Universita degli Studi Roma Tre *April 6, 2017*

http://www.rnta.eu/ThirdRNTA/index.html

The third mini symposium of the
Roman Number Theory Association

# Diophantine approximation and power series.

*Michel Waldschmidt*

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

# Abstract

We give an introduction to the theory of Diophantine approximation of power series, starting with continued fractions and culminating with parametric geometry of numbers.

Next we give a survey of a joint work with D. Roy, where we consider an analog for power series of the *parametric geometry of numbers*, initiated by W.M. Schmidt in 1982 and developed in 2009 and 2013 by W.M. Schmidt and L. Summerer and in 2015 by D. Roy.

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

# Introduction

In the introduction of his paper in 1873 where he proved the transcendence of $e$, Ch. Hermite starts by recalling the theory of simultaneous Diophantine approximation to several real numbers by rational tuples. He points out that the case of a single number is nothing else than the algorithm of continued fractions. He claims that he will do something similar with functions. This is the birth of the theory of Padé approximation, and Hermite pursues by giving an explicit solution for what is called now Padé approximants of type II for the exponential function.

# Charles Hermite and Ferdinand Lindemann

*Hermite (1873) :*
Transcendence of $e$
$e = 2.718\,281\,828\,4\ldots$

*Lindemann (1882) :*
Transcendence of $\pi$
$\pi = 3.141\,592\,653\,5\ldots$

# Charles Hermite 1873

ANALYSE. — *Sur la fonction exponentielle;* par M. **Hermite.**

« I. Étant donné un nombre quelconque de quantités numériques $\alpha_1, \alpha_2, \ldots, \alpha_n$, on sait qu'on peut en approcher simultanément par des fractions de même dénominateur, de telle sorte qu'on ait

$$\alpha_1 = \frac{A_1}{A} + \frac{\delta_1}{A\sqrt[n]{A}},$$
$$\alpha_2 = \frac{A_2}{A} + \frac{\delta_2}{A\sqrt[n]{A}},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots,$$
$$\alpha_n = \frac{A_n}{A} + \frac{\delta_n}{A\sqrt[n]{A}},$$

$\delta_1, \delta_2, \ldots, \delta_n$ ne pouvant dépasser une limite qui dépend seulement de $n$. C'est, comme on voit, une extension du mode d'approximation résultant de la théorie des fractions continues, qui correspondrait au cas le plus simple de $n = 1$. Or on peut se proposer une généralisation semblable de la théorie des fractions continues algébriques, en cherchant les expressions approchées de $n$ fonctions, $\varphi_1(x), \varphi_2(x), \ldots, \varphi_n(x)$ par des fractions rationnelles $\frac{\Phi_1(x)}{\Phi(x)}, \frac{\Phi_2(x)}{\Phi(x)}, \ldots, \frac{\Phi_n(x)}{\Phi(x)}$, de manière que les développements en série suivant les puissances croissantes de la variable coïncident jusqu'à une puissance déterminée $x^M$. Voici d'abord à cet égard un premier résultat qui s'offre immédiatement. Supposons que les fonctions $\varphi_1(x), \varphi_2(x), \ldots, \varphi_n(x)$ soient toutes développables en séries de la forme $\alpha + \beta x + \gamma x^2 + \ldots$ et faisons

# Felix Müller Jahrbuch der Mathematik

**Hermite, Ch.**
**On the exponential function. (Sur la fonction exponentielle.)** (French) JFM 05.0248.01
C. R. LXXVII, 18-24 (1873); C. R. LXXVII, 74-79, 226-233, 285-293 (1873).

Eine Aufgabe, welche als eine Verallgemeinerung des Problems der Annäherung durch algebraische Kettenbrüche angesehen werden kann, ist folgende: „Die $n$ rationalen Brüche

$$\frac{\Phi_1(x)}{\Phi(x)}, \frac{\Phi_2(x)}{\Phi(x)}, \cdots \frac{\Phi_n(x)}{\Phi(x)}$$

als Näherungswerthe der $n$ Functionen $\varphi_1(x), \varphi_2(x), \cdots \varphi_n(x)$ so zu bestimmen, dass die Reihenentwickelungen nach steigenden Potenzen von $x$ bis zur Potenz $x^M$ übereinstimmen". Es werde vorausgesetzt, dass sich die Functionen $\varphi(x)$ in Reihen von der Form $\alpha + \beta x + \gamma x^2 + \cdots$ entwickeln lassen, und man mache

$$\Phi(x) = Ax^m + Bx^{m-1} + \cdots + Kx + L.$$

Dann kann man im Allgemeinen über die Coefficienten $A, B, \cdots L$ so verfügen, dass in den Producten $\varphi_i(x)\Phi(x)$ die Glieder mit

$$x^M, x^{M-1}, \cdots x^{M-\mu_i+1},$$

wo $\mu_i$ irgend eine ganze Zahl ist, verschwinden. So bildet man $\mu_i$ homogene Gleichungen ersten Grades und hat

$$\varphi_i(x)\Phi(x) = \Phi_i(x) + \varepsilon_1 x^{M+1} + \varepsilon_2 x^{M+2} + \cdots,$$

wo $\varepsilon_1, \varepsilon_2, \cdots$ Constanten, $\Phi_i(x)$ ein ganzes Polynom vom Grade $M - \mu_i$. Da aber hieraus folgt, dass

$$\varphi_i(x) = \frac{\Phi_i(x)}{\Phi(x)} + \frac{\varepsilon_1 x^{M+1} + \varepsilon_2 x^{M+2} + \cdots}{\Phi(x)},$$

so sieht man, dass die Reihenentwickelungen des rationalen Bruches und der Function in der That dieselben sein werden bis zu $x^M$, und da die Gesammtzahl der gemachten Bedingungen gleich $\mu_1 + \mu_2 + \cdots + \mu_n$ ist, so genügt es, die einzige Bedingung

$$\mu_1 + \mu_2 + \cdots + \mu_n = m$$

hinzuzufügen, wo die ganzzahligen $\mu_i$ bis dahin ganz willkürlich geblieben sind. Diese Betrachtung ist der Ausgangspunkt, den der Herr Verfasser für die in seiner Arbeit entwickelte Theorie der Exponentialfunction genommen hat, indem er nämlich das Obige anwendet auf die Grössen

$$\varphi_1(x) = e^{ax}, \varphi_2(x) = e^{bx}, \cdots \varphi_n(x) = e^{hx}.$$

Reviewer: Müller, Felix, Dr. (Berlin)

**MSC:**

# Felix Müller Jahrbuch der Mathematik

**Lindemann, F.**

**On the number $\pi$. (Ueber die Zahl $\pi$.)** (German) JFM 14.0369.04

**Klein Ann. XX, 213-225 (1882).**

In seiner Abhandlung: Sur la fonction exponentielle (C. R. Bd. LXXVII., s. F. d. M. V. (1873.) p.248, JFM 05.0248.01) hat Herr Hermite die Unmöglichkeit einer Relation von der Form ×

$$N_0e^{z_0}+N_1e^{z_1}+\cdots+N_ne^{z_n}=0$$

bewiesen, wo sowohl die $z$ als die $N$ als ganz vorausgesetzt werden. Herr Lindemann (siehe auch JFM 14.0369.02, JFM 14.0369.03) erweitert die hier gemachten Schlüsse und gelangt zu folgendem Satze: „Sind

$$f_1(z)=0,\ f_2(z)=0,\ \dots,\ f_s(z)=0$$

$s$ algebraische Gleichungen, von denen jede irreductibel und von der Form

$$z^n+a_1z^{n-1}\dots+a_n=0$$

ist, wo unter $a_1, a_2, \dots, a_n$ ganze Zahlen zu verstehen sind, werden ferner mit $z_i, z_i', z_i'', \dots$ die Wurzeln der Gleichung $f_i(z)=0$ bezeichnet, wird kurz

$$\Sigma e^{z_i}=e^{z_i}+e^{z_i'}+e^{z_i''}+\dots$$

gesetzt, bedeuten endlich $N_0, N_1, \dots, N_s$ beliebige ganze Zahlen, welche nicht sämmtlich gleich Null sind, so kann eine Relation von der Form

$$0=N_0+N_1\Sigma e^{z_1}+N_2\Sigma e^{z_2}+\cdots+N_s\Sigma e^{z_s}$$

nicht bestehen, es sei denn, dass eine der Grössen $z$ gleich Null ist."

