Tenth course: September 28, 2007. [14]

2.2.9 Diophantine Approximation: historical survey

References for this section are [3, 4, 2, 1].

Definition. *Given a real irrational number ϑ, a function $\varphi = \mathbb{N} \to \mathbb{R}_{>0}$ is an irrationality measure for ϑ if there exists an integer $q_0 > 0$ such that, for any $p/q \in \mathbb{Q}$ with $q \geq q_0$,*

$$\left| \vartheta - \frac{p}{q} \right| \geq \varphi(q).$$

Further, a real number κ is an irrationality exponent for ϑ if there exists a positive constant c such that the function c/q^κ is an irrationality measure for ϑ.

From Dirichlet's box principle (see (i)⇒(iv) in Lemma 1.6) it follows that any irrationality exponent κ satisfies $\kappa \geq 2$. Irrational quadratic numbers have irrationality exponent 2. It is known (see for instance [4] Th. 5F p. 22) that 2 is an irrationality exponent for an irrational real number ϑ if and only if the sequence of *partial quotients* $(a_0, a_1, \ldots)$ in the continued fraction expansion of ϑ is bounded: these are called the *badly approximable numbers*.

From Liouville's inequality in Lemma 2.13 it follows that any irrational algebraic real number α has a finite irrationality exponent $\leq d$. Liouville numbers are by definition exactly the irrational real numbers which have no finite irrationality exponent.

For any $\kappa \geq 2$, there are irrational real numbers ϑ for which κ is an irrationality exponent and is the best: no positive number less than κ is an irrationality exponent for ϑ. Examples due to Y. Bugeaud in connexion with the triadic Cantor set (see [6]) are

$$\sum_{n=0}^{\infty} 3^{-\lceil \lambda\kappa \rceil^n}$$

where λ is any positive real number.

The first significant improvement to Liouville's inequality is due to the Norwegian mathematician Axel Thue who proved in 1909:

Theorem 2.40 (A. Thue, 1909)**.** *Let α be a real algebraic number of degree $d \geq 3$. Then any $\kappa > (d/2) + 1$ is an irrationality exponent for α.*

The fact that the irrationality exponent is $< d$ has very important consequences in the theory of Diophantine equations. We gave an example in § 2.2.3, here is the more general result of Thue on Diophantine equations.

[14] Updated: October 12, 2007

Theorem 2.41 (Thue)**.** *Let $f \in \mathbb{Z}[X]$ be an irreducible polynomial of degree $d \geq 3$ and m a non-zero rational integer. Define $F(X,Y) = Y^d f(X/Y)$. Then the Diophantine equation $F(x,y) = m$ has only finitely many solutions $(x,y) \in \mathbb{Z} \times \mathbb{Z}$.*

The equation $F(x,y) = m$ in Proposition 2.41 is called *Thue equation*. The connexion between Thue equation and Liouville's inequality has been explained in Lemma 2.20 in the special case $\sqrt[3]{2}$; the general case is similar.

Lemma 2.42. *Let α be an algebraic number of degree $d \geq 3$ and minimal polynomial $f \in \mathbb{Z}[X]$, let $F(X,Y) = Y^d f(X/Y) \in \mathbb{Z}[X,Y]$ be the associated homogeneous polynomial. Let $0 < \kappa \leq d$. The following conditions are equivalent:*
(i) There exists $c_1 > 0$ such that, for any $p/q \in \mathbb{Q}$,

$$\left| \alpha - \frac{p}{q} \right| \geq \frac{c_1}{q^\kappa} \cdot$$

(ii) There exists $c_2 > 0$ such that, for any $(x,y) \in \mathbb{Z}^2$ with $x > 0$,

$$|F(x,y)| \geq c_2 \; x^{d-\kappa}.$$

In 1921 C.L. Siegel sharpened Thue's result 2.40 by showing that any real number

$$\kappa > \min_{1 \leq j \leq d} \left(\frac{d}{j+1} + j \right)$$

is an irrationality exponent for α. With $j = [\sqrt{d}]$ it follows that $2\sqrt{d}$ is an irrationality exponent for α. Dyson and Gel'fond in 1947 independently refined Siegel's estimate and replaced the hypothesis in Thue's Theorem 2.40 by $\kappa > \sqrt{2d}$. The essentially best possible estimate has been achieved by K.F. Roth in 1955: any $\kappa > 2$ is an irrationality exponent for a real irrational algebraic number α.

