Updated: *June 16, 2010*

Diophantine approximation, irrationality and transcendence

Michel Waldschmidt

Course N°4, *April 28, 2010*

These are informal notes of my course given in April – June 2010 at IMPA (*Instituto Nacional de Matematica Pura e Aplicada*), Rio de Janeiro, Brazil.

This course was devoted to Liouville's inequality (§ 4.1).

The present notes consist of

- Pages 65–85 of [38] (begining of Chapter 3: Heights).
- Liouville's inequality for quadratic numbers.
- A short historical survey on Diophantine Approximation.

4.1.2 Liouville's inequality for quadratic numbers

Consider Lemma 24 in the special case $d = 2$ where α is a quadratic algebraic number. Write its minimal polynomial $f(X) = aX^2 + bX + c$ and let $\Delta := b^2 - 4ac$ be its discriminant. Since we are interested in the approximation of α by rational numbers, we assume $\Delta > 0$. If $\alpha = (-b \pm \sqrt{\Delta})/2a$, then the other root is $\alpha' = (-b \mp \sqrt{\Delta})/2a$ and

$$f'(\alpha) = a(\alpha - \alpha') = \pm\sqrt{\Delta}.$$

Lemma 40. *Let α be an algebraic number of degree 2 and minimal polynomial $P \in \mathbf{Z}[X]$. Define $c = |P'(\alpha)|$. Let $\epsilon > 0$. Then there exists an integer q_0 such that, for any $p/q \in \mathbf{Q}$ with $q \geq q_0$,*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{(\sqrt{\Delta} + \epsilon)q^2}.$$

The smallest positive discriminant of an irreducible quadratic polynomial with coefficients in $\mathbf{Z}$ is 5, which is the value of the discriminant of $X^2 - X - 1$, with roots Φ and $-\Phi^{-1}$ where $\Phi = 1.6180339887499\ldots$ denotes the Golden ratio.

The next result deals with the Fibonacci sequence $(F_n)_{n\geq 0}$:

$$F_0 = 0,\ F_1 = 1,\ F_n = F_{n-1} + F_{n-2} \quad (n \geq 2).$$

Lemma 41. *For any $q \geq 1$ and any $p \in \mathbf{Z}$,*

$$\left|\Phi - \frac{p}{q}\right| > \frac{1}{\sqrt{5}q^2 + (q/2)}.$$

On the other hand

$$\lim_{n\to\infty} F_{n-1}^2 \left|\Phi - \frac{F_n}{F_{n-1}}\right| = \frac{1}{\sqrt{5}}.$$

Proof. It suffices to prove the lower bound when p is the nearest integer to $q\Phi$. From $X^2 - X - 1 = (X - \Phi)(X + \Phi^{-1})$ we deduce

$$p^2 - pq - q^2 = q^2 \left(\frac{p}{q} - \Phi\right)\left(\frac{p}{q} + \Phi^{-1}\right).$$

The left hand side is a non-zero rational integer, hence has absolute value at least 1. We now bound the absolute value of the right hand side from above. Since $p < q\Phi + (1/2)$ and $\Phi + \Phi^{-1} = \sqrt{5}$ we have

$$\frac{p}{q} + \Phi^{-1} < \sqrt{5} + \frac{1}{2q}.$$

Hence

$$1 < q^2 \left| \frac{p}{q} - \Phi \right| \left(\sqrt{5} + \frac{1}{2q} \right)$$

The first part of Lemma 41 follows.

The real vector space of sequences $(v_n)_{n\geq 0}$ satisfying $v_n = v_{n-1}+v_{n-2}$ has dimension 2, a basis is given by the two sequences $(\Phi^n)_{n\geq 0}$ and $((-\Phi^{-1})^n)_{n\geq 0}$. From this one easily deduces the formula

$$F_n = \frac{1}{\sqrt{5}}(\Phi^n - (-1)^n \Phi^{-n})$$

due to A. De Moivre (1730), L. Euler (1765) and J.P.M. Binet (1843). It follows that F_n is the nearest integer to

$$\frac{1}{\sqrt{5}}\Phi^n,$$

hence the sequence $(u_n)_{n\geq 2}$ of quotients of Fibonacci numbers

$$u_n = F_n/F_{n-1}$$

satisfies $\lim_{n\to\infty} u_n = \Phi$.

By induction one easily checks

$$F_n^2 - F_n F_{n-1} - F_{n-1}^2 = (-1)^{n-1}$$

for $n \geq 1$. The left hand side is $F_{n-1}^2(u_n - \Phi)(u_n + \Phi^{-1})$, as we already saw. Hence

$$F_{n-1}^2 |\Phi - u_n| = \frac{1}{\Phi^{-1} + u_n},$$

and the limit of the right hand side is $1/(\Phi + \Phi^{-1}) = 1/\sqrt{5}$. The result follows.

