Eratostène joue-t-il aux dés ?

Probabilités élémentaires et nombres premiers

Jürgen Angst

Institut de Recherche Mathématique Avancée
Université Louis Pasteur, Strasbourg

Séminaire des doctorants,
8 Novembre 2007, Strasbourg

Le théorème d'Euclide

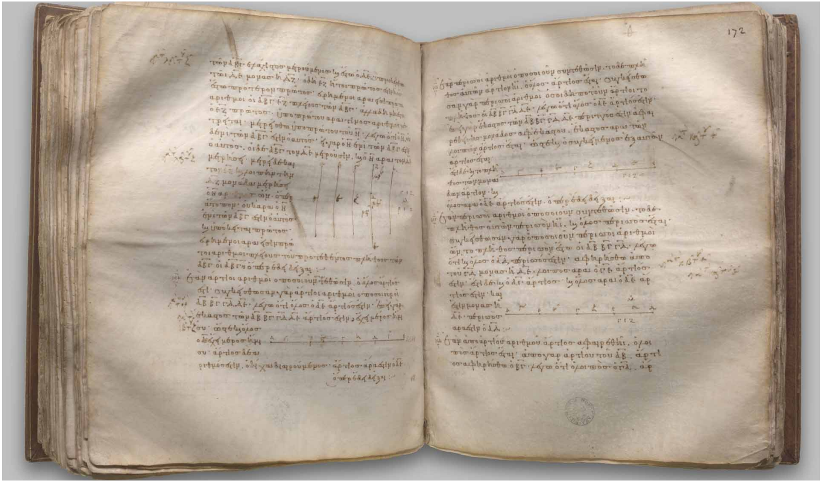
Théorème (Euclide, IIIème siècle av. J.C.)

Il existe une infinité de nombres premiers.

Preuve : Euclide raisonne par l'absurde, en utilisant la décomposition des entiers en produits de facteurs premiers. Si $\mathcal{P} = \{p_1, \dots, p_n\}$ est l'ensemble des nombres premiers, alors le nombre

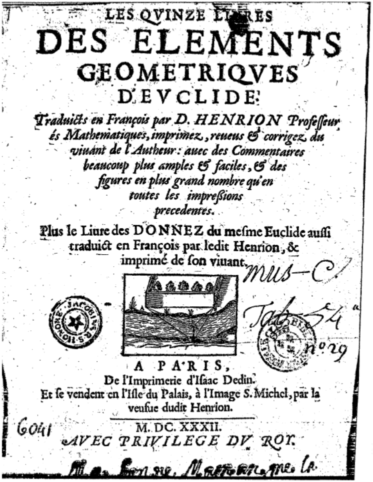
$$N = \prod_{i=1}^{n} p_i + 1$$

n'est divisible par aucun des p_i.



Les Éléments, édition byzantine de 888, The Bodleian Library, University of Oxford, source numérique : Rare book room.

La traduction de l'énoncé original du théorème d'Euclide, dans la traduction de D. Henrion de 1632. (source numéique : Gallica, Bnf)


LES QVINZE LIVRES
DES ELEMENTS
GEOMETRIQVES
D'EVCLIDE.
Traduicts en François par D. HENRION Professeur és Mathematiques, imprimez, reueus & corrigez du viuant de l'Autheur: auec des Commentaires beaucoup plus amples & faciles, & des figures en plus grand nombre qu'en toutes les impreßions precedentes.
Plus le Liure des DONNEZ du mesme Euclide aussi traduict en François par ledit Henrion, & imprimé de son viuant.
A PARIS,
De l'Imprimerie d'Isaac Dedin.
Et se vendent en l'Isle du Palais, à l'Image S. Michel, par la veufue dudit Henrion.
M. DC. XXXII.
AVEC PRIVILEGE DV ROY.

19. prop. 7. quatre nombres estans proport. le produict du second & troisiesme doit estre esgal au produict du premier & quatriesme.

THEOR. 18. PROP. XX.

Quelque multitude de nombres premiers qu'on propose, il s'en trouuera encores d'autres.

Soit quelconque multitude de nombres premiers, A, B, C. Ie dis qu'il s'en trouuera encores d'autres.

A..2 B...3 C.....5
D-------------------30 E.F
G-----

Car si on trouue le nombre D E, le plus petit de tous ceux qui peuuent estre mesurez par les trois nombres A, B, C, par la 37. prop. 7. & à iceluy D E on adiouste l'vnité EF, le tout D F sera premier ou non : S'il est premier, on a vn nombre premier autre que pas vn des proposez : Mais si DF n'est premier, il sera mesuré par quelque nombre premier, par la 34. prop. 7. Soit donc mesuré par G ; il est éuident que G ne peut pas estre vn des trois A, B, C : car s'il estoit quelqu'vn d'iceux, il mesureroit comme eux DE. Donc G mesurant le tout D F, & le retranché D E, par la 12. comm, sent. il mesureroit aussi le reste DF, sçauoir vn nombre l'vnité : Ce qui est absurde. Donc G est autre nombre premier que pas vn des proposez. Et en ceste façon on en peut trouuer infiny autres. Parquoy quelque multitude de nombres premiers qu'on propose, &c. Ce qu'il falloit demonstrer.

