Randonnée arithmétique

E. Kowalski

ETH Zürich

Nancy, 21 Janvier 2020

Étymologie : anglais *random*, de l'ancien français «randon», *course impétueuse*, d'où «randonnée» (chasse : *tour, circuit fait sur un même lieu par une bête qu'on a lancée*).

Étymologie : anglais *random*, de l'ancien français «randon», *course impétueuse*, d'où «randonnée» (chasse : *tour, circuit fait sur un même lieu par une bête qu'on a lancée*).

Références :

E.K., *An introduction to probabilistic number theory*,
`www.math.ethz.ch/~kowalski/probabilistic-number-theory.pdf`

C. Perret-Gentil, *Some recent interactions of probability and number theory*,
`https://corentinperretgentil.gitlab.io/static/documents/some-recent-interactions-probability-number-theory.pdf`

Théorie probabiliste des nombres

L'arithmétique des objets les plus simples peut sembler complètement imprévisible.

Théorie probabiliste des nombres

L'arithmétique des objets les plus simples peut sembler complètement imprévisible.

Par exemple : combien un entier n a-t-il de facteurs premiers ? Disons

$$n = 1234567891011121314151617181920212223242526272829303132 33$$

Théorie probabiliste des nombres

L'arithmétique des objets les plus simples peut sembler complètement imprévisible.

Par exemple : combien un entier n a-t-il de facteurs premiers ? Disons

$$n = 12345678910111213141516171819202122232425262728293031323 3$$

Voir l'expression décimale de n ne donne pratiquement pas d'information à ce sujet : il faut factoriser n pour trouver la réponse.

Théorie probabiliste des nombres

L'arithmétique des objets les plus simples peut sembler complètement imprévisible.

Par exemple : combien un entier n a-t-il de facteurs premiers ? Disons

$$n = 12345678910111213141516171819202122232425262728293031323 3$$

Voir l'expression décimale de n ne donne pratiquement pas d'information à ce sujet : il faut factoriser n pour trouver la réponse.

Si n est très grand, et qu'on doive répondre rapidement, il n'y a pas vraiment d'autre choix que de procéder en devinant.

Théorie probabiliste des nombres

L'arithmétique des objets les plus simples peut sembler complètement imprévisible.

Par exemple : combien un entier n a-t-il de facteurs premiers ? Disons

$$n = 1234567891011121314151617181920212223242526272829303132 33$$

Voir l'expression décimale de n ne donne pratiquement pas d'information à ce sujet : il faut factoriser n pour trouver la réponse.

Si n est très grand, et qu'on doive répondre rapidement, il n'y a pas vraiment d'autre choix que de procéder en devinant. Mais on peut deviner de manière intelligente, c'est-à-dire en étudiant d'abord ce qui se passe «en moyenne».

Le nombre de diviseurs premiers, en moyenne

Calculons :

$$\frac{1}{N}\sum_{n=1}^{N}\omega(n) = \frac{1}{N}\sum_{n=1}^{N}\sum_{p|n}1$$
$$= \frac{1}{N}\sum_{p\leqslant N}\sum_{\substack{n\leqslant N\\ p|n}}1 \approx \frac{1}{N}\sum_{p\leqslant N}\frac{N}{p} = \sum_{p\leqslant N}\frac{1}{p}.$$

Le nombre de diviseurs premiers, en moyenne

Calculons :

$$\frac{1}{N}\sum_{n=1}^{N}\omega(n) = \frac{1}{N}\sum_{n=1}^{N}\sum_{p|n}1$$
$$= \frac{1}{N}\sum_{p\leqslant N}\sum_{\substack{n\leqslant N\\ p|n}}1 \approx \frac{1}{N}\sum_{p\leqslant N}\frac{N}{p} = \sum_{p\leqslant N}\frac{1}{p}.$$

Or l'un des premiers résultats concernant la répartition des nombres premiers dit que

$$\sum_{p\leqslant N}\frac{1}{p} \sim \log\log N, \qquad N \to +\infty.$$

Le nombre de diviseurs premiers, en moyenne

Calculons :

$$\frac{1}{N}\sum_{n=1}^{N}\omega(n) = \frac{1}{N}\sum_{n=1}^{N}\sum_{p|n}1$$
$$= \frac{1}{N}\sum_{p\leqslant N}\sum_{\substack{n\leqslant N\\ p|n}}1 \approx \frac{1}{N}\sum_{p\leqslant N}\frac{N}{p} = \sum_{p\leqslant N}\frac{1}{p}.$$

Or l'un des premiers résultats concernant la répartition des nombres premiers dit que

$$\sum_{p\leqslant N}\frac{1}{p} \sim \log\log N, \qquad N \to +\infty.$$

Le nombre de facteurs premiers distincts d'un entier de grande taille N est donc en moyenne $\log\log N$.

Le nombre de diviseurs premiers, en moyenne

Calculons :

$$\frac{1}{N}\sum_{n=1}^{N}\omega(n) = \frac{1}{N}\sum_{n=1}^{N}\sum_{p|n}1$$
$$= \frac{1}{N}\sum_{p\leqslant N}\sum_{\substack{n\leqslant N\\ p|n}}1 \approx \frac{1}{N}\sum_{p\leqslant N}\frac{N}{p} = \sum_{p\leqslant N}\frac{1}{p}.$$

Or l'un des premiers résultats concernant la répartition des nombres premiers dit que

$$\sum_{p\leqslant N}\frac{1}{p} \sim \log\log N, \qquad N \to +\infty.$$

Le nombre de facteurs premiers distincts d'un entier de grande taille N est donc en moyenne $\log\log N$.

C'est le début de la *théorie probabiliste des nombres*.

