Updated: 09/11/2017

Linear recurrence sequences, exponential polynomials and Diophantine approximation

Michel Waldschmidt

Institut de Mathématiques de Jussieu — Paris VI
http://webusers.imj-prg.fr/~michel.waldschmidt/

Abstract

In the first part :

Linear recurrence sequences : an introduction

we gave a number of examples and we stated some properties of linear recurrence sequences.

Here we give more information on this topic and we include new results, arising from a joint work with Claude Levesque, involving families of Diophantine equations, with explicit examples related to some units of L. Bernstein and H. Hasse.

Linear recurrence sequences : definitions

A *linear recurrence sequence* is a sequence of numbers $\mathbf{u} = (u_0, u_1, u_2, \dots)$ for which there exist a positive integer d together with numbers $a_1, \dots, a_d$ with $a_d \neq 0$ such that, for $n \geq 0$,

$$(\star) \qquad u_{n+d} = a_1 u_{n+d-1} + \cdots + a_d u_n.$$

Here, a *number* means an element of a field $\mathbb{K}$ of zero characteristic.
Given $\underline{a} = (a_1, \dots, a_d) \in \mathbb{K}^d$, the set $E_{\underline{a}}$ of linear recurrence sequences $\mathbf{u} = (u_n)_{n\geq 0}$ satisfying $(\star)$ is a $\mathbb{K}$–vector subspace of dimension d of the space $\mathbb{K}^{\mathbb{N}}$ of all sequences .
The characteristic (or companion) polynomial of the linear recurrence is

$$f(X) = X^d - a_1 X^{d-1} - \cdots - a_d.$$

Linear recurrence sequences : examples

- Constant sequence : $u_n = u_0$.
Linear recurrence sequence of order 1 : $u_{n+1} = u_n$.
Characteristic polynomial : $f(X) = X - 1$.
Generating series :

$$\sum_{n\geq 0} X^n = \frac{1}{1-X}.$$

- Geometric progression : $u_n = u_0\gamma^n$.
Linear recurrence sequence of order 1 : $u_n = \gamma u_{n-1}$.
Characteristic polynomial $f(X) = X - \gamma$.
Generating series :

$$\sum_{n\geq 0} u_0\gamma^n X^n = \frac{u_0}{1-\gamma X}.$$

Linear recurrence sequences : examples

- $u_n = n$. This is a linear recurrence sequence of order 2 :

$$n+2 = 2(n+1) - n.$$

Characteristic polynomial

$$f(X) = X^2 - 2X + 1 = (X-1)^2.$$

Generating series

$$\sum_{n\geq 0} nX^n = \frac{1}{1-2X+X^2}\cdot$$

Power of matrices :

$$\begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix}^n = \begin{pmatrix} -n+1 & n \\ -n & n+1 \end{pmatrix}\cdot$$

Linear recurrence sequences : examples

- $u_n = f(n)$, where f is polynomial of degree d. This is a linear recurrence sequence of order $d+1$.

Proof. The sequences

$$(f(n))_{n\geq 0}, \quad (f(n+1))_{n\geq 0}, \quad \cdots, \quad (f(n+k))_{n\geq 0}$$

are $\mathbb{K}$–linearly independent in $\mathbb{K}^{\mathbb{N}}$ for $k = d-1$ and linearly dependent for $k = d$.

A basis of the space of polynomials of degree d is given by the $d+1$ polynomials

$$f(X),\ f(X+1),\ \dots,\ f(X+d).$$

`Question` : *which is the characteristic polynomial ?*

Linear sequences which are ultimately recurrent

The sequence

$$(1, 0, 0, \dots)$$

is not a linear recurrence sequence.

The condition

$$u_{n+1} = u_n$$

is satisfied only for $n \geq 1$.

The relation

$$u_{n+2} = u_{n+1} + 0u_n$$

with $d = 2$, $a_d = 0$ does not fulfill the requirement $a_d \neq 0$.

Order of a linear recurrence sequence

If $\mathbf{u} = (u_n)_{n\geq 0}$ satisfies the linear recurrence, the characteristic polynomial of which is f, then, for any monic polynomial $g \in \mathbb{K}[X]$ with $g(0) \neq 0$, this sequence $\mathbf{u}$ also satisfies the linear recurrence, the characteristic polynomial of which is fg.
`Example` : for $g(X) = X - \gamma$ with $\gamma \neq 0$, from

$$(\star) \qquad u_{n+d} - a_1 u_{n+d-1} - \cdots - a_d u_n = 0$$

we deduce

$$\begin{aligned} &u_{n+d+1} - a_1 u_{n+d} - \cdots - a_d u_{n+1} \\ &\qquad -\gamma(u_{n+d} - a_1 u_{n+d-1} - \cdots - a_d u_n) = 0. \end{aligned}$$

The *order* of a linear recurrence sequence is the smallest d such that $(\star)$ holds for all $n \geq 0$.

Generating series of a linear recurrence sequence

Let $\mathbf{u} = (u_n)_{n\geq 0}$ be a linear recurrence sequence

$$(\star) \qquad u_{n+d} = a_1 u_{n+d-1} + \cdots + a_d u_n \quad \text{for} \quad n \geq 0$$

with characteristic polynomial

$$f(X) = X^d - a_1 X^{d-1} - \cdots - a_d.$$

Denote by f^- the reciprocal polynomial of f :

$$f^-(X) = X^d f(X^{-1}) = 1 - a_1 X - \cdots - a_d X^d.$$

Then

$$\sum_{n=0}^{\infty} u_n X^n = \frac{r(X)}{f^-(X)},$$

where r is a polynomial of degree less than d determined by the initial values of $\mathbf{u}$.

Generating series of a linear recurrence sequence

Assume

$$u_{n+d} = a_1 u_{n+d-1} + \cdots + a_d u_n \quad \text{for} \quad n \geq 0.$$

Then

$$\sum_{n=0}^{\infty} u_n X^n = \frac{r(X)}{f^-(X)}.$$

Proof. Comparing the coefficients of X^n for $n \geq d$ shows that

$$f^-(X) \sum_{n=0}^{\infty} u_n X^n$$

is a polynomial of degree less than d

Taylor coefficients of rational functions

Conversely, the coefficients the Taylor expansion of any rational fraction $a(X)/b(X)$ with $\deg a < \deg b$ and $b(0) \neq 0$ satisfies the recurrence relation with characteristic polynomial $f \in K[X]$ given by $f(X) = b^-(X)$.

