≪ Nombres aléatoires ≫ versus ≪ nombres génériques ≫

Mathématiques, logique et mécanique céleste

« Nombres aléatoires » versus « nombres génériques »

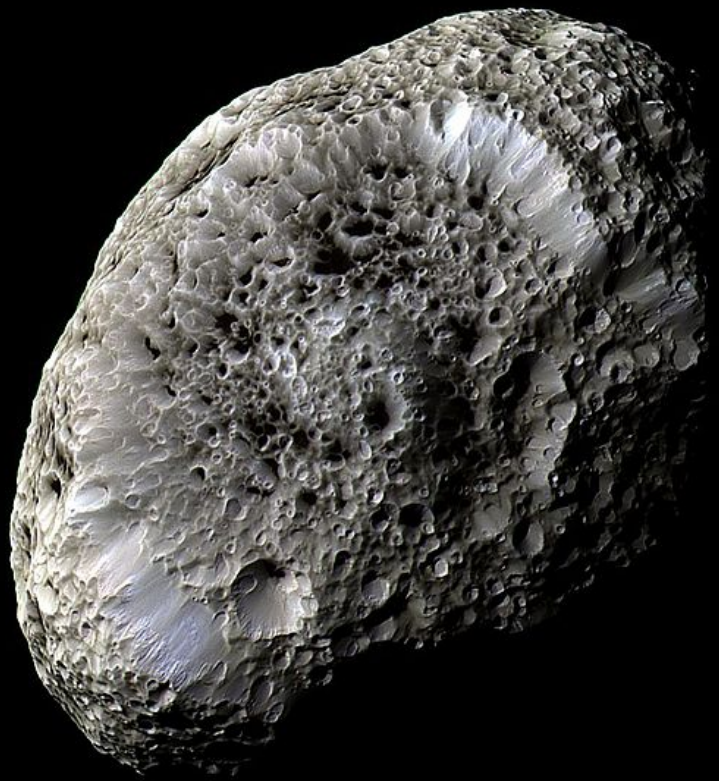
Mathématiques, logique et mécanique céleste

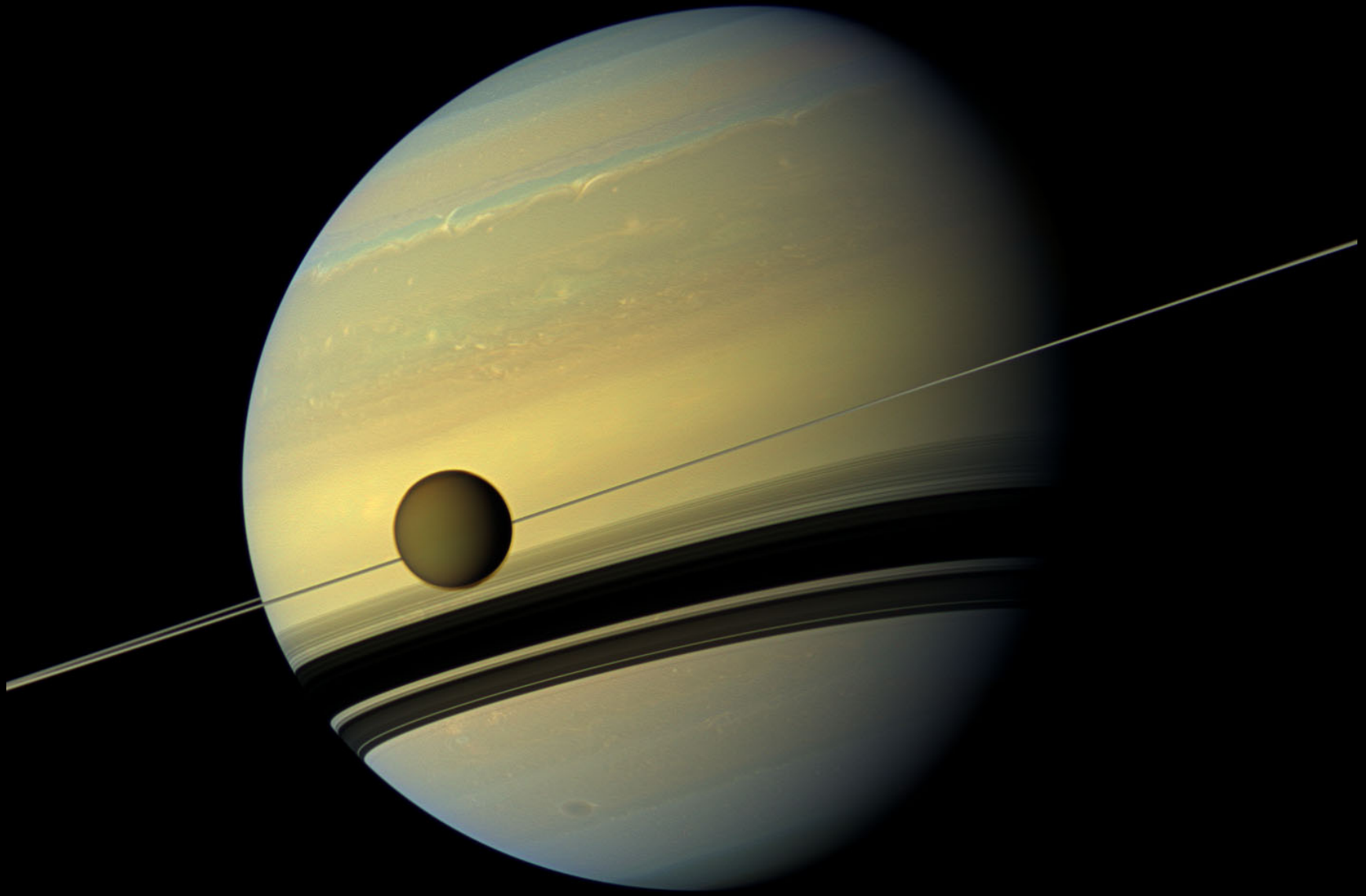
Le système solaire est-il stable ?

