Colloquium Université de Rennes

Peut-on distinguer les nombres algébriques des nombres transcendants par leur développement ?

Michel Waldschmidt

http ://www.math.jussieu.fr/∼miw/

Lundi 8 janvier 2007

Résumé

Le titre de l'exposé comporte une ambiguïté : le développement pourrait être par exemple dans une base donnée (décimale, binaire). Il pourrait aussi s'agir du développement en fraction continue. Dans un cas comme dans l'autre on ne sait pas répondre à la question, mais on a de bonnes (?) raisons de penser que la réponse est négative : ainsi Émile Borel a conjecturé (d'abord en 1909, puis en 1950) que si on fixe deux entiers $g \geq 2$ et $n \geq 1$, la fréquence d'apparition d'une suite donnée de n chiffres dans le développement en base g d'un nombre réel algébrique irrationnel ne dépend que de g et n. On s'attend à ce que le développement binaire ou décimal d'un nombre réel algébrique irrationnel se comporte en quelque sorte comme celui de presque tous les nombres réels.

Résumé (suite)

Bien que nos connaissances dans ce domaine soient extrêmement limitées, quelques progrès ont été faits récemment, notamment grâce au théorème du sous-espace de W.M. Schmidt. Le but principal de l'exposé est de présenter ces résultats récents.

Décimales de $\sqrt{2}$

http://wims.unice.fr/wims/wims.cgi

1.4142135623730950488016887242096980785696718753769480731766797379907324784621070388503875343276415727350138462309122970249248360558507372126441214970999358314132226659275055927557999505011527820605714701095599716059702745345968620147285174186408891986095523292304843087143214508397626036279952514079896872533965463318088296406206152583523950547457502877599617298355752203375318570113543746034084988471603868999706990048150305440277903164542478230684929369186215805784631115966687130130156185689872372352885092648612494977154218334204285686060146824720771435854874155657069677653720226485447015858801620758474922657226002085584466521458398893944370926591800311388246468157082630100594858704003186480342194897278290641045072636881313739855256117322040245091227700226941127573627280495738108967504018369868368450725799364729060762996941380475654823728997180326802474420629269124859052181004459842150591120249441341728531478105803603371077309182869314710171111683916581726889419758716582152128229518488472 …

Chiffres binaires de $\sqrt{2}$ http://wims.unice.fr/wims/wims.cgi

1.0110101000001001111001100110011111110011101111100110010010000
10001011001011111011000100110110011011101010100101010111110100
11111000111010110111101100000101110101000100100111011101010000
100110011101101000101111010110010000010110000011001100111001100
1000101010100101011111110010000011000000100001110101011100010100
0101100001110101000101100011111111001101111111011100100000011110
11011001110010000111101110100101010000101111001000011100111000
111101101001010011110000000001001000011100110110001111011111101
000100111011010001101001000100000000101110100001110100001010101
111000111110100111001010011000001011001110001100000000010001101
11100001100110111101111001010101100011011110010010001000101101
000100000100010110001010010001100000101010111100011100100010111
10111110001001110001100111100011011010101101010001010001110001
01110110111111010011101110011001011001010100110001101000011001
100011111001111100100001001101111101010010111100010010000011111
000001101101110010110000010111011101010101001001010000001000100
110010000001000000011001010010010101000000010011100101001010 . . .

Le fabuleux destin de $\sqrt{2}$

- Benoît Rittaud, Éditions *Le Pommier* (2006).

http://www.math.univ-paris13.fr/~rittaud/RacineDeDeux

- Calcul des décimales de $\sqrt{2}$:

1 542 calculées à la main par Horace Uhler en 1951
14 000 décimales calculées en 1967
1 000 000 décimales calculées en 1971
137 millions de décimales calculées par Yasumasa Kanada et Daisuke Takahashi en 1997 avec Hitachi SR2201 en 7 heures et 31 minutes.

- Motivation : calcul des décimales de π.

Émile Borel (1871–1956)

Émile Borel

- *Les probabilités dénombrables et leurs applications arithmétiques,*
  Palermo Rend. **27**, 247-271 (1909).
  Jahrbuch Database JFM 40.0283.01
  `http ://www.emis.de/MATH/JFM/JFM.html`
- *Sur les chiffres décimaux de* $\sqrt{2}$ *et divers problèmes de probabilités en chaînes,*
  C. R. Acad. Sci., Paris **230**, 591-593 (1950).
  Zbl 0035.08302

Développement en base g d'un nombre réel

- Soit g un entier ≥ 2. Tout nombre réel x possède un développement *unique s'il est irrationnel*

  $$x = a_{-k}g^k + \cdots + a_{-1}g + a_0 + a_1g^{-1} + a_2g^{-2} + \cdots$$

  où k est un entier ≥ 0 et où les a_i pour $i \geq -k$ (chiffres de x dans le développement en base g de x) appartiennent à l'ensemble $\{0, 1, \ldots, g-1\}$.
- On le note

  $$x = a_{-k} \cdots a_{-1}a_0, a_1a_2 \cdots$$

- Exemples : en base 10 (*développement décimal*) :

  $$\sqrt{2} = 1,41421356237309504880168872420 \ \ldots$$

  et en base 2 (*développement binaire*) :

  $$\sqrt{2} = 1,0110101000001001111001100110011111110 \ \ldots$$

Développement en base g d'un nombre algébrique

Soient $g \geq 2$ un entier et x un nombre réel algébrique irrationnel.

