From Simultaneous Approximations to Algebraic Independence

by

Michel WALDSCHMIDT

Abstract

Given a complex number θ, Dirichlet's box principle enables one to show that there exist three positive constants c_0, D_0, H_0 such that, for any $D \ge D_0$ and any $H \ge H_0$, there exists a non-zero polynomial $f \in \mathbb{Z}[X]$ of degree $\le D$ and naïve height (maximum of absolute values of the coefficients) $\le H$ with $|f(\theta)| \le H^{-c_0 D}$.

Assume now θ is transcendental. Using elimination procedures, one can select a root of f which is "close" to θ and deduce that θ possesses rather "good" approximations by algebraic numbers. Here is such a precise statement. For an algebraic number γ of degree $d = [\mathbf{Q}(\gamma) : \mathbf{Q}]$ with complex conjugates $\gamma_1, \ldots, \gamma_d$ and minimal polynomial $a_0(X-\gamma_1)\cdots(X-\gamma_d)$, we define $\mathrm{M}(\gamma)$ (Mahler's measure of γ) and $\mathrm{h}(\gamma)$ (absolute logarithmic height of γ) by

$$\mathrm{M}(\gamma) = a_0 \prod_{j=1}^{d} \max\{1, |\gamma_j|\} \qquad \text{and} \qquad \mathrm{h}(\gamma) = \frac{1}{d}\log \mathrm{M}(\gamma).$$

Let θ be a complex transcendental number. According to Wirsing, for any integer $D \ge 2$ there exist infinitely many algebraic numbers γ satisfying

$$[\mathbf{Q}(\gamma) : \mathbf{Q}] \le D, \qquad \text{and} \qquad |\theta - \gamma| \le \mathrm{M}(\gamma)^{-D/4}.$$

In a joint work with Damien Roy, we prove that for any $h \ge 10^7$, there is an infinite set of positive integers d for which there exists an algebraic number α of degree d and height $\mathrm{h}(\gamma) \le h$ satisfying

$$|\theta - \gamma| \le \exp\{-10^{-7} d^2 h\}.$$

Such a statement can be extended to a finite family $\{\theta_1, \ldots, \theta_m\}$ of complex numbers which generate a field of transcendence degree 1 over $\mathbb{Q}$. An interesting consequence is the following: *For a given set $\{\theta_1, \ldots, \theta_m\}$ of complex numbers, if one can produce a sufficiently sharp measure of simultaneous approximation, then the transcendence degree of the field $\mathbb{Q}(\theta_1, \ldots, \theta_m)$ is ≥ 2.*

As a matter of fact, there is a wide class of such families of complex numbers for which a measure of simultaneous approximation can be established. We give several examples. Further related recent results by D. Roy, M. Laurent and P. Philippon will be discussed.

Diophantine approximation with the naïve height

These lectures are related to transcendental number theory. By *numbers* we mean *complex numbers*. More precisely we start with the natural integers $\mathbb{N} = \{0, 1, 2, \ldots\}$. In order to get an additive group we need to introduce the set of rational integers $\mathbb{Z} = \{0, 1, -1, 2, -2, \ldots\}$. In the same way, in order to have a field, we consider the set of rational numbers $\mathbb{Q} = \bigl\{a/b\,;\, a \in \mathbb{Z},\, b \in \mathbb{Z} \setminus \{0\}\bigr\}$. These two first steps (from $\mathbb{N}$ to $\mathbb{Z}$, and from $\mathbb{Z}$ to $\mathbb{Q}$) involved only algebraic constructions. The next step belongs to analysis: the field $\mathbb{R}$ of real numbers is the completion of $\mathbb{Q}$ for the usual (archimedean) absolute value. The final step is again algebraic: $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$. We end up with the following inclusions:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}. \tag{1}$$

We need also to consider another algebraic closure, namely the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ into $\mathbb{C}$; this is the *field of algebraic numbers*, viz. the set of $\alpha \in \mathbb{C}$ such that there exists a nonzero polynomial $A \in \mathbb{Z}[X]$ with $A(\alpha) = 0$.

By definition, a *transcendental number* is a complex number which is not algebraic. Therefore the set of transcendental numbers is the complement of the field $\overline{\mathbb{Q}}$ into the field $\mathbb{C}$. As such, it does not have nice algebraic properties: no stability under sum or product. However the sum of a transcendental number and an algebraic number is a transcendental number, and the product of a transcendental number and a nonzero algebraic number is again a transcendental number.

When α is a complex algebraic number, its complex conjugate $\overline{\alpha}$ is algebraic, and its modulus $|\alpha|$ also. It follows that a complex number $x + iy$ (where x and y are real) is algebraic if and only if both numbers x and y are algebraic. Therefore $x + iy$ is transcendental if and only if one at least of the two real numbers x, y is transcendental.

In the present state of our knowledge, <u>all</u> transcendence proofs rest so far on a statement which belongs to Diophantine approximation. The prototype of such an argument is the following:

$$\text{for } n \in \mathbb{N},\ n \ne 0, \text{ we have } n \ge 1.$$

In our sequence of inclusions (1) we extend this result to $\mathbb{Z}$:

$$\text{for } n \in \mathbb{Z},\ n \ne 0, \text{ we have } |n| \ge 1$$

and then to $\mathbb{Q}$:

$$\text{for } p/q \in \mathbb{Q},\ q > 0,\ p \ne 0, \text{ we have } |p/q| \ge 1/q.$$

There is no similar inequality which would hold for the field $\mathbb{R}$: the last step is $\overline{\mathbb{Q}}$. For each $\alpha \in \overline{\mathbb{Q}}$, $\alpha \ne 0$, we shall produce a lower bound for $|\alpha|$. There are many such estimates. As far as I can see, all these inequalities which are actually used inside transcendence proofs rest on elementary arguments which are akin to Liouville's construction of transcendental numbers in 1844 (for this reason each of them is called *Liouville's inequality*). Much deeper estimates are available for certain classes of algebraic numbers; for instance the *Thue-Siegel-Roth Theorem* applies for algebraic numbers α of the form $q\beta - p$ for some fixed β

and for p, q in $\mathbb{Z}$. Extensions of this deep result have been achieved by W.M. Schmidt, but unfortunately we do not still know how to use them for transcendence purposes (apart from some special constructions of specific transcendental numbers).