Ersetzt man die Gleichungen $f_i(z)=0$ durch diejenigen irreduciblen Gleichungen, welche bez. von den Zahlen

$$Z_1=z_1, Z_2=z_1+z_2, Z_3=z_1+z_2+z_3, \dots, Z_n=z_1+z_2\cdots+z_n$$

befriedigt werden, so führt dieser besondere Fall zu dem Satze: „Ist $z$ eine von Null verschiedene rationale oder algebraisch irrationale Zahl, so ist $e^z$ immer transcendent." Damit ist bewiesen, dass die Ludolph'sche Zahl $\pi$ eine transcendente Zahl ist. Die angeführten Sätze bleiben bestehen, wenn man unter den $N_i$ nicht ganze oder rationale, sondern beliebige algebraisch-irrationale Zahlen versteht. Analog folgt aus dem obigen Satze der folgende: „Versteht man unter $N_0, N_1, \dots, N_n$ beliebige, und unter $z_0, z_1, \dots, z_n$ beliebige, von einander verschiedene (reelle oder complexe) algebraische Zahlen, so kann eine Relation von der Form

$$0=N_0e^{z_0}+N_1e^{z_1}+\cdots+N_ne^{z_n}$$

nicht bestehen, es sei denn, dass die $N_i$ sämmtlich gleich Null werden."

Reviewer: Müller, F.; Dr. (Berlin)

# Hermite p.77

» Il en résulte qu'on ne peut, en général, admettre que le déterminant proposé $\Delta$ s'annule, car les quantités $P = f(p)$, $Q = f(q), \ldots$, fonctions entières semblables des racines $p, q, \ldots$, de l'équation dérivée $f'(x) = 0$ seront comme ces racines différentes entre elles. C'est ce qu'il fallait établir pour démontrer l'impossibilité de toute relation de la forme

$$N + e^a N_1 + e^b N_2 + \ldots + e^h N_n = 0,$$

et arriver ainsi à prouver *que le nombre e ne peut être racine d'une équation algébrique de degré quelconque à coefficients entiers.*

# Hermite p.77

» Il en résulte qu'on ne peut, en général, admettre que le déterminant proposé $\Delta$ s'annule, car les quantités $P = f(p)$, $Q = f(q), \ldots$, fonctions entières semblables des racines $p, q, \ldots$, de l'équation dérivée $f'(x) = 0$ seront comme ces racines différentes entre elles. C'est ce qu'il fallait établir pour démontrer l'impossibilité de toute relation de la forme

$$N + e^a N_1 + e^b N_2 + \ldots + e^h N_n = 0,$$

et arriver ainsi à prouver *que le nombre e ne peut être racine d'une équation algébrique de degré quelconque à coefficients entiers.*

» Mais une autre voie conduira à une seconde démonstration plus rigoureuse ; on peut en effet, comme on va le voir, étendre aux fractions ration-

# Hermite p.77 – 78

» Il en résulte qu'on ne peut, en général, admettre que le déterminant proposé $\Delta$ s'annule, car les quantités $P=f(p)$, $Q=f(q)$,..., fonctions entières semblables des racines $p$, $q$,..., de l'équation dérivée $f'(x)=0$ seront comme ces racines différentes entre elles. C'est ce qu'il fallait établir pour démontrer l'impossibilité de toute relation de la forme

$$N + e^a N_1 + e^b N_2 + \ldots + e^h N_n = 0,$$

et arriver ainsi à prouver *que le nombre e ne peut être racine d'une équation algébrique de degré quelconque à coefficients entiers.*

» Mais une autre voie conduira à une seconde démonstration plus rigoureuse; on peut en effet, comme on va le voir, étendre aux fractions rationnelles

$$\frac{\Phi_1(x)}{\Phi(x)}, \quad \frac{\Phi_2(x)}{\Phi(x)}, \ldots, \quad \frac{\Phi_n(x)}{\Phi(x)}$$

le mode de formation des réduites donné par la théorie des fractions continues, et par là mettre plus complétement en évidence le caractère arithmétique d'une irrationnelle non algébrique. Dans cet ordre d'idées, M. Liouville a déjà obtenu un théorème remarquable qui est l'objet de son travail intitulé : *Sur des classes très-étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnelles algébriques* (*), et je rappellerai aussi que l'illustre géomètre a démontré le premier la proposition qui est le sujet de ces recherches pour les cas de l'équation du second degré et de



l'équation bicarrée [*Journal de Mathématiques* (*Note sur l'irrationnalité du nombre e*, t. V, p. 192)]. Sous le point de vue auquel je me suis placé, voici la première proposition à établir.

# Rational approximations to a real number

If $x$ is a rational number, there is a constant $c > 0$ such that for any $p/q \in \mathbb{Q}$ with $p/q \neq x$, we have $|x - p/q| \geq c/q$.

**Proof** : write $x = a/b$ and set $c = 1/b$.

If $x$ is a real irrational number, there are infinitely many $p/q \in \mathbb{Q}$ with $|x - p/q| < 1/q^2$.

The best rational approximations $p/q$ are given by the algorithm of continued fraction.

With a single real number $x$, it amounts to the same to investigate $|x - \frac{p}{q}|$ or $|qx - p|$ for $p$, $q$ in $\mathbb{Z}$, $q > 0$.

# Rational approximations to a real number

If $x$ is a rational number, there is a constant $c > 0$ such that for any $p/q \in \mathbb{Q}$ with $p/q \neq x$, we have $|x - p/q| \geq c/q$.

**Proof** : write $x = a/b$ and set $c = 1/b$.

If $x$ is a real irrational number, there are infinitely many $p/q \in \mathbb{Q}$ with $|x - p/q| < 1/q^2$.

The best rational approximations $p/q$ are given by the algorithm of continued fraction.

With a single real number $x$, it amounts to the same to investigate $|x - \frac{p}{q}|$ or $|qx - p|$ for $p$, $q$ in $\mathbb{Z}$, $q > 0$.

# Simultaneous approximation to a tuple of real numbers

Two generalisations of the problem in higher dimension.
Given real numbers $x_1, \ldots, x_m$, we may either consider

$$\max_{1\le i\le m} \left| x_i - \frac{p_i}{q} \right|,$$

for $p_1, \ldots, p_m, q$ in $\mathbb{Z}$ with $q > 0$, which is the simultaneous approximation of the tuple $(x_1, \ldots, x_m)$ by rational numbers with the same denominator, or else

$$|p_1 x_1 + \cdots + p_m x_m - q|$$

$p_1, \ldots, p_m, q$ in $\mathbb{Z}$ not all zero.
For power series, the first one corresponds to Padé approximants of type II, the second one corresponds to Padé approximants of type I.

# Padé approximants

Charles Hermite

(1822 – 1901)

Henri Padé

(1863 – 1953)

Kurt Mahler

(1903 – 1988)

1873, Hermite : type II, transcendence of $e$

1893, Hermite : type I, linear forms exponential function

1967, Mahler : application of type I to transcendence.

