Laurent Duval

Approximations diophantiennes

M. Georges RHIN

UNIVERSITÉ DE METZ

DEA de MATHÉMATIQUES APPLIQUÉES

ANNÉE 1995 – 1996

Mémoire sur un article de

Marshall W. BUCK et David P. ROBBINS

The continued fraction expansion of an algebraic power series satisfying a quartic equation

Journal of Number Theory 50, 335-344 (1995)

1. Table des matières

2. Notations

À cause des limitations du traitement de texte utilisé, les lettres N, Z, Q, R et C désigneront les ensembles usuels. Ces lettres pourront parfois avoir une autre signification, sans qu'une confusion soit possible. De même, nous utiliserons la lettre F pour désigner une partie finie de Z. La lettre *P* comme ensemble des indices d'une somme ou d'un produit désignera l'ensemble des nombres premiers.

La notation [*a*, *b*], où *a* et *b* sont des entiers désignera l'ensemble $\{a, a + 1, ..., b\}$.

3. Introduction

Deux ensembles qui possèdent une même structure algébrique, sans être isomorphes, présentent, en dehors de la structure sous-jacente, certaines analogies, ainsi que des différences sensibles. L'on peut citer pour l'exemple l'ensemble Z des entiers relatifs, et l'ensemble C[X] des polynômes à une indéterminée, à coefficients dans C.

Munis de leur structure d'anneau usuelle, Z et C[X] forment alors chacun un anneau commutatif, principal et intègre, et une fois définies les notions de divisibilité et d'éléments inversibles, on peut y définir les notions de PGCD et PPCM, de primalité, qui permettent d'établir, par exemple, la relation de Bachet-Bézout dans ces deux ensembles. Les polynômes premiers (polynômes unitaires irréductibles) jouent alors, dans une certaine mesure, un rôle analogue à celui des nombres premiers de Z, grâce auxquels on peut effectuer une décomposition "unique" d'un entier quelconque en facteurs premiers ; ce même processus de décomposition se retrouve dans C[X] : alors que tout entier relatif non nul *n* admet la décomposition unique (à l'ordre près des facteurs)

$$n = \varepsilon \prod p_i^{n_i} \ ,$$

les p_i étant des entiers premiers, les n_i des entiers positifs tous nuls à part un nombre fini, et ε€∈ €{-1, 1}, tout polynôme non nul *P(X)* ∈ €C[X] peut s'écrire

$$P(X) = \varepsilon \prod P_i^{n_i}(X) \, ,$$

avec pour P_i des polynômes unitaires premiers, n_i des entiers tous nuls sauf un nombre fini d'entre eux, et ε€∈ €C*. Le facteur de normalisation ε est choisi selon le cas dans {-1, 1} ou C*, qui représentent les éléments inversibles de Z et C[X], respectivement U(Z) et U(C[X]).

Trouver, pour un couple donné (A, B) d'entiers ou de polynômes, la relation de Bachet-Bézout revient en fait à résoudre l'équation diophantienne $\mathrm{uA} + \mathrm{vB}$ dans l'anneau considéré, ce que l'on sait faire, de même que dans Z, grâce à un algorithme basé sur une succession de divisions euclidiennes et de soustractions (opération appelée *anthyphérèse* par Marc Guinot dans [GUI]). La relation de Bachet-Bézout pour les polynômes (ou relation de Bézout) possède la même interprétation en termes de primalité que dans le cas des entiers, avec "unicité" du couple (u, v) si l'on impose des conditions supplémentaires, respectivement sur le degré et la valeur absolue de u et de v. Cette similitude permet d'esquisser les lien privilégiés qui existent entre la notion de degré d'un polynôme et celle de valeur absolue, liens que l'on perçoit aussi dans le cas des éléments inversibles de l'anneau (éléments de degré 0 vs. entiers de valeur absolue 1).

Cependant, la résolution de telles équations permet également d'obtenir certaines différences significatives entre les deux anneaux précités. Une telle divergence apparaît en particulier dans un problème célèbre et ancien, la "dernière" conjecture de Fermat, qui semble avoir été démontré récemment dans le cas des entiers par le mathématicien anglais Andrew Wiles. Le même problème, posé dans l'anneau de polynômes C[X], admet la même réponse, mais de façon beaucoup plus immédiate et, semble-t-il, difficilement applicable aux entiers (une démonstration est donnée en 9.1). L'analogie entre les deux anneaux n'est donc pas parfaite, mais il est cependant possible de tenter sa poursuite. Ceci peut être réalisé en utilisant dans chacun des outils, des développements ou extensions semblables. Ainsi, les résultats obtenus dans un ensemble peuvent parfois, sous certaines conditions, être transposés à l'autre.

Dans le cas de la résolution d'équations diophantiennes, non homogènes contrairement à la relation de Bézout ou à l'équation étudiée par Fermat, il est souvent nécessaire de sortir du cadre des entiers (ou polynômes), pour rechercher des solutions rationnelles (ou fractions rationnelles), voire expliciter des solutions plus générales. Dans un anneau de polynômes, il semble naturel de prolonger les fractions rationnelles en séries, et la découverte d'une solution de cette forme peut permettre, dans certains cas particuliers, d'obtenir par substitution des classes de solutions d'équations diophantiennes, au sens classique dans le corps des réels. De plus, nous verrons qu'il est possible de développer une théorie des approximations diophantiennes sur les corps de séries, en particulier quant à l'analogue du développement en fractions continues pour les éléments algébriques des corps de séries. Dans ce cas particulier, nous verrons que l'on peut obtenir "de meilleurs résultats" sur les approximations d'éléments algébriques de degré 3 que dans le cas des réels.

Dans les articles étudiés, il s'agit principalement d'anneaux de polynômes sur des corps finis et de leurs extensions. Les résultats seront exposés dans le cadre plus général des anneaux de polynômes sur un corps commutatif quelconque, et précisés dans le cas des anneaux sur un corps fini.

4. Anneaux de polynômes et extensions

Dans ce chapitre, K désignera toujours un corps commutatif (qui correspond – en général – au terme anglo-saxon *“field”*). L’hypothèse de commutativité n’est utile que pour les corps infinis, de caractéristique nulle, puisque l’on dispose des résultats suivants dans le cas d’un corps K fini de caractéristique p comportant q éléments :

- p est un nombre premier
- il existe un entier n tel que $q = p^n$
- il existe, à un isomorphisme près, un unique corps de q éléments que l’on appelle K_q
- le corps K_q est commutatif (théorème de Wedderburn).