« Nombres aléatoires » versus « nombres génériques »

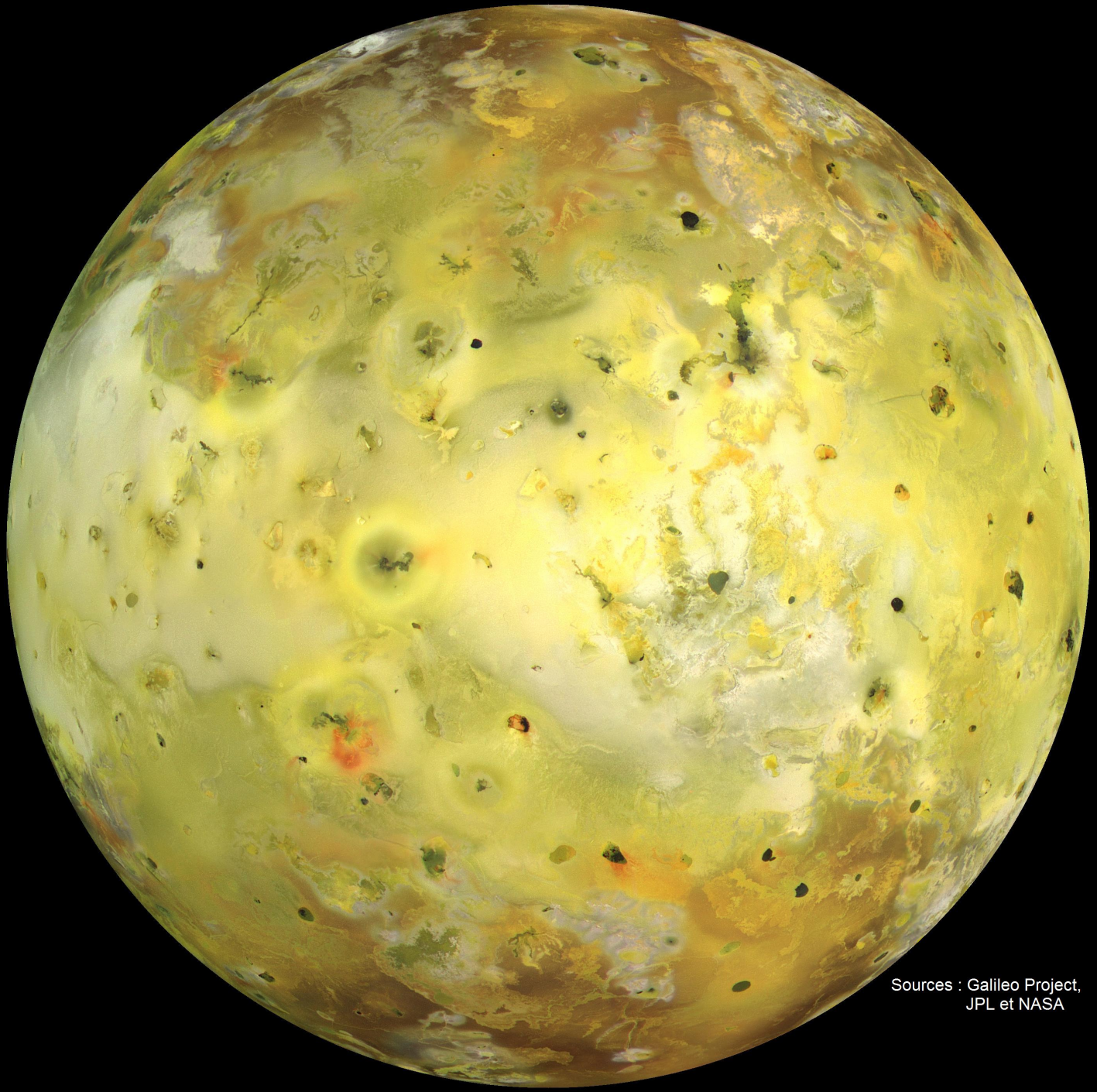
Mathématiques, logique et mécanique céleste

Le système solaire est-il presque périodique ?