- Si l'on introduit la fonction de comptage $\pi : \mathbb{R} \to \mathbb{N}$:

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

le théorème d'Euclide affirme simplement que

$$\lim_{x \to +\infty} \pi(x) = +\infty.$$

- Que peut-on dire du comportement asymptotique de la fonction π ?

- Si l'on introduit la fonction de comptage $\pi : \mathbb{R} \to \mathbb{N}$:

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

le théorème d'Euclide affirme simplement que

$$\lim_{x \to +\infty} \pi(x) = +\infty.$$

- Que peut-on dire du comportement asymptotique de la fonction π ?

Les conjectures de Legendre-Gauss

- Legendre (1796) constate que la fonction

$$x \mapsto \frac{x}{\log(x) + B}, \quad \text{avec} \quad B \approx 1.08,$$

est une bonne approximation de $\pi(x)$.

- A la même époque, Gauss conjecture que

$$\pi(x) \sim Li(x),$$

où $\quad Li(x) := \lim_{\delta \to 0} \left(\int_0^{1-\delta} + \int_{1+\delta}^{x} \right) \frac{dy}{\log(y)} \sim \frac{x}{\log(x)}.$

Les conjectures de Legendre-Gauss

- Legendre (1796) constate que la fonction

$$x \mapsto \frac{x}{\log(x) + B}, \quad \text{avec} \quad B \approx 1.08,$$

est une bonne approximation de $\pi(x)$.

- A la même époque, Gauss conjecture que

$$\pi(x) \sim Li(x),$$

où $\quad Li(x) := \lim_{\delta \to 0} \left(\int_0^{1-\delta} + \int_{1+\delta}^{x} \right) \frac{dy}{\log(y)} \sim \frac{x}{\log(x)}.$

Les résultats de Tchebychef

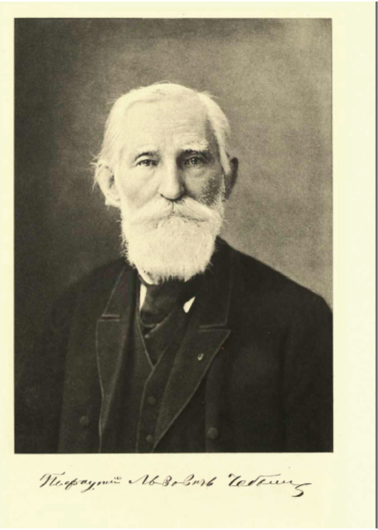
Le théorème de Tchebychef

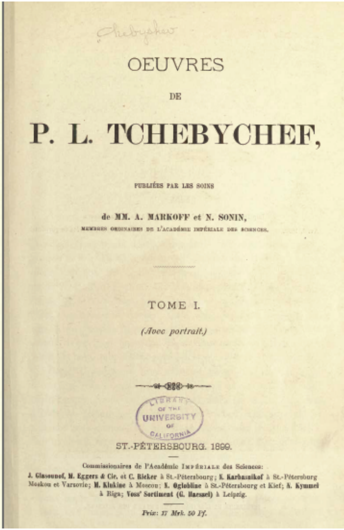
Dans son “Mémoire sur les nombres premiers” paru en 1852, Tchebychef établit le premier résultat significatif concernant la distribution des nombres premiers :

Théorème (Tchebychef, 1852)

Il existe deux constantes strictement positives C et C' telles que, lorsque x tend vers l'infini :

$$C\frac{x}{\log(x)} \leq \pi(x) \leq C'\frac{x}{\log(x)}.$$




Chebyshev

OEUVRES

DE

P. L. TCHEBYCHEF,

PUBLIÉES PAR LES SOINS

de MM. A. MARKOFF et N. SONIN,

MEMBRES ORDINAIRES DE L'ACADÉMIE IMPÉRIALE DES SCIENCES.

TOME I.

(Avec portrait.)

LIBRARY OF THE UNIVERSITY OF CALIFORNIA

ST.-PÉTERSBOURG. 1899.

Commissionaires de l'Académie Impériale des Sciences:
J. Glasounof, M. Eggers & Cie, et C. Ricker à St.-Pétersbourg; N. Karbasnikof à St.-Pétersbourg Moskou et Varsovie; M. Klukine à Moscou; N. Oglobline à St.-Pétersbourg et Kief; N. Kymmel à Riga; Voss' Sortiment (G. Haessel) à Leipzig.