Ces corps finis sont aussi appelés "corps de Galois". Dans la suite, dès qu'il sera fait mention d'un corps F_q, on appelera *p* sa caractéristique.

Sur le corps K, on construit l'anneau K[X] des polynômes à une indéterminée, à coefficients dans K, qui est un anneau commutatif. Dans le cas de $K_q[X]$, la formule du binôme prend une expression particulièrement simple pour certaines valeurs de l'exposant ; en effet, comme C_p^i est divisible par *p* pour *p* premier et $i \in [1, n-1]$, on a, pour deux polynômes quelconques *A* et *B* de K[X],

$$(A+B)^p = A^p + B^p \text{ (1)},$$

ainsi que la formule généralisée suivante, pour tout entier *n*

$$(A+B)^{p^n} = A^{p^n} + B^{p^n} \text{ (2)}.$$

En conséquence, comme l'application $x \to x^p$ préserve aussi la multiplication, c'est un automorphisme du corps F_q et un morphisme de l'anneau $F_q[X]$. Si l'on applique le résultat de ce développement à un polynôme *A* dans le corps $F_q[X]$, on obtient la formule suivante :

$$\{A(X)\}^{p^n} = A(X^{p^n}),$$

valable pour un quelconque entier *n*.

L'anneau K[X] est intègre, cela découle de la propriété selon laquelle si un anneau A est intègre, alors A[X] l'est aussi ; ici, l'anneau K est un corps, il est donc intègre par définition. Par analogie avec l'anneau des entiers, on veut munir K[X] d'une structure euclidienne, ce que l'on peut faire si l'on trouve au moins un stathme euclidien. Un stathme euclidien sur un anneau A est une application φ qui vérifie les axiomes suivants :

- $\varphi : A \setminus \{0\} \to N$
- soient *x* et *y* deux éléments non nuls de l'anneau *A*, tels que *x*|*y*, alors $\varphi(x) \leq \varphi(y)$
- pour tous *x* et *y* éléments de l'anneau *A*, avec $y \neq 0$, il existe au moins un couple $(q,\ r) \in A^2$ tel que $x = y.q + r$ et $r = 0$ ou $\varphi(r) \leq \varphi(y)$.

Dans Z, le stathme euclidien usuel est la valeur absolue, qui fournit une notion de distance. Un équivalent dans les anneaux de polynômes semble être la notion de degré. Celle-ci s'impose en premier lieu puisqu'elle correspond à l'algorithme naturel de division euclidienne. Les deux stathmes présentent naturellement des dissemblances, en particulier par le fait que la valeur absolue identifie un entier au signe près (c'est-à-dire à un facteur normatif près qui est un élément inversible de Z), et ce n'est plus le cas en général dans K[X] : deux polynômes unitaires de même degré ne sont généralement pas égaux. L'analogie structurelle reste forte cependant, si l'on considère la notion de distance p-adique. L'intervention des nombres p-adique n'est pas fortuite ici, puisqu'ils interviennent dans le lemme de Hensel, qui permet de montrer l'unicité de certaines solutions d'équations algébriques (cf. 9.3).

Ces propriétés conduisent à considérer dans l'anneau $K_q[X]$ une vraie notion de valeur absolue, afin d'accroître la symétrie entre les deux anneaux, en posant

$$|P(X)| = |P| = p^{d(P)} \text{ pour la valeur absolue du polynôme } P$$

et de retrouver entre autres, pour les polynômes, la formule classique sur les entiers

$$|x.y| = |x|.|y|,$$

par le fait que K_q étant un anneau commutatif, pour deux éléments quelconques P et Q de $K_q[X]$, on a l'égalité suivante

$$d(P.Q) = d(P) + d(Q).$$

Cette nouvelle formulation permet d'obtenir une vraie valeur absolue sur $K_q[X]$.

Muni du stathme approprié, l'anneau K[X] est euclidien, ce qui implique qu'il est principal, ainsi que factoriel. Les polynômes irréductibles forment alors dans K[X] une architecture analogue à celle des nombres premiers dans Z. Dans le cas particulier où K = C, ces polynômes irréductibles sont les polynômes de degré 1.

On construit naturellement sur un tel anneau (intègre) un corps de fractions, K(X), qui permet d'introduire la notion d'anneau intégralement clos, ce qu'est un anneau factoriel. Le problème posé devient alors celui de la résolution d'équations dont les inconnues et les coefficients sont des polynômes de K[X], c'est-à-dire l'équivalent des équations diophantiennes dans Z.

La résolution de ces équations passe par l'extension du corps de fractions, qui ne suffit pas à les résoudre toutes. Un prolongement naturel des polynômes et des fractions rationnelles sont les séries, et l'on peut obtenir, à l'instar des développements en séries entières pour des équations différentielles, des solutions d'équations polynomiales, par substitution.

Pour résoudre de telles équations, on peut choisir parmi deux types d'écriture de séries :

$$S(X) = \sum_{n=a}^{+\infty} a_n X^n \text{ , en série formelle, ou}$$

$$S(X) = \sum_{n=-\infty}^{b} b_n X^n \text{ , en série de Laurent formelle,}$$

avec a et b deux entiers relatifs. On notera que le fait de permettre le choix de l'indice du premier terme (a ou b) dans Z modifie peu de choses par rapport l'habitude de débuter la sommation à l'indice 0. On augmente ainsi la généralité du propos. On peut éventuellement s'y ramener, par ajout et produit de *S*(X) par un polynôme ou l'inverse d'un polynôme, ce que l'on peut faire sur le corps K(X). Par contre, ce n'est plus le cas si l'on prend les coefficients des équations dans un anneau, par exemple ; la distinction est alors essentiellement la même qu'entre nombres et entiers algébriques. C'est encore un problème mal resolu que celui du lien entre l'existence de solutions entières ou rationnelles d'une équation diophantienne en général.

L'ensemble des séries formelles, K((X)), et l'ensemble des séries de Laurent formelles, K((X^{-1})), forment chacun un corps commutatif, pour les opérations classiques d'addition et de multiplication. Dans le cas d'un corps fini K_q, pour les deux corps de séries, on retrouve la formule du binôme simplifiée pour les polynômes, dans le cas où l'exposant est une puissance de la caractéristique *p* :

$$\left(S_1 + S_2\right)^{p^n} = S_1^{\ p^n} + S_2^{\ p^n} \quad (3),$$

et

$$\left\{S(X)\right\}^{p^n} = S(X^{p^n}) \quad (4).$$

De même que pour les polynômes, $x \to x^p$ est un morphisme des corps ou espaces vectoriels K((X)) et K((X^{-1})). Cette propriété est utilisée dans [BR-95].