□

Remark. *The sequence $u_n = F_n/F_{n-1}$ is also defined by*

$$u_2 = 2,\ u_n = 1 + \frac{1}{u_{n-1}}, \quad (n \geq 3).$$

Hence

$$u_n = 1 + \frac{1}{1 + \dfrac{1}{u_{n-2}}} = 1 + \frac{1}{1 + \dfrac{1}{1 + \dfrac{1}{u_{n-3}}}} = \cdots$$

Remark. *It is known (see for instance [31] p. 25) that if k is a positive integer, if an irrational real number ϑ has a continued fraction expansion $[a_0; a_1, a_2, \dots]$ with $a_n \geq k$ for infinitely many n, then*

$$\liminf_{q\to\infty} q^2 \left|\vartheta - \frac{p}{q}\right| \leq \frac{1}{\sqrt{4+k^2}}.$$

4.1.3 Diophantine Approximation: historical survey

References for this section are [2, 31, 13, 1].

Definition Given a real irrational number ϑ, a function $\varphi = \mathbf{N} \to \mathbf{R}_{>0}$ is an irrationality measure for ϑ if there exists an integer $q_0 > 0$ such that, for any $p/q \in \mathbf{Q}$ 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) $\Rightarrow$ (iv) in Proposition 4) it follows that any irrationality exponent κ satisfies $\kappa \geq 2$. Irrational quadratic numbers have irrationality exponent 2. It is known (see for instance [31] 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* $(a_0, a_1, \dots)$ in the continued fraction expansion of ϑ is bounded: these are called the *badly approximable numbers*.

From Liouville's inequality in Lemma 24 it follows that any irrational algebraic real number α of degree d 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 [3]) 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 42 (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 corollaries in the theory of Diophantine equations. We start with a special example. Liouville's estimate for the rational Diophantine approximation of $\sqrt[3]{2}$ is

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{1}{9q^3}$$

for sufficiently large q (use Lemma 24 with $P(X) = X^3 - 2$, $c = 3\sqrt[3]{2} < 9$). Thue was the first to achieve an improvement of the exponent 3. A explicit estimate was then obtained by A. Baker, namely

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{1}{10^6 q^{2.955}},$$

and refined by Chudnovskii, Easton, Rickert, Voutier and others, until 1997 when M. Bennett proved that *for any $p/q \in \mathbf{Q}$,*

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| \geq \frac{1}{4\ q^{2,5}}.$$

From his own result, Thue deduced that *for any fixed $k \in \mathbf{Z} \setminus \{0\}$, there are only finitely many $(x, y) \in \mathbf{Z} \times \mathbf{Z}$ satisfying the Diophantine equation $x^3 - 2y^3 = k$.* The result of Baker shows more precisely that if $(x, y) \in \mathbf{Z} \times \mathbf{Z}$ is a solution to $x^3 - 2y^3 = k$, then

$$|x| \leq 10^{137} |k|^{23}.$$

M. Bennett gave the sharper estimate: *for any $(x, y) \in \mathbf{Z}^2$ with $x > 0$,*

$$|x^3 - 2y^3| \geq \sqrt{x}.$$

The connexion between Diophantine approximation to $\sqrt[3]{2}$ and the Diophantine equation $x^3 - 2y^3 = k$ is explained in the next lemma.

Lemma 43. *Let η be a positive real number. The two following properties are equivalent:*
(i) *There exists a constant $c_1 > 0$ such that, for any $p/q \in \mathbf{Q}$ with $q > 0$,*

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{c_1}{q^\eta}.$$

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

$$|x^3 - 2y^3| \geq c_2 x^{3-\eta}.$$

Properties (i) and (ii) are true but uninteresting with $\eta \geq 3$. They are not true with $\eta < 2$. It is not expected that they are true with $\eta = 2$, but it is expected that they are true for any $\eta > 2$.

Proof. We assume $\eta < 3$, otherwise the result is trivial. Set $\alpha = \sqrt[3]{2}$.

Assume (i) and let $(x, y) \in \mathbf{Z} \times \mathbf{Z}$ have $x > 0$. Set $k = x^3 - 2y^3$. Since 2 is not the cube of a rational number we have $k \neq 0$. If $y = 0$ assertion (ii) plainly holds. So assume $y \neq 0$.