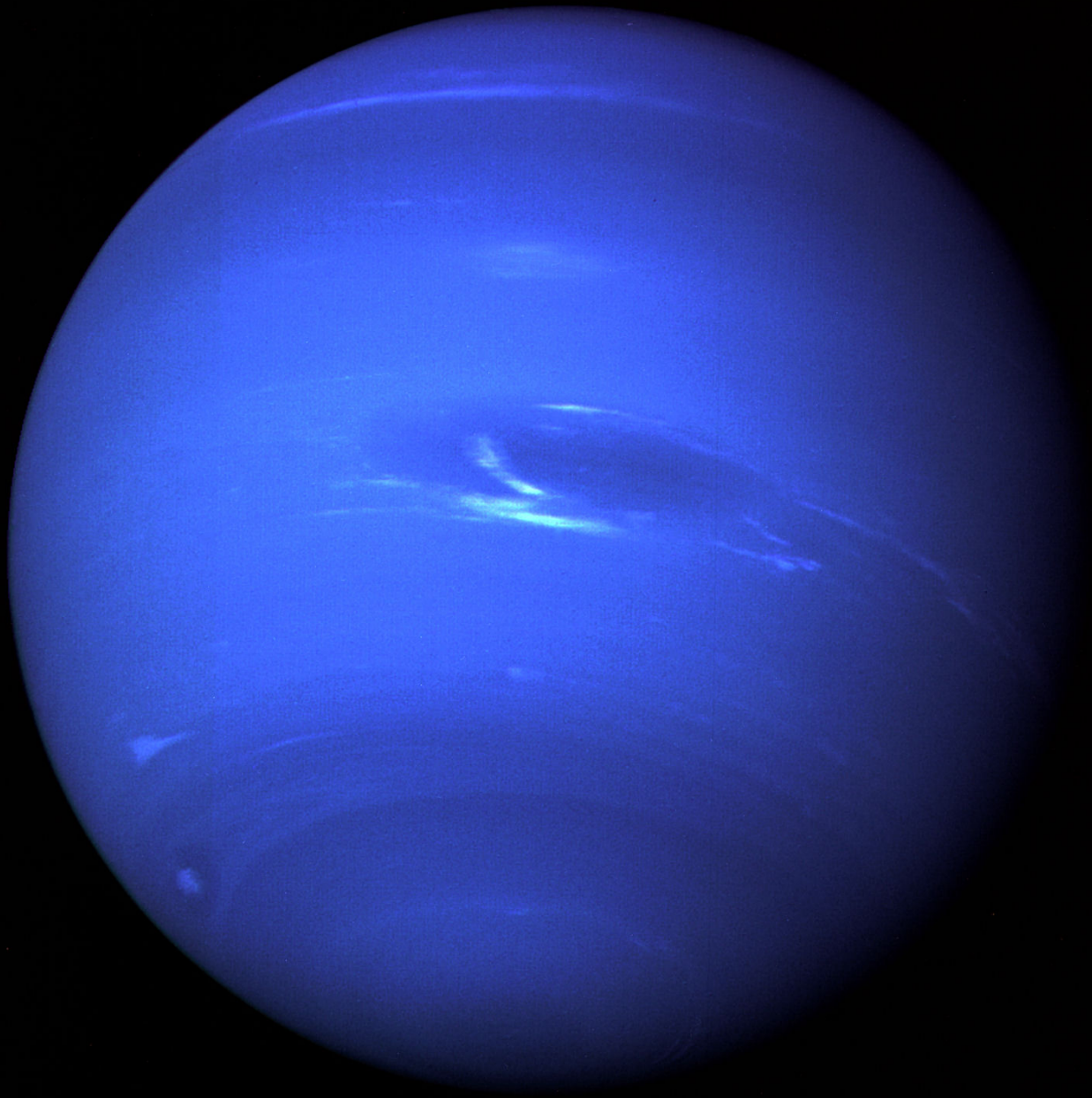


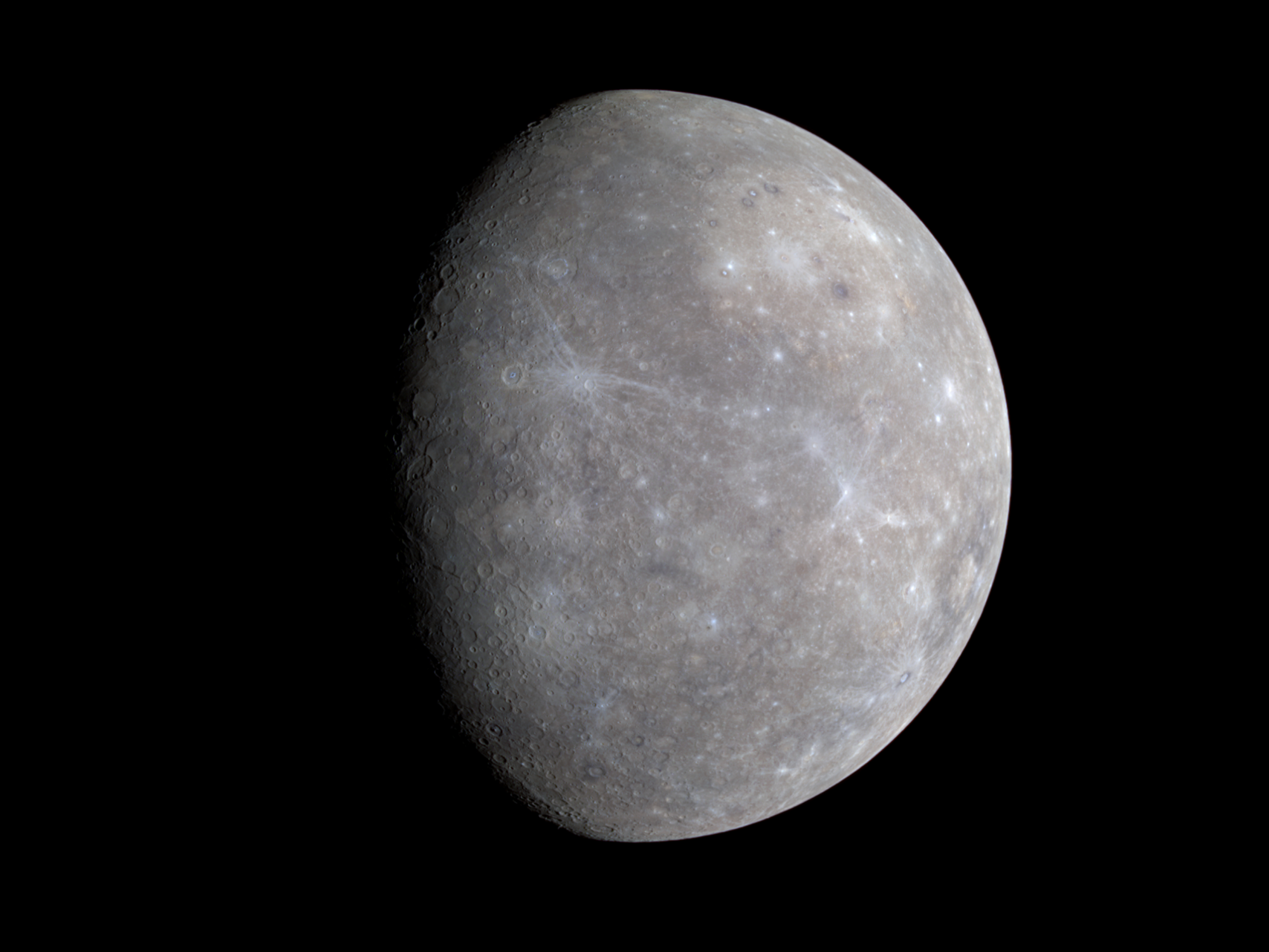
Jean-Dominique Cassini
1625-1712



Sources : Galileo Project,
JPL et NASA

Urbain Le Verrier
1811-1877





Presque périodicité

Le mot de Fibonacci

Presque périodicité

Le mot de Fibonacci

$$0 \to 1 \qquad 1 \to 10$$

Presque périodicité

Le mot de Fibonacci $0 \to 1 \quad 1 \to 10$

Presque périodicité

Le mot de Fibonacci $0 \to 1 \quad 1 \to 10$

0

Presque périodicité

Le mot de Fibonacci $0 \to 1 \quad 1 \to 10$

0
1

Presque périodicité

Le mot de Fibonacci $0 \to 1 \quad 1 \to 10$

0
1
10

Presque périodicité

Le mot de Fibonacci $0 \to 1 \quad 1 \to 10$

0
1
10
10

Presque périodicité

Le mot de Fibonacci $0 \to 1 \quad 1 \to 10$

0
1
10
101

Presque périodicité

Le mot de Fibonacci $0 \to 1 \quad 1 \to 10$

0
1
10
101

Presque périodicité

Le mot de Fibonacci $0 \to 1 \quad 1 \to 10$

0
1
10
101
10110

Presque périodicité

Le mot de Fibonacci $0 \to 1 \quad 1 \to 10$

0
1
10
101
10110
10110101
1011010110110
10110101101101010110
1011010110110101101011011010110
10110101101101011010110110101101011011010110101

Presque périodicité

Le mot de Fibonacci

Le mot de Fibonacci n'est pas périodique

Presque périodicité

Le mot de Fibonacci

Le mot de Fibonacci n'est pas périodique car sa proportion de 1 tend vers l'inverse du nombre d'or.