# Rational approximation to a single number

Continued fractions (Leonhard Euler)

Farey dissection (Sir John Farey)

Dirichlet's Box Principle (Gustav Lejeune – Dirichlet)

Geometry of numbers (Hermann Minkowski)

Euler

(1707 – 1783)

Farey

(1766 – 1826)

Dirichlet

(1805 – 1859)

Minkowski

(1864–1909)

# The algorithm of continued fractions

Let $x \in \mathbb{R}$. Euclidean division of $x$ by $1$ :

$$x = \lfloor x \rfloor + \{x\} \quad \text{with } \lfloor x \rfloor \in \mathbb{Z} \text{ and } 0 \leq \{x\} < 1.$$

If $x$ is not an integer, then $\{x\} \neq 0$. Set $x_1 = \frac{1}{\{x\}}$, so that

$$x = \lfloor x \rfloor + \frac{1}{x_1} \quad \text{with } \lfloor x \rfloor \in \mathbb{Z} \text{ and } x_1 > 1.$$

If $x_1$ is not an integer, set $x_2 = \frac{1}{\{x_1\}}$ :

$$x = \lfloor x \rfloor + \cfrac{1}{\lfloor x_1 \rfloor + \cfrac{1}{x_2}} \quad \text{with } x_2 > 1$$

# The algorithm of continued fractions

Let $x \in \mathbb{R}$. Euclidean division of $x$ by $1$ :

$$x = \lfloor x \rfloor + \{x\} \quad \text{with } \lfloor x \rfloor \in \mathbb{Z} \text{ and } 0 \le \{x\} < 1.$$

If $x$ is not an integer, then $\{x\} \neq 0$. Set $x_1 = \frac{1}{\{x\}}$, so that

$$x = \lfloor x \rfloor + \frac{1}{x_1} \quad \text{with } \lfloor x \rfloor \in \mathbb{Z} \text{ and } x_1 > 1.$$

If $x_1$ is not an integer, set $x_2 = \frac{1}{\{x_1\}}$ :

$$x = \lfloor x \rfloor + \cfrac{1}{\lfloor x_1 \rfloor + \cfrac{1}{x_2}} \quad \text{with } x_2 > 1$$

# The algorithm of continued fractions

Let $x \in \mathbb{R}$. Euclidean division of $x$ by $1$ :

$$x = \lfloor x \rfloor + \{x\} \quad \text{with } \lfloor x \rfloor \in \mathbb{Z} \text{ and } 0 \leq \{x\} < 1.$$

If $x$ is not an integer, then $\{x\} \neq 0$. Set $x_1 = \dfrac{1}{\{x\}}$, so that

$$x = \lfloor x \rfloor + \frac{1}{x_1} \quad \text{with } \lfloor x \rfloor \in \mathbb{Z} \text{ and } x_1 > 1.$$

If $x_1$ is not an integer, set $x_2 = \dfrac{1}{\{x_1\}}$ :

$$x = \lfloor x \rfloor + \cfrac{1}{\lfloor x_1 \rfloor + \cfrac{1}{x_2}} \quad \text{with } x_2 > 1$$

# Continued fraction expansion

Set $a_0 = \lfloor x \rfloor$ and $a_i = \lfloor x_i \rfloor$ for $i \geq 1$.

Then :

$$x = \lfloor x \rfloor + \cfrac{1}{\lfloor x_1 \rfloor + \cfrac{1}{\lfloor x_2 \rfloor + \cfrac{1}{\ddots}}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

the algorithm stops after finitely many steps if and only if $x$ is rational.

We use the notation

$$x = [a_0,\ a_1,\ a_2,\ a_3, \dots]$$

Remark : if $a_k \geq 2$, then

$[a_0,\ a_1,\ a_2,\ a_3, \dots, a_k] = [a_0,\ a_1,\ a_2,\ a_3, \dots, a_k - 1, 1]$.

# Continued fraction expansion

Set $a_0 = \lfloor x \rfloor$ and $a_i = \lfloor x_i \rfloor$ for $i \geq 1$.
Then :

$$x = \lfloor x \rfloor + \cfrac{1}{\lfloor x_1 \rfloor + \cfrac{1}{\lfloor x_2 \rfloor + \cfrac{1}{\ddots}}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

the algorithm stops after finitely many steps if and only if $x$ is rational.

We use the notation

$$x = [a_0,\ a_1,\ a_2,\ a_3, \ldots]$$

Remark : if $a_k \geq 2$, then
$[a_0,\ a_1,\ a_2,\ a_3, \ldots, a_k] = [a_0,\ a_1,\ a_2,\ a_3, \ldots, a_k - 1, 1]$.

# Continued fraction expansion

Set $a_0 = \lfloor x \rfloor$ and $a_i = \lfloor x_i \rfloor$ for $i \geq 1$.
Then :

$$x = \lfloor x \rfloor + \cfrac{1}{\lfloor x_1 \rfloor + \cfrac{1}{\lfloor x_2 \rfloor + \cfrac{1}{\ddots}}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

the algorithm stops after finitely many steps if and only if $x$ is rational.
We use the notation

$$x = [a_0,\ a_1,\ a_2,\ a_3, \dots]$$

Remark : if $a_k \geq 2$, then
$[a_0,\ a_1,\ a_2,\ a_3, \dots, a_k] = [a_0,\ a_1,\ a_2,\ a_3, \dots, a_k - 1, 1]$.

# Continued fraction expansion

Set $a_0 = \lfloor x \rfloor$ and $a_i = \lfloor x_i \rfloor$ for $i \geq 1$.
Then :

$$x = \lfloor x \rfloor + \cfrac{1}{\lfloor x_1 \rfloor + \cfrac{1}{\lfloor x_2 \rfloor + \cfrac{1}{\ddots}}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

the algorithm stops after finitely many steps if and only if $x$ is rational.
We use the notation

$$x = [a_0,\ a_1,\ a_2,\ a_3, \dots]$$

Remark : if $a_k \geq 2$, then
$[a_0,\ a_1,\ a_2,\ a_3, \dots, a_k] = [a_0,\ a_1,\ a_2,\ a_3, \dots, a_k - 1, 1]$.

# Continued fractions : the convergents

Given rational integers $a_0, a_1, \ldots, a_n$ with $a_i \geq 1$ for $i \geq 1$, the finite continued fraction

$$[a_0,\ a_1,\ a_2,\ a_3, \ldots, a_n]$$

can be written

$$\frac{P_n(a_0, a_1, \ldots, a_n)}{Q_n(a_1, a_2, \ldots, a_n)}$$

where $P_n$ and $Q_n$ are polynomials with integer coefficients. We wish to write these polynomials explicitly.