Therefore a sequence $\mathbf{u} = (u_n)_{n\geq 0}$ satisfies the recurrence relation $(\star)$ with characteristic polynomial $f \in K[X]$ if and only if

$$\sum_{n=0}^{\infty} u_n X^n = \frac{r(X)}{f^-(X)},$$

where r is a polynomial of degree less than d determined by the initial values of $\mathbf{u}$.

Linear differential equations

Given a sequence $(u_n)_{n\geq 0}$ of numbers, its exponential generating power series is

$$f(z) = \sum_{n\geq 0} u_n \frac{z^n}{n!}.$$

For $k \geq 0$, the k-the derivative $f^{(k)}$ of f satisfies

$$f^{(k)}(z) = \sum_{n\geq 0} u_{n+k} \frac{z^n}{n!}.$$

Hence the sequence satisfies the linear recurrence relation

$$(\star) \qquad u_{n+d} = a_1 u_{n+d-1} + \cdots + a_d u_n \quad \text{for} \quad n \geq 0$$

if and only if f satisfies the homogeneous linear differential equation

$$y^{(d)} = a_1 y^{(d-1)} + \cdots + a_d y.$$

Matrix notation for a linear recurrence sequence

The linear recurrence sequence

$$(\star) \qquad u_{n+d} = a_1 u_{n+d-1} + \cdots + a_d u_n \quad \text{for} \quad n \geq 0$$

can be written

$$\begin{pmatrix} u_{n+1} \\ u_{n+2} \\ \vdots \\ u_{n+d} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ a_d & a_{d-1} & a_{d-2} & \cdots & a_1 \end{pmatrix} \begin{pmatrix} u_n \\ u_{n+1} \\ \vdots \\ u_{n+d-1} \end{pmatrix}.$$

Matrix notation for a linear recurrence sequence

$$U_{n+1} = AU_n$$

with

$$U_n = \begin{pmatrix} u_n \\ u_{n+1} \\ \vdots \\ u_{n+d-1} \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ a_d & a_{d-1} & a_{d-2} & \cdots & a_1 \end{pmatrix}.$$

The determinant of $I_d X - A$ (the characteristic polynomial of A) is nothing but

$$f(X) = X^d - a_1 X^{d-1} - \cdots - a_d,$$

the characteristic polynomial of the linear recurrence sequence. By induction

$$U_n = A^n U_0.$$

Powers of matrices

Let $A = (a_{ij})_{1 \leq i,j \leq d} \in \mathrm{GL}_{d \times d}(\mathbb{K})$ be a $d \times d$ matrix with coefficients in $\mathbb{K}$ and nonzero determinant. For $n \geq 0$, define

$$A^n = \left(a_{ij}^{(n)}\right)_{1 \leq i,j \leq d}.$$

Then each of the d^2 sequences $\left(a_{ij}^{(n)}\right)_{n \geq 0}$, $(1 \leq i, j \leq d)$ is a linear recurrence sequence. The roots of the characteristic polynomial of these linear recurrences are the eigenvalues of A.

In particular the sequence $\big(\mathrm{Tr}(A^n)\big)_{n \geq 0}$ satisfies the linear recurrence, the characteristic polynomial of which is the characteristic polynomial of the matrix A.

Conversely :

Given a linear recurrence sequence $\mathbf{u} \in \mathbb{K}^{\mathbb{N}}$, there exist an integer $d \geq 1$ and a matrix $A \in \mathrm{GL}_d(\mathbb{K})$ such that, for each $n \geq 0$,

$$u_n = a_{11}^{(n)}.$$

The characteristic polynomial of A is the characteristic polynomial of the linear recurrence sequence.

Everest G., van der Poorten A., Shparlinski I., Ward T. – *Recurrence sequences*, Mathematical Surveys and Monographs (AMS, 2003), volume 104.

Linear recurrence sequences : simple roots

A basis of $E_{\underline{a}}$ over $\mathbb{K}$ is obtained by attributing to the initial values $u_0, \dots, u_{d-1}$ the values given by the canonical basis of $\mathbb{K}^d$.
Given γ in $\mathbb{K}^\times$, a necessary and sufficient condition for a sequence $(\gamma^n)_{n\ge0}$ to satisfy $(\star)$ is that γ is a root of the characteristic polynomial

$$f(X) = X^d - a_1X^{d-1} - \cdots - a_d.$$

If this polynomial has d distinct roots $\gamma_1, \dots, \gamma_d$ in $\mathbb{K}$,

$$f(X) = (X-\gamma_1)\cdots(X-\gamma_d), \quad \gamma_i \ne \gamma_j,$$

then a basis of $E_{\underline{a}}$ over $\mathbb{K}$ is given by the d sequences $(\gamma_i^n)_{n\ge0}$, $i = 1, \dots, d$.

Linear recurrence sequences : double roots

The characteristic polynomial of the linear recurrence $u_n = 2\gamma u_{n-1} - \gamma^2 u_{n-2}$ is $X^2 - 2\gamma X + \gamma^2 = (X-\gamma)^2$ with a double root γ.

The sequence $(n\gamma^n)_{n\ge0}$ satisfies

$$n\gamma^n = 2\gamma(n-1)n\gamma^{n-1} - \gamma^2(n-2)\gamma^{n-2}.$$

A basis of $E_{\underline{a}}$ for $a_1 = 2\gamma$, $a_2 = -\gamma^2$ is given by the two sequences $(\gamma^n)_{n\ge0}$, $(n\gamma^n)_{n\ge0}$.

Given $\gamma \in \mathbb{K}^\times$, a necessary and sufficient condition for the sequence $n\gamma^n$ to satisfy the linear recurrence relation $(\star)$ is that γ is a root of multiplicity ≥ 2 of $f(X)$.

Linear recurrence sequences : multiple roots

In general, when the characteristic polynomial splits as

$$X^d - a_1X^{d-1} - \cdots - a_d = \prod_{i=1}^{\ell}(X-\gamma_i)^{t_i},$$

a basis of $E_{\underline{a}}$ is given by the d sequences

$$(n^k\gamma_i^n)_{n\ge0}, \qquad 0 \le k \le t_i - 1, \quad 1 \le i \le \ell.$$

Polynomial combinations of powers

The sum and the product of any two linear recurrence sequences are linear recurrence sequences.