Theorem 2.43 (A. Thue, C.L. Siegel, F. Dyson, K.F. Roth 1955)**.** *For any real algebraic number α, for any $\epsilon > 0$, the set of $p/q \in \mathbb{Q}$ with $|\alpha - p/q| < q^{-2-\epsilon}$ is finite.*

It is expected that the result is not true with $\epsilon = 0$ as soon as the degree of α is ≥ 3, which means that it is expected no real algebraic number of degree at least 3 is badly approximable, but essentially nothing is known on the continued fraction of such numbers: we do not know whether there exists an irrational algebraic number which is not quadratic and has bounded partial quotient in its continued fraction expansion, but we do not know either whether there exists a real algebraic number of degree at least 3 whose sequence of partial quotients is not bounded!

A guide to state conjectures is to consider which properties are valid for *almost all numbers*, which means outside a set of Lebesgue measure 0, and to expect that algebraic numbers will share these properties. This guideline should not be followed carelessly: an intersection of subsets of full measure (that means that the complementary has measure 0) may be empty. For instance

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

Nevertheless, this point of view may yields valid guesses.

The so–called *metrical theory of Diophantine approximation* goes back to Cantor's proof of the existence of transcendental numbers. If you list the algebraic numbers in the interval $[0,1]$, if, for each of them, you write its binary expansion (writing the two expansions if this algebraic number is a rational number with denominator a power of two), then taking the digits on the diagonal yields a number θ such that $1-\theta$ is not in the list, hence θ is transcendental.

It is known from a result by Khinchin (1924) that for almost all real numbers, any $\kappa > 2$ is an irrationality exponent. Hence from this point of view algebraic numbers behave like almost all numbers.

Khinchin's Theorem is much more precise: Denote by $\mathcal{K}$ (like Khinchin) the set of *non-increasing* functions ψ from $\mathbb{R}_{\geq 1}$ to $\mathbb{R}_{>0}$. Set

$$\mathcal{K}_c = \left\{\Psi\in\mathcal{K}\,;\, \sum_{n\geq 1}\Psi(n) \text{ converges}\right\}, \quad \mathcal{K}_d = \left\{\Psi\in\mathcal{K}\,;\, \sum_{n\geq 1}\Psi(n) \text{ diverges}\right\}$$

Hence $\mathcal{K} = \mathcal{K}_c \cup \mathcal{K}_d$.

Theorem 2.44 (Khinchin)**.** *Let $\Psi\in\mathcal{K}$. Then for almost all real numbers ξ, the inequality*

$$|q\xi - p| < \Psi(q) \tag{2.45}$$

has

- *only finitely many solutions in integers p and q if $\Psi\in\mathcal{K}_c$*
- *infinitely many solutions in integers p and q if $\Psi\in\mathcal{K}_d$.*

For instance, for any $\epsilon > 0$, the set of irrational real numbers for which the function

$$q \mapsto \frac{1}{q^2(\log q)^{1+\epsilon}} \tag{2.46}$$

is not an irrationality measure has Lebesgue measure 0. One expects that for any irrational algebraic number α, the function 2.46 is an irrationality measure.

However B. Adamczewski and Y. Bugeaud noticed recently (see [6]) that for any $\xi\in\mathbb{R}\setminus\mathbb{Q}$, there exists $\psi\in\mathcal{K}_d$ for which the inequality (2.45) has no solution. Hence no real number behaves generically with respect to Khinchin's Theorem in the divergent case. Also S. Schanuel proved that the set of real numbers which behave like almost all numbers from the point of view of Khinchin's Theorem in the convergent case is the set of real numbers with bounded partial quotients, and this set has measure 0.

Here is an example of application of Diophantine approximation to transcendental number theory. Let $(u_n)_{n\ge 0}$ be an increasing sequence of integers and let b be a rational integer, $b \ge 2$. We wish to prove that the number

$$\vartheta = \sum_{n\ge 0} b^{-u_n} \tag{2.47}$$

is transcendental. A conjecture of Borel (1950 – see [5]) states that *the digits in the binary expansion of a real algebraic irrational number should be uniformly equidistributed*; in particular the sequence of 1's should not be lacunary.

For sufficiently large n, define

$$q_n = b^{u_n}, \quad p_n = \sum_{k=0}^{n} b^{u_n - u_k} \quad \text{and} \quad r_n = \vartheta - \frac{p_n}{q_n}\cdot$$

Since the sequence $(u_n)_{n\ge 0}$ is increasing, we have $u_{n+h} - u_{n+1} \ge h - 1$ for any $h \ge 1$, hence

$$0 < r_n \le \frac{1}{b^{u_{n+1}}} \sum_{h\ge 1} \frac{1}{b^{h-1}} = \frac{b}{2^{u_{n+1}}(b-1)} \le \frac{2}{q_n^{u_{n+1}/u_n}}\cdot$$

Therefore if the sequence $(u_n)_{n\ge 0}$ satisfies

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

then ϑ is a Liouville number, and therefore is transcendental. For instance $u_n = n!$ satisfies this condition: hence the number $\sum_{n\ge 0} b^{-n!}$ is transcendental.