# Continued fractions : the convergents

Let $\mathbb{F}$ be a field, $Z_0, Z_1, \ldots$ variables. We will define polynomials $P_n$ and $Q_n$ in $\mathbb{F}[Z_0, \ldots, Z_n]$ and $\mathbb{F}[Z_1, \ldots, Z_n]$ respectively such that

$$[Z_0, Z_1, \ldots, Z_n] = \frac{P_n}{Q_n}.$$

Here are the first values :

$$P_0 = Z_0, \quad Q_0 = 1, \quad \frac{P_0}{Q_0} = Z_0;$$

$$P_1 = Z_0 Z_1 + 1, \quad Q_1 = Z_1, \quad \frac{P_1}{Q_1} = Z_0 + \frac{1}{Z_1};$$

$$P_2 = Z_0 Z_1 Z_2 + Z_2 + Z_0, \quad Q_2 = Z_1 Z_2 + 1, \quad \frac{P_2}{Q_2} = Z_0 + \frac{1}{Z_1 + \frac{1}{Z_2}}.$$

# Continued fractions : the convergents

Let $\mathbb{F}$ be a field, $Z_0, Z_1, \ldots$ variables. We will define polynomials $P_n$ and $Q_n$ in $\mathbb{F}[Z_0, \ldots, Z_n]$ and $\mathbb{F}[Z_1, \ldots, Z_n]$ respectively such that

$$[Z_0, Z_1, \ldots, Z_n] = \frac{P_n}{Q_n}.$$

Here are the first values :

$$P_0 = Z_0, \quad Q_0 = 1, \quad \frac{P_0}{Q_0} = Z_0;$$

$$P_1 = Z_0 Z_1 + 1, \quad Q_1 = Z_1, \quad \frac{P_1}{Q_1} = Z_0 + \frac{1}{Z_1};$$

$$P_2 = Z_0 Z_1 Z_2 + Z_2 + Z_0, \quad Q_2 = Z_1 Z_2 + 1, \quad \frac{P_2}{Q_2} = Z_0 + \cfrac{1}{Z_1 + \cfrac{1}{Z_2}}.$$

# Continued fractions : the convergents

Let $\mathbb{F}$ be a field, $Z_0, Z_1, \ldots$ variables. We will define polynomials $P_n$ and $Q_n$ in $\mathbb{F}[Z_0, \ldots, Z_n]$ and $\mathbb{F}[Z_1, \ldots, Z_n]$ respectively such that

$$[Z_0, Z_1, \ldots, Z_n] = \frac{P_n}{Q_n}.$$

Here are the first values :

$$P_0 = Z_0, \quad Q_0 = 1, \quad \frac{P_0}{Q_0} = Z_0;$$

$$P_1 = Z_0 Z_1 + 1, \quad Q_1 = Z_1, \quad \frac{P_1}{Q_1} = Z_0 + \frac{1}{Z_1};$$

$$P_2 = Z_0 Z_1 Z_2 + Z_2 + Z_0, \quad Q_2 = Z_1 Z_2 + 1, \quad \frac{P_2}{Q_2} = Z_0 + \cfrac{1}{Z_1 + \cfrac{1}{Z_2}}.$$

# Continued fractions : the convergents

Let $\mathbb{F}$ be a field, $Z_0, Z_1, \dots$ variables. We will define polynomials $P_n$ and $Q_n$ in $\mathbb{F}[Z_0, \dots, Z_n]$ and $\mathbb{F}[Z_1, \dots, Z_n]$ respectively such that

$$[Z_0, Z_1, \dots, Z_n] = \frac{P_n}{Q_n}.$$

Here are the first values :

$$P_0 = Z_0, \quad Q_0 = 1, \quad \frac{P_0}{Q_0} = Z_0;$$

$$P_1 = Z_0 Z_1 + 1, \quad Q_1 = Z_1, \quad \frac{P_1}{Q_1} = Z_0 + \frac{1}{Z_1};$$

$$P_2 = Z_0 Z_1 Z_2 + Z_2 + Z_0, \quad Q_2 = Z_1 Z_2 + 1, \quad \frac{P_2}{Q_2} = Z_0 + \cfrac{1}{Z_1 + \cfrac{1}{Z_2}}.$$

# Continued fractions : the convergents

$$P_3 = Z_0Z_1Z_2Z_3 + Z_2Z_3 + Z_0Z_3 + Z_0Z_1 + 1,$$

$$Q_3 = Z_1Z_2Z_3 + Z_3 + Z_1,$$

$$\frac{P_3}{Q_3} = Z_0 + \cfrac{1}{Z_1 + \cfrac{1}{Z_2 + \cfrac{1}{Z_3}}}.$$

$$P_2 = Z_2P_1 + P_0, \quad Q_2 = Z_2Q_1 + Q_0.$$

$$P_3 = Z_3P_2 + P_1, \quad Q_3 = Z_3Q_2 + Q_1.$$

# Continued fractions : the convergents

$$P_3 = Z_0Z_1Z_2Z_3 + Z_2Z_3 + Z_0Z_3 + Z_0Z_1 + 1,$$

$$Q_3 = Z_1Z_2Z_3 + Z_3 + Z_1,$$

$$\frac{P_3}{Q_3} = Z_0 + \cfrac{1}{Z_1 + \cfrac{1}{Z_2 + \cfrac{1}{Z_3}}}.$$

$$P_2 = Z_2P_1 + P_0, \quad Q_2 = Z_2Q_1 + Q_0.$$

$$P_3 = Z_3P_2 + P_1, \quad Q_3 = Z_3Q_2 + Q_1.$$

# Continued fractions : the convergents

$$P_3 = Z_0 Z_1 Z_2 Z_3 + Z_2 Z_3 + Z_0 Z_3 + Z_0 Z_1 + 1,$$

$$Q_3 = Z_1 Z_2 Z_3 + Z_3 + Z_1,$$

$$\frac{P_3}{Q_3} = Z_0 + \cfrac{1}{Z_1 + \cfrac{1}{Z_2 + \cfrac{1}{Z_3}}}.$$

$$P_2 = Z_2 P_1 + P_0, \quad Q_2 = Z_2 Q_1 + Q_0.$$

$$P_3 = Z_3 P_2 + P_1, \quad Q_3 = Z_3 Q_2 + Q_1.$$

# Continued fractions : the convergents

$$P_3 = Z_0Z_1Z_2Z_3 + Z_2Z_3 + Z_0Z_3 + Z_0Z_1 + 1,$$

$$Q_3 = Z_1Z_2Z_3 + Z_3 + Z_1,$$

$$\frac{P_3}{Q_3} = Z_0 + \cfrac{1}{Z_1 + \cfrac{1}{Z_2 + \cfrac{1}{Z_3}}}.$$

$$P_2 = Z_2P_1 + P_0, \quad Q_2 = Z_2Q_1 + Q_0.$$

$$P_3 = Z_3P_2 + P_1, \quad Q_3 = Z_3Q_2 + Q_1.$$

# Continued fractions : the convergents

For $n = 2$ and $n = 3$, we observe that

$$P_n = Z_n P_{n-1} + P_{n-2}, \quad Q_n = Z_n Q_{n-1} + Q_{n-2}.$$

This will be our definition of $P_n$ and $Q_n$.

In matrix form, it is

$$\begin{pmatrix} P_n \\ Q_n \end{pmatrix} = \begin{pmatrix} P_{n-1} & P_{n-2} \\ Q_{n-1} & Q_{n-2} \end{pmatrix} \begin{pmatrix} Z_n \\ 1 \end{pmatrix}.$$

# Continued fractions : the convergents

For $n = 2$ and $n = 3$, we observe that

$$P_n = Z_n P_{n-1} + P_{n-2}, \quad Q_n = Z_n Q_{n-1} + Q_{n-2}.$$

This will be our definition of $P_n$ and $Q_n$.

In matrix form, it is

$$\begin{pmatrix} P_n \\ Q_n \end{pmatrix} = \begin{pmatrix} P_{n-1} & P_{n-2} \\ Q_{n-1} & Q_{n-2} \end{pmatrix} \begin{pmatrix} Z_n \\ 1 \end{pmatrix}.$$

# Definition of $P_n$ and $Q_n$

With $2 \times 2$ matrices :

$$\begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} = \begin{pmatrix} P_{n-1} & P_{n-2} \\ Q_{n-1} & Q_{n-2} \end{pmatrix} \begin{pmatrix} Z_n & 1 \\ 1 & 0 \end{pmatrix}.$$

Hence :

$$\begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} = \begin{pmatrix} Z_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} Z_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} Z_n & 1 \\ 1 & 0 \end{pmatrix}.$$

# Definition of $P_n$ and $Q_n$

With $2 \times 2$ matrices :

$$\begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} = \begin{pmatrix} P_{n-1} & P_{n-2} \\ Q_{n-1} & Q_{n-2} \end{pmatrix} \begin{pmatrix} Z_n & 1 \\ 1 & 0 \end{pmatrix}.$$

Hence :

$$\begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} = \begin{pmatrix} Z_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} Z_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} Z_n & 1 \\ 1 & 0 \end{pmatrix}.$$

# Continued fractions : definition of $P_n$ and $Q_n$

$$\begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} = \begin{pmatrix} Z_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} Z_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} Z_n & 1 \\ 1 & 0 \end{pmatrix} \quad \text{for } n \geq -1.$$

In particular

$$\begin{pmatrix} P_{-1} & P_{-2} \\ Q_{-1} & Q_{-2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

One checks $[Z_0, Z_1, \ldots, Z_n] = P_n/Q_n$ for all $n \geq 0$.