Un précurseur

La *fonction d'Euler normalisée* : $\dfrac{\varphi(n)}{n} = \prod_{p|n} \left(1 - \dfrac{1}{p}\right).$

Un précurseur

La *fonction d'Euler normalisée* : $\dfrac{\varphi(n)}{n} = \displaystyle\prod_{p|n}\Big(1-\frac{1}{p}\Big)$.

Théorème. (Schoenberg, 1928) – Lorsque $N \to +\infty$, la répartition empirique de $\varphi(n)/n$ pour $n \leqslant N$ devient la même que celle du produit

$$X = \prod_{p}\Big(1-\frac{B_p}{p}\Big)$$

où (B_p) est une suite de variables aléatoires indépendantes telles que

$$\mathbf{P}(B_p = 1) = \frac{1}{p}, \qquad \mathbf{P}(B_p = 0) = 1 - \frac{1}{p}.$$

Un précurseur

La *fonction d'Euler normalisée* : $$\frac{\varphi(n)}{n} = \prod_{p|n}\Big(1 - \frac{1}{p}\Big).$$

Théorème. (Schoenberg, 1928) – Lorsque $N \to +\infty$, la répartition empirique de $\varphi(n)/n$ pour $n \leqslant N$ devient la même que celle du produit

$$X = \prod_{p}\Big(1 - \frac{B_p}{p}\Big)$$

où (B_p) est une suite de variables aléatoires indépendantes telles que

$$\mathbf{P}(B_p = 1) = \frac{1}{p}, \qquad \mathbf{P}(B_p = 0) = 1 - \frac{1}{p}.$$

Autrement dit :

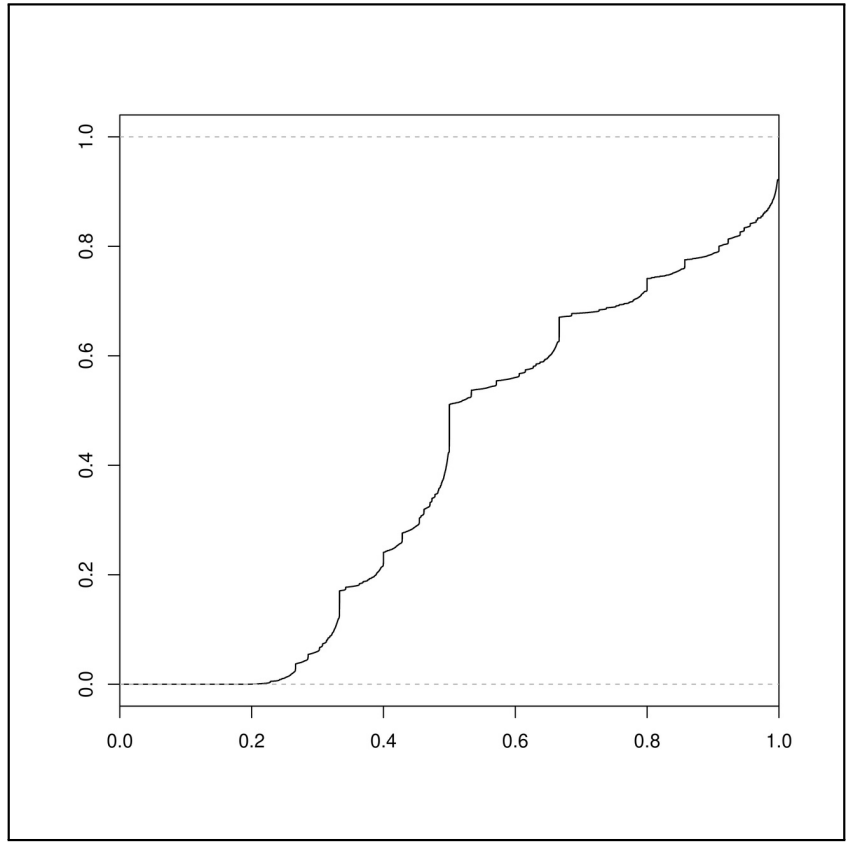
$$\lim_{N\to+\infty} \frac{1}{N}|\{n \leqslant N \mid \varphi(n) \leqslant \alpha n\}| = \mathbf{P}(X \leqslant \alpha).$$

Mystères de la fonction d'Euler

La variable aléatoire X n'est pas du tout générique !

Mystères de la fonction d'Euler

La variable aléatoire X n'est pas du tout générique ! Par exemple, Erdős a démontré que sa fonction de répartition $F(\alpha) = \mathbf{P}(X \leqslant \alpha)$ est continue, strictement croissante, mais que sa dérivée est nulle presque partout sur $[0, 1]$ (mesure sans atome mais singulière par rapport à la mesure de Lebesgue).



Pourquoi cette limite X ?

Écrivons

$$\frac{\varphi(n)}{n} = \prod_p \Big(1 - \frac{b_p(n)}{p}\Big),$$

où $b_p(n) = 1$ si $p \mid n$ et $b_p(n) = 0$ sinon.

Pourquoi cette limite X ?

Écrivons

$$\frac{\varphi(n)}{n} = \prod_p \Big(1 - \frac{b_p(n)}{p}\Big),$$

où $b_p(n) = 1$ si $p \mid n$ et $b_p(n) = 0$ sinon. Intuitivement, pour n grand :

- Il y a «une chance sur p» que $b_p(n) = 1$;
- Si $p_1 \neq p_2$, les quantités $b_{p_1}(n)$ et $b_{p_2}(n)$ sont indépendantes – connaître une de ces valeurs ne dit rien sur l'autre.

Pourquoi cette limite X ?