The set $\cup_{\underline{a}} E_{\underline{a}}$ of all linear recurrence sequences with coefficients in $\mathbb{K}$ is a sub–$\mathbb{K}$–algebra of $\mathbb{K}^{\mathbb{N}}$.

Given polynomials $p_1, \dots, p_\ell$ in $\mathbb{K}[X]$ and elements $\gamma_1, \dots, \gamma_\ell$ in $\mathbb{K}^\times$, the sequence

$$\bigl(p_1(n)\gamma_1^n + \cdots + p_\ell(n)\gamma_\ell^n\bigr)_{n\ge0}$$

is a linear recurrence sequence.

Conversely, any linear recurrence sequence is of this form.

Consequence

• When f is a polynomial of degree $< d$, the characteristic polynomial of the sequence $u_n = f(n)$ divides $(X-1)^d$.

Proof.

Set

$$A = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix} = I_d + N$$

where I_d is the $d \times d$ identity matrix and N is nilpotent : $N^d = 0$.

Consequence

The characteristic polynomial of A is $(X-1)^d$. Hence for $1 \le i, j \le d$, the sequence u_n of the coefficient $a_{ij}^{(n)}$ of A^n satisfies the linear recurrence relation

$$(\star) \qquad u_{n+d} = a_1 u_{n+d-1} + \cdots + a_d u_n,$$

that is

$$u_{n+d} = d u_{n+d-1} - \binom{d}{2} u_{n+d-2} + \cdots + (-1)^{d-2} d u_{n+1} + (-1)^{d-1} u_n.$$

The characteristic polynomial of this recurrence relation is $(X-1)^d$.

Characteristic polynomial of the recurrence sequence $f(n)$.

Since, for $1 \le i, j \le d$ and $n \ge 0$, we have

$$a_{ij}^{(n)} = \binom{n}{j-i}$$

(where we agree that $\binom{n}{k} = 0$ for $k < 0$ and for $k > n$, while $\binom{d}{0} = \binom{d}{d} = 1$), we deduce that each of the d polynomials

$$1, \quad \frac{X(X+1)\cdots(X+k-1)}{k!} \qquad k = 1, 2, \ldots, d-1$$

namely

$$1, X, \frac{X(X+1)}{2}, \ldots, \frac{X(X+1)\cdots(X+d-2)}{(d-1)!},$$

satisfies the recurrence $(\star)$. These d polynomials constitute a basis of the space of polynomials of degree $< d$.

Sum of polynomial combinations of powers

If $\mathbf{u}_1$ and $\mathbf{u}_2$ are two linear recurrence sequences of characteristic polynomials f_1 and f_2 respectively, then $\mathbf{u}_1 + \mathbf{u}_2$ satisfies the linear recurrence, the characteristic polynomial of which is

$$\frac{f_1 f_2}{\gcd(f_1, f_2)}.$$

Product of polynomial combinations of powers

If the characteristic polynomials of the two linear recurrence sequences $\mathbf{u}_1$ and $\mathbf{u}_2$ are respectively

$$f_1(T) = \prod_{j=1}^{\ell}(T-\gamma_j)^{t_j} \quad \text{and} \quad f_2(T) = \prod_{k=1}^{\ell'}(T-\gamma'_k)^{t'_k},$$

then $\mathbf{u}_1\mathbf{u}_2$ satisfies the linear recurrence, the characteristic polynomial of which is

$$\prod_{j=1}^{\ell}\prod_{k=1}^{\ell'}(T-\gamma_j\gamma'_k)^{t_j+t'_k-1}.$$

Linear recurrence sequences and Brahmagupta–Pell–Fermat Equation

Let d be a positive integer, not a square. The solutions $(x,y)\in\mathbb{Z}\times\mathbb{Z}$ of the Brahmagupta–Pell–Fermat Equation

$$x^2-dy^2=\pm 1$$

form a sequence $(x_n,y_n)_{n\in\mathbb{Z}}$ defined by

$$x_n+\sqrt{d}y_n=(x_1+\sqrt{d}y_1)^n.$$

From

$$2x_n=(x_1+\sqrt{d}y_1)^n+(x_1-\sqrt{d}y_1)^n$$

we deduce that $(x_n)_{n\geq 0}$ is a linear recurrence sequence. Same for y_n, and also for $n\leq 0$.

Doubly infinite linear recurrence sequences

A sequence $(u_n)_{n\in\mathbb{Z}}$ indexed by $\mathbb{Z}$ is a linear recurrence sequence if it satisfies

$$(\star) \qquad u_{n+d}=a_1u_{n+d-1}+\cdots+a_du_n.$$

for all $n\in\mathbb{Z}$.

Recall $a_d\neq 0$.

Such a sequence is determined by d consecutive values.

Discrete version of linear differential equations

A sequence $\mathbf{u}\in\mathbb{K}^{\mathbb{N}}$ can be viewed as a linear map $\mathbb{N}\longrightarrow\mathbb{K}$. Define the discrete derivative $\mathcal{D}$ by

$$\begin{array}{rccc}\mathcal{D}\mathbf{u}: & \mathbb{N} & \longrightarrow & \mathbb{K}\\ & n & \longmapsto & u_{n+1}-u_n.\end{array}$$

A sequence $\mathbf{u}\in\mathbb{K}^{\mathbb{N}}$ is a linear recurrence sequence if and only if there exists $Q\in\mathbb{K}[T]$ with $Q(1)\neq 1$ such that

$$Q(\mathcal{D})\mathbf{u}=0.$$

Linear recurrence sequences are a discrete version of linear differential equations with constant coefficients.

The condition $Q(1)\neq 0$ reflects $a_d\neq 0$ – otherwise one gets *ultimately* recurrent sequences.

