Boris Adamczewski

COMBINATOIRE DES MOTS ET PROBLÈMES DIOPHANTIENS

Boris Adamczewski

CNRS & Institut Camille Jordan, Université Claude Bernard Lyon 1,
21 avenue Claude Bernard, 69622 Villeurbanne cedex France.

E-mail : Boris.Adamczewski@math.univ-lyon1.fr

COMBINATOIRE DES MOTS ET PROBLÈMES DIOPHANTIENS

Boris Adamczewski

Résumé. — Le texte qui suit est issu de notes (plutôt informelles) que j'ai utilisées pour préparer un mini-cours pour la conférence "Développements Récents en Approximation Diophantienne" qui se déroulera au CIRM (Marseille) du 8 au 12 octobre 2007.

L'objet du cours, intitulé "Combinatoire des mots et problèmes diophantiens", est de présenter trois problèmes de théorie des nombres ayant connu des développements récents qui mettent en avant une interaction entre la combinatoire des mots et l'approximation diophantienne :

1. la complexité de la suite des chiffres des nombres algébriques ;
2. l'approximation des nombres réels par des entiers algébriques de degré borné ;
3. la recherche d'exemples explicites pour la conjecture de Littlewood.

Les mots finis ou infinis apparaissent naturellement en théorie des nombres dès que l'on souhaite représenter tous les éléments d'un certain ensemble (entiers, réels, p-adiques...) de façon unifiée. Ainsi, les développements décimaux, binaires ou en fraction continue permettent d'associer à tout nombre réel une unique suite finie ou infinie de chiffres. On étudiera à travers quelques exemples comment des propriétés combinatoires d'une suite de chiffres peuvent révéler certaines propriétés diophantiennes du nombre correspondant.

Le comportement du développement décimal ou du développement en fraction continue de la plupart des nombres réels est bien compris grâce aux propriétés ergodiques de systèmes dynamiques sous-jacents (associés à l'application $x \longmapsto 10x$ mod 1 pour le développement décimal ou à l'application de Gauss dans le cas du développement en fraction continue). En particulier, cela conduit, dans le contexte approprié, à la notion de 'nombre normal'. En dépit de spéculations audacieuses, dues notamment à É. Borel et S. Lang, il est malheureusement difficile d'obtenir des renseignements sur les suites des chiffres correspondant à des constantes mathématiques classiques comme π, $\zeta(3)$ ou encore $\sqrt{2}$. On montrera comment un outil diophantien puissant, le théorème du sous-espace de Schmidt, a récemment été utilisé afin d'obtenir de nouveaux résultats sur les représentations des nombres algébriques (voir [**6, 3, 1, 4**] et le survol [**63**]).

D'autre part, on expliquera comment certaines constructions combinatoires donnent vie à des nombres jouissant de propriétés diophantiennes remarquables.

Un exemple particulièrement intéressant vient de la découverte des nombres extrémaux par D. Roy (voir [**54, 55, 56**]). L'existence de tels nombres réels était totalement insoupçonnée et a permis d'infirmer une conjecture qui semblait alors naturelle sur l'approximation des nombres réels par des entiers algébriques cubiques, ainsi qu'une conjecture duale sur l'approximation simultanée et uniforme d'un nombre réel et de son carré.

Un autre exemple dans la même veine est la construction donnée dans [**2**] de couples explicites de nombres réels satisfaisant à la conjecture de Littlewood.

TABLE DES MATIÈRES

CHAPITRE 1

UNE INTRODUCTION À LA COMBINATOIRE DES MOTS

Afin de satisfaire ceux ou celles qui voudraient éventuellement en savoir plus, voici quelques références d'ouvrages intéressants portant sur la combinatoire des mots : les livres du collectif Lothaire [**37, 38, 39**], le livre de N. Pytheas Fogg [**50**] et celui d'Allouche et Shallit [**11**].

1.1. Notations

Etant donné un ensemble fini (ou éventuellement dénombrable) $\mathcal{A}$, on désigne par $\mathcal{A}^*$ le monoïde libre engendré par $\mathcal{A}$ (la loi sous-jacente étant la concaténation). Les élément de $\mathcal{A}$ sont appelés *lettres* ou *symboles* et les éléments de $\mathcal{A}^*$ sont appelés *mots finis* ou suites finis. Le mot vide, noté ε, est l'élément neutre de $\mathcal{A}^*$. Les éléments de l'ensemble $\mathcal{A}^{\mathbb{N}}$ sont appelés *mots infinis* ou suites infinis.

La combinatoire des mots a pour objet l'étude des propriétés combinatoires des mots finis ou infinis définis sur un alphabet $\mathcal{A}$ qui est le plus souvent fini.

Un mot fini $W = w_0w_1 \dots w_r$ est un *facteur* d'un mot infini $\mathbf{a} = a_0a_1 \dots$ s'il existe un entier i tel que $w_0w_1 \dots w_r = a_ia_{i+1} \dots a_{i+r-1}$. On dit que l'entier i est une *occurrence* de W dans $\mathbf{a}$. On appelle *langage* du mot infini $\mathbf{a}$ l'ensemble de ses facteurs que l'on note $\mathcal{L}(\mathbf{a})$. La *longueur* d'un mot fini W est le nombre de lettres qui le compose, elle est notée $|W|$. Le mot vide ε est l'unique mot de longueur 0.

L'ensemble $\mathcal{A}^{\mathbb{N}}$ est muni de la topologie produit des topologies discrètes sur chaque copie de $\mathcal{A}$. Cette topologie est induite par la distance d définie par

$$d(\mathbf{w}, \mathbf{w}') = \frac{1}{2^{\inf \{i \in \mathbb{N},\ w_i \neq w_i'\}}},$$

où $\mathbf{w} = w_0w_1 \dots$ et $\mathbf{w}' = w_0'w_1' \dots$ sont deux mots infinis définis sur $\mathcal{A}$ (avec la convention $\inf\{\emptyset\} = +\infty$). On construit souvent des mots infinis comme "limite de mots finis". Pour cela, il faut donner un sens à la notion de limite. On peut procéder de la façon suivante. On ajoute un symbole, noté $*$, à l'ensemble $\mathcal{A}$ sur lequel les mots finis sont définis, et on pose $\mathcal{A}' = \mathcal{A} \cup \{*\}$. Etant donné un mot fini $W = w_1w_2 \dots w_r \in \mathcal{A}^*$, on lui associe le mot infini $W' = w_1w2 \dots w_r * * * \dots$ appartenant à $\mathcal{A}'^{\mathbb{N}}$. On dit alors qu'une suite de mots finis $(W_n)_{n\geq 0}$ converge vers un mot infini dans $\mathcal{A}^{\mathbb{N}}$ si la suite $(W'_n)_{n\geq 0}$ converge dans $\mathcal{A}'^{\mathbb{N}}$ vers un élément de $\mathcal{A}^{\mathbb{N}}$.

Voici un exemple d'une telle construction. Posons $W_0 = 0$ et $W_1 = 1$, puis pour tout entier $n \geq 1$, $W_{n+1} = W_n W_{n-1}$. Cette suite de mots finis converge vers un mot infini

$$\mathbf{f} = 0100101001001010010100100101001001\ldots$$

Ce mot est appelé mot de Fibonacci. Notons que la suite $(|W_n|)_{n\geq 0}$ est la suite de Fibonacci (modulo un éventuel changement d'indice) puisque $|W_{n+1}| = |W_n|+|W_{n-1}|$, $|W_0| = 1$ et $|W_1| = 1$.

On peut également associer de façon naturelle un système dynamique topologique à tout mot infini $\mathbf{a} = a_0 a_1 \ldots$ défini sur un ensemble $\mathcal{A}$. Considérons l'application de décalage S (shift en anglais) définie sur $\mathcal{A}^{\mathbb{N}}$ par $S(w_0 w_1 \ldots) = w_1 w_2 \ldots$. Notons que S est une application continue. On définit alors l'orbite (positive) de $\mathbf{a}$ sous l'action de S par $\mathcal{O}(\mathbf{a}) = \{S^n(\mathbf{a}),\ n \geq 0\}$. En prenant la fermeture topologique de cet ensemble, on obtient un sous-ensemble compact de $\mathcal{A}^{\mathbb{N}}$ qui est invariant par S. Ainsi, $\mathcal{X} = (\overline{\mathcal{O}(\mathbf{a})}, S)$ est un système dynamique topologique appelé sous-shift ou sous-décalage associé à $\mathbf{a}$. Un des objets de la dynamique symbolique est d'étudier les propriétés de tels systèmes. Ces dernières dépendent évidemment des propriétés combinatoires du mot infini sous-jacent.

1.2. La suite de Thue–Morse

Considérons l'alphabet binaire $\mathcal{A} = \{0, 1\}$. Il n'est pas difficile de voir que tout mot de longueur supérieure ou égale à 4 contient un carré, c'est-à-dire, un mot de la forme XX, avec $X \in \{0, 1, 01, 10\}$. Ainsi, tout mot infini binaire contient une infinité de carrés et on dit que le motifs XX ou X^2 est inévitable, ou, plus simplement, que les carrés sont inévitables sur un alphabet binaire. Notons qu'il y a une différence importante entre la notion de mot et celle de motif. Ainsi, les mots 00, 11, 0101 et 1010 sont quatres exemples de mots différents qui reflètent le même motif XX.

En 1906 et 1912, le mathématicien norvégien A. Thue [**61**] (que les théoriciens des nombres connaissent davantage pour son résultat sur les équations diophantiennes qui portent désormais son nom) a écrit deux articles dans lesquels il étudie les deux problèmes suivants :

(1) Existe-t-il un mot infini binaire qui évite les cubes, c'est-à-dire, le motif XXX ?

(2) Existe-t-il un mot infini sur un alphabet ternaire qui évite les carrés ?

On considère souvent que ces articles marquent la naissance de la combinatoire des mots.

Thue a répondu par l'affirmative à ces deux questions en introduisant une suite infini binaire $\mathbf{t} = (t_n)_{n\geq 0}$ appelée aujourd'hui suite de Thue–Morse. On peut définir cette suite grâce aux relations de récurrence suivantes :

$$t_0 = 0 \quad \text{et} \quad t_{2n} = t_n,\ \ t_{2n+1} = 1 - t_n,\ \text{pour tout entier } n \geq 0.$$

Ainsi

$$\mathbf{t} = 0110100110010110100101100110100 1\ldots$$

La suite $\mathbf{t}$ a la propriété remarquable d'éviter tout *chevauchement*, c'est-à-dire, tout motif de la forme $xXxXx$, ou $x \in \mathcal{A}$ et $X \in \mathcal{A}^*$. On obtient en particulier une réponse positive à la question (1). La démonstration de ce résultat n'est pas difficile, mais il s'agit d'une étude de cas un peu technique.

Pour obtenir une suite ternaire sans carré à partir de $\mathbf{t}$, il suffit de considérer la suite $\mathbf{t}' = (t_n)_{n\geq 1}$, où t'_n désigne le nombre de 1 entre la n-ième et la $(n+1)$-ième occurrence de 0 dans $\mathbf{t}$. Ainsi,

$$\mathbf{t}' = 21020121012\ldots \tag{1}$$

Si $\mathbf{t}'$ contenait un carré, disons W^2 avec $W = w_1 \ldots w_r$, alors le mot

$$01^{w_1}01^{w_2}\ldots 01^{w_r}01^{w_1}\ldots 01^{w_r}0,$$

qui est un chevauchement, serait un facteur de la suite de Thue–Morse.

Alors que Thue avait simplement étudié ce problème “pour le développement des sciences logiques” (traduit de l'allemand) et sans application en vue, ses travaux ont été redécouverts plusieurs fois et la suite de Thue–Morse apparaît naturellement dans des domaines aussi variés que la théorie des groupes, la théorie ergodique, la géométrie différentielle, la théorie des nombres, la physique mathématique ou l'informatique théorique. D'autre part, la théorie des motifs inévitables s'est considérablement développée. Voici deux exemples illustrant l'ubiquité de la suite de Thue–Morse (voir [**10**] pour un survol sur ce sujet).

Le problème de Burnside. Il s'agit d'un problème classique de la théorie des groupes : existe-t-il un groupe infini G engendré par un nombre fini de générateurs et tel que $x^n = 1$ pour tout $x \in G$? La réponse au problème de Burnside est négative si $n = 2$, puisque dans ce cas le groupe est abélien. Dans les années 60, Adian et Novikov (voir [**9**]) ont résolu le problème de Burnside en montrant qu'il est possible de construire un tel groupe si n est assez grand (on sait que $n \geq 665$ convient). La démonstration de ce résultat fait intervenir la construction d'une suite binaire sans cube. Un problème assez similaire concernant les monoïdes nilpotents a été considéré par Hedlund et Morse [**47**]. Ces auteurs utilisent également la suite de Thue–Morse.

Géodésiques des surfaces à courbures négatives. Morse [**44**] a démontré que sur une surface de courbure négaitve, il existe un ensemble non dénombrable de géodésiques récurrentes qui ne sont pas fermées. La démonstration repose sur un codage des géodésiques, de sorte que l'on associe à toute géodésique un mot infini binaire. Les géodésiques fermés correspondent aux mot ultimement périodiques, tandis que la propriété de récurrence correspond aux mots uniformément récurrents ou minimaux. Une suite infinie est uniformément récurrente si pour tout entier n il existe un entier N tel que tout mot de longueur N contient tous les facteurs de longueur n de la suite. Cela est équivalent au fait que le sous-shift associé à $\mathbf{a}$ est minimal, c'est-àdire, que les seuls ouverts invariants par le décalage sont l'ensemble vide et X lui-même, ou encore que toute orbite est dense. Au final, la solution vient de l'exitence d'une suite uniformément récurrente et non périodique. Morse utilise la suite $\mathbf{t}$ qui réunit ces deux propriétés.

1.3. Mots engendrés par morphismes

Un procédé naturel pour construire des mots infinis sur un alphabet fini $\mathcal{A}$ consiste à utiliser les morphismes du monïde libre $\mathcal{A}^*$. Pour définir un tel morphisme, c'est assez simple, il suffit de connaître les images des éléments de $\mathcal{A}$.

Morphismes. Soient $\mathcal{A}$ et $\mathcal{B}$ deux ensembles finis. Une application σ de $\mathcal{A}$ vers $\mathcal{B}^*$ peut être étendue de façon unique en un homomorphisme du monoïde $\mathcal{A}^*$ vers le monoïde $\mathcal{B}^*$. On appellera simplement morphisme de $\mathcal{A}$ vers $\mathcal{B}$ un tel homomorphisme. Le morphisme σ est dit *non effaçant* ou *positif* si aucun élément de $\mathcal{A}$ n'a pour image le mot vide, et σ est dit k-uniforme si $|\sigma(a)| = k$ pour tout $a \in \mathcal{A}$. Un morphisme 1-unifome est appelé un codage. Dans la suite, nous nous intéressons plus particulièrement aux morphismes d'un alphabet $\mathcal{A}$ vers lui-même.