Écrivons

$$\frac{\varphi(n)}{n} = \prod_p \Big(1 - \frac{b_p(n)}{p}\Big),$$

où $b_p(n) = 1$ si $p \mid n$ et $b_p(n) = 0$ sinon. Intuitivement, pour n grand :

- Il y a «une chance sur p» que $b_p(n) = 1$;
- Si $p_1 \neq p_2$, les quantités $b_{p_1}(n)$ et $b_{p_2}(n)$ sont indépendantes – connaître une de ces valeurs ne dit rien sur l'autre.

On peut donc penser que $\varphi(n)/n$ aura les mêmes propriétés statistiques que

$$\prod_p \Big(1 - \frac{B_p}{p}\Big) = X.$$

Le théorème de Erdős–Kac

On peut naturellement essayer appliquer ce type d'heuristiques à $\omega(n)$.

Le théorème de Erdős–Kac

On peut naturellement essayer appliquer ce type d'heuristiques à $\omega(n)$. Pour N grand et $n \leqslant N$, écrivons

$$\omega(n) = \sum_{p|n} 1 = \sum_{p \leqslant N} b_p(n).$$

Le théorème de Erdős–Kac

On peut naturellement essayer appliquer ce type d'heuristiques à $\omega(n)$. Pour N grand et $n \leqslant N$, écrivons

$$\omega(n) = \sum_{p|n} 1 = \sum_{p \leqslant N} b_p(n).$$

Le raisonnement précédent suggère de rapprocher cela de la somme de variables aléatoires indépendantes

$$\sum_{p \leqslant N} B_p.$$

Le théorème de Erdős–Kac

On peut naturellement essayer appliquer ce type d'heuristiques à $\omega(n)$. Pour N grand et $n \leqslant N$, écrivons

$$\omega(n) = \sum_{p|n} 1 = \sum_{p \leqslant N} b_p(n).$$

Le raisonnement précédent suggère de rapprocher cela de la somme de variables aléatoires indépendantes

$$\sum_{p \leqslant N} B_p.$$

Bien que les variables (B_p) ne soient pas identiquement distribuées, le Théorème Limite Fondamental permet d'en déterminer le comportement asymptotique.

On calcule

$$\mathbf{E}\Big(\sum_{p\leqslant N} B_p\Big) \sim \log\log N, \qquad \mathbf{V}\Big(\sum_{p\leqslant N} B_p\Big) \sim \log\log N,$$

On calcule

$$\mathbf{E}\Big(\sum_{p\leqslant N} B_p\Big) \sim \log\log N, \qquad \mathbf{V}\Big(\sum_{p\leqslant N} B_p\Big) \sim \log\log N,$$

et alors

$$\mathbf{P}\Big(a < \frac{\sum_{p\leqslant N} B_p - \log\log N}{\sqrt{\log\log N}} < b\Big) \to \frac{1}{\sqrt{2\pi}} \int_a^b e^{-t^2/2} dt.$$

On calcule

$$\mathbf{E}\Big(\sum_{p\leqslant N} B_p\Big) \sim \log\log N, \qquad \mathbf{V}\Big(\sum_{p\leqslant N} B_p\Big) \sim \log\log N,$$

et alors

$$\mathbf{P}\Big(a < \frac{\sum_{p\leqslant N} B_p - \log\log N}{\sqrt{\log\log N}} < b\Big) \to \frac{1}{\sqrt{2\pi}} \int_a^b e^{-t^2/2} dt.$$

Et de fait...

Théorème (Erdős–Kac, 1940) – Pour tous réels $a < b$

$$\frac{1}{N}\Big|\Big\{n \leqslant N \mid a < \frac{\omega(n) - \log\log N}{\sqrt{\log\log N}} < b\Big\}\Big| \to \frac{1}{\sqrt{2\pi}} \int_a^b e^{-t^2/2} dt.$$

À qui se fier...

Voici trois énoncés de théorie probabiliste des nombres.

1. Le *théorème* de Erdős–Kac.
2. Une *conjecture* de Gallagher : pour $\lambda > 0$, $r \geqslant 0$,

$$\frac{1}{N}|\{n \leqslant N \mid \pi(n + \lambda \log N) - \pi(n) = r\}| = e^{-\lambda}\frac{\lambda^r}{r!}.$$

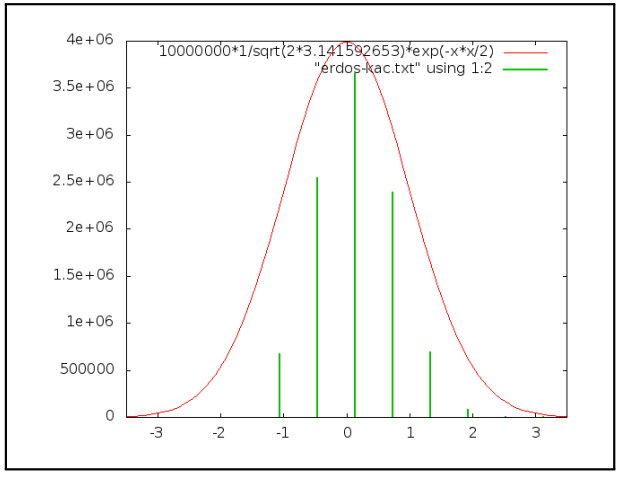
3. Une *conjecture* de Mongomery : notons $\frac{1}{2} + i\gamma_n$, où