# Continued fractions : definition of $P_n$ and $Q_n$

$$\begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} = \begin{pmatrix} Z_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} Z_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} Z_n & 1 \\ 1 & 0 \end{pmatrix} \quad \text{for } n \geq -1.$$

In particular

$$\begin{pmatrix} P_{-1} & P_{-2} \\ Q_{-1} & Q_{-2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

One checks $[Z_0, Z_1, \ldots, Z_n] = P_n/Q_n$ for all $n \geq 0$.

# Continued fractions : definition of $P_n$ and $Q_n$

$$\begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} = \begin{pmatrix} Z_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} Z_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} Z_n & 1 \\ 1 & 0 \end{pmatrix} \quad \text{for } n \geq -1.$$

In particular

$$\begin{pmatrix} P_{-1} & P_{-2} \\ Q_{-1} & Q_{-2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

One checks $[Z_0, Z_1, \ldots, Z_n] = P_n/Q_n$ for all $n \geq 0$.

# Simple continued fraction of a real number

For

$$x = [a_0,\ a_1,\ a_2, \ldots, a_n]$$

we have

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

with

$$p_n = P_n(a_0, a_1, \ldots, a_n) \quad \text{and} \quad q_n = Q_n(a_1, \ldots, a_n).$$

# Simple continued fraction of a real number

For

$$x = [a_0,\ a_1,\ a_2, \ldots, a_n, \ldots]$$

the rational numbers in the sequence

$$\frac{p_n}{q_n} = [a_0,\ a_1,\ a_2, \ldots, a_n] \qquad (k = 1, 2, \ldots)$$

give rational approximations for $x$ which are the best ones when comparing the quality of the approximation and the size of the denominator.

$a_0, a_1, a_2, \ldots$ are the *partial quotients*,
$p_n/q_n$ $(n \geq 0)$ are the *convergents*.
$x_n = [a_n, a_{n+1}, \ldots]$ $(n \geq 0)$ are the *complete quotients*.
Hence

$$x = [a_0, a_1, \ldots, a_{n-1}, x_n] = \frac{x_n p_{n-1} + p_{n-2}}{x_n q_{n-1} + q_{n-2}}.$$

# Simple continued fraction of a real number

For

$$x = [a_0,\ a_1,\ a_2, \dots, a_n, \dots]$$

the rational numbers in the sequence

$$\frac{p_n}{q_n} = [a_0,\ a_1,\ a_2, \dots, a_n] \qquad (k = 1, 2, \dots)$$

give rational approximations for $x$ which are the best ones when comparing the quality of the approximation and the size of the denominator.

$a_0, a_1, a_2, \dots$ are the *partial quotients*,

$p_n/q_n$ $(n \geq 0)$ are the *convergents*.

$x_n = [a_n, a_{n+1}, \dots]$ $(n \geq 0)$ are the *complete quotients*.

Hence

$$x = [a_0, a_1, \dots, a_{n-1}, x_n] = \frac{x_n p_{n-1} + p_{n-2}}{x_n q_{n-1} + q_{n-2}}.$$

# Simple continued fraction of a real number

For

$$x = [a_0,\ a_1,\ a_2, \ldots, a_n, \ldots]$$

the rational numbers in the sequence

$$\frac{p_n}{q_n} = [a_0,\ a_1,\ a_2, \ldots, a_n] \qquad (k = 1, 2, \ldots)$$

give rational approximations for $x$ which are the best ones when comparing the quality of the approximation and the size of the denominator.

$a_0, a_1, a_2, \ldots$ are the *partial quotients*,

$p_n/q_n$ $(n \geq 0)$ are the *convergents*.

$x_n = [a_n, a_{n+1}, \ldots]$ $(n \geq 0)$ are the *complete quotients*.

Hence

$$x = [a_0, a_1, \ldots, a_{n-1}, x_n] = \frac{x_n p_{n-1} + p_{n-2}}{x_n q_{n-1} + q_{n-2}}.$$

# Connection with the Euclidean algorithm

If $x$ is rational, $x = \frac{p}{q}$, this process is nothing else than Euclidean algorithm of dividing $p$ by $q$ :

$$p = a_0 q + r_0, \quad 0 \leq r_0 < q.$$

If $r_0 \neq 0$,

$$x_1 = \frac{q}{r_0} > 1.$$

Euclide :
($\sim$ -306, $\sim$ -283)

$$q = a_1 r_0 + r_1, \quad x_2 = \frac{r_0}{r_1}.$$

# Continued fractions and rational approximation

From

$$q_n = a_n q_{n-1} + q_{n-2} \quad \text{and} \quad q_n x - p_n = \frac{(-1)^n}{a_{n+1} q_n + q_{n-1}}$$

one deduces the inequalities

$$a_n q_{n-1} \le q_n \le (a_n + 1) q_{n-1}$$

and

$$\frac{1}{(a_{n+1}+2)q_n} < \frac{1}{q_{n+1}+q_n} < |q_n x - p_n| < \frac{1}{q_{n+1}} < \frac{1}{a_{n+1} q_n}.$$

# Convergents are the best rational approximations

Let $p_n/q_n$ be the $n$–th convergent of the continued fraction expansion of an irrational number $x$.

**Theorem**. Let $a/b$ be any rational number such that $1 \leq b \leq q_n$. Then :

$$|q_n x - p_n| \leq |bx - a|$$

with equality if and only if $(a, b) = (p_n, q_n)$.

**Corollary**. For $1 \leq b \leq q_n$ we have

$$\left| x - \frac{p_n}{q_n} \right| \leq \left| x - \frac{a}{b} \right|$$

with equality if and only if $(a, b) = (p_n, q_n)$.

# Convergents are the best rational approximations

Let $p_n/q_n$ be the $n$–th convergent of the continued fraction expansion of an irrational number $x$.

**Theorem**. Let $a/b$ be any rational number such that $1 \leq b \leq q_n$. Then :

$$|q_n x - p_n| \leq |bx - a|$$

with equality if and only if $(a, b) = (p_n, q_n)$.

**Corollary**. For $1 \leq b \leq q_n$ we have

$$\left| x - \frac{p_n}{q_n} \right| \leq \left| x - \frac{a}{b} \right|$$

with equality if and only if $(a, b) = (p_n, q_n)$.

# Power series

Let $\mathbb{F}$ be a field. For $P/Q \in \mathbb{F}(T)$, define

$$\left|\frac{P}{Q}\right| = e^{\deg P - \deg Q}$$

with $|0| = 0$. The completion of $\mathbb{F}(T)$ for this absolute value is $\mathbb{F}((1/T))$ ; for $x \in \mathbb{F}((1/T))$ with $x \neq 0$ write

$$x = a_{k_0} T^{k_0} + a_{k_0-1} T^{k_0-1} + \cdots = \sum_{k \leq k_0} a_k T^k$$

with $k_0 \in \mathbb{Z}$, $a_k \in \mathbb{F}$ for all $k \leq k_0$ and $a_{k_0} \neq 0$. Then $|x| = e^{k_0}$.

