Numération et théorie des nombres

Boris Adamczewski

Institut Camille Jordan
Boris.Adamczewski@math.univ-lyon1.fr
http ://math.univ-lyon1.fr/~adamczew

Préambule

—

Des nombres et des mots.

Le développement décimal

$$\frac{\pi\sqrt{163}}{3} - \log(640320)\ ?$$

L'écriture en base 10 des entiers ou des réels permet d'effectuer assez simplement un certain nombre d'opérations : additions, soustractions, multiplications, divisions...

$$\begin{array}{ccc} [0,1] & \longrightarrow & \{0,1,\ldots,9\}^{\mathbb{N}} \\ \xi & \longmapsto & 0.a_1a_2\cdots = \displaystyle\sum_{n=1}^{+\infty} \frac{a_n}{10^n}\,. \end{array}$$

À tout nombre réel correspond un unique mot fini ou infini sur l'alphabet $\{0,1,\ldots,9\}$ correspondant à sa suite de chiffres.

Nombres $\Longrightarrow$ Mots

Le développement décimal

Réciproquement, à tout mot fini ou infini sur l'alphabet $\{0, 1, \ldots, 9\}$ (ne se terminant pas par une infinité d'occurrences consécutives du chiffre 9) correspond un unique nombre réel.

Mots $\Longrightarrow$ Nombres

Le développement en fraction continue

Tout nombre réel admet un unique développement en fraction continue.

$$\begin{array}{ccc} [0,1] & \longrightarrow & (\mathbb{N}_{\geq 1})^{\mathbb{N}} \\ \xi & \longmapsto & [0, a_1, a_2, \ldots] = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}} \end{array}$$

À toute suite d'entiers strictement positifs correspond un unique nombre réel (si cette suite est finie, elle ne doit pas se terminer par le chiffre 1).

Analyse diophantienne. L'inégalité

$$\left| \xi - \frac{p}{q} \right| < \varphi(q)$$

a-t-elle un nombre fini ou infini de solutions rationnelles p/q ?

Si ξ est irrationnel et $\varphi(q) = 1/q^2$ alors il existe toujours une infinité de solutions, ce qui n'est plus nécessairement le cas si $q^2\varphi(q)$ tend vers zéro.

Quelques autres exemples classiques de numérations

• Les β-numérations : on remplace l'entier 10 par un nombre réel. $\Longrightarrow$ liens avec les systèmes dynamiques, les pavages de Rauzy–Thurston, la modélisation des quasi-cristaux...

• Les fractions continues de Rosen. $\Longrightarrow$ utile pour comprendre les géodésiques de certaines surfaces de Hecke (qui généralisent la surface modulaire).

• Le développement de Hensel des nombres p-adiques (remplace la base 10 dans ce contexte).

• Le développement en série de Laurent des fractions rationnelles.

Compter… pas seulement

—

Le don d'ubiquité.

Briller en société : le jeu de Nim

Ce jeu se joue à deux joueurs. On forme un nombre arbitraire de tas comportant chacun un nombre arbitraire d'allumettes.

Règle du jeu. Chaque joueur peut alternativement prendre autant d'allumettes (mais au moins une) qu'il le souhaite dans l'un des tas de son choix.

Le vainqueur est celui qui prend la dernière allumette.

Solution. L'un des deux joueurs a une stratégie gagnante qui repose sur l'écriture binaire des entiers.

Groupe des unités d'un corps quadratique réel


Pierre de Fermat.

On cherche à déterminer le groupe des unités de l'anneau des entiers du corps quadratique $\mathbb{Q}(\sqrt{d})$.
Le problème se ramène à la résolution de l'équation diophantienne de Pell–Fermat :

$$X^2 - dY^2 = \pm 1\,.$$

C'est-à-dire, à la recherche des solutions (X, Y) entières de cette équation.

Si d est un entier positif qui n'est pas un carré, l'équation de Pell-Fermat a une infinité de solutions.

Solution. Développer $\sqrt{d}$ en fraction continue.