Il existe une stricte équivalence entre les deux corps de séries, pour ce qui est de l'algébricité de leurs éléments. En effet, une série est dite algébrique sur K(X) lorsqu'elle est solution d'une équation polynomiale à coefficients dans K(X).

Considérons alors une série formelle algébrique S(X). Alors il existe un ensemble fini *F* et un nombre fini de polynômes p_n tels que

$$\sum_{n \in F} p_n(t) S^n(t) = 0.$$

On effectue le changement de variable $f = \frac{1}{t}$, et l'on pose $N = \sup_{n \in F} (d(p_n)) < +\infty$. On obtient alors l'équation suivante

$$\sum_{n \in F} f^N p_n\left(\frac{1}{f}\right) S^n\left(\frac{1}{f}\right) = 0 \quad (5).$$

Donc, en posant

$$p'_n(f) = f^N p_n\left(\frac{1}{f}\right)$$

et

$$S'(f) = S(\frac{1}{f}),$$

l'équation (5) devient

$$\sum_{n \in F} p'_n(f) S'^n(f) = 0,$$

chaque p'_n étant un polynôme en *f*. Donc la série formelle *S* est algébrique si et seulement si sa série de Laurent formelle associée *S'* l'est aussi.

Exemple : la série $S(X) = \sum_0^{+\infty} X^{p^n}$, où *p* est un nombre premier, est algébrique sur le corps $K_q(X)$, dès que $q = p^n$, car

$$S(X) = X + S(X^p) = X + \{S(X)\}^p.$$

Il en va de même par la série de Laurent formelle associée.

Chacune des notations présente ses avantages : la formulation en série formelle est généralement utilisée pour le développement propre d'une série, celle en série de Laurent formelle pour des développements en fractions continues, et nous utiliserons principalement cette dernière (cf. 5), pour une explication de ce choix). Dans la suite, le terme de "série" pourra être employé par ellipse pour "série de Laurent formelle".

Si l'on étudie la série de Laurent formelle *S* suivante,

$$S(X) = \sum_{-\infty}^{n} a_i X^i \text{, avec } a_n \neq 0,$$

on utilisera les définitions et les notations suivantes :

- le degré de la série *S* est : $d(f) = n$, cette définition restant cohérente avec la notion usuelle de degré d'un polynôme ou d'une fraction rationnelle
- $|S| = p^n$ représente la valeur absolue ou le module de la série *S*
- $|0| = 0$, par prolongement de la convention $d(0) = -\infty$
- $[S] = \sum_0^n a_i X^i$ correspond à la "partie entière" de *S*, c'est-à-dire le polynôme de K[X] le plus proche de *S*
- $\|S\| = |S - [S]|$, la norme de *S* représente la mesure de l'approximation de *S* par le polynôme $[S]$.

L'anneau $K_q[X]$ est discret dans le corps $K_q(X)$, qui est dense dans le corps $K_q((X^{-1}))$. Ce dernier est complet pour cette valeur absolue. Le corps des séries de Laurent formelles, muni de la valeur absolue non-archimédienne, est un corps topologique : une suite S_n de séries tend vers 0 si et seulement si $d(S_n) \xrightarrow[n\to+\infty]{} -\infty$.

5. Analogie de structures

La base naturelle $1, X, X^2, ..., X^n, ...$ des anneaux de polynômes présente des analogies avec les différentes bases numérales d'entiers, de même que la base

$$..., X^{-n}, ..., X^{-2}, X^{-1}, 1, X, X^2, ..., X^n$$

correspond au développement selon une base B d'un réel quelconque.

Produits et sommes de polynômes sont "proches" des opérations classiques sur les entiers, puisqu'en particulier la multiplication usuelle réalise de façon déguisée un produit de Cauchy, à ceci près qu'il n'y a pas de phénomène de retenue pour les polynômes ou les séries. Pour cette raison, il n'est pas toujours possible, par substitution de la variable, d'obtenir des résultats sur les réels à partir de résultats sur les séries. Dans certains cas, lorsqu'il n'y a pas propagation de retenue, la substitution est effectivement possible (cf. [PS-92]), et il semble alors plus pratique d'utiliser la notation en série de Laurent formelle, puisqu'il suffit de remplacer l'inconnue X par la base B désirée pour obtenir le B-développement un nombre réel, ou son développement en fractions continues, comme nous le verrons dans la suite.

De façon plus générale, on pourrait se poser pour les séries des questions analogues à celles qui concernent la normalité du développement propre d'un réel dans une base donnée, c'est-à-dire la régularité statistique de ses décimales. Le même problème peut être posé concernant la régularité statistique des coefficients de la série ou de ses quotients partiels.

6. Fractions continues

K désignant toujours un corps commutatif, du fait des structures d'anneaux analogues de K[X] et de Z, la plupart des résultats élémentaires des développements en fractions continues se retrouvent dans le corps $K((X^{-1}))$, ce qui ne signifie cependant pas qu'ils soient toujours identiques, nous en verrons quelques cas particuliers, qui semblent apparaître en partie à cause de la valeur absolue choisie.

Soit la série $S(X) = \sum_{-\infty}^{d} a_n X^n$. Il est possible de calculer son développement en fractions continues de façon progressive, en utilisant l'algorithme classique pour les réels, consistant à extraire la partie entière de $S(X)$ puis à inverser le résidu, etc., ce qui permet d'obtenir le développement suivant : en posant

$$S_0 = S,\ s_0 = [S_0],\ S_0 = s_0 + 1/S_1,\ s_1 = [S_1],\ S_1 = s_1 + 1/S_2,\ s_2 = [S_2],\ ...,$$

le développement de $S(X)$ devient

$$S(X) = s_0 + \cfrac{1}{s_1 + \cfrac{1}{s_2 + \cfrac{1}{s_3 + \dots}}}.$$

Les s_i sont des polynômes non constants pour i > 0, appelés quotients partiels, et $d(s_0)$ = max $(d, 0)$. Les S_i sont des séries, appelées quotients complets. La suite des s_i construits de cette façon est unique.