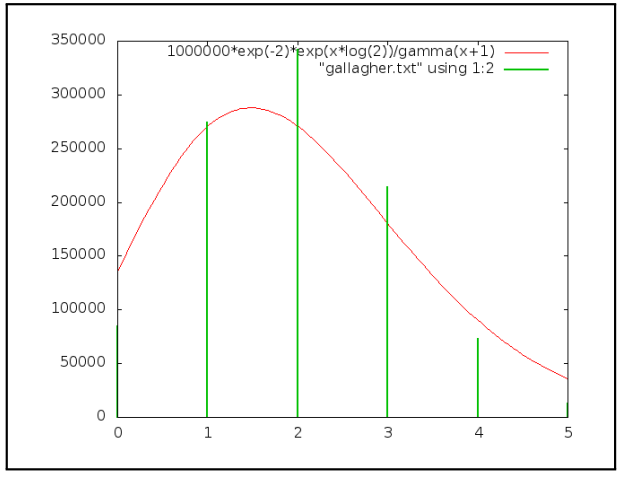
$$0 < \gamma_1 < \gamma_2 \leqslant \cdots \leqslant \gamma_n \leqslant \cdots$$

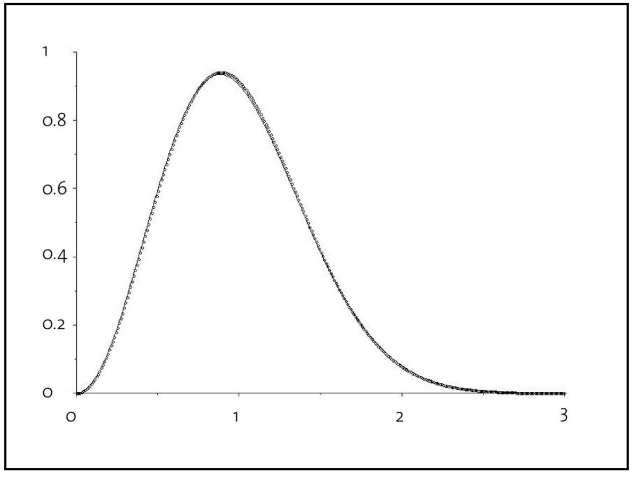
les zéros de partie imaginaire positive de la fonction zêta de Riemann et $\widetilde{\gamma}_n = \frac{1}{2\pi}\gamma_n \log \gamma_n$. Alors pour n grand, la différence $\widetilde{\gamma}_{n+1} - \widetilde{\gamma}_n$ se comporte statistiquement comme l'écart entre les angles propres successifs d'une matrice unitaire «aléatoire» de grande taille.

Le premier énoncé est un théorème ; le second ne l'est pas, mais peut se déduire de conjectures considérées comme «sûres» (Gallagher) ; le troisième est complètement mystérieux.

Le premier énoncé est un théorème ; le second ne l'est pas, mais peut se déduire de conjectures considérées comme «sûres» (Gallagher) ; le troisième est complètement mystérieux.
Les trois énoncés peuvent être testés numériquement.

