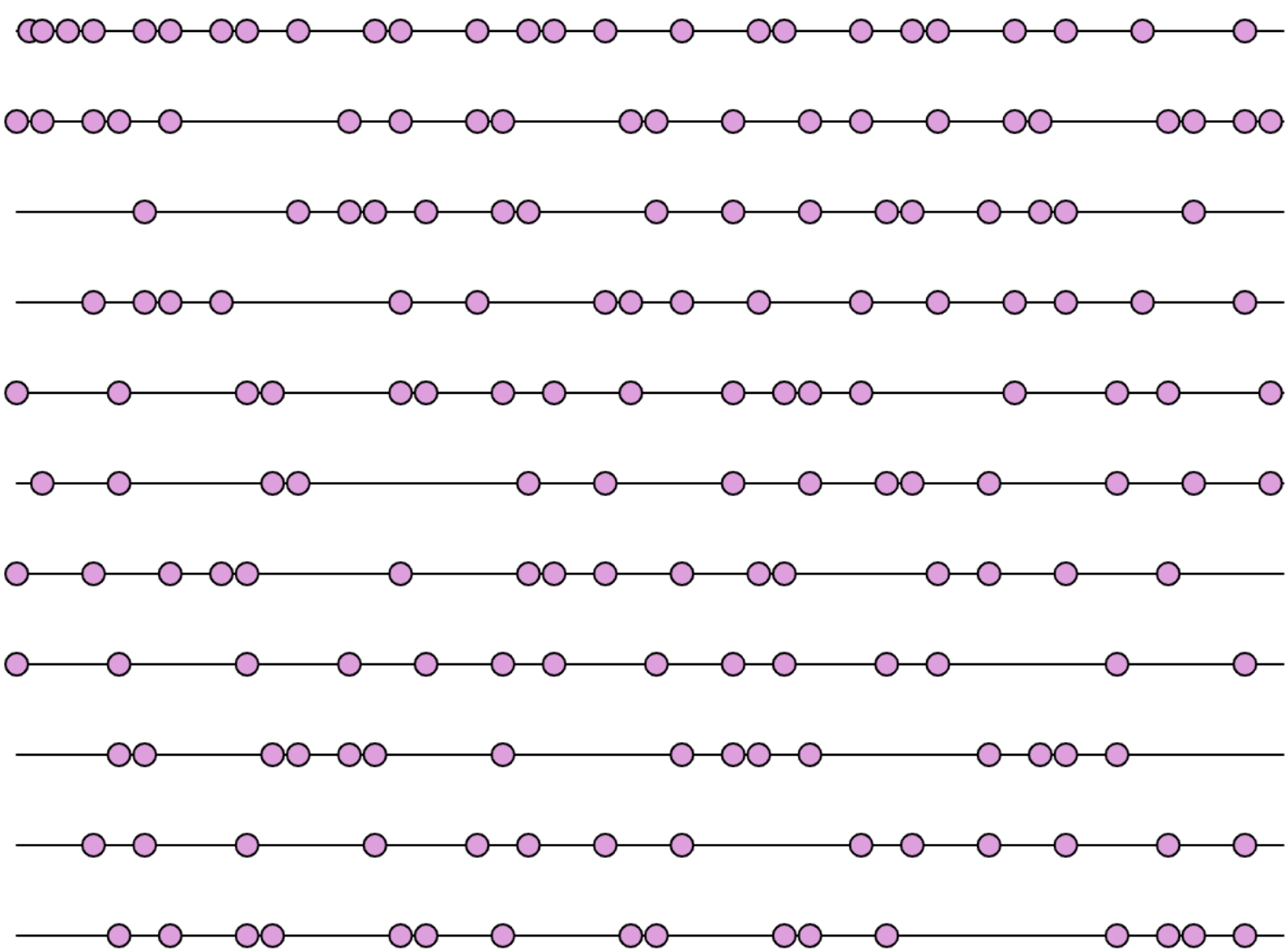
4. Valeurs premières de $n^2 + 1$

Il existe une infinité de nombres premiers de la forme $n^2 + 1$.