Presque périodicité

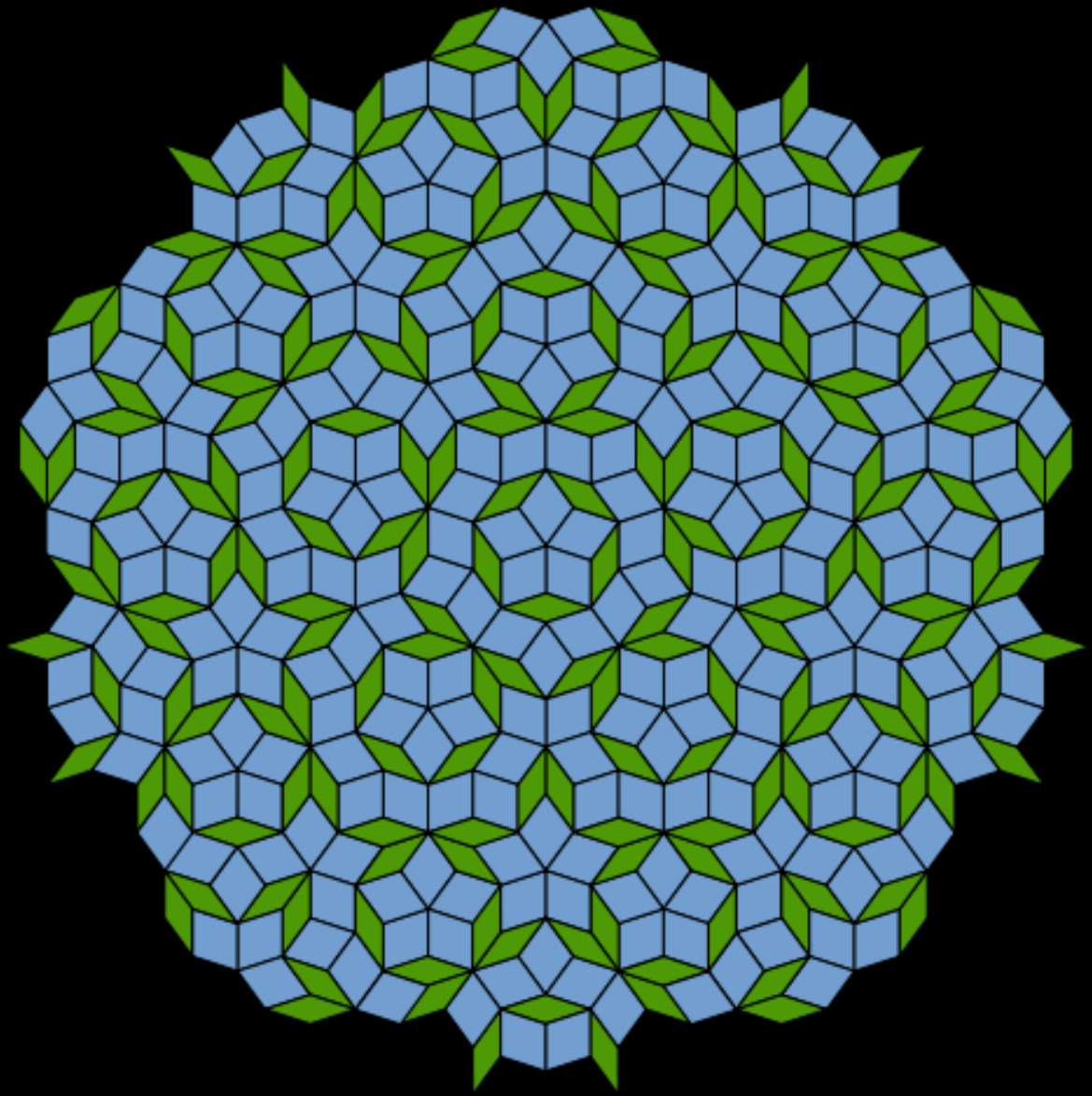
Le mot de Fibonacci

Le mot de Fibonacci n'est pas périodique car sa proportion de 1 tend vers l'inverse du nombre d'or.

Mais ce mot est *presque* périodique : pour tout mot fini qui apparaît dans le mot de Fibonacci, il existe $M \in \mathbb{N}$ tel que tout tronçon du mot de Fibonacci de longueur au moins M contienne le mot fini considéré.

Presque périodicité

En dimension 2, les pavages de Penrose



Presque périodicité

Fonctions presque périodiques

Soit f une fonction continue de $\mathbb{R}$ vers $\mathbb{C}$. Pour $\epsilon > 0$, une ϵ-presque période de f est un réel T tel que

$$\forall t \in \mathbb{R},\ |f(t+T) - f(t)| \leq \epsilon.$$

On dit que f est presque périodique si pour tout ϵ, il existe $M \in \mathbb{N}$ tel que l'ensemble des ϵ-presque périodes de f intersecte tout intervalle de longueur M.

Presque périodicité

Fonctions presque périodiques

Théorème

Une fonction continue $f : \mathbb{R} \to \mathbb{C}$ est presque périodique si et seulement si elle peut être arbitrairement bien approchée en norme infinie par des fonctions de la forme

$$t \mapsto \sum_{j=1}^{n} \alpha_j e^{i\lambda_j t}.$$

Equidistribution

On dit qu'une suite (x_n) d'éléments de $[0,1[$ est équidistribuée si pour tout $(a,b) \in [0,1]^2$,

$$\frac{|\{n \leq N : a \leq x_n \leq b\}|}{N} \underset{n\to\infty}{\longrightarrow} |b-a|.$$

Equidistribution

On dit qu'une suite (x_n) d'éléments de $[0,1[$ est équidistribuée si pour tout $(a,b) \in [0,1]^2$,

$$\frac{|\{n \leq N : a \leq x_n \leq b\}|}{N} \underset{n\to\infty}{\longrightarrow} |b-a|.$$

Théorème

Si α est irrationnel, alors pour tout réel x, la suite des parties fractionnaires de $x + \alpha n$ est équidistribuée.

Un problème plus précis

Soit $\alpha \in \mathbb{R}$. Soit $u : \mathbb{R}/\mathbb{Z} \to \mathbb{R}$ de classe C^∞. On suppose que

$$\int_{\mathbb{R}/\mathbb{Z}} u(x)\mathrm{d}x = 0.$$

Un problème plus précis

Soit $\alpha \in \mathbb{R}$. Soit $u : \mathbb{R}/\mathbb{Z} \to \mathbb{R}$ de classe C^∞. On suppose que

$$\int_{\mathbb{R}/\mathbb{Z}} u(x)\mathrm{d}x = 0.$$

Pour $x \in \mathbb{R}/\mathbb{Z}$, on se demande si cette suite est bornée :

$$(u(x) + u(x+\alpha) + \cdots + u(x+n\alpha))_{n\in\mathbb{N}}$$

Un problème plus précis

Théorème

Le réel α est diophantien si et seulement si pour tout (u, x), la suite considérée est bornée.

Un problème plus précis

Théorème

Le réel α est diophantien si et seulement si pour tout (u, x), la suite considérée est bornée.

Le réel α est dit diophantien s'il existe $\epsilon > 0$ et $M \in \mathbb{N}$ tels que

$$\forall (p, q) \in \mathbb{Z} \times \mathbb{N}^\star, \ \left| \alpha - \frac{p}{q} \right| \geq \frac{\epsilon}{q^M}.$$

Un problème plus précis

Démonstration de l'implication directe

Supposons α diophantien.

Un problème plus précis

Démonstration de l'implication directe

Supposons α diophantien. Nous allons construire une fonction continue $v : \mathbb{R}/\mathbb{Z} \to \mathbb{R}$ telle que

$$\forall x \in \mathbb{R}/\mathbb{Z},\ u(x) = v(x + \alpha) - v(x).$$

Un problème plus précis

Démonstration de l'implication directe

Supposons α diophantien. Nous allons construire une fonction continue $v : \mathbb{R}/\mathbb{Z} \to \mathbb{R}$ telle que

$$\forall x \in \mathbb{R}/\mathbb{Z},\ u(x) = v(x+\alpha) - v(x).$$

L'existence d'un tel v suffit pour conclure, puisqu'elle permet d'écrire la suite d'intérêt sous la forme $(v(x+n\alpha) - v(x))_{n\in\mathbb{N}}$.