Mots infinis engendrés par morphismes. Un morphisme ϕ de $\mathcal{A}$ dans lui-même est dit prolongeable s'il existe une lettre a telle que $\phi(a) = aW$, où W est un mot non vide tel que $\phi^k(W) \neq \varepsilon$ pour tout entier $k \geq 0$. Dans ce cas, la suite de mots finis $(\phi^k(a))_{k\geq 1}$ converge dans $\mathcal{A}^{\mathbb{N}}$ vers un mot infini $\mathbf{a}$. Ce mot est clairement invariant par ϕ et on dit alors que $\mathbf{a}$ est engendré par le morphisme ϕ. Plus généralement, une suite $\mathbf{a}$ appartenant à $\mathcal{A}^{\mathbb{N}}$ est dite morphique s'il existe une suite $\mathbf{u}$ engendrée par un morphisme défini sur un alphabet $\mathcal{B}$ et un morphisme ϕ de $\mathcal{B}$ vers $\mathcal{A}$ tels que $\mathbf{a} = \phi(\mathbf{u})$.

Exemples. Le morphisme de Thue–Morse τ defini sur l'alphabet $\{0, 1\}$ par $\tau(0) = 01$ et $\tau(1) = 0$ engendre le mot de Thue–Morse

$$\mathbf{t} = \lim_{n\to\infty} \tau^n(0) = 0110100110010110100101100110100 1\ldots$$

On vérifie facilement que le morphisme ϕ défini par $\phi(0) = 01$ et $\phi(1) = 0$ a un unique point fixe qui est le mot de Fibonacci

$$\mathbf{f} = \lim_{n\to\infty} \phi^n(0) = 0100101001001010010100100101001 0\ldots$$

1.4. Mots engendrés par des automates finis

Les automates finis sont l'un des modèles les plus basiques de calcul. Ils forment une classe de machines de Turing particulièrement simples. Intuitivement, une suite $\mathbf{a} = (a_n)_{n\geq 0}$ est dite k-automatique si a_n est une fonction assez simple (fonction à états finis) de l'écriture de l'entier n en base k. Ces suites ont une structure très riche et jouissent de nombreuses propriétés. Pour en savoir davantage sur ce sujet, le livre d'Allouche et Shallit [**11**] est une excellente référence.

Voici une définition plus formelle. Soit $k \geq 2$ un entier. On désigne par Σ_k l'alphabet $\{0, 1, \ldots, k-1\}$. Un k-automate fini est un 6-uplet

$$A = (Q, \Sigma_k, \delta, q_0, \Delta, \tau)\,,$$

où Q est un ensemble fini d'états, Σ_k est un alphabet d'entré, $\delta : Q \times \Sigma_k \to Q$ est la fonction de transition, q_0 est un élément de Q appelé état initial, Δ est l'alphabet de sortie et $\tau : Q \to \Delta$ est la fonction de sortie.

Etant donné un état q dans Q et un mot fini $W = w_1 w_2 \ldots w_n$ défini sur l'alphabet Σ_k, on définit récursivement $\delta(q, W)$ par $\delta(q, W) = \delta(\delta(q, w_1 w_2 \ldots w_{n-1}), w_n)$. Soit $n \geq 0$ un entier et $w_r w_{r-1} \ldots w_1 w_0 \in (\Sigma_k)^r$ le développement en base k de n, c'est-à-dire $n = \sum_{i=0}^{r} w_i k^i$. Notons W_n le mot $w_0 w_1 \ldots w_r$. Alors, une suite $\mathbf{a} = (a_n)_{n\geq 0}$ est dite engendré par un k-automate fini ou encore *k-automatique* s'il existe un k-automate fini A tel que $a_n = \tau(\delta(q_0, W_n))$ pour tout entier $n \geq 0$. Notons que l'on a choisi ici de lire les entiers donnés en entrée en commençant par le chiffre le moins significatif. On aurait pu choisir de lire d'abord le chiffre le plus significatif. Dans le cas des automates finis, cela ne change pas l'ensemble des suites obtenues.

La suite de Thue–Morse est un exemple emblématique de suite 2-automatique. En effet, $\mathbf{t} = (t_n)_{n\geq 0} = 0110100110010\ldots$ peut être définie de la façon suivante : a_n est égale à la somme modulo 2 des chiffres de l'écriture binaire de n. Il est facile de voir que cette suite est engendrée par le 2-automate fini suivant :

$$A = \big(\{q_0, q_1\}, \{0, 1\}, \delta, q_0, \{0, 1\}, \tau\big),$$

où

$$\delta(q_0, 0) = \delta(q_1, 1) = q_0, \qquad \delta(q_0, 1) = \delta(q_1, 0) = q_1,$$

et $\tau(q_0) = 0$, $\tau(q_1) = 1$. En image, tout est plus clair, comme le montre la figure 1.

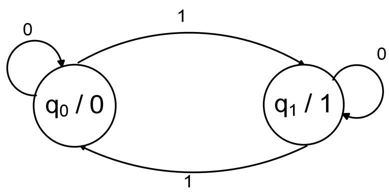

FIGURE 1. Automate fini engendrant la suite de Thue–Morse

Par exemple, si on entre le mot $w = 10110$ dans cet automate, on obtient en sortie 1, ce qui signifie que $t_{22} = 1$.

Un autre exemple en base 3 : la suite des entiers de Cantor. On définit la suite $\mathbf{k} = (k_n)_{n\geq 0}$ en posant $k_n = 1$ si n ne contient pas de 1 dans son développement ternaire et $k_n = 0$ sinon. Cette terminologie s'explique par l'analogie existant entre $\mathbf{k}$ et l'ensemble triadique de Cantor :

$$\mathcal{C} = \left\{ x \in [0,1],\ x = \sum_{n\geq 1} \frac{a_n}{3^n},\ a_n \in \{0, 2\} \right\}.$$

La suite $\mathbf{k}$ est 3-automatique. Elle est engendrée par l'automate représenté sur la figure 2.

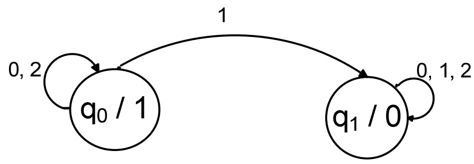

FIGURE 2. Automate fini engendrant la suite des entiers de Cantor

Il existe un lien profond entre les suites automatiques et les suites engendrées par morphismes, comme l'illustre le théorème suivant de Cobham [**21**].

Théorème 1.4.1. (*Cobham, 1972*) — *Une suite est k-automatique si, et seulement si, elle est l'image par un codage d'un point fixe de substitution k-uniforme.*

Par exemple, la suite $\mathbf{k}$ des entiers de Cantor est l'unique point fixe commençant par 1 du morphisme κ défini par $\kappa(0) = 000$ et $\kappa(1) = 101$.

Les automates finis permettent également de décrire les séries formelles à coefficients dans un corps fini qui sont algébriques sur le corps des fractions rationnelles, comme le montre le théorème de Christol énoncé ci-dessous [**18, 19**]. Si q une puissance d'un nombre premier p, on note $\mathbb{F}_q$ le corps à q éléments.

Théorème 1.4.2. (*Christol, 1979*) — *Soit q une puissance d'un nombre premier p. Une série formelle $\sum_{n\geq 0} a_n X^n$ appartenant au corps des séries de Laurent $\mathbb{F}_q((X))$ est algébrique sur $\mathbb{F}_q(X)$ si, et seulement si, la suite $(a_n)_{n\geq 0}$ est p-automatique.*

Voici un exemple illustrant ce théorème. Considérons la série formelle

$$t(X) = \sum_{n\geq 0} t_n X^n \in \mathbb{F}_2((X)),$$

où $(t_n)_{n\geq 0}$ est la suite de Thue–Morse. Puisque $t_{2n} = t_n$ et $t_{2n+1} = 1 - t_n$, il vient

$$\begin{aligned} t(X) &= \sum_{n\geq 0} t_{2n} X^{2n} + \sum_{n\geq 0} t_{2n+1} X^{2n+1} \\ &= \sum_{n\geq 0} t_n X^{2n} + \sum_{n\geq 0} (1 - t_n) X^{2n+1} \\ &= t(X^2) + X t(X^2) + \sum_{n\geq 0} X^{2n+1} \\ &= (1 + X) t(X^2) + \frac{X}{1 + X^2} \cdot \end{aligned}$$

Le clacul précédent peut sembler déroutant, mais il faut penser qu'on travaille sur le corps fini à deux éléments et donc que $1 = -1$. On obtient finalement

$$(1 + X)^3 t(X)^2 + (1 + X)^2 t(X) + X = 0,$$

ce qui signifie que la série formelle $t(X)$ est algébrique (en fait, quadratique) sur $\mathbb{F}_2(X)$.

1.5. Complexité d'un mot infini, entropie

Une façon classique de mesurer la complexité d'un mot infini $\mathbf{a} = a_1a_2\ldots$ prenant ses valeurs dans un ensemble fini $\mathcal{A}$ consiste à introduire la fonction de complexité qui à tout entier n associe l'entier $p(n, \mathbf{a})$ défini par

$$p(n, \mathbf{a}) = \mathrm{Card}\{(a_j, a_{j+1}, \ldots, a_{j+n-1}) : j \geq 1\}.$$

Par exemple, le mot $\mathbf{b} = bbb\ldots := b^\infty$ vérifie $p(n, \mathbf{b}) = 1$ pour tout entier n, tandis que le mot de Champernowne

$$\mathbf{c} = 01234567891011121314151617\ldots$$

vérifie $p(n, \mathbf{b}) = 10^n$ pour tout entier n. Cette notion a été introduite par Hedlund et Morse en 1938 [**45**].

Clairement, la fonction de complexité d'un mot infini est une fonction croissante (au sens large) qui vérifie

$$1 \leq p(n, \mathbf{a}) \leq (\mathrm{Card}\,\mathcal{A})^n, \quad \text{pour tout entier } n \geq 1.$$

Il est également facile de vérifier que la fonction de complexité d'un mot utlimement périodique est bornée (si $\mathbf{a} = UVVV\ldots = UV^\infty$, alors $|U| + |V|$ est un majorant de $p(n, \mathbf{a})$). En fait, cette proriété caractérise les suites ultimement périodiques, comme le montre le résultat suivant de Hedlund et Morse [**45**].

Théorème 1.5. (*Hedlund & Morse, 1938*) — *Soit* $\mathbf{a}$ *un mot infini non ultimement périodique. Alors, la fonction de complexité de* $\mathbf{a}$ *est strictement croissante. En particulier,*

$$p(n, \mathbf{a}) \geq n + 1,$$

pour tout entier positif n.

Démonstration. — Soit $\mathbf{a} = (a_n)_{n\geq 1}$ un mot infini. On sait déjà que la fonction de complexité p est croissante. Supposons qu'il existe un entier n tel que $p(n, \mathbf{a}) = p(n+1, \mathbf{a}) := M$, et montrons que $\mathbf{a}$ est ultimement périodique.

Pour chaque mot fini W de longueur n apparaissant dans $\mathbf{a}$, on choisit un entier $i(W)$ qui correspond a une occurrence de W, c'est-à-dire, tel que $W = a_{i(W)}a_{i(W)+1}\ldots a_{i(W)+n-1}$. On considère alors l'application e qui associe à W le mot $e(W) = a_{i(W)}a_{i(W)+1}\ldots a_{i(W)+n}$. L'application e est une injection entre deux ensembles qui par hypothèse ont le même cardinal (l'ensemble des facteurs de longueur n de $\mathbf{a}$ et celui des facteurs de longueur $n+1$). Il s'agit donc d'une bijection. Considérons maintenant l'application f définie par $f(W) = a_{i(W)+1}\ldots a_{i(W)+n}$. Il s'agit d'une application de l'ensemble des facteurs de longueur n de $\mathbf{a}$ dans lui-même. Comme cette ensemble est fini, cette application admet un cycle, c'est-à-dire, qu'il existe un facteur de longueur n de $\mathbf{a}$, disons W_0, et un entier $m \leq M$ tel que $f^m(W_0) = W_0$.

Considérons W un facteur de longueur n de $\mathbf{a}$ et un entier i (pas forcément égale à $i(W)$) qui est une occurrence de W. Notons W_1 le mot $a_i a_{i+1} \dots a_{i+n} = W a_{i+n}$. Puisque e est une bijection, il existe un mot W' tel que $W_1 = e(W')$. Par définition, W' est un préfixe de W_1 et donc $W' = W$. Ainsi, le suffixe de longueur n de W_1 est $f(W)$ et donc $i+1$ est une occurrence de $f(W)$. En itérant, on obtient que $i+j$ est une occurrence de $f^j(W)$, pour tout entier j.

Choisissons $W = W_0$. Alors, pour tout entier j, les entiers $i+j$ et $i+j+m$ sont des occurrences du même mot $f^j(W_0)$. En particulier, il vient

$$a_{i+j} = a_{i+j+m},$$

pour tout entier $j \geq 0$, ce qui signifie que le mot $\mathbf{a}$ est ultimement périodique. □

Mots de Fibonacci, mots sturmiens. Le théorème de Hedlund et Morse est en fait optimal. Il existe en effet des mots infinis $\mathbf{a}$ vérifiant $p(n, \mathbf{a}) = n+1$ pour tout entier $n \geq 1$. De tels mots sont appelés *mots sturmiens*. Le mot de Fibonacci $\mathbf{f}$ est un exemple de mot sturmien (en fait, c'est l'exemple canonique).

Les mots sturmiens peuvent être caractérisés de façon combinatoire, géométrique ou arithmétique. Ces mots apériodiques, qui par définition sont à la frontière de la périodicité, jouissent de nombreuses propriétés et ont fait l'objet d'une multitude de travaux dans des domaines variés (arithmétique, théorie ergodique, dynamique symbolique, pavages, quasi-cristaux, transcendance...).

Voici par exemple une description arithmétique de ces mots infinis que l'on doit également à Hedlund et Morse [**46**].

Théorème. (*Hedlund & Morse, 1940*) — *Un mot infini* $\mathbf{a}$ *sur l'alphabet* $\{0,1\}$ *est sturmien si, et seulement si, il existe un nombre irrationnel* α *appartenant à* $[0,1]$ *et un nombre réel* x *appartenant à* $[0,1]$ *tels que*

$$a_n = \lfloor (n+1)\alpha + x \rfloor - \lfloor n\alpha + x \rfloor \quad \textit{pour tout entier } n \geq 0 \tag{2}$$

ou

$$a_n = \lceil (n+1)\alpha + x \rceil - \lceil n\alpha + x \rceil \quad \textit{pour tout entier } n \geq 0.$$

Le nombre irrationnel α est l'*angle* de la suite sturmienne $\mathbf{a}$. Il correspond à la fréquence d'apparition de la lettre 1 dans cette suite. Le mot de Fibonacci correspond au cas où $\alpha = (\sqrt{5}-1)/2$ et $x = 0$ dans (2). On dit qu'une suite sturmienne est *caractéristique* lorsque $x = 0$.

Entropie. On définit l'entropie d'une suite $\mathbf{a}$ définie sur l'alphabet $\mathcal{A}$ par

$$h(\mathbf{a}) = \lim_{n\to\infty} \frac{\log p(n, \mathbf{a})}{n}\cdot$$

La limite existe existe bien comme conséquence de l'inégalité $p(n+m) \leq p(n)p(m)$ (qui se vérifie aisément). Si le logarithme considéré a pour base l'entier Card $\mathcal{A}$, alors $0 \leq h(\mathbf{a}) \leq 1$. Cette notion correspond en fait à l'entropie topologique du système dynamique naturellement associé à $\mathbf{a}$: le sous-shift engendré par la suite $\mathbf{a}$.