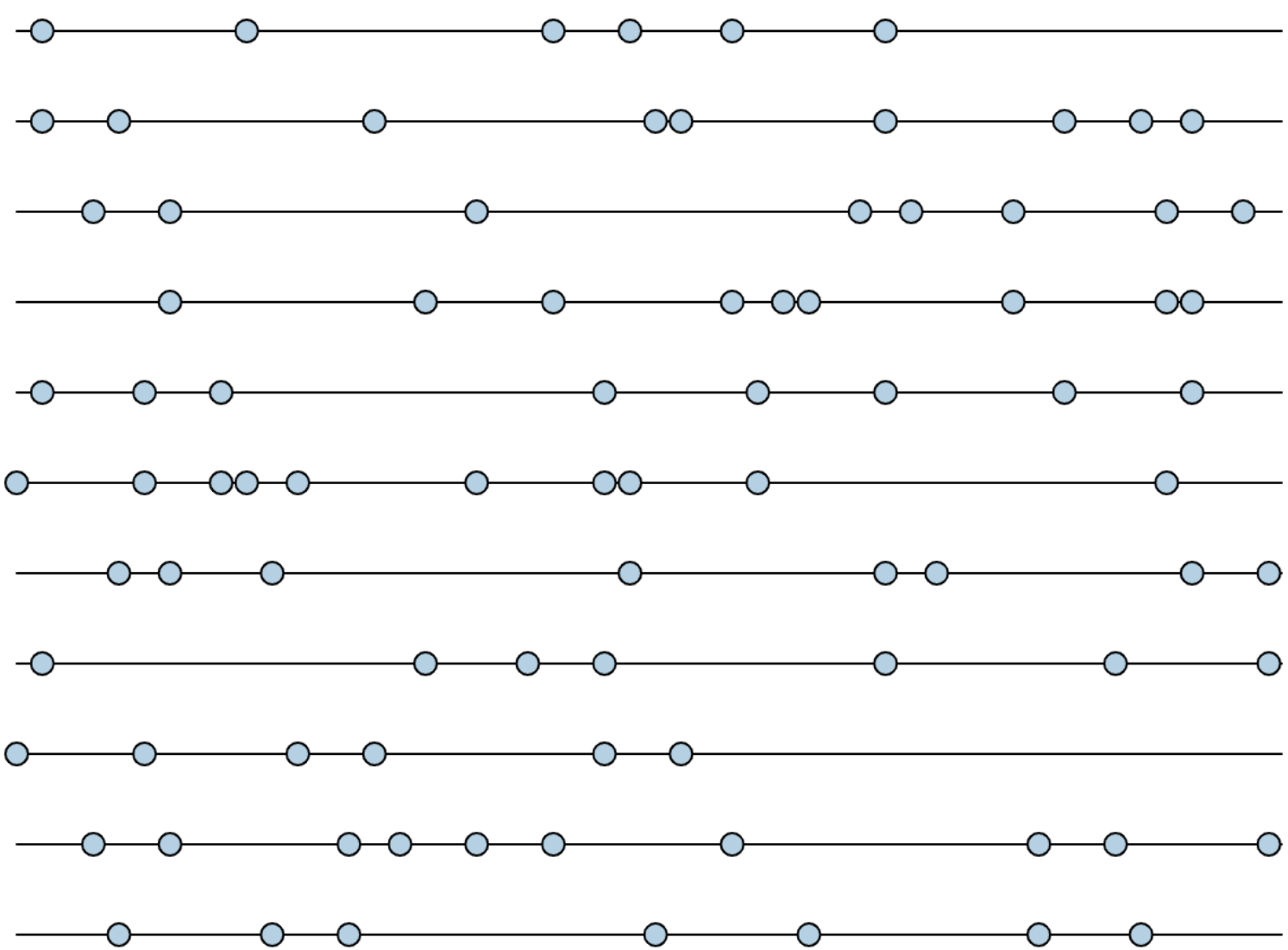
Les quatre problèmes sont toujours ouverts.

Distribution des nombres premiers : échelle macroscopique

Nombres premiers jusqu'à 1000



Nombres premiers entre 100 000 et 101 000



Naissance de la Théorie Analytique des Nombres

Combien de nombres premiers $\leqslant x$ (lorsque $x \to \infty$) ?

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

Gauss/Legendre (années 1790) ont conjecturé

$$\boxed{\pi(x) \sim \frac{x}{\log x}}$$

x	10^2	10^4	10^6	10^8	10^{10}	10^{12}	10^{14}
$\pi(x)$	25	1229	78498	5761455	455052512	37607912018	3204941750802
$x/\pi(x)$	4.000	8.137	12.739	17.357	21.975	26.590	31.202

Observation

Dernière ligne : semble croître $\approx$ linéairement avec l'exposant de 10 (augmente de ≈ 4.6 chaque fois)

Naissance de la Théorie Analytique des Nombres

Chebyshev (fin des années 1840) : démontre $\pi(x) \asymp x/\log x$.

Riemann (1859) : introduit l'idée d'utiliser l'analyse complexe pour étudier $\pi(x)$ via $\zeta(s)$.

Hadamard, De la Vallée Poussin (1896) : démontrent indépendamment le Théorème des Nombres Premiers

$$\pi(x) \sim \frac{x}{\log x}.$$

Terme principal et terme d'erreur

Le Théorème des Nombres Premiers dit que

$$\pi(x) = \underbrace{\frac{x}{\log x}}_{\text{terme principal}} + \underbrace{\varepsilon_1(x)\frac{x}{\log x}}_{\text{terme d'erreur}}$$

où $\varepsilon_1(x)$ est une fonction $\to 0$ quand $x \to \infty$.

Décroissance de $\varepsilon_1(x)$?

À quelle vitesse $\varepsilon_1(x) \to 0$?

Bornes plus précises pour $\pi(x)$

Définissons la fonction

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x}.$$

Alors (avec $\varepsilon_2(x) \to 0$)

$$\pi(x) = \mathrm{Li}(x) + \varepsilon_2(x)\frac{x}{\log x}.$$

x	$\pi(x)$	$\pi(x) - \frac{x}{\log x}$	$\pi(x) - \mathrm{Li}(x)$
10^{14}	3 204 941 750 802	$\approx$ 102 838 308 636	$\approx -314\,890$
		$3,2\%\,\pi(x)$	$-0,0000098\%\,\pi(x)$

L'Hypothèse de Riemann (ouvert)

$$|\pi(x) - \mathrm{Li}(x)| \ll x^{1/2}\log x.$$

Ce que l'on sait [1]

$$|\pi(x) - \mathrm{Li}(x)| \ll \frac{x}{(\log x)^{1\,000\,000}}.$$

1. Un résultat plus précis est donné par Vinogradov-Korobov (1958).

Distribution des nombres premiers : échelle microscopique

Écarts entre les nombres premiers

Soit p_n le n-ième nombre premier.