Prix: 17 Mrk. 50 Pf.

Heuristique de la preuve de Tchebychef

Tchebychef introduit plusieurs fonctions parmi lesquelles

$$\theta(x) := \sum_{p \leq x} \log(p), \quad \psi(x) := \sum_{p^\nu \leq x} \log(p), \quad T(x) := \sum_{n \leq x} \psi(x/n).$$

La fonction T s'écrit encore $T(x) = \log(\lfloor x \rfloor !)$ et l'on a

$$\liminf_{x \to +\infty} \frac{\pi(x)\log(x)}{x} = \liminf_{x \to +\infty} \frac{\theta(x)}{x} = \liminf_{x \to +\infty} \frac{\psi(x)}{x},$$

$$\limsup_{x \to +\infty} \frac{\pi(x)\log(x)}{x} = \limsup_{x \to +\infty} \frac{\theta(x)}{x} = \limsup_{x \to +\infty} \frac{\psi(x)}{x}.$$

Heuristique de la preuve de Tchebychef

§ 3. D'après cette équation, il n'est pas difficile de trouver plusieurs inégalités que la fonction $\psi(x)$ vérifie. Celles dont nous nous servirons dans ce mémoire sont les suivantes:

$$\psi(x) > T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right),$$

$$\psi(x) - \psi\left(\frac{x}{6}\right) < T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right).$$

Grâce à la formule de Stirling, Tchebychef montre que

$$T(x) < \log \sqrt{2\pi} + x \log x - x + \frac{1}{2} \log x + \frac{1}{12},$$

$$T(x) > \log \sqrt{2\pi} + x \log x - x - \frac{1}{2} \log x;$$

Heuristique de la preuve de Tchebychef

Il en déduit que

$$\psi(x) < \frac{6}{5} Ax + \frac{5}{4 \log 6} \log^2 x + \frac{5}{4} \log x + 1,$$
$$\psi(x) > Ax - \frac{5}{2} \log x - 1.$$

où $A = 0.92129202$, puis

$$\begin{cases} \theta(x) < \frac{6}{5} Ax - Ax^{\frac{1}{2}} + \frac{5}{4 \log 6} \log^2 x + \frac{5}{2} \log x + 2 \\ \theta(x) > Ax - \frac{12}{5} Ax^{\frac{1}{2}} - \frac{5}{8 \log 6} \log^2 x - \frac{15}{4} \log x - 3 \end{cases}$$

Explication de la preuve

La plus grande puissance de p qui divise $x!$ est donnée par

$$\left\lfloor \frac{x}{p} \right\rfloor + \left\lfloor \frac{x}{p^2} \right\rfloor + \left\lfloor \frac{x}{p^3} \right\rfloor + \dots \quad \text{ex.} \quad 10! = 10.\color{red}{9}\color{black}.8.7.\color{red}{6}\color{black}.5.4.\color{red}{3}\color{black}.2.1$$

On a donc

$$x! = \prod_{p \le x} p^{\left\lfloor \frac{x}{p} \right\rfloor + \left\lfloor \frac{x}{p^2} \right\rfloor + \left\lfloor \frac{x}{p^3} \right\rfloor + \cdots}$$

et

$$\log(x!) = \sum_{p \le x} \left(\left\lfloor \frac{x}{p} \right\rfloor + \left\lfloor \frac{x}{p^2} \right\rfloor + \left\lfloor \frac{x}{p^3} \right\rfloor + \dots \right) \log(p).$$

Explication de la preuve

D'après la formule de Stirling, lorsque x est grand :

$$x! \sim x^x e^{-x}\sqrt{2\pi x}, \quad i.e., \quad \log(x!) \sim x\log(x).$$

De l'égalité

$$\log(x!) = \sum_{p\leq x}\left(\left\lfloor\frac{x}{p}\right\rfloor + \left\lfloor\frac{x}{p^2}\right\rfloor + \left\lfloor\frac{x}{p^3}\right\rfloor + \dots\right)\log(p),$$

on “déduit” alors que

$$x\log(x) \quad\sim\quad \sum_{p\leq x}\left\lfloor\frac{x}{p}\right\rfloor\log(p) \quad\sim\quad x\sum_{p\leq x}\frac{\log(p)}{p}.$$

Explication de la preuve

La difficulté essentielle du résultat de Tchebychef concernant l'estimation des fonctions ψ et θ, repose sur la justification de l'équivalent

$$\sum_{p \leq x} \frac{\log(p)}{p} \sim \log(x).$$

Nous verrons tout à l'heure une démonstration simple de ce résultat qui n'utilise que des probabilités élémentaires.