An example of a Liouville inequality has been given in the first lecture by Hans-Peter Schlickewei. Here is another one. Let α be an algebraic number. By definition there exists a nonzero polynomial $A \in \mathbb{Z}[X]$ with $A(\alpha) = 0$. Since the ring $\mathbb{Z}[X]$ is factorial, there is a unique such A, which is also irreducible and with positive leading coefficient: this is the *minimal polynomial* of α over $\mathbb{Z}$. Let $A(X) = a_0X^d + a_1X^{d-1} + \cdots + a_d$ be the minimal polynomial of α over $\mathbb{Z}$, with $a_0 > 0$; the rational integers $a_0, \ldots, a_d$ have no common divisor in $\mathbb{Z}$, and the polynomial $A(X)$ is irreducible in $\mathbb{Q}[X]$. The integer $d = \deg A$ is then called the *degree* of α; it is usually denoted by $[\mathbb{Q}(\alpha) : \mathbb{Q}]$, but we shall also use the notation $\mathrm{d}(\alpha)$. The so-called *naïve height* $\mathrm{H}(\alpha)$ of α is defined by

$$\mathrm{H}(\alpha) = \max\{|a_0|, \ldots, |a_d|\}.$$

More generally, for a nonzero polynomial with coefficients in $\mathbb{Z}$, the *naïve height* is the maximum of the absolute values of the coefficients.

Lemma 2. – *For any nonzero algebraic number α,*

$$|\alpha| > \frac{1}{\mathrm{H}(\alpha) + 1}.$$

Proof. We start with the proof of the following statement:

(3) *For any algebraic number α, we have $|\alpha| < \mathrm{H}(\alpha) + 1$.*

This assertion clearly holds if $|\alpha| < 2$, because $\mathrm{H}(\alpha) \geq 1$. Therefore there is no loss of generality to assume $|\alpha| > 1$. We divide the relation

$$a_0\alpha^d + a_1\alpha^{d-1} + \cdots + a_d = 0$$

by α^{d-1}:

$$a_0\alpha = -a_1 - a_2\alpha^{-1} - \cdots - a_d\alpha^{-d+1}.$$

Since $a_0 \geq 1$ and $|a_i| \leq H$ for $1 \leq i \leq d$, we deduce

$$|\alpha| \leq |a_0\alpha| \leq H\bigl(1 + |\alpha|^{-1} + \cdots + |\alpha|^{-d+1}\bigr).$$

Since we have assumed $|\alpha| > 1$, the right hand side is less than

$$H\bigl(1 + |\alpha|^{-1} + |\alpha|^{-2} + \cdots\bigr) = \frac{H}{1 - |\alpha|^{-1}} = \frac{H|\alpha|}{|\alpha| - 1}.$$

Therefore

$$|\alpha| < H\frac{|\alpha|}{|\alpha| - 1}.$$

The desired inequality $|\alpha| - 1 < H$ follows. This completes the proof of assertion (3).

We come back to the proof of Lemma 2: we assume $\alpha \neq 0$ and we apply the estimate (3) to α^{-1}. Since $\mathrm{H}(\alpha) = \mathrm{H}(\alpha^{-1})$, we deduce

$$|\alpha|^{-1} = |\alpha^{-1}| < \mathrm{H}(\alpha^{-1}) + 1 = \mathrm{H}(\alpha) + 1.$$

Lemma 2 follows. □

Liouville's inequality is a main tool for transcendence proofs. Most often, this is the only place in the proof where we actually use the assumption that some numbers are algebraic. Here is another example of such an estimate (see for instance [3] and [4]), whose proof is left as an exercise. We introduce the following notations: for a polynomial f of degree D and naïve height H, and for an algebraic number α of degree $\mathrm{d}(\alpha)$ and height $\mathrm{H}(\alpha)$,

$$\mathrm{t}(f) = D + \log H \quad \text{and} \quad \mathrm{t}(\alpha) = \mathrm{d}(\alpha) + \log \mathrm{H}(\alpha).$$

Lemma 4. – *Let α be an algebraic number.*
(a) Let $f \in \mathbb{Z}[X]$ be a polynomial such that $f(\alpha) \neq 0$. Then

$$|f(\alpha)| \geq e^{-\mathrm{t}(f)\mathrm{t}(\alpha)}.$$

(b) Let β be an algebraic number with $\beta \neq \alpha$. Then

$$|\alpha - \beta| \geq e^{-2\mathrm{t}(\alpha)\mathrm{t}(\beta)}.$$

In addition to Liouville's inequality, another very useful tool in transcendental number theory is Dirichlet's box principle which is also called *pigeon-hole principle.* It was introduced in the theory of Diophantine approximation by A. Thue, and developed by C.L. Siegel, at the beginning of this century. This tool enabled one to construct auxiliary functions, and this was a key step in the solution by A.O. Gel'fond and Th. Schneider of Hilbert's seventh problem in 1934. A few years ago, M. Laurent showed how to avoid the construction of the auxiliary function by means of interpolation determinants. However this box principle still plays an important role in transcendental number theory, as we shall see.

We start with the following lemma which shows the existence of polynomials which take a small value at a given *real* point.