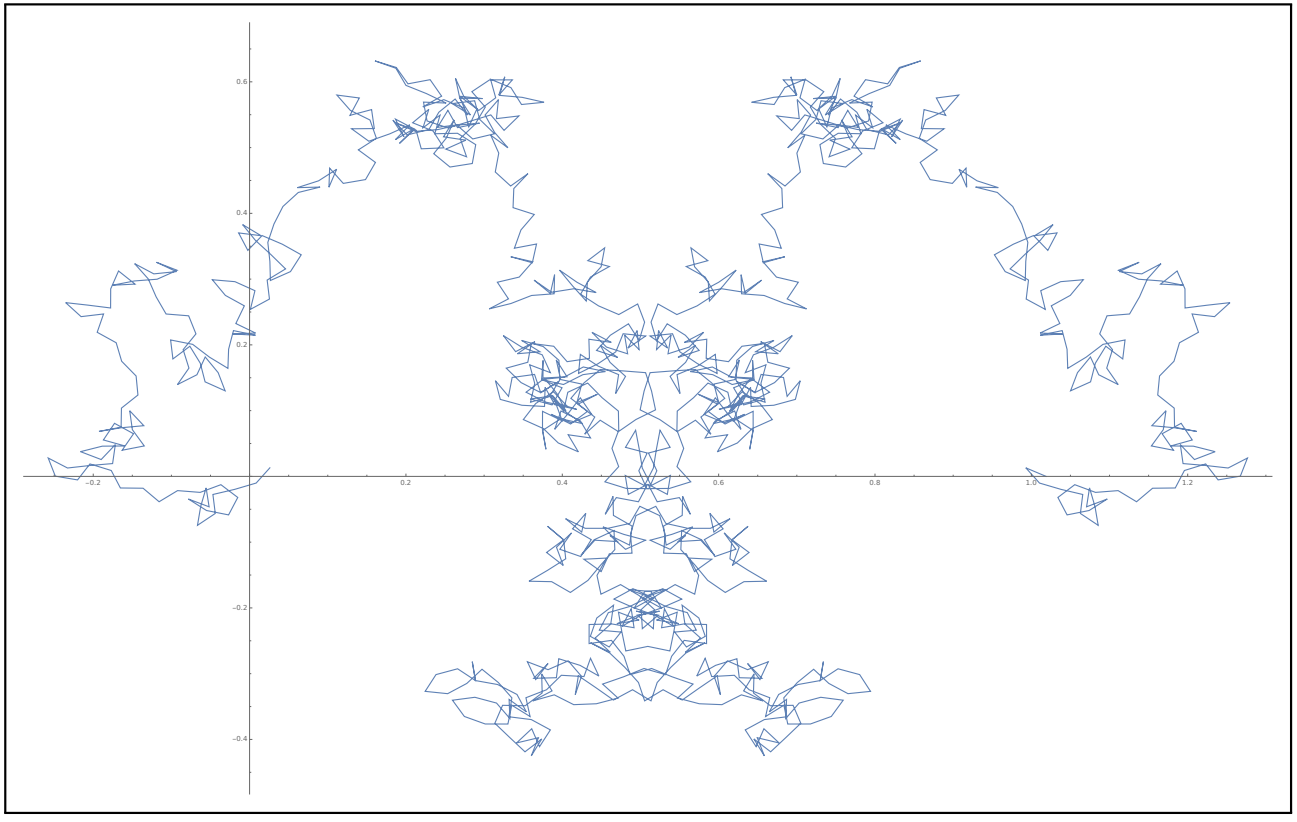






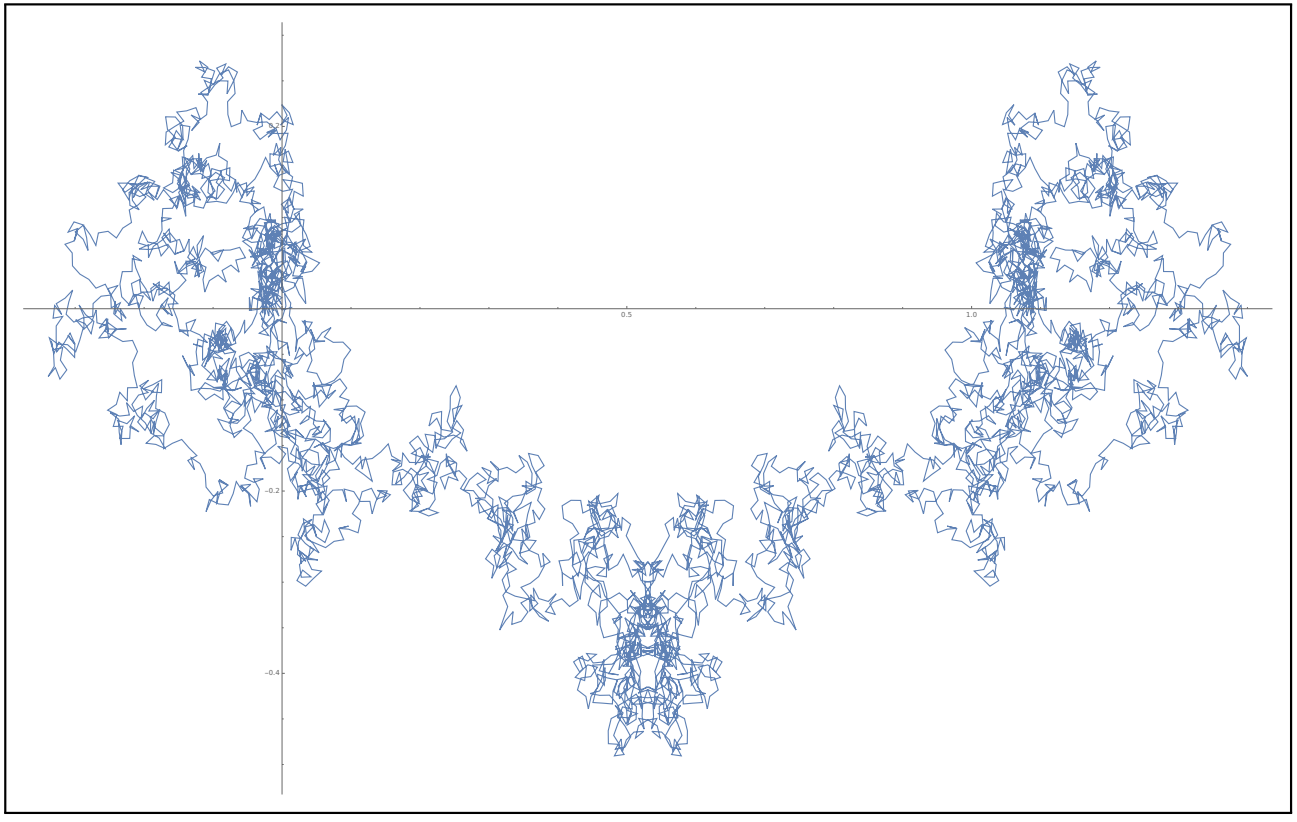
Sommes exponentielles

Considérons maintenant un sujet plutôt différent...