• É. Borel : *Le développement en base g de x devrait satisfaire certaines des lois que vérifient presque tous les nombres (pour la mesure de Lebesgue).*

• **Remarque** : aucun nombre ne peut satisfaire **toutes** les lois vérifiées en dehors d'un ensemble de mesure nulle car l'intersection de ces ensembles de mesure pleine est vide !

$$\bigcap_{x \in \mathbf{R}} \mathbf{R} \setminus \{x\} = \emptyset.$$

• Énoncés précis par B. Adamczewski.

Suggestion d'Émile Borel

• Dans le développement en base g d'un nombre réel algébrique irrationnel, *chacun des chiffres* $0, 1, \ldots, g-1$ *devrait apparaître au moins une fois.*
• Comme conséquence, on en déduirait que *chaque suite donnée de chiffres devrait apparaître une infinité de fois dans le développement de tout nombre algébrique irrationnel.*
• `Indication` : remplacer g par une puissance.
• Ainsi chacune des quatre suites $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$ devrait apparaître une infinité de fois dans le développement binaire de tout nombre réel algébrique irrationnel (prendre $g = 4$.)

Nombres simplement normaux dans une base

Soit g un entier ≥ 2.
• Un nombre réel x est dit *simplement normal en base* g si, dans son développement en base g, chacun des chiffres $\{0, 1, \dots, g-1\}$ apparaît avec la fréquence $1/g$.
• Par exemple le nombre décimal

$$0,123456789012345678901234567890\dots$$

est simplement normal en base 10. Il est rationnel :

$$= \frac{1\,234\,567\,890}{9\,999\,999\,999} = \frac{137\,174\,210}{1\,111\,111\,111}.$$

Nombres normaux dans une base

Soit g un entier ≥ 2.

- Un nombre réel x est appelé *normal en base* g si son développement en base g vérifie la propriété suivante :
  - pour chaque entier m, chaque suite de m chiffres apparaît avec la même fréquence $1/g^m$.
- Par conséquent un nombre réel est normal en base g si et seulement s'il est simplement normal en base g^n pour tout $n \geq 2$.

Nombres normaux

Un nombre réel est dit (absolument) normal s'il est normal en toute base $g \geq 2$, ce qui revient à dire qu'il est simplement normal en toute base $g \geq 2$.

• Borel a suggéré que tout nombre réel algébrique irrationnel est normal.

• On ne connaît aucun exemple explicite de triplet (g, a, x), où $g \geq 3$ est un entier, a un chiffre de l'ensemble $\{0, \ldots, g-1\}$ et x un nombre algébrique irrationnel, pour lequel on puisse affirmer que le chiffre a apparaît une infinité de fois dans le développement en base g de x.

Un résultat positif

• K. Mahler (1973) : *Pour tout $g \geq 2$ et tout $n \geq 1$, il existe des nombres réels algébriques irrationnels x tels que toute suite de n chiffres apparaisse une infinité de fois dans le développement en base g de x.*

Pour tout nombre réel irrationnel α et toute suite de k chiffres de l'ensemble $\{1, \ldots, g-1\}$, il existe un entier m tel que le développement en base g de $m\alpha$ contienne une infinité de fois la suite donnée. Selon Mahler, le plus petit m est borné par g^{2k+1}. Cette borne a été améliorée par D. Berend et M. D. Boshernitzan (2005) en $2g^{k+1}$ et on ne peut pas faire mieux que $g^k - 1$.

Nombres normaux : exemples

• Presque tous les nombres (pour la mesure de Lebesgue) sont normaux (Borel, 1909).
• Des exemples de nombres normaux ont été donnés de façons calculables (W. Sierpinski 1917, H. Lebesgue 1917, V. Becher et S. Figueira 2002) mais les algorithmes pour donner leur valeur sont très compliqués (ils sont qualifiés de "ridiculously exponential" par S. Figueira).

Le nombre de Champernowne

• Le nombre décimal

$$0.\,1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11\,12\,13\,14\,15\,16\,17\,18\,19\ldots$$

est normal en base 10, et le nombre binaire

$$0,\ 1\,10\,11\,100\,101\,110\,111\,1000\,1001\,1010\,1011\,1100\,1101\quad\ldots$$

est normal en base 2.

• Le nombre binaire de Champernowne (1933) s'écrit

$$\sum_{k\geq 1} k2^{-c_k} \qquad \text{avec} \qquad c_k = k + \sum_{j=1}^{k}[\log_2 j].$$

• S. S. Pillai (1940), Œuvres éditées par
R. Balasubramanian et R. Thangadurai, (2007).

Nombre normaux : autres exemples

- Nombres de Stoneham : Si a et g sont deux entiers > 1 premiers entre eux, alors le nombre

$$\sum_{n\geq 0} a^{-n} g^{-a^n}$$

est normal en base g.
Référence : R. Stoneham (1973), D.H. Bailey, J.M. Borwein, R.E. Crandall et C. Pomerance (2004).

- A.H. Copeland et P. Erdős (1946) : le nombre

$$0.2\,3\,5\,7\,11\,13\,17\,19\,23\,29\,31\,37\,41\,43\,47\,53\,59\,61\,67\ \ldots$$

obtenu en concaténant la suite des nombres premiers est normal en base 10.