Lemma 5. – *Let θ be a real number, $H \geq 1$ and $D \geq 1$ two positive integers. Then there exists a nonzero polynomial $f \in \mathbb{Z}[X]$ of degree $\leq D$ and naïve height $\mathrm{H}(f) \leq H$ such that*

$$|f(\theta)| < 2\bigl(1 + |\theta| + \cdots + |\theta|^D\bigr)H^{-D}.$$

Proof. There is no loss of generality to assume $\theta > 0$: indeed, if $\theta = 0$, then we can take $f(X) = X$, while for $\theta < 0$, we can take for f the polynomial $g(-X)$, where g does the job for $|\theta|$. Next, if the right hand side is >1, just take for f the constant polynomial 1. Therefore we assume, from now on, $\theta>0$ and

$$2(1+\theta+\cdots+\theta^D)\le H^D.$$

The set

$$E=\Bigl\{(a_0,\ldots,a_D)\in\mathbb{Z}^{D+1}\,;\,0\le a_i\le H,\,(0\le i\le D)\Bigr\}$$

has exactly $(H+1)^{D+1}$ elements. For each $\underline{a}=(a_0,\ldots,a_D)\in E$, the real number $\xi(\underline{a})=a_0+a_1\theta+\cdots+a_D\theta^D$ belongs to the interval $[0,L]$ where $L=\bigl(1+\theta+\cdots+\theta^D\bigr)H$. Let $L'\in\mathbb{Z}$ be the rational integer in the interval $L\le L'<L+1$. Select a positive integer N, and divide the interval $[0,L']$ into $L'N$ intervals of length $1/N$:

$$[0,1/N[,\quad [1/N,2/N[,\ldots,\quad [L'-(1/N),L'].$$

We shall choose N so that $L'N<(H+1)^{D+1}$. Then, from Dirichlet's box principle, it follows that there exist two distinct elements $\underline{a}$ and $\underline{b}$ in E with $|\xi(\underline{a})-\xi(\underline{b})|\le 1/N$. Define $\underline{c}=\underline{a}-\underline{b}=(c_0,\ldots,c_D)$ and consider the polynomial $f(X)=c_0+c_1X+\cdots+c_DX^D$. We obtain $f\ne 0$, $\deg f\le D$, $\mathrm{H}(f)\le H$ and $|f(\theta)|\le 1/N$.

We now choose for N the largest integer such that $(L+1)N\le(H+1)^{D+1}$. The condition $L'N<(H+1)^{D+1}$ is plainly satisfied. On the other hand we deduce from the choice of N the estimate $(L+1)(N+1)>(H+1)^{D+1}$. Using the inequalities $H<L\le\frac12H^{D+1}$, we deduce

$$\left(1+\frac1L\right)\left(\frac{H^{D+1}}{2}+L\right)<(H+1)H^D<(H+1)^{D+1},$$

hence

$$N>\frac{(H+1)^{D+1}}{L+1}-1>\frac{H^{D+1}}{2L}$$

and

$$|f(\theta)|\le\frac1N<\frac{2L}{H^{D+1}}=2(1+\theta+\cdots+\theta^D)H^{-D}.$$

This completes the proof of Lemma 5. □

Here is a similar statement for a *complex* number.

Lemma 6. – *Let θ be a complex number, $H\ge1$ a real number and $D\ge1$ a positive integer. There exists a nonzero polynomial $f\in\mathbb{Z}[X]$ of degree $\le D$ and naïve height* $\mathrm{H}(f)\le H$ *such that*

$$|f(\theta)|\le\sqrt2\bigl(1+|\theta|+\cdots+|\theta|^D\bigr)H^{-(D-1)/2}.$$

Proof. Define $X=[H]$. Since X is a positive integer we have

$$(X+1)^{(D+1)/2}\ge X(X+1)^{(D-1)/2}+1.$$

From the bound $H<X+1$ we deduce

$$(X+1)^{(D+1)/2}\ge XH^{(D-1)/2}+1.$$

It follows that there exists a rational integer $\ell\in\mathbb{Z}$ in the interval

$$XH^{(D-1)/2}\le\ell<(X+1)^{(D+1)/2}.$$

Define $U=1+|\theta|+\cdots+|\theta|^D$. Using Dirichlet's box principle in a way similar to the proof of Lemma 5, we deduce that there exists $(a_0,\ldots,a_D)\in\mathbb{Z}^{D+1}$ with $0<\max\{|a_0|,\ldots,|a_D|\}\le X$ such that

$$\begin{cases}\left|\displaystyle\sum_{i=0}^D a_i\Re e(\theta^i)\right|\le\dfrac{UX}{\ell}\\[2ex] \left|\displaystyle\sum_{i=0}^D a_i\Im m(\theta^i)\right|\le\dfrac{UX}{\ell}.\end{cases}$$

From the upper bound $X/\ell\le H^{-(D-1)/2}$ one concludes

$$\left|\sum_{i=0}^D a_i\theta^i\right|\le\sqrt2UH^{-(D-1)/2}.$$

□

We shall use the following weak form of Lemma 6: *For any $\theta\in\mathbb{C}$, there exist constants $c>0$, $D_0\ge1$ and $H_0\ge1$ such that, for any integer $D\ge D_0$ and any integer $H\ge H_0$, there exists a nonzero polynomial $f\in\mathbb{Z}[X]$ of degree $\le D$ and naïve height $\le H$ with*

$$|f(\theta)|\le H^{-cD}.$$

For instance

$$D_0=2,\quad c=1/5,\quad H_0=18^5\max\{1,|\theta|\}^{20}$$

are admissible values, because of the estimate

$$\sqrt2(D+1)\max\{1,|\theta|\}^DH^{1/2}<H^{3D/10}$$

which is true for $D\ge2$ and $H\ge18^5\max\{1,|\theta|\}^{20}$.

Exercise. Let $\theta_1,\ldots,\theta_m$ be complex numbers, H and D positive integers. Show that there exists a nonzero polynomial $f\in\mathbb{Z}[X_1,\ldots,X_m]$ of partial degrees $\le D$ and naïve height $\mathrm{H}(f)\le H$ such that

$$|f(\theta_1,\ldots,\theta_m)|\le cH^{1-\frac{(D+1)^m}{2}}$$

where

$$c=\sqrt2\sum_{i_1=0}^D\cdots\sum_{i_m=0}^D\bigl|\theta_1^{i_1}\cdots\theta_m^{i_m}\bigr|.$$

`Hint.` *Check the inequality*

$$(H+1)^{\frac{1}{2}(D+1)^m} - H^{\frac{1}{2}(D+1)^m} \geq 1$$

for integers $D \geq 1$ and $H \geq 1$, and deduce that there exists a rational integer $\ell \in \mathbb{Z}$ such that ℓ^2 belongs to the interval

$$H^{(D+1)^m} \leq \ell^2 < (H+1)^{(D+1)^m}.$$

An important feature of Dirichlet's argument is that, when it produces a nonzero $f \in \mathbb{Z}[X]$, it does not tell us whether $f(\theta)$ vanishes or not! In fact, in view of Lemma 4, if θ is algebraic, for D and H sufficiently large, the polynomial $f \in \mathbb{Z}[X]$ arising from the box principle does vanish at θ. But of course, if θ is transcendental, then $f(\theta)$ does not vanish!