Write

$$x^3 - 2y^3 = (x - \alpha y)(x^2 + \alpha xy + \alpha^2 y^2).$$

The polynomial $X^2 + \alpha X + \alpha^2$ has negative discriminant $-3\alpha^2$, hence has a positive minimum $c_0 = 3\alpha^2/4$. Hence the value at (x, y) of the quadratic form $X^2 + \alpha XY + \alpha^2 Y^2$ is bounded form below by $c_0 y^2$. From (i) we deduce

$$|k| = |y|^3 \left| \sqrt[3]{2} - \frac{x}{y} \right| (x^2 + \alpha xy + \alpha^2 y^2) \geq \frac{c_1 c_0 |y|^3}{|y|^\eta} = c_3 |y|^{3-\eta}.$$

This gives an upper bound for $|y|$:

$$|y| \leq c_4 |k|^{1/(3-\eta)}, \quad \text{hence} \quad |y^3| \leq c_4 |k|^{3/(3-\eta)}.$$

We want an upper bound for x: we use $x^3 = k + 2y^3$ and we bound $|k|$ by $|k|^{3/(3-\eta)}$ since $3/(3-\eta) > 1$. Hence

$$x^3 \leq c_5 |k|^{3/(3-\eta)} \quad \text{and} \quad x^{3-\eta} \leq c_6 |k|.$$

Conversely, assume (ii). Let p/q be a rational number. If p is not the nearest integer to $q\alpha$, then $|q\alpha - p| > 1/2$ and the estimate (i) is trivial. So we assume $|q\alpha - p| \leq 1/2$. We need only the weaker estimate $c_7 q < p < c_8 q$ with some positive constants c_7 and c_8, showing that we may replace p by q or q by p in our estimates, provided that we adjust the constants. From

$$p^3 - 2q^3 = (p - \alpha q)(p^2 + \alpha pq + \alpha^2 q^2),$$

using (ii), we deduce

$$c_2 p^{3-\eta} \leq c_{10} q^3 \left| \alpha - \frac{p}{q} \right|,$$

and (i) easily follows.

□

Here is the most general result of Thue on Diophantine equations.

Theorem 44 (Thue)**.** *Let $f \in \mathbf{Z}[X]$ 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 $(x,y) \in \mathbf{Z} \times \mathbf{Z}$.*

The equation $F(x,y) = m$ in Proposition 44 is called *Thue equation.* The connexion between Thue equation and Liouville's inequality has been explained in Lemma 43 in the special case $\sqrt[3]{2}$; the general case is similar.

Lemma 45. *Let α be an algebraic number of degree $d \geq 3$ and minimal polynomial $f \in \mathbf{Z}[X]$, let $F(X,Y) = Y^d f(X/Y) \in \mathbf{Z}[X,Y]$ 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 $p/q \in \mathbf{Q}$,*

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

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

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

In 1921 C.L. Siegel sharpened Thue's result 42 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 42 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 46 (A. Thue, C.L. Siegel, F. Dyson, K.F. Roth 1955)**.** *For any real algebraic number α, for any $\epsilon > 0$, the set of $p/q \in \mathbf{Q}$ 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!

If one restricts the denominators q of the rational approximations p/q by requesting that their prime factor belong to a given finite set, then the exponent 2 can be replaced by 1. This has been proved by D. Ridout in 1957.

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 $b \neq 0$, the number a/b^m is a S–integer for S the set of prime divisors of b.

Theorem 47 (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 $p/q \in \mathbf{Q}$, with q a S–integer and $|\alpha - p/q| < q^{-1-\epsilon}$, is finite.*

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 do not state it in full generality but we give only two special cases.

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

$$|\mathbf{x}| = \max\{|x_1|, \ldots, |x_m|\}.$$

Theorem 48 (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*

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

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

Thue–Siegel–Roth's Theorem 46 follows from Theorem 48 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 $\mathbf{Q}$-vector subspace of $\mathbf{Q}^2$ which is not $\{0\}$ not $\mathbf{Q}^2$ (that is *a proper subspace* generated by an element $(p_0, q_0) \in \mathbf{Q}^2$. There is one such subspace with $q_0 = 0$, namely $\mathbf{Q} \times \{0\}$ 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 48 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 $v_p(x) \in \mathbf{Z}$ (with only finitely many $v_p(x)$ distinct from 0), and set

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

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

$$|\mathbf{x}| = \max\{|x_1|_p, \ldots, |x_m|_p\}.$$

Theorem 49 (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 $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbf{Z}^m$ 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 $\mathbf{Q}^m$.

Ridout's Theorem 47 is a corollary of Schmidt's subspace Theorem: in Theorem 49 take $m = 2$,

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

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

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

and

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

since b is a S–integer.

Further references

References

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

[2] 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.

[3] M. Waldschmidt – *Report on some recent progress in Diophantine approximation*. To appear
http://www.math.jussieu.fr/∼miw/articles/pdf/miwLangMemorialVolume.pdf
Number Theory Math arXiv: http://fr.arxiv.org/abs/0908.3973
Archives Ouvertes http://hal.archives-ouvertes.fr/hal-00407199/fr/

Michel WALDSCHMIDT
Université P. et M. Curie (Paris VI)
Institut Mathématique de Jussieu
Problèmes Diophantiens, Case 247
4, Place Jussieu
75252 Paris CEDEX 05, France
miw@math.jussieu.fr
http://www.math.jussieu.fr/∼miw/

This text is available on the internet at the address
http://www.math.jussieu.fr/∼miw/enseignement.html