Un problème plus précis

On cherche v tel que $\forall x,\ u(x) = v(x+\alpha) - v(x)$.

Notant u_n les coefficients de Fourier de u et v_n ceux d'un hypothétique v qui convient, on a (formellement) :

Un problème plus précis

On cherche v tel que $\forall x,\ u(x) = v(x+\alpha) - v(x)$.

Notant u_n les coefficients de Fourier de u et v_n ceux d'un hypothétique v qui convient, on a (formellement) :

$$\sum_{n\in\mathbb{Z}} u_n e^{2i\pi nx} = \sum_{n\in\mathbb{Z}} v_n e^{2i\pi n(x+\alpha)} - \sum_{n\in\mathbb{Z}} v_n e^{2i\pi nx}$$

Un problème plus précis

On cherche v tel que $\forall x,\ u(x) = v(x+\alpha) - v(x)$.

Notant u_n les coefficients de Fourier de u et v_n ceux d'un hypothétique v qui convient, on a (formellement) :

$$\sum_{n\in\mathbb{Z}} u_n e^{2i\pi nx} = \sum_{n\in\mathbb{Z}} v_n (e^{2i\pi n\alpha} - 1) e^{2i\pi nx}$$

Un problème plus précis

On cherche v tel que $\forall x,\ u(x) = v(x+\alpha) - v(x)$.

Notant u_n les coefficients de Fourier de u et v_n ceux d'un hypothétique v qui convient, on a (formellement) :

$$\sum_{n\in\mathbb{Z}} u_n e^{2i\pi nx} = \sum_{n\in\mathbb{Z}} v_n (e^{2i\pi n\alpha} - 1) e^{2i\pi nx}$$

$$\forall n \in \mathbb{Z},\ u_n = v_n (e^{2i\pi n\alpha} - 1)$$

Un problème plus précis

On cherche v tel que $\forall x,\ u(x) = v(x+\alpha) - v(x)$.

Notant u_n les coefficients de Fourier de u et v_n ceux d'un hypothétique v qui convient, on a (formellement) :

$$\sum_{n\in\mathbb{Z}} u_n e^{2\mathrm{i}\pi nx} = \sum_{n\in\mathbb{Z}} v_n (e^{2\mathrm{i}\pi n\alpha} - 1) e^{2\mathrm{i}\pi nx}$$

$$\forall n \neq 0,\ v_n = u_n/(e^{2\mathrm{i}\pi n\alpha} - 1)$$

Un problème plus précis

On cherche v tel que $\forall x,\ u(x) = v(x+\alpha) - v(x)$.

Il suffit de montrer que la série $\sum_{n\in\mathbb{Z}} u_n/(e^{2\mathrm{i}\pi n\alpha} - 1)$ est absolument convergente.

Un problème plus précis

On cherche v tel que $\forall x,\ u(x) = v(x+\alpha) - v(x)$.

Il suffit de montrer que la série $\sum_{n\in\mathbb{Z}} u_n/(e^{2\mathrm{i}\pi n\alpha} - 1)$ est absolument convergente.

On prend $(\epsilon, M) \in \mathbb{R}_+^\star \times \mathbb{N}$ tel que

$$\forall (p,q) \in \mathbb{Z}\times\mathbb{N}^\star,\ \left|\alpha - \frac{p}{q}\right| \geq \frac{\epsilon}{q^M}.$$

Un problème plus précis

On cherche v tel que $\forall x,\ u(x) = v(x+\alpha) - v(x)$.

Il suffit de montrer que la série $\sum_{n\in\mathbb{Z}} u_n/(e^{2\mathrm{i}\pi n\alpha} - 1)$ est absolument convergente.

On prend $(\epsilon, M) \in \mathbb{R}_+^\star \times \mathbb{N}$ tel que

$$\forall (p,q) \in \mathbb{Z}\times\mathbb{N}^\star,\ \left|\alpha - \frac{p}{q}\right| \geq \frac{\epsilon}{q^M}.$$

$$\left|e^{2i\pi n\alpha} - 1\right| \geq 2/\pi \times d(2\pi n\alpha, 2\pi\mathbb{Z}) \geq 4\epsilon n^{1-M}$$

Un problème plus précis

On cherche v tel que $\forall x,\ u(x) = v(x+\alpha) - v(x)$.

Il suffit de montrer que la série $\sum_{n\in\mathbb{Z}} u_n/(e^{2\mathrm{i}\pi n\alpha} - 1)$ est absolument convergente.

$$\left|e^{2i\pi n\alpha} - 1\right| \geq 2/\pi \times d(2\pi n\alpha, 2\pi\mathbb{Z}) \geq 4\epsilon n^{1-M}$$

Comme u est lisse, la suite $(|u_n|)$ est à décroissance rapide, si bien que $(|u_n|n^{M-1})$ est sommable.

Un problème plus précis

On cherche v tel que $\forall x,\ u(x) = v(x+\alpha) - v(x)$.