We shall now address a related problem:

- *For a fixed transcendental number $\theta \in \mathbb{C}$, how small can be*

$$\inf\Big\{|\theta-\alpha|\,;\,\alpha \in \overline{\mathbb{Q}},\ \mathrm{d}(\alpha) \leq D,\ \mathrm{H}(\alpha) \leq H\Big\}$$

as a function of D and H?

In order to produce an upper bound for this number, we want to construct good algebraic approximations to θ. The idea is to extract from the polynomial $f \in \mathbb{Z}[X]$, which has been produced by Dirichlet's pigeonhole principle, a root at minimal distance from θ. From this argument one might expect that there is a constant $c(\theta) > 0$ such that the inequality

$$|\theta - \alpha| < H^{-cD}$$

has a solution α of degree $\leq D$ and naïve height $\leq H$, at least for *many* values of (D, H). In 1961, E. Wirsing proved such a statement:

Theorem 7. (Wirsing) – *Fix a complex transcendental number θ, an integer $D \geq 2$ and a positive real number ϵ. Then there are infinitely many $\alpha \in \overline{\mathbb{Q}}$ with $\mathrm{d}(\alpha) \leq D$ such that*

$$|\theta - \alpha| \leq \mathrm{H}(\alpha)^{-1-(D/4)+\epsilon}.$$

It has been noticed by A. Durand that Wirsing's Theorem yields the following criterion for a complex number to be transcendental: *A complex number θ is transcendental if and only if there exists a sequence $(\alpha_n)_{n\geq 0}$ of pairwise distinct algebraic numbers satisfying $0 < |\theta - \alpha_n| < 1$ for all $n \geq 0$ and*

$$\lim_{n\to\infty} \frac{\mathrm{t}(\alpha_n)}{\log|\theta - \alpha_n|} = 0.$$

A sharpening of Wirsing's Theorem has been achieved by Davenport and Schmidt in 1967 for quadratic approximations ($D = 2$). In the case of real numbers, they prove: *For any real θ which is not rational nor quadratic irrational, there is a constant $C > 0$ such that the inequality*

$$|\theta - \alpha| < C\mathrm{H}(\alpha)^{-3}$$

has infinitely many solutions in rational or real algebraic irrationals α. More recently, Kiril Tishchenko [15] has obtained a refinement of Wirsing's Theorem 7 for $D \leq 10$.

Another similar result has been proved by A. Durand in 1978.

Theorem 8. (Durand) – *For any transcendental number θ, there exists $c > 0$ such that, for any $T \geq 2400$, there is an algebraic number α satisfying $\mathrm{t}(\alpha) \leq T$ and*

$$|\theta - \alpha| \leq ce^{-T\mathrm{t}(\alpha)/80}.$$

Here is a new result of M. Laurent and D. Roy (Theorem 6 of [4]) which contains (up to the actual values of the numerical constants) both results of Wirsing and Durand.

Theorem 9. (Laurent-Roy) – *For any transcendental number θ, there exists a positive constant D_0 such that, for any $D \geq D_0$ and any $H \geq e^D$, there exists an algebraic number $\alpha \in \overline{\mathbb{Q}}$ of degree $\mathrm{d}(\alpha) \leq D$ and naïve height $\mathrm{H}(\alpha) \leq H$ satisfying*

$$|\theta - \alpha| \leq \mathrm{H}(\alpha)^{-cD} H^{-c\mathrm{d}(\alpha)}$$

with $c = 10^{-5}$.

For a fixed $D \geq D_0$, this yields a weak variant of Wirsing's Theorem 6, with 1/4 replaced by a smaller constant. For $D = [\log H]$, Theorem 9 implies a version of Durand's Theorem 8, again with a weaker absolute constant.

Diophantine approximation with the absolute logarithmic height

From now on we consider the problem of approximating θ by algebraic numbers α in terms of the *absolute logarithmic height*:

$$\mathrm{h}(\alpha) = \frac{1}{\mathrm{d}(\alpha)} \log \mathrm{M}(\alpha),$$

where $\mathrm{M}(\alpha)$ is *Mahler's measure* of α, which we now define. For a nonzero polynomial $f \in \mathbb{C}[X]$ one defines *Mahler's measure* $\mathrm{M}(f)$ by

$$\mathrm{M}(f) = \exp\left(\int_0^1 \log|f(e^{2i\pi t})|dt\right).$$

For an algebraic number α with minimal polynomial $A \in \mathbb{Z}[X]$, put $\mathrm{M}(\alpha) = \mathrm{M}(A)$.

Using Jensen's formula, one easily checks that for a polynomial $f \in \mathbb{C}[X]$ of degree d, leading coefficient a_0 and complex roots $\alpha_1, \ldots, \alpha_d$,

$$\mathrm{M}(f) = |a_0| \prod_{i=1}^{d} \max\{1, |\alpha_i|\}.$$

Mahler's measure of f is related to the naïve height of f by

$$2^{-d}\mathrm{H}(f) \leq \mathrm{M}(f) \leq \sqrt{d+1} \cdot \mathrm{H}(f).$$

One deduces from Dirichlet's box principle the following variant of Lemma 6: *Let θ be a complex number. There exists a positive integer D_0 such that, for any $D \geq D_0$ and* *any* $\mu \geq D$, *there is a nonzero polynomial* $f \in \mathbb{Z}[X]$ *of degree* $\leq D$ *and Mahler's measure* $\mathrm{M}(f) \leq e^{\mu}$ *such that*

$$|f(\theta)| \leq e^{-D\mu/4}.$$

From the inequalities relating $\mathrm{M}(f)$ and $\mathrm{H}(f)$ one deduces, for any $\alpha \in \overline{\mathbb{Q}}$,

$$-\log 2 \leq \mathrm{h}(\alpha) - \frac{1}{\mathrm{d}(\alpha)} \log \mathrm{H}(\alpha) \leq \frac{1}{2d} \log(d+1) \leq \frac{1}{2} \log 2.$$

In spite of these estimates, the results we are interested in are sensitive with the choice of the height. For instance, given positive numbers d and H, consider the set $E_{d,H}$ of algebraic numbers of degree $\leq d$ and naïve height $\leq H$ and the set $E'_{d,H}$ of algebraic numbers of degree $\leq d$ and logarithmic height $\leq \log H$; then nothing better than the inclusions

$$E_{d,H/2} \subset E'_{d,H} \subset E_{d,(2H)^d}$$

holds.