Si (X, Y) est une solution positive, alors

$$(X - \sqrt{d}\,Y)(X + \sqrt{d}\,Y) = \pm 1$$

et donc

$$\left|\sqrt{d} - \frac{X}{Y}\right| = \frac{1}{Y(X + \sqrt{d}\,Y)} < \frac{1}{2Y^2}\,.$$

Minima des formes quadratiques binaires indéfinies

Considérons une forme quadratique binaire

$$f(X,Y) = aX^2 + bXY + cY^2$$

à coefficient réels. Son discriminant est $\Delta(f) = b^2 - 4ac$.
On suppose que $\Delta(f) \neq 0$ et on pose

$$c(f) = m(f)/\sqrt{|\Delta(f)|}\,,$$

où $m(f)$ est le minimum de $|f(x,y)|$ sur $\mathbb{Z}^2 \setminus \{(0,0)\}$.

Spectre de Markoff. Ensemble des valeurs atteintes par $1/c(f)$ lorsque f parcourt les formes quadratiques binaires indéfinies ($\Delta(f) > 0$).

$$\mathcal{M} \cap \mathbb{R}_{<3} = \left\{\sqrt{5},\ \sqrt{8},\ \sqrt{221}/5,\ \sqrt{1517}/13,\ \ldots\right\}.$$

A. Markoff, *Sur les formes quadratiques binaires indéfinies*, Math. Ann., 1879.

Solution. Développer les racines de $f(x,1)$ en fraction continue.

Zéros des récurrences linéaires : le théorème de Skolem–Mahler–Lech

Soit $\mathbf{a} = (a_n)_{n\geq 0}$ une suite vérifiant une relation de récurrence linéaire sur un corps $\mathbb{K}$ de caractéristique nulle.

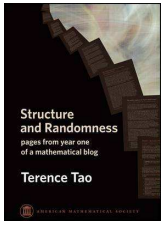
$$a_n = \lambda_1 a_{n-1} + \lambda_2 a_{n-2} + \cdots + \lambda_d a_{n-d}\,, \quad \lambda_k \in \mathbb{K}\,.$$

Posons

$$\mathcal{Z}(\mathbf{a}) = \{n \in \mathbb{N} \mid a_n = 0\}$$

Théorème. L'ensemble $\mathcal{Z}(\mathbf{a})$ est composé d'un ensemble fini et d'une union finie de progressions arithmétiques.

• Les preuves reposent toutes sur de l'analyse p-adique et rendent ce résultat ineffectif.



T. Tao, *Effective Skolem-Mahler-Lech theorem* in Structure and Randomness, Amer. Math. Soc., 2008.

Le théorème de Skolem–Mahler–Lech en caractéristique non nulle

Si $\mathbb{K}$ est un corps de caractéristique non nulle, la situation est plus délicate. Soit

$$a_n = (1+t)^n - t^n - 1 \in \mathbb{F}_p(t)\,.$$

La suite $\mathbf{a} = (a_n)_{n\geq 1}$ vérifie une relation de récurrence linéaire et

$$\mathcal{Z}(\mathbf{a}) = \{1, p, p^2, p^3, \ldots\}\ .$$

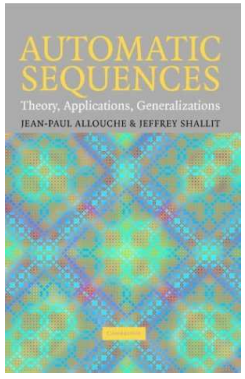
Solution. Utiliser le développement en base p de l'entier n.

Théorème. Si $\mathbb{K}$ est un corps de caractéristique p, l'ensemble $\mathcal{Z}(\mathbf{a})$ est un ensemble reconnaissable par un p-automate fini.

H. Derksen, *A Skolem-Mahler-Lech theorem in positive characteristic and finite automata*, Invent. Math., 2007.

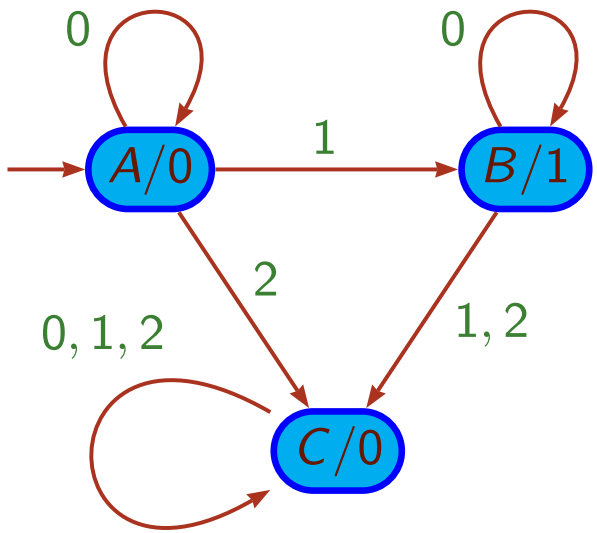
- L'approche de Derksen est effective !