CHAPITRE 2

LA SUITE DES CHIFFRES D'UN NOMBRE ALGÉBRIQUE

Dans cette partie, on s'intéresse au développement décimal, binaire, ou plus généralement en base b, des nombres réels, et plus particulièrement des nombres réels algébriques. Les nombres rationnels ont un développement ultimement périodique et leur structure est donc assez simple. Par contre, lorsque l'on s'intéresse aux chiffres de l'écriture décimale d'un nombre algébrique irrationnel, comme

$$\sqrt{2} = 1.4142135623730950488016887242096980785696718753769480731766797 37\ldots,$$

on ne voit apparaître aucune structure particulière (même en regardant plus de chiffres !). Tout ce qu'on peut dire, c'est que ça semble bien compliqué et on aimerait expliquer ce phénomène.

2.1. Qu'est ce qu'un nombre "complexe" ?

Pour savoir quoi chercher, il serait bon de définir ce qu'est un nombre complexe (relativement à son développement décimal ou binaire), ou au moins certaines des propriétés que l'on peut espérer retrouver dans la suite des chiffres d'un tel nombre. Il y a plusieurs façons de procéder et on va brièvement en décrire deux.

Approche probabiliste et normalité. Une première façon de faire est de penser à un nombre décimal complexe comme à une suite d'éléments choisis aléatoirement dans l'ensemble $\{0, 1, \ldots, 9\}$. Cette idée conduit à la notion de *nombre normal*.

Si $b \geq 2$ un entier, un nombre réel ξ est dit normal en base b si, pour tout entier n, chaque bloc de n chiffres apparaît dans le développement en base b de ξ avec une fréquence égale à $1/b^n$. Émile Borel [**12**] a introduit cette notion et démontré le résultat suivant (c'est une conséquence de la loi forte des grands nombres).

Théorème. (*E. Borel, 1909*) — *Presque tout nombre réel (au sens de la mesure de Lebesgue) est normal, c'est-à-dire, normal en toute base entière.*

Paradoxalement, on ne connait toujours aucun exemple naturel de tel nombre. Les nombres Ω de Chaitin, qui sont définis comme « les probabilités d'arrêt des machines de Turing universelles à programmes autodélimités »(voir par exemple[**15**]), sont bien des exemples explicites de nombres normaux en toute base entière, mais leur définition semble interdire le qualificatif d'« exemple naturel ». Par contre, on connait pas mal d'exemples de nombre normaux en base 10. Ainsi, Champernowne [**17**] a montré en 1933 que le nombre

$$0.12345678910111213 14\ldots,$$

est normal en base 10. Dans le même esprit, Copeland et Erdös [**22**] ont montré que le nombre

$$0.23571113171923293137 4143\ldots\ldots$$

est également normal en base 10.

La notion de normalité permet de formuler une conjecture parfois appelée conjecture de Borel en raison de [**13**]. Résoudre cette conjecture permettrait d'expliquer le comportement apparemment chaotique de la suite des chiffres décimaux d'un nombre comme $\sqrt{2}$.

Conjecture 2.1. — *Tout nombre algébrique irrationnel est normal.*

Comme on va le voir, on est bien loin de savoir résoudre ce problème...

Approche algorithmique : machine de Turing et autres complications. Les travaux fondateurs de Turing [**62**] conduisent à une classification grossière des nombres réels. D'un coté, il y a les nombres réels calculables, c'est-à-dire, les nombres réels dont le développement binaire peut être produit par une machine de Turing, tandis que d'un autre coté se trouvent les nombres réels incalculables qui, en quelque sorte, "échappeent aux ordinateurs". Bien que la plupart des nombres réels appartiennent à la seconde classe (la première étant dénombrable), les constantes mathématiques classiques sont généralement calculables.

Poursuivant les idées pionnières de Turing, Hartmanis et Stearns [**29**] ont suggéré de mesurer la complexité d'un nombre réel en utilisant l'aspect "quantitatif" de la notion de calculabilité et en prenant en compte le nombre $T(n)$ d'opérations nécessaire à une machine de Turing (à plusieurs rubans) pour produire les n premiers chiffres du développement binaire du nombre considéré. Dans cet esprit, un nombre réel est considéré comme d'autant plus simple qu'il peut être produit rapidement par une machine de Turing. Les nombres réels les plus simples en ce sens sont ceux pour lesquels $T(n) = O(n)$. On parle de nombres calculables en temps réel. Evidemment, on aimerait bien savoir où se situent les constantes mathématiques dans cette classification. C'est là encore une source de problèmes difficiles comme le problème d'Hartmanis–Stearns : existe-t-il des nombres algébriques irrationnels qui sont calculables en temps réels ? On attend plutôt une réponse négative à cette question.

Une autre approche algorithmique intéressante pour définir la complexité d'un nombre réel vient de la notion de complexité de Kolmogorov (voir par exemple [**35**]), mais on n'abordera pas ce sujet ici.

2.2. Transcendance des nombres bégayants

On va maintenant définir une nouvelle classe de mots infinis : les *mots bégayants*.

On rappelle que pour tout entier $k \geq 1$, le mot W^k désigne la concaténation k fois du mot W. Plus généralement, on peut définir une notion de répétition non entière. Etant donné un nombre réel $\alpha > 1$, on dit qu'un mot fini est une *puissance* α, s'il est de la forme $W^{\lfloor \alpha \rfloor} W'$ où W' est un préfixe de W tel que

$$|W^{\lfloor \alpha \rfloor} W'| \geq \alpha |W|.$$

Ainsi, le mot $0120120 = (012)^{2+1/3}$ est une puissance $2 + 1/3$ et un chevauchement est une puissance α, avec $\alpha > 2$. On appelle *bégaiement* une répétition non triviale, c'est-à-dire, une puissance α, avec $\alpha > 1$.

Soient $\mathbf{a} = (a_n)_{n\geq 1}$ un mot infini défini sur $\mathcal{A}$ et $w > 1$ un nombre réel. On dit que $\mathbf{a}$ est un *mot infini bégayant* s'il existe un nombre réel $w > 1$ et deux suites de mots finis $(U_n)_{n\geq 1}$ (U_n éventuellement vide) et $(V_n)_{n\geq 1}$ tels que :

(i) pour tout entier $n \geq 1$, le mot $U_n V_n^w$ est un préfixe de $\mathbf{a}$;

(ii) la suite $(|U_n|/|V_n|)_{n\geq 1}$ est bornée ;

(iii) la suite $(|V_n|)_{n\geq 1}$ est strictement croissante.

On dira qu'un nombre réel ξ est un *nombre réel bégayant* relativement à la base entière $b \geq 2$, si

$$\xi = \sum_{n=0}^{+\infty} \frac{a_n}{b^n}$$

où $\mathbf{a} = (a_n)_{n\geq 0} \in \{0, 1, \ldots, b-1\}^{\mathbb{N}}$ est un mot bégayant. Un nombre réel est dit bégayant s'il existe une base entière $b \geq 2$ relativement ̀laquelle il est bégayant.

Les mots bégayants sont, dans un certain sens, quasi-périodiques et nous allons exploiter cette propriété pour démontrer le résultat suivant [**6**].

Théorème 2.2. (*Adamczewski, Bugeaud & Luca, 2004*) — *Une nombre réel bégayant est soit rationnel, soit transcendant.*

On peut également interpréter ce résultat de la façon suivante : le développement d'un nombre algébrique irrationnel dans une base entière b est trop complexe pour être bégayant. On donnera dans les parties suivantes plusieurs conséquences intéressantes de ce théorème.

Démonstration. — Conservons les hypothèses du théorème. Soit $\mathbf{a} = (a_n)_{n\geq 1}$ un mot bégayant. Supposons que le paramètre $w > 1$ est fixé, ainsi que les suites $(U_n)_{n\geq 1}$ et $(V_n)_{n\geq 1}$ intervenant dans la définition d'une suite bégayante. Pour tout entier $n \geq 1$, posons $r_n = |U_n|$ et $s_n = |V_n|$. Nous allons montrer que

$$\alpha := \sum_{n=1}^{+\infty} \frac{a_n}{b^n}$$

est rationnel ou transcendant.

Remarque. Le point essentiel de cette démonstration est que α possède une infinité de bonnes approximations rationnelles obtenues en tronquant son développement et en le complétant par périodicité.

Plus précisément, pour tout entier $n \geq 1$, on définit la suite $(b_k^{(n)})_{k\geq 1}$ par $b_h^{(n)} = a_h$ pour $1 \leq h \leq r_n + s_n$ et $b_{r_n+h+js_n}^{(n)} = a_{r_n+h}$ pour $1 \leq h \leq s_n$ et $j \geq 0$. La suite $(b_k^{(n)})_{k\geq 1}$ est ultimement périodique, de pré-periode U_n et de période V_n. En posant

$$\alpha_n = \sum_{k=1}^{+\infty} \frac{b_k^{(n)}}{b^k}$$

on observe que

$$|\alpha - \alpha_n| < \frac{1}{b^{r_n+ws_n}} \tag{3}$$

puisque par hypothèse les $r_n + ws_n$ premiers chiffres du développement binaire de α et α_n sont identiques.

D'autre part, pour tout entier n, il existe un polynôme à coefficents entiers $P_n(X)$ de degré au plus $r_n + s_n - 1$ tel que

$$\alpha_n = \frac{P_n(b)}{b^{r_n}(b^{s_n} - 1)}. \tag{4}$$

En effet, on a

$$\begin{aligned}
\alpha_n &= \sum_{k=1}^{r_n} \frac{a_k}{b^k} + \sum_{k=r_n+1}^{+\infty} \frac{b_k^{(n)}}{b^k} = \sum_{k=1}^{r_n} \frac{a_k}{b^k} + \frac{1}{b^{r_n}} \sum_{k=1}^{+\infty} \frac{b_{r_n+k}^{(n)}}{b^k} \\
&= \sum_{k=1}^{r_n} \frac{a_k}{b^k} + \frac{1}{b^{r_n}} \sum_{k=1}^{s_n} \frac{a_{r_n+k}}{b^k} \left(\sum_{j=0}^{+\infty} \frac{1}{b^{js_n}} \right) \\
&= \sum_{k=1}^{r_n} \frac{a_k}{b^k} + \sum_{k=1}^{s_n} \frac{a_{r_n+k}}{b^{k+r_n-s_n}(b^{s_n} - 1)} = \frac{P_n(b)}{b^{r_n}(b^{s_n} - 1)},
\end{aligned}$$

où

$$P_n(X) = \sum_{k=1}^{r_n} a_k\, X^{r_n-k}(X^{s_n} - 1) + \sum_{k=1}^{s_n} a_{r_n+k}\, X^{s_n-k}.$$

Remarque. A ce stade, on vient de réaliser le programme de la première remarque. En écrivant $\alpha_n = p_n/q_n$, (3) et (4) impliquent que

$$\left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{q_n^{1+\delta}},$$

pour un certain $\delta > 0$. Les bégaiements nous ont donc permis d'hexiber une suite d'assez bonnes approximations rationnels de α. Notons que l'exposant $1 + \delta$ n'est à priori pas suffisant pour en déduire quoi que ce soit sur la transcendance (au mieux l'irrationalité de α si on est capable de montrer qu'une infinité de p_n/q_n sont distincts).

On rappelle en effet que tout nombre irrationnel admet une suite d'approximations rationnelles avec un exposant 2 (voir par exemple l'annexe B). Ici, ce qui va jouer en notre faveur c'est le fait que le dénominateur $q_n = b^{r_n}(b^{s_n} - 1)$ a une forme très particulière : c'est presque une puissance de b.

Reprenons notre démonstration. On va maintenant supposer que α est algébrique et on va monter que cela implique que α est rationnel. Pour cela, on considère les formes linéaires suivantes. Posons $L_{1,\infty}(x,y,z) = x$, $L_{2,\infty}(x,y,z) = y$, et $L_{3,\infty}(x,y,z) = \alpha x - \alpha y - z$. Ces formes linéaires sont indépendantes et à coefficients algégriques. D'après (3) et (4), il vient

$$|L_{3,\infty}(b^{r_n+s_n}, b^{r_n}, P_n(b))| \ll \frac{1}{b^{(w-1)s_n}}, \tag{5}$$

où la constante impliquée par le symbole $\ll$ est indépendante de n. On considère maintenant l'ensemble fini $\mathcal{S}$ des diviseurs premiers de b. Pour tout $p \in \mathcal{S}$, considérons les formes linéaires suivantes. Posons $L_{1,p}(x,y,z) = x$, $L_{2,p},(x,y,z) = y$, et $L_{3,p}(x,y,z) = z$. Il vient alors :

$$\prod_{p\in\mathcal{S}} \prod_{i=1}^{3} |L_{i,p}(b^{r_n+s_n}, b^{r_n}, P_n(b))|_p = \prod_{i=1}^{3} \left(\prod_{p\in\mathcal{S}} |L_{i,p}(b^{r_n+s_n}, b^{r_n}, P_n(b))|_p \right) \leq \frac{1}{b^{2r_n+s_n}}.$$

Ainsi, d'après (5), on a

$$\Pi := \left(\prod_{p\in\mathcal{S}} \prod_{i=1}^{3} |L_{i,p}(b^{r_n+s_n}, b^{r_n}, P_n(b))|_p \right) \prod_{i=1}^{3} |L_i(b^{r_n+s_n}, b^{r_n}, P_n(b))| \ll \frac{1}{b^{(w-1)s_n}}.$$

D'après la condition (ii) intervenant dans la définition d'une suite bégayante, on a

$$\Pi < \frac{1}{\max\{b^{r_n+s_n}, b^{r_n}, P_n(b)\}^{\varepsilon}}$$

pour un certain $\varepsilon > 0$.

La version p-adique du théorème du sous-espace (rapplelé dans l'annexe A) imlique alors que les points entiers $(b^{r_n+s_n}, b^{r_n}, P_n(b))$, $n \geq 1$, appartiennent à un une union finie de sous-espaces vectorielles propres de $\mathbb{Q}^3$. Il existe donc un triplet d'entiers non tous nuls (x_0, y_0, z_0) et une infinité d'entiers n tels que

$$x_0 - y_0 \frac{b^{r_n}}{b^{r_n+s_n}} - z_0 \frac{P_n(b)}{b^{r_n+s_n}} = 0.$$

En considérant de tels entiers n arbitrairement grands, on obtient $x_0 = z_0\alpha$. D'autre part, si $x_0 = z_0 = 0$ alors $y_0 = 0$, ce qui conduit à une contradiction. Ainsi, α est un nombre rationnel, ce qui termine cette démonstration. $\square$

2.3. Complexité des nombres algébriques

Soit $b \geq 2$ un entier et $\mathbf{a} = (a_n)_{n\geq 0}$ une suite à valeurs dans l'ensemble $\{0, 1, \ldots, b-1\}$. On a défini dans la partie 1.5 la fonction de complexité du mot $\mathbf{a}$ qui à tout entier

n associe l'entier $p(n, \mathbf{a})$ défini par

$$p(n, \mathbf{a}) = \mathrm{Card}\{(a_j, a_{j+1}, \ldots, a_{j+n-1}) : j \geq 1\}.$$

Si ξ est un nombre réel dont le développement en base b est

$$\xi = a_0.a_1a_2a_3\ldots,$$

on définit la fonction de complexite de ξ en base b, comme la fonction qui à tout entier n associe le nombre $p(n, \xi, b) = p(n, \mathbf{a})$.