Roth's Theorem 2.43 yields the transcendence of the number ϑ in (2.47) under the weaker hypothesis

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

The sequence $u_n = [2^{\theta n}]$ satisfies this condition as soon as $\theta > 1$. For example the transcendence of the number

$$\sum_{n\ge 0} b^{-3^n}$$

follows from Theorem 2.43.

A stronger result follows from Ridout's Theorem 2.48 below, using the fact that the denominators b^{u_n} are powers of b.

Let S be a set of prime. A rational number is called *a S–integer* if it can be written u/v where all prime factors of the denominator v belong to S. For instance when a, b and m are rational integers with $b \ne 0$, the number a/b^m is a S–integer for S the set of prime divisors of b.

Theorem 2.48 (D. Ridout, 1957). *Let S be a finite set of prime numbers. For any real algebraic number α, for any $\epsilon > 0$, the set of $p/q \in \mathbb{Q}$ with q a S–integer and $|\alpha - p/q| < q^{-1-\epsilon}$ is finite.*

Therefore the condition

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

suffices to imply the transcendence of the sum of the series (2.47). An example is the transcendence of the number

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

This result goes back to A. J. Kempner in 1916.

The theorems of Thue–Siegel–Roth and Ridout are very special cases of Schmidt's subspace Theorem (1972) together with its p-adic extension by H.P. Schlickewei (1976). We state do not state it in full generality but we give only two special cases.

For $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{Z}^m$, define $|\mathbf{x}| = \max\{|x_1|, \ldots, |x_m|\}$.

Theorem 2.49 (W.M. Schmidt (1970): simplified form). *For $m \geq 2$ let $L_1, \ldots, L_m$ be independent linear forms in m variables with algebraic coefficients. Let $\epsilon > 0$. Then the set*

$$\{\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{Z}^m \ ; \ |L_1(\mathbf{x}) \cdots L_m(\mathbf{x})| \leq |\mathbf{x}|^{-\epsilon}\}$$

is contained in the union of finitely many proper subspaces of $\mathbb{Q}^m$.

Thue–Siegel–Roth's Theorem 2.43 follows from Theorem 2.49 by taking

$$m = 2, \quad L_1(x_1, x_2) = x_1, \quad L_2(x_1, x_2) = \alpha x_1 - x_2.$$

A $\mathbb{Q}$-vector subspace of $\mathbb{Q}^2$ which is not $\{0\}$ not $\mathbb{Q}^2$ (that is *a proper subspace* is of the generated by an element $(p_0, q_0) \in \mathbb{Q}^2$. There is one such subspace with $q_0 = 0$, namely $\mathbb{Q} \times \{0\}$ generated by $(1, 0)$, the other ones have $q_0 \neq 0$. Mapping such a rational subspace to the rational number p_0/q_0 yields a 1 to 1 correspondence. Hence Theorem 2.49 says that there is only a finite set of exceptions p/q in Roth's Theorem.

For x a non–zero rational number, write the decomposition of x into prime factors

$$x = \prod_p p^{v_p(x)},$$

where p runs over the set of prime numbers and $v_p(x) \in \mathbb{Z}$ (with only finitely many $v_p(x)$ distinct from 0), and set

$$|x|_p = p^{-v_p(x)}.$$

For $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{Z}^m$ and p a prime number, define $|\mathbf{x}| = \max\{|x_1|_p, \ldots, |x_m|_p\}$.

Theorem 2.50 (Schmidt's Subspace Theorem)**.** *Let $m \geq 2$ be a positive integer, S a finite set of prime numbers. Let $L_1, \ldots, L_m$ be independent linear forms in m variables with algebraic coefficients. Further, for each $p \in S$ let $L_{1,p}, \ldots, L_{m,p}$ be m independent linear forms in m variables with rational coefficients. Let $\epsilon > 0$. Then the set of $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{Z}^m$ such that*

$$|L_1(\mathbf{x}) \cdots L_m(\mathbf{x}) \prod_{p \in S} |L_{1,p}(\mathbf{x}) \cdots L_{m,p}(\mathbf{x})|_p \leq |\mathbf{x}|^{-\epsilon}$$

is contained in the union of finitely many proper subspaces of $\mathbb{Q}^m$.

