Pseudo-aléa des chiffres des nombres premiers

Cathy Swaenepoel

IMJ-PRG, Université Paris Cité.

Mathématiques en mouvement,

IHP, 15 novembre 2025.

Soit $b \geqslant 2$.

Écriture d'un entier positif $k < b^n$ in base b :

$$k = \sum_{j=0}^{n-1} \varepsilon_j(k)\, b^j$$

où $\varepsilon_j(k) \in \{0, \ldots, b-1\}$ est le **chiffre** de k à la position j.

- En base 10, les chiffres appartiennent à $\{0, \ldots, 9\}$.

$$2025 = 2 \cdot 10^3 + 0 \cdot 10^2 + 2 \cdot 10^1 + 5 \cdot 10^0$$

- En base 2, les chiffres sont 0 ou 1 (écriture binaire).

$$2025 = 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 + 2^5 + 2^3 + 2^0 = (11111101001)_2$$

Chiffres comme variables aléatoires

$\varepsilon_j(k) =$ chiffre de k à la position j (en base b).

On choisit un entier positif $k < b^n$ au hasard.

$\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}$ peuvent être vus comme des variables aléatoires i.i.d..

- Chaque ε_j suit une loi uniforme : pour tout chiffre c,

$$\mathbb{P}(\varepsilon_j = c) = \frac{1}{b}.$$

- $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}$ sont indépendantes.
  Par exemple, pour toutes positions $j_1 \neq j_2$ et tous chiffres c_1, c_2,

$$\mathbb{P}(\varepsilon_{j_1} = c_1 \text{ et } \varepsilon_{j_2} = c_2) = \mathbb{P}(\varepsilon_{j_1} = c_1)\,\mathbb{P}(\varepsilon_{j_2} = c_2) = \frac{1}{b^2}.$$

Somme des chiffres binaires

Ici $b = 2$. On note $s_2(k)$ la somme des chiffres binaires de k : pour $0 \leqslant k < 2^n$,

$$s_2(k) = \sum_{j=0}^{n-1} \varepsilon_j(k) = \text{nombre de 1 dans l'écriture binaire de } k.$$
(population count, poids de Hamming)

s_2 suit une loi binomiale de paramètres n et $p = \frac{1}{2}$.

$$\mathbb{P}(s_2 = \ell) = \frac{1}{2^n}\binom{n}{\ell} \qquad (0 \leqslant \ell \leqslant n).$$

Chiffres d'entiers *intéressants*

Soit E un sous-ensemble infini *intéressant* de $\mathbb{N}$.

Les chiffres des entiers de E se comportent-ils comme les chiffres de tous les entiers ?

Chiffres d'entiers *intéressants*

Soit E un sous-ensemble infini *intéressant* de $\mathbb{N}$.

Les chiffres des entiers de E se comportent-ils comme les chiffres de tous les entiers ?

Soit P une propriété des chiffres.

Problème : Pour un grand nombre entier x, comparer

- la proportion, parmi les entiers de $[0, x] \cap E$, des entiers dont les chiffres vérifient la propriété P :
$$\frac{|\{k \in [0, x] \cap E : \text{les chiffres de } k \text{ vérifient } P\}|}{|[0, x] \cap E|},$$
- la proportion, parmi les entiers de $[0, x] \cap \mathbb{N}$, des entiers dont les chiffres vérifient la propriété P :
$$\frac{|\{k \in [0, x] \cap \mathbb{N} : \text{les chiffres de } k \text{ vérifient } P\}|}{|[0, x] \cap \mathbb{N}|}.$$

Chiffres d'entiers *intéressants*

Soit E un sous-ensemble infini *intéressant* de $\mathbb{N}$.

Les chiffres des entiers de E se comportent-ils comme les chiffres de tous les entiers ?

Soit P une propriété des chiffres.