Question

Que peut-on dire sur l'écart $p_{n+1} - p_n$?

Dans l'intervalle $[1, x]$ il y a $\sim \frac{x}{\log x}$ nombres premiers.

L'écart moyen entre deux nombres premiers successifs dans $[1, x]$ est :

$$\frac{1}{\pi(x)} \sum_{p_{n+1} \leqslant x} (p_{n+1} - p_n) \sim \log x.$$

Et les cas extrêmes ?

Petits écarts entre les nombres premiers

Est-ce que $p_{n+1} - p_n$ peut être petit (p.ex. $\leqslant 2$) pour une infinité de n ?

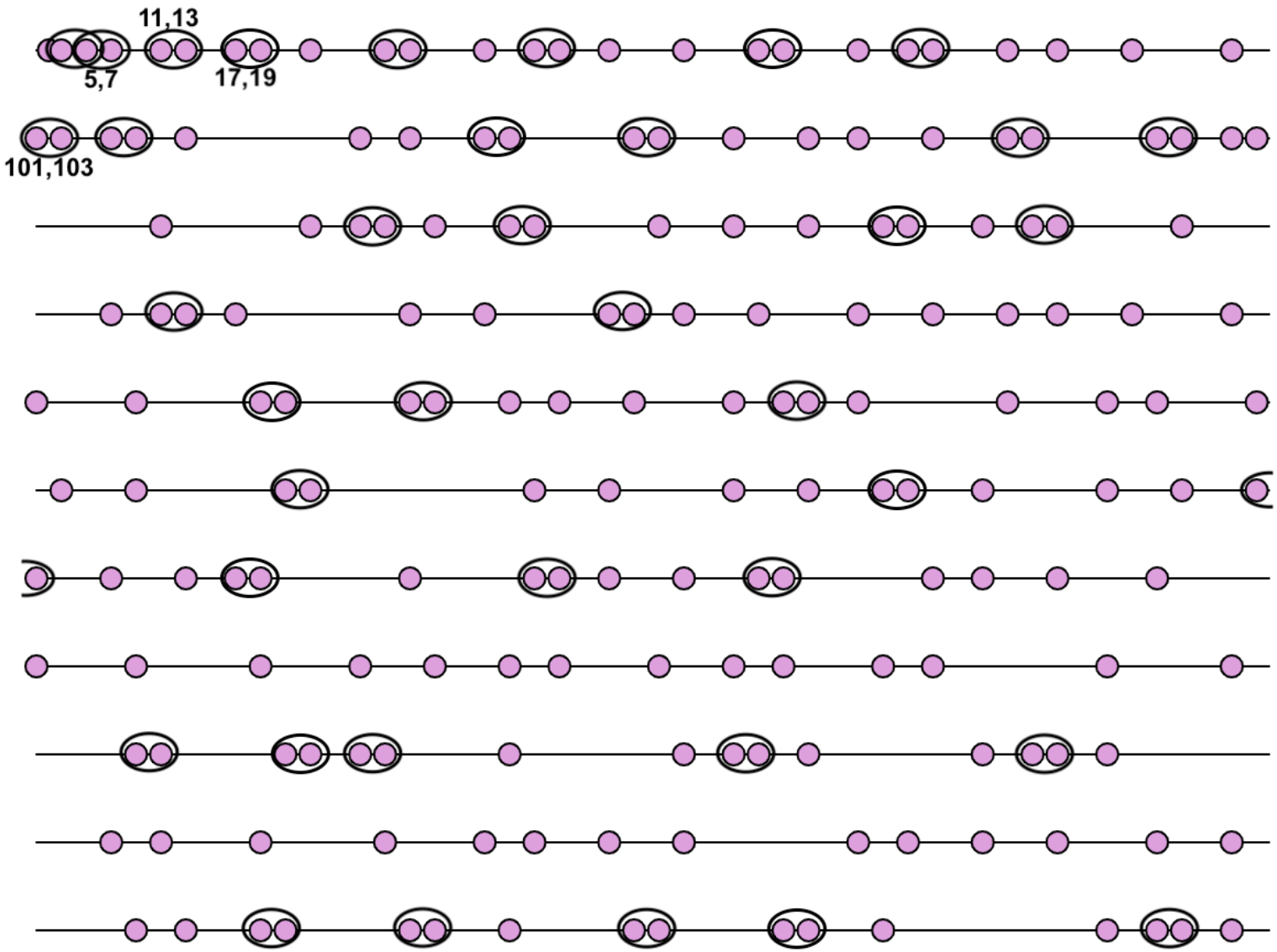
Grands écarts entre les nombres premiers

Quel est le plus grand écart $p_{n+1} - p_n$ avec $p_n \leqslant x$, quand $x \to \infty$?