Nombres BBP

• D.H. Bailey, P.B. Borwein, S. Plouffe (Math. Comp. 1997) : nombres BBP

$$\sum_{n\geq 1} \frac{p(n)}{q(n)} \cdot g^{-n}$$

où $g \geq 2$ est un entier, p et q des polynômes premiers entre eux dans $\mathbf{Z}[X]$ avec $q(n) \neq 0$ pour $n \geq 1$.

• $\log 2$ est un nombre BBP en base 2 car

$$\sum_{n\geq 1} \frac{1}{n} \cdot x^n = -\log(1-x) \quad \text{et} \quad \sum_{n\geq 1} \frac{1}{n} \cdot 2^{-n} = \log 2.$$

• $\log 2$ est un nombre BBP en base 9 car

$$\sum_{n\geq 1} \frac{1}{2n-1} \cdot x^{2n-1} = \log \frac{1+x}{1-x}, \quad \sum_{n\geq 1} \frac{6}{2n-1} \cdot 3^{-2n} = \log 2.$$

Nombres BBP : exemples

• D.H. Bailey, P.B. Borwein, S. Plouffe (1997) : π est un nombre BBP en base 16

$$\pi = \sum_{n\geq 0} \frac{1}{2^{4n}} \left(\frac{4}{8n+1} - \frac{2}{8n+4} - \frac{1}{8n+5} - \frac{1}{8n+6} \right) \cdot$$

• D.H. Bailey (2004) : $\log 3$ est un nombre BBP en base 4 :

$$\log 3 = 2\log 2 + \log(3/4) = \sum_{n\geq 0} \frac{1}{2^{2n}} \cdot \frac{1}{2n+1} \cdot$$

• π^2 et $(\log 2)^2$ sont des nombres BBP en base $2^6 = 64$, $\zeta(3)$ en base $2^{12} = 4096$, (D.H. Bailey et R.E. Crandall, 2001)
$\log 3$ et π^2 en base $3^6 = 729$ (D.J. Broadhurst 1998).

Systèmes dynamiques

• D.H. Bailey et R.E. Crandall "On the Random Character of Fundamental Constant Expansions" et "Random Generators and Normal Numbers", Experimental Math. 2001 et 2003 :
comportement des orbites du système dynamique discret $T_g(x) = gx \pmod 1$.
• Normalité en base 2 de constantes comme $\log 2$, π, $\zeta(3)$.
• J-C. Lagarias (Experimental Math. 2001) : lien avec des valeurs spéciales de G–fonctions au sens de Siegel.

Hypothèse A de Bailey et Crandall

Hypothèse A de D.H. Bailey et R.E. Crandall : *Soit*

$$\theta := \sum_{n\geq 1} \frac{p(n)}{q(n)} \cdot g^{-n}$$

où $g \geq 2$ *est un entier positif,* $R = p/q \in \mathbf{Q}(X)$ *une fraction rationnelle avec* $q(n) \neq 0$ *pour* $n \geq 1$ *et* $\deg p < \deg q$*. On pose* $y_0 = 0$ *et*

$$y_{n+1} = gy_n + \frac{p(n)}{q(n)} \pmod 1$$

On considère la suite $(y_n)_{n\geq 1}$*. Soit elle n'a qu'un nombre fini de points limites, soit elle est uniformément distribuée modulo* 1*.*

Nombre de 1 dans le développement binaire d'un nombre irrationnel

Référence : T. Rivoal (2006).

Désignons par $B(x, n)$ le nombre de 1 parmi les n premiers chiffres dans le développement binaire d'un nombre réel irrationnel x.

- Si x, y et $x + y$ sont irrationnels, alors

$$B(x + y, n) \leq B(x, n) + B(y, n) + 1.$$

- Si x, y et xy sont irrationnels, alors

$$B(xy, n) \leq B(x, n)B(y, n) + \log_2[x + y + 1].$$

- Si x est irrationnel, pour tout entier $A > 0$ on a

$$B(x, n)B(A/x, n) \geq n - 1 - \log_2[x + A/x + 1].$$

Nombre de 1 dans le développement binaire d'un nombre algébrique

• T. Rivoal :

$$B(\sqrt{2}, n) \geq n^{1/2} + O(1).$$

• D.H. Bailey, J.M. Borwein, R.E. Crandall et C. Pomerance.
On the Binary Expansions of Algebraic Numbers,
Journal de Théorie des Nombres de Bordeaux, vol. **16** (2004), pp. 487-518. MR214495

Si x est un nombre algébrique de degré $d \geq 2$, alors le nombre de 1 parmi les N premiers chiffres dans le développement binaire de x est au moins $CN^{1/d}$, où C est un nombre positif qui ne dépend que de x.

Application à la transcendance

Pour tout entier $d \geq 2$, le nombre

$$\sum_{n \geq 0} 2^{-d^n}$$

est transcendant.
A. J. Kempner (1916) : transcendance de

$$\sum_{n \geq 0} 2^{-2^n}$$

Séries de Fredholm (déjà considérées par Liouville)

$$\sum_{n \geq 0} z^{n^2}$$

Nature arithmétique du nombre $\sum_{n\geq 0} g^{-u_n}$

Soit g un entier ≥ 2 et soit $(u_n)_{n\geq 0}$ une suite croissante d'entiers positifs. On considère le nombre

$$\theta = \sum_{n\geq 0} g^{-u_n}.$$

Si la suite $(u_n)_{n\geq 0}$ tend suffisamment vite vers l'infini, alors le nombre θ est irrationnel, voire même transcendant.
Par exemple si la suite vérifie

$$u_{n+1} - u_n \to +\infty \quad \text{quand} \quad n \to +\infty$$

alors θ est irrationnel. Comme cas particulier, pour $u_n = n^2$ on en déduit l'irrationalité du nombre (Liouville–Fredholm)

$$\sum_{n\geq 0} g^{-n^2}.$$

Irrationalité de $\theta = \sum_{n\geq 0} g^{-u_n}$ quand $n \longrightarrow +\infty$

Supposons $u_{n+1} - u_n \to +\infty$ quand $n \to +\infty$. Montrons que θ est irrationnel.