A refinement of Theorem 9 has been obtained by G. Diaz [2]: *For any transcendental number* θ, *any* $D \geq 50$ *and any* $M \geq \max\{1 + D, (4 + |\theta|)^{100}\}$, *there exists an algebraic number* $\alpha \in \overline{\mathbb{Q}}$ *of degree* $\mathrm{d}(\alpha) \leq D$ *and Mahler's measure* $\mathrm{M}(\alpha) \leq M$ *satisfying*

$$|\theta - \alpha| \leq \mathrm{M}(\alpha)^{-cD} M^{-c\mathrm{d}(\alpha)}$$

with $c = 6 \cdot 10^{-3}$. Theorem 9 follows from this statement, but not conversely: using Theorem 9 one would need a lower bound for M/e^D in place of a lower bound for M/D in order to deduce Diaz' conclusion.

In terms of the absolute logarithmic height, Liouville's inequality (compare with Lemma 4) reads as follows: *Let* $f \in \mathbb{Z}[X]$ *be a polynomial of degree* $\leq D$ *and length* $\leq L$. *Let* θ *be an algebraic number of degree* $\mathrm{d}(\theta)$ *and absolute logarithmic height* $\mathrm{h}(\theta)$. *Assume* $f(\theta) \neq 0$. *Then*

$$|f(\theta)| \geq L^{1-d(\theta)} \exp\bigl\{-D\mathrm{d}(\theta)\mathrm{h}(\theta)\bigr\}.$$

Another example of a Liouville inequality is the following: *For* θ *and* γ *algebraic numbers with* $\theta \neq \gamma$,

$$|\theta - \gamma| \geq \exp\bigl\{-c(\theta)\mathrm{d}(\gamma)\mathrm{h}(\gamma)\bigr\}$$

with

$$c(\theta) = 2\mathrm{d}(\theta) \max\bigl\{1, \mathrm{h}(\theta) + \log 2\bigr\}.$$

Definition. Let θ be a complex number. An *approximation measure* for θ is a mapping

$$\varphi : \mathbb{N} \times \mathbb{R}_+ \longrightarrow \mathbb{R}_+ \cup \{\infty\}$$

such that there exist $D_0 \geq 1$ and $h_0 \geq 1$ with the following property: for all $D \geq D_0$, all $h \geq h_0$, and all $\gamma \in \overline{\mathbb{Q}}$ satisfying $\mathrm{d}(\gamma) \leq D$ as well as $\mathrm{h}(\gamma) \leq h$, we have

$$|\theta - \gamma| \geq \exp\bigl\{-\varphi(D, h)\bigr\}.$$

Remark. The value ∞ has been included only for the case where θ is algebraic. If θ is transcendental, then such an approximation measure exists and is finite. This follows from the fact that any set of algebraic numbers with bounded degree and bounded height is finite.

Examples (following [8]). An approximation measure for the number π is

$$1.3 \cdot 10^6 D^2 (h + \log D) \log D.$$

For θ a nonzero logarithm of an algebraic number, that means for algebraic $\alpha = e^{\theta}$, an approximation measure is

$$cD^3(h + \log D)(\log D)^{-1} \quad \text{with} \quad c = 3.2 \cdot 10^5 \cdot \max\bigl\{1, |\theta|, \mathrm{h}(\alpha)\bigr\}.$$

Similarly, an approximation measure for e^{β}, when β is a nonzero algebraic number, is

$$cD^2 h(\log h + D \log D)(\log h + \log D)^{-1} \quad \text{with} \quad c = 2.2 \cdot 10^5 \cdot \max\{1, |\beta|\}.$$

From an approximation measure one obtains a measure of irrationality (notice the condition $\mathrm{d}(\gamma) \leq D$ on the degree of γ in the definition of an approximation measure). For instance the above mentioned approximation measure for logarithms of algebraic numbers includes the estimate

$$\left| \pi - \frac{p}{q} \right| \geq q^{-c}$$

for all $p/q \in \mathbb{Q}$ with $q \geq 2$, for some absolute constant $c > 0$. Incidentally, the best known constant c for which this estimate holds is due to M. Hata: $c = 8.0161$, but this is not obtained as a special case of an approximation measure. In such an irrationality measure, it is known that one cannot expect a constant less than 2 (box principle again!).

More generally, *how good can an approximation measure be*? It is expected (loosely speaking) that a function like cD^2h is best possible. Here is a partial result in this direction (Theorem 3.2 of [13]).

Theorem 10. *(Roy-Waldschmidt) – If* θ *is a transcendental number and* φ *an approximation measure for* θ, *then for any sufficiently large* h,

$$\limsup_{D \to \infty} \frac{1}{D^2} \varphi(D, h) \geq 10^{-7} h.$$

The idea of the proof is to start with a nonzero polynomial $f \in \mathbb{Z}[X]$ given by Lemma 6 satisfying

$$\deg f \leq D, \quad \log \mathrm{M}(f) \leq 10^{-5} Dh \quad \text{and} \quad |f(\theta)| < e^{-10^{-7} D^2 h}.$$

Denote by $Z(f)$ the set of zeroes in $\mathbb{C}$ of f and by $\mathrm{dist}\bigl(\theta, Z(f)\bigr)$ the distance of θ to this set:

$$\mathrm{dist}\bigl(\theta, Z(f)\bigr) = \min_{\zeta \in Z(f)} |\theta - \zeta|.$$

We claim that, for infinitely many D's, we have $\deg f \geq 10^{-4}D$ and $\mathrm{dist}\big(\theta, Z(f)\big) < e^{-10^{-7}D^2h}$. If so, we deduce

$$\mathrm{h}(\alpha) \leq \frac{1}{\deg f}\log \mathrm{M}(f) \leq h \quad \text{and} \quad |\theta-\alpha| < e^{-10^{-7}D^2h}$$

for some element α in $Z(f)$. The main tool for the proof of our claim is the resultant $R(F,G)$ of two polynomials F and G in $\mathbb{C}[X]$, which enables one to prove the next result (proposition 3.5 of [13]).