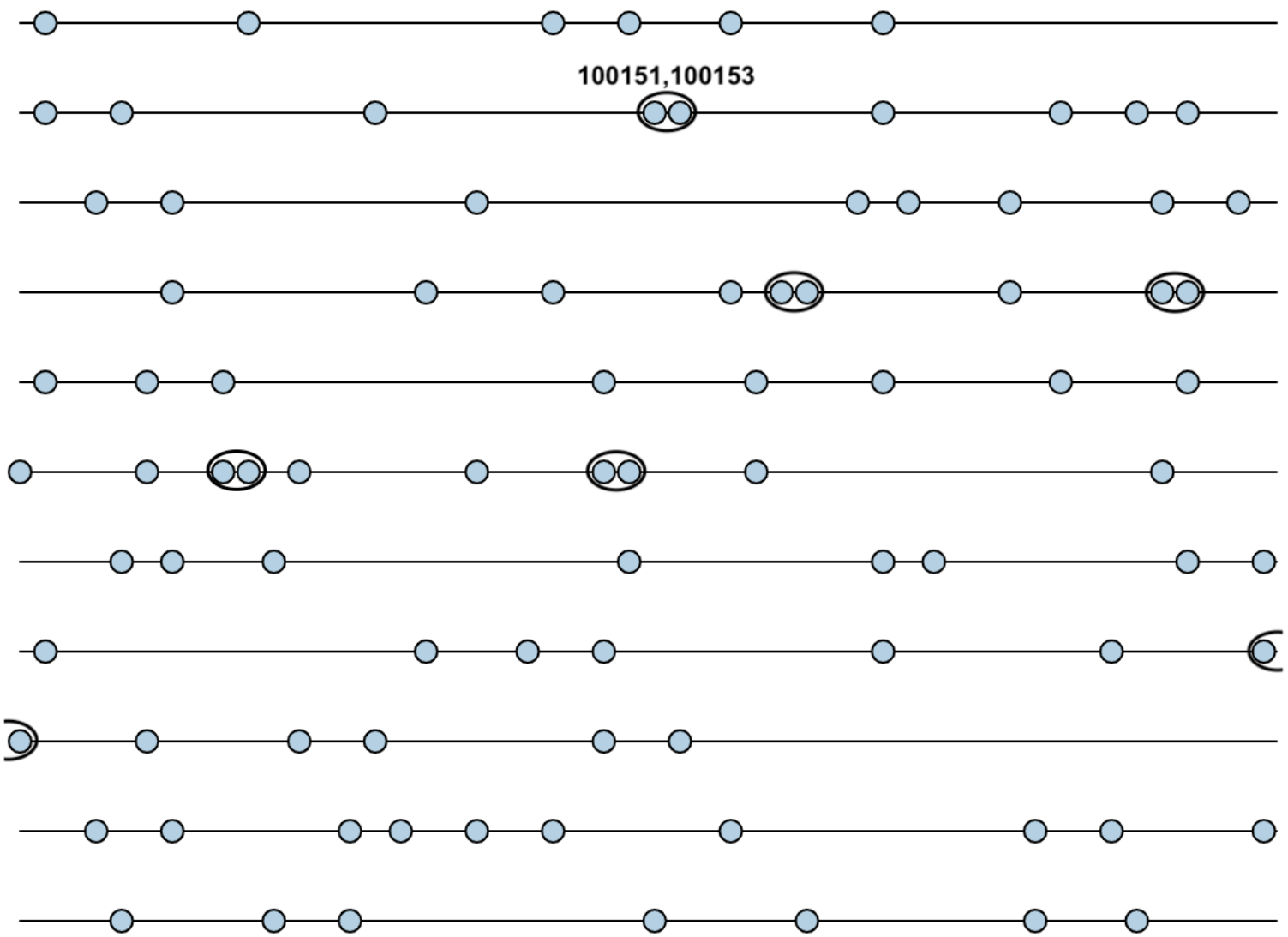
Distribution des nombres premiers : échelle microscopique

Petits écarts entre les nombres premiers

Paires de nombres premiers jumeaux jusqu'à 1000



Paires de nombres premiers jumeaux entre 100 000 et 101 000



Pourquoi pense-t-on qu'il y a une infinité de nombres premiers jumeaux ?

Cramér : modèle probabiliste pour les nombres premiers

Pour chaque $n \geqslant 1$, indépendamment, on "lance une pièce" biaisée :

	`Pile`	`Face`
Probabilité	$\frac{1}{\log n}$	$1 - \frac{1}{\log n}$

Soit $\mathcal{P}$ la suite (aléatoire) d'entiers $n \geqslant 1$ où on a obtenu `Pile`. Alors

$$\mathbb{E}\Big[\sum_{n \leqslant x} 1_{n \in \mathcal{P}} 1_{n+2 \in \mathcal{P}}\Big] \sim \frac{x}{(\log x)^2}$$

est le nombre de paires de nombres premiers jumeaux $\leqslant x$ prédites par le modèle de Cramér.

Modèle de Cramér-Granville

On peut raffiner le modèle de Cramér :

- ne lancer une pièce que quand n est impair,
- ne lancer une pièce que quand n n'est pas divisible par 2 et 3,
- $\dots$
- ne lancer une pièce que quand n n'est pas divisible par $2, 3, 5, \dots, p_k$, puis faire tendre k vers $+\infty$.