Ensembles d'entiers reconnus par un automate fini



Un ensemble d'entiers $\mathcal{E}$ est k-automatique, s'il existe un automate fini qui, lorsqu'on lui donne en entrée le développement de l'entier n en base k, retourne le symbole 1 si n appartient à $\mathcal{E}$ et le symbole 0 sinon.

Exemple. La suite des puissances de 3, $\{1, 3, 9, 27, 81, \ldots\}$, est 3-automatique.



Théorème (Minsky and Papert). La suite des nombres premiers n'est pas automatique.

Ces nombres qui n'existent pas

—

Le poids des mots.

Construire des nombres transcendants

Inégalité de Liouville, 1844. Si α est un nombre algébrique de degré d, alors il existe $c > 0$ telle que

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^d},$$

pour tout nombre rationnnel p/q.

Idée. Si le développement décimal d'un nombre réel ξ contient de très grandes plages de 0, alors ce nombre est très bien approché par des nombres rationnels.

Exemple. Le nombre

$$\sum_{n\geq 1} \frac{1}{10^{n!}} = 0.110\,010\,000\,000\,000\cdots$$

est transcendant.

Approcher un nombre réel par des nombres algébriques

Théorème (Davenport et Schmidt, 1969). Soit ξ un nombre réel qui n'est ni rationnel, ni quadratique. Alors, il existe une contante c et une infinité d'entiers algébriques cubiques α tels que

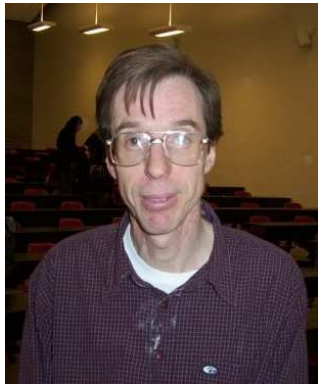
$$|\xi - \alpha| < \frac{c}{H(\alpha)^{\gamma^2}},$$

où $\gamma = (1+\sqrt{5})/2$ et $H(\alpha)$ désigne la hauteur de α.

Rappel. La hauteur (naïve) d'un nombre algébrique est le maximum des valeurs absolues des coefficients de son polynôme minimal.

En lien avec une conjecture classique de Wirsing, on s'attendait à ce que l'exposant γ^2 puisse être remplacé par 3... jusqu'à ce que Roy prouve le contraire : la valeur γ^2 est en fait optimale !

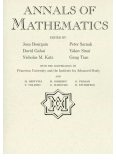
Nombres extrémaux de Roy



Théorème (Roy). Il existe une constante c et un nombre réel ξ qui n'est ni rationnel, ni quadratique et tel que

$$|x_0| < X,\ |x_0\xi - x_1| < cX^{-1/\gamma},\ |x_0\xi^2 - x_2| < cX^{-1/\gamma},$$

a une solution non nulle $(x_0, x_1, x_2) \in \mathbb{Z}^3$ pour tout $X > 1$.



D. Roy, *Approximation to real numbers by cubic algebraic integers, II*, Annals of Math., 2003.

Idée. Utiliser le développement en fraction continue. Une solution est donnée par le nombre

$$\xi = [1, 2, 1, 1, 2, 1, 2, 1, 1, 2, \ldots].$$

Mot de Fibonacci. On pose $U_0 = 1$, $U_1 = 12$, puis $U_{n+1} = U_n U_{n-1}$. On obtient successivement 1, 12, 121, 12112, 12112121,...

Roy utilise le fait que le mot de Fibonacci est le mot apériodique avec le plus de préfixes palindromes.