Démonstration. On tronque la série :

$$\theta = \sum_{n=0}^{N} g^{-u_n} + \sum_{n\geq N+1} g^{-u_n}.$$

On pose $q = g^{u_N}$ et $p = \sum_{n=0}^{N} g^{u_N - u_n}$. Alors pour N suffisamment grand

$$0 < q\theta - p = \sum_{n\geq N+1} \frac{1}{g^{u_n - u_N}} < \frac{2}{g^{u_{N+1} - u_N}}.$$

Critère d'irrationalité

Soit x un nombre réel. Si x est rationnel, disons $x = a/b$, alors pour tout $p/q \in \mathbf{Q}$ distinct de x on a

$$|qx - p| \geq 1/b.$$

Contraposée : Si x est un nombre réel et s'il existe une suite de nombres rationnels $p_n/q_n \neq x$ tels que

$$|q_n x - p_n| \to 0,$$

alors x est irrationnel.
Inversement cette condition fournit un critère d'irrationalité : *si x est un nombre réel irrationnel, il existe une infinité de $p/q \in \mathbf{Q}$ satisfaisant*

$$0 < \left| x - \frac{p}{q} \right| < \frac{1}{\sqrt{5}q^2}.$$

Approximation Diophantienne

• Liouville (1844) : si α est un nombre algébrique de degré d, alors pour tout nombre rationnel $p/q \neq \alpha$

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^d}.$$

• Thue (1909) : remplace $c(\alpha)/q^d$ par $c(\alpha, \epsilon)/q^\kappa$ où $\kappa = (d/2) + 1 + \epsilon$.
• Siegel (1921) : $\kappa = 2\sqrt{d} + \epsilon$.
• Gel'fond et Dyson (1947) : $\kappa = \sqrt{2d} + \epsilon$.
• Roth (1954) : $\kappa = 2 + \epsilon$.
• Schmidt (1970) : Théorème du sous-espace.
• **Reference :** Yuri Bilu, Séminaire Bourbaki, Novembre 2006 : *The many faces of the Subspace Theorem* [after Adamczewski, Bugeaud, Corvaja, Zannier...]
http://www.math.u-bordeaux.fr/~yuri/publ/subspace.pdf

Transcendance de $\sum_{n\geq 0} g^{-u_n}$: Liouville

Le théorème de Liouville donne la transcendance de

$$\sum_{n\geq 0} g^{-u_n}$$

à condition que la suite croissante $(u_n)_{n\geq 0}$ satisfasse

$$\limsup_{n\to\infty} \frac{u_{n+1}}{u_n} = +\infty.$$

Par exemple la suite $u_n = n!$ satisfait cette condition, donc le nombre $\sum_{n\geq 0} g^{-n!}$ est transcendant.

Transcendance de $\sum_{n\geq 0} g^{-u_n}$: Roth

Le théorème de Thue-Siegel-Roth donne la transcendance de

$$\sum_{n\geq 0} g^{-u_n}$$

sous l'hypothèse moins restrictive

$$\limsup_{n\to\infty} \frac{u_{n+1}}{u_n} > 2.$$

Par exemple la suite $u_n = [g^{\lambda n}]$ vérifie cette condition dès que $\lambda > 2$. Ainsi la transcendance du nombre

$$\sum_{n\geq 0} g^{-3^n}$$

se déduit du théorème de Roth.

Transcendance de $\theta = \sum_{n\geq 0} g^{-u_n}$: Ridout

On peut encore améliorer le résultat en utilisant le fait que les dénominateurs g^{u_n} sont des puissances de g.

• D. Ridout, (1957). Pour tout nombre algébrique réel α, pour tout $\epsilon > 0$, l'ensemble des $p/q \in \mathbf{Q}$ avec $q = g^k$ et $|\alpha - p/q| < q^{-1-\epsilon}$ est fini.

Donc la condition

$$\limsup_{n\to\infty} \frac{u_{n+1}}{u_n} > 1$$

suffit pour obtenir la transcendance de θ.

Exemple : $\sum_{n\geq 0} g^{-2^n}$ est un nombre transcendant.

Le nombre de Liouville-Fredholm

D.H. Bailey, J.M. Borwein, R.E. Crandall et C. Pomerance (2004) : le nombre

$$\theta = \sum_{n\geq 0} 2^{-n^2}$$

n'est pas quadratique.
Conséquences du théorème de Nesterenko (1996) sur la transcendance des valeurs de fonctions thêta en des points rationnels. ce nombre θ est transcendant (D. Bertrand 1997 ; D. Duverney, K. Nishioka, K. Nishioka et I. Shiokawa 1998).