Ridout's Theorem 2.48 is a consequence of Schmidt's subspace Theorem: in Theorem 2.50 take $m = 2$,

$$L_1(x_1, x_2) = L_{1,p}(x_1, x_2) = x_1,$$
$$L_2(x_1, x_2) = \alpha x_1 - x_2, \quad L_{2,p}(x_1, x_2) = x_2.$$

For $(x_1, x_2) = (b, a)$ with b a S–integer and $p \in S$, we have

$$|L_1(x_1, x_2)| = b, \quad |L_2(x_1, x_2)| = |b\alpha - a|,$$
$$|L_{1p}(x_1, x_2)|_p = |b|_p, \quad |L_{2,p}(x_1, x_2)|_p = |a|_p \leq 1.$$

and

$$\prod_{p \in S} |b|_p = b^{-1}$$

since b is a S–integer.

Problem of effectivity.

`Content of the lecture:` Sketch of proof of Thue's inequality, of Roth's refinement. Upper bound for the number of exceptions in Roth's Theorem, for the number of exceptional subspaces in Schmidt's Theorem. Effective refinement of Liouville's inequality, consequences to Diophantine equations: Baker's method.

2.2.10 Hilbert's seventh problem and its development.

Euler question, Hilbert's 7th problem: transcendence of α^β, of quotients of logartithms. Examples: $2^{\sqrt{2}}$, e^π.

Weierstraß: example of transcendental entire functions with many algebraic values. Interpolation series (see Exercise 2.51).

Polya (1914): integer valued entire functions — 2^z is the "smallest" entire transcendental function mapping the positive integers to rational integers. More precisely, *if $f(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}_{\geq 0}$, then*

$$\limsup_{R \to \infty} 2^{-R} |f|_R \geq 1.$$

Interpolation series: write

$$f(z) = f(\alpha_1) + (z - \alpha_1) f_1(z), \quad f_1(z) = f(\alpha_2) + (z - \alpha_2) f_2(z), \ldots$$

We deduce an expansion

$$f(z) = a_0 + a_1(z-\alpha_1) + a_2(z-\alpha_1)(z-\alpha_2) + \cdots$$

with

$$a_0 = f(\alpha_1), \quad a_1 = f_1(\alpha_2), \ldots, a_n = f_n(\alpha_{n+1}).$$

Exercise 2.51. *Let x, z, $\alpha_1, \ldots, \alpha_n$ be complex numbers with $x \notin \{z,\ \alpha_1, \ldots, \alpha_n\}$.*
a) Check

$$\frac{1}{x-z} = \frac{1}{x-\alpha_1} + \frac{z-\alpha_1}{x-\alpha_1} \cdot \frac{1}{x-z}\cdot$$

b) Deduce the next formula due to Hermite:

$$\frac{1}{x-z} = \sum_{j=0}^{n-1} \frac{(z-\alpha_1)(z-\alpha_2)\cdots(z-\alpha_j)}{(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{j+1})} + \frac{(z-\alpha_1)(z-\alpha_2)\cdots(z-\alpha_n)}{(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)} \cdot \frac{1}{x-z}\cdot$$

c) Let $\mathcal{D}$ be an open disc containing $\alpha_1, \ldots, \alpha_n$, let $\mathcal{C}$ denote the circumference of $\mathcal{D}$, let $\mathcal{D}'$ be an open disc containing the closure of $\mathcal{D}$ and let f be an analytic function in $\mathcal{D}'$. Define

$$A_j(z) = \frac{1}{2i\pi} \int_{\mathcal{C}} \frac{F(x)dx}{(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{j+1})} \qquad (0 \le j \le n-1)$$

and

$$R_n(z) = (z-\alpha_1)(z-\alpha_2)\cdots(z-\alpha_n) \cdot \frac{1}{2i\pi} \int_{\mathcal{C}} \frac{F(x)dx}{(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)(x-z)}\cdot$$

Check the following formula, known as Newton interpolation expansion*: for any $z \in \mathcal{D}'$,*

$$f(z) = \sum_{j=0}^{n-1} A_j(z-\alpha_1)\cdots(z-\alpha_j) + R_n(z).$$

G.H. Hardy, G. Pólya, D. Sato, E.G. Straus, A. Selberg, Ch. Pisot, F. Carlson, F. Gross,. . . .
Gel'fond (1929): same problem for $\mathbb{Z}[i]$: A transcendental entire function f such that $f(a+ib) \in \mathbb{Z}[i]$ for all $a+ib \in \mathbb{Z}[i]$ satisfies

$$\limsup_{R\to\infty} \frac{1}{R^2} \log |f|_R \ge \gamma.$$

Weierstraß sigma function (Hadamard canonical product for $\mathbb{Z}[i]$): $\gamma \le \pi/2$.
A.O. Gel'fond: $\gamma = 10^{-45}$.
Fukasawa, D.W. Masser, F. Gramain (1981): $\gamma = \pi/(2e)$.
Connection with $e^\pi = 23,140\,692\,632\,779\,269\,005\,729\,086\,367\ \ldots$
Siegel (1929): Dirichlet's box principle, lemma of Thue–Siegel, application to transcendence (elliptic curves).