L'inverse de la série $S(X) = \sum_{-\infty}^{s} a_n X^n$, avec $a_s \neq 0$, est la série $T(X) = \sum_{-\infty}^{t} b_n X^n$, que l'on calcule de la façon suivante :

$$s + t = 0,$$
$$b_t = \frac{1}{a_s},$$
$$b_{t-1} = -\frac{1}{a_s}\left(a_{s-1} b_t\right),$$

et, pour tout $i \in N$,

$$b_{t-i} = -\frac{1}{a_s}\left(\sum_{k=1}^{i} a_{s-k} b_{t+k-1}\right).$$

Il s'agit de la méthode utilisée par Buck, Robbins et Mills dans [MR-86] et [BR-95], mais l'on peut préférer la méthode axiomatique suivante, proposée par Baum et Sweet, qui insistent sur la notion de qualité de l'approximation. Nous suivrons ici [BS-76] pour son exposé.

Étant donnée une série $S(X) = \sum_{-\infty}^{s} a_n X^n$, on définit une suite p_n/q_n de meilleures approximations de S par :

- $q_0 = 1$
- les polynômes q_n sont de degrés strictement croissants
- $|q_{n+1} S - p_{n+1}| < |q_n S - p_n| < 1$
- $|q_n S - p_n| \leq |q\ S - p|$, pour tout polynôme q vérifiant $d(q_n) \leq d(q) < d(q_{n+1})$.

Cette formulation correspond à un théorème de Lagrange dans le cas réel, et reste cohérente avec l'algorithme pratique de calcul des réduites, si l'on précise que chaque nouveau couple (p_n, q_n) calculé est obtenu de façon unique à un facteur de normalisation (appartenant à K) près. Il n'est pas besoin de prendre cette précaution dans K_2. Ainsi, les réduites sont-elles "bien définies".

Il est possible de développer ces calculs avec des notations plus maniables, comme la représentation du développement sous forme matricielle (matrices 2x2). Ainsi, si l'on s'assure que l'on a utilisé au cours des démonstrations uniquement les propriétés structurelles identiques dans Z et dans K(X), les résultats se transposent sans difficultés, mais restent alors élémentaires, car certaines divergences par rapport au cas réel apparaissent rapidement. Par exemple, dans R, un théorème affirme que si a est irrationnel,

$$\left|a.q_n - p_n\right| < \frac{1}{\left|q_{n+1}\right|},$$

alors qu'il y a égalité dans le cas des séries. De même, il suffit d'avoir

$$\left|S.q - p\ \right| < \frac{1}{|q|},$$

pour que p/q soit une réduite de S, alors que le théorème classique de Legendre ajoute un facteur ½, sans lequel p/q est soit une réduite, soit une réduite secondaire

Le théorème de Borel-Hurwitz, lui, n'a pas d'équivalent direct, du fait de la valeur absolue non-archimédienne choisie, pour laquelle la borne $\frac{1}{\sqrt{5}}$ n'a vraiment de sens, puisque comprise entre ½ et ¼.

Le théorème de Lagrange sur la périodicité des quotients partiels des nombres algébriques d'ordre 2 possède un équivalent direct dans les corps de séries, ainsi que le théorème de Liouville. Par contre, la majoration de ce dernier ne peut être améliorée en général, si bien que le théorème de Thue-Siegel-Roth ne s'applique pas aux séries formelles.

De plus, sauf résultats très récents, on ne connait pas de nombre algèbrique d'ordre 3 ou supèrieur à quotients partiels non bornés, alors qu'un tel résultat a été établi par Baum et Sweet, donnant dans [BS-76] le premier exemple de série formelle d'ordre 3 à quotients partiels non bornés (dans $K_2((X^{-1}))$).

Enfin, des travaux sont actuellement en cours pour mettre en défaut – dans les corps de séries – un théorème de W. Schmidt sur l'approximation simultanée de réels algébriques.

On voit ainsi que s'il existe des analogies très importantes entre R et $K((X^{-1}))$ en général, les deux ensembles restent suffisamment distincts pour qu'on ne puisse pas transposer directement les résultats de l'un à l'autre, à moins de disposer de meilleures passerelles que celles dont on dispose déjà.

7. Etude sommaire de l'article et tentative de conclusion

Le développement de la solution de l'équation

$$S^4 + S^2 - x.S + 1 = 0,$$

donnée dans le corps $K_3((X^{-1}))$, fournit une très bonne approximation, puisque la séquence Ω_n comporte asymptotiquement plus de $2{,}4^n$ termes, et donc fournit environ la moitié de quotients partiels.

Si l'on appelle $d(\Omega)$ le degré maximal des polynômes de la séquence Ω_n, on voit aisément que $d(\Omega_n) \geq 3.d(\Omega_{n-2})$, et comme $d(\Omega_n) = 3$, les quotients partiels ne sont pas bornés. Il n'est donc pas possible d'engendrer cette suite avec un automate fini.

Je n'ai pas réussi à obtenir d'amélioration notable de la démonstration, pas plus que de meilleure représentation de la solution de l'équation dans $K_{13}((X^{-1}))$.

Il semble qu'historiquement parlant, l'invention des nombres p-adiques par Kurt Hensel soit issue d'une méthode de Weierstrass de développement en séries de fonctions algébriques. Dans ce contexte, les nombres p-adiques, qui sont parfois interprétés comme une complétion de Q, à un titre différent de la complétion que forme R, ont peut-être un rôle important à jouer dans le domaine, autrement que par le seul lemme de Hensel.

Il semble, pour reprendre les termes de Mills et Robbins dans [MR-86], que les résultats ne font qu'égratigner la surface d'un vaste ensemble de problèmes de résolution d'équations algébriques, mais aussi qu'ils révèlent en même temps un grand nombre de méthodes et outils utilisables. Le chapitre suivant tente d'en proposer quelques uns.

8. Prolongements possibles

8.1 Une autre approche des séries formelles

Le calcul des développements de solutions d'équations diophantiennes fait parfois appel à la théorie des graphes, par l'utilisation de procédures d'obtention de suites d'éléments, qu'il s'agisse de développement propre ou en fractions continues. Cette théorie a permis d'obtenir des résultats importants (cf. 9.4), comme celui cité dans [CKMR-80], et la question se pose de savoir si des résultats analogues peuvent être obtenus dans le cas des quotients partiels. Si les graphes ont fait leur preuves dans le cas réel (cf. [RAN-73]), leur mise en œuvre semble plus délicate dans le maniement de polynômes plutôt que d'entiers.