Mots infinis

Soit A un un alphabet fini avec g éléments,

- Nous allons considérer des *mots infinis*
  $w = a_1 \ \ldots \ a_n \ \ldots$
  Un *facteur de longueur* m d'un tel w est un mot de la forme $a_k a_{k+1} \ \ldots \ a_{k+m-1}$ pour un $k \geq 1$.
- La *complexité* d'un mot infini w est la fonction $p(m)$ qui compte, pour chaque $m \geq 1$, le nombre de facteurs distincts de w de longueur m.
- Ainsi on a $1 \leq p(m) \leq g^m$ et la fonction $m \mapsto p(m)$ est monotone croissante (au sens large).
- Selon la suggestion de Borel, la complexité de la suite des chiffres en base g d'un nombre réel irrationnel algébrique devrait être $p(m) = g^m$.

Mots sturmiens

Supposons $g = 2$, disons $A = \{a, b\}$.

- Un mot est périodique si et seulement si sa complexité est bornée.
- Si la complexité $p(m)$ d'un mot w vérifie $p(m) = p(m + 1)$ pour une valeur de m, alors $p(m + k) = p(m)$ pour tout $k \geq 0$, donc le mot est périodique. Par conséquent *un mot non périodique w a une complexité minorée par $p(m) \geq m + 1$*.
- Un mot infini de complexité minimale $p(m) = m + 1$ est appelé *sturmien* (Morse et Hedlund, 1938).
- Les mots sturmiens sont ceux donnés par des suites qui codent par 0 et 1 les trajectoires d'une boule de billard carré pour un angle d'attaque irrationnel.

Exemple : le mot de Fibonacci

Prenons $A = \{a, b\}$.

- On commence avec $f_1 = b$, $f_2 = a$ et on pose (concaténation) : $f_n = f_{n-1}f_{n-2}$.
- Ainsi $f_3 = ab$ $f_4 = aba$ $f_5 = abaab$
  $f_6 = abaababa$ $f_7 = abaababaabaab$
  $f_8 = abaababaabaababaababa$
- Le *mot de Fibonacci*

  $$w = abaababaabaababaababaabaababaabaab\ \ldots$$

  est le point fixe du morphisme $a \mapsto ab$, $b \mapsto a$;
  l'image par ce morphisme de f_n est f_{n+1}.

Le mot de Fibonacci est sturmien

- Le mot de Fibonacci

  $$w = abaababaabaababaababaabaababaabaab\ \ldots$$

  est sturmien.
- Sur l'alphabet $\{a,\ b\}$, un mot w est sturmien si et seulement si, *pour chaque* $m \geq 1$, *il y a exactement un facteur* v *de* w *de longueur* m *tel que* va *et* vb *soient facteurs de* w *de longueur* $m+1$.

Le mot de Fibonacci $abaababaabaababaababaabaababaabaab\ \ldots$ est sturmien

$$
\begin{tikzcd}
 & & & & aabaa \\
a \arrow[r] \arrow[dr] & aa \arrow[r] & aab \arrow[r] & aaba \arrow[r] \arrow[ur] & aabab \\
 & ab \arrow[r] & aba \arrow[r] \arrow[dr] & abaa \arrow[r] & abaab \\
 & & & abab \arrow[r] & ababa \\
b \arrow[r] & ba \arrow[r] \arrow[dr] & baa \arrow[r] & baab \arrow[r] & baaba \\
 & & bab \arrow[r] & baba \arrow[r] & babaa
\end{tikzcd}
$$

Transcendance et mots sturmiens

- S. Ferenczi, C. Mauduit, 1997 : un nombre dont la suite des chiffres est sturmienne est transcendant. Critère combinatoire : *la complexité du développement en base g d'un nombre algébrique irrationnel vérifie*

$$\liminf_{m\to\infty}(p(m)-m)=+\infty.$$

- *Propriétés combinatoires des suites sturmiennes* : contiennent des suites qui se ressemblent. Donne des approximations rationnelles trop bonnes pour des nombres algébriques.
- *Outil :* la version p–adique du théorème de Thue–Siegel–Roth due à Ridout (1957).

Résultats de transcendance sur les développements en base g

- J-P. Allouche et L.Q. Zamboni(1998).
- R.N. Risley et L.Q. Zamboni(2000).
- B. Adamczewski et J. Cassaigne (2003).

Méthode de Mahler

• K. Mahler (1930, 1969) : soit $d \geq 2$; la fonction $f(z) = \sum_{n \geq 0} z^{d^n}$ vérifie $f(z^d) + z = f(z)$ pour $|z| < 1$.

• Conséquence : transcendance du nombre de Kempner–Mahler

$$\xi = \sum_{n \geq 0} g^{-d^n}$$

pour $g \geq 2$.

• *Remarque sur les nombres de Kempner–Mahler* (T. Rivoal) : aucune des puissances du nombre ξ n'est simplement normale en base g.

La suite de Prouhet-Thue-Morse

- Pour $n \geq 0$ on pose $a_n = 0$ si la somme des chiffres binaires de n est paire, $a_n = 1$ si elle est impaire. La *suite de Prouhet-Thue-Morse* $(a_n)_{n\geq 0}$ ainsi définie commence par

$$0\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ \ldots$$

- Dans cette suite il n'y a pas trois blocs consécutifs identiques de la forme :

$$(0\ 0\ 0) \quad (1\ 1\ 1) \quad (01\ 01\ 01) \quad (10\ 10\ 10) \quad (001\ 001\ 001)\ \ldots$$

- E. Prouhet 1851, A. Thue 1906, M. Morse 1921

$$u_0 = 0, \quad v_0 = 1, \quad u_{n+1} = u_n v_n, \quad v_{n+1} = v_n u_n \qquad (n \geq 0).$$

Le mot de Prouhet-Thue-Morse $abbabaabbaababbab\dots$

Dans la suite de Prouhet-Thue-Morse
$01101001100101101\ \dots$ on remplace 0 par a et 1 par b.
Le *mot de Prouhet-Thue-Morse*

$$w = abbabaabbaababbab\ \dots$$

est le point fixe du morphisme $a \mapsto ab$, $b \mapsto ba$.