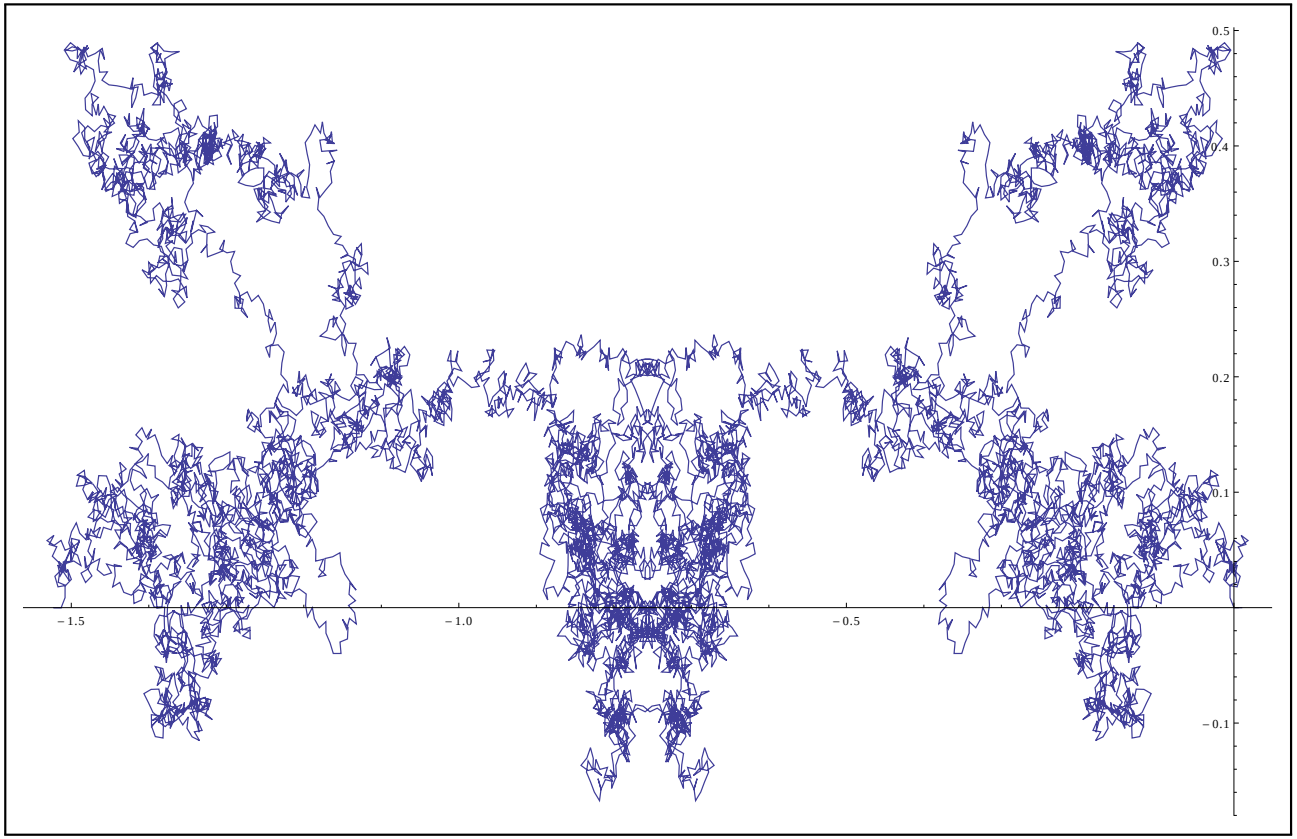
Sommes exponentielles

Considérons maintenant un sujet plutôt différent...



Sommes exponentielles

Considérons maintenant un sujet plutôt différent...



Chemins de Kloosterman

On prend un nombre premier p et deux entiers a et b premiers à p (dans le dernier exemple, $p = 10007$, $a = b = 1$).

Chemins de Kloosterman

On prend un nombre premier p et deux entiers a et b premiers à p (dans le dernier exemple, $p = 10007$, $a = b = 1$). On forme la ligne brisée dans le plan (identifié à $\mathbf{C}$) dont les sommets successifs sont les nombres complexes

$$z_j = \frac{1}{\sqrt{p}} \sum_{1 \leqslant n \leqslant j} \exp\Big(\frac{2i\pi}{p}(an + b\bar{n})\Big), \qquad n\bar{n} \equiv 1 \,(\mathrm{mod}\, p)$$

où $0 \leqslant j \leqslant p-1$. Noter que $z_0 = 0$ et que z_{p-1} est un nombre réel («somme de Kloosterman», définies originellement par Poincaré).

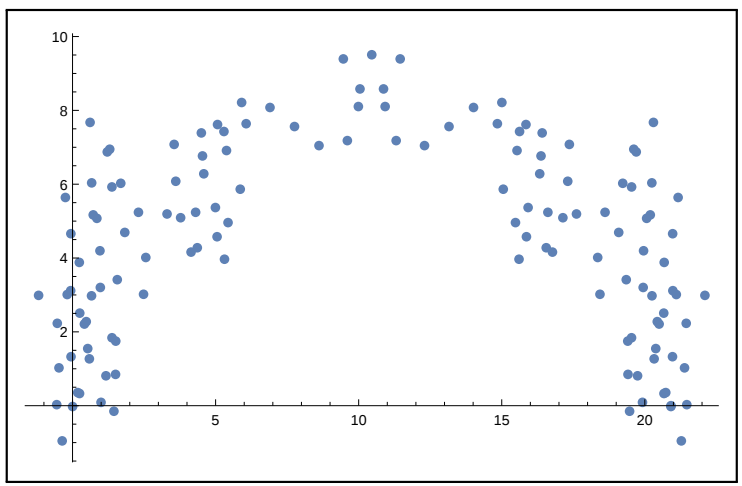
Chemins de Kloosterman

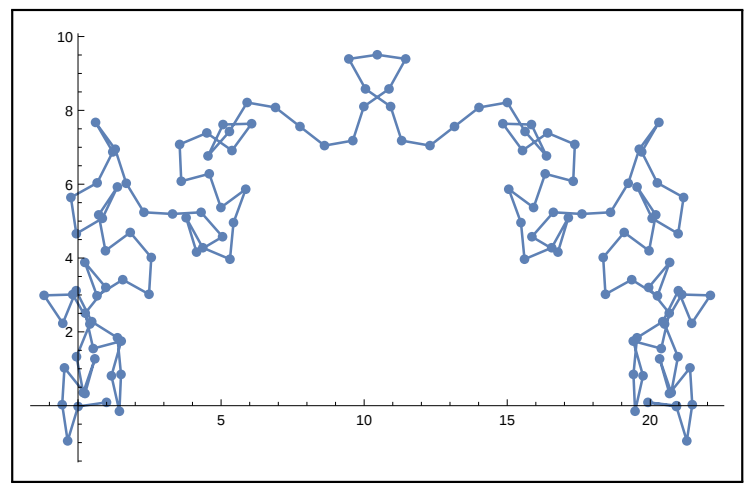
On prend un nombre premier p et deux entiers a et b premiers à p (dans le dernier exemple, $p = 10007$, $a = b = 1$). On forme la ligne brisée dans le plan (identifié à $\mathbf{C}$) dont les sommets successifs sont les nombres complexes

$$z_j = \frac{1}{\sqrt{p}} \sum_{1 \leqslant n \leqslant j} \exp\Big(\frac{2i\pi}{p}(an + b\bar{n})\Big), \qquad n\bar{n} \equiv 1 \,(\mathrm{mod}\, p)$$

où $0 \leqslant j \leqslant p-1$. Noter que $z_0 = 0$ et que z_{p-1} est un nombre réel («somme de Kloosterman», définies originellement par Poincaré).