Pourtant, il est possible de rapprocher fortement les notions de graphes et de séries, en utilisant une autre définition de ces dernières, moins naturelle que la définition classique, mais plus proche du raisonnement par automates. Celle-ci se base sur les travaux de Marc-Paul Schützenberger, et continués en particulier par Reutenauer et Berstel (cf. [RB]). Sans entrer dans les détails, on introduit souvent la théorie des langages et des automates par les structures de monoïdes et de demi-anneaux. On considère un ensemble *A* fini non vide, appelé alphabet, et dont les éléments sont des lettres, ou symboles, sur lequel on construit un monoïde libre *A**, composé de mots, qui sont des assemblages finis de lettres, pour l'opération de concaténation, qui consiste à accoler deux mots (les principales opérations sont définies dans [RB] et [ROD]). *A** contient tous les mots possibles que l'on peut former avec les lettres de *A*, et la théorie des automates s'articule principalement autour de sous-parties de A^*, appelées langages, et surtout ceux d'entre eux qui vérifient certaines "bonnes propriétés".

Selon Reutenauer et Berstel, une série formelle S est une application

$$A^* \to K,$$

où K est un demi-anneau. On bâtit ensuite une structure de demi-anneau autour de l'ensemble des séries formelles, en définissant des notions de somme et de produit. Si l'on appelle support d'une série formelle S le langage formé des mots de A^* dont l'image par S n'est pas l'élément nul du demi-anneau K, soit

$$Supp(S) = \left\{ m \in A^*, S(m) \neq 0 \right\},$$

les polynômes sont définis comme les séries formelles de support fini. Le degré d'un polynôme est alors la longueur maximale des mots de son support, et par convention $-\infty$ s'il est nul.

Dans le cas particulier où l'alphabet A est réduit à un singleton $\{X\}$, l'on retrouve les notions usuelles de polynômes, ainsi que de séries formelles (cf.[RB]).

En fait, cette nouvelle définition "pose" en premier lieu les séries formelles, dont les polynômes ne sont plus qu'un cas particulier, un sous-ensemble, si bien que l'on n'a plus cette construction successive, qui passe par les polynômes, les fractions rationnelles puis les séries. Plus encore, cette approche escamote la notion même de fraction rationnelle, qui forment seulement une sous-classe des séries formelles, dont on ne les distingue plus particulièrement.

Cette définition semble de mise en œuvre plus complexe que la définition classique, mais pas uniquement du fait des notations ; elle conduit en effet à utiliser le même formalisme pour l'objet (les séries) et pour l'outil (les automates), d'où peuvent survenir des confusions d'écriture.

Cependant, elle possède l'avantage d'une plus grande généralité, surtout si l'on souhaite appliquer la théorie à un plus grand nombre de variables, ou à des problèmes d'approximations simultanées. De plus, cette homogénéité entre l'outil et l'objet est susceptible d'induire une plus grande interaction entre les méthodes et les résultats, à l'image de la notion de dualité dans les espaces vectoriels, afin si possible de mieux synthétiser le développement des séries algébriques en faction continue.

Mais outre cette approche de séries, il est possible d'étendre le champ d'application des développements limités comme dans le cas des réels, en cherchant des approximations simultanées, voire en utilisant des développements impropres de séries, développements féconds semble-t-il dans certains calculs de transcendance, en particulier pour celui de $\zeta(3)$, dont la transcendance été démontrée par ce biais par Roger Apéry en 1978. Van der Poorten et Shallit font appel à de tels développements dans [PS].

Enfin, il pourrait être intéressant de développer dans le corps des fractions rationneles une théorie analogue à celle du prolongement p-adique des rationnels.

8.2 Une autre approche des automates

L'approche automatique des séries formelles peut tirer profit de notions de la théorie des langages et des automates plus complexes que les automates finis déterministes, en considérant par exemple ceux qui sont non-déterministes ou infinis, les automates à pile, à mémoire, etc.

Cependant, la seule théorie des automates finis appliquée à la résolution d'équations possède suffisamment de complexité en elle-même, puisqu'il faut trouver le bon automate, celui-ci qui décrira correctement la série formelle que l'on veut obtenir.

Il peut cependant être utile de poursuivre la recherche d'un outil automatique, qui soit plus "satisfaisant". Selon des résultats relativement récents, il se pourrait que la suite des quotients partiels d'une série algébrique dans $K_p(X)$ (qui est p-automatique, cf. 9.4) ne soit pas forcément p-automatique, mais possède une structure plus complexe (d'après des échos du Séminaire Lotharingien de Combinatoire).

En tout état de cause, comme l'on sait (cf. [BS-76]) qu'il existe des séries algébriques, de degré supérieur ou égal à trois, dont la suite des quotients partiels n'est pas bornée, la notion d'automate fini montre ses limites, et l'on peut envisager de trouver des procédures automatiques qui caractérisent exactement les développements en fractions continues de séries algébriques, comme les q-automates caractérisent les séries algébriques sur le corps $K_q(X)$ (cf. 9.4).

8.3 Limitation des résultats obtenus

La plupart des articles consultés sur les développements en fractions continues de séries formelles relativisent les résultats obtenus, en souligant le fait que nombre d'entre eux sont des résultats très partiels, de par la spécificité des équations résolues, ainsi celle des solutions, explicitées dans certains corps finis seulement. En particulier, on remarque que les théorèmes et conjectures concernent surtout K_2, qui possède la structure la plus simple, ainsi que K_3 et K_{13}, plus quelques exemples dans K_p, *p* premier (cf. MR-86), c'est-à-dire des corps dont les lois additive et multiplicative sont plus simples, puisqu'il s'agit de celles du corps Z/pZ, avec *p* premier. Et, comme le soulignent Buck et Robbins dans [BR-95], certaines démonstrations semblent dépendre de coïncidences troublantes qui ne dévoilent pas les raisons sous-jacentes profondes. Par exemple, l'apparente symétrie du développement de la solution dans $K_3((X^{-1}))$ de l'équation

$$S^4 + S^2 - x.S + 1 = 0,$$

est en fait trompeuse, puisqu'elle disparaît en partie "à l'infini". Découvrir puis exploiter une telle symétrie peut se révéler beaucoup difficile pour des solutions ou des équations moins singulières. C'est le cas en particulier de la conjecture formulée par Buck et Robbins pour la solution de cette même équation dans $K_{13}((X^{-1}))$.