Transcendance du nombre de Prouhet-Thue-Morse

Soit $(a_n)_{n\geq 0}$ la suite de Prouhet-Thue-Morse et soit $g \geq 2$.

- K. Mahler (1929) *: le nombre*

$$\sum_{n\geq 0} a_n g^{-n}$$

est transcendant.

Transcendance du nombre de Prouhet-Thue-Morse

Schéma de démonstration : pour $|z| < 1$ la fonction

$$f(z) = \prod_{n \geq 0} (1 - z^{2^n}) \quad \text{vérifie} \quad f(z) = \sum_{n \geq 0} (-1)^{a_n} z^n$$

où $(a_n)_{n \geq 0}$ la suite de Prouhet-Thue-Morse . Pour $a \in \{0, 1\}$, on a $(-1)^a = 1 - 2a$. On en déduit

$$f(z) = \sum_{n \geq 0} (1 - 2a_n) z^n = \frac{1}{1 - z} - 2 \sum_{n \geq 0} a_n z^n.$$

Utilisant l'équation fonctionnelle $f(z) = (1 - z) f(z^2)$, Mahler montre que $f(\alpha)$ est transcendant pour α algébrique avec $0 < |\alpha| < 1$. $\square$

Méthode de Mahler et nombres automatiques

• Annonce de J.H. Loxton et A.J. van der Poorten (1982–1988) : la méthode de Mahler permet de démontrer que *tout nombre* **automatique** *irrationnel est transcendant*. Reste un problème ouvert.
• P.G. Becker (1994) : *pour toute suite automatique qui n'est pas ultimement périodique* $\mathbf{u} = (u_1, u_2, \ldots)$, *le nombre réel*

$$\sum_{k \geq 1} u_k g^{-k}$$

est transcendant, à condition que l'entier g *soit suffisamment grand (en fonction de* $\mathbf{u}$*).*

Automates

Un *automate fini* est constitué de
• l'*alphabet initial* $\mathcal{A}$, habituellement formé des chiffres $\{1, 2, \ldots, g-1\}$;
• l'ensemble fini $\mathcal{Q}$ des états, avec au moins 2 éléments, dont l'un privilégié, *l'état initial* i ;
• L'*application de transition* $\mathcal{Q} \times \mathcal{A} \to \mathcal{Q}$, qui, à chaque état, en associe un autre, dépendant de l'entrée courante ;
• l'*alphabet* de sortie $\mathcal{B}$, avec l'*application de sortie* $f : \mathcal{Q} \to \mathcal{B}$.

Suites automatiques

- Soit $g \geq 2$ un entier. Une suite infinie $(a_n)_{n\geq 0}$ est dite g– automatique s'il existe un automate fini qui produise a_n comme sortie quand l'entrée est le développement en base g de n.
- A. Cobham, 1972 : *La complexité d'une suite automatique est* $p(m) = O(m)$*.*
- Les suites automatiques sont intermédiaires entre la périodicité et le chaos. Elles apparaissent en liaison avec l'analyse harmonique, la théorie ergodique, les objets fractals, les cascades de Feigenbaum, les quasi–cristaux.

Suites automatiques et physique théorique

- J.P. Allouche et M. Mendes-France : calcul des constantes physiques d'une chaîne d'Ising unidimensionnelle ayant des impuretés réparties de façon automatique.
  Référence : J-P. Allouche et M. Mignotte, *Arithmétique et Automates*, Images des Mathématiques 1988, Courrier du CNRS Supplément au N° 69, 5–9.
- Modèle d'Ising : modèle de mécanique statistique pour étudier les transitions de phase.
  Référence : Raphaël Cerf, *Le modèle d'Ising et la coexistence des phases*, Images des Mathématiques (2004), 47–51.
  `http ://www.spm.cnrs-dir.fr/actions/publications/IdM.htm`

Automates : référence

Jean-Paul Allouche et Jeffrey Shallit
Automatic Sequences : Theory,
Applications, Generalizations,
Cambridge University Press (2003).

http ://www.cs.uwaterloo.ca/∼shallit/asas.html

Exemple : puissances de 2

Le nombre binaire

$$\sum_{n\geq 0} 2^{-2^n} = 0,1101000100000001000\cdots = 0,a_1a_2a_3\ \ldots$$

avec

$$a_n = \begin{cases} 1 & \text{if } n \text{ est une puissance de } 2, \\ 0 & \text{sinon} \end{cases}$$

est produit par l'automate

$$\begin{tikzcd} \boxed{i} \arrow[loop above, "0"] \arrow[r, "1"] & \boxed{a} \arrow[loop above, "0"] \arrow[r, "1"] & \boxed{b} \arrow[loop above, "0"] \arrow[loop below, "1"] \end{tikzcd}$$

avec $f(i) = 0$, $f(a) = 1$, $f(b) = 0$.