97th Indian Science Congress, 2010

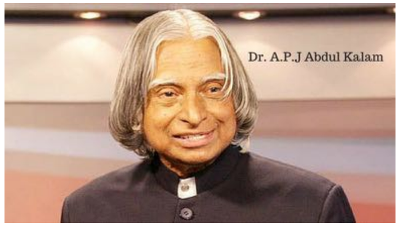
A.K. Agarwal

Invited by Ashok Agrawal to the 97th Indian Science Congress in Thiruvananthapuram (Trivandrum, Kerala), January 3-7, 2010.
• Lecture on *Number Theory Challenges of 21st Century*

A. P. J. Abdul Kalam (1931-2015)

Public Lecture during the 97th Indian Science Congress, Thiruvananthapuram – 4 January 2010 Thiruvananthapuram

Basic research is vital for enhancing national and international competitiveness



http://www.abdulkalam.com/kalam/theme/jsp/guest/content-display.jsp

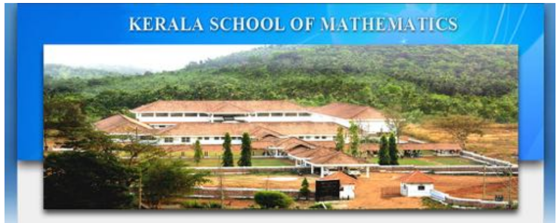
Kerala 2010

Sudhir Ghorpade Jugal K. Verma Ambar Vijayatkumar

January 9-10, 2010, Cochin = Kochi (Kerala) Department of Mathematics, Cochin University of Science and Technology CUSAT

KSOM 2010

January 8, 2010, Calicut = Kozhikode (Kerala) The Kerala School of Mathematics (KSoM)



A. J. Parameswaran, Director of the Kerala School of Mathematical Science (KSOM) in Kozikhode (Calicut)

KSOM 2010

Work on dynamical systems by A. J. Parameswaran and S.G. Dani

A. J. Parameswaran

S.G. Dani

A dynamical system

Let V be a finite dimensional vector space over a field of zero characteristic, H an hyperplane of V, $f : V \to V$ an endomorphism (linear map) and x an element in V.

Theorem. *If there exist infinitely many $n \geq 1$ such that $f^n(x) \in H$, then there is an (infinite) arithmetic progression of n for which it is so.*

Skolem – Mahler – Lech Theorem

Theorem (Skolem 1934 – Mahler 1935 – Lech 1953). *Given a linear recurrence sequence, the set of indices $n \geq 0$ such that $u_n = 0$ is a finite union of arithmetic progressions.*

Linear recurrence sequence :

$$u_{n+d} = a_1 u_{n+d-1} + \cdots + a_d u_n, \qquad n \geq 0 \qquad (a_d \neq 0).$$

Characteristic polynomial :

$$X^d - a_1 X^{d-1} - \cdots - a_d = \prod_{j=1}^{\ell} (X - \gamma_j)^{t_j}$$

$$u_n = \sum_{j=1}^{\ell} \sum_{i=0}^{t_j - 1} c_{ij} n^i \gamma_j^n.$$

Wolfgang M. Schmidt

Thue – Siegel – Roth – Schmidt,

Schmidt's Subspace Theorem. The generalized S–unit Theorem

Let $\mathbb{K}$ be a field of characteristic zero, let G be a finitely multiplicative subgroup of the multiplicative group $\mathbb{K}^\times = \mathbb{K} \setminus \{0\}$ and let $n \geq 2$. Then the equation

$$u_1 + u_2 + \cdots + u_n = 1,$$

where the values of the unknowns $u_1, u_2, \cdots, u_n$ are in G for which no nontrivial subsum

$$\sum_{i \in I} u_i \qquad \emptyset \neq I \subset \{1, \ldots, n\}$$

vanishes, has only finitely many solutions.

Schmidt's subspace Theorem

Wolfgang M. Schmidt

Pietro Corvaja

Umberto Zannier

Balu's 60's Birthday, 2011

December 15 - 20, 2011 : HRI : International Meeting on Number Theory 2011 celebrating the 60th Birthday of Professor R. Balasubramanian.

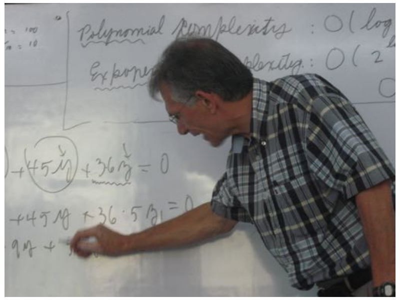
Pietro Corvaja

M. Manickam, director of KSOM.

December 16, 2011 : lecture on *Families of Thue-Mahler equations*.

Joint work with Claude Levesque

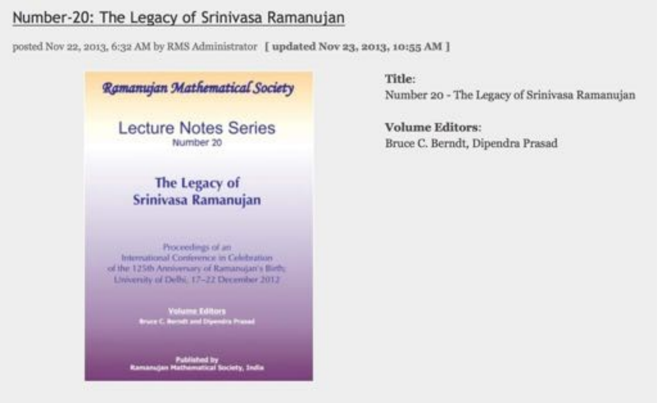
http://arxiv.org/abs/1505.06653



Solving simultaneously Thue Diophantine equations : almost totally imaginary case
Proceedings of the International Meeting on Number Theory HRI 2011, in honor of R. Balasubramanian.

Ramanujan Mathematical Society, Lecture Notes Series **23**, *Highly composite : papers in number theory*, (2016), 137–156. Editors Kumar Murty, Ravindranathan Thangadurai.
http://www.ramanujanmathsociety.org/publications/rms-lecture-notes-series

http://www.ramanujanmathsociety.org/publications/rms-lecture-notes-series



Number-20: The Legacy of Srinivasa Ramanujan

posted Nov 22, 2013, 6:32 AM by RMS Administrator **[updated Nov 23, 2013, 10:55 AM]**

Ramanujan Mathematical Society

Lecture Notes Series
Number 20

The Legacy of
Srinivasa Ramanujan

Proceedings of an
International Conference in Celebration
of the 125th Anniversary of Ramanujan's Birth;
University of Delhi, 17–22 December 2012

Volume Editors
Bruce C. Berndt and Dipendra Prasad

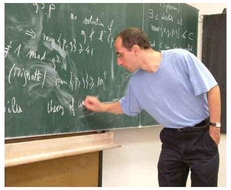
Published by
Ramanujan Mathematical Society, India

Title:
Number 20 - The Legacy of Srinivasa Ramanujan

Volume Editors:
Bruce C. Berndt, Dipendra Prasad

KSOM 2013

Workshop *number theory and dynamical systems* in KSOM (Director M. Manickam) in February 2013



Yann Bugeaud

Pietro Corvaja

S.G. Dani

Reference

M. Waldschmidt. *Diophantine approximation with applications to dynamical systems.* Proceedings of the International Conference on Pure and Applied Mathematics ICPAM–LAE 2013, South Pacific Journal of Pure and Applied Mathematics, vol. 1, No 2 (2014), 1–18.