On vérifie immédiatement que la fonction de complexité d'un nombre réel ξ normal en base b est maximale, c'est-à-dire, qu'on a $p(n, \xi, b) = b^n$ pour tout entier n. Motivé par la conjecture 2.1, on cherche dans cette partie à minorer la fonction de complexité des nombres algébriques irrationnels. Dans cette direction, on peut tout d'abord reformuler le théorème 1.5 de la façon suivante.

Théorème. (*Hedlund & Morse, 1938*) — *Soient $b \geq 2$ un entier et α un nombre algébrique irrationnel. Alors,*

$$p(n, \alpha, b) \geq n + 1,$$

pour tout entier n.

En fait, c'est la seule minoration connue qui soit valable pour tout entier n. Ce résultat a ensuite été étendu par Ferenczi et Mauduit [**27**] en1997 à l'aide du théorème de Ridout (voir l'annexe A). Ces auteurs ont montré que le développement b-adique d'un nombre algébrique α ne peut pas être un mot sturmien. On en déduit assez facilement que

$$\lim_{n\to\infty} p(n, \alpha, b) - n = +\infty.$$

Le théorème 2.2 permet d'améliorer ce résultat de façon significative [**3**].

Théorème. (*Adamczewski & Bugeaud, 2007*) — Soient $b \geq 2$ un entier et α un nombre algébrique irrationnel. Alors,

$$\lim_{n\to\infty} \frac{p(n, \alpha, b)}{n} = +\infty.$$

Démonstration. — D'après le théorème 2.2, il suffit de montrer qu'un mot $\mathbf{a} = a_1a_2\ldots$ dont la complexité vérifie

$$p(n, \mathbf{a}) \leq cn \qquad \text{pour une infinité d'entiers } n \geq 1,$$

pour un certain c, est bégayant.

Considérons une telle suite. Soit n un entier tel que $p(n, \mathbf{a}) \leq cn$. Pour tout entier k, on note $U(k)$ le préfixe de $\mathbf{a}$ de longueur k. Le principe des tiroirs assure alors l'existence d'au moins un mot M_n de longueur n admettant (au moins) deux occurrences dans $U((c+1)n)$. Il existe donc des mots finis (éventuellement vides) A_n, B_n, C_n et D_n, tels que

$$U((c+1)n) = A_nM_nC_nD_n = A_nB_nM_nD_n \quad \text{et} \quad |B_n| \geq 1.$$

Clairement, $|A_n| \leq cn$. On doit distinguer trois cas :

(i) $|B_n| > |M_n|$;
(ii) $\lceil |M_n|/3 \rceil \leq |B_n| \leq |M_n|$;
(iii) $1 \leq |B_n| < \lceil |M_n|/3 \rceil$.

(i). Il existe alors un mot E_n tel que

$$U((c+1)n) = A_n M_n E_n M_n D_n.$$

Puisque $|E_n| \leq (c-1)|M_n|$, le mot $A_n(M_nE_n)^s$, où $s = 1 + 1/c$, est un préfixe de $\mathbf{a}$. De plus, on a

$$|M_nE_n| \geq |M_n| \geq \frac{|A_n|}{c}\cdot$$

(ii). Il existe alors deux mots E_n et F_n tels que

$$U((c+1)n) = A_n M_n^{1/3} E_n M_n^{1/3} E_n F_n.$$

Le mot $A_n(M_n^{1/3}E_n)^2$ est donc un préfixe de $\mathbf{a}$. De plus, on a

$$|M_n^{1/3}E_n| \geq \frac{|M_n|}{3} \geq \frac{|A_n|}{3c}\cdot$$

(iii). Dans ce dernier cas, B_n est clairement un préfixe de M_n, et puisque $B_nM_n = M_nC_n$, on obtient que B_n^t est un préfixe de M_n, où t désigne la partie entière de $|M_n|/|B_n|$. En particulier, $t \geq 3$. En posant $s = \lfloor t/2 \rfloor$, on obtient que $A_n(B_n^s)^2$ est un préfixe de $\mathbf{a}$ et

$$|B_n^s| \geq \frac{|M_n|}{4} \geq \frac{|A_n|}{4c}\cdot$$

Dans chacun des trois cas considérés, on a donc montré qu'il existe des mots finis U_n et V_n tels que $U_nV_n^{1+1/c}$ est un préfixe de $\mathbf{a}$, $|U_n| \leq cn$ et $|V_n| \geq n/4$. On en déduit que le mot $\mathbf{a}$ est bégayant, ce qui termine cette démonstration. □

2.4. Conjecture de Cobham–Loxton–van der Poorten

En 1968, Cobham [**20**] proposa de restreindre le problème de Hartmanis et Stearns à une classe plus simple de machines de Turing, en considérant le cas des automates finis. Plusieurs tentatives pour résoudre ce problème sont dues à Cobham en 1968, puis à Loxton et van der Poorten en 1982 et en 1988 [**40, 41**], et leurs noms sont restés attachés à cette conjecture (la conjecture en question est devenue le théorème 2.4 ci-dessous). Le théorème 2.2 permet de la démontrer facilement [**3**].

Théorème 2.4. (*Adamczewski & Bugeaud, 2007*) — Le développement en base b d'un nombre algébrique irrationnel ne peut pas être engendré par un automate fini.

Démonstration. — D'après le théorème 2.2, il suffit de montrer que toute suite automatique est bégayante. Pour cela, on va utiliser le théorème de Cobham (théorème 1.4.1) qui lie morphismes uniformes et suites automatiques.

Soit $\mathbf{a} = (a_n)_{n\geq 1}$ une suite automatique déninie sur un alphabet $\mathcal{A}$. Il existe alors un morphisme uniforme σ sur un alphabet $\mathcal{B} = \{1, 2, \ldots, r\}$, un point fixe pour ce morphisme $\mathbf{u} = \sigma^\infty(1)$ et un codage φ de $\mathcal{B}$ dans $\mathcal{A}$ tels que $\mathbf{a} = \varphi(\mathbf{u})$. Evidemment, si $\mathbf{u}$ est un mot bégayant, le mot $\mathbf{a}$ bégaie également. Il suffit donc de montrer que $\mathbf{u}$ est un mot bégayant.

Le principe des tiroirs assure que le préfixe de longueur $r+1$ de $\mathbf{u}$ peut s'écrire sous la forme $W_1uW_2uW_3$, où u est une lettre et W_1, W_2, W_3 sont des mots finis (éventuellement vides). Pour tout entier $n \geq 1$, posons $U_n = \sigma^n(W_1)$ et $V_n = \sigma^n(uW_2)$. Puisque $\mathbf{u}$ est un point fixe de σ, le mot $\sigma^n(W_1uW_2u) = \sigma^n(W_1)\sigma^n(uW_2)\sigma^n(u)$ est, pour tout entier $n \geq 0$, un préfixe de $\mathbf{u}$. D'autre part, comme σ est un morphisme uniforme, on obtient que

$$\frac{|U_n|}{|V_n|} \leq \frac{|W_1|}{1+|W_2|} \leq r-1$$

et que $\sigma^n(u)$ est un préfixe de V_n de longueur $1/r$ fois la longueur de V_n. Le mot $U_nV_n^{1+1/r}$ est donc un préfixe de la suite $\mathbf{u}$, ce qui implique que cete suite est bégayante. □

En utilisant le même genre d'arguments, on peut montrer que les points fixes de morphisme binaire sont rationnels ou transcendants [**3**].

Théorème. — Un nombre algébrique irrationnel binaire n'est point fixe d'aucun morphisme non trivial.

En combinant le théorème de Christol et le théorème 2.4, on obtient le résultat suivant [**3**].

Théorème. — Soient p un nombre premier et $(a_n)_{\geq 0}$ une suite à valeurs dans $\{0, 1, \ldots, p-1\} \simeq \mathbb{F}_p$ qui n'est pas ultimement périodique. Considérons la série formelle

$$\sum_{n=0}^{+\infty} a_n X^n$$

et le nombre réel

$$\sum_{n=0}^{+\infty} a_n/p^n.$$

Alors, si l'un de ces deux "nombres" est algébrique (resp. sur les corps $\mathbb{F}_p(X)$ et $\mathbb{Q}$), l'autre est nécessairement transcendant.

En utilisant les bégaiements des mots engendrés par des automates finis, on peut aussi démontrer une conjecture proposée par Shallit : le développement en base b d'un nombre de Liouville (ce sont des nombres extrêmement bien approchables par des nombres rationnels) ne peut pas être engendré par un automate fini (voir [**7**]).

2.5. Motifs inévitables par les nombres algébriques binaires

Il n'est pas difficile de montrer que les quatre mots 0, 1, 01 et 10 doivent apparaître infiniment souvent dans le développement binaire d'un nombre algébrique irrationnel. Il s'agit d'une conséquence directe du fait que les nombres algébriques irrationnels ne peuvent pas avoir un développement binaire ultimement périodique. Cependant, si on fixe un nombre algébrique irrationnel α et un mot fini W dans $\{0,1\}^* \setminus \{\varepsilon, 0, 1, 01, 10\}$, on n'est toujours pas capable de dire si W apparaît infiniment souvent dans le développement binaire de α.

Plutôt que de s'intéresser aux occurrences de blocs de chiffres spécifiques (ce qui semble être un problème trop difficile pour le moment) on va se concentrer ici sur le squelette du développement binaire des nombres algébriques, en ce sens qu'on va oublier les mots pour ne regarder que les motifs. Puisque tout mot binaire de longueur 4 contient un carré, ce motif est évidemment inévitable par les nombres algébriques binaires. Par contre, si l'on considère des motifs un peu plus répétitifs comme des chevauchements, les choses sont nettement moins simples. Dans cette direction, Mahler [**42**] a démontré en 1929 que le nombre de Thue–Morse

$$\sum_{n\geq 0} \frac{t_n}{2^n},$$

(qui comme on l'a déjà vu évite les chevauchements) est transcendant.

Une conséquence de l'hypothétique normalité des nombres algébriques irrationnels est que tout motif répétitif X^α, avec $\alpha > 1$, devrait être inévitable par les nombres algébriques. On va maintenant montrer un résultat très partiel dans cette direction qui généralise celui de Mahler (voir [**8**]).

Théorème 2.5. (*Adamczewski & Rampersad, 2007*) — *Le développement binaire d'un nombre algébrique continent une infinité de puissances* $7/3$*, et donc en particulier une infinité de chevauchements.*

La démonstration du théorème 2.5 combine le théorème de transcendance des nombres bégayants (théorème 2.2) et un théorème de structure pour les mots infinis évitant les puissances $7/3$. Ce dernier résultat, du à Karhumäki et Shallit [**30**], est rappelé ci-dessous.

Théorème. (*Karhumäki & Shallit, 2004*) — *Soient* $\mathbf{a}$ *un mot infini évitant les puissances* $7/3$ *et* τ *le morphisme de Thue–Morse. Alors, il existe un mot fini* $U \in \{\epsilon, 0, 1, 00, 11\}$ *et un mot binaire infini* $\mathbf{b}$ *évitant les puissances* $7/3$ *tels que* $\mathbf{a} = U\sigma(\mathbf{b})$.

Démonstration du théorème 2.5. — On va montrer que toute suite binaire qui évite les puissances $7/3$ est bégayante.

Soient $\mathbf{a} = (a_n)_{n\geq 0}$ une suite binaire évitant les puissances $7/3$ et k un entier. En appliquant le résultat de Karhumäki et Shallit k fois au mot infini $\mathbf{a}$, on obtient la factorisation suivante :

$$\mathbf{a} = U_1\tau(U_2)\tau^2(U_3)\cdots\tau^{k-1}(U_k)\tau^k(\mathbf{b}),$$

où chaque U_i est un mot binaire de longueur au plus 2 et où $\mathbf{b}$ est un mot infini évitant les puissances 7/3. On rappelle que chaque mot binaire de longueur 4 contient au moins un carré. Il existe donc un mot A (éventuellement vide) de longueur au plus 2 et un mot B de longueur 1 ou 2 tel que $\mathbf{b}$ commence par ABB. Posons

$$V_k = U_1\tau(U_2)\tau^2(U_3)\cdots\tau^{k-1}(U_k)\tau^k(A) \tag{6}$$

et

$$W_k = \tau^k(B).$$

D'après (6), la suite $\mathbf{a}$ commence par $V_k W_k^2$. De plus, un rapide calcul donne

$$|V_k| < 2^{k+2} \text{ et } 2^k \leq |W_k| \leq 2^{k+1}.$$

Sans perte de généralité, on peut supposer que la suite $(|V_n|)_{n\geq 1}$ est strictement croissante (en effet, on peut, si nécessaire, considérer la suite strictement croissante $(V_{2n})_{n\geq 1}$). La suite $\mathbf{a}$ est donc une suite bégayante.

D'après le théorème 2.2, un nombre binaire qui évite les puissances 7/3 est soit transcendant, soit rationnel. D'autre part, les nombres rationnels ont un développement binaire ultimement périodique et ne peuvent donc éviter aucune puissance. On obtient que tout nombre algébrique binaire contient au moins une puissance 7/3. Puisque l'algébricité ne dépend pas des premiers chiffres du développement binaire, on obtient le résultat souhaité. □

Il est intéressant de noter, qu'assez paradoxalement, les mots qui évitent les puissances 7/3 sont bégayants et donc, en un certain sens, très répétitifs.

CHAPITRE 3

APPROXIMATION SIMULTANÉE D'UN NOMBRE ET DE SON CARRÉ, D'APRÈS ROY

3.1. Présentation du problème

Dans tout ce chapitre, γ désigne le nombre d'or, c'est-à-dire, $\gamma = (1 + \sqrt{5})/2$.

L'étude de l'approximation d'un nombre réel par des nombres algébriques de degré borné a débuté avec un article de Wirsing en 1960 [**60**]. Il démontra que si $n > 1$ est un entier, et si ξ désigne un nombre réel qui n'est pas un nombre algébrique de degré inférieur ou égal à n, alors il existe une infinité de nombres algébriques de degré au plus n tels que

$$|\xi - \alpha| \ll H(\alpha)^{-(n+3)/2}, \tag{7}$$

où $H(\alpha)$ désigne la hauteur naïve de α, c'est-à-dire, le maximum des valeurs absolues des coefficients du polynôme minimal de α. La constante sous-entendue par le symbole $\ll$ ne dépend ici que de n et ξ. Une célèbre conjecture, due à Wirsing, est que l'exposant $(n + 3)/2$ dans (7) peur être remplacé par $n + 1$. Jusqu'à présent, la conjecture de Wirsing n'a été démontrée que pour $n = 2$; il s'agit d'un résultat obtenu par Davenport et Schmidt en 1967 [**24**].

En 1969, ces mêmes auteurs ont considéré une question similaire, mais en se restreignant à l'approximation par des entiers algébriques de degré borné. Dans cette partie, on s'intéressera plus spécifiquement à l'approximation par des entiers algébriques cubiques, ce qui est a rapproché du cas $n = 3$ dans (7). Dans cette direction, Davenport et Schmidt ont démontré le résultat suivant [**25**].

Théorème. (*Davenport & Schmidt, 1969*) — *Soit ξ un nombre réel qui n'est ni rationnel, ni quadratique. Alors, il existe une constante c et une infinité d'entiers algébriques α de degré au plus 3 tels que*

$$|\xi - \alpha| \leq cH(\alpha)^{-\gamma^2},$$

où $H(\alpha)$ désigne la hauteur du nombre algébrique α.