Il suffit de montrer que la série $\sum_{n\in\mathbb{Z}} u_n/(e^{2\mathrm{i}\pi n\alpha} - 1)$ est absolument convergente.

$$\left|e^{2i\pi n\alpha} - 1\right| \geq 2/\pi \times d(2\pi n\alpha, 2\pi\mathbb{Z}) \geq 4\epsilon n^{1-M}$$

Comme u est lisse, la suite $(|u_n|)$ est à décroissance rapide, si bien que $(|u_n|n^{M-1})$ est sommable. □

Bref retour au problème initial

Le théorème KAM

Perturbons un système képlérien. Pour de petites perturbations aussi abondantes que le sont les nombres diophantiens parmi les réels, on sait démontrer que le système obtenu est presque-périodique.

C'est le théorème KAM, pour Kolmogorov, Arnold et Moser.

Là est la question.

Les nombres diophantiens sont-ils rares ou abondants ?

Là est la question.

Les nombres diophantiens sont-ils rares ou abondants ?

Oui

Là est la question.

Les nombres diophantiens sont-ils rares ou abondants ?

Oui, ils sont rares et abondants.

Là est la question.

Les nombres diophantiens sont-ils rares ou abondants ?

Ils sont rares au sens de la topologie et abondants au sens des probabilités.

Rares ou abondants ?

Une partie P de $[0,1]$ sera dite grosse au sens des probabilités si elle contient un borélien de mesure de Lebesgue égale à 1.

Rares ou abondants ?

Une partie P de $[0,1]$ sera dite grosse au sens des probabilités si elle contient un borélien de mesure de Lebesgue égale à 1.

Une partie P de $[0,1]$ sera dite grosse au sens de la topologie si elle contient une intersection dénombrable d'ouverts denses.

Rares ou abondants ?

Ces deux notions de grosseur satisfont aux axiomes naturels suivants :

- l'ensemble vide n'est pas gros ;
- l'espace $[0, 1]$ tout entier est gros ;
- si une partie contient une grosse partie, alors elle est également grosse ;
- l'intersection de deux grosses parties est grosse ;

Rares ou abondants ?

Ces deux notions de grosseur satisfont aux axiomes naturels suivants :

- l'ensemble vide n'est pas gros ;
- l'espace $[0, 1]$ tout entier est gros ;
- si une partie contient une grosse partie, alors elle est également grosse ;
- l'intersection de deux grosses parties est grosse ;
- une intersection dénombrable de grosses parties est grosse.

Rares ou abondants ?

Un nombre générique n'est pas diophantien.

Rares ou abondants ?

Un nombre générique n'est pas diophantien.

L'ensemble D des réels diophantiens entre 0 et 1 est défini comme

$$\bigcup_{n,M} \bigcap_{p,q} \left\{ \alpha : \left| \alpha - \frac{p}{q} \right| \geq \frac{1}{nq^M} \right\}.$$

Rares ou abondants ?

Un nombre générique n'est pas diophantien.

L'ensemble D des réels diophantiens entre 0 et 1 est défini comme

$$\bigcup_{n,M} \bigcap_{p,q} \left\{ \alpha : \left| \alpha - \frac{p}{q} \right| \geq \frac{1}{nq^M} \right\}.$$

Or $\bigcap_{p,q} \left\{ \alpha : \left| \alpha - \frac{p}{q} \right| \geq \frac{1}{nq^M} \right\}$ est fermé d'intérieur vide.

Rares ou abondants ?

Un nombre générique n'est pas diophantien.

L'ensemble D des réels diophantiens entre 0 et 1 est défini comme

$$\bigcup_{n,M} \bigcap_{p,q} \left\{ \alpha : \left| \alpha - \frac{p}{q} \right| \geq \frac{1}{nq^M} \right\}.$$

Or $\bigcap_{p,q} \left\{ \alpha : \left| \alpha - \frac{p}{q} \right| \geq \frac{1}{nq^M} \right\}$ est fermé d'intérieur vide. $\square$

Rares ou abondants ?

Un nombre aléatoire est diophantien.

L'ensemble D des réels diophantiens entre 0 et 1 est défini comme

$$\bigcup_{M}\bigcup_{n}\bigcap_{p,q}\left\{\alpha : \left|\alpha - \frac{p}{q}\right| \geq \frac{1}{nq^{M}}\right\}.$$

Rares ou abondants ?

Un nombre aléatoire est diophantien.

L'ensemble D des réels diophantiens entre 0 et 1 est défini comme

$$\bigcup_M \bigcup_n \bigcap_{p,q} \left\{ \alpha : \left| \alpha - \frac{p}{q} \right| \geq \frac{1}{nq^M} \right\}.$$

Montrons que le complémentaire de $\bigcap_{p,q} \left\{ \alpha : \left| \alpha - \frac{p}{q} \right| \geq \frac{1}{nq^3} \right\}$ a une mesure qui tend vers 0 quand n tend vers l'infini.

Rares ou abondants ?

Un nombre aléatoire est diophantien.

L'ensemble D des réels diophantiens entre 0 et 1 est défini comme

$$\bigcup_M \bigcup_n \bigcap_{p,q} \left\{ \alpha : \left| \alpha - \frac{p}{q} \right| \geq \frac{1}{nq^M} \right\}.$$

Le borélien $\bigcup_{p,q} \left\{ \alpha \in [0,1] : \left| \alpha - \frac{p}{q} \right| < \frac{1}{nq^3} \right\}$ a une mesure qui tend vers 0 quand n tend vers l'infini car cette mesure est majorée par $2n^{-1} \sum_q \frac{q+1}{q^3}$.

Rares ou abondants ?

Un nombre aléatoire est diophantien.