Plutôt que juste une ligne brisée, on interprète l'image comme le graphe d'une fonction continue $K_p(a,b)\colon [0,1] \to \mathbf{C}$, où $j/p \mapsto z_j$.





Comportement statistique

Théorème (K. – Sawin) – Lorsque $p \to +\infty$ et qu'on fait varier a et b, les fonctions continues $K_p(a, b)$ ont le même comportement statistique que la fonction (série de Fourier) aléatoire

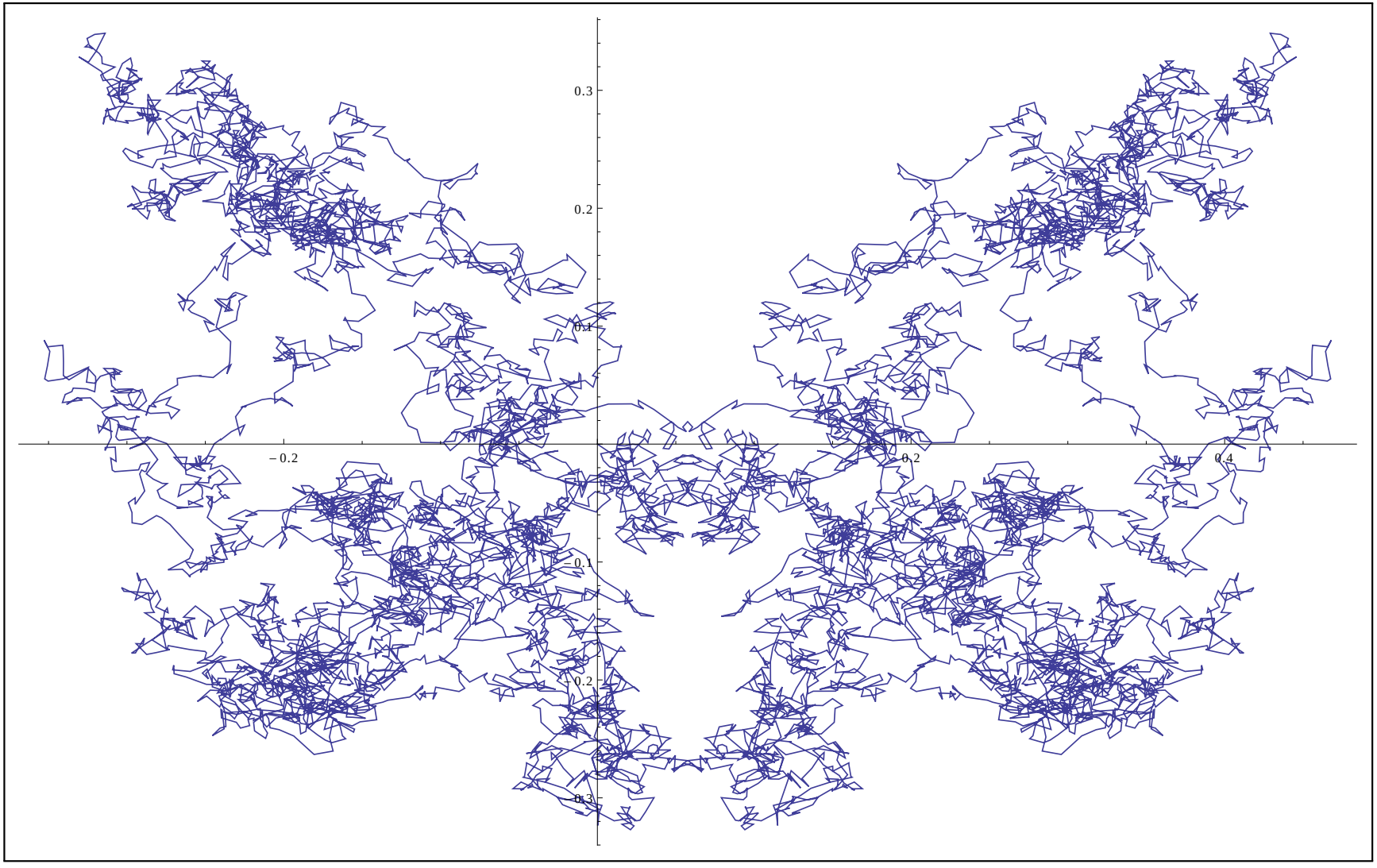
$$Y(t) = tX_0 + \sum_{\substack{h \in \mathbf{Z} \\ h \neq 0}} \frac{\exp(2i\pi ht) - 1}{2i\pi h} X_h$$

où $(X_h)_{h \in \mathbf{Z}}$ est une suite de v.a.i.i.d de loi commune

$$\frac{1}{\pi} \sqrt{1 - \frac{x^2}{4}}\, dx \qquad \text{sur } [-2, 2].$$

(La série converge presque sûrement uniformément, donc la somme est continue ; elle est aussi presque sûrement nulle part dérivable).