Proposition 11. – *Let θ be a complex number. Further, let F, G be two non-constant polynomials in $\mathbb{C}[X]$, with leading coefficients of absolute value ≥ 1. Furthermore, let m, n be two positive integers with $m \geq \deg F$ and $n \geq \deg G$. Define*

$$\varrho = \mathrm{dist}\big(\theta, Z(F)\cup Z(G)\big).$$

Then, for any integer $s \geq 0$,

$$\min\big\{1, \varrho^{s^2/4}\big\}|R(F,G)| \leq 2^{mn}\mathrm{M}(F)^n\mathrm{M}(G)^m \max\big\{|F(\theta)|, G(\theta)|\big\}^s.$$

Simultaneous approximation

The definition of an approximation measure involves a single complex number θ. We consider a similar situation were several complex numbers are involved. For a measure of irrationality, one natural and classical extension is to consider simultaneous rational approximations: given real numbers $\theta_1,\ldots,\theta_m$ and rational numbers $p_1/q,\ldots,p_m/q$, one wish to estimate from below the quantity

$$\max_{1\leq i\leq m}\left|\theta_i - \frac{p_i}{q}\right|.$$

The point is that the approximations $p_i/q \in \mathbb{Q}$ have the same denominator q (it is not assumed that the rational numbers p_i/q are reduced).

Our point of view here is quite different: we are interested with approximations of the θ's (which are now complex numbers) by algebraic numbers of potentially large degree. More precisely we consider algebraic numbers $\gamma_1,\ldots,\gamma_m$, of degrees $\mathrm{d}(\gamma_i)$ bounded by a large number, and we are interested with $\max_{1\leq i\leq m}|\theta_i-\gamma_i|$. We could ask also for a bound for the projective point $(1:\gamma_1:\cdots:\gamma_m)$, which would entail some simultaneous condition generalizing the situation of simultaneous rational approximation. However it turns out that, for our purpose, there is no need to use the logarithmic height on projective spaces. The difference with what we are going to do would be only on the constant terms, which we do not care about. Here, the simultaneous condition will be on the degree: in place of an upper bound for each degree $\mathrm{d}(\gamma_i)$, we ask for an upper bound for the degree of the field generated by $\gamma_1,\ldots,\gamma_m$.

Definition. Let $\theta_1,\ldots,\theta_m$ be complex numbers. A map

$$\varphi : \mathbb{N}\times\mathbb{R}_+ \longrightarrow \mathbb{R}_+\cup\{\infty\}$$

is a *measure of simultaneous approximation* for $(\theta_1,\ldots,\theta_m)$ if there exist $D_0 \geq 1$ and $h_0 \geq 1$ such that, for any $D \geq D_0$, any $h \geq h_0$, and any $(\gamma_1,\ldots,\gamma_m) \in \overline{\mathbb{Q}}^m$ satisfying

$$[\mathbb{Q}(\gamma_1,\ldots,\gamma_m):\mathbb{Q}] \leq D \quad \text{and} \quad \max_{1\leq i\leq m}\mathrm{h}(\gamma_i) \leq h,$$

we have

$$\max_{1\leq i\leq m}|\theta_i-\gamma_i| \geq \exp\big\{-\varphi(D,h)\big\}.$$

Remark. If $\theta_1,\ldots,\theta_m$ are not all algebraic, then such a measure of simultaneous approximation exists and is finite (viz. with values in $\mathbb{R}_+$).

Example. According to N.I. Feldman, if $\log\alpha_1,\ldots,\log\alpha_m$ are $\mathbb{Q}$-linearly independent logarithms of algebraic numbers, then there exists $c > 0$ such that

$$cD^{2+(1/m)}(h+\log D)(\log D)^{-1}$$

is a measure of simultaneous approximation for $(\log\alpha_1,\ldots,\log\alpha_m)$.

Here is the first connection between a measure of simultaneous approximation and algebraic independence of two numbers (Corollary 1.2 of [13]).

Theorem 12. *(Roy-Waldschmidt) – Let $\theta_1,\ldots,\theta_m$ be complex numbers and let $\varphi(D,h)$ be a measure of simultaneous approximation. Assume that, for all sufficiently large h,*

$$\frac{1}{D^2}\varphi(D,h) \longrightarrow 0 \qquad \text{as } D\to\infty.$$

Then two at least of the number $\theta_1,\ldots,\theta_m$ are algebraically independent.

A more general result has recently been achieved by M. Laurent and D. Roy [5]:

Theorem 13. *(Laurent-Roy) – Let $\theta_1,\ldots,\theta_m$ be complex numbers such that the field $\mathbb{Q}(\theta_1,\ldots,\theta_m)$ has transcendence degree 1 over $\mathbb{Q}$. There exist three effectively computable positive numbers c_0, c_1 and c_2 satisfying the following property. Let $(d_n)_{n\geq 0}$ be a sequence of positive integers and $(h_n)_{n\geq 0}$ a sequence of positive real numbers with*

$$c_0 \leq d_n \leq d_{n+1} \leq 2d_n, \quad c_0 \leq h_n \leq h_{n+1} \leq 2h_n \quad \text{and} \quad \lim_{n\to\infty} d_nh_n = \infty.$$

Then, for infinitely many $n \geq 0$, there exists $(\gamma_1,\ldots,\gamma_m) \in \overline{\mathbb{Q}}^m$ such that

$$c_1d_n \leq [\mathbb{Q}(\gamma_1,\ldots,\gamma_m):\mathbb{Q}] \leq d_n, \quad \max_{1\leq i\leq m}\mathrm{h}(\gamma_i) \leq h_n,$$

and

$$\max_{1\leq i\leq m}|\theta_i-\gamma_i| \leq \exp\big\{-c_2d_n^2h_n\big\}.$$

Therefore, under the assumptions of Theorem 13, if $\varphi(D,h)$ is a measure of simultaneous approximation for $(\theta_1,\ldots,\theta_m)$, then for infinitely many n,

$$\varphi(d_n,h_n) \geq c_2d_n^2h_n.$$

However it is a remarquable feature of Theorem 13 that it tells more: it also includes a lower bound for the degree of the field $\mathbb{Q}(\gamma_1,\ldots,\gamma_m)$.