Problème : Pour un grand nombre entier x, comparer

- la proportion, parmi les entiers de $[0, x] \cap E$, des entiers dont les chiffres vérifient la propriété P :
$$\frac{|\{k \in [0, x] \cap E : \text{les chiffres de } k \text{ vérifient } P\}|}{|[0, x] \cap E|},$$
- la proportion, parmi les entiers de $[0, x] \cap \mathbb{N}$, des entiers dont les chiffres vérifient la propriété P :
$$\frac{|\{k \in [0, x] \cap \mathbb{N} : \text{les chiffres de } k \text{ vérifient } P\}|}{|[0, x] \cap \mathbb{N}|}.$$

Si les deux proportions sont proches alors les chiffres des entiers de E sont *pseudo-aléatoires* pour la propriété P.

Difficulté : sur E, les chiffres ne sont plus des variables aléatoires i.i.d. !

Ensembles E *intéressants*

écriture en base b $\longleftrightarrow$ décomposition en facteurs premiers

L'étude des liens entre la structure additive et la structure multiplicative des entiers fait partie des sujets parmi les plus importants en théorie des nombres.

Exemples d'ensembles E *intéressants* : des ensembles d'entiers avec une décomposition en facteurs premiers particulière, comme :

- les nombres premiers,
- les carrés, les cubes, ...,
- les entiers sans facteur carré,
- les nombres friables.

Nombres premiers

Un nombre entier $k \geqslant 2$ est un nombre premier si ses seuls diviseurs sont 1 et k :

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19, \ldots$$

La lettre p désignera un nombre premier.

On note $\pi(x)$ le nombre de nombres premiers plus petits que x.

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

$$\pi(x) \sim \frac{x}{\log x} \qquad (x \to +\infty).$$

Nombres premiers dont les chiffres vérifient certaines propriétés

1. Nombres premiers dont la somme des chiffres est congrue à a modulo m (Mauduit–Rivat).

2. Nombres premiers dont la somme des chiffres est égale à ℓ (Drmota–Mauduit–Rivat).

3. Nombres premiers avec un chiffre interdit (Maynard).

Nombres premiers dont les chiffres vérifient certaines propriétés

1. Nombres premiers dont la somme des chiffres est congrue à a modulo m (Mauduit–Rivat).
2. Nombres premiers dont la somme des chiffres est égale à ℓ (Drmota–Mauduit–Rivat).
3. Nombres premiers avec un chiffre interdit (Maynard).

Théorème (Gelfond, 1968)

Pour tous entiers $q \geqslant 1$, $m \geqslant 1$, $c \in [\![0, q-1]\!]$, $a \in [\![0, m-1]\!]$,

$$|\{k \leqslant x : k \equiv c \bmod q,\ s_2(k) \equiv a \bmod m\}| \underset{x \to +\infty}{\sim} \frac{x}{mq}.$$

En particulier :

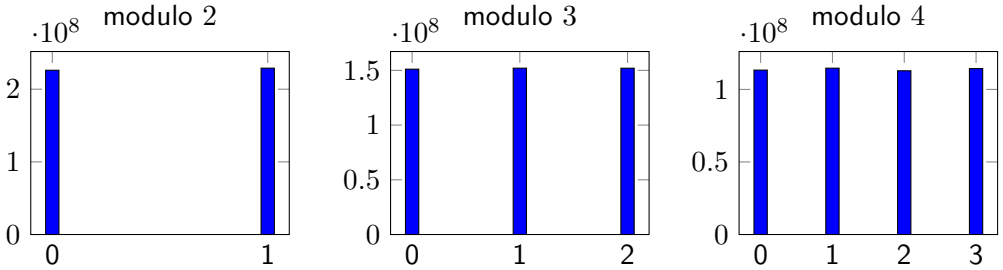
$$\frac{|\{k \leqslant x : s_2(k) \equiv a \bmod m\}|}{x} \underset{x \to +\infty}{\sim} \frac{1}{m}.$$

Problème (Gelfond, 1968) : Estimer $|\{p \leqslant x : s_2(p) \equiv a \bmod m\}|$.

$$\frac{|\{p \leqslant x : s_2(p) \equiv a \bmod m\}|}{\pi(x)} \overset{?}{\underset{x \to +\infty}{\sim}} \frac{1}{m}$$

Nombres premiers p tels que $s_2(p) \equiv a \bmod m$

$$|\{p \leqslant 10^{10} : \ s_2(p) \equiv a \bmod m\}|$$



Nombres premiers p tels que $s_2(p) \equiv a \bmod m$

Théorème (Mauduit–Rivat, 2010)

Pour tous entiers $m \geqslant 1$ *et* $a \in [\![0, m-1]\!]$,

$$|\{p \leqslant x : s_2(p) \equiv a \bmod m\}| \underset{x \to +\infty}{\sim} \frac{\pi(x)}{m}.$$

La somme des chiffres binaires des nombres premiers est bien répartie $\bmod m$.