# Analogy : numbers – series

$$\begin{array}{ccccc} \mathbb{Z} & \subset & \mathbb{Q} & \subset & \mathbb{R} \\ \updownarrow & & \updownarrow & & \updownarrow \\ \mathbb{F}[T] & \subset & \mathbb{F}(T) & \subset & \mathbb{F}((1/T)) \end{array}$$

$$\left|\frac{a}{b}\right| = \max\{|a|, |b|\}, \qquad \sum_{n \geq -k} a_n g^{-n},$$

$$\left|\frac{P}{Q}\right| = e^{\deg P - \deg Q} \qquad \sum_{n \geq -k} a_n T^{-n}.$$

# Analogy : numbers – functions

Rolf Nevanlinna

Paul Vojta

Wolfgang M. Schmidt

There is a formal analogy between Nevanlinna theory and Diophantine approximation. Via Vojta's dictionary, the Second Main Theorem in Nevanlinna theory corresponds to Schmidt's Subspace Theorem in Diophantine approximation.

# Regular continued fraction of a power series

Notice that any element in $\mathbb{F}(T)$ has a unique continued fraction expansion $[A_0, A_1, \ldots, A_n]$ with $A_i \in \mathbb{F}[T]$ for $i \geq 0$ and $\deg A_i \geq 1$ for $i \geq 1$.
For $x \in \mathbb{F}((1/T))$ :

$$x = [A_0, A_1, \ldots].$$

*Partial quotients* : $A_n$.
*Convergents* : $P_n/Q_n$ with $P_n = P_n(A_0, A_1, \ldots, A_n)$ and $Q_n = Q_n(A_1, \ldots, A_n)$.
*Complete quotients* : $x_n = [A_n, A_{n+1}, \ldots]$.
Hence

$$x = [A_0, A_1, \ldots, A_{n-1}, x_n] = \frac{x_n P_{n-1} + P_{n-2}}{x_n Q_{n-1} + Q_{n-2}}.$$

# Diophantine approximation and continued fractions

*For* $x = [A_0, A_1, \dots] \in \mathbb{F}((1/T))$,

$$P_n = P_n(A_0, A_1, \dots, A_n), \quad Q_n = Q_n(A_1, \dots, A_n),$$

*we have*

$$|Q_n| = |A_n| \cdot |A_{n-1}| \cdots |A_1| \quad (n \geq 1)$$

*and*

$$\left| x - \frac{P_n}{Q_n} \right| = \frac{1}{|Q_n| \; |Q_{n+1}|} = \frac{1}{|A_{n+1}| \; |Q_n|^2} \quad (n \geq 0).$$

# Convergents are the best rational approximations

Let $P_n/Q_n$ be the $n$–th convergent of the continued fraction expansion of $x \in \mathbb{F}((T^{-1})) \setminus \mathbb{F}(T)$.

**Theorem**. Let $A/B$ be any element in $\mathbb{F}(T)$ such that $|B| \leq |Q_n|$. Then :

$$|Q_n x - P_n| \leq |Bx - A|$$

with equality if and only if $(A, B) = (P_n, Q_n)$.

**Corollary**. For $|B| \leq |Q_n|$ we have

$$\left| x - \frac{P_n}{Q_n} \right| \leq \left| x - \frac{A}{B} \right|$$

with equality if and only if $(A, B) = (P_n, Q_n)$.

# Convergents are the best rational approximations

Let $P_n/Q_n$ be the $n$–th convergent of the continued fraction expansion of $x \in \mathbb{F}((T^{-1})) \setminus \mathbb{F}(T)$.

**Theorem**. Let $A/B$ be any element in $\mathbb{F}(T)$ such that $|B| \leq |Q_n|$. Then :

$$|Q_n x - P_n| \leq |Bx - A|$$

with equality if and only if $(A, B) = (P_n, Q_n)$.

**Corollary**. For $|B| \leq |Q_n|$ we have

$$\left| x - \frac{P_n}{Q_n} \right| \leq \left| x - \frac{A}{B} \right|$$

with equality if and only if $(A, B) = (P_n, Q_n)$.

# Legendre Theorem

Adrien–Marie Legendre

(1752 – 1833)

**Real numbers** : *If*

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{2q^2},$$

*then* $p/q$ *is a convergent of* $x$.

**Power series** : *If*

$$\left| x - \frac{P}{Q} \right| < \frac{1}{|Q|^2},$$

*then* $P/Q$ *is a convergent of* $x$.

# Lagrange Theorem

Lagrange

(1736 – 1813)

**Real numbers** : *The continued fraction expansion of a real irrational number $x$ is ultimately periodic if and only if $x$ is quadratic.*

**Power series** : *If the continued fraction expansion of an element $x \in \mathbb{F}((T^{-1})) \setminus \mathbb{F}(T)$ is ultimately periodic, then $x$ is quadratic over $\mathbb{F}(T)$.*

The converse is true when the field has nonzero characteristic and is an algebraic extension of its prime field $\mathbb{F}_p$, but not otherwise.

# Pseudo–periodic expansion

An element $x \in \mathbb{F}((T^{-1})) \setminus \mathbb{F}(T)$ has a pseudo periodic expansion

$$[A_0, A_1, \ldots, A_{n-1}, B_1, \ldots, B_{2t}, aB_1, a^{-1}B_2, aB_3, \ldots, a^{-1}B_{2t},$$

$$a^2B_1, a^{-2}B_2, \ldots, a^{-2}B_{2t}, a^3B_1, a^{-3}B_2, \ldots]$$

if and only if there exist $R, S, T, U$ in $\mathbb{F}[T]$ with

$$x = \frac{Rx + S}{Tx + U}$$

where $\begin{pmatrix} R & S \\ T & U \end{pmatrix}$ has determinant $1$ and is not a multiple of the identity matrix.

If $D$ is polynomial which is irreducible over any quadratic extension of $\mathbb{F}$ then the regular continued fraction expansion of $\sqrt{D}$ is not pseudo–periodic.

# Pseudo–periodic expansion

An element $x \in \mathbb{F}((T^{-1})) \setminus \mathbb{F}(T)$ has a pseudo periodic expansion

$$[A_0, A_1, \ldots, A_{n-1}, B_1, \ldots, B_{2t}, aB_1, a^{-1}B_2, aB_3, \ldots, a^{-1}B_{2t},$$

$$a^2B_1, a^{-2}B_2, \ldots, a^{-2}B_{2t}, a^3B_1, a^{-3}B_2, \ldots]$$

if and only if there exist $R, S, T, U$ in $\mathbb{F}[T]$ with

$$x = \frac{Rx + S}{Tx + U}$$

where $\begin{pmatrix} R & S \\ T & U \end{pmatrix}$ has determinant $1$ and is not a multiple of the identity matrix.

If $D$ is polynomial which is irreducible over any quadratic extension of $\mathbb{F}$ then the regular continued fraction expansion of $\sqrt{D}$ is not pseudo–periodic.

# References on continued fractions of power series

Alain Lasjaunias

A. Lasjaunias.
A survey of Diophantine approximation in fields of power series.
*Monatsh. Math.*, 130(3) :211–229, 2000.

A. Lasjaunias.
A short survey on diophantine approximation in fields of formal numbers.
https://www.math.u-bordeaux.fr/~alasjaun/survey.pdf.

# References on continued fractions of power series

Wolfgang M. Schmidt

W. M. Schmidt.
On continued fractions and Diophantine approximation in power series fields.
*Acta Arith.*,
95(2) :139–166, 2000.

# Geometry of numbers

Hermann Minkowski

(1864–1909)

Reference :
Eva Bayer–Fluckiger.

Hermann Minkowski, Grand prix de l'Académie à 18 ans.