Approche systématique

—

La tentation bourbakiste.

Les questions classiques

1. Conditions d'admissibilité et vitesse de convergence.

2. Caractérisation des nombres ayant un développement :
   - ultimement périodique,
   - fini,
   - purement périodique.

3. Déterminer certaines propriétés statistiques du développement d'un nombre « choisi au hasard ».

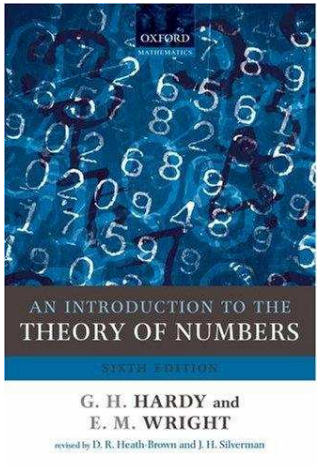
4. Determiner certaines propriétés des suites de chiffres de nombres « naturels » comme $\sqrt{2}$ ou π.

Développement décimal

• Le développement décimal d'un nombre réel ξ est fini $\Longleftrightarrow$ ξ est un nombre rationnel dont le dénominateur (sous forme réduite) est une puissance de 10.

• Le développement décimal d'un nombre réel ξ est ultimement périodique $\Longleftrightarrow$ ξ est un nombre rationnel.

• Le développement décimal d'un nombre réel ξ est purement périodique $\Longleftrightarrow$ ξ est un nombre rationnel dont le dénominateur (sous forme réduite) est premier avec 10.



Développement en fraction continue

• Le développement en fraction continue d'un nombre réel ξ est fini $\iff$ ξ est un nombre rationnel.

Exemple. $\frac{30}{13} = [2, 3, 4]$.

Théorème (Lagrange). Le développementen fraction continue d'un nombre réel ξ est ultimement périodique $\iff$ ξ est un nombre irrationnel quadratique.

Exemple. $\sqrt{2} = [1, 2, 2, 2, \ldots]$.

Théorème (Galois). Le développement en fraction continue d'un nombre réel $\xi > 1$ est purement périodique $\iff$ ξ est un nombre irrationnel quadratique dont le conjugué de Galois appartient à l'intervalle $[-1, 0]$.

Exemple. $(1 + \sqrt{5})/2 = [1, 1, 1, \ldots]$.

Développement d'un nombre « choisi au hasard »

Définition. Un nombre réel est dit simplement normal en base b si chaque chiffre apparaît dans son développement en base b avec la même fréquence $1/b$.

Théorème (Borel). Presque tout nombre réel est un nombre normal.

É. Borel, *Les probabilités dénombrables et leurs applications arithmétiques*, Rend. Circ. Mat. Palermo, 1909.

Soit X_n la variable aléatoire réelle qui associe à un nombre x la valeur 1 si sa n-ième décimale est égale à 7 et 0 sinon.

Loi forte des grands nombres. Pour presque tout nombre réel x, on a :

$$\frac{1}{N}\sum_{k=0}^{N-1} X_k(x) \to \frac{1}{10}\,.$$

Développement d'un nombre « choisi au hasard »

Notons $T : \quad x \longmapsto 1/x \mod 1$ l'application de Gauß. Le système dynamique mesuré $\mathcal{X} = ([0,1], T, \mu)$ est ergodique, où μ désigne la mesure de Gauß, c'est-à-dire, la mesure absolument continue de densité

$$\frac{1}{\log 2(1+x)}\,.$$

D'après le théorème ergodique de Birkhoff, pour toute fonction mesurable f sur $[0,1]$, on a :

$$\lim_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} f(T^k(x)) = \int f d\mu\,,$$

pour presque tout nombre réel x dans $[0,1]$.

Conséquence. Un nombre réel « choisi au hasard » a environ 41% de ses quotients partiels égaux à 1, environ 17% égaux à 2...

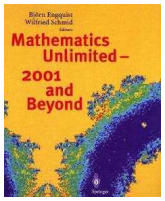
Ces nombres qui existent

—

Que j'aime à faire apprendre un nombre utile aux sages !
Immortel Archimède, artiste, ingénieur,
Qui de ton jugement peut priser la valeur ?
Pour moi ton problème eut de pareils avantages.