La recherche d'autres résultats, dans d'autres corps finis, de cardinal premier mais aussi non premier, semble donc être un axe naturel de travail, même s'il semble plus difficile, du fait des problèmes de représentation de ces corps, et du choix de la représentation adéquate pour le calcul des coefficients d'une série.

Mais l'on peut aussi rechercher des résultats analogues dans les corps de caractéristique nulle, comme Q ou C. Même si C présente l'aspect singulier d'avoir uniquement des éléments premiers de degré 1, il semble offrir des analogies plus immédiate avec le cas des entiers, ce que semble attester (selon d'autres auteurs) certains travaux d'Alexandre Grothendieck (schéma de Grothendieck) ou plus récemment d'Arakelov, visant à établir une similarité plus importante entre C et l'ensemble des nombres premiers. Il est même possible de travailler avec un corps non commutatif, voire même, si l'on suit la définition d'une série donnée dans [RB], avec des anneaux ou des demi-anneaux.

8.4 Autres stathmes, autres normes...

Il est possible que certaines divergences entre les deux anneaux euclidiens proviennent du stathme euclidien utilisé. Une de leur principale différence est le fait que le degré ne permet d'identifier de façon unique un polynôme unitaire, ce que permet la valeur absolue.

De plus, la valeur absolue définie pour les séries de Laurent formelles est une distance ultramétrique. En effet, du fait de l'inégalité

$$d(P+Q) \leq Max(d(P), d(Q)),$$

valable dès que l'anneau A est commutatif, deux séries quelconques *f* et *g* vérifient

$$|f+g| \leq Max(|f|, |g|).$$

Or ceci influe dès que l'on veut établir les inégalités de meilleure approximation, par exemple ; à un même degré d'approximation, une distance ultramétrique semble plus "précise" qu'une distance qui peut atteindre la majoration de l'inégalité triangulaire, comme le fait la valeur absolue.

Une voie pourrait alors consister en le développement d'une théorie des fractions continues sur les entiers munis d'une norme analogue à celle du degré d'un polynôme, un "degré de primalité" ; de même que, pour un polynôme *P(X)* admettant la décomposition (sur un ensemble générateur quelconque)

$$P(X) = \varepsilon \prod P_i^{n_i}(X),$$

on a

$$d(P) = \sum n_i ,$$

on poserait, pour un entier *n* non nul quelconque,

$$d(n) = \sum n_i ,$$

avec

$$n = \varepsilon \prod p_i^{n_i} .$$

On peut alors prolonger les conventions usuelles en posant $d(0) = -\infty$. Dans cette acception, le degré de 1 est 0, celui des entiers premiers est 1. Cette définition se prolonge sans difficulté aux rationnels, à la manière des fractions rationnelles :

$$\frac{75}{26} = \frac{5^3}{2^1 \times 13^1}, \text{ d'où } d(\frac{75}{26}) = 3 - (1+1) = 1.$$

Si l'on définit ensuite sur N une valeur absolue associée, de même que pour les séries, on pourrait calculer le développement correspondant en fractions continues d'un réel, en suivant l'algorithme permettant de déterminer les meilleures approximations de ce réel. Ses quotients partiels devraient être de degré supérieur à un, donc devraient être des entiers différents de 0, 1 ou -1, si l'on veut considérer des développements impropres.

Il convient cependant de noter que cette définition présente de prime abord certaines difficultés de calcul effectif. En effet, si l'on se ramène au cas classique, il n'existe qu'un nombre fini d'entiers inférieurs à un entier N donné. De même, pour un entier q donné, il n'existe qu'un nombre fini de polynômes de K_q de degré inférieur à un entier D donné (en fait, il existe $(D+1)^q$ tels polynômes). Ce n'est plus le cas avec cette nouvelle valeur absolue, puisqu'il existe un nombre dénombrable d'entiers composés de D nombres premiers. On retrouve cette fois-ci le même problème dans C[X], puisqu'il existe une infinité (non dénombrable) de polynômes premiers.

Mais dans ce cas, la difficulté peut être contournée, en utilisant le procédé de calcul de développement en fractions continues par extractions de partie entière et divisions successive, sans se préoccuper des calculs de meilleures approximations.

Enfin, en conservant la définition des quotients partiels par meilleures approximations, il est possible d'utiliser d'autres normes pour les séries formelles, tenant par exemple mieux compte du fait que les coefficients appartiennent à un corps, fini ou non. On peut se limiter éventuellement à certaines sous-parties des corps de séries, comme celles dont la suite des coefficients sont dans l^2, si l'on s'intéresse au cas où le corps K est R. On peut rappeler que l'utilisation de différents types de normes est un outil important des approximations simultanées dans le cas réel.

8.5 Prolongements divers

Ce chapitre est le lieu pour quelques remarques assez vagues et isolées, avec l'espoir qu'elles pourraient être, après plus amples réflexions, mieux reliées au sujet.

- Dans le but de relier les propriétés des quotients partiels aux coefficients de la série, on peut se demander ce qui se passe quand on inverse les deux notions : une suite de quotients partiels d'une série algébrique se transforme-t-elle en série algébrique, et réciproquement ? Le passage d'un champ à l'autre pourrait permettre d'apdapter au mieux des besoins l'outil automatique, par un phénomène de point fixe d'une substitution d'une série à une autre, pour reprendre le langage de la théorie des automates.

- Tout laisse à penser que le développement propre et le développement en fractions continues ne sont pas les seuls possibles pour un réel ou une série. Il est donc envisageable de mener des investigations analogues pour ceux-ci.

- Comme suggéré dans [CKMR-80], les automates quantifiant une forme de régularité d'une suite, on peut envisager de mesurer la régularité statistique (au sens des nombres "normaux") de la suite des coefficients du développement propre de la série, ainsi que celle de la suite des quotients partiels.

- Dans la continuité des problèmes de changement de base, il pourrait être intéressant d'observer le comportement de séries algébriques sur un corps de fractions donné dans d'autres corps de fractions, afin de déterminer les conditions sous lesquelles ces suites peuvent perdre leur algébricité. Cette étude pourrait mettre en lumière les "transitions" qui régissent le changement de corps de base.

- Enfin, l'utilisation par Van der Poorten et Shallit d'idées de pliages successifs semble intéressante, ne serait-ce que par le formalisme différent qu'elle suggère.