Un argument de "dualité" permet de lier l'approximation d'un nombre réel par des nombres algebriques de degré borné avec l'approximation simultanée et uniforme des puissances successives de ce nombre. En particulier, l'approximation d'un nombre réel

ξ par des entiers algébriques cubiques dépend fortement de l'approximation simultanée et uniforme de ξ et ξ^2 par des nombres rationnels. Ainsi, Davenport et Schmidt [**24**] ont obtenu le théorème précédent à l'aide du résultat ci-dessous.

Théorème. (*Davenport & Schmidt, 1969*) — *Soit ξ un nombre réel qui n'est ni rationnel, ni quadratique. Alors, il exist une constante $c > 0$ telle que le système d'inégalités*

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

n'a aucune solution non nulle $(x_0, x_1, x_2) \in \mathbb{Z}^3$ pour des nombres réels X arbitrairement grands.

3.2. Les théorèmes de Roy

On s'est longtemps attendu à ce que la constante γ^2 dans le théorème de Davenport et Schmidt ne soit pas optimale et puisse être remplacée par 3. Ce n'est en fait pas le cas, comme l'a récemment démontré Roy [**54**].

Théorème. (*Roy, 2003*) — *Il existe un nombre réel ξ qui n'est ni rationnel, ni quadratique, et tel que pour tout entier algébrique α de degré au plus 3, on a*

$$|\xi - \alpha| \geq cH(\alpha)^{-\gamma^2},$$

pour une certaine constante c.

Pour obtenir ce résultat, Roy a d'abord démontré que la valeur γ est en fait optimale dans le second théorème de Davenport et Schmidt. Ce résultat est là encore plutôt surprenant puisqu'il va à l'encontre de la conjecture naturelle qui consistait à remplacer γ par 2.

Théorème 3.2. (*Roy, 2004*) — *Il existe une constante c et un nombre réel ξ, qui n'est ni rationnel, ni quadratique, tels que le système d'inégalités*

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

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

Suite aux travaux de Roy [**56**], un nombre réel satisfaisant à la condition diophantienne exceptionnelle du théorème précédent est appelé un *nombre extrémal*. Roy a démontré que l'ensemble des nombres extrémaux est dénombrable. De façon surprenante, Roy a également pu donner un exemple explicite de nombre extrémal. En effet, a et b sont deux entiers distincts strictement positifs, alors le nombre réel

$$\xi_{a,b} := [a, b, a, a, b, a, b, a, a, b, \cdots],$$

où $abaababaab\cdots$ désigne le mot de Fibonacci sur l'alphabet $\{a, b\}$, est nombre extrémal.

Evidemment, les travaux de Roy ont motivé d'autres études. Etant donné un nombre réel ξ, on définit l'exposant $\hat{\lambda}_2(\xi)$ comme le supremum des nombres réels λ tels que le systèmes d'inégalités

$$|x_0| \leq X,\ |x_0\xi - x_1| \leq X^{-1/\lambda},\ |x_0\xi^2 - x_2| \leq X^{-1/\lambda},$$

a une solution non nulle $(x_0, x_1, x_2) \in \mathbb{Z}^3$ pour tout X assez grand. Bugeaud et Laurent [**14**] ont montré comment utiliser la construction de Roy pour produire des exemples explicites de nombres réels dont l'exposant $\hat{\lambda}_2$ prend des valeurs comprises entre 2 (la valeur attendueet presque sûre) et γ (la valeur optimale).

Théorème. (*Bugeaud & Laurent, 2005*) — *Soient a et b deux entiers distincts strictement positifs. Soit $\alpha := [0, a_1, a_2, \cdots]$ un nombre réel irrationnel et $(b_n)_{n\geq 1}$ la suite sturmienne caractéristique d'angle α définie sur l'alphabet $\{a, b\}$. Soit ξ le nombre réel irrationnel et non quadratique défini par*

$$\xi := [0, b_1, b_2, \cdots].$$

Alors,

$$\hat{\lambda}_2(\xi) = \frac{\sigma + 1}{2\sigma + 1},$$

où $\sigma := \limsup_{n\to\infty} [a_n, a_{n-1}, \cdots, a_1]$.

Les définitions d'une suite sturmienne caractéristique et de l'angle d'une suite sturmienne sont rappelées dans la partie 1.5.

3.3. Approximation simultanée, fractions continues et palindromes

On va maintenant expliquer le point crucial de la démonstration du second théorème de Roy : les fractions continues peuvent être utilisées pour trouver de bonnes approximations simultanées d'un nombre et de son carré grâce à la notion de palindrome.

Un palindrome est un mot fini $W = a_1 a_2 \ldots a_n$ qui est égal à son image miroir. Cela signifie que $\overline{W} := a_n a_{n-1} \ldots a_1 = a_1 a_2 \ldots a_n = W$. En d'autres termes, le mot W est symétrique. Par exemple, les mots *elle* ou *étêté* sont des palindromes.

Il s'agit à présent d'utiliser la formule du miroir (lemme B.3 de l'annexe B). Si $p_n/q_n = [0, a_1, a_2, \ldots, a_n]$, on rappelle que :

$$\frac{q_{n-1}}{q_n} = [0, a_n, a_{n-1}, \cdots, a_1]. \tag{8}$$

Soient $\xi = [0, a_1, a_2, \cdots]$ un nombre réel et p_n/q_n le n-ième convergent de ξ. Si le mot $a_1 \cdots a_n$ est un palindrome, alors (8) implique que

$$\frac{q_{n-1}}{q_n} = [0, a_n, a_{n-1}, \cdots, a_1] = [0, a_1, \cdots, a_n] = \frac{p_n}{q_n}.$$

Dans ce cas, on obtient $p_n = q_{n-1}$. On rappelle d'autre part (voir annexe B) que

$$\left|\xi - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2} \quad \text{et} \quad \left|\xi - \frac{p_{n-1}}{q_{n-1}}\right| < \frac{1}{q_{n-1}^2}.$$

Ainsi, Puisque $0 < \xi < 1$, $a_1 = a_n$ et $q_n \leq (a_n+1)q_{n-1}$, on obtient

$$\begin{aligned}\left|\xi^2 - \frac{p_{n-1}}{q_n}\right| &\leq \left|\xi^2 - \frac{p_{n-1}}{q_{n-1}} \times \frac{p_n}{q_n}\right| \leq \left|\xi + \frac{p_{n-1}}{q_{n-1}}\right| \times \left|\xi - \frac{p_n}{q_n}\right| + \frac{1}{q_n q_{n-1}} \\ &\leq 2\left|\xi - \frac{p_n}{q_n}\right| + \frac{1}{q_n q_{n-1}} < \frac{a_1+3}{q_n^2}.\end{aligned}$$

En résumé, si le mot $a_1 a_2 \cdots a_n$ est un palindrome, alors

$$(9) \qquad |q_n\xi - p_n| < \frac{1}{q_n} \quad \text{et} \quad |q_n\xi^2 - p_{n-1}| < \frac{a_1+3}{q_n}.$$

Cela signifie que chaque fois qu'un convergent p_n/q_n est palindromique ($a_1 \cdots a_n$ est un palindrome), on obtient une excellente approximation simultanée de ξ et ξ^2 en considérant les deux nombres rationnels p_n/q_n et p_{n-1}/q_n.

Un aspect essentiel du problème que nous étudions est qu'il s'agit d'un problème d'approximation uniforme, c'est-à-dire, que pour tout X assez grand, on veut qu'un certain système d'inégalités ait une solution entière dont les coefficients sont majorés par X.

Soit $(a_n)_{n\geq 1}$ une suite d'entiers strictement positifs et supposons que le mot infini $\mathbf{a} = a_1 a_2 \cdots a_n \cdots$ commence par une infinité de palindromes. On note $(n_i)_{i\geq 1}$ la suite croissante formée par les longueurs des préfixes de $\mathbf{a}$ qui sont des palindromes. On pose alors

$$\xi := [0, a_1, a_2, \ldots].$$

Si la suite $\mathbf{n}$ est suffisamment dense pour garantir l'existence d'un nombre réel τ tel que $q_{n_{i+1}} \ll q_{n_i}^{\tau}$. Alors, les inégalités (9) assurent que, pour tout nombre réel X assez grand, le système d'équations

$$(10) \qquad |x_0| \leq X,\ |x_0\xi - x_1| \leq cX^{-1/\tau},\ |x_0\xi^2 - x_2| \leq cX^{-1/\tau},$$

a une solution non nulle $(x_0, x_1, x_2) \in \mathbb{Z}^3$. En effet, étant donné X, il existe un entier i tel que $q_{n_i} \leq X < q_{n_i+1}$, et le triplet $(q_{n_i}, p_{n_i}, p_{n_i-1})$ est une solution non nulle pour (10).

La morale de l'histoire : si un nombre réel ξ est tel que son développement en fraction continue commence par *beaucoup* de palindromes, alors ξ et ξ^2 sont *uniformément* bien approchés par des nombres rationnels de même dénominateur. Une approche possible pour étudier notre problème consiste donc à chercher un mot infini dont de nombreux préfixes (le plus possible !) sont des palindromes. On va voir que le mot de Fibonacci est un candidat idéal.

3.4. Mot de Fibanocci et démonstration d'un théorème de Roy

Soient a et b deux entiers distincts strictement positifs. On considère le mot de Fibonacci $\mathbf{f} = abaab \cdots$ sur l'alphabet $\{a, b\}$ et on pose $\xi_{a,b} := [a, b, a, a, b, \cdots]$. On se propose de démontrer que $\xi_{a,b}$ est un nombre extrémal au sens de Roy.

Pour cela, on va tout d'abord déterminer les préfixes de $\mathbf{f}$ qui sont des palindromes.

Proposition 3.4. — *Pour tout entier $i \geq 1$, le préfixe de $\mathbf{f}$ de longueur*

$$n_i := F_{i+3} - 2, \tag{11}$$

où F_i désigne le i-ème nombre de Fibonacci, est un palindrome.

Démonstration. — On rappelle tout d'abord que $\mathbf{f}$ est la limite de la suite de mots finis définis par : $W_1 = a$, $W_2 = b$ et $W_{n+1} = W_n W_{n-1}$. Une récurrence rapide permet de montrer que pour tout entier $n \geq 2$, le mot W_{2n} se termine par ba tandis que le mot W_{2n+1} se termine par ab. De plus, on a $|W_n| = F_n$.

Notons P_i le préfixe de $\mathbf{f}$ de longueur n_i. On obtient facilement par récurrence que $P_1 = a$, $P_2 = aba$, $P_3 = abaaba$ et

$$P_i = P_{i-1} ab Pi - 2, \text{ pour tout entier } i \geq 4 \text{ pair,}$$

tandis que

$$P_i = P_{i-1} ba Pi - 2, \text{ pour tout entier } i \geq 5 \text{ impair.}$$

On observe alors que

$$P_i = Pi - 2ba P_{i-1} ab P_{i-2}, \text{ pour tout entier } i \geq 4 \text{ pair,} \tag{12}$$

tandis que

$$P_i = Pi - 2ab P_{i-1} ba P_{i-2}, \text{ pour tout entier } i \geq 5 \text{ impair.} \tag{13}$$

On en déduit à nouveau par récurrence que P_i est un palindrome pour tout entier $i \geq 1$, puisque les mots P_1, P_2 et P_3 sont des palindromes. □

Démonstration du théorème 3.2. — On est maintenant prêt à terminer la démonstration du théorème de Roy. Pour cela, il suffit en effet, d'après la remarque faite avant (10) et la proposition 3.4, de démontrer qu'il existe une constante c independante de i telle que

$$q_{n_{i+1}} \leq c q_{n_i}^{\gamma}, \tag{14}$$

où $\gamma = \frac{1+\sqrt{5}}{2}$ désigne le nombre d'or.

On va procéder par récurrence. D'après (12) et (13), la théorie des continuants (lemme B.4 de l'annexe B) garantie l'existence de deux constantes strictement positives A et B telles que

$$A < \frac{q_{n_{i+1}}}{q_{n_i} q_{n_{i-1}}} < B, \tag{15}$$

pour tout entier $i \geq 2$. Sans perte de généralité on peut supposer que

$$B \geq \left\{ \frac{(Aq_{n_1})^{\gamma}}{q_{n_2}}, \frac{(Aq_{n_2})^{1/\gamma}}{q_{n_1}} \right\}. \tag{16}$$

On pose $C = A^{\gamma}/B$ et $D = B^{\gamma}/A$ et on va montrer par récurrence que

$$C q_{n_i}^{\gamma} \leq q_{n_{i+1}} \leq D q_{n_i}^{\gamma} \tag{17}$$

pour tout entier $i \geq 2$. Pour $i = 2$, cela découle de (15) et (16). Supposons que (17) soit vérifiée pour tout entier $i \geq 2$. D'après (15), on a

$$Aq_{n_i}^{\gamma}\left(q_{n_i}^{1-\gamma}q_{n_{i-1}}\right) < q_{n_{i+1}} < Bq_{n_i}^{\gamma}\left(q_{n_i}^{1-\gamma}q_{n_{i-1}}\right)$$

et comme $\gamma(\gamma-1) = 1$, il vient

$$Aq_{n_i}^{\gamma}\left(q_{n_i}q_{n_{i-1}}^{-\gamma}\right)^{1-\gamma} < q_{n_{i+1}} < Bq_{n_i}^{\gamma}\left(q_{n_i}q_{n_{i-1}}^{-\gamma}\right)^{1-\gamma}.$$

On déduit alors de (17) que

$$\left(AD^{1-\gamma}\right)q_{n_i}^{\gamma} < q_{n_{i+1}} < \left(CA^{1-\gamma}\right)q_{n_i}^{\gamma}.$$

Par définition de C et D, et comme $\gamma(\gamma-1) = 1$, cela donne

$$Cq_{n_i}^{\gamma} < q_{n_{i+1}} < Dq_{n_i}^{\gamma},$$

ce qui correspond au résultat cherché.

On a ainsi démontré que $\xi_{a,b}$ est un nombre extrémal au sens de Roy, ce qui conclut cette démonstration. □

3.5. Densité palindromique, d'après Fischler

Si $\mathbf{w} = w_1w_2\cdots w_n\cdots$ est un mot infini commençant par des palindromes arbitrairement longs, on note comme précédemment $(n_i)_{i\geq 1}$ la suite croissante formée par les longueurs des préfixes de $\mathbf{w}$ qui sont des palindromes. Par hypothèse, cette suite est infinie. On peut alors définir la *densité palindromique* d'un mot infini $\mathbf{w}$, notée $d_p(\mathbf{w})$, par

$$d_p(\mathrm{w}) := \left(\limsup_{i\to\infty}\frac{n_{i+1}}{n_i}\right)^{-1}$$

(en posant $d_p(\mathbf{w}) = 0$ si le mot $\mathbf{w}$ ne commence que par un nombre fini de palindromes). Clairement,

$$0 \leq d_p(\mathbf{w}) \leq 1.$$

De plus, si $\mathbf{w} = WWW\cdots$ est un mot périodique, alors $d_p(\mathbf{w}) = 1$ s'il existe deux palindromes (éventuellement vides) U et V tels que $W = UV$, et $d_p(\mathbf{w}) = 0$ sinon. D'autre part, on peut facilement montré qu'un mot ultimement périodique qui commence par des palindromes arbitrairement longs est en fait périodique. Ainsi, la densité palindromique d'un mot ultimement périodique est soit maximale, soit minimale. On peut alors naturellement se poser la question suivante : quelle est la plus grande densité palindromique qui puisse être atteinte par un mot non périodique ? Ce problème, motivé par les travaux de Roy sur l'approximation uniforme et simultanée d'un nombre et de son carré, a été résolu de façon complètement combinatoire par Fischler [**28**].