Les idées novatrices de Riemann

L'article de Riemann

En 1859, Riemann publie un article de 8 pages intitulé " Über die Anzahl der Primzahlen unter einer gegebenen Grösse". Dans cet article révolutionnaire, Riemann introduit entre autre les nouvelles méthodes suivantes en arithmétique :

- Le prolongement analytique (de ζ).
- L'intégration sur des contours (de $d\log(\zeta)$).
- L'inversion de Fourier.

L'article de Riemann

En 1859, Riemann publie un article de 8 pages intitulé " Über die Anzahl der Primzahlen unter einer gegebenen Grösse". Dans cet article révolutionnaire, Riemann introduit entre autre les nouvelles méthodes suivantes en arithmétique :

- Le prolongement analytique (de ζ).
- L'intégration sur des contours (de $d\log(\zeta)$).
- L'inversion de Fourier.

L'article de Riemann

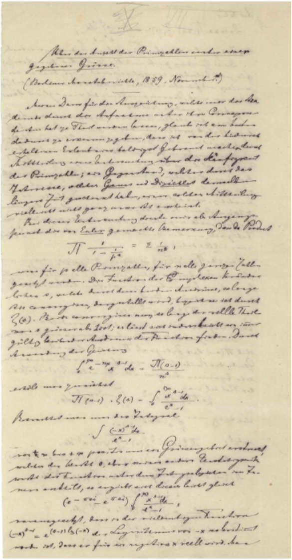
En 1859, Riemann publie un article de 8 pages intitulé " Über die Anzahl der Primzahlen unter einer gegebenen Grösse". Dans cet article révolutionnaire, Riemann introduit entre autre les nouvelles méthodes suivantes en arithmétique :

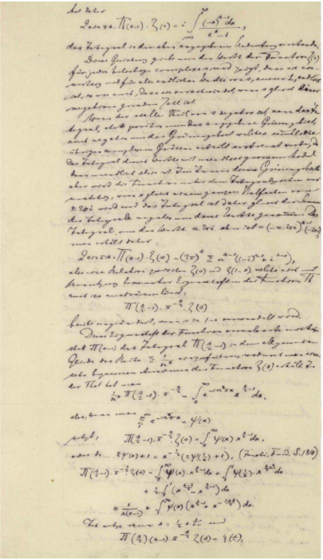
- Le prolongement analytique (de ζ).
- L'intégration sur des contours (de $d\log(\zeta)$).
- L'inversion de Fourier.

L'article de Riemann

En 1859, Riemann publie un article de 8 pages intitulé " Über die Anzahl der Primzahlen unter einer gegebenen Grösse". Dans cet article révolutionnaire, Riemann introduit entre autre les nouvelles méthodes suivantes en arithmétique :

- Le prolongement analytique (de ζ).
- L'intégration sur des contours (de $d\log(\zeta)$).
- L'inversion de Fourier.


Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse.
(Berliner Monatsberichte, 1859, November.)



Le lien entre les fonctions ψ et ζ

- ψ est donnée par $\psi(x) = \sum_{p^\nu \leq x} \log(p) = \sum_{n \leq x} \Lambda(n)$, et l'on a

$$Z(s) := -\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{+\infty} \frac{\Lambda(n)}{n^s} \qquad (\Re(s) > 1).$$

- En utilisant le procédé de sommation d'Abel, il vient

$$Z(s) = s \int_1^{+\infty} \frac{\psi(u)}{u^{s+1}} du, \qquad (\Re(s) > 1).$$

Le lien entre les fonctions ψ et ζ

- ψ est donnée par $\psi(x) = \sum_{p^\nu \leq x} \log(p) = \sum_{n \leq x} \Lambda(n)$, et l'on a

$$Z(s) := -\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{+\infty} \frac{\Lambda(n)}{n^s} \qquad (\Re(s) > 1).$$

- En utilisant le procédé de sommation d'Abel, il vient

$$Z(s) = s \int_1^{+\infty} \frac{\psi(u)}{u^{s+1}} du, \qquad (\Re(s) > 1).$$

Le lien entre les fonctions ψ et ζ

- Il revient au même de montrer que

$$\psi(x) \sim x \quad \text{ou} \quad \Psi(x) = \int^x \psi(y)dy \sim \frac{1}{2}x^2.$$

- En intégrant par parties, il vient

$$Z(s) = s(s+1)\int_1^{+\infty} \frac{\Psi(u)}{u^{s+2}}du, \qquad (\Re(s) > 1),$$

et on peut “inverser” la formule :

$$\frac{\Psi(x)}{x^2} = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{Z(s)x^{s-1}}{s(s+1)}ds, \qquad (\forall\, c > 1).$$

Le lien entre les fonctions ψ et ζ

- Il revient au même de montrer que

$$\psi(x) \sim x \quad \text{ou} \quad \Psi(x) = \int^x \psi(y)dy \sim \frac{1}{2}x^2.$$