Gel'fond–Schneider's Theorem in 1934.
"Criteria" for analytic functions satisfying differential equations: Schneider, Lang. Statement of the Schneider–Lang Theorem. Corollaries: Hermite–Lindemann, Gel'fond–Schneider.
Mahler's method:

$$f(z) = \sum_{n \geq 0} 2^{-n(n-1)} z^n, \quad f(z) = 1 + zf(z/4), \quad f(1/2) = \sum_{n \geq 0} 2^{-n^2}.$$

Also $f(z) = \sum_{n \geq 0} z^{d^n}$, for $d \geq 2$, satisfies the functional equation $f(z^d) + z = f(z)$ for $|z| < 1$.
Baker's Theorem.
Algebraic independence: Gel'fond's criterion, algebraic independence of $2^{\sqrt[3]{2}}$ and $2^{\sqrt[3]{4}}$. Gel'fond–Schneider problem on the transcendence degree of $\mathbb{Q}(\alpha^{\beta_1}, \ldots, \alpha^{\beta_m})$ (see Exercise 2.52).
Algebraic independence of π and $\Gamma(1/4)$: Chudnovskii (1978). Algebraic independence of π, e^π and $\Gamma(1/4)$: Nesterenko (1996).
Schanuel's conjecture. Consequences.
Auxiliary functions, zero estimates, Laurent's interpolation determinants. Arakelov Theory (J-B. Bost): slope inequalities.

Exercise 2.52. *Let α be a non-zero algebraic number and let ℓ be any non–zero number such that $e^\ell = \alpha$. For $z \in \mathbb{C}$ define α^z as $\exp\{z\ell\}$ (which is the same as $e^{z\ell}$). Show that the following statements are equivalent.*
(i) For any irrational algebraic complex number β, the transcendence degree over $\mathbb{Q}$ of the field

$$\mathbb{Q}\big\{\alpha^{\beta^i} \; ; \; i \geq 1\big\}$$

is $d-1$ where d is the degree of β.
(ii) For any algebraic numbers $\beta_1, \ldots, \beta_m$ such that the numbers $1, \beta_1, \ldots, \beta_m$ are $\mathbb{Q}$-linearly independent, the numbers $\alpha^{\beta_1}, \ldots, \alpha^{\beta_m}$ are algebraically independent.
`Remark:` *that both statements are true is a conjecture of Gel'fond and Schneider. It is not yet proved.*

Exercise 2.53. *Deduce from Schanuel's Conjecture the following statement: the numbers*

$$\begin{aligned} &e,\ \pi,\ e^\pi,\ \pi^e,\ e^e,\ \pi^\pi,\ (\log 2)^{\log 3},\ (\log 3)^{\log 2},\ \pi^{\log 2},\ \pi^{\log 3},\\ &\log \pi,\ \log\log \pi,\ \log\log 2,\ \log\log 3 \end{aligned} \tag{2.54}$$

are algebraically independent.

References

[1] Y. Bugeaud – *Approximation by algebraic numbers*, Cambridge Tracts in Mathematics, vol. 160, Cambridge University Press, Cambridge, 2004.

[2] N.I. Fel′dman & Yu.V. Nesterenko – *Transcendental numbers*, in *Number Theory, IV*, Encyclopaedia Math. Sci., vol. **44**, Springer, Berlin, 1998, p. 1–345.

[3] N.I. Fel’dman & A.B. Šidlovskiĭ – *The development and present state of the theory of transcendental numbers*, (Russian) Uspehi Mat. Nauk **22** (1967) no. 3 (135) 3–81; Engl. transl. in Russian Math. Surveys, **22** (1967), no. 3, 1–79.

[4] W. M. Schmidt – *Diophantine approximation*, Lecture Notes in Mathematics, vol. 785, Springer-Verlag, Berlin, 1980.

[5] M. Waldschmidt – *Words and Transcendence.* To appear http://www.math.jussieu.fr/∼miw/articles/pdf/WordsTranscendence.pdf

[6] M. Waldschmidt – *Report on some recent progress in Diophantine approximation.* To appear http://www.math.jussieu.fr/∼miw/articles/pdf/miwLangMemorialVolume.pdf