Skolem – Mahler – Lech Theorem

Theorem (Skolem 1934 – Mahler 1935 – Lech 1953). *Given a linear recurrence sequence, the set of indices $n \geq 0$ such that $u_n = 0$ is a finite union of arithmetic progressions.*

Thoralf Albert Skolem
(1887 – 1963)

Kurt Mahler
(1903 – 1988)

Christer Lech

An *arithmetic progression* is a set of positive integers of the form $\{n_0, n_0 + k, n_0 + 2k, \ldots\}$. Here, we allow $k = 0$.

A dynamical system

Let V be a finite dimensional vector space over a field of zero characteristic, W a subspace of V, $f : V \to V$ an endomorphism (linear map) and x an element in V.

Corollary of the Skolem – Mahler – Lech Theorem. *The set of $n \geq 0$ such that $f^n(x) \in W$ is a finite union of arithmetic progressions.*

By induction, it suffices to consider the case where $W = H$ is an hyperplane of V.

Idea of the proof of the corollary

Choose a basis of V. The endomorphism f is given by a square $d \times d$ matrix A, where d is the dimension of V. Consider the characteristic polynomial of A, say

$$X^d - a_{d-1}X^{d-1} - \cdots - a_1X - a_0.$$

By the Theorem of Cayley – Hamilton,

$$A^d = a_{d-1}A^{d-1} + \cdots + a_1A + a_0I_d$$

where I_d is the identity $d \times d$ matrix.

Theorem of Cayley – Hamilton

Arthur Cayley
(1821 – 1895)

Sir William Rowan Hamilton
(1805 – 1865)

Hence, for $n \geq 0$,

$$A^{n+d} = a_{d-1}A^{n+d-1} + \cdots + a_1A^{n+1} + a_0A^n.$$

It follows that each entry $a_{ij}(n)$, $1 \leq i, j \leq d$, satisfies a linear recurrence relation, the same for all i, j.

Hyperplane membership

Let $b_1x_1 + \cdots + b_dx_d = 0$ be an equation of the hyperplane H in the selected basis of V. Let ${}^t\underline{b}$ denote the $1 \times d$ matrix $(b_1, \ldots, b_d)$ (transpose of a column matrix $\underline{b}$). Using the notation $\underline{v}$ for the $d \times 1$ (column) matrix given by the coordinates of an element v in V, the condition $v \in H$ can be written ${}^t\underline{b}\,\underline{v} = 0$.

Let x be an element in V and $\underline{x}$ the $d \times 1$ (column) matrix given by its coordinates. The condition $f^n(x) \in H$ can now be written

$${}^t\underline{b}A^n\underline{x} = 0.$$

The entry u_n of the 1×1 matrix ${}^t\underline{b}A^n\underline{x}$ satisfies a linear recurrence relation, hence, the Skolem – Mahler – Lech Theorem applies.

Remark on the theorem of Skolem–Mahler–Lech

T.A. Skolem treated the case $K = \mathbb{Q}$ of in 1934

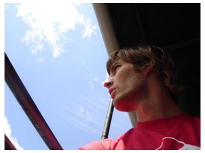
K. Mahler the case $\mathbb{K} = \overline{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$, in 1935

The general case was settled by C. Lech in 1953.

Finite characteristic

C. Lech pointed out in 1953 that such a result may not hold if the characteristic of $\mathbb{K}$ is positive : he gave as an example the sequence $u_n = (1+x)^n - x^n - 1$, a third-order linear recurrence over the field of rational functions in one variable over the field $\mathbb{F}_p$ with p elements, where $u_n = 0$ for $n \in \{1, p, p^2, p^3, \dots\}$. A substitute is provided by a result of Harm Derksen (2007), who proved that the zero set in characteristic p is a p–automatic sequence. Further results by Boris Adamczewski and Jason Bell.

Harm Derksen


Boris Adamczewski

Jason Bell

Polynomial-linear recurrence relation

A generalization of the Theorem of Skolem–Mahler–Lech has been achieved by Jason P. Bell, Stanley Burris and Karen Yeats who prove that the same conclusion holds if the sequence $(u_n)_{n\geq 0}$ satisfies a polynomial-linear recurrence relation

$$u_n = \sum_{i=1}^{d} P_i(n) u_{n-i}$$

where d is a positive integer and $P_1, \dots, P_d$ are polynomials with coefficient in the field $\mathbb{K}$ of zero characteristic, provided that $P_d(x)$ is a nonzero constant.

Algebraic maps, algebraic groups

There are also analogues of the Theorem of Skolem–Mahler–Lech for algebraic maps on varieties (Jason Bell).

A version of the Skolem–Mahler–Lech Theorem for any algebraic group is due to Umberto Zannier.

Jason Bell

Umberto Zannier

Open problem

One main open problem related with Theorem of Skolem–Mahler–Lech is that it is not effective : explicit upper bounds for the number of arithmetic progressions, depending only on the order d of the linear recurrence sequence, are known (W.M. Schmidt, U. Zannier), but no upper bound for the arithmetic progressions themselves is known. A related open problem raised by T.A. Skolem and C. Pisot is :

> *Given an integer linear recurrence sequence, is the truth of the statement "$x_n \neq 0$ for all n" decidable in finite time ?*

T. Tao, *Effective Skolem Mahler Lech theorem*. In "Structure and Randomness : pages from year one of a mathematical blog", American Mathematical Society (2008), 298 pages.
http://terrytao.wordpress.com/2007/05/25/open-question-effective-skolem-mahler-lech-theorem/

Zeros of linear recurrence sequences

Jean Berstel et Maurice Mignotte. – Deux propriétés décidables des suites récurrentes linéaires Bulletin de la S.M.F., tome 104 (1976), p. 175-184.
`http://www.numdam.org/item?id=BSMF_1976__104__175_0`
Given a linear recurrence sequence with integer coefficients ; are there finitely or infinitely many zeroes ?