- En intégrant par parties, il vient

$$Z(s) = s(s+1)\int_1^{+\infty} \frac{\Psi(u)}{u^{s+2}}du, \qquad (\Re(s) > 1),$$

et on peut “inverser” la formule :

$$\frac{\Psi(x)}{x^2} = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{Z(s)x^{s-1}}{s(s+1)}ds, \qquad (\forall\, c > 1).$$

Le lien entre les fonctions ψ et ζ

- Montrer le théorème des nombres premiers revient à montrer que lorsque x tend vers l'infini :

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\frac{Z(s)x^{s-1}}{s(s+1)}ds \longrightarrow \frac{1}{2}.$$

- On a envie d'intégrer sur un contour fermé. La fonction Z est sans singularité dans le demi plan $\Re(s) > 1$, le contour doit nécéssairement déborder dans le demi plan $\Re(s) < 1$. (On montre que Z est prolongeable à $\Re(s) > 1$).

Le lien entre les fonctions ψ et ζ

- Montrer le théorème des nombres premiers revient à montrer que lorsque x tend vers l'infini :

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\frac{Z(s)x^{s-1}}{s(s+1)}ds \longrightarrow \frac{1}{2}.$$

- On a envie d'intégrer sur un contour fermé. La fonction Z est sans singularité dans le demi plan $\Re(s) > 1$, le contour doit nécéssairement déborder dans le demi plan $\Re(s) < 1$. (On montre que Z est prolongeable à $\Re(s) > 1$).

Le lien entre les fonctions ψ et ζ

- Montrer le théorème des nombres premiers revient à montrer que lorsque x tend vers l'infini :

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\frac{Z(s)x^{s-1}}{s(s+1)}ds \longrightarrow \frac{1}{2}.$$

- Les seuls pôles de l'intégrande sont les éventuels zéros de ζ et les points $s=-1,\ 0$ et $s=1$ où les résidus valent respectivement

$$-Z(-1)/x^2, \quad Z(0)/x, \quad \text{et} \quad 1/2.$$

Si l'on arrive à trouver un contour qui évite les zéros de ζ, c'est gagné.

Hypothèse de Riemann

- S'il existait un $\beta < 1$ tel que $\zeta(s) \neq 0$ pour $\Re(s) > \beta$, on pourrait intégrer sur un rectangle.
- Dans son article, Riemann émet la conjecture selon laquelle $\zeta(s) \neq 0$ pour $\Re(s) > 1/2$: c'est la fameuse "conjecture de Riemann".
- Aujourd'hui encore, on ne sait pas si un tel β existe !

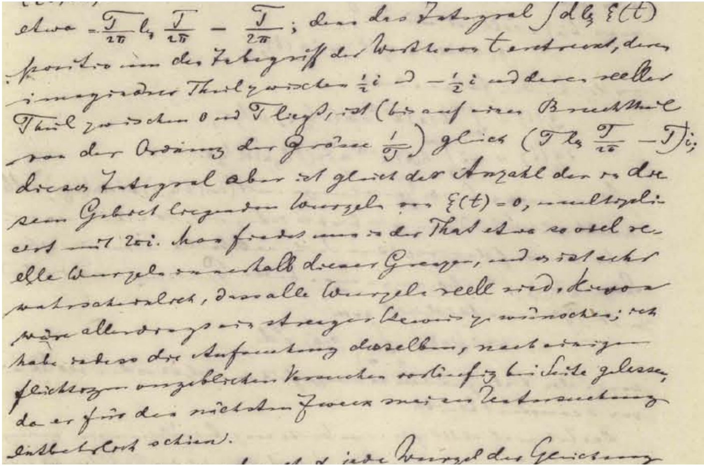
Hypothèse de Riemann

- S'il existait un $\beta < 1$ tel que $\zeta(s) \neq 0$ pour $\Re(s) > \beta$, on pourrait intégrer sur un rectangle.
- Dans son article, Riemann émet la conjecture selon laquelle $\zeta(s) \neq 0$ pour $\Re(s) > 1/2$: c'est la fameuse “conjecture de Riemann".
- Aujourd'hui encore, on ne sait pas si un tel β existe !

Hypothèse de Riemann

- S'il existait un $\beta < 1$ tel que $\zeta(s) \neq 0$ pour $\Re(s) > \beta$, on pourrait intégrer sur un rectangle.
- Dans son article, Riemann émet la conjecture selon laquelle $\zeta(s) \neq 0$ pour $\Re(s) > 1/2$: c'est la fameuse “conjecture de Riemann".
- Aujourd'hui encore, on ne sait pas si un tel β existe !