Périodes

Une période est un nombre complexe dont les parties réelles et imaginaires sont les valeurs d'intégrales absolument convergentes de fractions rationnelles à coefficients rationnels sur des domaines de $\mathbb{R}^n$ définis par des (in)égalités polynomiales à coefficients rationnels.



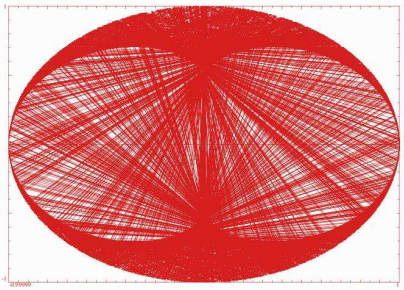
M. Kontsevich and D. Zagier, *Mathematics unlimited—2001 and beyond*, Springer-Verlag, 2001.

Exemples.

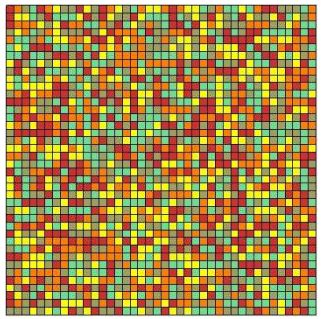
$$\sqrt{2} = \int_{0 \leq 2x^2 \leq 1} dx, \quad \pi = \int_{x^2+y^2 \leq 1} dxdy, \quad \log 3 = \int_1^3 \frac{1}{x} dx,$$

$$\zeta(s) = \int_{1>x_1>x_2>\ldots>x_s>0} \frac{dx_1}{x_1} \cdots \frac{dx_{s-1}}{x_{s-1}} \cdots \frac{dx_s}{1-x_s}.$$

La machine à conjectures



Principe d'indépendance. Par défaut, le développement d'une période dans une base entière devrait se comporter plus ou moins comme celui d'un nombre choisi au hasard.



Ce principe permet de formuler un grand nombre de conjectures difficiles. En voici deux exemples concernant les périodes les plus élémentaires, à savoir : les nombres algébriques.

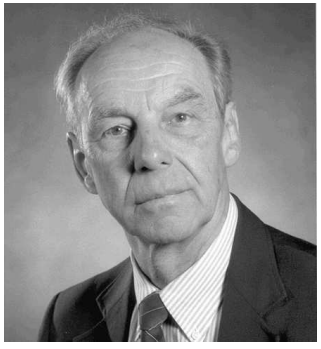
- Développements dans une base entière.

  Conjecture. Tout nombre algébrique irrationnel est normal.

- Développement en fraction continue.

  Conjecture. Tout nombre algébrique de degré au moins 3 a une suite de quotients partiels non bornée.

Comlexité algorithmique : le problème d'Hartmanis et Stearns



En 1965, Hartmanis et Stearns ont développé l'aspect quantitatif de la notion de calculabilité introduite par Turing. Ils ont introduit la notion de complexité algorithmique en temps pour les nombres réels calculables.

J. Hartmanis and R. E. Stearns, *On the computational complexity of algorithms*, Trans. Amer. Math. Soc., 1965.

Définition. Un nombre réel est dit calculable en temps $T(n)$ s'il existe une machine de Turing qui produit les n premiers chiffres de son développement binaire (ou dans une base entière) en au plus $O(T(n))$ opérations.

Problème. Existe-t-il des nombres algébriques irrationnels calculables en temps réel par une machine de Turing ?

La conjecture de Cobham

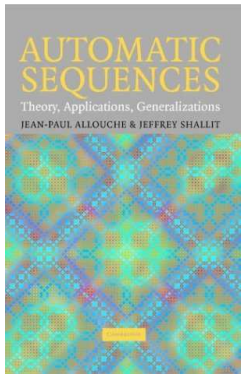
En 1968, Cobham proposa de restreindre le problème de Hartmanis et Stearns au cas d'une classe de machines de Turing simples qui calculent en temps réel : les automates finis.

Conjecture. La suite des chiffres du développement d'un nombre algébrique irrationnel dans une base entière est trop complexe pour pouvoir être engendrée par un automate fini.