Philippe Robba. – Zéros de suites récurrentes linéaires. Groupe de travail d'analyse ultramétrique (1977-1978) Volume : 5, page 1-5.

L. Cerlienco, M. Mignotte, F. Piras. Suites récurrentes linéaires. Propriétés algébriques et arithmétiques. L'Enseignement Mathématique **33** (1987).

Zeros of linear recurrence sequences

Maurice Mignotte Propriétés arithmétiques des suites récurrentes linéaires. Besançon, 1989
`http://pmb.univ-fcomte.fr/1989/Mignotte.pdf`

E. Bavencoffe and J-P. Bézivin *Une famille remarquable de suites recurrentes lineaires*. – Monatshefte für Mathematik, (1995) **120** 3, 189–203

Karim Samake. – Suites récurrentes linéaires, problème d'effectivité. Inst. de Recherche Math. Avancée, 1996 - 62 pages

Reference

Everest, Graham ; van der Poorten, Alf ; Shparlinski, Igor ; Ward, Tom – *Recurrence sequences*, Mathematical Surveys and Monographs (AMS, 2003), volume 104. `1290 references.`

Graham Everest

Alf van der Poorten

Igor Shparlinski

Tom Ward

Berstel's sequence

`http://oeis.org/A007420`

$0,\ 0,\ 1,\ 2,\ 0,\ -4,\ 0,\ 16,\ 16,\ -32,\ -64,\ 64,\ 256,\ 0,\ -768,\ \dots$

Jean Berstel

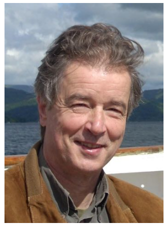
$b_0 = b_1 = 0,\ b_2 = 1,$
$b_{n+3} = 2b_{n+2} - 4b_{n+1} + 4b_n$
for $n \geq 0$.

Linear recurrence sequence of order 3 with exactly 6 zeros : $n = 0,\ 1,\ 4,\ 6,\ 13,\ 52.$

`http://www-igm.univ-mlv.fr/~berstel/`

Ternary linear recurrences

Berstel's sequence is a linear recurrence sequence of order 3 with 6 zeroes.



Frits Beukers

Frits Beukers (1991) : up to trivial transformation, any other linear recurrence of order 3 with finitely many zeroes has at most 5 zeros.

Edgard Bavencoffe and Jean-Paul Bézivin

Let $n \geq 2$. The sequence with initial values

$$u_0 = 1,\ u_1 = \cdots = u_{n-1} = 0$$

satisfying the recurrence relation of order n with characteristic polynomial

$$\frac{X^{n+1} - (-2)^{n-1}X + (-2)^n}{X+2}$$

has at least

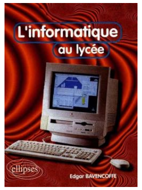
$$\frac{n(n+1)}{2} - 1$$

zeroes.

Edgard Bavencoffe and Jean-Paul Bézivin

For $n = 3$ one obtains Berstel's sequence which happens to have an extra zero.

$$\frac{X^4 + 4X - 8}{X+2} = X^3 - 2X^2 + 4X - 4.$$



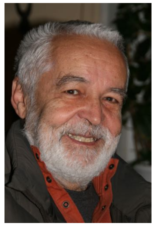
Edgard Bavencoffe

Jean-Paul Bézivin

Berstel's sequence

$$0,\ 0,\ 1,\ 2,\ 0,\ -4,\ 0,\ 16,\ 16,\ -32,\ -64,\ 64,\ 256,\ 0,\ -768,\ \dots$$

$b_0 = b_1 = 0,\ b_2 = 1,\ b_{n+3} = 2b_{n+2} - 4b_{n+1} + 4b_n$ for $n \geq 0$.

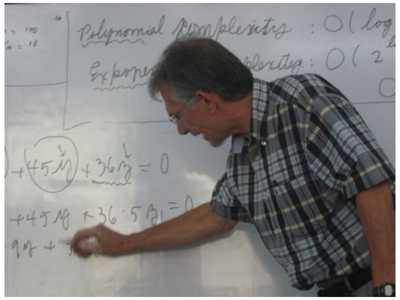


Maurice Mignotte

The equation $b_m = \pm b_n$ has exactly 21 solutions (m, n) with $m \neq n$.

The equation $b_n = \pm 2^r 3^s$ has exactly 44 solutions (n, r, s).

Joint work with Claude Levesque



Linear recurrence sequences and twisted binary forms. Proceedings of the International Conference on Pure and Applied Mathematics ICPAM-GOROKA 2014. South Pacific Journal of Pure and Applied Mathematics.

http://webusers.imj-prg.fr/~michel.waldschmidt//articles/pdf/ProcConfPNG2014.pdf

Families of binary forms

Consider a binary form $F_0(X,Y) \in \mathbb{C}[X,Y]$ which satisfies $F_0(1,0)=1$. We write it as

$$F_0(X,Y) = X^d + a_1X^{d-1}Y + \cdots + a_dY^d \; = \prod_{i=1}^{d}(X-\alpha_iY).$$

Let $\epsilon_1,\dots,\epsilon_d$ be d nonzero complex numbers not necessarily distinct. Twisting F_0 by the powers $\epsilon_1^n,\dots,\epsilon_d^n$ $(n\in\mathbb{Z})$ boils down to considering the family of binary forms

$$F_n(X,Y) = \prod_{i=1}^{d}(X-\alpha_i\epsilon_i^nY),$$

which we write as

$$X^d - U_1(n)X^{d-1}Y + \cdots + (-1)^dU_d(n)Y^d.$$

Therefore

$$U_h(0) = (-1)^ha_h \qquad (1\le h\le d).$$

Families of Diophantine equations

With Claude Levesque, we considered some families of diophantine equations

$$F_n(x,y)=m$$

obtained in the same way from a given irreducible form $F(X,Y)$ with coefficients in $\mathbb{Z}$, when $\epsilon_1,\dots,\epsilon_d$ are algebraic units and when the algebraic numbers $\alpha_1\epsilon_1,\dots,\alpha_d\epsilon_d$ are Galois conjugates with $d\ge 3$.