Tangente, n°111, Juillet-Août 2006.

http://alg-geo.epfl.ch/~bayer/files/MINKOWSKI.pdf

# Minkowski geometry of numbers

XX.

## Zur Geometrie der Zahlen.

(Mit Projektionsbildern auf einer Doppeltafel.)

(Verhandlungen des III. Internationalen Mathematiker-Kongresses. Heidelberg 1904. S. 164—173.)

Im folgenden möchte ich versuchen, in kurzen Zügen einen Bericht über ein eigenartiges, zahlreicher Anwendungen fähiges Kapitel der Zahlentheorie zu geben, ein Kapitel, von dem Charles Hermite einmal als der „introduction des variables continues dans la théorie des nombres" gesprochen hat. Einige hervorstechende Probleme darin betreffen die Abschätzung der kleinsten Beträge kontinuierlich veränderlicher Ausdrücke für ganzzahlige Werte der Variablen.

Die in dieses Gebiet fallenden Tatsachen sind zumeist einer geometrischen Darstellung fähig, und dieser Umstand ist für die in letzter Zeit hier erzielten Fortschritte derart maßgebend gewesen, daß ich geradezu das ganze Gebiet als die *Geometrie der Zahlen* bezeichnet habe.

H. Minkowski ICM 1904

# Parametric geometry of numbers : references

Wolfgang M. Schmidt

W. M. Schmidt.
Open problems in Diophantine approximation.
§1 : a viewpoint.

In *Diophantine approximations and transcendental numbers (Luminy, 1982)*, volume 31 of *Progr. Math.*, pages 271–287. Birkhäuser Boston, Boston, MA, 1983.

# Parametric geometry of numbers : references

Wolfgang M. Schmidt

Leo Summerer


W. M. Schmidt and L. Summerer.
Parametric geometry of numbers and applications.
*Acta Arith.*, 140(1) :67–91, 2009.

W. M. Schmidt and L. Summerer.
Diophantine approximation and parametric geometry of numbers.
*Monatsh. Math.*, 169(1) :51–104, 2013.

# Parametric geometry of numbers

Damien Roy

D. Roy.
On Schmidt and Summerer parametric geometry of numbers.
*Ann. of Math. (2)*, 182(2) :739–786, 2015.

# Parametric geometry of numbers

Aminata Keita

A. Keita.
Continued fractions and parametric geometry of numbers.
*J. Théor. Nombres Bordeaux* **29** (2017), 129–135.

A. Keita.
On a conjecture of Schmidt for the parametric geometry of numbers.
*Moscow Journal of Combinatorics and Number Theory* **6** *(2016), 166–176.*

https://www.idrc.ca/fr/article/preparer-la-prochaine-generation-de-scientifiques-africains

# Simultaneous approximation to a tuple of real numbers

For $\mathbf{u} = (u_1, \ldots, u_n)$ and $\mathbf{x} = (x_1, \ldots, x_n)$ in $\mathbb{R}^n$, set

$$\|\mathbf{u}\| = \max_{1 \le i \le n} |u_i| \quad \text{and} \quad \mathbf{x} \cdot \mathbf{u} = x_1 u_1 + \cdots + x_n u_n.$$

Given $\mathbf{u} \in \mathbb{R}^n$, we are interested in finding $\mathbf{x} \in \mathbb{Z}^n$ where $\|\mathbf{x}\|$ is not too large and $|\mathbf{x} \cdot \mathbf{u}|$ is as small as possible. In case $n = 2$, the answer is given by the theory of continued fractions. Say $\mathbf{u} = (u_1, u_2)$ with $u_1 \neq 0$, the best rational approximations are given by the quotients $p_n/q_n$ associated with the continued fraction of $u_2/u_1$.

# A convex body

For $n \geq 2$, in order to use Minkowski's geometry of numbers, we need a symmetric convex body. The idea behind parametric geometry of numbers (in $\mathbb{R}^n$) is to introduce a parameter $q \geq 0$ and to consider a family of convex bodies.
For $q > 0$, set

$$\mathcal{C}(e^q) = \left\{ \mathbf{x} \in \mathbb{R}^n \ \mid \ \|\mathbf{x}\| \leq 1, \ |\mathbf{x} \cdot \mathbf{u}| \leq e^{-q} \right\}.$$

*Best approximations* : given $q$, find $t$ as small as possible such that there exists $\mathbf{x} \in e^t \mathcal{C}(e^q) \setminus \{0\}$. In other words, $e^t$ is the first minimum of $\mathbb{Z}^n$ with respect to $\mathcal{C}(e^q)$.

# Successive minima

Let $\mathbf{u} \in \mathbb{R}^n$ with $\|\mathbf{u}\| = 1$.
Consider the successive minima of $\mathbb{Z}^n$ with respect to this body : define $L_{\mathbf{u},i}(q)$ the logarithm of the $i$-th minimum ; hence $L_{\mathbf{u},i}(q)$ is the smallest $t \geq 0$ such that the solutions $\mathbf{x} \in \mathbb{Z}^n$ of

$$\|\mathbf{x}\| \leq e^t, \ |\mathbf{x} \cdot \mathbf{u}| \leq e^{t-q}$$

span a subspace of dimension $\geq i$. The *combined graph* is the map

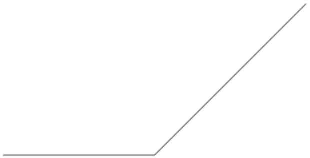
$$\begin{array}{rccc} \mathrm{L}_{\mathbf{u}} : & [0, \infty) & \longrightarrow & \mathbb{R}^n \\ & q & \longmapsto & (L_{\mathbf{u},1}(q), \ldots, L_{\mathbf{u},n}(q)). \end{array}$$

# Trajectory of a point

Trajectory of a point $\mathbf{x} \in \mathbb{Z}^n$ :

$$q \longmapsto L_{\mathbf{x}}(q) = \max\{\log|\mathbf{x}|\ ,\ q + \log|\mathbf{x}\cdot\mathbf{u}|\}.$$

Graph : straight horizontal segment from $0$ to $\log|\mathbf{x}| - \log|\mathbf{x}\cdot\mathbf{u}|$ with value $\log|\mathbf{x}|$, next a half line with slope $1$.

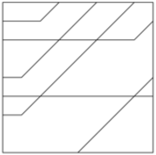


# Trajectories in a box

Consider all such trajectories for $\mathbf{x} \in \mathbb{Z}^n$.

Given a bounded subset of $\mathbb{R}^2$, only finitely many trajectories intersect it.

The intersection consists of horizontal segments and segments with slope $1$.



The combined graph $\mathrm{L}_{\mathbf{u}}$ consists to a union of subsets of some of these trajectories.
There are $n$ points above a given $q$.

# $n$–systems (according to D. Roy)

An $n$–*system* is a map

$$\begin{array}{rccc} P: & [0,\infty) & \longrightarrow & \mathbb{R}^n \\ & q & \longmapsto & (P_1(q),\dots,P_n(q)) \end{array}$$

such that, for each $q \geq 0$,

(S1) we have $0 \leq P_1(q) \leq \cdots \leq P_n(q)$ and $P_1(q) + \cdots + P_n(q) = q$,

(S2) there exist $\epsilon > 0$ and integers $k, \ell \in \{1,\dots,n\}$ such that

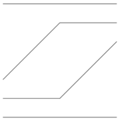
$$\mathbf{P}(t) = \begin{cases} \mathbf{P}(q) + (t-q)\mathbf{e}_\ell & \text{when } \max\{0, q-\epsilon\} \leq t \leq q, \\ \mathbf{P}(q) + (t-q)\mathbf{e}_k & \text{when } q \leq t \leq q+\epsilon, \end{cases}$$

where $\mathbf{e}_1 = (1,0,\dots,0), \ \dots \ , \mathbf{e}_n = (0,\dots,0,1)$,

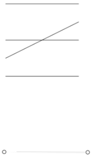
(S3) if $q > 0$ and if the integers $k$ and $\ell$ from (S2) satisfy $k > \ell$, then $P_\ell(q) = \cdots = P_k(q)$.