Puissances de 2 *(suite)*

En remplaçant 0 par a et 1 par b dans le développement du nombre binaire automatique

$$\sum_{n\geq 0} 2^{-2^n} = 0,1101000100000001000\cdots$$

on obtient le mot infini

$$\mathbf{v} = v_1 v_2 \cdots v_n \cdots = bbabaaabaaaaaaabaaa\cdots$$

où

$$v_n = \begin{cases} b & \text{si } n \text{ est une puissance de } 2, \\ a & \text{sinon.} \end{cases}$$

La complexité $p(m)$ de $\mathbf{v}$ est bornée par $2m$:

$$\begin{array}{rcccccccc} m = & 1 & 2 & 3 & 4 & 5 & 6 & \cdots \\ p(m) = & 2 & 4 & 6 & 7 & 9 & 11 & \cdots \end{array}$$

La suite de Prouhet-Thue-Morse

- L'automate

$$\begin{tikzcd} \boxed{i} \arrow[loop above, "0"] \arrow[rr, bend left, "1"] & & \boxed{a} \arrow[loop above, "0"] \arrow[ll, bend left, "1"] \end{tikzcd} \qquad \text{avec } f(i) = 0,\ f(a) = 1$$

produit la suite $a_0 a_1 a_2 \ldots$ où, par exemple, a_9 est $f(i) = 0$, car $1001[i] = 100[a] = 10[a] = 1[a] = i$. C'est la suite de Prouhet-Thue-Morse, dans laquelle le $n + 1$-ème terme a_n est 1 si le nombre de 1 dans le développement binaire de n est impair, 0 s'il est pair.
Le nombre de Prouhet-Thue-Morse est $\sum_{n \geq 0} a_n 2^{-n}$.

La suite de Baum-Sweet

- Pour $n \geq 0$ on pose $a_n = 1$ si le développement binaire de n ne contient pas de suite de longueur impaire de 0, $a_n = 0$ sinon : la suite de Baum-Sweet $(a_n)_{n\geq 0}$ commence par

$$1\;1\;0\;1\;1\;0\;0\;1\;0\;1\;0\;0\;1\;0\;0\;1\;1\;0\;0\;1\;0\;\ldots$$

- Cette suite est produite par l'automate

$$\begin{tikzcd}
\boxed{i} \arrow[loop above, "1"] \arrow[r, bend left, "0"] & \boxed{a} \arrow[l, bend left, "0"] \arrow[r, "1"] & \boxed{b} \arrow[loop above, "0"] \arrow[loop below, "1"]
\end{tikzcd}$$

avec $f(i) = 1$, $f(a) = 0$, $f(b) = 0$.

La suite du pliage de papier

On plie une bande de papier toujours dans le même sens, puis on la déplie : les plis peuvent être entrants ou sortants, on les code par 0 ou 1. On obtient une suite

$$1101100111001001 \ \ldots$$

qui vérifie

$$u_{4n} = 1, \quad u_{4n+2} = 0, \quad u_{2n+1} = u_n$$

et qui est produite par l'automate

$$\begin{tikzcd}
 & & \boxed{b} \arrow[loop above, "0"] \arrow[loop right, "1"] \\
\boxed{i} \arrow[loop above, "1"] \arrow[r, "0"] & \boxed{a} \arrow[ur, "0"] \arrow[dr, "1"'] & \\
 & & \boxed{c} \arrow[loop above, "0"] \arrow[loop right, "1"]
\end{tikzcd}$$

avec $f(i) = f(a) = f(b) = 1$, $f(c) = 0$.

Le mot de Fibonacci n'est pas automatique

• Cobham (1972) : la fréquence d'une lettre qui apparaît dans un mot automatique est un nombre rationnel.
• Conséquence : le mot de Fibonacci

$$abaababaabaababaababa\dots$$

n'est pas automatique. La fréquence des a (resp. des b) est $1/\Phi$ (resp. $1/\Phi^2$), où $\Phi = (1+\sqrt{5})/2$ est le nombre d'or (irrationnel).

Complexité du développement en base g d'un nombre algébrique

- **Théorème** (B. Adamczewski, Y. Bugeaud, F. Luca 2004). *La complexité binaire p d'un nombre réel algébrique irrationnel x vérifie*

$$\liminf_{m\to\infty} \frac{p(m)}{m} = +\infty.$$

- Corollaire (conjecture de A. Cobham (1968)) : *si la suite des chiffres binaires d'un nombre réel irrationnel x est automatique, alors x est transcendant.*

Transcendance de nombres automatiques

En d'autres termes :

• **Théorème** (B. Adamczewski, Y. Bugeaud, F. Luca, 2004 – conjecture de A. Cobham, 1968) : *La suite des chiffres d'un nombre réel algébrique irrationnel n'est pas automatique.*

Outil : le théorème du sous-espace de W.M. Schmidt.

Mesures d'irrationalité de nombres automatiques

- Nouveaux progrès par B. Adamczewski et J. Cassaigne, Y. Bugeaud (2006) – solution d'une conjecture de J. Shallit (1999) : *La suite des chiffres binaires d'un nombre de Liouville ne peut pas être engendré par un automate fini.*
- La mesure d'irrationalité du nombre automatique défini par $\sigma(0) = 0^n 1$ et $\sigma(1) = 1^n 0$ est au moins n.
- Le nombre de Prouhet-Thue-Morse-Mahler ξ a un exposant d'irrationalité ≤ 5 :

$$\left| \xi - \frac{p}{q} \right| \geq \frac{c}{q^5}.$$

Indépendance de développements de nombres algébriques

Si on croit Borel et que les développements dans une base donnée de deux nombres comme $\sqrt{2}$ et $\sqrt{3}$ se comportent de façon aléatoire, on peut se demander si ces deux suites de chiffres se comportent de façon indépendante.
B. Adamczewski et Y. Bugeaud remarquent que c'est vrai pour presque tous les couples de nombres algébriques réels (par le lemme de Borel-Cantelli), ils conjecturent que le seul cas où ce n'est pas vrai est quand la fin des développements des deux nombres est la même.