9. Annexes

9.1 La conjecture de Fermat dans C[X]

Il s'agit de montrer que l'équation

$$P^n + Q^n = R^n$$

n'a pas de solution en un triplé non trivial de polynômes de C[X], dès que $n > 2$.

Lemme :
si trois polynômes *A*, *B* et *C* de C[X], premiers entre eux, vérifient

$$A(X) + B(X) = C(X) \quad (6),$$

alors

$$\max\{d(A), d(B), d(C)\} \leq z(ABC) - 1,$$

où *z(P)* dénote le nombre de zéros distincts du polynôme *P*.

Preuve :
on suppose que *A*, *B* et *C* vérifient la relation (6). On écrit ensuite le développement des polynômes

$$A(X) = A_0 \prod_1^a (X - a_i)^{\alpha_i} \ ,$$
$$B(X) = B_0 \prod_1^b (X - b_i)^{\beta_i} \ ,$$
$$C(X) = C_0 \prod_1^c (X - c_i)^{\gamma_i} \ .$$

Soit *W* le wronskien de *B* et *C*, considérés comme fonctions,

$$W = \begin{vmatrix} B & C \\ B' & C' \end{vmatrix}.$$

On en déduit une première inéqualité

$$d(W) \leq d(B) + d(C) - 1.$$

De plus

$$\prod_1^b (X - b_i)^{\beta_i - 1} \prod_1^c (X - c_i)^{\gamma_i - 1} \text{ divise } W(X),$$

et comme

$$W = \begin{vmatrix} B & A+B \\ B' & A'+B' \end{vmatrix} = \begin{vmatrix} B & A \\ B' & A' \end{vmatrix},$$

on peut affirmer que le polynôme

$$\prod_1^a (X - a_i)^{\alpha_i - 1} \prod_1^b (X - b_i)^{\beta_i - 1} \prod_1^c (X - c_i)^{\gamma_i - 1} \text{ divise } W(X),$$

et que par conséquent

$$d(B) + d(C) \geq d(W) \geq d(A) - a + d(B) - b + d(C) - c \ ,$$

d'où

$$d(A) \leq a + b + c - 1 \leq z(ABC) - 1.$$

Cette inégalité restant valable pour *B* et *C* (par permutation), on en déduit

$$\max\{d(A), d(B), d(C)\} \leq z(ABC) - 1.$$

On applique ce résultat à l'équation de Fermat, avec des polynômes P, Q et R tels que $PGCD(P, Q, R) = 1$, ce que l'on peut supposer puisque l'équation est homogène. Alors, d'après 7,

$$\max\left\{d(P^n), d(Q^n), d(R^n)\right\} \leq z((PQR)^n) - 1,$$

soit

$$n \max\left\{d(P), d(Q), d(R)\right\} \leq d(P) + d(Q) + d(R) - 1,$$

ce qui est impossible dès que n > 2.

9.2 Élements sur les distances p-adiques

Soit p un nombre premier, et n un entier. On note

$$ord_p(n) = \max\left\{i \in N, p^i | n\right\}$$

que l'on peut rapprocher de

$$ord_a(P) = \max\left\{i \in N, (X-a)^i | P(X)\right\},$$

l'ordre de la racine complexe a de $P(X)$. Si l'on définit

$$|n|_p = p^{-ord_p(n)},$$

on a, d'après la formule de Legendre

$$\log|n| + \sum_{p \in P} \log|n|_p = \log|n| - \sum_{p \in P} ord_p(n). \log(p) = 0,$$

qui correspond à

$$\deg(P) - \sum_{a \in C} ord_a(P) = 0.$$

Les valeurs absolues p-adiques $|\,.\,|_p$ sur N sont ultramétriques :

$$|a+b|_p \leq \max(|a|_p, |b|_p).$$

Il en va de même pour $ord_a(\,.\,)$, donc aussi pour $|\,.\,|$, la norme associée aux séries de Laurent formelles. Cette analogie justifie la recherche de liens plus forts entre l'ensemble P des nombres premiers et celui des nombres complexes.

9.3 Le lemme de Hensel

Les nombres p-adiques interviennent naturellement dans les problèmes de résolution d'équations diophatiennes, par l'intermédiaire du lemme de Hensel (qui est aussi le fondateur de la théorie moderne des corps), dont se servent plusieurs auteurs afin de prouver l'unicité de solution de certaines équations, comme en particulier, MM. Baum et Sweet pour l'équation

$$S^3 + x^{-1}.S + 1 = 0\,,$$

qui possède une unique solution dans $K_2((X^{-1}))$.

Une formulation de ce lemme est la suivante :

soit P un polynôme à coefficients entiers et p un nombre premier. S'il existe un entier $a \in \left]0, p\right[$ tel que $P(a) \equiv 0 \bmod (p)$ et $P'(a)$ est non nul modulo p, alors il existe un unique entier *p-adique b* tel que *P(b) = 0* et *b = a* modulo *p*.

On décrit parfois ce résultat comme la "méthode de Newton pour les nombres p-adiques".

9.4 Quelques résultats sur la transcendance et les automates finis

Nous utiliserons principalement ici le formalisme des séries entières, dans le corps K((X)), avec K corps commutatif.

Les premiers résultats dans le domaine des automates semblent le fait de Cobham (cf. 10.2, Table des matières), ainsi que de Christol, Kamae, Mendès-France et Rauzy, et les études de régularité de mots, de suites celui de Thüe. Ils consistent à rechercher une certaine régularité (selon un protocole à définir) des coefficients des séries formelles algébriques, du fait de l'existence de régularité dans des cas déjà connus.

En particulier, on sait qu'une série formelle $\sum_{d}^{+\infty} a_n X^n$ est algébrique de degré 1 si et seulement s'il existe un entier non nul *p* et un *p*-uplet $(b_1, b_2, \ldots, b_p)$ d'éléments de K tels que, pour tout entier *n* à partir d'un certain rang, on ait

$$a_n = b_1 a_{n-1} + b_2 a_{n-2} + \ldots + b_p a_{n-p}\,,$$

résultat que l'on obtient facilement en résolvant l'équation

$$B(X).S(X) = A(X)\,.$$

Ces résultats peuvent se prolonger en introduisant la notion d'automate fini. Les définitions données par certains auteurs différent parfois légèrement (il en existe à lecture directe ou indirecte), mais l'on peut trouver des équivalences entre ces différentes définitions. Nous nous reporterons ici la définition donnée dans [CKMR-80].