A. Cobham, *On the Hartmanis-Stearns problem for a class of tag machines*, Symposium on Switching and Automata Theory, 1968.

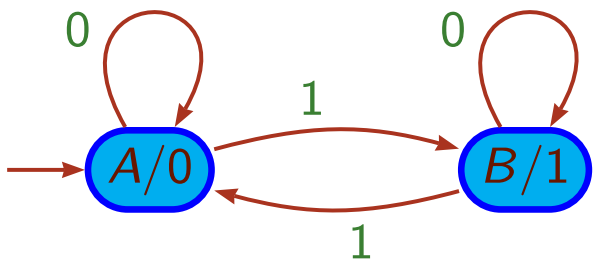
De façon équivalente, il faut donc démontrer que tout nombre irrationnel engendré par un automate fini est transcendant.

Nombres réels engendrés par automates finis



Une suite (a_n) est k-automatique, s'il existe un automate fini qui, lorsqu'on lui donne en entrée le développement de l'entier n en base k, produit en sortie le symbole a_n.

L'exemple le plus célèbre est la suite de Thue–Morse (t_n) définie par $t_n = 0$ si la somme des chiffres binaires de n est paire et $t_n = 1$ si cette somme est impaire.



On obtient :

$$t_0 t_1 t_2 t_3 \cdots = 01101001100101 \cdots .$$

Un nombre réel est engendré par un automate fini si son développement dans une base entière est automatique.

Une approche fonctionnelle

À la suite de Thue–Morse (t_n), on associe la fonction $f(z) = \sum_{n \geq 0} t_n z^n$.
Cette fonction analytique vérifie l'équation fonctionnelle

$$f(z^2) = \frac{f(z)}{1-z} - \frac{z}{(1-z^2)(1-z)}\,.$$

En suivant une approche classique due à Mahler, on peut démontrer la transcendance de $f(z)$ en tout point algébrique non nul z du disque unité complexe.

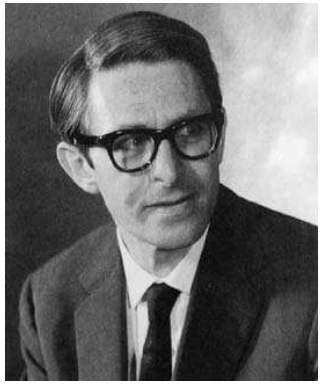
En particulier $f(1/b)$ est un nombre transcendant pour tout entier $b \geq 2$.

K. Mahler, *Arithmetische Eigenschaften der Lösungen einer Klasse von Funktionalgleichungen*, Math. Ann., 1929.

Plus généralement, il faut travailler avec des systèmes d'équations fonctionnelles associés aux nombres automatiques.

J. H. Loxton and A. J. van der Poorten, *Arithmetic properties of automata : regular sequences*, J. Reine Angew. Math., 1988.

Une approche « à la Liouville »



Théorème (Roth, 1955). Soient α un nombre algébrique et $\varepsilon > 0$. Alors, l'inégalité

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}},$$

n'a qu'un nombre fini de solutions rationnelles p/q.

K. F. Roth, *Rational approximations to algebraic numbers*, Mathematika, 1955.

Conséquence. Le nombre automatique

$$\sum_{n \geq 1} \frac{1}{10^{3^n}}$$

est transcendant.

Remarque. Dans la suite de Thue–Morse, il n'y a jamais plus de deux 0 consécutifs...

Au-delà des océans de zeros

Principe. Imaginons que le développement en base 10 du nombre réel ξ commence par

$$0.123\,735\,418\,\underbrace{923\,923\,923\,923}_{\text{motif redondant}}\,712\,\cdots$$

Alors, ξ est proche du nombre rationnel

$$\frac{p}{q} = 0.123\,735\,418\,\overline{923} = 0.123\,735\,418\,923\,923\,923\,923\,\cdots\,.$$

Plus précisément,

$$\left|\xi - \frac{p}{q}\right| < \frac{1}{q^{1+\varepsilon}}$$

avec

$$\varepsilon = \frac{9}{12} > 0 \quad \text{et} \quad q = 10^9(10^3 - 1).$$

On obtient malheureusement souvent des approximations rationnelles de piètre qualité, mais leur dénominateur a une forme très particulière, à savoir :

$$10^r(10^s - 1)\,.$$

Le théorème du sous-espace de Schmidt

Au début des années 70, W. M. Schmidt a obtenu une généralisation spectaculaire du théorème de Roth qui s'exprime en termes d'approximation simultanée de formes linéaires à coefficients algébriques.