Théorème. (*Fischler, 2006*) — *Soit* $\mathbf{w}$ *un mot infini qui n'est pas ultimement périodique. Alors,*

$$d_p(\mathrm{w}) \leq \frac{1}{\gamma}\cdot$$

En particulier, la densité palindromique maximale, parmi les mots apériodiques, est atteinte par le mot de Fibonacci.

3.6. Transcendance et palindromes

Voici un autre résultat produit par la formule du miroir et l'idée de Roy. D'autres résultats de transcendance utilisant certains phénomènes de symétrie dans les fractions continues sont donnés dans [**5**].

Théorème 3.6. (*Adamczewski & Bugeaud, 2007*) — *Soit* $\mathbf{a} = (a_n)_{n\geq 1}$ *une suite non ultimement périodique d'entiers strictement positifs. Si* $\mathbf{a}$ *commence par des palindromes arbitrairement longs, alors le nombre réel*

$$\xi = [0; a_1, a_2, \ldots]$$

est transcendant.

Démonstration. — On cherche à démontrer que le nombre ξ est transcendant. Par hypothèse, la suite $\mathbf{a}$ n'est pas ultimement périodique, et donc, le théorème d'Euler–Lagrange implique que ξ n'est ni rationnel, ni quadratique (voir l'annexe B).

On suppose par l'absurde que α est un nombre quadratique de degré au moins 3 et on cherche une contradiction. Notons $(p_\ell/q_\ell)_{\ell\geq 1}$ la suite des convergents de ξ. Puisque la suite $\mathbf{a}$ commence par des palindromes arbitrairement longs, il existe d'après (9) une suite strictement croissante d'entiers $(n_i)_{i\geq 1}$ telle que :

$$|q_{n_i}\xi - p_{n_i}| < \frac{1}{q_{n_i}} \quad \text{et} \quad |q_{n_i}\xi^2 - p_{n_i-1}| < \frac{a_1+3}{q_{n_i}}\cdot$$

On considère alors les trois formes linéaires suivantes :

$$L_1(X_1,X_2,X_3) = \xi X_1 - X_2,\ L_2(X_1,X_2,X_3) = \xi^2 X_1 - X_3,\ \text{et}\ L_3(X_1,X_2,X_3) = X_1.$$

Ces formes linéaires sont indépendantes et à coefficients algébriques (par hypothèse). En évaluant le produit de ces formes linéaires au points entiers $(q_{n_i}, q_{n_i-1}, p_{n_i})$, on obtient

$$\prod_{1\leq j\leq 3} |L_j(q_{n_i}, p_{n_i}, p_{n_i-1})| < \frac{1}{q_{n_i}}\cdot$$

Le théorème du sous-espace (voir l'annexe A) implique donc que les points entiers $(q_{n_i}, p_{n_i}, p_{n_i-1})$, $i \geq 1$, appartiennent à un même plan vectoriel de $\mathbb{Q}^3$. Il existe donc un triplet d'entier non tous nuls (x_1, x_2, x_3) et un ensemble infini d'entiers distincts $\mathcal{N}$ tels que

$$x_1 q_{n_i} + x_2 p_{n_i} + x_3 p_{n_i-1} = 0,$$

pour tout entier i dans $\mathcal{N}$. En divisant par q_{n_i} et faisant tendre i vers l'infini selon $\mathcal{N}$, il vient :

$$x_1 + x_2\xi + x_3\xi^2 = 0.$$

Puisque les entiers x_1, x_2 et x_3 ne sont pas tous nuls, on en déduit que ξ est un nombre rationnel ou quadratique. On obtient donc la contradiction recherchée. $\square$

CHAPITRE 4

EXEMPLES EXPLICITES POUR LA CONJECTURE DE LITTLEWOOD

4.1. Ennoncé de la conjecture de Littlewood

La théorie des fractions continues ou le théorème de Dirichlet assure que pout tout nombre réel α, il existe une infinité d'entiers $q \geq 1$ tels que

$$q \cdot \|q\alpha\| < 1, \tag{18}$$

où $\| \cdot \|$ désigne la distance à l'entier le plus proche. En particulier, pour tout couple (α, β) de nombres réels, il existe une infinité d'entiers $q \geq 1$ tels que

$$q \cdot \|q\alpha\| \cdot \|q\beta\| < 1.$$

La conjecture de Littlewood à laquelle nous allons nous intéresser, suggère un résultat légèrement plus fort : pour tout couple de nombres réels (α, β), on a

$$\inf_{q \geq 1} q \cdot \|q\alpha\| \cdot \|q\beta\| = 0. \tag{19}$$

Il semble que Littlewood ait énoncé cette conjecture vers 1930 (voir [**36**]). En dépit de son apparente simplicité, ce résultat n'est toujours pas démontré...

4.2. Mise en jambes : deux remarques utiles

Première remarque. Dans la suite, on appellera **Bad** l'ensemble des nombres réls mal approchables par des nombres rationnels, c'est-à-dire,

$$\mathbf{Bad} = \left\{ \alpha \in \mathbb{R} : \inf_{q \geq 1} q \cdot \|q\alpha\| > 0 \right\}.$$

Il n'est pas difficile de montrer qu'un nombre réel appartient à l'ensemble **Bad** si, et seulement si, la suite de ses quotients partiels (dans son développement en fraction continue) est bornée.

Ainsi, il suffit qu'un des deux nombres α ou β ait des quotients partiels non bornés pour que le couple (α, β) vérifie la conjecture de Littlewood. Une conséquence importante de cette remarque est :

Proposition 1. — *La conjecture de Littlewood est vérifiée pour presque tout (au sens de la mesure de Lebesgue) couple de nombres réels.*

Ce résultat est une conséquence d'un théorème classique de Khintchine [**33**].

Théorème. (*Khintchine, 1924*) — *Soit $\Psi : \mathbb{N} \to \mathbb{R}^+$ une fonction continue telle que $x \mapsto x\Psi(x)$ est décroissante. Alors, l'ensemble*

$$\mathcal{K}(\Psi) := \{\xi \in \mathbb{R} : \|q\xi\| < \Psi(q) \text{ pour une infinité d'entiers } q\}$$

est de mesure nulle si $\sum_{q=1}^{+\infty} \Psi(q)$ est une série convergente, et $\mathcal{K}(\Psi)$ est un ensemble de mesure pleine lorsque cette série est divergente.

Démonstration de la Proposition 1. — Il suffit d'appliquer le théorème de Khintchine avec la fonction définie par $\Psi(q) = 1/(q \log q)$. $\square$

Deuxième remarque. Il est également intéressant de noter le résultat suivant :

Proposition 2. — *La conjecture de Littlewood est vérifiée par tout couple (α, β) tel que 1, α, et β soient linéairement dépendants sur $\mathbb{Q}$.*

Démonstration. — Considérons un couple de nombres réels (α, β) tel que 1, α, et β soient linéairement dépendants sur $\mathbb{Q}$. On peut supposer sans perte de généralité que α et β sont irrationnels.

Soit $q \geq 1$ un entier tel que

$$\|q\alpha\| < \frac{1}{q}\cdot$$

Puisque 1, α, et β sont linéairement dépendants sur $\mathbb{Q}$, il existe des entiers A, B et C non tous nuls, tels que

$$A\alpha + B\beta + C = 0.$$

Le fait que α et β soient supposés irrationnels assure de plus que A et B sont non nuls. Ainsi, $\|qA\alpha\| = \|qB\alpha\| < A/q$. Il vient

$$\|qAB\alpha\| < \frac{AB}{q} \quad \text{et} \quad \|qAB\beta\| < \frac{A^2}{q}.$$

Finalement, on obtient

$$Q \cdot \|Q\alpha\| \cdot \|Q\beta\| < \frac{A^5 B^3}{Q},$$

où $Q = qAB$. Ainsi, d'après (18), le couple (α, β) vérifie la conjecture de Littlewood. $\square$

4.3. Un rapide historique

Le premier résultat significatif en direction de la conjecture de Littlewood est du à Cassels et Swinnerton-Dyer [**16**]. Il concerne les couples de nombres algébriques.

Théorème (*Cassels & Swinnerton-Dyer, 1955*) — *Si α et β désignent deux nombres réels appartenant à même corps cubique, alors la conjecture de Littlewood est vérifiée par le couple (α, β).*

On peut remarquer que le cas des couples de nombres appartenant à un même corps quadratique ne pose pas de problème. Il découle de la proposiiton 2.

Un résultat bien plus récent est du à Pollington et Velani [**49**]. Il s'agit d'un résultat de nature métrique et donc complètement différent de celui de Cassels et Swinnerton-Dyer. Il permet d'aller au-delà des conséquences découlant du théorème de Khintchine. La preuve requiert des outils assez fins de la théorie métrique des nombres, comme un résultat d'équirépartition de Davenport, Erdős et LeVeque [**23**] ou certaines mesures supportées par des ensembles de Cantor introduites par Kaufman [**31**].

Théorème. (*Pollington & Velani, 2000*) — *Etant donné α dans* **Bad**, *il existe un sous-ensemble $A(\alpha) \subset$* **Bad** *de dimension de Hausdorff égale à* 1 *et tel que pour tout β appartenant à $A(\alpha)$, on ait*

$$q \cdot \|q\alpha\| \cdot \|q\beta\| \leq \frac{1}{\log q},$$

pour une infinité d'entiers q. En particulier, la conjecture de Littlewood est vérifiée par le couple (α, β).

Récemment, Einsiedler, Katok et Lindenstrauss [**26**] ont considérablement amélioré ce résultat en utilisant une approche complètement différente. Ils obtiennent le résultat suivant :

Théorème. (*Einsiedler, Katok & Lindenstrauss, 2006*) — *L'ensemble des couples (α, β) qui ne vérifient pas la conjecture de Littlewood est de dimension de Hausdorff nulle.*

En fait, ces auteurs ont démontré une partie d'une conjecture de Margulis concernant les actions ergodiques de l'espace homogène $SL_k(\mathbb{R})/SL_k(\mathbb{Z})$, pour $k \geq 3$. Il était déjà connu qu'un tel résultat aurait des implications en approximation diophantienne et en particulier sur la conjecture de Littlewood (pour cela, on utilise seulement le cas $k = 3$).

Remarque. Un point important qui mérite d'être signalé : contrairement à celle utilisée par Pollington et Velani, l'approche suivie par Einsiedler, Katok et Lindenstrauss n'est pas métrique par essence et pourrait conduire à une résolution complète du problème. Pour ceux ou celles qui veulent en savoir plus, cette dernière méthode sera développée dans le cours d'Emmanuel Breuillard.

4.4. Le problème des exemples explicites

Au vu des deux remarques de la partie 4.2, la question suivante semble assez naturelle : peut-on trouver des exemples *non triviaux* de couples (α, β) vérifiant la conjecture de Littlewood. Ici et dans la suite, un couple (α, β) est dit non trivial si :

- Les nombres α et β appartiennent tous deux à l'ensemble **Bad** ;
- Les nombres 1, α et β sont linéairement indépendants sur $\mathbb{Q}$.

Les théorèmes PV et EKL impliquent bien sûr que de tels exemples existes. En particulier, pour tout élément α dans **Bad**, il existe "beaucoup" de couples non triviaux (α, β) vérifiant la conjecture de Littlewood. Malheureusement, aucun des résultats de la partie 4.3 n'apporte un élément de réponse à la question suivante :

Question. — *Etant donné un nombre réel α dans* **Bad**, *peut-on donner un exemple explicite de couple (α, β) vérifiant non trivialement la conjecture de Littlewood ?*

Il semble que ce soit de Mathan qui ait le premier considéré cette question des exemples explicites suite à une question posée par Zannier aux Journées Arithmétiques de Lille en 2001 (voir [**43**]). On va maintenant voir comment une approche combinatoire élémentaire développée dans [**2**] permet de répondre à cette question.

Soit $\alpha := [0, a_1, a_2, \ldots]$ un nombre réel dont les quotients partiels sont bornés par un certain entier $M \geq 2$. Etant données une suite d'entiers strictement croissante $\mathbf{n} = (n_i)_{i \geq 1}$ et une suite $\mathbf{t} = (t_i)_{i \geq 1}$ à valeurs dans l'ensemble $\{M+1, M+2\}$, on va construire un nombre réel $\beta_{\mathbf{n},\mathbf{t}}$ de la façon suivante. Pour tout entier $n \geq 1$, A_n désigne le mot $a_1 a_2 \ldots a_n$ et $\overline{A_n}$ désigne l'image miroir de A_n, c'est-à-dire, $\overline{A_n} = a_n a_{n-1} \ldots a_1$. On pose alors

$$\beta_{\mathbf{n},\mathbf{t}} = [0; \overline{A_{n_1}}, t_1, \overline{A_{n_2}}, t_2, \overline{A_{n_3}}, t_3, \ldots].$$

Le but du jeu est alors de montrer que si la suite $\mathbf{n}$ croît suffisamment vite, le couple $(\alpha, \beta_{\mathbf{n},\mathbf{t}})$ vérifie non trivialement la conjecture de Littlewood. Plus précisément, on peut montrer le résultat suivant [**2**].

Théorème. (*Adamczewski & Bugeaud, 2006*) — *Conservons les notations précédentes et supposons de plus que la suite* $\mathbf{n}$ *vérifie :*

$$\liminf_{i \to +\infty} \frac{n_{i+1}}{n_i} > \frac{4 \log(M+3)}{\varepsilon \log 2} \cdot$$

Alors, les nombres réels 1, α *et* $\beta_{\mathbf{n},\mathbf{t}}$ *sont linéairement indépendants sur* $\mathbb{Q}$ *et il existe une infinité d'entiers* q *tels que*

$$q \cdot \|q\alpha\| \cdot \|q\beta_{\mathbf{n},\mathbf{t}}\| \leq \frac{1}{q^{1-\varepsilon}} \cdot$$

En particulier, le couple $(\alpha, \beta_{\mathbf{n},\mathbf{t}})$ vérifie non trivialement la conjecture de Littlewood.

Tout comme dans la partie 3, la formule du miroir va jouer un rôle essentiel dans cette démonstration.

Démonstration. — Dans cette démonstration, on va à nouveau utiliser le formalisme des continuants et les lemmes 1, 2, 3 et 4 qui sont rappelés dans l'annexe B.