On peut interpréter un k-automate (k > 1) comme une machine permettant de générer une suite d'éléments, calculés récursivement en fonction de l'indice de l'élément, décomposé sur la base k. Chaque élément calculé est ainsi pris en compte pour le calcul des suivants, et ce procédé fournit une "mesure" d'un certain caractère non-aléatoire de la suite (à relier éventuellement à des processus markoviens). Si l'on peut bien sûr calculer des suites k-périodiques ad-hoc, il est plus difficile de prouver qu'une suite donnée (par la résolution d'une équation algébrique par exemple) est k-reconnaissable ou non, c'est-à-dire s'il existe un k-automate capable de la générer. Cet outil impose que les éléments de la suite soient en nombre fini, si bien que cet outil s'applique bien au développement de réels, dans une base quelconque, ou de séries à coefficients dans un corps fini, mais non à une suite quelconque de quotients partiels, qui peuvent ne plus être bornés dès que la série est de degré supérieur à 3.

Quand la série est algébrique d'ordre 1 (ou rationnelle) ou d'ordre 2, on sait que la suite de ses quotients partiels est soit finie, soit périodique, si bien que la question de l'automaticité est résolue. Et de façon plus générale, tous les exemples de suites de quotients partiels donnés dans [BS-76] ont été prouvés automatiques (cf. [ALL-88]).

Le principal théorème liant algébricité et automates est le suivant, démontré sur la base de résultats de Cobham dans [CKMR-80] :

soit $S(X) = \sum_{n=0}^{+\infty} a_n X^n$ une série formelle à coefficients dans K_q. Les deux propositions suivantes sont équivalentes :

i) *S(X)* est algébrique sur $K_q(X)$
ii) la suite $\left(a_n\right)_{n\in N}$ est q-automatique.

Il existe d'autres résultats intéressants si l'on s'intéresse aux séries à coefficients sur des corps finis ; on sait que l'ensemble $K_A((X))$ des séries algébriques sur K(X) possède une structure d'espace vectoriel, et forme même un anneau, quand on le munit du produit de Cauchy de séries.

Se pose alors la question de la stabilité de cet ensemble vis-à-vis d'autres opérations, en particulier pour le produit de Hadamard, ou usuel, de séries, c'est-à-dire, étant données deux séries formelles algébriques sur K(X), $\sum_{n=0}^{+\infty} a_n X^n$ et $\sum_{n=0}^{+\infty} b_n X^n$, la série-produit $\sum_{n=0}^{+\infty} a_n b_n X^n$ est-elle toujours algébrique ?

Ce résultat est infirmé par exemple si K = Q, comme le montre Harry Furstenberg dans [FUR], grâce à la série $\sum_{n=0}^{+\infty} \binom{2n}{n} X^n = (1-4x)^{-\frac{1}{2}}$, algébrique sur Q(X), alors que la série $\sum_{n=0}^{+\infty} \binom{2n}{n}^2 X^n$ ne l'est pas.

Par contre, Furstenberg montre que le résultat mentionné plus haut est toujours vrai si le corps K est fini.

10. Bibliographie

10.1 Bibliographie consultée

[ALL-88] Jean-Paul ALLOUCHE
Sur le développement en fraction continue de certaines séries formelles
Comptes rendus de l'Académie des Sciences de Paris 307, série I, 631-633 (1988)

[BR-95] Marshall W. BUCK et David P. ROBBINS
The continued fraction expansion of an algebraic power series satisfying a quartic equation
Journal of Number Theory 50, 335-344 (1995)

[BS-76] Leonard E. BAUM et Melvin M. SWEET
Continued fractions of algebraic power series in characteristic 2
Annals of Mathematics 103, 593-610 (1976)

[BS-77] Leonard E. BAUM et Melvin M. SWEET
Badly approximable power series in characteristic 2
Annals of Mathematics 105, 573-580 (1977)

[CKMR-80] G. CHRISTOL, T. KAMAE, M. MENDES-FRANCE et G. RAUZY
Suites algébriques, automates et substitutions
Bulletin de la Société Mathématique de France 108, 401-419 (1980)

[FUR] H. FURSTENBERG
Algebraic functions over finite fields
Journal of Algebra 7, 271-277 (1967)

[GUI] Marc GUINOT
Arithmétique pour amateurs (tome 1)
IREM, ALÉAS ÉDITEUR (1992)

[MR-86] W. H. MILLS et David P. ROBBINS
Continued fractions for certain algebraic power series
Journal of Number Theory 23, 388-404 (1986)

[PS-92] Alfred J. VAN DER POORTEN et J. SHALLIT
Folded continued fractions
Journal of Number Theory 40, 237-250 (1992)

[RAN-73] George N. RANEY
On continued fractions and finite automata
Mathematische Annalen 206, 265-283 (1973)

[RB] Ch. REUTENAUER et J. BERSTEL
Les séries rationnelles et leurs langages
Coll. Études et recherches en informatique, Masson (1984)

[ROD] François RODRIGUEZ
Théorie des langages et des automates
Cours polycopié de l'ENSEEIHT

10.2 Bibliographie complémentaire

J. V. ARMITAGE
The Thüe-Siegel-Roth theorem in caracteristic *p*
Journal of Algebra 9, 183-189 (1968)

V.M. BEYNON
A formal account of some elementary continued fractions algorithms
Journal of algorithms 4, 221-240 (1983)

A. COBHAM
Uniform tag sequances
Math. Systems Theory 6, 164-192 (1972)

N. CHOMSKY, M.-P. SCHÜTZENBERGER
The algebraic theory of context-free langages
Computer Programming and Formal Systems (1963)

P. HUMMEL
Continued fractions and matrices
Tohuku Mathematical Journal 46 (1940)

M. MENDÈS-FRANCE
Quelques problèmes relatifs à la théorie des fractions continues limitées
Séminaire de théorie des nombres, Bordeaux, 4 bis, 01-09 (1971-72)

M. MENDÈS-FRANCE
Sur les fractions continues limitées
Acta Arithmetica 23, 207-215 (1973)

A. J. Van der POORTEN
Continued fractions of formal power series
Advances in number theory, Proc. of the 3rd conf. of the CNTA, 453-466 (1991)

G. RAUZY
Une généralisation du développement en fractions continues
Séminaire de théorie des nombres, Paris (1976)