La conjecture Riemann dans le texte



etwa $= \frac{T}{2\pi} \log \frac{T}{2\pi} - \frac{T}{2\pi}$; denn das Integral $\int d \log \xi(t)$ positiv um den Inbegriff der Werthe von t erstreckt, deren imaginärer Theil zwischen $\frac{1}{2}i$ und $-\frac{1}{2}i$ und deren reeller Theil zwischen 0 und T liegt, ist (bis auf einen Bruchtheil von der Ordnung der Grösse $\frac{1}{T}$) gleich $\left(T \log \frac{T}{2\pi} - T\right)i$; dieses Integral aber ist gleich der Anzahl der in diesem Gebiet liegenden Wurzeln von $\xi(t) = 0$, multiplicirt mit $2\pi i$. Man findet nun in der That etwa so viel reelle Wurzeln innerhalb dieser Grenzen, und es ist sehr wahrscheinlich, dass alle Wurzeln reell sind. Hiervon wäre allerdings ein strenger Beweis zu wünschen; ich habe indess die Aufsuchung desselben nach einigen flüchtigen vergeblichen Versuchen vorläufig bei Seite gelassen, da er für den nächsten Zweck meiner Untersuchung entbehrlich schien.

… jede Wurzel der Gleichung

La conjecture Riemann dans le texte

"...es ist sehr wahrscheinlich, dass alle Wurzeln reell sind. Hiervon wäre allerdings ein strenger Beweis zu wünschen ; ich habe indess die Aufsuchung desselben nach einigen flüchtigen vergeblichen Versuchen vorläufig bei Seite gelassen, da er für den nächsten Zweck meiner Untersuchung entbehrlich schien."

"...il est très probable que toutes les racines sont réelles. Bien entendu, une preuve rigoureuse serait nécéssaire. Après quelques tentatives infructueuses, j'ai pour le moment mis de côté la quète d'une démonstration de ce résultat, celui-ci n'étant pas nécéssaire quant à mes prochains objectifs de recherche."

Le théorème des nombres premiers

Le théorème des nombres premiers

En 1896, La Vallée Poussin et Hadamard montrent indép. que la fonction ζ ne s'annule pas sur la droite $\Re(s) = 1$. En intégrant la fonction précedente sur un contour bien choisi, ils en déduisent :

Théorème (de la Vallée Poussin, Hadamard, 1896)

$$\pi(x) \sim Li(x) = \lim_{\delta \to 0} \left(\int_0^{1-\delta} + \int_{1+\delta}^{x} \right) \frac{dy}{\log(y)} \sim \frac{x}{\log(x)}.$$

Formulations équivalentes

- Si p_n désigne le $n^{\text{ème}}$ nombre premier, le théorème des nombres premiers revient à dire que lorsque n tend vers l'infini, on a :

$$p_n \sim n\log(n), \quad \text{ou encore} \quad Li(p_n) \sim n.$$

- L'hypothèse de Riemann est alors équivalente à l'une ou l'autre des assertions suivantes :

$$\pi(x) = \frac{x}{\log(x)} + O(x^{1/2+\varepsilon}), \qquad \forall\, \varepsilon > 0,$$

ou

$$E(n) := Li(p_n) - n = O(n^{1/2+\varepsilon}), \qquad \forall\, \varepsilon > 0.$$

Formulations équivalentes

- Si p_n désigne le $n^{\text{ème}}$ nombre premier, le théorème des nombres premiers revient à dire que lorsque n tend vers l'infini, on a :

$$p_n \sim n \log(n), \quad \text{ou encore} \quad Li(p_n) \sim n.$$

- L'hypothèse de Riemann est alors équivalente à l'une ou l'autre des assertions suivantes :

$$\pi(x) = \frac{x}{\log(x)} + O(x^{1/2+\varepsilon}), \qquad \forall\, \varepsilon > 0,$$

ou

$$E(n) := Li(p_n) - n = O(n^{1/2+\varepsilon}), \qquad \forall\, \varepsilon > 0.$$

Seconde partie (avec des proba dedans)

Une preuve élémentaire du résultat de Tchebychef

On a vu que théorème de Tchebychef revient à montrer l'équivalent suivant, lorsque x tend vers l'infini :

$$\sum_{p \leq n} \frac{\log(p)}{p} \sim \log(n).$$

Le preuve suivante est due à I. Kontoyiannis (2007), elle est basée sur une heuristique de Billingsley (1970') et utilise essentiellement la notion d'entropie (de Shannon).