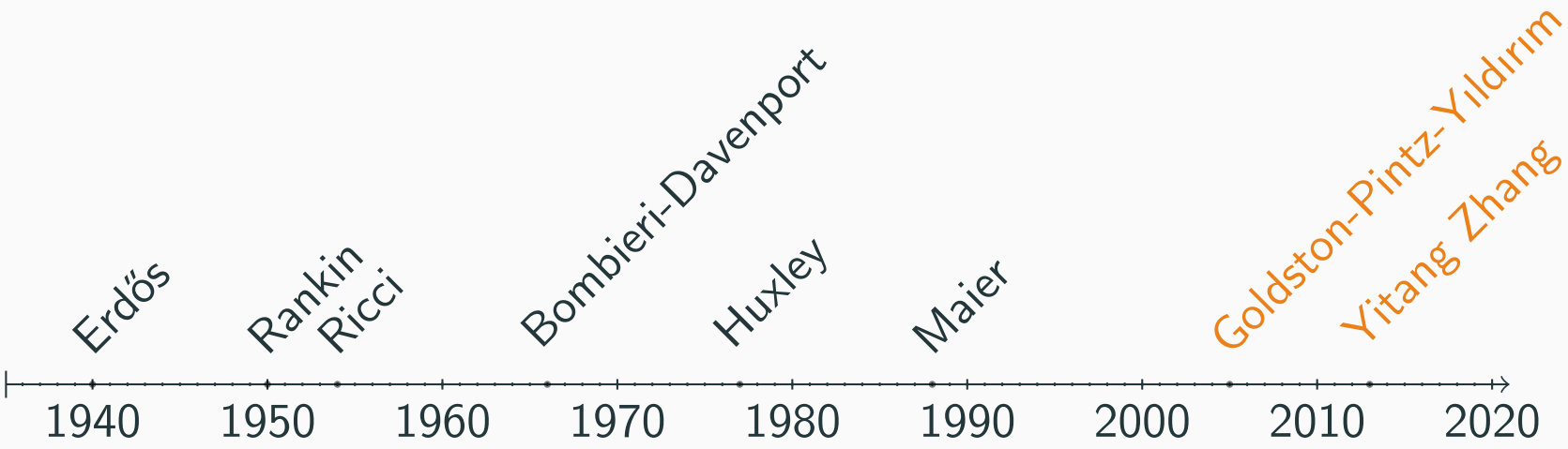
Conjecture

Le nombre de paires de nombres premiers jumeaux $(p, p+2)$ avec $p \leqslant x$ est

$$\sim c_2 \frac{x}{(\log x)^2}$$

où $c_2 = 2\prod_{p \geqslant 3}(1-2/p)(1-1/p)^{-2} \approx 1.3203$.

Petits écarts : historique des résultats



Il existe une infinité de n tels que

- (Avant 2005) $p_{n+1} - p_n \leqslant c \log p_n$ pour un certain $c < 1$,
- (GPY, 2005) $p_{n+1} - p_n \leqslant \varepsilon \log p_n$ pour tout $\varepsilon > 0$ donné,
- (Zhang, 2013) $p_{n+1} - p_n \leqslant 70\,000\,000$.

Zoom sur l'année 2013

Borne supérieure pour une infinité de $p_{n+1} - p_n$

- (Avril) Zhang : 70 000 000
- (Juin - Octobre) le projet Polymath8a : 4680
- (Novembre) Maynard : 600
- (Novembre 2013 - Juin 2014) Polymath8b : 246

Petits intervalles avec beaucoup de nombres premiers

Théorème (Zhang, 2013)

Pour $C = 70\,000\,000$, il existe une infinité d'intervalles $[n, n + C]$ contenant $\geqslant 2$ nombres premiers.

Maynard a introduit de nouvelles méthodes pour démontrer l'existence d'une infinité de "groupements" de m nombres premiers pour chaque m.

Théorème (Maynard, 2013) [2]

Pour tout $m \geqslant 2$, il existe une borne $B(m)$ avec la propriété suivante : il existe une infinité d'intervalles $[n, n + B(m)]$ contenant $\geqslant m$ nombres premiers.

De plus, Maynard montre que l'on peut prendre $B(m) \ll m^3 e^{4m}$.

2. +Tao

Distribution des nombres premiers : échelle microscopique

Grands écarts entre les nombres premiers

Grands écarts : différents modèles probabilistes

Soit

$$G(x) = \max_{p_{n+1} \leqslant x} (p_{n+1} - p_n)$$

le plus grand trou/écart entre deux nombres premiers $\leqslant x$.

La situation est plus délicate :

$G(x) \sim (\log x)^2$	modèle de Cramér
$G(x) \geqslant (2e^{-\gamma} - \varepsilon)(\log x)^2$	modèle de Cramér-Granville ($2e^{-\gamma} \approx 1.12$)
$G(x) \ll (\log x)^2 \frac{\log\log x}{\log\log\log x}$	modèle de Banks-Ford-Tao
$G(x) \sim 2e^{-\gamma} (\log x)^2$	modèle de Banks-Ford-Tao + conjectures

> *"It is evident that the primes are randomly distributed but, unfortunately, we don't know what 'random' means.*
> *— R. C. Vaughan (1990)"*

Taille du plus grand trou : bornes inférieures

On sait : il existe $p_n \leqslant x$ tel que l'écart $p_{n+1} - p_n$ est plus grand que

$(\log x)V(x)$, pour une fonction $V(x) \to +\infty$	Westzynthius (1931)
$(\log x)\dfrac{c_0(\log\log x)(\log\log\log\log x)}{(\log\log\log x)^2}$	Erdős-Rankin (1935)

Erdős a offert \$10 000 à quiconque pourrait améliorer cette borne.