Nombres premiers p tels que $s_2(p) \equiv a \bmod m$

On note $\mathrm{e}(x) = \exp(2\pi i x)$. D'après la formule d'orthogonalité :

$$\frac{1}{m}\sum_{h=0}^{m-1} \mathrm{e}\left(\frac{hq}{m}\right)\overline{\mathrm{e}\left(\frac{ha}{m}\right)} = \begin{cases} 1 & \text{si } q \equiv a \bmod m \\ 0 & \text{si } q \not\equiv a \bmod m, \end{cases}$$

on a

$$\begin{aligned} |\{p \leqslant x : s_2(p) \equiv a \bmod m\}| &= \sum_{p\leqslant x} \frac{1}{m}\sum_{h=0}^{m-1} \mathrm{e}\left(\frac{hs_2(p)}{m}\right)\overline{\mathrm{e}\left(\frac{ha}{m}\right)} \\ &= \frac{1}{m}\sum_{h=0}^{m-1} \mathrm{e}\left(\frac{-ha}{m}\right)\sum_{p\leqslant x} \mathrm{e}\left(\frac{hs_2(p)}{m}\right). \end{aligned}$$

La contribution de $h = 0$ est $\frac{\pi(x)}{m}$ (terme principal).
La contribution des $h \neq 0$ est en valeur absolue majorée par

$$\frac{1}{m}\sum_{h=1}^{m-1} \left|\sum_{p\leqslant x} \mathrm{e}\left(\frac{hs_2(p)}{m}\right)\right| \stackrel{?}{=} o(\pi(x))$$

Principal résultat *technique* (avec la notation $\mathrm{e}(x) = \exp(2\pi i x)$) :

Théorème (Mauduit–Rivat, 2010)

Si $\alpha \in \mathbb{R} \setminus \mathbb{Z}$ alors il existe $C(\alpha) > 0$ et $\sigma(\alpha) > 0$ tels que

$$\left| \sum_{p \leqslant x} \mathrm{e}(\alpha s_2(p)) \right| \leqslant C(\alpha)\ x^{1-\sigma(\alpha)}.$$

$\mathrm{e}(x) = \exp(2\pi i x)$. Soit $\alpha \in \mathbb{R}$.

Transformée de Fourier de $u \mapsto \mathrm{e}(\alpha s_2(u))$: pour $h \in \mathbb{Z}$,

$$\begin{aligned} F_n(h) &= \frac{1}{2^n} \sum_{u=0}^{2^n-1} \mathrm{e}\left(\alpha s_2(u) - \frac{h}{2^n} u\right) \\ &= \frac{1}{2^n} \sum_{u_0=0}^{1} \cdots \sum_{u_{n-1}=0}^{1} \mathrm{e}\left(\alpha(u_0 + \cdots + u_{n-1}) - \frac{h}{2^n}(u_0 2^0 + \cdots + u_{n-1} 2^{n-1})\right) \\ &= \frac{1}{2^n} \prod_{j=0}^{n-1} \left(\sum_{u_j=0}^{1} \mathrm{e}\left(\alpha u_j - \frac{h}{2^n} u_j 2^j\right)\right) = \prod_{j=0}^{n-1} \frac{1}{2}\left(1 + \mathrm{e}\left(\alpha - \frac{h}{2^n} 2^j\right)\right). \end{aligned}$$

D'où

$$|F_n(h)| = \prod_{j=0}^{n-1} \left|\cos \pi(\alpha - h 2^{j-n})\right|.$$

Nombres premiers dont les chiffres vérifient certaines propriétés

1. Nombres premiers dont la somme des chiffres est congrue à a modulo m (Mauduit–Rivat).
2. Nombres premiers dont la somme des chiffres est égale à ℓ (Drmota–Mauduit–Rivat).
3. Nombres premiers avec un chiffre interdit (Maynard).