On conserve les notations précédentes. On note $(p_j/q_j)_{j\geq 1}$ (resp. $(r_j/s_j)_{j\geq 1}$) la suite des convergents de α (resp. de $\beta_{\mathbf{n},\mathbf{t}}$) et on pose $m_j = n_1+n_2+\ldots+n_j+(j-1)$. D'après la formule du miroir (lemme B.3), on obtient

$$\frac{s_{m_j-1}}{s_{m_j}} = [0, a_1, \ldots, a_{n_j}, t_{j-1}, a_1, \ldots, a_{n_{j-1}}, t_{j-2}, \ldots, t_1, a_1, \ldots, a_{n_1}],$$

et donc d'après le Lemme B.2, il vient

$$\|s_{m_j}\alpha\| \leq s_{m_j}\, q_{n_j}^{-2}. \tag{20}$$

On rappelle d'autre part que la théorie des fractions continues assure que

$$s_{m_j} \cdot \|s_{m_j}\beta_{\mathbf{n},\mathbf{t}}\| < 1 \tag{21}$$

Il nous faut donc démontrer que

$$s_{m_j}\, q_{n_j}^{-2} < \frac{1}{s_{m_j}^{(1-\varepsilon)}},$$

c'est-à-dire, que

$$q_{n_j} > s_{m_j}^{(1-\varepsilon/2)}. \tag{22}$$

D'après (20) et (21), on obtiendra ce qu'on veut, c'est-à-dire,

$$s_{m_j} \cdot \|s_{m_j}\alpha\| \cdot \|s_{m_j}\beta_{\mathbf{n},\mathbf{t}}\| \leq \|s_{m_j}\alpha\| \leq s_{m_j}\, q_{n_j}^{-2} \leq \frac{1}{s_{m_j}^{1-\varepsilon}}.$$

Pour démontrer (22), on va se servir du formalisme des continuants. L'idée est très simple : si la suite $\mathbf{n}$ croît très vite alors le mot $a_1a_2\ldots a_{n_j}$ est beaucoup plus long que $t_{j-1}a_1\ldots a_{n_{j-1}}t_{j-2}\ldots t_1a_1\ldots, a_{n_1}$. Puisque les quotients partiels sont tous majorés par $M+2$, cela implique que l'entier $q_{n_j} = K(a_1, a_2, \ldots, a_{n_j})$ est très grand par rapport à

$$K_j := K(t_{j-1}, a_1, \ldots, a_{n_{j-1}}, t_{j-2}, \ldots, t_1, a_1, \ldots, a_{n_1}).$$

Puisque

$$q_{n_j}K_j \leq s_{m_j} \leq 2q_{n_j}K_j, \tag{23}$$

on obtient alors le résultat souhaité.

Voici le détail des calculs. D'après le lemme B.4, on a

$$s_{m_j} \geq 2^{(m_j-1)/2}$$

et, puisque la suite des quotients partiels de $\beta_{\mathbf{n},\mathbf{t}}$ est bornée par $M+2$, on obtient également en utilisant le lemme B.1 que

$$K_j < (M+3)^{m_{j-1}+1}.$$

Ainsi,

$$K_j < (M+3)^{m_{j-1}+1} = 2^{(m_{j-1}+1)\log(M+3)/\log 2} \leq S_{m_j}^{(m_{j-1}+1)/(m_j-1)\cdot 2\log(M+3)/\log 2}.$$

D'autre part, l'hypothèse de croissance faite sur la suite $\mathbf{n}$ assure que

$$\frac{m_{j-1}}{m_j} \leq \frac{n_{j-1}}{n_j}$$

pour j assez grand, ce qui implique ensuite que

$$K_j \leq \frac{1}{2} \cdot S_{m_j}^{\varepsilon/2}$$

pour j assez grand. L'inégalité (22) découle alors de (23).

Il ne reste plus qu'à montrer que 1, α et $\beta_{\mathbf{n},\mathbf{t}}$ sont linéairement indépendants sur $\mathbb{Q}$. On suppose par l'absurde que ce n'est pas le cas et on cherche une contradiction. Dans ce cas, il existe un triplet d'entiers non tous nuls (A, B, C) tel que

$$A\alpha + B\beta_{\mathbf{n},\mathbf{t}} + C = 0.$$

Ainsi,

$$\|s_{m_j} A\alpha\| = \|s_{m_j} B\beta_{\mathbf{n},\mathbf{t}}\| \leq |B| \cdot \|s_{m_j}\beta_{\mathbf{n},\mathbf{t}}\| \ll \frac{1}{s_{m_j}} \ll \frac{1}{q_{n_j} K_j}. \tag{24}$$

D'autre part, le lemme B.2 implique que

$$|s_{m_j}\alpha - s_{m_j-1}| \gg \frac{s_{m_j}}{q_{n_j}^2} \gg \frac{q_{n_j} K_j}{q_{n_j}^2} \gg \frac{K_j^2}{q_{n_j} K_j}.$$

Comme pour j assez grand, on a

$$|s_{m_j} A\alpha - s_{m_j-1} A| < \frac{1}{2},$$

Ainsi,

$$\|s_{m_j} A\alpha\| = |s_{m_j} A\alpha - s_{m_j-1} A| = |A| \cdot |s_{m_j}\alpha - s_{m_j-1}|$$

et on obtient finalement que

$$\|s_{m_j} A\alpha\| \gg \frac{2^{m_{j-1}}}{s_{m_j}},$$

ce qui contredit (24) et termine cette démonstration. □

En utilisant cette approche, on peut aussi montrer le résultat suivant qu'on peut par exemple appliquer aux fractions continue de Thue–Morse et de Fibonacci.

Théorème. — *Soit α un nombre réel dont le développement en fraction continue commence par des palindromes arbitrairement longs. Soit β un nombre réel image de α par une homographie rationnelle. Alors, la conjecture de Littlewood est vérifiée par le couple (α, β) et, de plus, on a*

$$\liminf_{q \to +\infty} q^2 \cdot \|q\alpha\| \cdot \|q\beta\| < +\infty.$$

Le fait que la conjecture de Littlewood est vérifiée par le couple $(\alpha, 1/\alpha)$ lorsque α vérifie l'hypothèse du théorème précédent a été observé pour la première fois par M. Queffélec au cours d'une conférence qui s'est déroulée à l'I.H.P. en juin 2004.

CHAPITRE 5

ANNEXE A : LE THÉORÈME DU SOUS-ESPACE

5.1. Les théorèmes de Roth et Ridout

Le théorème de Roth [**52**] est un résultat classique d'approximation diophantienne qui exprime le fait qu'un nombre algébrique irrationnel ne peut pas être trop bien approché par des nombres rationnels. Il a quand même valu à Roth d'obtenir la médaille Fields en 1958.

Théorème. (*Roth, 1955*) — *Soit α un nombre algébrique et ε un nombre réel strictement positif. Alors, l'inégalité*

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

ne possède qu'un nombre fini de solutions rationnelles.

Notons que d'après la théorie des fraction continues (voir l'annexe B), l'exposant 2 dans le théorème de Roth est optimal. Evidemment, on peut utiliser ce résultat pour démontrer que certains nombres sont transcendants. Par exemple, le théorème de Roth implique que le nombre

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

est transcendant, mais il s'avère insuffisant pour traiter le cas du nombre

$$\sum_{n\geq 1} \frac{1}{10^{2^n}}.$$

Le théorème de Ridout. On rappelle que si p désigne un nombre premier, on définit la valuation p-adique d'un entier $n \geq 1$, $\nu_p(n)$, comme la plus grande puissance de p qui divise n, de sorte que

$$n = \prod_{p\in\mathcal{P}} p^{\nu_p(n)}.$$

Si $n = 0$ on opte pour la convention $\nu_p(n) = +\infty$. La valeur absolue p-adique de n, notée $|n|_p$, est alors définie par
$$|n|_p = \frac{1}{p^{\nu_p(n)}}.$$
En particulier, $|n|_p \leq 1$ pour tout entier n.

Une version p-adique du théorème de Roth est connue sous le nom de théorème de Ridout [**53**]. Ce résultat dit en substance la chose suivante : si l'on fixe un ensemble fini de nombres premiers, un nombre algébrique ne peut pas être *trop bien approché* par des nombres rationnels dont les dénominateurs et/ou les numérateurs sont *trop divisibles* par ces nombres premiers. C'est très intéressant car cela permet parfois de passer sous la barre, a priori infranchissable, de l'exposant 2 du théorème de Roth.

Théorème. (*Ridout, 1957*) — *Soient α un nombre algébrique, $\mathcal{S}$ un ensemble fini de nombres premiers et ε un nombre réel strictement positif. Alors, l'inégalité*
$$\left(\prod_{\mathfrak{p}\in\mathcal{S}} |p|_{\mathfrak{p}}\ |q|_{\mathfrak{p}}\right)\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}}$$
ne possède qu'un nombre fini de solutions rationnelles.

A l'aide de ce résultat, on démontre par exemple facilement que les nombres
$$\sum_{n\geq 1} \frac{1}{10^{2^n}} \quad \text{et} \quad \sum_{n\geq 1} \frac{1}{10^{F_n}}$$
sont transcendants (ici, F_n désigne le n-ième nombre de Fibonacci). C'est intéressant car on sait par exemple que le premier de ces nombres est mal approchable par des nombres rationnels (au sens défini au chapitre 4). Il n'y a donc aucune chance de pouvoir appliquer le théorème de Roth à ce nombre.

5.2. Le théorème du sous-espace de W. M. Schmidt

On rappelle ici l'énoncé du théorème du sous espace, qui est une généralisation multidimensionnelle du théorème de Roth. Ce résultat obtenu par W.M. Schmidt en 1972 (voir [**58, 59**]) est réellement un outil très puissant. Il intervient (ou sa version p-adique rappelée plus bas) dans les deux démonstrations de transcendance (théorèmes 2.2 et 3.6) dont il est question dans ce cours.

Théorème. (*W. M. Schmidt, 1972*) — *Soient $m \geq 2$ un entier et $\varepsilon > 0$. Considérons $L_1, \dots, L_m$ des formes linéaires en les variables $X_1, \dots, X_m$, à coefficients algébriques et linéairement indépendantes sur $\overline{\mathbb{Q}}$. Alors, l'ensemble des solutions entières $\mathbf{x} = (x_1, \dots, x_m) \in \mathbb{Z}^m$ de l'inégalité*
$$|L_1(\mathbf{x}) \dots L_m(\mathbf{x})| \leq (\max\{|x_1|, \dots, |x_m|\})^{-\varepsilon}$$
est contenu dans une uninon finie de sous-espaces vectoriels propres de $\mathbb{Q}^m$.

Pour mieux appréhender ce résultat, on va montrer comment le théorème de Roth se déduit facilement du théorème du sous-espace (cela donne une petite idée de la puissance de ce résultat). On raisonne par l'absurde, en supposant que α est un nombre algébrique pour lequel il existe une infinité de nombres rationnels distincts $(p_n/q_n)_{n\geq 1}$ tels que

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^{2+\varepsilon}}$$

pour un certain $\varepsilon > 0$ fixé. Alors,

$$|q_n|\;|q_n\alpha - p_n| < q_n^{-\varepsilon}$$

et, si n est assez grand, on obtient

$$|q_n|\;|q_n\alpha - p_n| < \max\{|p_n|,|q_n|\}^{-\varepsilon}. \tag{25}$$

En effet, si $|\alpha - p_n/q_n| < 1$, on a $p_n < q_n(|\alpha|+1)$.

On pose alors $L_1(X_1, X_2) = X_1 - \alpha X_2$ et $L_2(X_1, X_2) = X_2$. Ces deux formes linéaires en deux variables sont linéairement indépendantes sur $\overline{\mathbb{Q}}$ (en fait sur $\mathbb{R}$) et à coefficients algébriques. D'après (25), le théorème du sous-espace implique que les points entiers (p_n, q_n) sont contenus dans une union finie de sous-espaces vectoriels propres de $\mathbb{Q}^2$, c'est-à-dire, dans une union finie de droites vectorielles. Le principe des tiroirs assure alors qu'il existe une infinité de ces points qui appartiennent à une même droite. Ainsi, il existe $(x, y) \neq (0, 0) \in \mathbb{Z}^2$ tel que

$$xp_n + yq_n = 0$$

pour une infinité d'entiers n. Si $x = 0$, il vient $y = 0$ ce qui est impossible. On a donc

$$\frac{p_n}{q_n} = -\frac{y}{x}$$

pour une infinité d'entiers n. On obtient une contradiciton puisque les nombres rationnels p_n/q_n sont tous distincts, ce qui prouve le théorème de Roth.

Version p-adique du théorème du sous-espace. Voici enfin une version p-adique minimaliste du théorème du sous-espace dont on se sert au chapitre 2 (c'est le principal outil de la démonstration du théorème 2.2). Des versions plus générales de ce résultat sont dues à Schlickewei (voir [**57**]).

Théorème. (*Schlickewei, 1977*) — *Soient $m \geq 2$ un entier, $\mathcal{S}$ un ensemble fini de nombres premiers et $\varepsilon > 0$. Considérons $L_1, \ldots, L_m$ des formes linéaires en les variables $X_1, \ldots, X_m$, à coefficients algébriques et linéairement indépendantes sur $\overline{\mathbb{Q}}$. Alors, l'ensemble des solutions entières $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{Z}^m$ de l'inégalité*

$$\left(\prod_{p\in\mathcal{S}}\prod_{i=1}^{m}|x_i|_p\right)|L_1(\mathbf{x})\ldots L_m(\mathbf{x})| \leq (\max\{|x_1|,\ldots,|x_m|\})^{-\varepsilon}$$

est contenu dans une uninon finie de sous-espaces vectoriels propres de $\mathbb{Q}^m$.

De même que le théorème du sous-espace implique facilement le théorème de Roth, le théorème de Ridout découle de la version p-adique du théorème du sous-espace.

CHAPITRE 6

ANNEXE B : BOITE À OUTILS “FRACTIONS CONTINUES”

On rappelle ici quelques propriétés élémentaires de la théorie des fractions continues qui sont utilisées dans ce cours. Ces résultats classiques se trouvent par exemple dans le livre de Perron [**48**]. On ne donne pas de démonstration, mais il s'agit presque toujours de récurrences assez simples (exception faite du théorème d'Euler–Lagrange). Quelques références d'ouvrages traitant de fractions continues : le livre de Perron [**48**] (très bien, mais pas facile à trouver), le livre de Khintchine [**32**] ou celui de Lang [**34**].

6.1. Notations

On rappelle que tout nombre réel rationnel admet une unique écriture en fraction continue

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}$$

où a_0 est entier positif, les a_i, $i \geq 1$, sont des entiers strictement positifs et $a_n \geq 2$. On utlisera généralement la notation abrégée $[a_0, a_1, \ldots, a_n]$. Les coefficients $a_0, a_1, \ldots, a_n$ sont appelés les *quotients partiels* de la fraction continue.

De même, tout nombre réel irrationnel ξ admet une unique écriture en fraction continue de la forme

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n + \cfrac{1}{\ddots}}}} = [a_0, a_1, \cdots, a_n, \cdots],$$

où a_0 est entier positif et les a_i, $i \geq 1$, sont des entiers strictement positifs. Ce développement est appelé le développement en fraction continue de ξ. Réciproquement, à toute suite d'entier strictements positifs $(a_n)_{n\geq 1}$ correspond un nombre réel irrationnel ξ compris strictement entre 0 et 1 tel que

$$\xi = [0, a_1, a_2, \ldots].$$

Avec ces notations, le nombre rationnel $p_n/q_n := [a_0, a_1, \ldots, a_n]$ est appelé le n-ième convergent de ξ. Les entier p_n et q_n vérifient les relations fondamentales suivantes :

$$p_{-1} = 1, p_0 = a_0, q_{-1} = 0, q_0 = 1$$

et

$$p_{k+1} = a_{k+1}p_k + p_{k-1} \quad \text{et} \quad q_{k+1} = a_{k+1}q_k + q_{k-1}$$

pour $k \geq 0$.