The key lemma for the proof of Theorem 13 is the following:

Lemma 14. *(Laurent-Roy) – Let d be an integer and μ, b real numbers satisfying*

$$0 < b \le 1/4, \quad 0 < d \le \mu, \quad 21 \le b^2 d\mu.$$

Suppose that there exist three non zero polynomials P_1, P_2, P_3 in $\mathbb{Z}[X]$, which are pairwise relatively prime, such that, for $i = 1, 2, 3$,

$$\deg P_i \le d, \quad \log \mathrm{M}(P_i) \le \mu, \quad \log |P_i(\theta)| \le -bd\mu.$$

Then there is a zero α of the product $P_1P_2P_3$ which satisfies

$$(b^2/9)d \le [\mathbb{Q}(\alpha) : \mathbb{Q}] \le d, \quad \log \mathrm{M}(\alpha) \le \mu, \quad \log |\theta - \alpha| \le -(b^2/3)d\mu.$$

For the proof of Theorem 13, arguing by contradiction, it is not difficult to produce two relatively prime polynomials, say P_1 and P_2, with sharp upper bounds for the degree, for Mahler's measure as well as for the values at a point θ. However Lemma 14 requires three such polynomials. The trick of [5] is to introduce the polynomial $P_3 = P_1 + P_2$.

Algebraic independence

After the construction by Liouville of transcendental numbers in 1844 came the work of Hermite in 1873 (transcendence of e) and of Lindemann in 1882 (transcendence of π) which gave rise to the so-called *Theorem of Hermite-Lindemann: For any nonzero algebraic number β, the number e^β is transcendental.* Another equivalent formulation is: *For any non-zero algebraic number α and any nonzero value $\log\alpha$ of its logarithm, the number $\log\alpha$ is transcendental.*

Historically, the next result is the *Theorem of Lindemann-Weierstraß*: *If $\beta_1, \ldots, \beta_m$ are $\mathbb{Q}$-linearly independent algebraic numbers, $e^{\beta_1}, \ldots, e^{\beta_m}$ are algebraically independent.* This means that if $P \in \mathbb{Z}[X_1, \ldots, X_m]$ is a nonzero polynomial, then $P(e^{\beta_1}, \ldots, e^{\beta_m})$ does not vanish.

When K is a subfield of $\mathbb{C}$, the *transcendence degree* of K over $\mathbb{Q}$ is the maximal number of elements in K which are algebraically independent over $\mathbb{Q}$. If L is an algebraic extension of K (which means that any element in L is algebraic over K), then K and L have the same transcendence degree over K. A field of transcendence degree 0 is nothing else than an algebraic extension of $\mathbb{Q}$. Hence the field of algebraic numbers $\overline{\mathbb{Q}}$ is the maximal subfield of $\mathbb{C}$ with transcendence degree 0.

If $\theta_1, \ldots, \theta_m$ are algebraically independent over $\mathbb{Q}$, then they are algebraically independent over $\overline{\mathbb{Q}}$ and for any non-constant polynomial $f \in \overline{\mathbb{Q}}[X_1, \ldots, X_m]$, the number $f(\theta_1, \ldots, \theta_m)$ is transcendental.

A well known open problem is the algebraic independence of e and π. We do not know whether $e + \pi$ is rational, or algebraic irrational, or else is transcendental (it is expected that the later is the truth). However it is easy to deduce from either the transcendence of e or from the transcendence of π that the complex number $e + \pi + ie\pi$ is transcendental!

It is not known whether the number π^e is transcendental. But it is known for e^π (Gel'fond, 1929). It is a consequence of the solution, by *Gel'fond and Schneider* (1934),

of Hilbert's seventh problem: *For α a nonzero algebraic number, $\log\alpha$ a nonzero value for its logarithm, and β an irrational algebraic number, the number $\alpha^\beta = \exp(\beta\log\alpha)$ is transcendental.* For instance $2^{\sqrt{2}}$ (take $\alpha = 2$, $\beta = \sqrt{2}$) and e^π (take $\alpha = 1$, $\log\alpha = 2i\pi$, $\beta = -i/2$) are transcendental, as well as $(\log 2)/(\log 3)$ (take $\alpha = 3$, $\beta = (\log 2)/(\log 3)$, so that $\alpha^\beta = 2$).

In 1996, Yu.V. Nesterenko [6], [7] ((see also [3], [9], [10], [16], [17]) proved that the two numbers π and e^π are algebraically independent. His proof actually shows a stronger statement:

Theorem 15. *(Nesterenko) – The three numbers π, e^π and $\Gamma(1/4)$ are algebraically independent.*

The algebraic independence of π and $\Gamma(1/4)$ was already known (Chudnovsky, 1976). One main tool in Nesterenko's proof is the use of modular functions, and more precisely of Eisenstein series (cf. Kuznetsov's lectures). The recent proof by K. Barré-Sirieix, G. Diaz, F. Gramain and G. Philibert [1] of the transcendence of $J(q)$ for algebraic q with $0 < |q| < 1$ gave the impetus to Nesterenko's work (see [6]).