Nombres entiers k tels que $s_2(k) = \ell$

Supposons n pair et $0 \leqslant \ell \leqslant n$. On a

$$|\{k < 2^n : s_2(k) = \ell\}| = \binom{n}{\ell} \leqslant \binom{n}{n/2}.$$

Comme

$$\binom{n}{n/2} \underset{n\to+\infty}{\sim} \sqrt{\frac{2}{\pi n}} \cdot 2^n,$$

on en déduit que

$$|\{k < 2^n : s_2(k) = \ell\}| = o(2^n).$$

L'ensemble des entiers k tels que $s_2(k) = \ell$ est donc *rare*.

Nombres premiers p tels que $s_2(p) = \ell$

Problème : Comparer

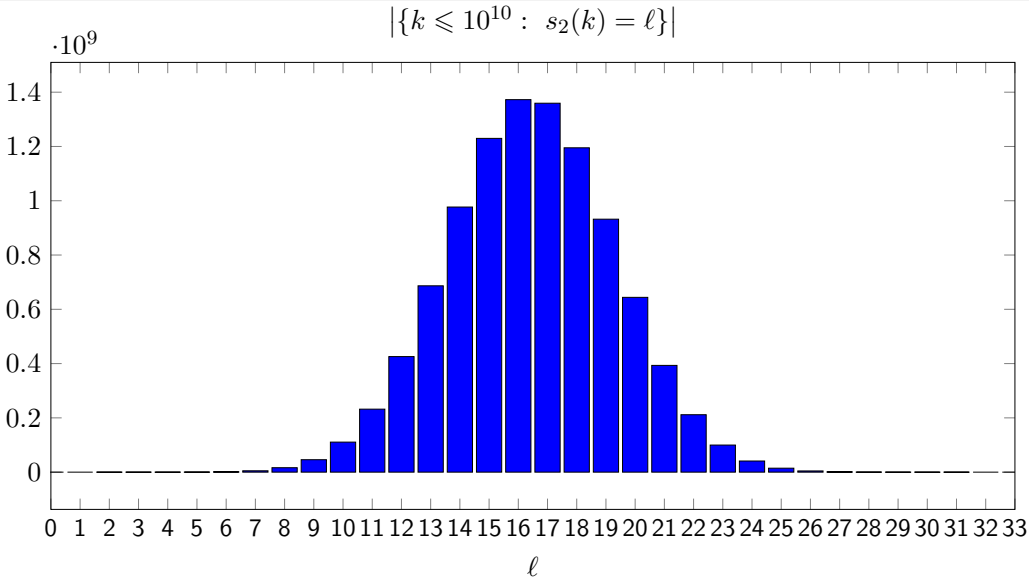
$$\frac{|\{p \leqslant x : s_2(p) = \ell\}|}{\pi(x)} \quad \text{avec} \quad \frac{|\{k \leqslant x : s_2(k) = \ell\}|}{x}.$$

Ce problème s'inscrit dans l'étude des nombres premiers dans un ensemble *rare*.