L'ensemble D des réels diophantiens entre 0 et 1 est défini comme

$$\bigcup_M \bigcup_n \bigcap_{p,q} \left\{ \alpha : \left| \alpha - \frac{p}{q} \right| \geq \frac{1}{nq^M} \right\}.$$

Le borélien $\bigcup_{p,q} \left\{ \alpha \in [0,1] : \left| \alpha - \frac{p}{q} \right| < \frac{1}{nq^3} \right\}$ a une mesure qui tend vers 0 quand n tend vers l'infini car cette mesure est majorée par $2n^{-1} \sum_q \frac{q+1}{q^3}$.

□

Nombres aléatoires et nombres génériques

On a plus ou moins donné un sens à « un nombre générique/aléatoire vérifie une propriété » mais on ne sait pas donner de sens à ce qu'est un nombre générique/aléatoire.

Nombres aléatoires et nombres génériques

Un élément de $[0,1]$ est dit aléatoire s'il appartient à toute partie qui est grosse au sens des probabilités.

Un élément de $[0,1]$ est dit générique s'il appartient à toute partie qui est grosse au sens de la topologie.

Nombres aléatoires et nombres génériques

Un élément de $[0,1]$ est dit aléatoire s'il appartient à toute partie calculable qui est grosse au sens des probabilités.

Un élément de $[0,1]$ est dit générique s'il appartient à toute partie calculable qui est grosse au sens de la topologie.

Nombres aléatoires et nombres génériques

Quelques faits

Nombres aléatoires et nombres génériques

Quelques faits

Un nombre qui est générique ou aléatoire n'est pas calculable.

Nombres aléatoires et nombres génériques

Quelques faits

Un nombre qui est générique ou aléatoire n'est pas calculable.

L'ensemble des nombres génériques est gros au sens de la topologie.

Nombres aléatoires et nombres génériques

Quelques faits

Un nombre qui est générique ou aléatoire n'est pas calculable.

L'ensemble des nombres génériques est gros au sens de la topologie.

L'ensemble des nombres aléatoires est gros au sens des probabilités.

Nombres aléatoires et nombres génériques

Quelques faits

Un nombre qui est générique ou aléatoire n'est pas calculable.

L'ensemble des nombres génériques est gros au sens de la topologie.

L'ensemble des nombres aléatoires est gros au sens des probabilités.

Aucun nombre n'est à la fois générique et aléatoire.

Nombres aléatoires et nombres génériques

Définition de la calculabilité

On s'intéresse, pour simplifier, à $(\{0,1\}^{\mathbb{N}}, \mathrm{Ber}(1/2)^{\otimes\mathbb{N}})$ plutôt qu'à $([0,1], \mathrm{d}x)$. L'espace $\{0,1\}^{\mathbb{N}}$ est muni de la topologie produit. Un ouvert U est dit calculable s'il existe un programme qui, étant donné un mot fini m, répond à la question suivante :

« Est-ce que tout élément de $\{0,1\}^{\mathbb{N}}$ commençant par m appartient à U ? »

Nombres aléatoires et nombres génériques

Définition de la calculabilité

Une suite d'ouverts (U_n) est dite calculable s'il existe un programme qui, étant donnés un mot fini m et un entier n, répond à la question suivante :

« Est-ce que tout élément de $\{0,1\}^{\mathbb{N}}$ commençant par m appartient à U_n ? »

Nombres aléatoires et nombres génériques

Enfin les vraies définitions...

Un élément de $\{0,1\}^{\mathbb{N}}$ est dit aléatoire si pour toute suite décroissante calculable d'ouverts de mesure tendant vers 0, il n'appartient qu'à un nombre fini de ces ouverts.

Un élément de $\{0,1\}^{\mathbb{N}}0$ est dit générique s'il appartient à tout ouvert dense calculable.

Nombres aléatoires et nombres génériques

Le nombre Ω de Chaitin

Tapez en C un programme infini en choisissant le $n^{\text{ème}}$ caractère du programme uniformément parmi ceux disponibles, et ce de façon indépendante.

Nombres aléatoires et nombres génériques

Le nombre Ω de Chaitin

Tapez en C un programme infini en choisissant le $n^{\text{ème}}$ caractère du programme uniformément parmi ceux disponibles, et ce de façon indépendante.

On note Ω la probabilité que le programme (auquel on ne donne aucun argument en entrée) tourne correctement et s'arrête en temps fini.

Nombres aléatoires et nombres génériques

Le nombre Ω de Chaitin

Tapez en C un programme infini en choisissant le $n^{\text{ème}}$ caractère du programme uniformément parmi ceux disponibles, et ce de façon indépendante.

On note Ω la probabilité que le programme (auquel on ne donne aucun argument en entrée) tourne correctement et s'arrête en temps fini.

Le nombre Ω, bien que défini de façon univoque, est aléatoire : en particulier, il n'est pas calculable.

Nombres aléatoires et nombres génériques

Le nombre Ω de Chaitin

Théorème

Quelle que soit l'axiomatisation (raisonnable) des mathématiques que vous choisissiez, seul un nombre fini des énoncés suivants est décidable :

1. *le premier chiffre de Ω est 0,*
2. *le deuxième chiffre de Ω est 0,*
3. *le troisième chiffre de Ω est 0,*
4. *le quatrième chiffre de Ω est 0,*

   . . .

Merci pour votre attention.

Merci aux sources suivantes pour les images astronomiques :

NASA, JPL, SSI.

Les diapositives de cet exposé ainsi que des références et compléments sont disponibles ici :

`perso.ens-lyon.fr/sebastien.martineau/pampers`