On fixe un nombre entier n (grand). On tire ensuite un nombre $N \in \{1, \ldots, n\}$ selon la loi uniforme et on écrit sa décomposition en facteurs premiers :

$$N = \prod_{p \leq n} p^{X_p}.$$

Il y a exactement $\lfloor n/p^k \rfloor$ multiples de p^k entre 1 et n, donc

$$\mathbb{P}(X_p \geq k) = \mathbb{P}(\{p^k | N\}) = \frac{1}{n} \left\lfloor \frac{n}{p^k} \right\rfloor \approx \left(\frac{1}{p}\right)^k,$$

$$\mathbb{P}(X_{p_i} \geq k_i, \text{ pour } p_1, p_2, \ldots, p_m) \approx \left(\frac{1}{p_1}\right)^{k_1} \cdots \left(\frac{1}{p_m}\right)^{k_m},$$

$$\mathbb{E}\left[X_p\right] = \sum_{k \geq 1} \mathbb{P}(X_p \geq k) \leq \sum_{k \geq 1} \left(\frac{1}{p}\right)^k = \frac{1}{p-1} := \mu_p.$$

Pour une variable aléatoire Y à valeurs entière :

$$H(Y) := -\sum_{k} \mathbb{P}(Y = k) \log \mathbb{P}(Y = k).$$

Il y a une bijection entre la donnée de N et la donnée des X_p :

$$\log(n) = H(N) = H(X_p;\ p \leq n).$$

L'heuristique de Billingsley est la suivante :

$$\log(n) = H(N) = H(X_p;\ p \leq n) \approx \sum_{p \leq n} H(X_p) \approx \sum_{p \leq n} H(geom(\mu_p)).$$

Pour une variable aléatoire Y à valeurs entière :

$$H(Y) := -\sum_k \mathbb{P}(Y=k)\log\mathbb{P}(Y=k).$$

Il y a une bijection entre la donnée de N et la donnée des X_p :

$$\log(n) = H(N) = H(X_p;\ p \le n).$$

En fait, on a toujours :

$$\log(n) = H(N) = H(X_p;\ p \le n) \le \sum_{p\le n} H(X_p) \le \sum_{p\le n} H(geom(\mu_p)).$$

Le calcul montre que

$$\sum_{p\leq n} H(geom(\mu_p)) = \sum_{p\leq n}\left[\frac{\log(p)}{p-1} - \log\left(1-\frac{1}{p}\right)\right] \sim \sum_{p\leq n}\frac{\log(p)}{p},$$

on en déduit qu'asymptotiquement

$$\log(n) \leq \sum_{p\leq n}\frac{\log(p)}{p}.$$

La seconde inégalité est démontrée par des méthodes plus classiques.

Le crible de Hawkins

Le crible d'Eratostène (≈ 240 av. J.C.)

$$\begin{array}{cccccccccc}
 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\
11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \\
21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 \\
31 & 32 & 33 & 34 & 35 & 36 & 37 & 38 & 39 & 40 \\
41 & 42 & 43 & 44 & 45 & 46 & 47 & 48 & 49 & 50 \\
51 & 52 & 53 & 54 & 55 & 56 & 57 & 58 & 59 & 60 \\
61 & 62 & 63 & 64 & 65 & 66 & 67 & 68 & 69 & 70 \\
71 & 72 & 73 & 74 & 75 & 76 & 77 & 78 & 79 & 80 \\
81 & 82 & 83 & 84 & 85 & 86 & 87 & 88 & 89 & 90 \\
91 & 92 & 93 & 94 & 95 & 96 & 97 & 98 & 99 & 100 \\
\vdots & & & \vdots & & & \vdots & & & \vdots
\end{array}$$

Le crible d'Eratostène

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
⋮			⋮			⋮			⋮

Le crible d'Eratostène

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
$\vdots$			$\vdots$			$\vdots$			$\vdots$

Le crible d'Eratostène

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
$\vdots$			$\vdots$			$\vdots$			$\vdots$

Le crible d'Eratostène

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
$\vdots$			$\vdots$			$\vdots$			$\vdots$

Le crible d'Eratostène

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
$\vdots$			$\vdots$			$\vdots$			$\vdots$

Le crible d'Eratostène

Etape 1 : On considère l'ensemble $A_1 := \{2, 3, 4, 5, \ldots\}$, et on note $p_1 = \min A_1$. Dans l'ensemble $A_1 - \{p_1\}$, on élimine tous les multiples de p_1. Statistiquement, on élimine donc un nombre sur p_1. On note A_2 le sous-ensemble de $A_1 - \{p_1\}$ obtenu.

Etape n : Soit $p_n = \min A_n$. Dans l'ensemble $A_n - \{p_n\}$, on élimine tous les multiples de p_n. Statistiquement, on élimine donc un nombre sur p_n. On note A_{n+1} le sous-ensemble de $A_n - \{p_n\}$ obtenu.

Résultat : L'ensemble des nombre premiers est

$$\mathcal{P} = \{p_1, p_2, p_3, \ldots\}.$$

Le crible de Hawkins

Etape 1 : On considère l'ensemble $A_1 := \{2, 3, 4, 5, \ldots\}$, et on note $p_1 = \min A_1$. Les eléments de $A_1 - \{p_1\}$ sont éliminés avec une probabilité $1/p_1$, indépendamment les uns des autres. On note A_2 l'ensemble obtenu.