The first connection between these results of algebraic independence and simultaneous approximation estimates arose as follows [14]:

Theorem 16. *(Roy-Waldschmidt) – A measure of simultaneous approximation for π and $\Gamma(1/4)$ is $cD^{3/2}(h + \log D)^{3/2}$.*

For fixed h, this function is $o(D^2)$, hence Theorem 12 implies Chudnovsky's above mentioned statement: *the field $\mathbb{Q}(\pi, \Gamma(1/4))$ has transcendence degree 2 over $\mathbb{Q}$.*

For the three numbers π, e^π, $\Gamma(1/4)$, a measure of simultaneous approximation has been worked out by P. Philippon [9] who gets $c(\epsilon)(Dh)^{(4/3)+\epsilon}$. For fixed h, this is $o(D^{3/2})$. Philippon deduces the algebraic independence of these three numbers by means of an extension of his own of Theorem 12 [11]. More generally, one expects that the following should hold.

Conjecture 17. *Let $\theta_1, \ldots, \theta_m$ be complex numbers, t be the transcendence degree over $\mathbb{Q}$ of the field $\mathbb{Q}(\theta_1, \ldots, \theta_m)$ and $\varphi(D, h)$ be a measure of simultaneous approximation for $(\theta_1, \ldots, \theta_m)$. Then*

$$\limsup_{h\to\infty} \frac{1}{h} \limsup_{D\to\infty} \frac{1}{D^{1+(1/t)}} \varphi(D, h) > 0$$

and

$$\limsup_{D\to\infty} \frac{1}{D^{1+(1/t)}} \limsup_{h\to\infty} \frac{1}{h} \varphi(D, h) > 0.$$

This conjecture would also include the Lindemann-Weierstraß Theorem, because the following measure of simultaneous approximation for $e^{\beta_1}, \ldots, e^{\beta_m}$ when $\beta_1, \ldots, \beta_m$ are $\mathbb{Q}$-linearly independent algebraic numbers (see [14]):

$$\varphi(D, h) = cD^{1+(1/m)} h(\log h + D\log D)(\log h + \log D)^{-1}$$

satisfies

$$\limsup_{D\to\infty} \frac{1}{D^{m/(m-1)}} \limsup_{h\to\infty} \frac{1}{h} \varphi(D, h) = 0.$$

References

We provide a short list including only very recent references on this topic. Further information on this subject will be found in these papers.

[1] K. BARRÉ-SIRIEIX, G. DIAZ, F. GRAMAIN, G. PHILIBERT - *Une preuve de la conjecture de Mahler-Manin*, Invent. Math. **124** (1996), 1–9.

[2] G. DIAZ - *Une nouvelle propriété d'approximation diophantienne*, C. R. Acad. Sc. Paris, Sér. I **324** (1997), 969–972.

[3] M. LAURENT - *New methods in algebraic independence*, in "Number Theory – Diophantine, Computational and Algebraic Aspects", K.Gyory, A.Petho and V.T.Sos, eds., Proc. Conf. Number Theory Eger 1996, W. de Gruyter, to appear.

[4] M. LAURENT and D. ROY - *Criteria of algebraic independence with multiplicities and interpolation determinants*, Trans. Amer. Math. Soc, to appear.

[5] M. LAURENT and D. ROY - *Sur l'approximation d'un nombre complexe transcendant par des nombres algébriques*, in preparation.

[6] Yu.V. NESTERENKO - *Modular functions and transcendence problems*, C. R. Acad. Sc. Paris, Sér. 1 **322** (1996), 909–914.

[7] Yu.V. NESTERENKO - *Modular functions and transcendence questions*, Mat. Sb., **187** N° 9 (1996), 65–96. Engl. Transl., Sbornik Math., **187** N° 9-10 (1996), 1319–1348.

[8] Yu.V. NESTERENKO and M. WALDSCHMIDT - On the approximation of the values of exponential function and logarithm by algebraic numbers; (en russe) Mat. Zapiski, **2** *Diophantine approximations, Proceedings of papers dedicated to the memory of Prof. N. I. Feldman*, ed. Yu. V. Nesterenko, Centre for applied research under Mech.-Math. Faculty of MSU, Moscow (1996), 23–42.

[9] P. PHILIPPON - *Indépendance algébrique et K-fonctions*, J. reine angew. Math., to appear; Prépublication Inst. Math. Jussieu **71** (1996).

[10] P. PHILIPPON - *Une approche méthodique pour la transcendance et l'indépendance algébrique de valeurs de fonctions analytiques*, J. Number Theory, **64** (1997), 291-338.

[11] P. PHILIPPON - *Approximations algébriques des points dans les espaces projectifs*, J. Number Theory, to appear.

[12] D. ROY and M.WALDSCHMIDT - *Quadratic relations between logarithms of algebraic numbers*, Proc. Japan Acad. Ser. A Math. Sci. **71** (1995), 151–153.

[13] D. ROY and M.WALDSCHMIDT - *Approximation diophantienne et indépendance algébrique de logarithmes*, Ann. scient. Ec. Norm. Sup., 4ème Sér., **30** (1997), à paraître (44 pp.).

[14] D. ROY and M.WALDSCHMIDT - *Simultaneous Approximation and Algebraic Independence*, The Ramanujan Journal, **1** fasc. 4 (1997), 379–430.

[15] K. TISHCHENKO - *Approximation of real numbers by algebraic integers of degree* ≤ 10, The international conference on Diophantine analysis and its applications in honour of Acad. Sprindžuk, Sept. 1-8, 1996, Minsk (Belarus).

[16] M. WALDSCHMIDT - *Sur la nature arithmétique des valeurs de fonctions modulaires*, Sém. Bourbaki 49ème année (1996/97), N° 824, 37pp.; to appear in Astérisque (Soc. Math. Fr.).

[17] M. WALDSCHMIDT - *Transcendance et indépendance algébrique de valeurs de fonctions modulaires*, Proceedings of the Fifth Conference of the Canadian Number Theory Association, Carleton, August 1996; éd.: Rajiv Gupta et Kenneth Williams, à paraître.

Michel Waldschmidt
Université P. et M. Curie (Paris VI)
Institut Mathématique de Jussieu
Problèmes Diophantiens, Case 247
4, Place Jussieu
F – 75252 PARIS CEDEX 05
FRANCE
e-mail: miw@math.jussieu.fr
internet: http://www.math.jussieu.fr/~miw