Theorem. *Let $\mathbb{K}$ be a number field of degree $d\ge 3$, S a finite set of places of $\mathbb{K}$ containing the places at infinity. Denote by $\mathcal{O}_S$ the ring of S–integers of $\mathbb{K}$ and by $\mathcal{O}_S^\times$ the group of S–units of $\mathbb{K}$. Assume $\alpha_1,\dots,\alpha_d,\epsilon_1,\dots,\epsilon_d$ belong to $\mathbb{K}^\times$ Then there are only finitely many (x,y,n) in $\mathcal{O}_S\times\mathcal{O}_S\times\mathbb{Z}$ satisfying*

$$F_n(x,y)\in\mathcal{O}_S^\times, \quad xy\neq 0 \quad \textit{and} \quad \mathrm{Card}\{\alpha_1\epsilon_1^n,\dots,\alpha_d\epsilon_d^n\}\ge 3.$$

Families of Diophantine equations

Each of the sequences $\bigl(U_h(n)\bigr)_{n\in\mathbb{Z}}$ coming from the coefficients of the relation

$$F_n(X,Y) = X^d - U_1(n)X^{d-1}Y + \cdots + (-1)^dU_d(n)Y^d$$

is a linear recurrence sequence.
For example, for $n\in\mathbb{Z}$,

$$U_1(n) = \sum_{i=1}^{d}\alpha_i\epsilon_i^n, \quad U_d(n) = \prod_{i=1}^{d}\alpha_i\epsilon_i^n.$$

For $1\le h\le d$, the sequence $\bigl(U_h(n)\bigr)_{n\in\mathbb{Z}}$ is a linear combination of the sequences

$$\bigl((\epsilon_{i_1}\cdots\epsilon_{i_h})^n\bigr)_{n\in\mathbb{Z}}, \quad (1\le i_1<\cdots<i_h\le d).$$

Some units of Bernstein and Hasse

Let t and s be two positive integers, D an integer ≥ 1, and $c \in \{-1,+1\}$. Let $\omega > 1$ satisfy

$$\omega^{st} = D^{st} + c,$$

where it is assumed that $\mathbb{Q}(\omega)$ is of degree st.
Consider

$$\alpha = D - \omega, \quad \epsilon = D^t - \omega^t.$$

L. Bernstein and H. Hasse noticed that α and ϵ are units of degree st and s respectively, and showed that these units can be obtained from the Jacobi–Perron algorithm. H.-J. Stender proved that for $s = t = 2$, $\{\alpha, \epsilon\}$ is a fundamental system of units of the quartic field $\mathbb{Q}(\omega)$.

Helmut Hasse (1898-1979)

$D > 0$, $s \geq 1$, $t \geq 1$,
$c \in \{-1,+1\}$, $\omega > 0$,

$$\omega^{st} = D^{st} + c,$$

$$\alpha = D - \omega,$$

$$\epsilon = D^t - \omega^t.$$

$$(\alpha - D)^{st} = (-1)^{st}(D^{st} + c).$$

Diophantine equations associated with some units of Bernstein and Hasse

The irreducible polynomial of α is $F_0(X,1)$, with

$$F_0(X,Y) = (X - DY)^{st} - (-1)^{st}(D^{st} + c)Y^{st}.$$

For $n \in \mathbb{Z}$, the binary form $F_n(X,Y)$, obtained by twisting $F_0(X,Y)$ with the powers ϵ^n of ϵ, is the homogeneous version of the irreducible polynomial $F_n(X,1)$ of $\alpha\epsilon^n$. So F_n depends of the parameters n, D, s, t and c.

Theorem (LW). *Suppose $st \geq 3$. There exists an effectively computable constant κ, depending only on D, s and t, with the following property. Let m, a, x, y be rational integers satisfying $m \geq 2$, $xy \neq 0$, $[\mathbb{Q}(\alpha\epsilon^a) : \mathbb{Q}] = st$ and*

$$|F_n(x,y)| \leq m.$$

Then

$$\max\{\log|x|, \log|y|, |n|\} \leq \kappa \log m.$$

Hankel determinants

To test an arbitrary sequence $\mathbf{u} = (u_n)_{n\geq 0}$ of elements of a field $\mathbb{K}$ for the property of being a linear recurrence sequence, consider the Hankel determinants

$$\Delta_{N,d}(\mathbf{u}) = \det\left(u_{d+i+j}\right)_{0\leq i,j\leq N}.$$

Hermann Hankel
(1839–1873)

The sum

$$f(z) = \sum_{n=0}^{\infty} u_n z^n$$

represents a rational function if and only if for some d, $\Delta_{N,d}(\mathbf{u}) = 0$ for all sufficiently large N

Hankel determinants

Alan Haynes, Wadim Zudilin. – Hankel determinants of zeta values
(Submitted on 7 Oct 2015)

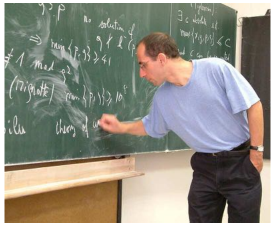
`Abstract:` *We study the asymptotics of Hankel determinants constructed using the values $\zeta(an+b)$ of the Riemann zeta function at positive integers in an arithmetic progression. Our principal result is a Diophantine application of the asymptotics.*

Alan Haynes

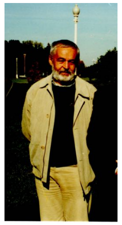
Wadim Zudilin

Perfect powers in the Fibonacci sequence

Yann Bugeaud, Maurice Mignotte, Samir Siksek (2004) : The only perfect powers (squares, cubes, etc.) in the Fibonacci sequence are 1, 8 and 144.