Défi relevé par

1. Ford-Green-Konyagin-Tao (20 Août 2014) ,
2. and Maynard (21 Août 2014).

Ensemble, il ont montré qu'il y a une infinité de x pour lesquels

$$G(x) \gg (\log x)\frac{(\log\log x)(\log\log\log\log x)}{\log\log\log x}.$$

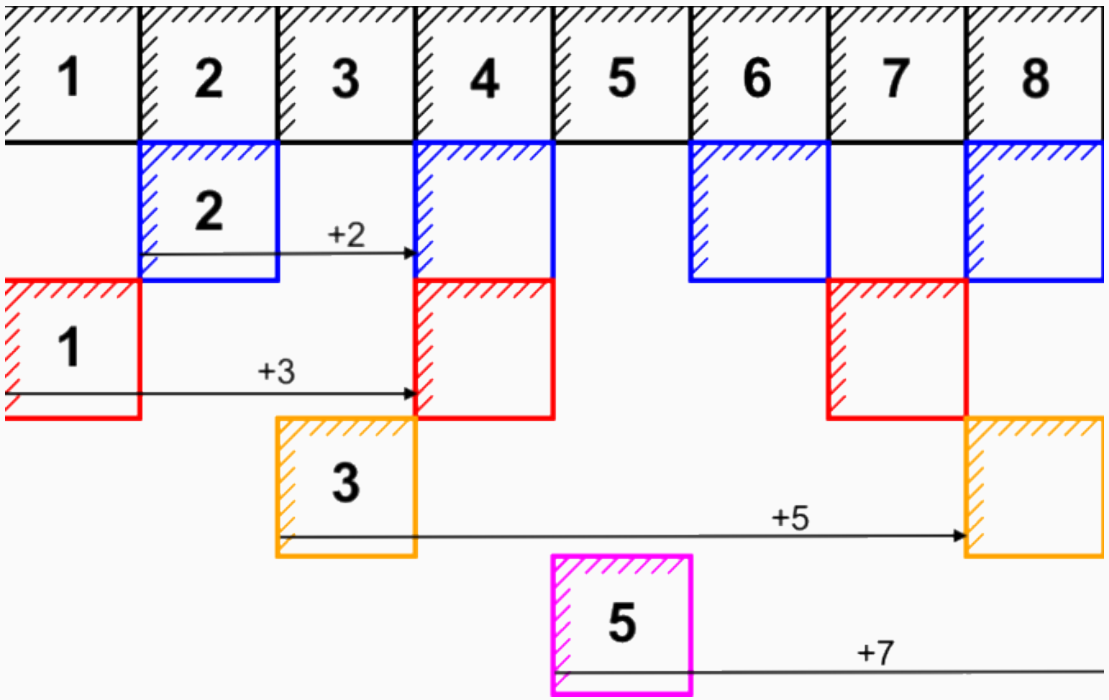
Stratégie de preuve : recouvrement par congruences

Soit $N \in \mathbb{N}$. But : trouver un k, le plus petit possible, et des entiers $a_1, \ldots, a_k$, tels que l'intervalle

$$\{1, 2, \ldots, N\}$$

est entièrement recouvert par les progressions arithmétiques

$$a_1 + p_1\mathbb{Z},\ a_2 + p_2\mathbb{Z},\ \ldots,\ a_k + p_k\mathbb{Z}.$$



Approximations rationnelles de nombres réels

$$\pi = 3.14159265...$$

Approximations “efficaces” :

$$\frac{22}{7} = 3.14285714...$$

$$\frac{355}{113} = 3.14159292...$$

$$\vdots$$

À comparer avec $\frac{31\,415\,927}{10\,000\,000}$.

Résultat classique

Théorème d'approximation de Dirichlet

Pour tout $\alpha \in \mathbb{R}$ il existe une infinité de $a, q \in \mathbb{Z}$ tels que

$$\left|\alpha - \frac{a}{q}\right| \leqslant \frac{1}{q^2}.$$

Se déduit facilement du résultat suivant :

Théorème d'approximation de Dirichlet, version 2

Soit $D \in \mathbb{N}$. Pour tout $\alpha \in \mathbb{R}$ il existe $a, q \in \mathbb{Z}$ tels que $1 \leqslant q \leqslant D$ et

$$\left|\alpha - \frac{a}{q}\right| \leqslant \frac{1}{qD}.$$

Théorème d'approximation de Dirichlet, version 2

Soit $D \in \mathbb{N}$. Pour tout $\alpha \in \mathbb{R}$ il existe $a, q \in \mathbb{Z}$ tels que $1 \leqslant q \leqslant D$ et

$$\left|\alpha - \frac{a}{q}\right| \leqslant \frac{1}{qD}.$$

Démonstration.

On considère les $D+1$ nombres $0, \{\alpha\}, \{2\alpha\}, \{3\alpha\}, \ldots, \{D\alpha\}$, où $\{x\}$ est la partie fractionnaire de x.

Comme ils sont tous dans $[0,1[$ on peut en trouver deux, disons $\{n\alpha\}$ et $\{m\alpha\}$ (avec $n \neq m$), tels que

$$|\{n\alpha\} - \{m\alpha\}| \leqslant \frac{1}{D}.$$

Alors, comme $\{x\} = x - \lfloor x \rfloor$, il existe un entier h tel que $|(n-m)\alpha + h| \leqslant \frac{1}{D}$, et donc $\left|\alpha - \frac{h}{n-m}\right| \leqslant \frac{1}{(n-m)D}$. □

Améliorer et généraliser le thm d'approximation de Dirichlet ?