Etape n : Soit $p_n = \min A_n$. Les eléments de $A_n - \{p_n\}$ sont éliminés avec une probabilité $1/p_n$, indépendamment les uns des autres. On note A_{n+1} le sous-ensemble de $A_n - \{p_n\}$ obtenu.

Résultat : Un ensemble de nombres entiers aléatoires

$$\mathcal{P} = \{p_1, p_2, p_3, \ldots\}.$$

Le crible de Hawkins

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
$\vdots$			$\vdots$			$\vdots$			$\vdots$

Le crible de Hawkins

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
$\vdots$			$\vdots$			$\vdots$			$\vdots$

Le crible de Hawkins

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
$\vdots$			$\vdots$			$\vdots$			$\vdots$

Le crible de Hawkins

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
⋮			⋮			⋮			⋮

Le crible de Hawkins

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
$\vdots$			$\vdots$			$\vdots$			$\vdots$

Dans le cadre des nombres premiers, nous avons vu que le théorème des nombres premiers et la conjecture de Riemann sont équivalents aux assertions

$$p_n \sim n \log(n), \quad \text{et} \quad E(n) = Li(p_n) - n = O(n^{1/2+\varepsilon}), \forall\, \varepsilon > 0.$$

Par ailleurs, en 1874, Mertens a montré que

$$\lim_{n \to +\infty} \frac{1}{\log(n)} \prod_{p \leq n} \left(1 - \frac{1}{p}\right)^{-1} = e^{\gamma}$$

où $\gamma \approx 0.57721$ est la constante d'Euler.

Dans le cas où les p_n sont obtenus via le crible de Hawkins, en posant

$$q_n := \prod_{k \leq n} \left(1 - \frac{1}{p_k}\right)^{-1},$$

on a le théorème analogue :

Théorème (Wunderlich, Neudecker, Williams, 1974)

Presque sûrement, lorsque n tend vers l'infini :

$$p_n \sim n \log(n), \quad et \quad q_n \sim \log(n).$$

D'autre part, la suite $(p_n \exp(-q_n))_{n \geq 1}$ converge p.s. vers une variable aléatoire $\ell \in]0, +\infty[$.

Toujours dans le cas où les p_n sont obtenus via le crible de Hawkins, Neudecker et Williams ont montré que la conjecture de Riemann est vraie :

Théorème (Neudecker, Williams, 1974)

Presque sûrement, lorsque n tend vers l'infini, on a

$$E(n) := \ell\, Li(p_n/\ell) - n = O(n^{1/2+\varepsilon}), \quad \forall\, \varepsilon > 0.$$

Le terme d'erreur $E(n)$ a été étudié de façon plus fine par Williams et Foster qui ont montré le résultat suivant :

Théorème (Foster, Williams, 1978)

Quitte à "grossir" l'espace de probabilité ambiant, on peut construire un mouvement brownien $(B_t)_{t\geq 0}$, tel que

$$E(n) := \ell\, Li(p_n/\ell) - n = B_n + O\left(\left[n \log\log n\right]^{1/2} / \log(n)\right).$$

Désignons par $\Pi_{X,X+2}(x)$ le nombre de “premiers jumeaux" inférieurs à x. La conjecture de Hardy-Littlewood affirme que

$$\Pi_{X,X+2}(x) \sim 2C_2 \, \frac{x}{\log(x)^2}, \quad \text{où} \quad C_2 = \prod_{p \geq 3} \frac{p(p-2)}{(p-1)^2}.$$

Théorème (Wunderlich, 1974)

Pour les nombres premiers obtenus via le crible de Hawkins, presque sûrement, lorsque x tend vers l'infini :

$$\Pi_{X,X+2}(x) \sim \frac{x}{\log(x)^2}.$$

Plus généralement, on a les résultats suivants

Théorème (Bui, Keating, 2007)

Pour tout entier k fixé, presque sûrement, lorsque x tend vers l'infini :

$$\Pi_{X,X+k}(x) \sim \frac{x}{\log(x)^2}.$$

Théorème (Bui, Keating, 2007)

Pour toute suite d'entiers $k_1, k_2, \ldots, k_{l-1}$ fixée, presque sûrement, lorsque x tend vers l'infini :

$$\Pi_{X,X+k_1,X+k_2,\ldots,X+k_{l-1}}(x) \sim \frac{x}{\log(x)^l}.$$

Corollaire (Bui, Keating, 2007)

Pour tous entiers d et l fixés, presque sûrement, lorsque x tend vers l'infini :

$$\Pi_{X,X+d,X+2d,\ldots X+(l-1)d}(x) \sim \frac{x}{\log(x)^l}.$$

A mettre en rapport avec le résultat de Green et Tao en 2004, sur l'existence de progression arithmétique arbitrairement longue dans l'ensemble des nombres premiers...