# $n$–systems

$k = \ell$



$k < \ell$

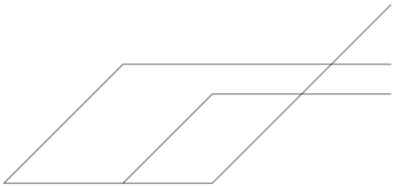


$k > \ell$.

Not allowed in case $k > \ell$:

# An example of a $3$–system

three segments (one horizontal, two with slope $1$)
three half lines (two horizontal, one with slope $1$)



# Roy's main result ($\mathbb{R}^n$)

**Theorem** (D. Roy, 2015) *Modulo the additive group of bounded functions, the class of combined graphs* $\mathrm{L}_{\mathbf{u}}$ *is the same as the class of* $n$*–systems.*

# Power series

$K = \mathbb{F}(T)$, $K_\infty = \mathbb{F}((1/T))$, $\mathbf{u} \in K_\infty^n$, $\|\mathbf{u}\| = 1$.

$$\mathcal{C}(e^q) = \left\{ \mathbf{x} \in \mathbb{K}_\infty^n \;\mid\; \|\mathbf{x}\| \leq 1,\; |\mathbf{x} \cdot \mathbf{u}| \leq e^{-q} \right\}.$$

Combined graph :

$$\mathrm{L}_{\mathbf{u}} : [0, \infty) \longrightarrow \mathbb{R}^n.$$

**Main Theorem** (with D. Roy) : *The set of maps* $\mathrm{L}_{\mathbf{u}}$ *with* $\|\mathbf{u}\| = 1$ *is the set of* $n$*–systems.*

# Perfect systems (K. Mahler, H. Jager)

Kurt Mahler

Henk Jager

(with Rob Tijdeman)

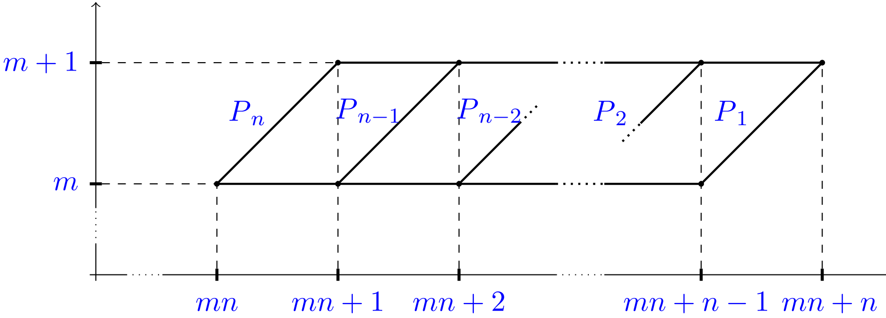
There is exactly one such $n$-system for which

$$P_1(q) = \left\lfloor \frac{q}{n} \right\rfloor \quad \text{and} \quad P_n(q) = \left\lceil \frac{q}{n} \right\rceil \quad \text{for each } q \in \mathbb{N}.$$

When $q \equiv 0 \mod n$, such a system necessarily has $P_1(q) = \cdots = P_n(q) = q/n$.

# Perfect systems

This figure shows the union of the graphs of $P_1, \ldots, P_n$ over an interval of the form $[mn, (m+1)n]$ with $m \in \mathbb{N}$.



# Example of a perfect system

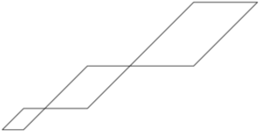
Suppose that $\mathbb{F}$ has characteristic zero. Let $\omega_1, \ldots, \omega_n$ be distinct elements of $\mathbb{F}$, and let $\mathbf{u} = \left(e^{\omega_1/T}, \ldots, e^{\omega_n/T}\right)$, where

$$e^{\omega/T} = \sum_{j=0}^{\infty} \frac{\omega^j}{j!} T^{-j} \in \mathbb{F}[[1/T]] \quad (\omega \in \mathbb{F}).$$

Then, we have $\|\mathbf{u}\| = 1$ and the combined graph $\mathbf{L}_\mathbf{u}$ is a perfect $n$-system.

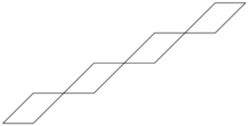
# Combined graph of a continued fraction

Continued fractions $[a_0, a_1, \ldots, a_m, \ldots]$ with $\deg a_0 = 0$, $\deg a_i \geq 1$ $(i \geq 1)$.



# Combined graph of a perfect continued fraction

Perfect continued fractions : $[a_0, a_1, \ldots, a_m, \ldots]$ with $\deg a_0 = 0$, $\deg a_i = 1$ $(i \geq 1)$.



Example (Fibonacci–like power series) :
$\theta = [0, T, T, \ldots] = 1/(T + \theta)$, root of $\theta^2 + T\theta - 1 = 0$.

# Littlewood's Conjecture

John Edensor Littlewood

(1885–1977)

**Littlewood's Conjecture** :
for any real numbers $\theta$ and $\phi$,
for any $\epsilon > 0$, there exists
$n \geq 1$ such that

$$n\|n\theta\| \, \|n\phi\| \leq \epsilon.$$

Here, $\| \cdot \|$ is the distance to the nearest integer.

# Counterexample for power series

Harold Davenport

(1907–1969)

Donald J. Lewis

(1926–2015)

**H. Davenport–D. Lewis** : there exists $\Theta$ and $\Phi$ in $\mathbb{R}((1/T))$ such that for any $N \in \mathbb{R}[T]$, we have

$$|N| \, \|N\Theta\| \, \|N\Phi\| \geq e^{-2}.$$

Here, $|\cdot|$ is the ultrametric absolute value on $\mathbb{R}((1/T))$ which is $e^{\deg(\cdot)}$ on $\mathbb{R}[T]$, while $\|\cdot\|$ is the distance to the nearest element in $\mathbb{R}[T]$.

# Explicit counterexample

Alan Baker

**A. Baker** : For any $N \in \mathbb{R}[T]$, we have

$$|N| \, \|Ne^{1/T}\| \, \|Ne^{2/T}\| \geq e^{-5}.$$

More generally, for any nonzero distinct real numbers $\lambda_1, \ldots, \lambda_r$, for any $N \in \mathbb{R}[T]$, we have

$$|N| \, \|Ne^{\lambda_1/T}\| \cdots \|Ne^{\lambda_r/T}\| \geq e^{-(r^3+r)/2}.$$

# Consequence of an adelic estimate (with Damien Roy)

Let $a_1(T), \ldots, a_n(T)$ be nonzero polynomials in $\mathbb{C}[T]$. Then, we have

$$\left| a_1(T)e^{\omega_1/T} + \cdots + a_n(T)e^{\omega_n/T} \right| \prod_{i=2}^{n} |a_i(T)| \geq C(n)^{-1}$$

and

$$|a_1(T)| \prod_{i=2}^{n} \left| a_1(T)e^{\omega_i/T} - a_i(T)e^{\omega_1/T} \right| \geq C(n)^{-(n-1)}$$

with $C(n) = \exp(n(n-1)/2)$.

Universita degli Studi Roma Tre *April 6, 2017*

http://www.rnta.eu/ThirdRNTA/index.html

The third mini symposium of the
Roman Number Theory Association

**Diophantine approximation and power series.**

*Michel Waldschmidt*

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