Généraliser

Peut-on ajouter des contraintes sur le dénominateur q, par exemple demander que q soit premier ?

Améliorer

Peut-on remplacer $1/q^2$ par une fonction qui tend plus vite vers 0 ?

Si $\alpha = \frac{1+\sqrt{5}}{2}$, alors $\left|\alpha - \frac{a}{q}\right| \geqslant \frac{3}{8q^2}$ pour tous $a, q \in \mathbb{Z}$.

Conclusion : autoriser un petit ensemble d'exceptions

On remplace "pour tout $\alpha \in \mathbb{R}$" par "pour presque tout $\alpha \in \mathbb{R}$".

Presque tout = au sens de la mesure/des probabilités

Résultats pour “presque tout” α

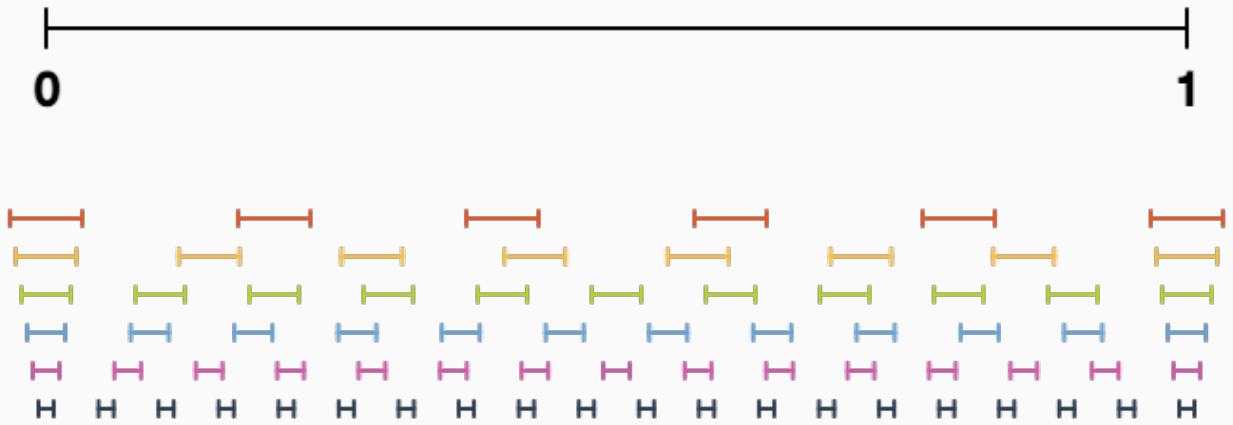
Théorème (Khintchine, 1924)

Critère exact pour déterminer quelles suites $\varepsilon_1, \varepsilon_2, \ldots \geqslant 0$ décroissantes ont la propriété suivante.

Pour presque tout $\alpha \in [0,1]$, il y a une infinité de $a, q \in \mathbb{Z}$ tels que

$$\left|\alpha - \frac{a}{q}\right| \leqslant \frac{\varepsilon_q}{q^2}.$$

Le critère : divergence ou convergence de $\sum_{q \geqslant 1} q\varepsilon_q$.



Corollaire

Soit $\varepsilon > 0$. Pour presque tout $\alpha \in [0,1]$:

- il existe une infinité de $a, q \in \mathbb{Z}$ tels que $\left|\alpha - \frac{a}{q}\right| \leqslant \frac{1}{q^2 \log q}$,
- il existe un nombre fini de $a, q \in \mathbb{Z}$ tels que $\left|\alpha - \frac{a}{q}\right| \leqslant \frac{1}{q^2 (\log q)^{1+\varepsilon}}$.

Résultats pour "presque tout" α

Théorème (Duffin-Schaeffer, 1941) [3]

Soit $\varepsilon > 0$. Pour presque tout $\alpha \in [0,1]$, il existe une infinité de $a \in \mathbb{Z}$ et p premier tels que

$$\left|\alpha - \frac{a}{p}\right| \leqslant \frac{1}{p^{2-\varepsilon}}.$$

Comparer avec ce que l'on sait pour tout α :

Théorème (Matomäki, 2009)

Soit $\varepsilon > 0$. Pour tout irrationel $\alpha \in [0,1]$, il existe une infinité de $a \in \mathbb{Z}$ et p premier tels que

$$\left|\alpha - \frac{a}{p}\right| \leqslant \frac{1}{p^{4/3-\varepsilon}}.$$

3. Le théorème est plus général et plus précis.

Le critère ultime

Pour $\Delta_1, \Delta_2, \ldots \geqslant 0$, on définit

$$\mathscr{L}_0 = \left\{\alpha \in [0,1] : \left|\alpha - \frac{a}{q}\right| \leqslant \Delta_q \text{ pour une infinité de } a, q \in \mathbb{N}\right\}$$

$$\mathscr{L} = \left\{\alpha \in [0,1] : \left|\alpha - \frac{a}{q}\right| \leqslant \Delta_q \text{ pour une infinité de } a, q \in \mathbb{N} \text{ premiers entre eux}\right\}.$$

Conjecture de Duffin-Schaeffer (1941)

- Si $\sum_{q\geqslant 1} \varphi(q)\Delta_q < \infty$, alors $\mathrm{mesure}(\mathscr{L}) = 0$.
- Si $\sum_{q\geqslant 1} \varphi(q)\Delta_q = \infty$, alors $\mathrm{mesure}(\mathscr{L}) = 1$.