La suite de rationnels $(p_n/q_n)_{n\geq 0}$ converge bien vers ξ. En effet, pour tout entier $n \geq 1$, on a

$$\frac{1}{q_n(q_n + q_{n+1})} < \left|\xi - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}}.$$

6.2. Vitesse de convergence et croissance des dénominateur des convergents

Il est parfois utile d'évaluer la croissance de la suite q_n des dénominateurs des convergents d'un nombre réel. Voici un résultat peu précis, mais qui a le mérite d'être à la fois simple et général.

Lemme B.1. — *Soit $(a_n)_{n\geq 0}$ une suite d'entiers strictement positifs. Soit $n \geq 1$ un entier. Posons $p_n/q_n = [a_0, a_1, a_2, \ldots, a_n]$ et $M = \max\{a_0, \ldots, a_n\}$. Alors, on a*

$$\sqrt{2}^{(n-1)} \leq q_n \leq (M+1)^n.$$

De façon assez instinctive, on peut penser que deux nombres dont les premiers quotients partiels coincident sont assez proches. Le lemme suivant permet de quantifier cette remarque.

Lemme B.2. — *Soient $\xi = [a_0, a_1, a_2, \cdots]$ et $\eta = [b_0, b_1, b_2, \cdots]$ deux nombres réels. Soit $n \geq 1$ un entier tel que $a_j = b_j$ pour tout $j = 0, \ldots, n$. Alors, on a*

$$|\xi - \eta| \leq q_n^{-2},$$

où q_n désigne le n-ième convergent de ξ. Si on suppose de plus que les quotients partiels de ξ et de η sont majorés par M, et si $a_{n+1} \neq b_{n+1}$, alors

$$|\xi - \eta| \geq \frac{1}{(M+2)^3 q_n^2}.$$

6.3. La formule du miroir

Si la théorie des fractions continues est un outil parfaitement adapté à l'étude de l'approximation rationnel d'un nombre réel, elle n'a a priori pas grand chose à apporter aux problèmes de l'approximation simultanée de plusieurs nombres réels (par des nombres rationnels de même dénominateur). Pourtant, les chapitres 3 et 4 montrent que cette idée n'est pas tout-à-fait exacte. Bien que complètement élémentaire, le résultat suivant, joue un rôle essentiel dans les deux problèmes d'approximation simultanée abordés dans ces chapitres.

Lemme B.3. (*Formule du miroir*) — *Soient $\xi = [a_0, a_1, a_2, \cdots]$ un nombre réel et $(p_n/q_n)_{n\geq 0}$ la suite de ses convergents. Alors, pour tout entier $n \geq 1$, on a*

$$\frac{q_n}{q_{n-1}} = [a_n, a_{n-1}, \dots, a_1].$$

6.4. Les continuants

Etant donné des entiers $a_1, \dots, a_m$, on désigne par $K_m(a_1, \dots, a_m)$ le dénominateur de l'écriture réduite du nombre rationnel $[0, a_1, \dots, a_m]$. Une telle quantité est appelé un *continuant*. On dira que $K_m(a_1, \dots, a_m)$ est le continuant associé aux entiers $a_1, \dots, a_m$. Dans l'étude de problèmes diophantiens liés aux fractions continues, on est parfois conduit à évaluer la hauteur de certains nombres rationnels définis par leur développement en fraction continue, disons $p/q := [a_0, a_1, a_2, \dots, a_r]$. Cela revient donc à évaluer la quantité $K_r(a_1, a_2, \dots, a_r)$ et le formalisme des continuants s'avère souvent pratique. Il intervient à plusieurs reprises, dans les chapitres 3 et 4, mais on se contente d'utiliser le résultat élémentaire suivant.

Lemme B.4. — *Etant donnés des entiers strictements positifs $a_1, \dots, a_m$ et un entier k tel que $1 \leq k \leq m-1$, on a*

$$K_m(a_1, \dots, a_m) = K_m(a_m, \dots, a_1)$$

et

$$\begin{aligned} K_k(a_1, \dots, a_k) \cdot K_{m-k}(a_{k+1}, \dots, a_m) &\leq K_m(a_1, \dots, a_m) \\ &\leq 2\, K_k(a_1, \dots, a_k) \cdot K_{m-k}(a_{k+1}, \dots, a_m). \end{aligned}$$

6.5. Le théorème d'Euler–Lagrange

Comme on l'a déjà mentionné, les développements en fraction continue finis correspondent aux nombres rationnels. Le théorème d'Euler–Lagrange caractérise le développement en fraction continue des nombres quadratiques irrationnels.

Théorème. (*Euler–Lagrange*) — *Un nombre réel a un développement en fraction continue ultimement périodique si, et seulement si, il s'agit d'un nombre quadratique irrationnel.*

Ce résultat montre, en un certain sens, la supériorité du développement en fraction continue sur le développement décimal ou binaire, puisqu'on peut facilement décrire le développement en fraction continue d'un nombre algébrique irrationnel quadratique comme

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{\ddots}}}}$$

alors qu'on ne sait pratiquement rien sur son développement dans une base entière (cf. chapitre 2). Evidemment, pour additionner ou multiplier des nombres, c'est une autre histoire...

BIBLIOGRAPHIE

[1] B. Adamczewski *&* Y. Bugeaud, On the complexity of algebraic numbers II. Continued fractions, *Acta Math.* **195** (2005) 1–20.

[2] B. Adamczewski, *&* Y. Bugeaud, On the Littlewood conjecture in simultaneous Diophantine approximation, *J. London Math. Soc.* **73** (2006) 355–366.

[3] B. Adamczewski *&* Y. Bugeaud, On the complexity of algebraic numbers I. Expansions in integer bases, *Annals of Math.* **165** (2007), 547–565.

[4] B. Adamczewski *&* Y. Bugeaud, On the Maillet-Baker continued fractions, *J. Reine Angew. Math.* **606** (2007), 105–121.

[5] B. Adamczewski *&* Y. Bugeaud, Palindromic continued fractions, *Ann. Inst. Fourier* **57** (2007), 1557–1574.

[6] B. Adamczewski, Y. Bugeaud *&* F. Luca, Sur la complexité des nombres algébriques, *C. R. Acad. Sci. Paris* **339** (2004), 11–14.

[7] B. Adamczewski *&* J. Cassaigne, Diophantine properties of real numbers generated by finite automata, *Compositio Math.* **142** (2006), 1351-1372.

[8] B. Adamczewski *&* N. Rampersad, On patterns occurring in binary algebraic numbers, *Proc. Amer. Math. Soc.*, in press.

[9] S. I. Adian, *The Burnside problem and identities in groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete **95**, Springer Verlag, 1979.

[10] J.-P. Allouche *&* J. Shallit, *The ubiquitous Prouhet-Thue-Morse sequence*, in Sequences and Their Applications (Singapore, 1998), Springer Ser. Discrete Math. Theor. Comput. Sci., Springer-Verlag, London, 1999, pp. 1–16.

[11] J.-P. Allouche *&* J. Shallit, *Automatic Sequences : Theory, Applications, Generalizations*, Cambridge University Press, Cambridge, 2003.

[12] É. Borel, Les probabilités dénombrables et leurs applications arithmétiques, *Rend. Circ. Math. Palermo* **27** (1909), 247–271.

[13] É. Borel, Sur les chiffres décimaux de $\sqrt{2}$ et divers problèmes de probabilités en chaîne, *C. R. Acad. Sci. Paris* **230** (1950), 591–593.

[14] Y. Bugeaud & M. Laurent, Exponents of Diophantine and Sturmian continued fractions, *Ann. Inst. Fourier* **55** (2005) 773–804.

[15] C. S. Calude, *Information and Randomness. An algorithmic perspective*, Texts in Theoretical Computer Science, an EATCS series, Springer-Verlag, 2002.

[16] J. W. S. Cassels & H. P. F. Swinnerton-Dyer, On the product of three homogeneous linear forms and the indefinite ternary quadratic forms, *Philos. Trans. Roy. Soc. London. Ser. A* **248** (1955) 73–96.

[17] D. G. Champernowne, The construction of decimals normal in the scale of ten, *J. London Math. Soc.* **8** (1933), 254–260.

[18] G. Christol, Ensembles presque périodiques k-reconnaissables, *Theoret. Comput. Sci.* **9** (1979), 141–145.

[19] G. Christol, T. Kamae, M. Mendès France & G. Rauzy, Suites algébriques, automates et substitutions, *Bull. Soc. Math. France* **108** (1980), 401–419.

[20] A. Cobham, *On the Hartmanis-Stearns problem for a class of tag machines*, Conference Record of 1968 Ninth Annual Symposium on Switching and Automata Theory, Schenectady, New York (1968), 51–60.

[21] A. Cobham, Uniform tag sequences, *Math. Systems Theory* **6** (1972), 164–192.

[22] A. H. Copeland & P. Erdös, Note on Normal Numbers, *Bull. Amer. Math. Soc.* **52** (1946), 857–860.

[23] H. Davenport, P. Erdős & W. J. LeVeque, On Weyl's criterion for uniform distribution, *Michigan Math. J.* **10** (1963) 311–314.

[24] H. Davenport & W. M. Schmidt, A theorem on linear forms, *Acta Arith.* **14** (1967-1968) 209–223.

[25] H. Davenport & W. M. Schmidt, Approximation to real numbers by algebraic integers, *Acta Arith.* **15** (1968-1969) 393–416.

[26] M. Einsiedler, A. Katok & E. Lindenstrauss, Invariant measures and the set of exceptions to the Littlewood conjecture, *Annals of Math.* **164** (2006) 513–560.

[27] S. Ferenczi & C. Mauduit, Transcendence of numbers with a low complexity expansion, *J. Number Theory* **67** (1997), 146–161.

[28] S. Fischler, Palindromic prefixes and episturmian words, *J. Combin. Theory, Ser. A* **113** (2006) 1281–1304.

[29] J. Hartmanis *&* R. E. Stearns, On the computational complexity of algorithms, *Trans. Amer. Math. Soc.* **117** (1965), 285–306.

[30] J. Karhumäki *&* J. Shallit, Polynomial versus exponential growth in repetition-free binary words, *J. Combin. Theory, Ser. A* **105** (2004), 335–347.

[31] R. Kaufman, Continued fractions and Fourier transforms, *Mathematika* **27** (1980) 262–267.

[32] A. Ya. Khintchine, *Continued fractions*, The University of Chicago Press (1964).

[33] A. Ya. Khintchine, Einige Sätze über Kettenbrüche mit Anwendungen auf die Theorie der diophantischen Approximationen, *Math Ann.* **92** (1924) 115–125.

[34] S. Lang, *Introduction to Diophantine Approximations*, Springer Verlag (1995).

[35] M. Li, P. Vitnayi, *Kolmogorov Complexity and its Applications*, Springer Verlag, New York, 1997.

[36] J. E. Littlewood, *Some problems in real and complex analysis*, D. C. Heath and Co. Raytheon Education Co., Lexington, Mass., 1968.

[37] M. Lothaire, *Combinatorics on words*, Cambridge University Press, 1997.

[38] M. Lothaire, *Algebraic Combinatorics on Words*, Vol. 90 of *Encyclopedia of Mathematics and Its Applications*, Cambridge University Press, 2002.

[39] M. Lothaire, *Applied combinatorics on words.*, Vol. 105 of *Encyclopedia of Mathematics and Its Applications*, Cambridge University Press, 2005.

[40] J. H. Loxton *&* A. J. van der Poorten, Arithmetic properties of the solutions of a class of functional equations, *J. Reine Angew. Math.* **330** (1982), 159–172.

[41] J. H. Loxton *&* A. J. van der Poorten, Arithmetic properties of automata : regular sequences, *J. Reine Angew. Math.* **392** (1988), 57–69.

[42] K. Mahler, Arithmetische Eigenschaften der Lösungen einer Klasse von Funktionalgleichungen, *Math. Annalen* **101** (1929), 342–366. Corrigendum **103** (1930), 532.

[43] B. de Mathan, Conjecture de Littlewood et récurrences linéaires, *J. Théor. Nombres Bordeaux* **13** (2003), 249–266.

[44] M. Morse, Recurrent geodesics on a surface of negative curvature, *Trans. Amer. Math. Soc.* **22** (1921) 84–100.

[45] M. Morse *&* G. A. Hedlund, Symbolic dynamics, *Amer. J. Math.* **60** (1938), 815–866.

[46] M. Morse *&* G. A. Hedlund, Symbolic dynamics II, *Amer. J. Math.* **62** (1940), 1–42.

[47] M. Morse *&* G. A. Hedlund, Unending chess, symbolic dynamics and a problem in semigroups, *Duke Math. J.* **11**, (1944). 1–7.

[48] O. Perron, *Die Lehre von den Kettenbrüchen*, Teubner, Leibzig, 1929.

[49] A. D. Pollington *&* S. L. Velani, On a problem in simultaneous Diophantine approximation : Littlewood's conjecture, *Acta Math.* **185** (2000) 287–306.

[50] N. Pytheas Fogg, *Substitutions in Dynamics, Arithmetics and Combinatorics*, Lecture Notes in Mathematics **1794**, Springer, 2002.

[51] M. Queffélec, Transcendance des fractions continues de Thue-Morse, *J. Number Theory* **73** (1998) 201–211.

[52] K. F. Roth, Rational approximations to algebraic numbers, *Mathematika* **2** (1955), 1–20 ; corrigendum 168.

[53] D. Ridout, Rational approximations to algebraic numbers, Mathematika **4** (1957), 125–131.

[54] D. Roy, Approximation simultanée d'un nombre et de son carré, *C. R. Math. Acad. Sci. Paris* **336** (2003) 1–6.

[55] D. Roy, Approximation to real numbers by cubic algebraic integers, II, *Annals of Math.* **158** (2003) 1081–1087.

[56] D. Roy, Approximation to real numbers by cubic algebraic integers, I, *Proc. London Math. Soc.* **88** (2004) 42–62.

[57] H. P. Schlickewei, The $\mathfrak{p}$-adic Thue-Siegel-Roth-Schmidt theorem, *Arch. Math.* **29** (1977), 267–270.

[58] W. M. Schmidt, Norm form equations, *Annals of Math.* **96** (1972), 526–551.

[59] W. M. Schmidt, *Diophantine approximation*, Lecture Notes in Mathematics **785**, Springer, 1980.

[60] E. Wirsing, Approximation mit algebraischen Zahlen beschränkten Grades, *J. Reine Angew. Math.* **206** (1960) 67–77.

[61] A. Thue, Über die gegenseitige Lage gleicher Teile gewisser Zeichenreihen, *Norske vid. Selsk. Skr. Mat. Nat. Kl.* **1** (1912) 1–67 ; reprinted in *Selected Mathematical Papers of Axel Thue*, T. Nagell, ed., Universitetsforlaget, Oslo, 1977, pp. 413–478.

[62] A. M. Turing, On computable numbers, with an application to the Entscheidungsproblem, *Proc. London Math. Soc.* **42** (1937), 230–265.

[63] M. Waldschmidt, Words and Transcendence, to appear in a volume to be published by Cambridge University Press, `http ://www.institut.math.jussieu.fr/ miw/index2.html`.