Christol, Kamae, Mendes-France, Rauzy

Une conséquence du théorème de B. Adamczewski, Y. Bugeaud et F. Luca liée au résultat de G. Christol, T. Kamae, M. Mendès-France et G. Rauzy (1980) est la suivante :

Corollaire. *Soient* $g \geq 2$ *un entier,* p *un nombre premier et* $(u_k)_{k\geq 1}$ *une suite d'entiers dans l'intervalle* $\{0, \ldots, p-1\}$. *La série formelle*

$$\sum_{k\geq 1} u_k X^k$$

et le nombre réel

$$\sum_{k\geq 1} u_k g^{-k}$$

sont simultanément algébriques (sur $\mathbf{F}_p(X)$ *et* $\mathbf{Q}$*, respectivement) si et seulement s'ils sont rationnels.*

La suite de Prouhet-Thue-Morse

Soit $(a_n)_{n\geq 0}$ la suite de Prouhet-Thue-Morse. La série

$$F(X) = \sum_{n\geq 0} a_n X^n$$

est algébrique sur $\mathbf{F}_2(X)$:

$$(1+X)^3F^2 + (1+X)^2F + X = 0.$$

On en déduit une nouvelle démonstration du théorème de Mahler sur la transcendance du nombre

$$\sum_{n\geq 0} a_n g^{-n}.$$

Autres résultats de transcendance

Conséquences du théorème de Nesterenko (1996) sur la transcendance des valeurs de fonctions modulaires.

- Le nombre $\sum_{n\geq 0} 2^{-n^2}$ est transcendant (D. Bertrand 1997 ; D. Duverney, K. Nishioka, K. Nishioka et I. Shiokawa 1998).
- Pour le mot

$$\mathbf{u} = 01212212221222212222212222221222 \ \ldots$$

engendré par le morphisme $0 \mapsto 012$, $1 \mapsto 12$, $2 \mapsto 2$, le nombre $\eta = \sum_{k\geq 1} u_k 3^{-k}$ est transcendant.

Fractions continues

- Des questions analogues se posent sur le développement en fraction continue d'un nombre réel au lieu de son développement en base g.

$$[a_0;\ a_1,\ a_2,\dots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

- Les nombres rationnels sont ceux dont le développement en fraction continue est fini, les nombres réels quadratiques sont ceux dont le développement est infini périodique.

Question de Khinchin

- Problème ouvert – A.Ya. Khinchin (1949) : *les quotients partiels du développement en fraction continue d'un nombre réel algébrique irrationnel non quadratique peuvent-ils être bornés ?*
- On ne connaît aucun exemple !

Transcendance de fractions continues

- J. Liouville, 1844
- É. Maillet, 1906, O. Perron, 1929
- H. Davenport et K.F. Roth, 1955
- A. Baker, 1962
- J.L. Davison, 1989

Transcendance de fractions continues (suite)

- M. Queffélec, 1998 : *transcendance de la fraction continue de Prouhet-Thue–Morse.*
- J-P. Allouche, J.L. Davison, M Queffélec et L.Q. Zamboni, 2001 : *transcendance de fractions continues sturmiennes ou morphiques.*
- B. Adamczewski, Y. Bugeaud, J.L. Davison, 2005 : *transcendance des fractions continues de Rudin-Shapiro et de Baum–Sweet.*

Problèmes ouverts

- Donner un exemple explicite d'un nombre réel automatique $x > 0$ tel que $1/x$ ne soit pas automatique.
- Montrer que
$$\log 2 = \sum_{n \geq 1} \frac{1}{n} 2^{-n}$$
n'est pas 2-automatique.
- Montrer que
$$\pi = \sum_{n \geq 0} \left(\frac{4}{8n+1} - \frac{2}{8n+4} - \frac{1}{8n+5} - \frac{1}{8n+6} \right) 2^{-4n}$$
n'est pas 2-automatique.

Problèmes sur les nombres normaux (T. Rivoal)

- Donner un exemple explicite d'un nombre réel irrationnel simplement normal en base g tel que $1/x$ ne soit pas simplement normal en base g .
- Donner un exemple explicite d'un nombre réel irrationnel normal en base g tel que $1/x$ ne soit pas normal en base g .
- Donner un exemple explicite d'un nombre réel irrationnel normal tel que $1/x$ ne soit pas normal.

Autre problème ouvert

Soit $(e_n)_{n\geq 1}$ une suite infinie sur $\{0,1\}$ qui n'est pas ultimement périodique. Est-il vrai que *l'un au moins des deux nombres*

$$\sum_{n\geq 1} e_n 2^{-n}, \qquad \sum_{n\geq 1} e_n 3^{-n}$$

est transcendant ?

D'après Borel, comme le second nombre est irrationnel et ne comporte pas de 2 dans son développement en base 3, il devrait toujours être transcendant.

Colloquium Université de Rennes

Peut-on distinguer les nombres algébriques des nombres transcendants par leur développement ?

Michel Waldschmidt

http ://www.math.jussieu.fr/∼miw/

Lundi 8 janvier 2007