Y. Bugeaud



M. Mignotte

S. Siksek

Powers in recurrence sequences

Mike Bennett

M. A. Bennett, Powers in recurrence sequences : Pell equations, Trans. Amer. Math. Soc. **357** (2005), 1675-1691.

`http://www.math.ubc.ca/~bennett/paper31.pdf`

Bases of the space of linear recurrence sequences

Given $a_1, \dots, a_d$ with $a_d \neq 0$, consider the vector space of linear recurrence sequences satisfying, for $n \geq 0$,

$$(\star) \qquad u_{n+d} = a_1 u_{n+d-1} + \cdots + a_d u_n.$$

Assuming the characteristic polynomial

$$f(X) = X^d - a_1 X^{d-1} - \cdots - a_d$$

of the recurrence splits completely in $\mathbb{K}$,

$$f(X) = \prod_{j=1}^{\ell} (X - \gamma_j)^{t_i}$$

we have two bases. The first one given by the initial conditions $(u_0, \dots, u_{d-1})$, and the second one is given by the sequences

$$(n^i \gamma_j^n)_{n\geq 0}, \quad 0 \leq i \leq t_j - 1, \; 1 \leq j \leq \ell.$$

Change of basis

The matrix of change of bases is

$$M = \begin{pmatrix} M_1 \\ \vdots \\ M_\ell \end{pmatrix}$$

where

$$M_j = \begin{pmatrix} 1 & \gamma_j & \gamma_j^2 & \cdots & \gamma_j^{t_j-1} & \gamma_j^{t_j} & \cdots & \gamma_j^{d-1} \\ 0 & 1 & \binom{2}{1}\gamma_j & \cdots & \binom{t_j-1}{1}\gamma_j^{t_j-2} & \binom{t_j}{1}\gamma_j^{t_j-1} & \cdots & \binom{d-1}{1}\gamma_j^{d-2} \\ 0 & 0 & 1 & \cdots & \binom{t_j-1}{2}\gamma_j^{t_j-3} & \binom{t_j}{2}\gamma_j^{t_j-2} & \cdots & \binom{d-1}{2}\gamma_j^{d-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & \binom{t_j}{t_j-1}\gamma_j & \cdots & \binom{d-1}{t_j-1}\gamma_j^{d-t_j} \end{pmatrix}$$

Exponential polynomials

The sequence of derivatives of an exponential polynomial evaluated at one point satisfies a linear recurrence relation.
Let $p_1(z), \dots, p_\ell(z)$ be nonzero polynomials of $\mathbb{C}[z]$ of degrees smaller than $t_1, \dots, t_\ell$ respectively. Let $\gamma_1, \dots, \gamma_\ell$ be distinct complex numbers. Suppose that the function

$$F(z) = p_1(z)e^{\gamma_1 z} + \cdots + p_\ell(z)e^{\gamma_\ell z}$$

is not identically 0. Then its vanishing order at a point z_0 is smaller than or equal to $t_1 + \cdots + t_\ell - 1$.
In other terms, when the complex numbers γ_j are distinct, the determinant

$$\left| \left(\frac{\mathrm{d}}{\mathrm{d}z}\right)^a \left(z^i e^{\gamma_j z}\right)_{z=0} \right|_{\substack{0 \le i \le t_j - 1,\ 1 \le j \le \ell \\ 0 \le a \le d-1}}$$

is different from 0. This is no surprise that we come across the determinant of the matrix M.

The matrix M

The determinant of M is

$$\det M = \prod_{1 \le i < j \le \ell} (\gamma_j - \gamma_i)^{t_i t_j}.$$

For $1 \le j \le \ell$, $0 \le i \le t_j - 1, \quad 0 \le k \le d-1$, the $(s_j + i, k)$ entry of the matrix M is

$$\frac{1}{i!}\left(\frac{\mathrm{d}}{\mathrm{d}T}\right)^i T^k \Big|_{T=\gamma_j} = \binom{k}{i}\gamma_j^{k-i}.$$

The matrix M is associated with the linear system of d equations in d unknowns which amounts to finding a polynomial $f \in K[z]$ of degree $< d$ for which the d numbers

$$\frac{\mathrm{d}^i f}{\mathrm{d}z^i}(\gamma_j), \qquad (1 \le j \le \ell,\ 0 \le i \le t_j - 1)$$

take prescribed values.

Interpolation

Let γ_j $(1 \le j \le \ell)$ be distinct elements in $\mathbb{K}$, t_j $(1 \le j \le \ell)$ be positive integers, η_{ij} $(1 \le j \le \ell,\ 0 \le i \le t_j - 1)$ be elements in $\mathbb{K}$. Set $d = t_1 + \cdots + t_\ell$. There exists a unique polynomial $f \in \mathbb{K}[z]$ of degree $< d$ satisfying

$$\frac{\mathrm{d}^i f}{\mathrm{d}z^i}(\gamma_j) = \eta_{ij}, \qquad (1 \le j \le \ell,\ 0 \le i \le t_j - 1).$$

Truncated Taylor expansion

Let $g \in \mathbb{K}(z)$, let $z_0 \in \mathbb{K}$ and let $t \geq 1$. Assume z_0 is not a pole of g. We set

$$T_{g,z_0,t}(z) = \sum_{i=0}^{t-1} \frac{\mathrm{d}^i g}{\mathrm{d}z^i}(z_0) \frac{(z-z_0)^i}{i!}.$$

In other words, $T_{g,z_0,t}$ is the unique polynomial in $\mathbb{K}[z]$ of degree $< t$ such that there exists $r(z) \in \mathbb{K}(z)$ having no pole at z_0 with

$$g(z) = T_{g,z_0,t}(z) + (z-z_0)^t r(z).$$

Notice that if g is a polynomial of degree $< t$, then $g = T_{g,z_0,t}$ for any $z_0 \in \mathbb{K}$.

Explicit solution to the interpolation problem

For $j = 1, \dots, \ell$, define

$$h_j(z) = \prod_{\substack{1 \leq k \leq \ell \\ k \neq j}} \left(\frac{z-\gamma_k}{\gamma_j - \gamma_k} \right)^{t_k} \quad \text{and} \quad p_j(z) = \sum_{i=0}^{t_j-1} \eta_{ij} \frac{(z-\gamma_j)^i}{i!}.$$

Then the solution f of the interpolation problem

$$\frac{\mathrm{d}^i f}{\mathrm{d}z^i}(\gamma_j) = \eta_{ij}, \qquad (1 \leq j \leq \ell,\ 0 \leq i \leq t_j - 1).$$

is given by

$$f = \sum_{j=1}^{\ell} h_j T_{\frac{p_j}{h_j},\gamma_j,t_j}.$$

Updated: 09/11/2017

Linear recurrence sequences, exponential polynomials and Diophantine approximation

Michel Waldschmidt

Institut de Mathématiques de Jussieu — Paris VI
http://webusers.imj-prg.fr/~michel.waldschmidt/