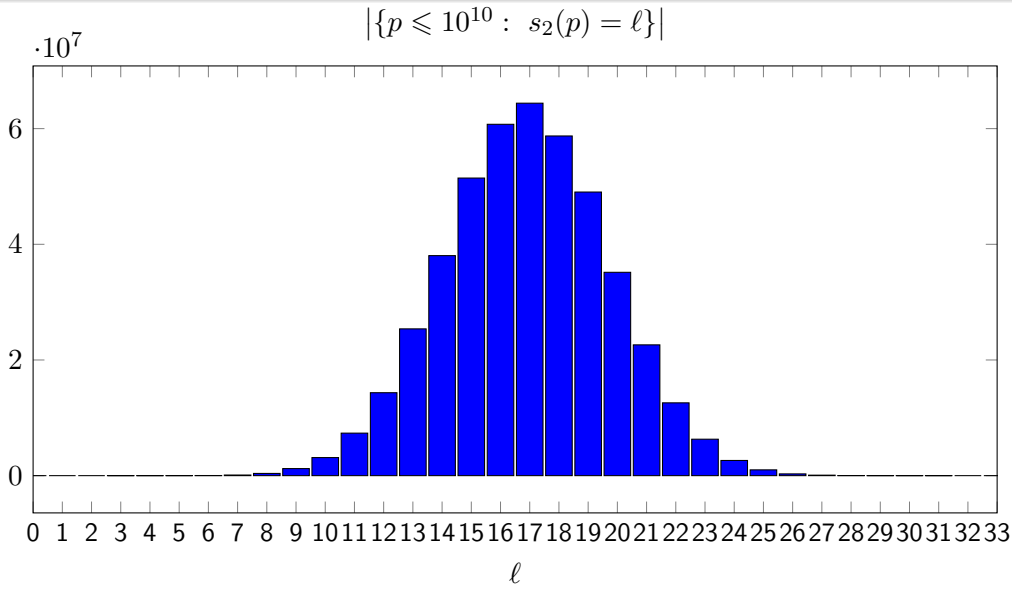
Existence d'une infinité de nb premiers

- de la forme $2^m - 1$ (premiers de Mersenne) ?
- de la forme $m^2 + 1$?

Histogramme de la somme des chiffres binaires des entiers (loi binomiale)



Histogramme de la somme des chiffres binaires des nombres premiers



Théorème (Drmota–Mauduit–Rivat, 2009)

Pour ℓ proche de $n/2$,

$$\frac{|\{p < 2^n : s_2(p) = \ell\}|}{\pi(2^n)} \underset{n\to+\infty}{\sim} \frac{|\{k < 2^n : s_2(k) = \ell\}|}{2^n}.$$

En particulier si n est pair alors

$$\frac{|\{p < 2^n : s_2(p) = n/2\}|}{\pi(2^n)} \underset{n\to+\infty}{\sim} \sqrt{\frac{2}{\pi n}}.$$

Nombres premiers dont les chiffres vérifient certaines propriétés

1. Nombres premiers dont la somme des chiffres est congrue à a modulo m (Mauduit–Rivat).

2. Nombres premiers dont la somme des chiffres est égale à ℓ (Drmota–Mauduit–Rivat).

3. Nombres premiers avec un chiffre interdit (Maynard).

Entiers avec un chiffre interdit

On considère ici la base 10. Soit $c \in \{0, \ldots, 9\}$.

$$\mathcal{A} = \{k \in \mathbb{N} : \text{l'écriture de } k \text{ en base 10 ne comporte pas le chiffre } c\}.$$

On a

$$|\{k < 10^n : k \in \mathcal{A}\}| = 9^n = (10^n)^{\frac{\log 9}{\log 10}} = o(10^n).$$

donc l'ensemble $\mathcal{A}$ est *rare*.

Nombres premiers avec un chiffre interdit

$$\mathcal{A} = \{k \in \mathbb{N} : \text{l'écriture de } k \text{ en base 10 ne comporte pas le chiffre } c\}.$$

On a

$$\frac{|\{k < 10^n : k \in \mathcal{A}\}|}{10^n} = \left(\frac{9}{10}\right)^n.$$

Théorème (Maynard, 2019)

Il existe deux constantes $C_2 > C_1 > 0$ telles que pour tout $n \geqslant 1$,

$$C_1 \left(\frac{9}{10}\right)^n \leqslant \frac{|\{p < 10^n : p \in \mathcal{A}\}|}{\pi\left(10^n\right)} \leqslant C_2 \left(\frac{9}{10}\right)^n.$$

Ainsi il existe une infinité de nombres premiers sans chiffre 3 (par exemple) en base 10.

L'étude des chiffres des nombres premiers met en œuvre des notions mathématiques très variées, notamment :

- théorie des nombres,
- combinatoire,
- analyse complexe,
- analyse harmonique,
- probabilités.

L'étude des chiffres des nombres premiers met en œuvre des notions mathématiques très variées, notamment :

- théorie des nombres,
- combinatoire,
- analyse complexe,
- analyse harmonique,
- probabilités.

Merci pour votre attention !