Un échantillon de la série aléatoire



Propriétés probabilistes

1. La série ressemble à celle du mouvement brownien, mais comme les v.a. X_h ne sont pas gaussiennes, certaines propriétés sont très différentes.

Propriétés probabilistes

1. La série ressemble à celle du mouvement brownien, mais comme les v.a. X_h ne sont pas gaussiennes, certaines propriétés sont très différentes.
2. En particulier, les z_j ne sont pas une «marche au hasard» au sens usuel (pas de propriété de Markov).

Propriétés probabilistes

1. La série ressemble à celle du mouvement brownien, mais comme les v.a. X_h ne sont pas gaussiennes, certaines propriétés sont très différentes.
2. En particulier, les z_j ne sont pas une «marche au hasard» au sens usuel (pas de propriété de Markov).
3. Si on prend $t = 1$, on trouve que la somme de Kloosterman z_{p-1} est statistiquement répartie comme X_0 ; on a $|X_0| \leqslant 2$, et en fait $|z_{p-1}| \leqslant 2$ pour tout (a, b) («majoration de Weil», 1948).

Propriétés probabilistes

1. La série ressemble à celle du mouvement brownien, mais comme les v.a. X_h ne sont pas gaussiennes, certaines propriétés sont très différentes.
2. En particulier, les z_j ne sont pas une «marche au hasard» au sens usuel (pas de propriété de Markov).
3. Si on prend $t = 1$, on trouve que la somme de Kloosterman z_{p-1} est statistiquement répartie comme X_0 ; on a $|X_0| \leqslant 2$, et en fait $|z_{p-1}| \leqslant 2$ pour tout (a, b) («majoration de Weil», 1948).
4. Or $\sqrt{p} \times z_{p-1}$ est la somme de $p - 1$ nombres complexes de module 1 qui semblent «aléatoires» ; la majoration $|z_{p-1}| \leqslant 2$ correspond à la philosophie du Théorème Limite Central ... mais il n'y a aucune grande déviation !

Ingrédients de la preuve

Bien que les objets considérés soient extrêmement simples et concrets (des sommes finies de racines de l'unité), la preuve du théorème requiert (en plus de résultats assez simples de probabilité dans les espaces de fonctions) des outils de géométrie algébrique très sophistiqués.

Ingrédients de la preuve

Bien que les objets considérés soient extrêmement simples et concrets (des sommes finies de racines de l'unité), la preuve du théorème requiert (en plus de résultats assez simples de probabilité dans les espaces de fonctions) des outils de géométrie algébrique très sophistiqués.

- Interprétation spectrale de sommes de Kloosterman comme traces de matrices dans SU_2 (Weil).

Ingrédients de la preuve

Bien que les objets considérés soient extrêmement simples et concrets (des sommes finies de racines de l'unité), la preuve du théorème requiert (en plus de résultats assez simples de probabilité dans les espaces de fonctions) des outils de géométrie algébrique très sophistiqués.

- Interprétation spectrale de sommes de Kloosterman comme traces de matrices dans SU_2 (Weil).
- Hypothèse de Riemann sur les corps finis dans la forme la plus forte donnée par Deligne (et tout le formalisme sous-jacent).

Ingrédients de la preuve

Bien que les objets considérés soient extrêmement simples et concrets (des sommes finies de racines de l'unité), la preuve du théorème requiert (en plus de résultats assez simples de probabilité dans les espaces de fonctions) des outils de géométrie algébrique très sophistiqués.

- Interprétation spectrale de sommes de Kloosterman comme traces de matrices dans SU_2 (Weil).
- Hypothèse de Riemann sur les corps finis dans la forme la plus forte donnée par Deligne (et tout le formalisme sous-jacent).
- Calculs de «groupes de symétrie» par Katz et propriétés d'indépendances.

Développements

- Versions quantitatives, en particulier pour trouver des «grandes» valeurs de certains z_j (bien sûr z_0 et z_{p-1} sont bornés uniformément, mais pour tout $c > 0$ fixé et $c(p-1) \leqslant j < p-1$, on peut trouver pour p grand des (a, b) tels que z_j est de taille $\log\log p$; Lamzouri, Bonolis, Autissier–Bonolis–Lamzouri).

Développements

- Versions quantitatives, en particulier pour trouver des «grandes» valeurs de certains z_j (bien sûr z_0 et z_{p-1} sont bornés uniformément, mais pour tout $c > 0$ fixé et $c(p-1) \leqslant j < p-1$, on peut trouver pour p grand des (a, b) tels que z_j est de taille $\log\log p$; Lamzouri, Bonolis, Autissier–Bonolis–Lamzouri).
- Calcul du «support» de la série aléatoire pour déterminer quels sont les images qui peuvent vraiment apparaître quand on dessine les chemins de Kloosterman (K.–Sawin).

Développements

- Versions quantitatives, en particulier pour trouver des «grandes» valeurs de certains z_j (bien sûr z_0 et z_{p-1} sont bornés uniformément, mais pour tout $c > 0$ fixé et $c(p-1) \leqslant j < p-1$, on peut trouver pour p grand des (a, b) tels que z_j est de taille $\log\log p$; Lamzouri, Bonolis, Autissier–Bonolis–Lamzouri).
- Calcul du «support» de la série aléatoire pour déterminer quels sont les images qui peuvent vraiment apparaître quand on dessine les chemins de Kloosterman (K.–Sawin).
- En particulier : le support contient des courbes remplissant un carré (J. Bober, Heilbronn Conference 2019).

Application android

http://blogs.ethz.ch/~kowalski/the-kloostermania-page