Corollaire : Conjecture de Catlin (1976)

- Si $\sum_{q\geqslant 1} \varphi(q)\widetilde{\Delta_q} < \infty$, alors $\mathrm{mesure}(\mathscr{L}_0) = 0$.
- Si $\sum_{q\geqslant 1} \varphi(q)\widetilde{\Delta_q} = \infty$, alors $\mathrm{mesure}(\mathscr{L}_0) = 1$.

Théorème (Koukoulopoulos-Maynard, 2020)

La conjecture de Duffin-Schaeffer (et donc celle de Catlin) est vraie.

D'autres résultats de James Maynard

Nombres premiers dans les progressions arithmétiques

Question fondamentale

Soient $q \geqslant 1$ et $a \in \mathbb{Z}$ premier avec q.

Combien y a-t-il de nombres premiers $p \leqslant x$ tels que $p \equiv a \pmod{q}$?

Pour $q = 1$, on retrouve le Théorème des Nombres Premiers, l'Hypothèse de Riemann, etc.

Soit $\pi(x; a, q) = \{p \leqslant x : p \equiv a \pmod{q}\}$.

Théorème de Siegel-Walfisz (1936)

$$\pi(x; a, q) = \frac{\mathrm{Li}(x)}{\varphi(q)} + O\left(\frac{x}{(\log x)^{1\,000\,000}}\right)$$

Hypothèse de Riemann Généralisée

$$\pi(x; a, q) = \frac{\mathrm{Li}(x)}{\varphi(q)} + O\left(x^{1/2} \log x\right)$$

L'Hypothèse de Riemann Généralisée implique que

$$\pi(x; a, q) \sim \frac{\mathrm{Li}(x)}{\varphi(q)} \tag{1}$$

seulement lorsque $q \leqslant x^{1/2-\varepsilon}$ alors que $q \leqslant x^{1-\varepsilon}$ devrait être suffisant.

Maynard parvient à dépasser cette barrière de $1/2$ dans certaines situations favorables.

Maynard (résultats techniques)

11 Juin 2020 : "Primes in arithmetic progressions to large moduli I : Fixed residue classes" (102 p.)

12 Juin 2020 : "Primes in arithmetic progressions to large moduli II : Well-factorable estimates" (26 p.)

15 Juin 2020 : "Primes in arithmetic progressions to large moduli III : Uniform residue classes" (79 p.)

Valeurs premières de polynômes à plusieurs variables

Appelons un polynôme (à plusieurs variables et à coefficients entiers) peu dense s'il prend $\ll x^c$ valeurs dans l'intervalle $[1, x]$, pour un $c < 1$.

Friedlander-Iwaniec (1998)

Il y a une infinité de nombres premiers de la forme $a^2 + b^4$.

Heath-Brown (2001)

Il y a une infinité de nombres premiers de la forme $a^3 + 2b^3$.

Avant Maynard, il s'agissait des seuls exemples de polynômes peu denses pour lesquels on pouvait démontrer qu'ils prennent une infinité de valeurs premières.

Maynard (2015) : "Primes represented by incomplete norm forms"

Donne une famille infinie de polynômes peu denses, chacun prenant une infinité de valeurs premières.

Revenons aux problèmes de Landau (CIM 1912)

1. Conjecture de Goldbach

Tout entier $n > 2$ pair est somme de deux nombres premiers.

2. Premiers jumeaux – petits écarts entre nombres premiers

Il y a une infinité de p tels que $p + 2$ est aussi premier.

3. Conjecture de Legendre – grands écarts entre nombres premiers

Pour tout $n \geqslant 1$, il existe un nombre premier entre n^2 et $(n + 1)^2$.

4. Valeurs premières de $n^2 + 1$ — valeurs premières de polynômes

Il existe une infinité de nombres premiers de la forme $n^2 + 1$.

Revenons aux problèmes de Landau (CIM 1912)

1. Conjecture de Goldbach

Tout entier $n > 2$ pair est somme de deux nombres premiers.

Théorème (Vinogradov, 1930)

Tout entier impair n suffisamment grand est somme de trois nombres premiers.

Matomäki-Maynard-Shao (2016)

Soit $\varepsilon > 0$. Tout entier impair n suffisamment grand s'écrit comme somme de trois nombres premiers

$$p_1, p_2, p_3 \in \left[n/3 - n^{0.55+\varepsilon},\ n/3 + n^{0.55+\varepsilon}\right].$$

Remarque : on ne sait même pas s'il existe un nombre premier dans l'intervalle $[x, x + x^{0.52}]$ pour tout x suffisamment grand.

Nombres premiers avec chiffres restreints

Maynard (2016)

Soit $a_0 \in \{0, \ldots, 9\}$. Il y a une infinité de nombres premiers p dont l'écriture décimale ne contient pas le chiffre a_0.

La probabilité qu'un nombre "aléatoire" à n chiffres n'ait pas de chiffre 7 en base 10 est $\approx (9/10)^n$.

Plus précisément, il y a $\asymp x^{\log_{10} 9}$ nombres $\leqslant x$ sans 7 dans leur écriture décimale : c'est un ensemble très peu dense.

“James Maynard reçoit la médaille Fields 2022 pour ses contributions à la théorie analytique des nombres, qui ont conduit à des avancées majeures dans la compréhension de la structure des nombres premiers et dans l’approximation diophantienne.
— Union Mathématique Internationale”

Merci pour votre attention !