W. M. Schmidt, Diophantine approximation, Lecture Notes in Math., Springer, 1980.

Conséquence. Soient α un nombre algébrique, b un entier et $\varepsilon > 0$. Alors, il n'existe qu'un nombre fini de nombres rationnels p/q tels que

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{1+\varepsilon}}$$

et tels que q soit de la forme $b^r(b^s - 1)$.

Yu. Bilu, *The many faces of the subspace theorem [After Adamczewski, Bugeaud, Corvaja, Zannier...]*, Séminaire Bourbaki, Astérisque, 2008.

Suites automatiques et morphismes de monoïdes libres

Morphismes. Une application d'un alphabet fini $\mathcal{A}$ dans le monoïde $\mathcal{A}^*$ définit un (unique) morphisme du monoïde libre $\mathcal{A}^*$.

L'action d'une telle application s'étend naturellement par continuité aux éléments de $\mathcal{A}^{\mathbb{N}}$.

Un morphisme est dit k-uniforme si chaque lettre a pour image un mot de longueur k. Un codage est un morphisme 1-uniforme entre deux monoïdes.

Exemple. La suite de Thue–Morse est l'unique point fixe, commençant par 0, du morphisme 2-uniforme τ défini sur $\{0,1\}^*$ par $\tau(0) = 01$ et $\tau(1) = 10$.

On obtient :

$\tau(0) = 01$ et donc $\tau^2(0) = \tau(01) = \tau(0)\tau(1) = 0110$, puis $\tau^3(0) = 01101001, \ldots$

Théorème (Cobham). Une suite est k-automatique si, et seulement si, elle est l'image par un codage d'un point fixe d'un morphisme k-uniforme.

Retour sur le nombre de Thue–Morse

Considérons le nombre de Thue–Morse défini par :

$$\xi = \sum_{n \geq 0} \frac{t_n}{10^{n+1}} = 0.011\,010\,011 \cdots .$$

Observation. Le développement décimal de ξ commence par le bloc de chiffres 011 qui comporte le motif redondant 11.

Itération. On en déduit que pour tout entier n le développement décimal de ξ commence par le bloc de chiffres $\tau^n(011) = \tau^n(0)\tau^n(1)\tau^n(1)$.

Approximations rationnelles. Posons

$$p_n/q_n = 0.\tau^n(0)\,\overline{\tau^n(1)} = 0.\tau^n(0)\,\tau^n(1)\;\tau^n(1)\;\tau^n(1)\cdots$$

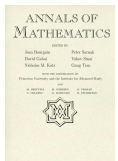
Un rapide calcul montre que l'on peut choisir $q_n = 10^{2^n}(10^{2^n} - 1)$.

Les $3 \cdot 2^n$ premiers chiffres de p_n/q_n et ξ sont donc égaux. Il suit :

$$\left|\xi - \frac{p_n}{q_n}\right| < \frac{1}{10^{3\cdot 2^n}} \quad \text{et ainsi} \quad \left|\xi - \frac{p_n}{q_n}\right| < \frac{1}{q_n^{1+1/2}} . \qquad \square$$

Confirmation de la conjecture de Cobham

Théorème. Le développement dans une base entière d'un nombre algébrique irrationnel ne peut pas être engendré par un automate fini.



B. Adamczewski and Y. Bugeaud, *On the comlexity of algebraic numbers I. Expansions in integer bases*, Annals of Math., 2007.

Cette approche peut être utilisée pour étudier le développement des nombres algébriques dans d'autres systèmes de numération comme par exemple le développement en fraction continue.

B. Adamczewski and Y. Bugeaud, *On the comlexity of algebraic numbers II. Continued fractions*, Acta Math., 2005.

B. Adamczewski and Y. Bugeaud, *On the Maillet–Baker continued fractions*, J. Reine Angew. Math., 2007.